연구보고 2016-06

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

김 현 희

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

연구보고 2016-06

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

김 현 희

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

생체정보의 활용 및 보호를 위한 법제 정비방안 연구

A Study on Reforming Laws Pertaining to the Use and Protection of Biometric Data

연구자 : 김현희(연구위원)
Kim, Hyun-Hee

2016. 10. 31.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

요 약 문

Ⅰ. 배경 및 목적

□ 사회적 관계에서 내가 누구인지를 알리고, 내가 정당한 권한을 가졌다는 것을 알려야 하는 상황은 매우 빈번하게 발생하며, 이를 확인하는 수단으로 오래 전부터 지문이나 비밀번호 등이 사용되어 왔음

□ 최근 과학기술과 정보통신기술의 발전을 토대로 새로운 인증방식과 인증기술로 등장한 지문인식, 홍채인식, 안면인식, 음성인식 등의 생체정보라 할 수 있음

□ 생체정보는 편리함으로 그 활용분야가 점차 확대되고 있으며 특히 최근에는 전자금융거래 등에서 적극 도입되고 있음

□ 이러한 활용분야의 확대에도 불구하고 우리 법제에서는 생체정보에 관하여 고유의 체계를 인정받지 못하고 있기에 이에 관한 법제 정비방안을 제안하고자 함

Ⅱ. 주요 내용

□ 생체정보의 의의

○ 사람의 고유한 신체적, 행동적 특징을 이용하여 개인의 신원을 확인할 수 있게 하는 정보로서, 지문, 홍채, 망막, 정맥패턴, 얼

굴, 음성, 서명패턴 등 개인을 직접 나타내는 정보를 말함. 생체정보는 개인을 인식하거나 인증하기 위한 목적을 가진 “생체인식정보”로 파악하는 것이 필요함

○ 생체정보는 만인부동, 평생불변이라는 특성과 함께 언제 어디서나 쉽고 편리하게 사용할 수 있다는 점에서 강점과 위험을 모두 가지고 있음

□ 생체정보의 활용현황

○ 생체정보를 통하여 본인을 인식하고 인증하는 사례는 일상적인 영역에서부터 특수한 분야에 이르기까지 다양하게 찾을 수 있음

○ 금융분야에서는 본인확인을 위한 전자적 인증수단으로서 이용자의 생체정보를 활용하고 있는데, 최근 비대면 거래의 활성화로 인하여 앞으로 확대 사용될 가능성이 높음

○ 의료 및 헬스케어분야에서는 긴급의료, 의료기기용 앱, 모바일 등에서 생체정보를 활용하고 있는데, 이것이 본인인증이나 본인식별을 위한 목적으로 사용되는 것이 아니어서 의료(건강)정보와의 관계에서 대부분의 생체정보는 제외되겠지만 앞으로 원격의료가 본격적으로 도입되는 경우 그 규율에 문제가 발생할 수 있음

○ 범죄수사분야에서는 오래전부터 과학수사의 일환으로 혈액이나 DNA, 걸음걸이 등 생체정보가 활용되어 왔는데, 기본권 침해여부의 문제와는 별도로 본인인식이나 본인인증을 위한 목적으로 사용하는 생체정보로 보기에는 어려움이 있음

□ 생체정보 관련 법제

○ 생체정보에 관한 법령은 활용 분야에 따라 다양하게 분류할 수 있으나 아직 우리 법령이 생체정보에 관한 고유의 통일된 규율 체계를 가지지 못하였기 때문에 개인정보의 틀 속에서 파악할 수밖에 없는 한계가 있음

○ 생체정보가 민감정보라고 보기에도 어려운 면이 있음

○ 생체정보를 명시적으로 언급한 경우로는「전자금융거래법」상의 "생체정보",「전자통신망법」시행령 상의 "바이오정보",「전자서명법」상의 "생체특성에 관한 정보" 정도를 들 수 있음

○ 이들 법령이 생체정보의 개념을 인정하였다고 하여 그 특유의 보호체계를 갖춘 것은 아니며, 생체정보의 보호에 관하여는 여전히「개인정보보호법」상의 일련의 보호조치가 적용되는 것으로 볼 수 있음

□ 주요 외국의 생체정보 관련 법제

○ 생체정보의 개념을 명시적으로 언급하고 그 규율체계를 기존의 개인정보와 별도로 정하고 있는 국가는 아직 존재하지 않는 것으로 보임. 외국의 입법례는 그 국가에서 그것을 활용하는 분야가 발전한 정도에 따라 규율의 밀도가 달라지는 것으로 파악됨

○ 유럽연합은 1995년「개인정보지침」을 2016년「개인정보보호규칙」으로 대체하면서 적용대상을 확대하고 다양한 정보처리의 원칙과 정보보호조치를 강화하였음. 여기에는 생체정보의 개념 등도 포함되었음

○ 독일에서는 공공분야, 즉 테러 등 국가안보와 관련된 다수의 분야에서 지문 등의 생체정보를 활용하고 그에 대한 안전한 사용을 정하고 있음

○ 미국에서는 민간분야, 특히 금융산업과 관련한 연방 법률에서 생체정보를 언급하고 있으나 아직 포괄적 규율체계는 없고, 일부 주법에서 프라이버시보호와 관련하여 생체정보의 개념과 범위, 보호체계를 명시한 것으로 파악됨

○ 일본에서는 아직 생체정보를 법령에서 도입하지 않고 개인정보의 하나로 파악하고 개인정보 보호체계를 적용하고 있는 것으로 보임

□ 법제 정비방안

○ 생체정보의 개념과 용어를 명확하게 통일하는 것이 필요하며, 그 규율체계를 설계함에 있어서는 일반법인 개인정보보호법에 개인정보, 민감정보와는 별개의 생체정보 규정을 둘 것인가, 생체정보를 적용하는 다수의 개별법에 별도의 조문을 둘 것인가, 아니면 생체정보에 관한 자기완결적 법률을 둘 것인가에 대한 선택이 필요함

○ 생체정보는 생체원본정보와 생체인식정보로 구별되어야 하는데, 생체원본정보의 경우 도난이나 위조가 되는 경우 회복이 불가능하기 때문에 가급적 원본정보를 저장하지 않도록 하며, 저장 또는 송수신하게 되는 경우 반드시 비식별화할 필요가 있음

○ 생체정보는 일반적인 개인정보 식별자와는 다르며, 민감정보라고 단정하기에도 어렵기 때문에 고유의 보호조치가 필요하며, 가장 기본적인 것은 법령 등에 최소한의 기술적·물리적·관리

적 보호조치에 관한 사항을 규정하는 것이 필요하며, 그 외에 정보처리자의 의무를 강화하고 정보주체의 동의절차를 보다 실효적으로 구성할 필요가 있음

○ 생체인식 기반 본인확인서비스의 안전성과 신뢰성 확보를 위해 일원화된 관리·감독 체계와 인증제도를 도입할 필요가 있음

○ 중요한 생체정보인 유전자정보는 어떠한 경우에도 비식별조치가 되어야 하며, 유전자정보가 해외로 유출되는 것을 막기 위해 원칙적으로 국외이전을 금지하거나 엄격히 제한하여야 할 필요가 있음

Ⅲ. 기대효과

□ 생체정보의 법제 정비방안에 관한 연구는 그동안 단편적으로 이루어져 왔던 개별법적 관점에서의 논의를 종합함으로써 법체계적 정합성을 유지하고 추후 법령 개정 시 참고할 수 있는 기초자료로서 활용될 수 있을 것으로 기대함

□ 특히 정부에서 수립하려고 하는 「바이오정보보호 가이드라인」을 발전시키거나 이를 법제화하고자 하는 때에 참고자료가 될 수 있음

주제어 : 생체정보(바이오정보), 생체인식정보, 생체원본정보, 개인정보, 민감정보

Abstract

Ⅰ. Background and Purpose

□ Having to verify one's identity or provide evidence of an entitlement is a situation we all face routinely. Traditionally, fingerprints and identification numbers or passwords have been the main means used for this purpose.

□ In recent years, new types of authentication methods have emerged, aided by technological progress. Authentication technologies such as fingerprint, iris, face and voice recognition are all based on biometric data.

□ Due to the relative ease of use, biometrics has become increasingly prevalent in a growing number of fields. Notably, there is an accelerating trend toward the integration of biometric recognition technologies into electronic banking systems.

□ In spite of the heightened prevalence of biometrics, currently, there exists no specific regulatory mechanism overseeing the use of biometric data within the Korean legal system. Thus, the goal of this study is to fill such a vacuum by providing

suggestions on how to build a legal framework for the protection of biometric information.

Ⅱ. Main Contents

□ Definition and Purpose of Biometrics

○ Biometric data are information based on physiological and behavioral characteristics of a person, used for the purpose of verification of identity. They are information that directly identifies a person, such as fingerprints, iris, retina and artery patterns, facial features, voice and signature patterns. Biometric data are, in other words, 'biometric recognition data,' allowing the recognition of a person or authentication of his/her identity.

○ Biometric data are unchanging physical characteristics and can be easily acquired and used in most circumstances. These advantages of biometrics are also precisely what makes its use potentially dangerous.

□ Current Utilization of Biometric Data

○ Examples of the use of biometric data for recognition or authentication purposes can be found in wide-ranging contexts, from everyday tasks to more special and less common processes and procedures.

- In banking, biometric data are used for verification of identity, as part of the electronic authentication process. Given the growing prevalence of non-face-to-face transactions, the utilization of biometric data are likely to further increase, going forward.

- In medical and healthcare fields, biometric data are used for the delivery of emergency care, medical device apps and mobile systems. Here, the purpose of using biometric data is not that of verifying or authenticating one's own identity or credentials. For this reason, most typical biometric data are also not relevant in the context of healthcare. However, once telemedicine becomes more widely practiced, this can give rise to complex regulatory and legal issues.

- In criminal investigation, such biometric data as blood type, DNA and gait have long been used as part of biological or behavioral evidence. Aside from privacy concerns this raises, the utilization of biometric data for criminal identification is also rather distinct from their use for the purpose of verifying or authenticating one's own identity or credentials.

□ Laws and Regulations Related to Biometric Data

- While there are various laws applicable to biometric data depending on the context of their use, there exists no separate body of law or set of procedures that explicitly and

comprehensively govern related issues. As a result, biometric data are devoid of a clearly-defined legal status and can only be regulated as part of personal information under the legal framework for privacy.

○ Meanwhile, biometric data cannot necessarily be equated with sensitive personal data.

○ Examples of explicit references to biometric data in existing laws are limited to “biological information” mentioned in the <Electronic Financial Transactions Act>, “bio-metric information” in the enforcement decree to the <Electronic Communications Network Act> and “information regarding biometric characteristics” in the <Digital Signature Act>.”

○ While these references may be interpreted as a legal recognition of the concept of biometric data, the fact remains that a system is yet to be put in place for their protection, which is currently ensured only through a series of provisions under the <Personal Information Protection Act>.

□ Biometrics Laws in Major Countries

○ A regulatory framework in which the concept of biometric data is explicitly defined and is clearly distinguished from personal information in general appears to be lacking in

most countries across the world, at least for the time being. Legislative examples from countries outside Korea suggest that regulatory density depends largely on the stage of development of the fields in which biometric data are utilized.

○ In the EU, the <General Data Protection Regulation> which will replace and supersede the <1995 Data Protection Directive> entered into force in 2016. The Regulation expands the scope of protected data, stipulates stronger protection measures and requires stricter standards for the handling of personal data. The scope of data protected under the new Regulation covers biometric data.

○ In Germany where fingerprints and other biometric data are used in various sectors of government for security initiatives against terrorism and for national defense purposes, there are pre-established guidelines to guarantee their safe utilization.

○ In the US, although biometric data are mentioned in federal laws related to the use of personal data by private-sector businesses, and more particularly, the financial industry, a comprehensive regulatory framework is yet to be established. Some state laws, however, define the concept and scope of biometric data and stipulate the system for their protection.

○ In Japan, there is currently no law on the utilization and protection of biometric data. Biometric data are considered a variety of personal data and are thus regulated through the personal data protection system.

□ Building a Legal Framework for Biometric Data

○ A clear definition of biometric data both as a concept and a term is of paramount importance. In designing a regulatory mechanism, a choice must be made. Either a new set of provisions on biometric data, distinct from those on general or sensitive personal data, would be added to the existing <Personal Information Protection Act> or to each of the individual laws having to do with biometric data. Or a new self-contained law that governs biometric data exclusively must be created.

○ A distinction is needed between original biometric data and biometric recognition data. Storing original biometric data should be avoided as much as possible, as they are not recoverable, if stolen or forged. In situations where they must be stored or transmitted over a network, it is imperative that they be in an anonymized form.

○ Biometric data are unlike general PIN codes and do not necessarily fall into the category of sensitive personal data. They, therefore, require protection measures that are

uniquely and specifically adapted to them. Related rules must include provisions stipulating the minimum required standards for technical, physical and administrative measures toward their protection. Also essential is to strengthen the duties and obligations of those who handle personal data. Moreover, the procedures for obtaining the consent of individuals concerned must be designed in such a way that they are practically valid and effective.

○ To guarantee the safety and reliability of biometric recognition-based identification services, a single, unified system of management and oversight has to be set up, along with an authentication system.

○ Genetic information, given its special importance as biometric data, should be at all times and in any circumstance be anonymized. Also, to prevent genetic information from becoming exported to a country outside Korea, the transfer of this information to a foreign destination must be prohibited a priori or strictly controlled.

Ⅲ. Expected Effect

□ This study is a comprehensive discussion of directions and strategies for the creation of an effective legal framework for the use and protection of biometric data, based on a synthetic

review of existing studies which were most often limited in scope or were concerned with individual laws. The suggestions offered in this study are attentive to the consistency and harmony of the legal system and may serve as reference in future legislative projects.

□ This study can be particularly useful for a project to take the 'Guidelines on the Protection of Biological Information' – set to be established by the Korean government - to the next level or legislate them.

Key Words : Biometrics, Biometric Data/Information, Biometric Sample Data, Original Biometric Data, Personal Data, Sensitive Personal Data

목 차

제 1 장 서 론

제 1 절 연구의 필요성 및 목적

Ⅰ. 연구의 필요성

디지털 정보사회에서 인간은 거의 모든 사회적 관계에서 내가 누구인지를 알리고, 내가 정당한 권한을 가졌다는 것을 알려야 하는 상황에 접하게 된다. 나를 증명하는 정보로 가장 대표적인 것은 아이디나 비밀번호와 같은 각종 암호가 있으며, 공적인 분야서는 외국의 사회보장번호나 우리의 주민등록번호와 같은 독특한 메커니즘도 인정되고 있다. 이렇게 출입국이나 출입통제, 금융결제 등 공공과 민간의 다양한 분야에서 매우 일상적이고 빈번하게 사용되는 각종의 인증수단은 일반적으로 글자나 번호 등 일정한 범위가 정해진 기호로 구성되기 때문에 분실이 되거나 타인에게 노출될 가능성이 매우 크다. 해킹 또는 정보유출로 수많은 개인정보가 노출된 수차례의 사례를 돌이켜 보면 개인정보에 대하여 보호 내지 보안조치가 기술적으로나 제도적으로 더 강화되어야 할 상황에 이른 것이 아닌가 생각된다.

그리하여 오랫동안 사용되어 왔던 기존의 “고전적인” 인증수단의 단점을 극복하고 과학기술과 정보통신기술의 발전을 토대로 새로운 인증방식을 논의하고자 하는 것이 바로 “생체정보”이다. 생체정보는 인간으로서 가지고 있는 각종의 신체적 정보와 행동적 정보로서, 이는 그러한 성격의 정보를 시스템적으로 인식할 수 있는 “생체인식기술”을 기반으로 하는 개인정보를 말한다.[1] 단순하게는 도어락, 무인민원발급기, 출입통제시스템 등의 지문인식으로부터 복잡하게는 첨단의

1) https://ko.wikipedia.org/wiki/%EB%B0%94%EC%9D%B4%EC%98%A4%EB%A9%94%ED%8A%B8%EB%A6%AD%EC%8A%A4

SF영화에 등장하는 바와 같이 홍채인식, DNA인식, 음성인식, 얼굴인식 등에 이르기까지, 현대의 자동화된 IT기술은 기존에는 불가능하게 여겨졌던 영역에서도 생체정보를 일상적으로 사용할 수 있도록 획기적인 발전을 진행 중이다. 이러한 생체정보의 활용은 최근 핀테크(Fin-Tech) 산업의 발전 및 비대면 실명인증제의 도입과 관련하여 정보보안 산업적 측면에서도 큰 관심의 대상이 되고 있다.[2)]

그러나 생체정보는 "생체"라는 용어에서도 느껴지듯이 그 자체로서 개인의 완결적인 정보로서의 성격을 가지기 때문에 그것이 노출되는 경우 비밀번호와 같은 다른 개인정보와 달리 정보주체에 대하여 더 심각한 정신적·재산적 손해를 입힐 수 있다. 따라서 이러한 생체정보를 활용함에 있어서는 매우 정교한 제도적 설계가 뒷받침되어 있어야 하며, 그러한 위험에 이르지 않기 위한 기술적 발전도 필수적으로 선행되거나 병행되어야 한다.

이러한 점에 근거하여 일부 외국에서는 생체정보의 기술발전과 함께 그 제도적 규율에 관한 논의를 계속 진행하고 있는데, 특히 생체정보의 개념과 범위를 구체화하여 입법에 반영하는 등의 동향을 보이고 있으며, 우리의 경우도 2000년대부터 꾸준히 생체정보에 관한 논의를 진행시켜오고 있다. 다만, 괄목할만한 생체인식기술의 진보에도 불구하고 제도적으로는 중요한 쟁점사항에 관하여는 아직 학문적으로나 사회적으로 합의를 이루고 있지 못한 상황이며, 이를 법제화하는 데에도 많은 어려움이 있다. 그럼에도 불구하고 생체정보가 가지는 특수성과 중요성으로 인하여 제도화에 관한 논의는 계속되어야 하며, 일부 쟁점에 관하여는 시급하기까지 하다.

다만, 생체정보는 그 "활용"과 "보호(보안)"에 관한 양 측면 모두에서 논의될 필요가 있는데, 생체정보의 "활용"과 관련하여서는 2008년

2) 심우민, "스마트 시대의 생체정보 보호를 위한 입법과제", 「이슈와 논점」, 국회입법조사처, 제1129호, 2016. 3. 3, 1면.

여권법의 전부개정 시 이슈가 된 이래로 최근 전자금융거래 시 공인인증을 대신하는 본인인증 방식으로서 논의되고 있으며, 빅데이터 환경에 있어서 u-헬스케어(의료기기 등)의 대상정보 기타 범죄수사 등에 있어서 적극적으로 활용되고 있다. 반면에, 생체정보의 "보호"와 관련하여서는 개인의 매우 "개인적이며 민감한" 생체정보가 유출되거나 악용(위・변조) 되는 경우, 정보주체의 법률관계가 심각하게 침해될 수 있기 때문에 생체정보의 수집, 관리, 폐기에 이르는 전 과정을 신중하게 관리하고 보장하기 위한 제도적 보호장치가 강하게 요구되고 있다.

따라서 이러한 생체정보의 활용과 보호에 관한 논의를 진행시킴에 있어서 과연 생체정보가 기존의 다른 개인정보와 어떻게 다르며 양자는 어떠한 관계에 있는지, 기존의 개인정보의 활용 및 보호에 관한 제도만으로는 부족한 것인지, 생체정보에 대한 보호수준 내지 취약성을 극복하기 위한 수단은 어느 정도가 되어야 하는지에 대하여 짚어보아야 한다. 그리고 이러한 논의를 구체적 입법으로 실현함에 있어서는 입법론적으로 생체정보에 대한 개별 법령을 제정하여 그 정의부터 보호에 이르기까지 독자적인 입법체계를 구축하는 것이 필요한지 아니면 기존의 법령의 틀 속에서 개인정보와의 관계를 고려한 일부 개정을 통하여 충분히 해결을 할 수 있는지 등에 관한 문제들을 구체적으로 제시하는 것이 필요한 시점에 와있다고 할 수 있다.

Ⅱ. 연구의 목적

본 연구는 생체정보의 개념과 성격을 정확하게 이해하고, 본인 인증, 헬스서비스, 수사 등 생체정보가 다양하게 활용되고 있는 현황과 그에 관한 법제가 적절하게 규율하고 있는지를 살펴보고, 현행 규범이 가진 문제점과 개선방안을 제시하는 것을 목적으로 한다.

이러한 연구목적은 기존의 개인정보와의 관계 및 개인정보보호의 체계적인 틀과의 관계 속에서 논의되어야 하는 필요가 있는데, 즉 생체정보라는 특수한 성격의 정보에 대한 정의와 유형을 어떻게 정하느냐에 따라 그 수집, 활용 및 보호에 있어서 발생할 수 있는 다양한 법률관계를 규율하는 법령이 정하여 지기 때문이다. 따라서 기존의 법령과의 조화 내지 새로운 체계를 구축하기 위하여 생체정보에 관한 규범을 어떻게 정비하여야 하는지에 대한 구체적인 방안을 제시하고자 한다.

제 2 절 연구의 범위 및 방법

Ⅰ. 연구의 범위

1. 선행연구

가장 대표적인 생체정보라 할 수 있는 지문정보 같은 경우 사실 최근에 이르러서야 주목을 받게 된 것은 아니다. 다만, 본 연구의 대상과 같이 생체인식기술을 전제로 한 생체정보에 관한 논의는 본격적으로 2000년대 초반부터 있어 온 것으로 볼 수 있다. 당시 생체인식기술이 급속도로 발전하였고 그에 대한 관심은 미디어에서도 반영되어 SF영화 등에서 홍채나 망막으로부터 다양한 인적 정보를 추출하거나 생체인식로봇이 활발하게 활동하는 모습으로 구현되기도 하였다. 특히, 미국에서 발생한 9·11테러는 생체인식기술을 이용하여 전 세계적으로 모든 국가가 보안 및 안보를 강화하는 데에 집중적인 기술개발과 제도를 마련하게 되는 중요한 계기가 되었다. 그리하여 입국비자사증 또는 여권에 생체정보를 포함시키도록 의무화하면서 그에 대한 제도적 논의가 국제적으로 본격화되었다.

우리나라에서도 생체정보에 관한 연구는 꾸준히 진행되어 왔는데, 대부분은 개인정보와 관련하여 생체정보의 개념과 특성을 이해하고 정보보호의 필요성을 특히 강조하는 연구가 대부분이었다(생체인식 "기술"에 관한 연구는 논외로 한다). 그 중 일부로서 본 연구에서 인용된 선행연구를 분류하여 보면, 생체인식기술에 대한 소개와 정책적·제도적 개선방안에 관한 논의가 주를 이루고 있으며,[3] 국제적 규범으로서 개인정보의 보호와 관련된 OECD가이드라인과 EU지침을 소개하거나, 주요 선진 외국의 개인정보 내지 생체정보와 관련한 법령을 소개하면서 우리나라 법제와의 비교 내지 제도도입을 제안하고자 하는 연구가 활발히 진행되었다.[4] 구체적인 영역으로 생체정보에 대한 프라이버시보호의 측면에서 전자여권 사례의 검토[5]가 이루어지기도 하였다. 무엇보다도 2005년 12월 당시 정보통신부 및 한국정보보호진흥원(이하 KISA)에서 제정한 「생체정보 보호 가이드라인」은 그간의 생체정보에 관한 논의를 구체화하였다는 점에 의의가 있다.

그 후 생체정보에 관한 연구가 축적되면서 생체정보와 관련하여 보다 개별적이고 세밀한 논의가 진행되고 있는데, 최근의 대부분의 연구는 생체정보의 개념과 성격, 나아가 생체정보의 각 식별자의 특성까지도 고려하고 있으며, 대형 금융사 등의 개인정보 유출사건 등으로 인하여 개인보호의 중요성을 강조하는 차원에서 특히 금융개인정

3) 이민영, "생체정보의 보호에 관한 법제도적 정책방향", 「정보통신정책」, 제16권제21호(통권제359호), 정보통신정책연구원, 2004. 11. 16; 김일환, "생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안연구", 「법과정책」, 제주대학교 사회과학연구소, 제13집제2호, 2007. 8.

4) 연광석, "생체인식정보 보호에 관한 연구(비교법적 검토를 중심으로)", 「법제현안」, 제2005-4호, 통권 제173호, 국회사무처 법제실, 2005. 9; 조규범, "생체정보보호를 위한 입법론적 대응방안", 「국회도서관회보」, 제45권제9호(통권352호), 2008. 10, 49면 및 "생체정보보호를 위한 입법론적 고찰", 「공법연구」, 제37집제1-2호, 2008. 10; 박정훈, "바이오매트릭스의 이용에 따른 법적 과제", 「경희법학」, 제47권제2호, 2012 등 다수의 연구가 존재한다.

5) 박정훈·김행문, "생체정보 프라이버시의 쟁점 및 정책 시사점 - 전자여권 사례를 중심으로-", 「정보화정책」, 제15권제3호, 2008 가을호.

보와 생체개인정보의 차이를 논의하거나,[6] 의료정보와의 통합개념화를 통하여 공공기관에서의 활용을 고려하고,[7] 형사정책적 활용을 검토하는[8] 등 점차 세분화되고 전문화되어가고 있는 특징을 보인다. 앞에서 언급한 정보통신부・KISA의 「생체정보 보호 가이드라인」은 2015년 12월 현재 행정자치부가 「바이오정보 보호 가이드라인(안)」으로서 보다 발전시켜 검토하고 있는 것으로 알려져 있어 관심이 주목되고 있다.

2. 선행연구와의 차별성

앞에서 언급한 바와 같이 생체정보에 관하여는 선행연구가 어느 정도 축적되어 있지만, 대부분은 생체정보를 여전히 개인정보의 하나로 파악하여 생체정보를 어떻게 보호할 것인가 그리고 그 검토대상으로서 외국 규범은 어떠한가를 개인정보보호의 차원에서 논의하여 왔다고 할 수 있다.

그러나 생체정보에 대한 인식기술이 비약적으로 발전하고 있고 생체정보가 일반적인 개인정보와는 다른 성격을 가진 독특한 성격을 가진 것으로 받아들여지고 있는 현재와 같은 상황에서는 생체정보에 관하여 독자적인 연구가 필요하다고 해도 과언이 아니다. 즉, 생체정보를 아무런 의심 없이 개인정보의 하나로서 파악하여 개인정보보호의 수준을 논의하는 것은 현행 제도를 뛰어넘는 발전에는 별로 도움이 되지 않을 것이기 때문에, 지금은 좀 더 근본적이고 현실적인 입장에서 (일반적인 개인정보와는 다른) 생체정보만의 고유한 개념과 성격을

6) 오길영, "개인정보보호 법제의 법적 문제 - 금융개인정보와 생체개인정보를 중심으로", 「민주법학」, 제53호, 2013. 11.

7) 박미정, 「공공정보의 이차활용을 위한 법제도에 관한 연구」, 연세대학교대학원 보건학 박사학위논문, 2014, 12.

8) 이원상, "빅데이터 환경에서 생체정보의 형사정책적 활용에 대한 고찰", 「비교형사법연구」, 제17권제1호(통권제32호), 2015. 4.

정해야 하고, 그것이 기술 분야에서 적극적으로 활용될 수 있는 영역과, 개인의 프라이버시가 최대한 보호되어야 하는 영역을 구분해야 할 필요가 있으며, 이에 대한 제도적·규범적 개선안도 도출되어야 하는 시점에 온 것이다. 이러한 점에서 기존의 연구는 금융이나 의료, 수사와 같은 어느 한 분야의 관점에서 이루어져 왔으며, 때문에 생체정보와 관련된 규범을 펼쳐놓고 전체적인 관점에서 체계적인 문제점을 지적하고 개선방안을 도출하는 데에는 한계가 있었다고 할 수 있다.

그리하여 본 연구는 기존 선행연구의 한계를 극복하고 조금 더 종합적인 관점에서 생체정보에 관한 다양한 논의를 진행하며 그 결론을 도출함에 있어서도 보다 현실적이고 구체적인 대안을 제시한다.

우선, 생체정보의 개념과 성격, 특성을 개인정보의 개념과 비교하면서 검토한다. 생체정보의 개념을 규범으로 만들어 내기 위해서는 구체적으로 현재 생체정보가 어떠한 분야에서 어떻게 활용되는지를 살펴보는 것이 필요한데, 그 기술 분야와 산업적 발전이 어느 정도에 이르렀는지 간단히라도 살펴는 것이 필요하다고 본다(제2장).

이어서, 현재 법령 등이 생체정보라는 개념을 어느 정도로 수용하고 있는지 관련 법제의 현황을 살펴본다(제3장). 이는 크게 생체정보를 규율하는 현행 법제를 전반적으로 고찰할 필요가 있다. 생체정보는 현행 법령에서 개인정보의 하나로 인정되기고 하고 생체정보라는 개념이 직접적으로 규정이 되기도 하기 때문에 이러한 차이점에 기하여 생체정보 개념을 어떻게 설정하는 것이 적절한지 판단하는 데에 단초가 될 것이다.

또한 다양한 국가에서 생체정보에 관한 개념을 어떻게 정의하고 있는지, 어떠한 규범 속에서 어떻게 규율하고 있는지 최근의 입법동향을 소개한다. 그 대상으로서 소위 정보선진국이라 할 수 있는 미국, 독일, 일본 등 선진 외국에서 생체정보를 어떻게 활용하고 있으며, 그들은 규범을 어떻게 정하고 있는지에 관하여도 살펴본다(제4장).

이러한 다양한 검토를 통해서 현재의 우리 법제도 내에서 생체정보가 어떻게 위치하는 것이 적절한지에 대하여 결론을 도출한다(제5장). 현행 법제에 대한 개선방안으로는 생체정보에 관하여 기존의 「개인정보보호법」과의 관계에서 논의되는 것이 가장 중요하다. 즉, 별도의 개별법으로 입법을 하는 방안도 있을 수 있고, 기존 법령에 대한 특례 등 개별 규정으로 존재할 수도 있을 것이다. 다만, 어떠한 결론의 경우에도 생체정보만의 특성이 반영되고 그 나름대로의 규율의 틀이 정해질 필요가 있다는 점을 유의할 필요가 있다.

Ⅱ. 연구의 방법

본 연구는 생체정보에 관한 선행연구로서 문헌자료를 대부분 참고하였다. 온오프라인에서 생체정보에 관한 학술논문, 연구보고서 및 산업계 현황보고서를 두루 참조하였다.

한편, 생체정보에 관한 연구는 기술적 측면과 규범적 측면에서 매우 전문적이고 민감한 사항을 포함하고 있기 때문에, 각 분야의 실무에서 직접적으로 문제를 접하고 해결하기 위하여 고민하는 전문가의 조언 없이 연구를 수행하는 것은 사실상 불가능하며 무의미한 일이 될 것이다. 그리하여 관련 분야의 전문가의 자문을 충분히 활용하였다. 다만, 본 연구는 제도적, 규범적 관점에서의 연구라는 한계를 가지고 있어 생체인식과 관련된 기술적인 사항에 대하여는 설명이나 평가가 부족할 수 있음을 밝혀둔다.

짧은 연구기간임에도 불구하고 생체정보의 기술 및 활용현황을 살펴보고 그와 관련된 다양한 문제들을 검토하기 위하여 약 5차례에 걸쳐 워크숍을 개최하였다. 본 보고서에 담지 못한 상세한 내용은 별책 자료집을 통하여 그 내용을 참고할 수 있을 것이다.

제 2 장 생체정보 일반론

제 1 절 생체정보의 의의

Ⅰ. 개 념

"생체정보"(biometric data/information)란 사람의 고유한 신체적 또는 행동적 특징을 이용하여 개인의 신원을 확인할 수 있게 하는 정보로서, 지문, 홍채, 망막, 정맥패턴, 얼굴, 음성, 서명패턴 등 개인을 직접 나타내는 정보를 말한다.[9] 생체정보는 사람이라면 누구나 가지고 있는 것이지만 사실 가지고 있는 그 자체로는 아무런 의미가 없으며, 일정한 목적 하에 이를 인식할 수 있음을 전제로 하여서만 그 목적에 따른 기능과 의미를 가지게 된다. 그리하여 생체정보를 통하여 개인을 인식하거나 인증할 수 있게 하는 일정한 목적과 기술이 전제되어야 하는데, 이를 "생체인식기술"이라 한다. 생체인식기술은 각 개인의 생체적, 즉 신체적 특성과 행동적 특성을 자동화된 장치로 측정하여 이를 데이터베이스화하고, 이렇게 축적된 생체정보의 자료를 통하여 개인을 식별하거나 인증하는 기술로서 "생체인식"이라고도 한다.[10]

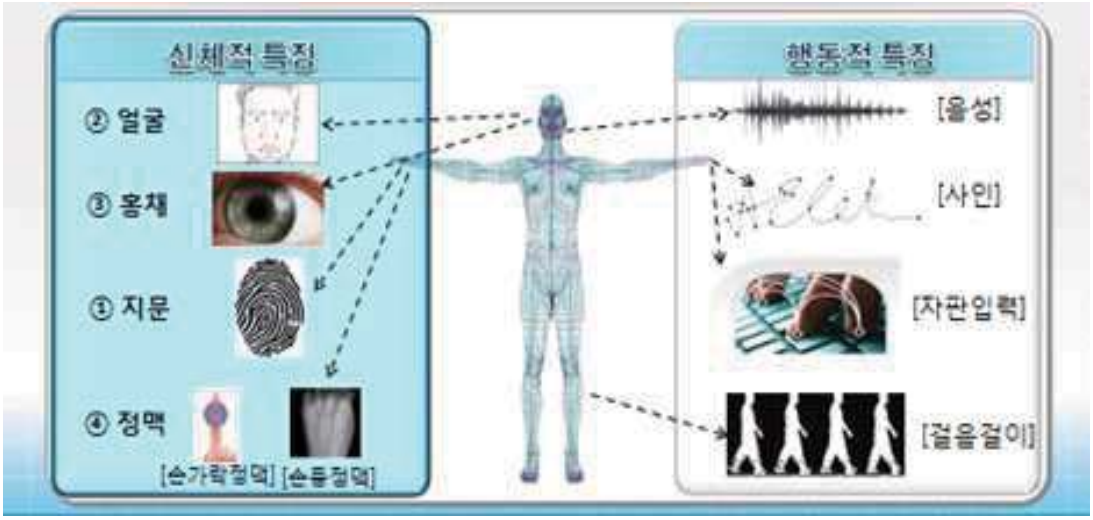
생체정보는 그 식별자(identifier)에 따라 크게 신체적(선천적, 생래적) 특징을 가진 것과 행동적(후천적) 특징을 가진 것으로 구분할 수 있는데, 사람이 태어나면서부터 지니고 변하지 않는 지문, 홍채, 망막, 정

9) 본 보고서에 정의하는 생체정보의 개념은 김일환, 앞의 "생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안연구", 65-66면; 이민영, 앞의 글, 41면; 심우민, 앞의 글, 1면; 박정훈, 앞의 글, 401-402면; 조규범, 앞의 "생체정보보호를 위한 입법론적 대응방안", 49면; 연광석, 앞의 보고서, 5면; 박정훈・김행문, 앞의 글, 86면 등의 문헌에서 유사한 내용으로 정의하고 있는 생체정보의 개념을 가급적 포괄하여 재구성한 것이다.

10) 이재득, "바이오인식기술의 금융서비스 적용현황 및 발전과제", 「지급결제와 정보기술」, 제57호, 2014. 7, 4면.

맥 등이 전자의 대표적인 예이고, 후자의 경우 서명패턴 내지 필체, 타이핑 리듬, 걸음걸이 등이 이에 속한다.[11)]

< 생체정보의 유형 >



출처 : 이승재, "생체인증(바이오인식인증)을 이용한 인증기술 및 시장현황", 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 58면.

생체정보의 식별자 중에서 가장 대표적인 것은 단연 "지문"이라고 할 수 있다. 지문은 가장 오래 사용된 생체정보로서 임신 24주째에 생성되어 평생 변하지 않는 특성을 가진다.[12)] 일부 극소수의 경우 무지문증, 다한증이나 직업적 이유로 지문을 취득하기가 어려운 경우가 있으나, 지문이 가지는 만인부동(萬人不同), 종생불변(終生不變)의 장점은 그동안 가장 정확하고 효율적으로 개인의 신원을 확인할 수 있는 수단으로서 인식될 수 있게 한 장점으로 인정되어 왔다.[13)]

11) 생체정보의 각 식별자의 특징에 관하여는 전동훈, "바이오인식 기술의 종류와 활용현황", 「생체정보의 활용 및 보호를 위한 법제정비방안 연구 : 워크숍 자료집」, 2016, 70-75면 참조.

12) YTN science, [Science & Investigation] "바이오 인식 기술", 2013. 12. 4. 방송.

13) 이상명, "주민등록 지문날인제도의 위헌성, 「한양법학」, 제22권제4집, 통권 제36

우리나라는 1975년「주민등록법」시행령의 개정으로 전 국민이 만 17세가 되면 주민등록증을 발급받아야 하고 그 신청 시 열 손가락의 지문을 모두 날인하여 이를 경찰청에서 보관하고 있도록 하고 있어[14] 지문에 관한 한 (헌법적 정당성 여부에 관한 논의는 별론으로 하더라도[15]) 다른 여느 국가보다 생체정보를 매우 적극적으로 광범위하게 활용해 온 국가라고 할 수 있다.

한편, 사람마다 고유한 특성을 가지고 있다는 "홍채" 또한 생후 18개월 이후 완성된 후 평생 변하지 않는 특성을 가지고 있으며, 홍채의 내측연 가까이에 융기되어 있는 원형의 홍채 패턴은 사람마다 모양이 모두 다르고, 지문과 달리 홍채는 민감한 신체 부위로 눈꺼풀과 각막에 의해 다중으로 보호받기 때문에 손상으로 인한 변화 확률도 매우 희박하여 개인에 대한 유일성을 보장하는 데 뛰어난 정보로 평가받고 있다.[16] 무엇보다도 직접 접촉하지 않는 비접촉방식으로 거부감이 적게 인식할 수 있는 장점이 있어 최근 IT기기에서 활용되고 있다.

"얼굴"도 신체적 특징을 나타내는 대표적인 생체정보라고 할 수 있다. 다만, 얼굴인식은 지문 등 다른 인식기술 보다 영상에 영향을 미치는 환경적 요소가 매우 다양하다. 즉, 같은 얼굴이라도 조명이라든가

집, 2011. 11, 321면.

14) 경찰청은 1990년 개인의 인적 사항과 지문등이 포함되어 있는 주민등록증 발급 신청서를 대용량컴퓨터에 이미지 형태로 입력한 다음 필요시 단말기에 현출시켜 지문을 확인하거나 또는 변사자의 인적 사항 및 현장유류지문 등을 자동으로 검색하여 동일인 여부를 확인하는 지문자동검색시스템(AFIS)를 도입하였다. 이상명, 앞의 글, 323면.

15) 헌법재판소는 주민등록법상 지문정보의 수집을 합헌이라고 결정(헌재 2005. 5. 26 99헌마513, 2004헌마190(병합))한 바 있는데, 이에 대하여는 과거의 비민주적이고 반법치적으로 도입되었던 지문날인제도의 합헌성을 인정한 것이며, 이렇게 수집된 지문정보를 그대로 경찰청장에게 넘겨 이를 전산화하고 이용하는 것 또한 지식정보사회에서 개인정보의 새로운 침해를 허용한 것이라는 비판이 있다. 김일환, "주민등록법상 지문정보의 목적 외 이용에 대한 헌법적 고찰",「공법연구」, 제41집 제1호, 2012. 10, 107면; 이상명, "주민등록 지문날인제도의 위헌성",「한양법학」, 제22권제4집(통권제36집), 2011. 11. 349면.

16) 전동훈, 앞의 글, 72면.

각도, 표정이나 화장, 헤어스타일 등에 따라 특징점의 변화가 커서 다른 식별자들에 비하여 오인식률이 높고, 취득된 영상을 비슷한 형태로 변환하는 전처리 과정에 많은 자원과 시간이 소모되는 특징이 있다.

그밖에 “음성”(성문), “정맥”, “손모양” 등 신체적 특성을 기반으로 하는 생체정보는 물론이거니와 “서명패턴”, “걸음걸이” 등 행동적 특성을 기반으로 하는 생체정보 등이 있는데, 각 식별자가 단독으로 사용되기도 하지만 두 개 이상의 식별자를 동시에 사용하는 다중인식시스템으로 응용하기도 한다.[17)]

각 식별자마다 각각 장단점을 가지고 있어 그 성격이나 비용에 따라 활용분야가 다양하게 나뉜다. 사실 생체정보의 식별자를 개별적으로 검토하여 각 활용상황에서 발생하는 기술적 문제들도 함께 살펴보는 것이 필요하겠지만, 본 연구는 생체정보라는 추상적 형태의 정보에 대한 규범적 문제로 보기로 한다.

< 각 생체정보 식별자의 장・단점 >

생체정보	장 점	단 점
지 문	- 가장 오래 사용된 식별자 - 비용 저렴, 우수한 안전성 - 만인부동, 평생불변	- 무지문증, 다한증 등 사용자 중 약 2% 정도는 지문취득 불가
얼 굴	- 쉽고, 빠르고 비용 저렴 - 비접촉방식으로 사용자의 거부감 적음	- 환경(안경, 가발, 조명 등) 및 자세에 따라 영향 - 인식 시간이 오래 걸림
손금/손모양	- 최소의 저장용량 요구	- 처리속도가 늦고 정확도 떨어짐
정 맥	- 지문이나 손가락이 없어도 손등 또는 손가락의 혈관 측정 가능	- 하드웨어 구성이 복잡 - 시스템 소형화가 어려움 - 제품가격의 고가화

17) 전동훈, 앞의 글, 70면.

생체정보	장 점	단 점
홍 채	- 기계와의 접촉이 불필요하여 거부감 적음 - 만인부동, 평생불편	- 대용량 특징의 벡터(256bytes)
망 막	- 안정성 우수 - 만인부동, 평생불편	- 사용 거부감
성 문	- 비용 저렴, - 원격 접근에 적당	- 처리속도 느림 - 사람 상태에 쉽게 영향
필 체	- 비용 저렴	- 사람 상태에 쉽게 영향 - 높은 오인식률

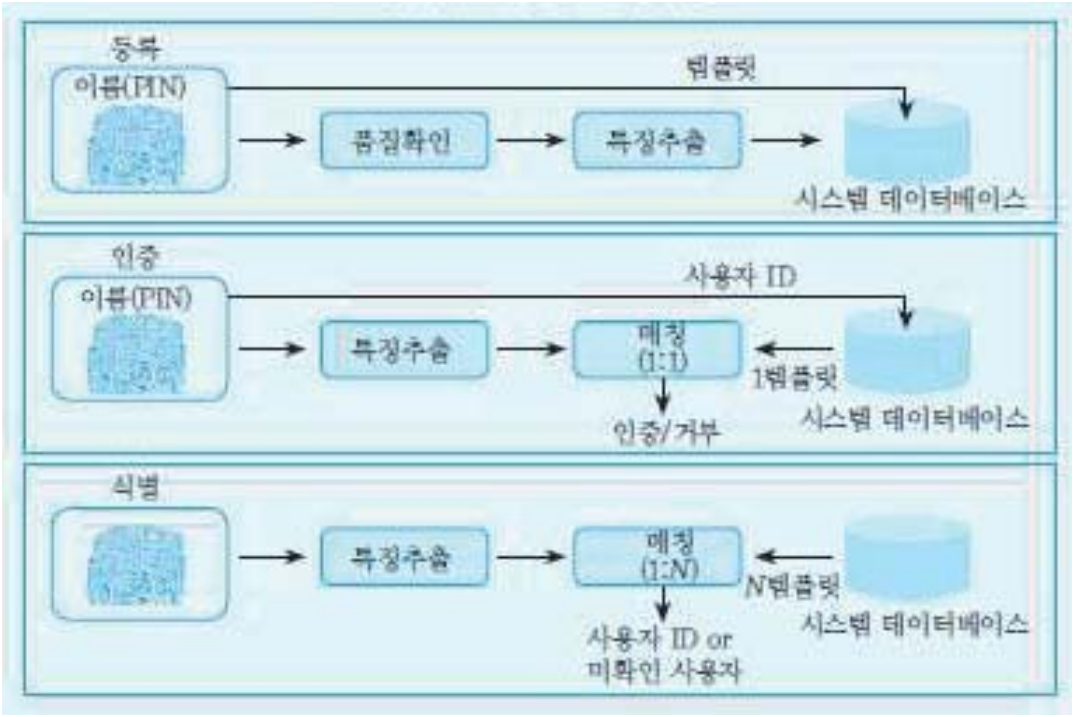
출처 : 중앙일보, “지문・얼굴・홍채・정맥... 진화하는 IT생체인식기술”, 2013. 12. 9.을 전동훈, 앞의 글, 69-70면에서 재인용 및 수정.

Ⅱ. 기 능

생체정보를 사용 내지 활용하고자 하는 데에는 적어도 어느 하나의 “이유” 내지 “목적”이 있다. 하나는, 어떤 사람을 데이터베이스에 등록된 다른 개인들로부터 구별하기 위한 것으로서 “당신은 누구인가?”에 대한 대답, 즉 “인식” 내지 “식별”(identification)을 위한 것이다. 그리고 다른 하나는, 어떤 사람이 어떠한 권한을 주장할 수 있는 그 사람이 맞는지를 확인하기 위한 것으로서 “당신이 권한 있는 그 자가 맞는가?”에 대한 대답, 즉 “인증” 내지 “검증”(verification)을 위한 것이라 할 수 있다. 즉, “인식” 시스템은 템플릿 데이터베이스 전체를 검색하여 개인을 1:N으로 인식하는 것으로, 데이터베이스에 등록되어 있는 템플릿을 이용하여 “누구인지”를 판별하는 것을 말하며, “인증” 시스템은 입력한 바이오 정보와 시스템에 미리 저장되어있는 템플릿과 비교하는 것에 의해 사람의 신분을 1:1로 인증하는 것으로, 신분이 제시한 “권리”를 판단하는 것을 말한다. [18]

18) 전동훈, 앞의 글, 79면

< 사용자등록 · 인증 · 식별 과정 >



출처 : 문기영, “생체인식 기술현황 및 전망”, 「TTA Journal」, No. 98, 한국정보통신기술협회, 2005, 39면을 이재득, 앞의 보고서, 5면에서 재인용.

이러한 생체정보는 “인식” 또는 “인증”이라는 기능에 따라 사용되는 생체정보나 발전의 양상도 조금씩 달라질 수 있다. 즉, 범죄수사나 보건의료, 상업적 마케팅 등과 같은 분야는 일반적으로 대상의 “인식” 기능이 우선이고 그것이 본인이 권한자임을 인증할 필요성이 크지 않은 분야이지만, 금융결제나 출입통제, 사회복지서비스의 수급 등과 같은 분야는 반드시 본인임을 “인식”함과 동시에 권한자임을 “인증”까지 하여야 하는 분야라고 할 수 있다. 이러한 기능은 그것을 사용하는 분야, 즉 공공분야와 민간분야로 나누어 살펴볼 수도 있을 것이다.

이렇게 인식이나 인증의 기능에 대한 분류는 그것을 활용하고자 하는 목적과 실제 활용하게 되는 분야에 따라 그 정보를 어떻게, 어느

정도로 보호할 것인가와 밀접한 관계가 있기 때문에 면밀하게 살펴볼 필요가 있다.

< 생체인식의 기술 적용분야 >

활용분야	적용례
금 융	ATM-KIOSK, 모바일뱅킹, 증권거래, 전자상거래, 지불 및 결제수단 등
보 안	정보보안(시스템 및 데이터 접근・인증제어), 생체로그인(PC), 휴대폰・노트북・자동차 등 기기사용자 인증 등
출입관리	공항(출입국 심사, 불법출입국자 확인 등), 기업(출입통제, 근태관리) 등
의료복지	환자신분 확인, 기록관리, 원격진료, 무인전자처방전 등
공공(수사)	범죄자 인식(지문대조, 성문분석 등), 전자주민증(신분증), 선거관리(본인확인 등)
검 역	안면인식을 통한 신종플루 감염자 식별
엔터테인먼트	얼굴인식을 통한 인물사진 분류 및 관리, 닮은 사람 찾기
마케팅	고객 연령 및 성별 추정, 타겟 마케팅(포인트적립 및 이벤트 제공 등)

출처 : 연구성과실용화진흥원, “생체인식 기술 및 시장동향”, S&T Market Report, vol. 39, 2016. 2, 4면 보완.

Ⅲ. 성격 및 특징

생체정보는 사람이 고유하게 가진 신체적・행동적 특성으로 그의 신원을 확인할 수 있는 정보를 말하며, 정보를 가진 그 사람과 불가분의 관계에 있다. 즉, 생체정보는 항상 자신의 몸에 지니고 있는 불가변의

정보이기 때문에 이 세상에서 나만이 가진 불변의 정보이며, 이를 이용하여 언제 어디서나 본인을 손쉽게 인증할 수 있고, 항상 본인과 함께 존재하므로 다른 정보와 달리 도난이나 분실의 우려가 거의 없다.[19][20]

그런데 반대로 생체정보의 이러한 "민감한" 성격은 오히려 그 자체로 매우 취약성을 드러내는 것이라 할 수 있다. 즉, 절대적으로 변경할 수 없다는 그 강한 특수성으로 인하여 일단 유출이 되면 결코 회복할 수 없는 손해를 입게 된다. 이미 개인정보 유출이 심각한 사회문제로까지 대두된 적이 수차례 있었고, 그로 인하여 소송을 통하여 주민등록번호를 변경하는 사태에 까지 이르게 되면서 정보의 노출이나 유출에 대한 경계와 거부감이 상당히 강하게 형성되어 온 것도 사실이다. 그런데 이러한 주민등록번호나 비밀번호 등 기존의 개인정보는 유출이 된 경우 일정한 절차를 통하여 얼마든지 교체 또는 폐기할 수 있지만, 생체정보는 이러한 정보와는 달리 임의로 변경을 할 수가 없는 정보이기 때문에 일단 유출이 되고 나면 다른 생체정보로 대체하지 않는 이상 그 생체정보는 더 이상 사용할 수가 없게 되는 점에 문제가 더 크다. 더욱이 기술의 발달로 비대면 정보수집이 가능해지면서 정보주체의 다양한 생체정보가 빈번하게 그리고 무의식적으로 원격시스템 등을 통해 노출되고 간단히 취득될 수 있는 상황에 이르렀기 때문이다.[21]

---

19) 미국 국토안보부(DHS)에서 발간한 생체정보의 수집 및 사용에 관한 2012년 보고서(The data privacy and integrity advisory committee on privacy and the department's collection and use of biometrics), 2면은 생체정보인식에 대한 유용성 평가(Evaluating the usefulness and Utility of Biometrics)로서 다음과 같이 5가지 특징을 명시하고 있다. 즉, ① 보편성(Universality), ② 유일성(uniqueness), ③ 영구성(Permanence), ④ 획득성(Collectability), ⑤ 수용성(Acceptability)이 그것이다.
https://www.dhs.gov/sites/default/files/publications/DPIAC%20Recommendations%20Paper%202012-02.pdf (2016.10.20. 최종접속)

20) 이러한 편리성과 경제성 덕분에 바이오와 정보기술의 융합이라는 새로운 기술적 패러다임으로 평가되고 산업적으로도 고도의 부가가치를 창출할 새로운 산업군으로 전망되기도 한다. 조규범, 앞의 "생체정보보호를 위한 입법론적 대응방안", 50면.

21) John D. Woodward Jr., Biometrics: Identifying Law and Policy Concerns, in biometrics: Personal Identification in Networked Society, Chapter 19 (Anil K. Jain et al. eds., 1998), at 385-405.

그리하여 생체정보는 매우 민감한 개인정보로서의 특유한 성격을 가진 것으로 파악하여 정보의 내용과 정보주체를 보호할 필요가 있다. 그동안 가장 강하게 보호되어 왔던 개인정보로서 주민등록번호의 경우 그 유출로 인한 피해가 심각한 상황에 이르게 되어 변경이 불가능하게 여겨졌던 주민등록번호까지 변경할 수 있게 된 현 상황은 개인정보의 변경가능성이 얼마나 중요한 것인지를 깨닫게 하며, 만약 생체정보가 불법 유출 또는 오·남용되는 경우 그 피해를 최소화하기 위한 제도적 정비가 어떠해야 하는지를 환기시켜 준다고 하겠다.[22)]

이러한 취지에서 중요한 것은 생체정보를 통하여 확인할 수 있게 되는 각종 정보를 보호하기 위하여 생체정보의 "원본정보"와 "인식정보"를 구별할 필요가 있다는 점이다. 즉, 생체정보를 그대로 보관하거나 활용하도록 할 것이 아니라, 반드시 일정한 "암호화 내지 비식별화"를 거쳐서 특징값으로 생성된 인식정보로서만 활용하도록 하여 분실·유출의 경우에 정보주체와의 관련성을 단절시키고 재발급의 가능성을 확보하도록 하는 것이 필요한 것이다.

22) 헌재 2015. 12. 23. 2013헌바68, 2014헌마449(병합) 결정요지 중 : "주민등록번호는 표준식별번호로 기능함으로써 개인정보를 통합하는 연결자로 사용되고 있어, 불법 유출 또는 오·남용될 경우 개인의 사생활뿐만 아니라 생명·신체·재산까지 침해될 소지가 크므로 이를 관리하는 국가는 이러한 사례가 발생하지 않도록 철저히 관리하여야 하고, 이러한 문제가 발생한 경우 그로 인한 피해가 최소화되도록 제도를 정비하고 보완하여야 할 의무가 있다. 그럼에도 불구하고 주민등록번호 유출 또는 오·남용으로 인하여 발생할 수 있는 피해 등에 대한 아무런 고려 없이 주민등록번호 변경을 일체 허용하지 않는 것은 그 자체로 개인정보자기결정권에 대한 과도한 침해가 될 수 있다."

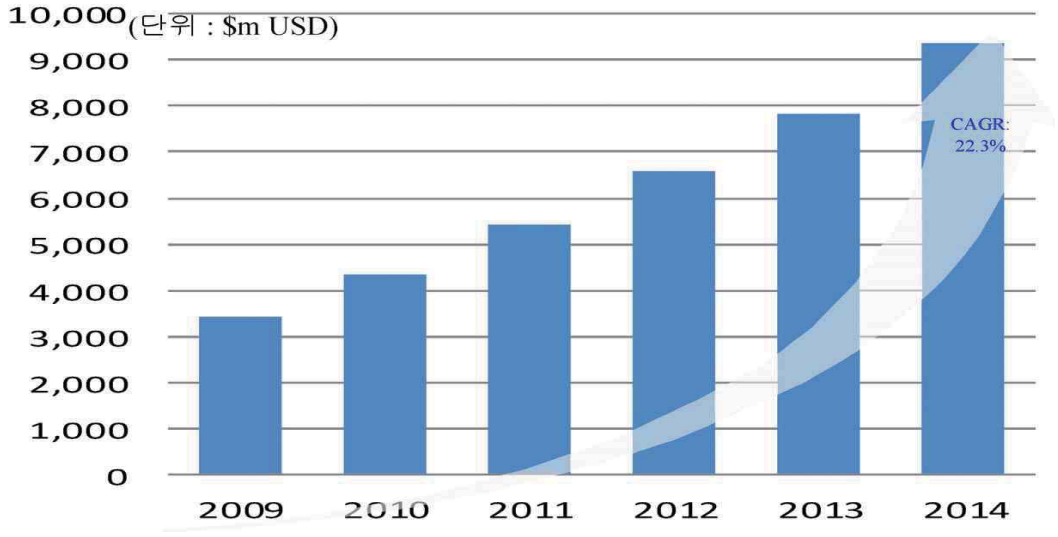
제 2 절 생체정보의 활용 현황

Ⅰ. 서 설

생체정보의 대명사인 지문이 오랫동안 다방면에서 본인 인식이나 인증의 수단으로 활용되어 온 것은 주지의 사실이다. 그러나 생체정보 자체가 “사회적 가치”로서 중요성을 가지게 된 직접적인 계기는 2001년 미국에서 발생한 9.11테러로 인하여 신원확인의 필요성과 그에 대한 수단으로 인정되기 시작한 것이라고 할 수 있다. 즉, 이 사건으로 인하여 미국과 유럽 등의 각 국가의 출입국사무소에서 생체정보를 인식하는 기기 및 제품을 도입하는 외에 생체정보에 관한 본격적인 연구가 추진되면서 급기야 타 IT산업에 비해 고부가가치의 고성장산업으로까지 인정받게 된 것이다. 이러한 국제적 추세에 따라 우리나라의 경우도 2000년대부터 생체정보에 관한 기술개발이 이루어지고 있다.

< 생체인식기술의 발전 동향 >

< 세계 생체인식 산업 시장규모 >



출처(상・하) : 유장희, 조현숙, “바이오인식기술의 현황 및 진화”, 「정보처리학회지」, 제20권제3호, 2013. 5, 6면.

다만, 우리나라는 외국에서와 같이 생체인식산업의 시장규모가 그리 크지 않은 것으로 보인다. 즉, “바이오인식산업”은 세계적으로 약 94억 달러 정도의 규모(2014년 기준)인 것으로 평가되는데, 이는 2011년 54억이었던 것에 비하면 연평균 20% 성장한 것으로 매우 큰 성장을 보이는 반면에,[23] 국내 매출은 아래 실태조사에서 보는 바와 같이 2013년 1,724억원에서 2015년 1,871억원 정도로[24] 시장의 규모 자체가 크지 않고 성장세 또한 그리 현저히 눈에 띄고 있지는 않다.[25]

23) 이승재, 앞의 글, 61면.

24) 연매출 1,800억원은 보는 관점에 따라 평가가 달라질 수 있으나 한 때 선풍적인 인기를 모았던 과자제품의 연매출 규모가 이 정도였음을 견주어 본다면 단일규모가 아닌 업계의 시장규모로서는 매우 작은 것이라고 평가하지 않을 수 없다. http://www.edaily.co.kr/news/NewsRead.edy?SCD=JC21&newsid=01659686612647608&DCD=A00302&OutLnkChk=Y (2016.10.9. 최종접속)

25) 그러나 생체인식을 이용한 스마트기기(모바일)의 시장은 연평균 67%씩 성장하여 2020년에는 346억 달러 약 38.2조원을 달성할 것으로 전망되고 있다. 이승재, 앞의 글, 62면.

< 바이오인식산업 매출 현황 >

구 분		2013년	2014년	2015년	증감율(%)
물리보안제품	DVR	670,657	566,294	533,033	-5.9
	카메라	1,130,188	1,007,600	1,029,021	2.1
	IP영상장치	381,364	410,919	415,685	1.2
	엔진/칩셋	106,286	117,068	147,488	26.0
	Solution	289,904	293,762	327,853	11.6
	주변장비	319,789	66,925	77,839	16.3
	Access Control	478,758	400,613	430,180	7.4
	바이오인식	**172,431**	**174,527**	**186,119**	**6.6**
	알람/모니터링	137,810	179,251	192,943	7.6
	기타	162,439	177,631	194,918	9.7
	소계	**3,849,326**	**3,394,590**	**3,535079**	**4.1**
물리보안서비스	출동보안서비스	1,194,722	1,441,616	1,551,882	7.6
	영상보안서비스	336,689	467,514	498,417	6.6
	기타보안서비스	88,355	215,732	233,792	8.4
	소계	**1,619,766**	**2,124,862**	**2,284,091**	**7.5**
합계		**5,469,092**	**5,519,452**	**5,819,170**	**5.4**

출처 : 한국정보보호산업협회,「2015 국내정보보호산업 실태조사」, 2015. 12, 81면.

이에 생체정보의 산업적·기술적 발전을 도모하기 위하여 최근「정보보호산업의 진흥에 관한 법률」이 제정되었다.[26] 이 법은 정보보호

26)「정보보호산업법」이라 불리는 이 법은 2015년 12월부터 시행되었으며, 주요 내용은 크게 수요자 측면에서의 정보보호산업 활성화에 관한 사항(구매수요정보의 제공, 공공기관등의 정보보호시스템 구축 계약 등, 사업 하도급의 승인, 정보보호시스

산업을 활성화하고, 정보보호산업의 진흥을 위한 기반을 조성하기 위한 다양한 지원책을 마련하고 있는데, 추후 실효적인 효과를 거둘 수 있으리라 기대한다. 생체정보의 보호는 기술적 발전이 선도적으로 이루어져야 하는 분야이기 때문에 기술발전을 위한 정책적·제도적 지원이 반드시 병행되어야 할 것이다.

한편, 구체적인 생체정보의 활용과 관련하여, 가장 대표적인 생체정보는 "지문", "안면", "홍채", "성문" 등이며, 이는 대부분 본인을 인식하거나 인증하는 영역, 즉 출입통제나 근태관리, 금융거래의 분야에서 이미 많이 활용되어 왔다.[27] 최근에는 의료서비스라든가 범죄수사 등의 분야에서 최첨단의 과학기술이 응용되면서 생체정보에 대한 활용의 수요가 급격히 확대되고 있다. 때문에 생체정보가 어느 분야에서 어떻게 활용되고 있는지 현황을 살펴보는 것이 우선이라 할 수 있다.

생체정보의 활용은 그 기능에 따라 인식이나 인증의 목적으로 크게 구분할 수 있고, 그것을 활용하는 분야도 공공분야와 민간분야로 나누어 살펴볼 수 있음은 앞에서 언급한 바와 같다. 다만, 본 연구에서는 공공과 민간의 구별실익이 크지 않다는 판단 하에 주요 활용분야로서 금융, 의료서비스, 수사분야로 나누어 살펴보기로 한다.

템의 하자담보 책임, 정보보호제품 및 정보보호서비스의 대가, 정보보호산업의 융합 촉진, 정보보호 준비도 평가 지원 등, 정보보호 공시)과 공급자 측면에서의 정보보호산업 활성화를 위한 사항(기술개발 및 표준화 추진, 전문인력 양성, 국제협력 추진, 성능평가 지원, 우수 정보보호기술등의 지정, 우수 정보보호기업의 지정, 자금융자, 수출 지원, 세제 지원 등, 정보보호 전문서비스 기업의 지정·관리, 한국정보보호산업협회의 설립)으로 구성되어 있다.

27) 생체정보를 통한 근태관리의 적법성 여부에 관하여는 논의하지 않기로 한다. 다만, 기관장이 초과근무 관리를 위해 지문인식기를 운영하는 경우 정보주체의 지문등록 동의 여부 확인 절차를 지키고, 동의하지 않는 자에 대한 대체수단을 마련하는 등 개인정보보호법의 규정과 취지를 준수할 필요가 있다는 인권위 권고(사건 14진정0765900)에 대하여는 유의할 필요가 있다. 국가인권위원회 보도자료, "동의절차 및 대체수단 없는 지문인식기 도입은 개인정보자기결정권 침해", 2015. 3. 1. 1면.

Ⅱ. 금융 분야

생체정보를 통하여 본인을 인증하는 사례는 출입국관리, 금융결제, 출입통제 등 이제는 일상적인 생활영역에서 쉽게 찾을 수 있다. 특히 금융거래에 있어서 인증기술이 발전함에 따라 텔레뱅킹, 인터넷뱅킹, 모바일뱅킹, SNS뱅킹 등 시간과 공간의 제한을 넘어서 획기적인 거래 방식이 선을 보이고 급속도로 확산되고 있다.[28)]

그런데 이러한 기술발전의 편리함 뒤에는 해킹, 보이스피싱 또는 피싱사이트를 통하여 고객의 계좌번호나 계좌비밀번호, 보안카드 번호 등의 중요한 개인정보를 불법으로 취득하여 인터넷 뱅킹을 이용하여 타인명의의 공인인증서를 부정하게 발급받아 고객 예금을 인출해가는 사기가 지속적으로 발생하는 문제가 동시에 자리잡고 있다.[29)] 이러한 문제에 대한 대비책으로서 좀 더 확실하고 안전한 본인확인을 할 수 있는 방안이 모색되고 본격적으로 추진되었다.[30)] 공인인증서를 재발급하거나 인터넷뱅킹을 통해 일정 금액을 이체하는 경우 본인확인 절차를 추가하게 된 것이 가장 대표적인 조치이다.

"본인확인"이란 정보통신망을 통하여 정보시스템 또는 행정정보를 이용하는 업무담당자, 민원인 또는 시스템 관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것이다(「행정기관 정보시스템 접근권한 관리규정」 제3조제5호).[31)] 이는 오프라인 환경에서

---

28) 이재득, 앞의 글, 34면.

29) 공인인증서 유출사고는 급증하고 있다. 2014년 국감제출 자료에 의하면, 2014년 1월~9월 악성코드, 스미싱으로 인해 사용자의 컴퓨터 및 스마트폰에서 16,338건의 공인인증서가 유출되었다고 한다. 송영관, 「기술표준화, 정부개입, 그리고 공인인증서」, 「한국개발연구」, 제37권 특별호(통권제127호), 2014. 8, 6면. 이는 2012년 8건, 2013년 8,710건에 비하면 폭발적으로 급증한 것이다.

30) 금융위원회 보도자료, 「전자금융사기 예방서비스」, 2013. 9. 16, 1면.

31) "본인확인"의 개념과 비교하여 "실명확인"이란 사용자가 사용한 명의가 실제로 존재하는 자의 명의인가 여부를 확인하는 것을 말한다. "본인확인"이나 "실명확인"

는 주민등록증과 같은 신분증을 의미하는 것이며, 온라인 환경에서는 전자적인 정보로 구성된 인증수단으로서 현재 매우 다양한 유형의 전자적 인증수단이 활용되고 있다.[32)]

< 전자적 인증수단 >

인증수단	방 식
ID/Password	서버에 저장된 아이디와 아이디에 매칭되는 비밀번호로 본인을 인증방식
I-PIN	명의도용이 쉬운 주민등록번호를 대신하여 이용자에게 부여되는 인터넷 개인식별번호
보안카드	비밀번호 도용에 의한 금융사고를 방지를 위해 사용하며 35개의 표에 4자리숫자들이 기록되어 있는 형태의 카드
진위확인	식별정보를 이용하여 문서의 진위를 확인해 주는 서비스
공인인증서	공인인증기관이 인증한 전자서명으로 법령에서 서명 또는 기명날인을 요구한 경우 그 요건을 충족한 인증서
보안토큰 (HSM)	소프트웨어 형태의 토큰을 안전하게 보관하기 위해 고안된 하드웨어형 토큰
OTP	로그인할 때마다 그 세션에서만 사용할 수 있는 1회성 패스워드를 생성하는 보안서비스
휴대폰SMS	입력한 주민등록번호와 휴대폰번호 + 휴대폰 가입시 등록한 가입자 주민등록번호가 맞는지를 이동통신사를 통해 확인하는 서비스

의 개념은 다수의 법령에서 사용하고는 있는데, 예컨대, 정보통신망법 제44조의5(게시판 이용자의 본인확인), 전자정부법 제10조(민원인 등의 본인확인) 등에서는 본인확인을, 공직선거법 제82조의6(인터넷언론사게시판·대화방 등의 실명확인)은 실명확인을 요구한다. 현실적으로나 제도적으로 구별의 필요가 있는 개념이기에 가급적 법령에서 직접 규정을 두어 용어를 사용하도록 하는 것이 필요하다고 본다.

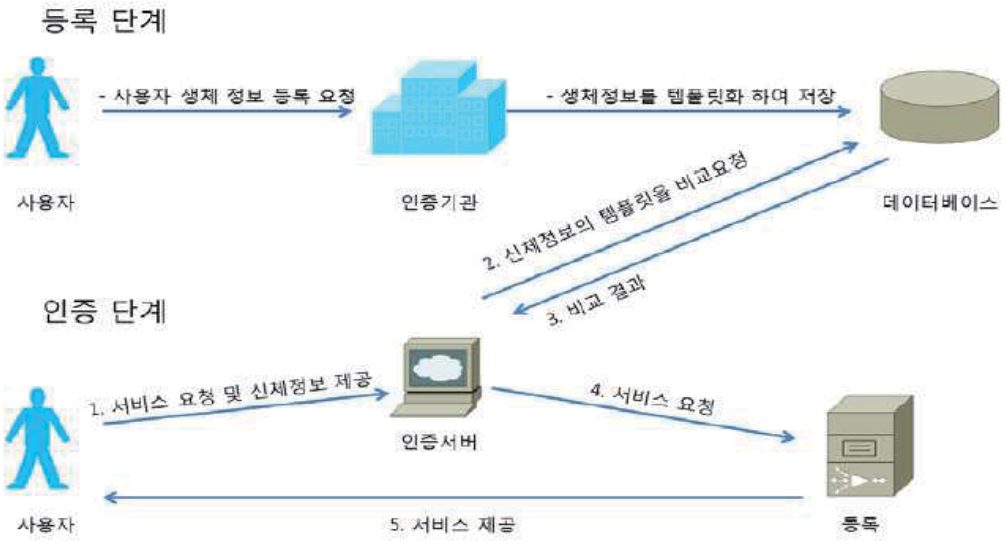
32) 전자인증수단의 유형별 특징에 관하여 자세한 것은 염홍열 외, 「전자인증수단 이용기반 확대를 위한 안전성 기준 연구」, 한국인터넷진흥원, 2011. 12, 2-8면 참조.

인증수단	방 식
2채널 인증	임의로 생성된 1회용 비밀번호를 반드시 사용자의 전화에서 입력하는 인증을 거쳐야만 거래가 가능하도록 하는 서비스
PC등록 인증	사전에 등록된 PC에 한하여 거래가 가능하도록 하는 서비스
생체정보 인증	**이용자의 생체정보(지문인식, 얼굴인식, 전자펜서명인식 등)를 이용하여 본인 확인을 하는 서비스**

출처 : 염홍열 외, 「전자인증수단 이용기반 확대를 위한 안전성 기준 연구」, 한국인터넷진흥원, 2011. 12, 18-44면에서 인용, 정리함.

위의 다양한 전자적 인증수단은 크게 ① 비밀번호나 패턴을 사용하는 방식, ② 공인인증서 또는 OTP생성기를 이용하는 방식, ③ 생체적 특징정보를 활용하는 방식 등으로 나눌 수 있다. 각 인증방식은 나름의 장단점을 가지고 있기 때문에 최근에는 이들 인증방식 중 둘 이상의 수단을 복합적으로 사용하는 경우가 많은데, 이렇게 복합적 인증수단에 있어서 생체정보가 매우 확실한 본인확인 수단으로서 기능하는 것이다.

< 생체정보의 인증과정 >



출처 : 염홍열 외, 앞의 보고서, 34면.

한편, 지금까지는 고객이 예금・증권 등 금융상품에 가입하기 위하여 계좌를 개설할 때 종전에는 금융회사 창구를 방문하여 금융회사 직원에게 주민등록증 등 신분증을 제시하고 실명확인절차를 거쳐야 했다. 즉 금융실명제 도입(1993.8) 당시부터 금융회사 직원이 고객의 실명을 "대면"(face to-face)으로 확인해야 한다는 유권해석이 지속되어 왔던 것이다.[33] 오프라인 환경인 대면거래에서는 본인확인의 수단으로서 주민등록증 등의 신분증이 이용되며, 직원이 사진과 본인의 얼굴을 비교하는 절차를 통하여 인증이 이루어진다.

그러나 최근 정부가 핀테크 발전 추세 및 해외사례 등을 감안하여 비대면 실명확인 방식도 사용할 수 있도록 하는「비대면 실명확인 허용 방안」발표하면서(2015.5) 시간・장소에 구애받지 않고 금융서비스를 편리하게 이용할 수 있게 되었다. 온라인 환경인 비대면거래에서는 오프라인에서의 주민등록증 같은 신분증 대신에 아이디나 카드 등으로 신원을 제시하고 I-PIN과 같은 개인식별번호나 비밀번호 등으로 인증을 받게 된다. 그런데 이러한 카드를 소지하거나 개인식별번호 등의 일련번호를 반드시 기억해야 하는 번거로움이나 분실・도난 등의 위험이 항상 존재한다는 단점이 있다.[34]

그리하여 공인인증서나 일회용 비밀번호(OTP), 보안카드 등과 같이 보관의 필요성이 적고 이용이 편리하며[35] 강력한 신원확인의 수단으로서 생체정보를 활용하는 방안이 도입되었다. 다만, 정부는 실명확인의 중요성을 감안하여 다음과 같이 "복수의" 본인확인 방식으로 하도록 하였다. 생체정보가 주요한 본인확인 수단으로서 인정된 대목이다.

---

33) 금융위원회 보도자료, "비대면 실명확인 운영 현황 및 향후 계획", 2016. 5. 26, 1면.

34) 이정현, "스마트환경에서의 공인인증서 활용과 문제점",「Internet & Security Focus」, 한국인터넷진흥원, 2013. 3, 27-28면.

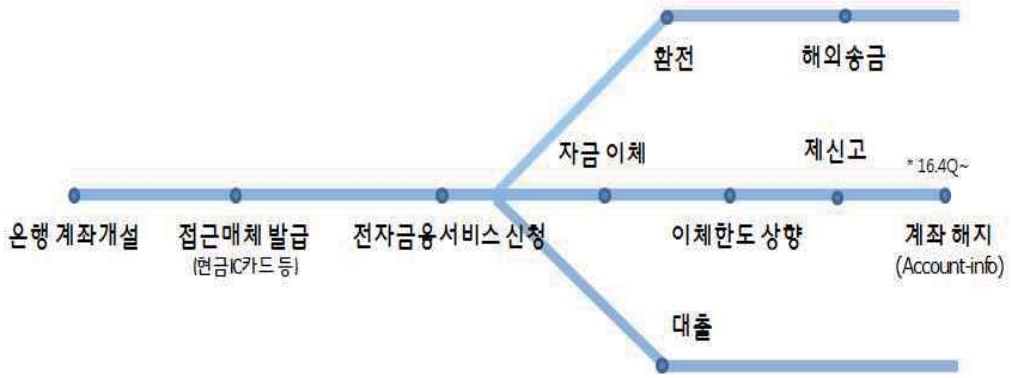
35) 스마트폰의 경우 지문인식은 물론 최근 홍채인식이나 영상통화 인증이 기존의 아이디나 비밀번호, 공인인증서 기반의 인증체계에 대한 대안으로서 급부상하게 된 것이다. 윤재호・홍진실,「바이오인증기술 최신 동향 및 정책과제」, 지급결제조사자료 2016-7, 한국은행, 2016. 8, 1면.

< 본인확인의 유형 >

* (이중확인: 필수) ① 신분증 사본, ② 영상통화, ③ 접근매체 전달시 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 새로운 방식(바이오인증 등) 중 “2가지” 의무 적용
* (다중확인: 권고) ⑥ 타기관 확인결과 활용(휴대폰 인증 등), ⑦ 다수의 개인정보 검증까지 포함하여 ①~⑦ 중 추가확인

출처 : 금융위원회 보도자료, 앞의 “비대면 실명확인 운영 현황 및 향후 계획”, 1면.

< 은행 업무 비대면 처리 프로세스 >



출처 : 금융위원회 보도자료, 앞의 “비대면 실명확인 운영 현황 및 향후 계획”, 3면.

이러한 비대면 실명확인 허용 후 약 6개월간 31개 금융회사가 비대면 실명확인 서비스를 시행 중이며, 아직은 “신분증 사본제출 + 기존계좌 활용 + 핸드폰 인증” 방식을 조합하여 사용하는 경우가 대부분이지만, 다양한 인증방식이 개발되고 있으며 생체정보를 적극적으로 활용하게 될 가능성이 높아졌다.

Ⅲ. 의료 및 헬스케어 분야

의료 내지 헬스케어(healthcare)는 그 개념 자체로 “생체”와 맞닿아 있으며, 당연히 수많은 생체정보를 다루는 분야이다. 통신기술의 발전과 스마트기기의 발달로 인하여 사람과 사물의 모든 주체와 객체가 언제 어디서나 원하는 형태로 연결되는 소위 “초연결사회”(Hyper-Connected Society)가 도래하였으며,[36] 인터넷에 연결된 (의료)기기를 통하여 개인의 생체정보를 제공하고 그에 대한 적절한 판단과 처방을 받는 원격진료 및 응급치료가 가능한 시대가 되었다. 나아가 급속도로 발전한 유전자(DNA) 분석은 암, 치매 등의 유전적 질환이나 난치병 또는 불치병의 예방 및 치료 등에 다양하게 이용되고, 제대혈(탯줄혈액), 세포・줄기세포, 난자 등은 체세포복제, 체세포핵이식, 단성생식 등의 연구에 활용되고 있으며, 세계 각국에서 경쟁적으로 연구를 하고 있다.[37]

특히, 의료기기와 정보통신의 발달로 생체정보의 수집과 공유는 중증응급환자 등록관리 프로그램, 호흡감염 중증환자 추적관리 프로그램, 이송환자 의무기록 정보연계 프로그램, 개인의무기록 정보제공 프로그램, 응급의료 정보통신망 구축 프로그램 등에서 활발히 이루어지고 있다.[38]

웰빙(well-being)에 대한 욕구의 증가로 환자가 아닌 경우에도 개인의 건강관리 차원에서 매우 다양한 헬스케어 서비스가 이루어지고 있

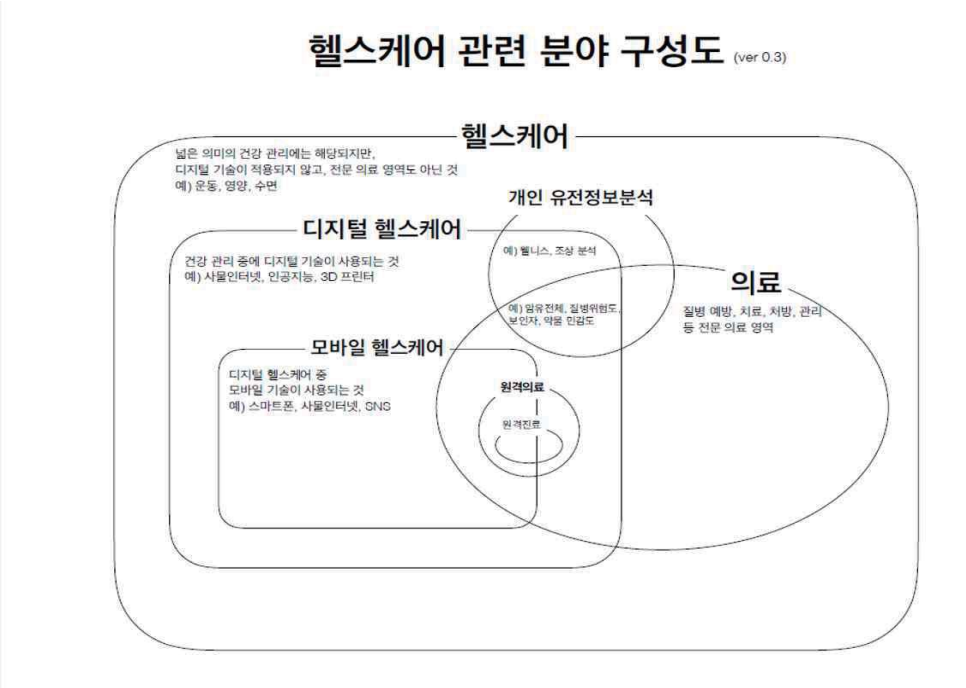
---

36) 이민영, “아이오티 관련 개인정보보호법제 조망”, 「신산업 활성화와 개인정보보호」, 개인정보보호법학회・한국인터넷진흥원 공동학술대회 자료집, 2016. 6, 47면. 또한, 개인의 생체정보가 집적되고 분석되며 추적되는 데에 그치지 않고 접속된 다른 단말기나 잠재적으로 다른 이용자와도 공유될 수 있는 환경이 형성될 수 있기에 주의해야 한다고 강조한다. Marie-Helen Maras, Internet of Things : Security and Privacy Implications, International Data Privacy Law, Vol.5, Iss. 2, 2015, pp.102-102을 이민영, 앞의 “아이오티 관련 개인정보보호법제 조망”, 49면에서 재인용.

37) 이창범, “생체정보의 분야별 활용현황 – 금융, 의료, 수사 분야”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 116면.

38) 배현아, “생체정보의 분야별 활용현황 - 의료분야”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 135면.

는데, 의료기기 외에 의료용 소프트웨어, 나아가 의료용 모바일 앱[39] 등을 통한 개인용 건강관리제품의 출시가 잇따르고 있으며, 각종의 웨어러블 장치(Wearable Devices)를 통하여 누구든지 언제 어디서나 손쉽게 생체정보를 수집하여 지속가능한 건강관리가 가능해졌다. 다만, 의료기기와 헬스케어기기는 목적과 기능이 다르고 그에 적용되는 법규가 달라지기 때문에 판단기준 등이 명확해야 하고 적용범위가 분명히 정해져 있어야 할 필요가 있다.



출처 : 최윤섭, “How the Implement Digital Healthcare in the Future”, BIOKOREA, 2016을 배현아, 앞의 글, 140면에서 재인용.

그런데 의료 및 헬스케어 분야에서 다루는 생체정보는 그 유형에 따라 개인의 “인식이나 인증”을 목적으로 하는 정보와 “치료 및 연

39) 모바일앱의 유형은 크게 ① 의료기기를 원격으로 제어하는 앱, ② 의료기기 등에서 측정된 데이터 등을 전송받아 표시, 저장, 분석하는 앱, ③ 모바일 플랫폼에 전극, 센서 등을 부착 또는 추가하여 모바일 플랫폼을 의료기기로 사용하는 앱, ④ 모바일 플랫폼에 내장된 센서를 이용하여 모바일 플랫폼을 의료기기로 사용하는 앱 등 매우 다양하다. 배현아, 앞의 글, 135면.

구”를 목적으로 하는 정보로 구별할 수 있으며, 아직까지는 치료나 연구의 목적으로 활용하는 경우가 일반적이라 할 수 있기 때문에, 생체정보의 개념을 이 분야와 어떻게 연관지어야 하는지에 관하여 논의할 필요가 있다. 즉, 의료 및 헬스케어 분야에 있어서는 생체정보의 식별자에 따라 그것이 애초에 식별성을 가지지 않는 것(예컨대, 혈압이나 혈당 등)과 가지는 것(예컨대, DNA와 심전도는 개인을 식별하기 위한 목적으로의 활용이 기술적으로도 가능한 상태이다[40])으로 구별하는 것이 필요하고, 식별성을 가지는 생체정보의 경우라도 그 활용목적이 치료나 연구목적으로 활용하는 것인지 개인식별을 목적으로 활용하는 것인지를 구체적으로 사례에 따라 파악하여야 한다.

현재, 추후 과학 및 의료기술이 발달함에 따라 다양한 생체적 정보가 생체인식정보로서 활용될 수 있는 가능성이 무한대로 열려있기 때문에 생체정보를 어떻게 보호해야 하는지에 대해서는 지속적으로 관심을 가져야 할 필요가 있다.

Ⅳ. 범죄수사 분야

생체정보는 과학수사의 일환으로 범죄를 특정하고 범인을 식별하기 위한 방법으로서 매우 오래 전부터 활용되어 왔다. 대표적으로 활용되고 있는 생체정보로는 지문, DNA, 얼굴, 음성, 걸음걸이 등을 들 수 있으며, 여러 가지의 식별자들이 다중으로 활용되기도 한다.

“지문”의 경우, 가장 빠르고 편리한 신원 확인 방법으로서 경찰청은 지문 데이터베이스를 운용하여 현재 약 4억 개의 지문을 수록하고 있으며 2010년과 2012년에 지문 데이터베이스를 새로 입력하고 검색 프로그램인 지문검색시스템(Automated Fingerprint Identification System, AFIS)의 성능을 향상하였다. 그리하여 2010년 이후 매년 살인·성폭

40) 김재성, “바이오인식시스템 보안위협과 차세대 Medical biometrics”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 43면.

력・강도・절도 등 공소시효가 남은 주요 미제 사건에 대해 지문 재검색을 실시, 약 5년간 총 3032개의 사건 관련 지문을 재검색해 1,157명의 신원을 새로 확인하였는데, 덕분에 영구미제로 남을 뻔한 374건을 해결한 것으로 알려져 있다.[41]

또한「실종아동등의 보호 및 지원에 관한 법률」에 근거하여 2012년부터 시행된 "실종아동 찾기"는 보호자가 원하는 경우 지문, 사진, 보호자 정보를 사전에 등록하여 아동, 지적 장애인, 치매환자의 실종이 있는 경우 신속한 대응이 가능한데, 2015년 8월 기준 241만 명이 등록하여 2015년 상반기 발생한 11세 미만의 실종 아동 2041명을 전원 찾았다고 하니 활용의 성과가 크다고 할 수 있다.[42]

CCTV를 통한 "얼굴인식"과 "걸음걸이"(법보행)는 범죄수사의 첫 단계에서 활용된다. 경찰청은 그동안 각 지자체에서 운영하는 CCTV통합관제센터와 연계해 영상정보를 실시간으로 수집하는 시스템을 개발하여 범죄자나 뺑소니범 검거 등에 활용하고 있었으나,「개인정보보호법」상 정보주체의 사전 동의 원칙에 위배된다는 지적으로 해당 시스템 사용을 중단하였다.[43] 그러나 CCTV의 활용범위를 극대화하기 위해 추적동선을 따라 확보한 CCTV 인물 간 동일성 확인 및 CCTV 인물과 용의자 사이의 동일성 확인 등을 위하여 '걸음걸이 분석기법'을 개발되어 활용이 계속되고 있다.[44]

---

41) 중앙일보, "10초면 열 손가락 지문 파악 "척 보면 용의자 알아요", 2015. 7. 11. http://news.joins.com/article/18217655 (2016.6.20. 최종접속)

42) 파이낸셜뉴스, "실종자 찾기, 우리 모두의 몫", 2015. 8. 1. http://www.fnnews.com/news/201508071657143432 (2016.6.20. 최종접속)

43) 경제신문 디지털타임스, "'안전지킴이 CCTV, 개인정보보호법에 발목", 2014. 11. 19. http://www.dt.co.kr/contents.html?article_no=2014112002100260800001 (2016.6.20 최종접속)

44) YTN science, [Science & Investigation] 바이오 인식 기술, 2013. 12. 4. 방송. http://science.ytn.co.kr/program/program_view.php?s_mcd=0082&s_hcd=&key=201312041631167881 (2016.9.20 최종접속)

최근에 범죄수사에 가장 완벽한 생체정보로서 활용되고 있는 것은 “DNA”라고 할 수 있다. 우리 법제는 일단 한번이라도 죄를 지으면 모두 재범 가능성이 있는 것으로 보고 수형인 등으로부터의 디엔에이 감식시료 채취를 폭넓게 인정하고 있기 때문에(「디엔에이신원확인정보의 이용 및 보호에 관한 법률」(이하 디엔에이법) 제5조), 이를 통하여 장기 미제사건이 유전자 검사를 통해 해결되는 등 범죄수사 분야에서 DNA의 활용가치는 매우 크다고 할 수 있다. 다만, 이러한 인식기술의 발전이 범죄퇴치의 측면에서 매우 효율적으로 기여한다는 장점은 분석시스템이 대규모화 내지 일상화 하는 경우에 대한 부작용과도 연결되기에 우려하지 않을 수 없다. 특히 얼굴인식의 경우 정보주체의 인식이나 거부감 없이 생체정보를 손쉽게 취할 수 있어 그 광범위한 사용은 공공영역에서 익명성을 배제하고 개인에 대한 끊임없는 추적이 가능하게 된다는 점에서, 그리고 DNA의 경우 개인의 건강과 관련된 매우 민감한 정보가 공개 또는 유출될 위험이 항상 뒤따르게 된다는 점에서 매우 유의하여야 한다.

그럼에도 불구하고 디엔에이법은 DNA의 데이터베이스의 관리·운영에 대한 적절한 관리 감독 체계를 마련하고 있지 않고 있어 사실상 경찰과 검찰의 자율에 맡겨져 있다는 점에서 이에 대한 제도개선이 시급하다.[45] 나아가 심리생리검사라 불리는 소위 거짓말탐지기, 지능형 전자발찌 등과 관련하여서도 생체정보의 활용에 대한 타당성 논의도 계속되고 있는데,[46] 다각적 측면에서 파악되어야 할 필요가 있다.

---

45) 이창범, 앞의 글, 124면은 같은 취지에서 「형사사법절차 전자화 촉진법」에 따른 ‘형사사법정보시스템’도 형사사법정보의 전자화에만 관심이 있고, 누구에 관하여, 어떤 정보가, 어떻게, 언제까지, 어떤 방식으로, 어떤 목적을 위해 이용되고 있는지 공개되어 있지 않은 점 등 관리 감독 체계가 전무하다는 비판을 함께 지적한다.

46) 자세한 것은 정소영, “생체정보의 분야별 활용현황 – 범죄수사 분야”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 148-150면 참조.

그런데 이러한 범죄수사 분야에서의 생체정보는 앞에서 언급한 의료 및 헬스케어분야에서의 생체정보 경우와 마찬가지로 “인식”이나 “인증”의 목적을 가진 본래의 생체인식정보(biometric data)가 아닌 생체적 정보 내지 생명정보(bio information)가 포함될 수 있으므로 모든 생체정보를 획일적으로 단정하기에는 어려운 면이 있다. 다만, 범죄수사라는 분야의 특수성은 그러한 인식 또는 인증의 목적인 생체정보는 물론이거니와 그러한 목적을 가지지 못한 생체적 정보라 하더라도 그러한 개인정보를 수집하거나 활용하는 부분에 대해서는 국민의 기본권을 직접적으로 침해할 우려가 크기 때문에, 최대한 개인의 신체적 자유가 보장되는 한도 내에서 그 정의와 보호수준이 별도로 정해져야 할 필요가 있다.

제 3 절 소 결

Ⅰ. 생체정보의 개념과 용어

우선, “생체정보”라는 용어와 관련하여 행정자치부에서 마련하고 있는 「바이오정보보호 가이드라인(안)」 등 정부부처에서는 “생체”라는 용어가 가진 생체실험 등과 같은 부정적 연관성 등으로 업계 및 학계가 가치중립적으로 생체의 영어발음 그대로 바이오라는 용어를 사용하기로 묵시적 합의를 본 것으로 보인다.[47] 그런데 “바이오정보”라고 하는 경우 생체인식정보(biometric data)가 아닌 일반적인 건강정보 내지 생명 정보[48](bio information)까지도 포함하는 것으로 오인할 가능성이 있으며,[49] 그렇게 되는 경우 본질적인 논의에 접근하는 데에 어려움이 있다(생체정보와 건강정보와의 차이는 후술한다). 그리하여 이하

47) 생체정보와 생체인식정보, 바이오정보 등 정의와 개념에 관하여는 박정훈・김행분, 앞의 글, 85-86면 참조.
48) 이원상, 앞의 글, 110면.
49) 심우민, 앞의 글, 4면.

에서는 “생체인식정보”의 의미를 가지는 것을 전제로 하여 “생체정보”로 표기하기로 한다.

생체정보는 사람의 고유한 신체적·행동적 특징으로 개인을 식별할 수 있게 하는 정보로서 그 자체로서 한 사람을 특정할 수 있기 때문에 보호의 필요성이 매우 크다.

그런데 생체정보는 매우 추상적이어서 그것이 정확히 무엇을 의미하는지를 정할 필요가 있다. 즉, 위에서 정의한 바와 같이 “개인의 식별이나 인증을 위한” 정보일 수도 있지만, “개인의 식별과는 무관한” (생명·건강에 관한) 정보일 수도 있다. 그리하여 최근에는 전자를 “생체인식정보”라고 하여 법령 등이 특별히 보호하여야 할 개인정보로 분류하여야 할 필요가 있음을 주장하는 견해가 많아지고 있다.[50] 영어의 경우 전자를 “biometric data” 또는 “biometrics”라 하여 “bio informatics”라는 건강정보와는 용어가 명확히 구분되지만 우리말의 경우 혼용하여 사용되기에 별도로 구별할 필요가 있는 것이다.

“생체”라는 용어가 주는 불편함으로 인하여 “바이오정보”라 사용하는 경우가 많은데, 2007년 수립된 정보통신부 및 KISA의 「바이오정보 가이드라인」에서의 정의나 「정보통신망법」 시행령 제15조(개인정보의 보호조치)에서의 사용이 그러하다. 바이오정보 또한 생체정보의 경우와 같은 의미인 것으로 보아 그것이 인식이나 식별기능을 하는 특정한 경우에 사용되는 것이라면 “바이오인식정보”라고 보다 정확히 표현할 필요가 있다. 이는 행정자치부에서 수립 중인 가이드라인(안)에서는 적절하게 반영이 되어 있는 것으로 보인다(자세한 내용은 후술한다).

다만, 이는 용어의 명칭 내지 개념에 관한 문제이기 때문에, 과연 이러한 생체정보를 용어까지 구별하여 사용할 규범적 실익이 있느냐

50) 이원상, 앞의 글, 111면은 생체정보를 개인식별을 위한 “생체인식정보/바이오인식정보”, 맥박이나 심전도와 같은 “생체신호”, 신장이나 몸무게 같은 “신체외관정보”로 분류하고 있는데, 분류의 취지에 동감한다.

는 의문을 가질 수 있다. 왜냐하면 일부 법령에서 “생체적 특성” 또는 “바이오정보”라고 규정하고 있지만, 그 의미에 있어서는 모두 “식별기능”이 있는 생체정보를 의미하는 것이고, 식별자의 유형의 예시도 그러한 취지에서 들고 있다는 점에서 본질적인 면에서는 차이가 없기 때문이다. 그러나 개념 자체의 문제는 정보보호의 목적과 범위, 보호의 정도를 정하기 위하여 구분하여 이해할 필요가 있으며, 무엇보다도 규범을 명확히 할 필요가 있다는 점에서 짚어볼 필요가 있다.

Ⅱ. 생체정보의 범위

넓은 의미로 사용되는 모든 생체정보와 식별기능에 초점을 맞춘 생체인식정보의 구별 필요성은 생체정보와 의료(건강)정보에서 명확해진다. 의료는 생체와 맞닿아 있으며, 수많은 생체정보를 다루는 분야이기 때문이다. 그러나 질병 치료를 목적으로 하는 환자의 개인정보는 진료정보 내지 의료정보라 할 수 있으며, 이는 인식이나 인증을 목적으로 하는 것이 아니고 따라서 「보건의료기본법」과 「의료법」의 보호대상이 되며, 그 법에 의하여 개인정보로서 보호된다는 점에는 의문이 없다. 다만, (원격의료에 관한 사회적 합의가 이루어지지 않고 있어 단정적으로 언급을 할 수는 없지만) “헬스케어”와 “의료”의 영역이 분명하게 나누어져 있지 않으며, 더욱이 그 안에서 사용되는 생체정보의 성격이나 범주, 보호조치 등에 대하여는 명백한 구분이 없는 것이 사실이다.

특히 「의료법」상 전자의무기록에 저장된 개인정보에는 “환자의 이름・주소・주민등록번호 등과 같은 ‘개인식별정보’ 뿐만 아니라 환자에 대한 진단・치료・처방 등과 같이 공개로 인하여 개인의 건강과 관련된 내밀한 사항 등이 알려지게 되고, 그 결과 인격적・정신적 내면생활에 지장을 초래하거나 자유로운 사생활을 영위할 수 없게 될

위험성이 있는 의료내용에 관한 정보도 포함된다"는 법원의 해석[51]에 비추어 볼 때, 의료분야 혹은 경계가 불분명한 헬스케어 분야에서 생체정보를 어떻게 파악하고 그것을 수집 및 관리(활용)할 것인지에 관한 논의가 적극적으로 진행되어야 할 것이다. 이는 의료분야에서 생체정보가 가지는 이중적 기능을 보장하기 위한 것이기도 한데, 개인정보로서 매우 강한 정보주체의 보호가 필요한 반면에, 생명공학 및 의학적 연구를 위하여 가능한 한 많은 생체정보를 보유하고 그것을 활용하여 의학발전에 기여하는 것도 불가피하기 때문이다.

그리하여 "치료 및 연구목적"의 생체정보와 "개인식별목적"의 생체인식정보는 분리하여 파악하는 것이 필요한데, 전자의 경우 과학기술과 산업의 발전을 위하여 자유롭게 활용할 수 있도록 하고,[52] 후자에 해당하는 경우에는 그것이 비록 의료정보라 하더라도 그 정보의 수집과 이용 및 폐기에 관하여 정보주체가 철저하게 관리할 수 있도록 각종의 보호장치를 마련해야 할 것이다.[53][54]

---

51) 대법원 2013. 12. 12. 선고 2011도9538.

52) 이인호, "「개인정보보호법」상의 '개인정보' 개념에 대한 해석론 - 익명화한 처방전 정보를 중심으로-", 「정보법학」, 제19권제1호, 2015. 4, 70-71면. 이는 개인정보는 '정보주체의 것'이니까 다른 사람은 정보주체의 동의 없이는 원칙적으로 수집·이용·제공할 수 없다는 '절대적 보호'에 치우치는 것은 개인정보보호법의 목적과 성격을 잘못 이해한 것으로서 정보의 '보호'와 '이용'의 적절한 균형이 필요하다는 논리를 전제로 한 것이다. 이인호, 앞의 글, 64-65면.

53) 참고로, 미국 의료정보보호법(HIPPA)에서는 '개인을 식별할 수 있는 의료정보', 즉 개인을 식별하거나 또는 그 정보가 개인을 식별하는데 사용될 수 있다고 믿을 만한 합리적인 근거가 있는 의료정보에 한하여 정보보호의 대상이 된다는 명문의 규정을 두어 이러한 논의를 입법적으로 해결하였다. 42 U.S.C. §1302d(6) 참조. https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d-6.pdf (2016.10.20. 최종접속)

54) 앞의 각주에서 보호대상인 개인정보로서 HIPPA에서 제시하고 있는 "완전히 제거되어야 하는 개인식별자"는 다음과 같다. 즉, 이들 정보는 무단으로 공개, 사용, 접근하는 것을 방지하기 위하여 "익명화"되어야 하는 정보목록인 것이다.

> 1. 이름, 2. 우편번호 및 그와 동등한 지역번호, 3. 생년월일, 입학일, 졸업일, 사망일, 개인과 관련된 날짜의 모든 요소, 4. 전화번호, 5. 팩스번호, 6. 이메일주

Ⅲ. 생체정보의 성격

생체정보는 사람의 신체적·행동적 특징을 기반으로 개인의 신원을 확인할 수 있는 정보를 말하며, 성명이나 주민등록번호 등과 같은 개인정보 식별자와 결합되어 개인을 식별하게 되기 때문에 당연히 "개인정보"에 해당된다. 그런데 현행법에서의 개인정보의 정의규정은 그 외관상 생체정보를 모두 포함하고 있는 것처럼 볼 수 있지만, 생체정보는 인간의 신체에 대한 정보를 개인식별을 위하여 사용하는 영역이기 때문에 개인정보와 동일한 개념으로 파악하기에는 문제가 있어 보이며, 보다 두터운 보호장치가 필요한 것이 아닌가 생각이 된다.

또한 생체정보는 일반 개인정보보다 민감한 사항이 다루어질 수 있는 영역이라는 점[55]에서 "민감정보"와 유사한 성격을 가진다. 규범적인 의미로서가 아니더라도 생체정보는 그야말로 개인의 "민감한 정보"이기 때문에 누구든지 당연히 민감정보에 속하는 것으로 여길 수 있다. 그러나 우리 법령에서 정하고 있는 민감정보는 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보"이어야 하는데다가 "대통령령으로 정하는 정보"이어야 하기 때문에 현행대로라면 '생체정보가 곧 민감정보이다' 라고 단정하기에도 어려운 면이 있다.[56]

소, 7. 사회보장번호, 8. 진료기록번호, 9. 건강보험 수급자 번호, 10. 은행계좌번호, 11. 면허증번호, 12. 자동차등록번호와 자동차식별번호 및 고유번호, 13. 의료기기 식별항목 및 고유번호, 14. Web URL, 15. 인터넷프로토콜(IP)주소, 16. 지문, 음성 등 생체측정정보, 18. 유일한번호, 특징, 기호.

출처 : 박미정, 앞의 논문, 122-123면에서 인용.

55) 조규범, 앞의 "생체정보 보호를 위한 입법론적 고찰", 193면.

56) 오길영, 앞의 글, 236면은 지문이나 정맥, 얼굴화상 또는 성문 등 대다수의 생체정보는 그 자체만으로 건강이나 유전정보를 담고 있지 않기 때문에 동법이 규정하고 있는 민감정보로서의 보호를 받지 못한다는 의견을 제시한다.

이러한 점에서 생체정보를 기존의 개인정보나 민감정보와 동일하거나 유사한 유형 정도로 파악하는 것은 현실적 규율의 필요성에 대한 수요를 충족시키지 못하는 면이 있다. 따라서 법령 등에서 개인정보나 민감정보와는 다른 별도의 정보로서 인정하고 그에 관한 개념이나 별도의 보호장치를 두어 생체정보만이 가진 편리성과 위험성이라는 양면적 특성에 대비할 필요가 있다고 생각한다.

제 3 장 생체정보 관련 법제 현황

제 1 절 서 설

Ⅰ. 생체정보의 도입

생체정보는 그 의미와 기능에 따라 금융, 의료, 수사 등의 분야에서 매우 활발하게 활용되고 있으며 앞으로 더 많은 식별자가 더 다양한 분야에서 개발될 가능성이 인정된다. 생체정보에 대한 활용의 수요가 많아짐에 따라 기술적·산업적 발전이 이를 충족시키는 것은 자연스러운 현상으로서 생활의 편리함에 있어서는 큰 이점이 있지만, 그 이면에 도난 및 유출의 가능성이 커지며 정신적·재산적 피해도 막심하기 때문에 정보의 보호 내지 보안에 대한 준비가 필요한 것이다. 특히 생체정보의 불가변적 및 만인부동의 성격은 도난이나 유출이 발생한 경우 그 회복이 매우 어렵기 때문에 그에 대한 기술적·제도적 예방 및 보호조치들이 반드시 사전에 마련되어 있어야 할 것이다

그렇다면 우리 현행 법제에서 마련되어 있는 생체정보에 관한 규율은 어떠한지에 대하여 살펴볼 필요가 있다.

우선, 주지하는 바와 같이 우리나라는 70년대부터 주민등록증 신청하기 위하여 지문을 찍도록 하였고 그 근거규정을 「주민등록법」 및 같은 법 시행령에 두었는데, 이는 생체정보의 본래적인 이용, 즉 본인을 인식하고 인증하기 위한 수단으로서 인정한 초기의 입법례라고 할 수 있다. 다만, 이것은 행정이나 범죄수사의 공공분야에서 폐쇄적으로 사용되었던 것으로 현재와 같이 민간영역에서 인터넷을 통해 상업적으로 이용하고 활용하는 수준은 아니였다. 「주민등록법」과는 달리 여권법에서는 비교적 늦게 2008년에 이르러서야 여권에 수록되는 정보로서 지문을 추가하였다.

“생체정보” 내지 “바이오정보”이라는 용어를 법령의 규정에 도입한 입법례는 그리 많지 않다. 이것은 아직은 법률이 생체정보의 개념을 개인정보와 같은 것으로 인식하고 있으며 개인정보에 대한 보호와 같은 수준으로 규율하는 것으로 충분하다고 인식하는 정도에 머무르고 있기 때문인 것 같다. 생체정보가 보다 본격적으로 법률 규정에 처음으로 도입된 것은 2007년 「전자금융거래법」을 제정하면서 부터였다. 전자금융거래에서 전자금융의 이용자 및 거래내용의 진실성과 정확성을 위하여 사용되는 일정한 정보를 “접근매체”라 하는데, 이러한 접근매체로서 각종의 비밀번호와 전자정보 외에 “생체정보”를 명시한 것이다(제2조 제10호). 그 후 2008년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법) 시행령의 개정을 통하여 정보통신서비스제공자 등으로 하여금 이용자의 비밀번호 및 “바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)”에 대한 보안조치를 하도록 의무를 부과하였다(제15조제4항제1호).

이렇듯 아직은 생체정보 개념과 성격이 명확히 정립되지 않은 이유로 생체정보에 관한 규정이 기존의 법제에 전면적으로 포섭되고 있는 것 같지 않다. 그리하여 이하에서는 생체정보를 명문으로 둔 법령을 포함하여, 현재 생체정보의 개념을 포섭할 수 있는 개인정보의 관점에서 관련 법제의 현황을 살펴보고자 한다.

Ⅱ. 관련 법제의 분류

생체정보에 관하여 완결적인 입법이 없기 때문에 아직 그것은 개인정보의 틀 속에서 이해하여야 하는 한계가 있다. 그러나 개인정보에 관하여는 매우 다양한 법령들이 그 개념과 범위 및 보호조치 등에 대해 규정을 두고 있기 때문에, 생체정보를 활용되는 분야에 따라 입법

의 필요성 등에 관한 논의 가능성은 충분히 열려있다고 본다. 그리하여 관련 법령을 어떠한 기준으로 구분하여 적용법규를 파악하는 것이 좋은지에 대하여도 아직은 정해진 바는 없다.

우선, 첫째로, 생체정보의 활용영역을 기준으로 공공분야와 민간분야로 구분할 수 있다. 이 경우 「주민등록법」이나 「여권법」, 범죄수사와 관련된 법령 등은 전자에 해당될 것이고, 각종의 금융관계법과 의료관계법 등은 후자에 해당될 것이다. 이 두 분야에 망라하여 적용되는 「개인정보보호법」은 중요한 기능을 담당한다.

둘째로, 생체정보에 적용되는 법령을 기준으로 일반법과 특별법으로 구분할 수 있다. 즉 「개인정보보호법」은 분야를 막론하고 가장 개인정보에 관한 한 일반적으로 적용되는 법으로서 "다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에 따른다"(제6조)는 규정에 근거하여 개별 규정이 있는 경우에 대응하여 일반법으로 구분할 수 있다. 또한 금융분야에 있어서는 「정보통신망법」도 이러한 일반법적인 지위를 가지며(제5조), 의료분야에 있어서 「생명윤리법」의 경우도 일반법적 성격을 가진다고 할 수 있다(제4조).

셋째로, 생체정보의 기능을 기준으로 하여 인식 또는 인증분야와 헬스케어 서비스분야, 공공행정 분야 등으로 개별적으로 판단하여 관련 법령을 구분하는 것이다. 즉 금융관련 법령에서는 생체정보의 인식 및 인증기능이 중요하고, 의료관계법에서는 건강정보와 생체정보의 관계가 문제되며, 행정 분야에 있어서는 「주민등록법」이나 「여권법」, 범죄수사와 관련하여 다양한 생체정보가 활용되기 때문이다.

이와 같이 생체정보의 기능과 활용영역에 따라 법령을 다양하게 구분할 수 있지만, 위에서 언급한 바와 같이 생체정보라는 정확한 개념과 기능을 법률이 아직은 제대로 인식하고 있지 못하고 있기 때문에 "개인정보"라는 넓은 개념 속에서 법제의 현황을 파악해야 하는 한계가 있다. 그리하여 이하에서는 생체정보의 개념과 기능 및 활용분야

를 전체적으로 반영하여 현행의 법령의 주요 규정을 위주로 법제 현황을 소개하고자 한다.

제 2 절 생체정보 관련 법제

Ⅰ. 개인정보보호법

1. 입법목적 및 체계

「개인정보보호법」은 개인정보의 유출·오용·남용 등 개인정보 침해에 대하여 국민의 프라이버시 침해는 물론 정신적·금전적 피해를 예방하거나 최소화하기 위하여 국제 수준에 부합하는 개인정보 처리 원칙 등을 규정함으로써 국민의 사생활의 비밀을 보호하고 개인정보에 대한 권리와 이익을 보장하고자[57] 2011년 3월에 제정되었다. '공공부문과 민간영역을 모두 아우르는'[58] 일반법으로서 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다(제6조).

이 법은 개인정보의 수집, 이용, 처리 등과 관련하여 정보주체의 권리와 개인정보처리자의 의무에 관한 내용을 주된 규율사항으로 한다.

< 개인정보보호법의 체계 >

제1장 총칙 제2장 개인정보 보호정책의 수립 등 제3장 개인정보의 처리

57) 「개인정보보호법」의 제정이유 참고.
http://www.law.go.kr/lsInfoP.do?lsiSeq=111327&ancYd=20110329&ancNo=10465&efYd=20110930&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2016.10.10. 최종접속)

58) 김민호, "개인정보처리자에 관한 연구", 「성균관법학」, 제26권제4호, 2014. 12, 243면.

제1절 개인정보의 수집, 이용, 제공 등
제2절 개인정보의 처리 제한
제4장 개인정보의 안전한 관리
제5장 정보주체의 권리 보장
제6장 개인정보 분쟁조정위원회
제7장 개인정보 단체소송
제8장 보칙
제9장 벌칙

2. 개인정보 관련 규정

(1) 개인정보의 개념

「개인정보보호법」에서 다루고 있는 개인정보는 가장 일반적인 개념이라고 할 수 있으며, 그밖에 "특수한" 개인정보로 처리가 제한되어야 하는 경우로서 "민감정보", "고유식별정보", "주민등록번호", "영상정보" 등을 특정하여 그러한 정보는 가중된 처리제한의 요건을 부여하고 있다(제23조 내지 제25조).

우선, 이 법에 의하면, "**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(제2조제1호).

이 법은 이러한 개인정보를 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인인 개인정보처리자(같은 조 제5호)에 대하여 개인정보의 수집, 이용, 제공, 처리 및 안전한 관리를 위한 일련의 제한 내지 의무를 규정하고 있다.[59] 즉, 개인정보처리자는 법률이

59) 이러한 개인정보의 처리와 안정성 등을 위한 위임행정규칙으로서 「표준 개인정보 보호지침」(행정자치부고시 제2014-1호), 「개인정보보호 관리체계 인증 등에 관한

정하는 일정한 경우에 한하여 **"정보주체의 동의"**를 받아 개인정보를 수집할 수 있고 그 **"수집 목적의 범위에서만"** 이용할 수 있으며(제15조), 개인정보를 수집하는 경우에도 그 목적에 필요한 **"최소한의"** 개인정보를 수집하여야 하며(제16조), 수집된 정보는 일정한 경우에만 제3자에게 제공할 수 있고(제17조), 법률이 정한 목적의 범위를 초과하여 이용하거나 제3자에게 제공하여서는 안된다(제18조).

또한 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 그 수집출처 등을 고지하여야 하며(제20조), 보유기관이 경과하거나 개인정보의 처리목적이 달성되는 등 개인정보가 불필요하게 되었을 때에는 지체없이 그 정보를 **"파기"**하여야 한다(제21조).

(2) 민감정보의 개념

「개인정보보호법」은 특히 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는" "**민감정보**"에 관하여 규정하고 있다. 여기서 "대통령령이 정하는" 민감정보의 범위는 같은 법 시행령 제18조에 따라 ① 유전자검사 등의 결과로 얻어진 유전정보, ②「형의 실효 등에 관한 법률」제2조 제5호에 따른 범죄경력자료에 해당하는 정보에 한한다.

개인정보처리자는 민감정보의 처리와 관련하여 ① 정보주체에게 법률이 정한 사항을 알리고 다른 개인정보의 처리에 대한 동의와 **별도로** 동의를 받은 경우와, ② 법령에서 민감정보의 처리를 요구하거나 허용하는 경우가 아닌 한 이를 처리할 수 없다(제23조)는 원칙을 두고 있다.

고시」(행정자치부고시 제2016-28호),「개인정보의 안전성 확보조치 기준」(행정자치부고시 제2014-7호) 등이 있다.

3. 개인정보의 보호

「개인정보보호법」에서의 개인정보보호는 일반적으로 적용되는 규율로서 그것은 개인정보처리자가 지켜야 하는 다양한 의무로 규정되어 있다. 그 체계를 크게 보면 “개인정보의 처리”에 관한 것으로서 개인정보의 수집, 이용, 제공 등에 있어서의 원칙과 처리제한의 경우로 구별할 수 있다.

개인정보의 처리와 관련하여 가장 기본적인 원칙은, 개인정보를 수집하기 위하여는 정보주체의 “동의”를 받아야 하고, 그 수집 “목적”에 구속되며, 이러한 동의와 목적의 효력기간이 다한 때에는 지체없이 그 개인정보를 파기하여야 한다는 것이다.

< 「개인정보보호법」상 개인정보보호의 체계 >

제3장 개인정보의 처리
제1절 개인정보의 수집, 이용, 제공 등
 제15조 개인정보의 수집·이용
 제16조 개인정보의 수집 제한
 제17조 개인정보의 제공
 제18조 개인정보의 목적 외 이용·제공 제한
 제19조 개인정보를 제공받은 자의 이용·제공 제한
 제20조 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지
 제21조 개인정보의 파기
 제22조 동의를 받는 방법
제2절 개인정보의 처리 제한
 제23조 민감정보의 처리 제한
 제24조 고유식별정보의 처리 제한
 제24조의2 주민등록번호 처리의 제한
 제25조 영상정보처리기기의 설치·운영 제한

(1) 개인정보의 처리

개인정보처리자는 정보주체의 “동의”를 받는 등 일정한 경우에 한하여 개인정보를 수집할 수 있으며, “그 수집 목적의 범위에서” 이용할 수 있다(제15조제1항). 우선, 개인정보의 수집 시에 동의를 받을 때에는 정보주체에게 “① 개인정보의 수집·이용목적, ② 수집하려는 개인정보의 항목, ③ 개인정보의 보유 및 이용기간, ④ 동의를 거부할 권리가 있다는 사실 및 동의거부에 따른 불이익이 있는 경우에는 그 불이익의 내용”을 알려야 한다(같은 조 제2항).

그리고 정보를 수집함에 있어서는 “그 수집 목적”에 필요한 “최소한의 개인정보”를 수집하여야 한다(제16조). 이러한 “동의”와 “목적”에

의한 제한은 개인정보처리자가 정보주체의 개인정보를 제3자에게 제공하는 경우에도 유지된다(제17, 18조). 특히 이러한 제3자제공의 경우에는 정보주체에게 "① 개인정보를 제공받는 자, ② 개인정보를 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목, ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용"을 알려야 한다(제17조제2항).

(2) **민감정보의 처리**

한편, 개인정보가 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는" 민감정보인 경우에는 원칙적으로 처리가 금지되며, 예외규정으로 정한 바에 한하여 이를 허용한다. 즉, 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 경우에만 가능하며, 이러한 민감정보를 처리하는 경우 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조(안전조치의무)에 따른 안전성 확보에 필요한 조치를 하여야 한다(제23조).

안전조치의무에 관한 제29조 규정에 의하면, "개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 **기술적·관리적 및 물리적 조치**를 하여야 한다."

(3) **영상정보의 처리**

영상정보처리기기, 즉 CCTV는 원칙적으로 공개된 장소에 설치·운영되어선 안된다. 다만, 일정한 경우, 즉 ① 법령에서 구체적으로 허

용하고 있는 경우, ② 범죄의 예방 및 수사를 위하여 필요한 경우, ③ 시설안전 및 화재 예방을 위하여 필요한 경우, ④ 교통단속을 위하여 필요한 경우, ⑤ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우에 한하여 가능하다(제25조제1항).

특히 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 안된다. 이러한 영상정보처리기기를 설치·운영하는 자는 정보주체가 쉽게 인식할 수 있도록 안내판을 설치하는 등 필요한 조치를 하여야 한다. 안내판에는 ① 설치 목적 및 장소, ② 촬영 범위 및 시간, ③ 관리책임자 성명 및 연락처, ④ 그 밖에 대통령령으로 정하는 사항이 포함되어야 한다(같은 조 제4항).

Ⅱ. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

1. 입법취지 및 체계

「정보통신망법」은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하기 위한 법이다(제1조).

이 법은 그 목적을 달성하기 위하여 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제인 정보통신망을 이용하여 과정에서 개인정보를 처리할 때 준수하여야 하는 내용을 담고 있다(제22조 이하).

따라서 정보통신망을 통하여 개인정보를 취급할 때에는 이 법이 「개인정보보호법」의 특별법으로 우선 적용되며, 이러한 한도에서 생체정보를 규율하는 일반법으로 기능한다고 볼 수 있다.

< 정보통신망법의 체계 >

제1장 총칙
제2장 정보통신망의 이용촉진
제3장 삭제 <2015.6.22>
제4장 개인정보의 보호
 제1절 개인정보의 수집·이용 및 제공 등
 제2절 개인정보의 관리 및 파기 등 <신설 2007.1.26>
 제3절 이용자의 권리
제5장 정보통신망에서의 이용자 보호 등 <개정 2007.1.26>
제6장 정보통신망의 안정성 확보 등
제7장 통신과금서비스 <신설 2007.12.21>
제8장 국제협력 <신설 2007.12.21>
제9장 보칙 <신설 2007.12.21>
제10장 벌칙 <신설 2007.12.21>

2. 개인정보 관련 규정

「정보통신망법」은 "**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"(제2조제6호)고 정의하고 있다. 이 법에서 정한 개인정보와 「개인정보보호법」 상의 개인정보의 개념과 본질적으로는 같은 사항이지만, 「정보통신망법」은 적용분야의 특성을 고려하여 개인정보를 보다 구체화한 것으로 볼 수 있다.

< 개인정보 개념의 비교 >

개인정보보호법	정보통신망법
“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.	“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.

이 법은 제4장(개인정보의 보호)에서 개인정보의 수집·이용 및 제공(제2절), 개인정보의 관리 및 파기(제2절), 이용자의 권리(제3절)에 관하여 다수의 규정을 두고 있다.「개인정보보호법」상의 개인정보처리자가 이 법에서는 정보통신서비스제공자로 되어 있는 외에 정보통신서비스에 대한 **접근권한**(제22조의2)이나 본인확인업무를 수행하는 **본인확인기관의 지정**(제23조의3) 등에 관한 규정이 추가되어 있으며,「개인정보보호법」상의 개인정보수집, 이용, 제공, 처리 등에서 지켜져야 하는 주요한 원칙들은 이 법에서도 유효하게 적용되어 있다.

한편, 개인정보의 수집제한과 관련하여「개인정보보호법」상의 “민감정보”는 이 법에서는 그 용어가 명시적으로 사용되고 있지는 않으나 유사한 취지의 규정이 마련되어 있다.

< 민감정보 개념의 비교 >

개인정보보호법	정보통신망법
제23조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노같은	제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사

개인정보보호법	정보통신망법
조합・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. 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	상, 신념, 가족 및 친인척관계, 학력(學歷)・병력(病歷), 기타 사회활동 경력 등 개인의 권리・이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다. ② ~ ③ 생략

3. 개인정보의 보호 : 바이오정보의 암호화 저장

「정보통신망법」은 2009년 개정을 통하여 주민등록번호의 유출로 인한 피해를 예방하기 위하여 정보통신망서비스제공자로 하여금 주민등록번호 외의 회원가입 방법을 의무적으로 제공하도록 하였다. 그리하여 주민등록번호의 수집을 최소화함과 동시에 개인정보의 보호조치를 강화하는 조치를 취하였다.

그리하여 이 법 제28조는 개인정보의 보호조치로서 "정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실・도난・유출・위조・변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 **기술적・관리적 조치**를 하여야 한다."고 규정하고 있다. 「개인정보보호법」의 "기술적・관리적 및 물리적 조치"와 비슷한 보호조치로 정할 필요가 있다.

< 개인정보 보호조치의 비교 >

개인정보보호법	정보통신망법
제29조(안전조치의무) 규정에 의하면, “개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 **기술적·관리적 및 물리적 조치**를 하여야 한다.	제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 **기술적·관리적 조치**를 하여야 한다. 1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 **4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치** 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 ② 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다.

이러한 기술적·관리적 조치가 필요한 영역으로서 법률은 “개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조

치”(제4호)를 언급하고 있다. 이에 따라 이 법 시행령은 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 일정한 보안조치를 하도록 의무를 부과하고 있다(제15조제4항).

중요한 것은 이러한 보안조치의 하나로서 이 법 시행령은 2009년 개정을 통하여 “주민등록번호, 계좌정보 및 **바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)** 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장”(제2호)을 추가하였다는 점이다. 이는 바이오정보, 즉 생체정보에 관하여 용어와 정의 및 유형을 명문화한 첫 입법례로서 의미가 있다.

< 개인정보의 보호조치의 변화 >

2009년 이전	2009년 개정	현행(2014. 11)
제15조(개인정보의 보호조치) ① 법 제28조에 따른 개인정보의 안전성 확보에 필요한 기술적·관리적 조치는 다음 각 호와 같다. 1. 개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한	제15조(개인정보의 보호조치) ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다. 1. 비밀번호 및 **바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장** 2. ~ 4. 생략	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 **바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다) 등 방송**

2009년 이전	2009년 개정	현행(2014. 11)
조치 **4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치** 5.~6. 생 략		**통신위원회가 정하여 고시하는 정보의 암호화 저장**

이 시행령 규정은 2014년 11월 28일 개정을 통해 바이오정보를 암호화함에 있어서 "일방향" 암호화 저장을 하도록 규정한 데에 대하여, 이러한 제한문구를 삭제하여 "양방향" 내지 "쌍방향" 암호화 저장도 가능하도록 하고 있는데, 이는 암호화 방식의 제한을 삭제함으로써 전자결재의 간소화할 수 있도록 한 것으로 평가된다.[60]

Ⅲ. 전자금융거래법

1. 입법취지 및 체계

「전자금융거래법」은 전자금융거래의 법률관계를 명확히 하여 전자금융거래의 안전성과 신뢰성을 확보함과 아울러 전자금융업의 건전한 발전을 위한 기반조성을 함으로써 국민의 금융편의를 꾀하고 국민경제의 발전에 이바지함을 목적으로 한다(제1조).

이 법은 전자금융거래와 전자지급거래에 관련된 용어의 의미를 명확히 하고, 전자금융의 당사자인 금융회사와 전자금융업자, 이용자의 범위와 함께 결제중계시스템, 전자문서, 각 종의 지급수단 등의 안전성과 신뢰성 확보에 관한 규정을 두고 있다. 전자거래에서 이용자 본

60) 이승재, 위 발표문, 64면 참조. 다만, "일방향" 및 "양방향(쌍방향)"의 보안성에 관하여는 기술적으로 논란의 여지가 있는 것으로 보인다.

인인 확인하는 수단인 “접근매체”는 가장 기본적으로 개인정보와 관련된 사항이라 할 수 있다.

< 전자금융거래법의 체계 >

제1장 총칙 제2장 전자금융거래 당사자의 권리와 의무 제3장 전자금융거래의 안전성 확보 및 이용자 보호 제4장 전자금융업의 허가와 등록 및 업무 제5장 전자금융업무의 감독 제6장 보칙 제7장 벌칙

2. 생체정보 관련 규정

「전자금융거래법」에서 생체정보와 관련이 있는 중요한 개념은 “접근매체”로서 제2조는 이를 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 일정한 수단 또는 정보로 정의하면서 다음과 같이 각 호를 들어 예시하고 있다(제10호).

가. 전자식 카드 및 이에 준하는 전자적 정보,
나. 「전자서명법」 제2조제4호의 전자서명생성정보 및 같은 조 제7호의 인증서,
다. 금융회사 또는 전자금융업자에 등록된 이용자번호,
라. 이용자의 생체정보,
마. 가목 또는 나목의 수단이나 정보를 사용하는데 필요한 비밀번호.

다만, 여기서 이용자의 생체정보는 2007년 이 법이 제정될 때부터 포함이 되었던 사항으로서, 현재 논의되고 있는 다양한 생체정보 식

별자를 다양하게 활용하기 위한 취지에서 도입된 규정이라고 보기에는 어렵겠고, 본인을 확인할 수 있는 지문 정도를 의미한 것으로 추측할 수 있다.

3. 개인정보의 보호

이 법은 명시적으로 “개인정보의 보호”라는 규정을 두고 있지는 않고, 그것이 상징적으로 포함되어 있는 접근매체 자체의 보안과 접근매체를 통한 다양한 금융거래의 안전을 포괄하여 규정한다. 즉, 접근매체 자체의 보안과 관련하여서는 금융회사 또는 전자금융업자는 접근매체를 선정하여 사용 및 관리함에 있어서는 이용자의 신원, 권한 및 거래지시의 내용 등을 확인하여야 하며 접근매체를 양도·양수하거나 대가를 수수(授受)·요구 또는 약속하면서 접근매체를 대여받거나 대여하는 행위 또는 보관·전달·유통하는 행위 등을 할 수 없고(제6조), 접근매체의 위조나 변조로 발생한 사고 등에 대하여는 이용자에게 손해가 발생한 경우 그 손해를 배상하여야 한다(제9조).

한편, 전자거래의 안전성을 확보하기 위하여 금융회사 등은 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치, 소요경비 등의 정보기술부문, 전자금융업무 및 「전자서명법」에 의한 인증서의 사용 등 인증방법에 관하여 금융위원회가 정하는 기준을 준수하여야 한다(제21조). 여기서 “금융위원회가 정하는 기준”으로 「전자금융감독규정」이 제정되어 있다. 즉, 이 규정은 「전자금융거래법」및 동법 시행령에서 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정함을 목적으로 한다(제1조). 이 규정은 전자금융거래의 안전성확보 및 이용자보호에 관하여 인력, 조직 및 예산부문, 시설부

문, 정보기술부문, 정보기술부문 내부통제에 있어서 금융기관 또는 전자금융업자가 준수하여야 하는 의무 등을 정하고 있다.

Ⅳ. 전자서명법

1. 입법취지 및 체계

「전자서명법」은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 1999년에 제정되었다.

"전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보로서(제2조제1호), 전자문서에 서명자가 전자문서에 서명을 하는 되는 경우 그 인증과 효력에 관한 규율로서 공인인증기관과 공인인증서, 인증업무의 안정성 및 신뢰성을 위한 다양한 사항을 정한다.

< 전자서명법의 체계 >

제1장 총칙
제2장 공인인증기관
제3장 공인인증서
제4장 인증업무의 안전성 및 신뢰성 확보
제5장 전자서명인증정책의 추진 등
제6장 보칙
제7장 벌칙

2. 개인정보 관련 규정

「전자서명법」은 "**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 말한다고 규정한다(제2조 제13호).

이 규정은 "생체특성에 관한 정보"라 하여「정보통신망법」상의 바이오정보와 유사한 의미를 가지는 생체정보를 명문화하고 있다. 다만, 바이오정보와 같이 지문, 홍채 등 각 식별자의 열거를 통하여 적극적인 방식으로 정의하기 보다는 식별성에 초점을 두어 "당해 개인을 알아볼 수 있는(식별할 수 있는) 생체특성에 관한 정보"로 표현하고 있다.

< 개인정보 개념의 비교 >

정보통신망법	전자서명법
"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.	"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.

이 법은 "전자서명"을 서명자의 서명 또는 서명날인이라는 행동적 특성에 기반하여 "서명자를 확인하고 서명자가 당해 전자문서에 서명

을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보"로 이해한다. 61)

이러한 전자서명을 생명하기 위한 전자적 정보(전자서명생성정보)가 **가입자에게 유일하게 속한다는 사실**을 확인하고 증명하는 "인증"과 관련된 사항을 주된 내용으로 한다. 따라서 이러한 인증을 담당하는 공인인증기관(제2장)과 공인인증서(제3장) 및 인증업무(제4장)가 이 법에서는 매우 중요하다.

3. 개인정보의 보호

「전자서명법」에서는 공인인증기관이 본인임을 확인하고 발급하는 "공인인증서"가 중요한 규율대상이기에, 이 분야에서는 공인인증서를 발급하는 단계에서의 개인정보보호와, 본인을 확인(인증)하는 단계에서의 개인정보보호가 동시에 문제가 된다.

공인인증서를 발급하는 경우 거기에는 ① 가입자의 이름(법인의 경우에는 명칭을 말한다), ② 가입자의 전자서명검증정보, ③ 가입자와 공인인증기관이 이용하는 전자서명 방식, ④ 공인인증서의 일련번호, ⑤ 공인인증서의 유효기간, ⑥ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보, ⑦ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항, ⑧ 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항, ⑨ 공인인증서임을 나타내는 표시가 포함되어야 한다(제15조).

한편, 공인인증기관은 인증업무에 관한 시설의 안전성 확보를 위하여 미래창조과학부령이 정하는 보호조치를 취하여야 하는데(제18조의3), 여기서 인증업무에 관한 시설의 안정성 확보를 위하여 하여야 하

61) "전자서명"과 "디지털서명"은 일반적으로 같은 것으로 이해되지만, 디지털서명은 공개키 암호방식(비대칭적 암호체계)을 이용한 전자서명의 한 종류라 할 수 있다. http://terms.naver.com/entry.nhn?docId=1222567&cid=40942&categoryId=31819 (2016.10.24. 최종접속)

는 보호조치는 ① 전자적 침해행위로부터 보호조치, ② 외부인의 출입통제 등 방호조치, ③ 화재·수해 등 재해에 대비한 조치, ④ 그밖에 인증업무에 관한 시설의 안전성 확보를 위한 관리적 조치이다(같은 법 시행령 제13조의4). 이러한 기술적 조치 이외에 이 법은 전자서명생성정보의 보호와 개인정보의 보호에 관하여 개별 규정을 두고 있다.

< 「전자서명법」 상의 개인정보의 보호 >

전자서명생성정보의 보호(제23조)	개인정보의 보호(제24조)
① 누구든지 타인의 전자서명생성정보를 도용 또는 누설하여서는 아니된다. ② 누구든지 타인의 명의로 공인인증서를 발급받거나 발급받을 수 있도록 하여서는 아니된다. ③ 누구든지 공인인증서가 아닌 인증서 등을 공인인증서로 혼동하게 하거나 혼동할 우려가 있는 유사한 표시를 사용하거나 허위로 공인인증서의 사용을 표시하여서는 아니된다. ④ 누구든지 공인인증서를 이용범위 또는 용도에서 벗어나 부정하게 사용하여서는 아니된다. ⑤ 누구든지 행사하게 할 목적으로 다른 사람에게 공인인증서를 양도 또는 대여하거나 행사할 목적으로 다른 사람의 공인인증서를 양도 또는 대여 받아서는 아니된다.	① 공인인증기관은 인증업무 수행과 관련하여 개인정보를 보호하여야 한다. ② 삭제

Ⅴ. 의료 관계법

의료 분야는 환자를 진료하는 과정에서 필연적으로 생체정보 내지 개인정보를 다루게 되어 있다는 점에서 관계 법률로서 살펴보는 것이 필요하다. 다만, 의료분야에서는 생체정보를 개인을 식별하기 위한 인식정보로서 보는 경우와 진료 및 치료목적의 정보로서 보는 경우가 혼재되어 있을 수 있어 과연 진료정보를 생체인식정보와 명백하게 구별하는 것이 가능하고 필요한지에 관하여는 논란의 여지가 있다.

아래에서는 의료분야에서 개인정보에 관하여 규정을 두고 있는 대표적인 법률로서 「생명윤리 및 안전에 관한 법률」(생명윤리법), 「보건의료기본법」, 「의료법」에 관하여 관련 규정을 살펴보기로 한다.

1. 생명윤리 및 안전에 관한 법률

최근 암, 치매 등의 유전적 질환이나 난치병 또는 불치병의 예방 및 치료 등을 위하여 유전자 분석이 활발하게 이용되고 있으며, 제대혈(탯줄혈액), 세포·줄기세포, 난자 등은 체세포복제, 체세포핵이식, 단성생식 등의 연구에 없어서는 안 될 중요한 연구검체로 인정되고 있다. 이러한 검체는 그 자체로서 개인의 중요한 정보에 속하기 때문에 이를 무제한으로 허용하는 경우 인권적으로 윤리적으로 매우 심각한 병폐를 낳을 수 있기 때문에 법적으로 그 허용범위를 명확히 정할 필요가 있다. 이러한 취지에서 「생명윤리법」은 인간과 인체유래물 등을 연구하거나, 배아나 유전자 등을 취급할 때 인간의 존엄과 가치를 침해하거나 인체에 위해(危害)를 끼치는 것을 방지함으로써 생명윤리 및 안전을 확보하고 국민의 건강과 삶의 질 향상에 이바지하는 것을 그 목적으로 한다(제1조).

이 법은 사람을 대상으로 물리적으로 개입하거나 의사소통, 대인 접촉 등의 상호작용을 통하여 수행하는 연구 또는 **개인을 식별할 수 있**

는 정보를 이용하는 연구로서 대통령령으로 정하는 연구(인간대상연구)를 규율하는 법으로서, 그 대상은 "인체유래물" 즉, 인체로부터 수집하거나 채취한 조직・세포・혈액・체액 등 인체 구성물 또는 이들로부터 분리된 혈청, 혈장, 염색체, DNA, RNA, 단백질 등이다.

이 법에서 다루는 정보로는 유전정보(제14호), 개인식별정보(제17호), 개인정보(제18호) 등이 있다(제2조).

< 생명윤리법상의 "정보" >

유전정보	개인식별정보	개인정보
인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보	연구대상자와 배아・난자・정자 또는 인체유래물의 기증자("연구대상자 등")의 성명・주민등록번호 등 개인을 식별할 수 있는 정보	개인식별정보, 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보

이 법은 인간대상연구자 또는 유전자검사기관은 대상자의 개인정보 또는 검사대상물을 수집・채취하는 경우 반드시 "서면동의"를 받아야 하는 것이 원칙임을 규정하고 있다(제16조, 제42조, 51조). 또한 이 경우 제3자에게 제공하거나 처리하기 위하여는 반드시 "익명화"하여야 한다고 규정하고 있다(제18조, 제44조). 다만, 연구대상자가 개인식별정보를 포함하는 것에 동의한 경우에는 그러하지 아니하다(제18조, 제38조, 제43조)고 하여 예외를 두고 있다.

이 법에서 규정하고 있는 유전정보, 개인식별정보, 개인정보 등은 치료목적 내지 연구목적에 한정된 범위 내에서 수집하고 활용하도록 허용하고 있다는 점에 의미가 있다.

2. 보건의료기본법

「보건의료기본법」은 보건의료에 관한 국민의 권리·의무와 국가 및 지방자치단체의 책임을 정하고 보건의료의 수요와 공급에 관한 기본적인 사항을 규정함으로써 보건의료의 발전과 국민의 보건 및 복지의 증진에 이바지하는 것을 목적으로 한다(제1조).

이 법은 "보건의료정보"를 "보건의료와 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료"로 정의하고 있다(제3조제6호). 대상 정보가 보건의료라는 특정한 분야라는 것을 제외하고는 "개인정보"의 개념과 유사하다.[62]

이러한 보건의료정보에 대해서 이 법은 보건복지부장관으로 하여금 보건의료기관, 관련 기관·단체 등이 보유하고 있는 보건의료정보를 널리 보급·확대하기 위하여 필요한 시책을 강구하여야 하며(제56조), 보건의료정보의 효율적 운영과 호환성 확보 등을 위하여 보건의료정보의 표준화를 위한 시책을 강구하여야 한다(제57조)는 규정을 두고 있을 뿐이며, 보건의료정보의 성격이나 개인정보와의 관계 및 그러한 정보의 보호를 위한 조치 등에 관하여는 명시적인 언급이 없다.

3. 의료법

「의료법」은 모든 국민이 수준 높은 의료 혜택을 받을 수 있도록 국민의료에 필요한 사항을 규정함으로써 국민의 건강을 보호하고 증진하는 것을 목적으로 한다(제1조).

「의료법」의 경우 다른 법률들과는 달리 정의규정을 따로 두고 있지 아니하며, 특히 개인정보와 관련하여서도 처방전(제18조), 전자의무기

62) 이한주, "개인의료정보보호법 제정의 필요성과 입법방향", 「한국의료법학회지」, 제22권제1호, 2014. 6, 180면.

록(제23조) 등의 개별 규정에서 정보의 범위를 따로 언급하고 있으며, 이러한 정보의 누설을 금지하는 일반규정을 두고 있다(제19조).

> 제18조(처방전 작성과 교부) ① ~ ② 생략
> **③ 누구든지 정당한 사유 없이 전자처방전에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.**
>
> 제19조(정보 누설 금지) ① 의료인이나 의료기관 종사자는 이 법이나 다른 법령에 특별히 규정된 경우 외에는 의료·조산 또는 간호업무나 제17조에 따른 진단서·검안서·증명서 작성·교부 업무, 제18조에 따른 처방전 작성·교부 업무, 제21조에 따른 진료기록 열람·사본 교부 업무, 제22조제2항에 따른 진료기록부등 보존 업무 및 제23조에 따른 **전자의무기록 작성·보관·관리 업무를 하면서 알게 된 다른 사람의 정보를 누설하거나 발표하지 못한다.**
>
> 제23조(전자의무기록) ① 의료인이나 의료기관 개설자는 제22조의 규정에도 불구하고 진료기록부등을 「전자서명법」에 따른 전자서명이 기재된 전자문서(이하 "전자의무기록"이라 한다)로 작성·보관할 수 있다.
> ② 생략
> **③ 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.**

한편, 생체정보와 관련하여서는 「의료법」상 "원격의료"를 언급하지 않을 수가 없는데, 원격의료를 위하여는 생체정보의 수집과 활용이 반드시 전제되어야 하기 때문이다. 앞에서 언급한 바와 같이 어느 개인을 특정하여 식별하기 위한 목적으로서의 생체정보인지 아니면 치료 내지 연구를 위한 건강정보로서의 생체정보인지에 따라 평가가 달라질 수 있는데, 「의료법」은 아직 그러한 구분을 하고 있지 않다. 다만, 이 법은 "의료인(의료업에 종사하는 의사·치과의사·한의사만 해당한다)은 … 컴퓨터·화상통신 등 정보통신기술을 활용하여 먼 곳에 있는 의료인에게 의료지식이나 기술을 지원하는 원격의료를 할 수 있다"고 규정하고 있는데(제34조), 앞으로 원격의료가 본격적으로 도입

이 되어 활성화되는 경우 정보통신기술을 활용하여 어떠한 생체정보를, 어떤 목적으로, 어떻게 수집하고 처리할 것인가, 어느 한계까지 보호할 것인가 등에 대한 세부적인 내용이 정해질 필요가 있다.

Ⅵ. 주민등록법 / 여권법

1. 주민등록법

「주민등록법」은 시(특별시·광역시는 제외하고, 특별자치도는 포함한다. 이하 같다)·군 또는 구(자치구를 말한다. 이하 같다)의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것을 목적으로 한다(제1조). 주민등록법령은 우리나라에서 생체정보 식별자 중 가장 대표적이라 할 수 있는 "지문"을 본인식별을 위해 사용한 최초의 규범으로서 의미가 있다.

이 법에 의하면, 시장·군수 또는 구청장은 주민에게 개인별로 고유한 등록번호, 즉 "주민등록번호"를 부여하여야 하며(제7조), 관할 구역에 주민등록이 된 자 중 17세 이상인 자에 대하여 주민등록증을 발급한다(제24조제1항). 이러한 주민등록증에선 성명, 사진, 주민등록번호, 주소, 지문(指紋), 발행일, 주민등록기관을 수록한다(제24조제2항). 이렇게 생체정보의 하나인 "지문"이 "법률" 속에 포함이 된 것은 1997년 12월 17일 개정에 의한 것이며 그 전까지는 주민등록증의 발급절차와 관련하여 "시행령"에 규정되던 것이었다.

< 주민등록법 시행령 상의 지문 규정 >

1975년 8월 26일 시행령	현행 시행령
제33조(주민등록증 발급절차) ② 제1항의 주민등록증 발급통지를 받은	제36조(주민등록증의 발급절차) ③ 제1항 및 제2항에 따라 주민등록증

1975년 8월 26일 시행령	현행 시행령
자는 통지서를 받은 날로부터 15일 이내에 그 자신이 발급업무 담당공무원에게 사진(6월내에 촬영한 가로 2.5센치, 세로 3센치의 탈모상반신 정면사진) 3매를 제출하고, 본인임을 소명한 후 그 공무원 앞에서 **별지 제33호서식에 의한 주민등록증 발급신청서와 주민등록용지에 지문을 찍어야 한다.**	발급통지를 받은 사람 또는 공고된 사람은 그 통지서 또는 공고문에 적힌 발급신청기간 내에 본인이 직접 주민등록이 되어 있는 시·군·자치구(이하 "주민등록지의 시·군·구"라 한다)의 관계 공무원에게 사진(6개월 이내에 촬영한 가로 3센티미터, 세로 4센티미터 또는 가로 3.5센티미터, 세로 4.5센티미터의 귀와 눈썹이 보이는 탈모상반신 사진을 말한다. 이하 같다) 1장을 제출하고 본인임을 밝힌 후, 그 공무원 앞에서 **별지 제30호서식에 따른 주민등록증 발급신청서에 지문을 찍어 신청하여야 한다.** 이하 생략

이 법은 "지문"이라는 개인정보의 보호에 관하여 다른 법령에서와 같이 적극적인 정보보호조치를 정하는 규정을 두지 않고, 주민등록표 보유기관 등의 주의의무와 같이 추상적이고 간접적인 방식으로 규정하고 있다. 즉, "주민등록표 보유기관의 장"은 주민등록표를 관리할 때에 주민등록표가 멸실, 도난, 유출 또는 손상되지 아니하도록 필요한 안전조치를 하여야 하고, "주민등록표의 관리자"는 이 법의 규정에 따른 보유 또는 이용목적 외의 목적을 위하여 주민등록표를 이용한 전산처리를 하여서는 안되고, "주민등록업무에 종사하거나 종사하였던 자 또는 그 밖의 자로서 직무상 주민등록사항을 알게 된 자"는 다른 사람에게 이를 누설하여서는 안된다(제31조). 정보보호조치에 관한 세부적이고 구체적인 규율의 보완이 필요하다.[63]

63) 아울러, 주민등록표 상의 지문날인제도는 앞에서 언급한 바와 같이 정보주체에게 선택의 자유없이 강제로 날인하게 하고, 그 이용에 관한 법적 근거없이 이를 범죄

2. 여권법

여권은 외국을 여행하는 국민에게 정부가 발급하는 증명서류로서, 여행자의 국적・신분을 증명하고, 해외여행을 허가하며, 외국 관헌의 보호를 부탁하는 문서로서,[64] 그 발급과 효력 등에 관하여는「여권법」에 의한다(제1조).

「여권법」에 의하여 여권에 수록되는 정보는 ① 여권의 종류, 발행국, 여권번호, 발급일, 기간만료일과 발급관청, ② 여권의 명의인(名義人)의 성명, 국적, 성별, 생년월일, 주민등록번호와 **사진**이다(제7조). 또한 외교부장관은 여권에 수록하는 정보를 포함하여, 여권을 발급받는 사람의 **지문(指紋),** 주소, 연락처, 국내 긴급연락처, 여권발급기록 등 외교부령으로 정하는 바에 따라 여권업무의 수행에 필요한 정보를 수집・보관하고 관리할 수 있다. 다만, **지문은 여권발급 과정에서 본인 여부를 확인하기 위한 목적 외에는 수집・보관・관리할 수 없으며 그 보관 및 관리 기간은 3개월 이내로 한다**(제8조).「여권법」에 지문과 같은 구체적인 생체정보가 포함된 것은 2008년 개정을 통해서이다. 1970년대에 도입된 주민등록법이나 2007년의 전자금융거래법에 비하면 약간 늦은 편이다.

한편, 여권을 발급받으려는 사람은 제8조의 정보를 제공하면서 외교부장관에게 여권의 발급을 신청하여야 하는데, 다만, 지문을 채취할 수 없는 부득이한 사정이 있는 등 대통령령으로 정하는 경우에는 지문을 제공하지 아니할 수 있다(제9조).

수사에까지 이용하는 것은 개인정보수집의 일반원칙에 위배되고, 모든 국민을 예비적 범죄자로 취급하는 것이어서 무죄추정의 원칙과 영장주의 원칙을 위반한 입법이라는 점 등에서 조속한 개정을 요구하는 견해가 있다. 김일환, 앞의 "주민등록법상 지문정보의 목적 외 이용에 대한 헌법적 고찰", 107면; 이상명, 앞의 논문, 349면.

64) 네이버 두산백과, 여권(passport, 旅券)의 정의.
http://terms.naver.com/entry.nhn?docId=1125980&cid=40942&categoryId=31659 (2016.10.3. 최종접속)

Ⅶ. 디엔에이신원확인정보의 이용 및 보호에 관한 법률

「디엔에이법」이라 불리는 이 법은 개인의 신원을 확인하는 데에 필요한 정보 중 특히 디엔에이(DNA)신원확인정보의 수집·이용 및 보호에 필요한 사항을 정함으로써 범죄수사 및 범죄예방에 이바지하고 국민의 권익을 보호함을 목적으로 한다(제1조).

DNA는 생물의 생명현상에 대한 정보가 포함된 화학물질인 디옥시리보 핵산(Deoxyribonucleic acid, DNA)을 말한다(제2조제1호). 사람을 식별하는 매우 유용하고도 중요한 생체정보이긴 하지만, 오히려 그 결정적 성격으로 인하여 위조, 누출될 경우 심각한 피해를 입기 때문에 수집, 관리 및 활용에는 매우 신중을 기하여야 하며, 보안이 특별히 강화되어야 한다. 그리하여 이 법은 디엔에이신원확인정보를 관리하며 이를 이용함에 있어 인간의 존엄성 및 개인의 사생활이 침해되지 아니하도록 필요한 시책을 마련하여야 한다고 규정하고 있으며, 데이터베이스에 수록되는 디엔에이신원확인정보에는 개인 식별을 위하여 필요한 사항 외의 정보 또는 인적사항이 포함되어서는 아니 된다는 원칙을 국가의 책무로서 정하고 있다(제3조).

이 법은 디엔에이를 채취하고 데이터베이스화하며 “목적 외 사용을 제한”하는, 개별 생체정보 식별자에 대한 하나의 분야를 전체적으로 규율하는 법률이라는 점에 의미가 있다.

제 3 절 소 결

생체정보는 그 활용 현황의 파급효과에 비추어 규범적 보호장치가 마련되어 있어야 함에도 불구하고 아직은 우리 법제에서 독자적인 규율의 영역으로 자리잡고 있지 못하며, 개인정보의 하나 정도로 인정

되고 있는 것으로 보인다. 비록 생체정보라는 고유한 용어가 사용된 것은 아니지만, 대표적인 생체정보인 지문의 사용에 관하여 1970년대부터 「주민등록법」이 존재하여 왔고, 전 국민이 13자리의 일련번호인 주민등록번호를 사용하여 왔던 현실을 돌이켜보면, 굳이 생체정보라는 별도의 정보의 유형을 또 정하는 것이 필요한가에 대한 의문이 발생할 수 있다. 하지만 주민번호의 유출이나 보안 실패 등으로 인한 정신적·재산적인 피해가 속출하는 데에 대한 경계는 보다 안전하고 확실한 본인확인정보를 필요로 하게 된 것이다. 이러한 유일성을 가진 정보의 추구는 앞으로 계속될 것으로 보이기에 더 이상은 기존 법령의 틀 속에서 해석 등을 통하여 판단할 것이 아니라 새로운 영역으로 설계하여 규율할 필요성이 있는 것이다.

현행 법제에서는 전자금융과 관계된 「정보통신망법」과 「전자금융거래법」에는 “바이오정보” 또는 “생체특성”로 개념적으로는 포섭이 되어 있다. 그 의미적으로는 개인식별에 초점이 맞춰져 있는 생체인식정보로 파악하고 있는 것으로 보여 정의나 유형(범위)를 새로 정해야 하는 큰 입법적 부담은 없는 것으로 보인다. 그러나 일반법이 아닌 각 개별 분야에서 개인식별의 필요성에 따라 개인정보 중의 하나로서 구성되어 있다 보니, 기존의 개인정보와 동일한지 아니면 차이가 있는지에 대한 구별이 확실하지 않다. 또한 성격적으로 민감하기에 「개인정보보호법」상의 “민감정보”로 볼 수 있겠으나 규정 자체만으로 보면 그것도 어려운 상황이다.

이러한 문제는 결국 생체정보가 가지는 유일한(unique) 성격 상 일반 개인정보의 보호보다 좀 더 강한 보호조치가 필요하다는 점으로 귀결된다고 할 것이다.

그리하여 규범적인 측면에 있어서는 생체정보의 개념을 어떻게 정의할 것이며, 법적인 지위는 어떻게 설정하고, 다른 유형의 개인정보

와의 구별은 어떻게 볼 것이며, 보호조치는 어느 정도로 설정할 것인가가 가장 중요한데, 아직 우리 현행법제에서는 이러한 통일적 또는 다각적인 관점에서 생체정보를 취급하고 있지 않아 이에 대한 체계적인 정비가 시급하다.

제 4 장 생체정보 관련 해외 입법례

제 1 절 서 설

지문과 같은 생체정보는 일찍이 미국이나 캐나다 등과 같이 본인확인제도가 발달하지 않은 국가에서 사회보장의 부정수급을 방지하기 위한 수단으로 활용되어 왔던 것이다.[65] 특히, 9.11테러로 인하여 여권 등 각종 본인확인을 위한 문서에 생체정보를 포함시킴으로써 출입국이나 범죄수사와 같은 공공분야로부터 다양한 인식 및 인증의 기반으로 마련되었다고 할 수 있다. 최근에는 지문·홍채·얼굴인식 등 바이오인식 기술과 공개키 암호화 기술을 융합해 비밀번호의 입력이 없이 지문인식 한번만으로 결제가 가능한 온라인 간편인증(FIDO, Fast IDentity Online) 기술이 본격적으로 개발되고,[66] 2012년 FIDO 얼라이언스[67]가 설립되어 생체인식기술을 활용한 인증방식에 대한 기술이 표준화되면서 이러한 새로운 인식 및 인증에 관한 각 국의 제도적 규율도 본격적으로 이루어지고 있다. 다만, 아직 어떠한 국가에서도 여전히 생체정보에 대한 "규범"이 독자적으로 구축된 것 같지는 않고, 기존의 개인정보 내지 민감정보와 관련하여 그 전체적인 틀 속에서 이해되고 보호되는 것으로 보인다.

생체정보의 활용에 있어서는 전 세계에 걸쳐 과학기술의 특성상 보편적이고 일반적인 성격을 가지지만, 각 국가마다 처한 기술적 상황 및 규율의 필요성에 차이가 있기 때문에 외국의 법제도를 단순하게 비교 평가하는 것은 문제가 있다.

---

65) 이창범, 앞의 글, 113면.

66) 한국인터넷진흥원 보도자료, "KISA, 바이오인식 기술 연계한 공인인증 활용 기술 개발 추진", 2015. 5. 21, 1면.

67) FIDO Alliance는 온라인 환경에서 편리하고 안전한 인증시스템을 공동으로 구축하고 인증시스템에 대한 기술표준을 제시하기 위하여 2012년 설립된 '모바일 결제 표준 국제협회'를 말한다. 윤재호·홍진실, 앞의 보고서, 12면.

따라서 이하에서는 생체정보의 활용현황에 비추어 생체정보의 개념과 범위 등이 명확하지 않은 우리 법제의 현실을 환기하고 개선방안을 논의하기 위한 방법으로서 외국의 법제가 어떻게 구축되어 있는지 소개하는 데에 주안점을 두며, 앞으로 보다 심도있는 연구가 진행될 수 있기 위한 선행 자료를 제공하는 데에 의미를 두고자 한다.

제 2 절 EU 및 OECD

Ⅰ. EU

1. 지침(Directive)에서 규정(Regulation)으로

유럽연합은 일찍이 1995년에 개인정보의 처리에 있어 정보주체를 보호하고 EU 회원국 간 개인정보의 자유로운 이동을 보장하기 위하여 「EU 개인정보보호지침」[68]을 정한 바 있다. 이 지침에서 말하는 개인정보(personal data)는 신원이 확인되었거나 확인할 수 있는 자연인에 관한 정보로서, 특히 신원을 확인할 수 있는 자는 직·간접적으로 특정 식별번호 또는 그의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 동일성에 관하여 하나 또는 그 이상의 식별요소에 기하여 확인될 수 있는 자“를 말한다(제2조). 이 지침의 개인정보의 정의 속에는 신체적, 생리적 식별요소라는 생체정보의 징표가 포함되어 있어 생체정보는 곧 개인정보로서 자연스럽게 해석될 수 있다.

그런데 이 지침은 2016년 “지침”(Directive)이 아닌 “규정”(Regulation)의 형식인 General Data Protection Regulation(이하 GDPR), 즉 개인정보

68) 「개인정보의 처리와 자유로운 이동 시의 개인의 보호에 관한 1995년 10월 24일 유럽의회 및 유럽이사회지침」(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).

보호일반규정[69] 내지 통합개인정보보호규정[70]으로 대체되었다.[71]

GDPR은 지금까지 유지되어 왔던 개인정보보호에 대한 일반원칙, 즉, "허가유보부의 일반적 금지", "정보최소화의 원칙(Datenvermeidung und Datensparsamkeit)", "합목적성" 및 "투명성" 등과 같은 원칙들은 그대로 유지하고 발전시켜 나가는 것을 기초로 하고 있다. 이 규정은 외국에 대한 정보제공과 관련하여 개별 당사자의 권리에 중대한 영향을 끼치므로 더 세분화된 규칙을 마련하였다.[72] 즉, 제3국 또는 국제기구에의 개인정보 제공이 GDPR에서 정하는 요건을 충족할 경우에만 가능하도록 한 것이다(제44조 이하). 먼저, 유럽집행위원회가 적절한 보호수준이 존재한다고 결정하는 경우(제45조)에만 정보제공이 가능하며, 집행위원회의 결정이 없을 때에는 권리보호에 대한 적절한 보장이 준비되어 있고 당사자가 유효한 법적 구제수단을 행사할 수 있을 경우(제46조)에만 정보제공이 가능하다. 또한 예외적으로 당사자가 정보교부의 리스크를 충분히 인지한 상태에서 행한 명시적 동의가 있을 때(제49조)에도 정보제공이 가능하다.

한편, GDPR에서 새로이 규율하고 있는 내용도 있다. 먼저, GDPR 제3조제2항은 유럽연합 내에 근거를 두고 있는 기업 외에도, 그 상품이 유럽연합 내의 특정 국내 시장을 목표로 하거나 개인정보의 처리가 유럽연합 내에 있는 사람의 행동에 관한 것일 경우에는 유럽연합

69) 보안뉴스, "EU 개인정보보호 일반규정(GDPR)과 정보주체의 권리", 2016. 6. 18. http://www.boannews.com/media/view.asp?idx=50952&kind=6 (2016.10.13. 최종접속)

70) 보안뉴스, "유럽은 지금 통합개인정보보호법규(GDPR)로의 이행기", 2016. 7. 10. http://www.boannews.com/media/view.asp?idx=51126&kind=6 (2016.10.13. 최종접속)

71) 지침(Richtlinie)이 각 회원국에 대하여 지침의 내용에 상응하는 구체적인 입법(이행법률)의 의무를 부여하는 데 반하여, 규정(Verordnung)은 "유럽연합의 기능에 관한 조약(Vertrag über die Arbeitsweise der Europäischen Union: AEUV)" 제288조제2항에 따라 일반적 효력을 가지고 각 회원국에 직접 적용되므로, 개인정보보호일반규정은 유럽연합의 회원국 및 국민 전체에 대하여 직접적인 구속력을 가진다. Oppermann/Classen/Nettesheim, Europarecht 5. Auflage, C. H. Beck, München 2011, Rn. 71 ff. 참조. BFDI, Datenschutz-Grundverordnung, 2016. 5, S. 9.

72) *Ibid*.

밖에 있는 기업도 본 규칙의 규율 범위 안에 포함시킴으로써 그 적용 범위를 “유럽시장” 전체로 확대하고 있다. 또한, 유럽연합 내에서의 통일적인 법적용을 가능케 하기 위해, 공공부문 외에서 일어나는 국경을 넘어서는 정보 취급에 대해서 몇 가지 조치를 도입하고 있다. 원칙적으로 여러 회원국에서 영업 중인 기업의 경우 각 지역의 정보보호 감독청들 사이에서 합의와 협력을 통해 감독 업무를 진행하게 되며, 본사에 대해 감독청의 결정 내용을 송부하는 것이 보통이다(이른바 “One-Stop-Shop” 메커니즘).

< 지침과 규칙의 체계 비교 >

Directive 95/46 EC	GDPR 2016/679
CHAPTER I General provisions **CHAPTER II General rules on the lawfulness of the processing of personal data** Section 1 Principles relation to data quality Section 2 Criteria for making data processing legitimate Section 3 Special categories of processing Section 4 Information to be given to the data subject SSection 5 The data subject’s right of access to data Section 6 Exemptions and restrictions Section 7 The data subject’s right to object Section 8 Confidentiality and security of procession	**CHAPTER I General provisions** **CHAPTER II Principles** **CHAPTER III Rights of the data subject** Section 1 Transparency and modalities Section 2 Information and access to personal data Section 3 Rectification and erasure Section 4 Right to object and automated individual decision-making Section 5 Restrictions **CHAPTER IV Controller and processor** Section 1 General obligations Section 2 Security of personal data Section 3 Data protection impact assessment and prior consultation Section 4 Data protection officer Section 5 Codes of conduct and certification

Directive 95/46 EC	GDPR 2016/679
Section 9 Notification **CHAPTER III Judicial remedies, liability and sanctions** **CHAPTER V Code of conduct** **CHAPTER VI Supervisory authority and working party on the protection of individuals with regard to the processing of personal data** **CHAPTER VII Community implementing measures**	**CHAPTER V Transfers of personal data to third countries or international organisations** **CHAPTER VI Independent supervisory authorities** Section 1 Independent status Section 2 Competence, tasks and powers **CHAPTER VII Cooperation and consistency** Section 1 Cooperation Section 2 Consistency Section 3 European data protection board **CHAPTER VIII Remedies, liability and penalties** **CHAPTER IX Provisions relating to specific processing situations** **CHAPTER X Delegated acts and implementing acts** **CHAPTER XI Final provisions**

2. 개인정보의 개념

GDPR은 개인정보보호에 관한 기존의 지침을 포함하고 있고 지침의 내용에 관하여는 국내에 소개가 되어 있기 때문에 이하에서는 GDPR에서 생체정보와 관련하여 특별한 고려를 하고 있는 규정을 중심으로 소개하고자 한다. 먼저, GDPR은 보호대상인 개인정보의 범위를 세분화하고(다만, 제4조의 정의규정을 보면, 개인정보의 유형으로 되어 있지만, 개인정보의 하위개념이 아닌 병렬적인 개념으로 나열하고 있다) 특히 생체정보의 개념을 명문으로 두었다.

< GDPR에서의 각종 정보의 개념 >

개인정보 (personal data)	(1) “개인정보”란 식별된 또는 식별 가능한 개인(정보주체)과 관련된 일체의 정보를 말한다. 식별 가능한 개인이란 직접 또는 간접적으로, 특히 이름이나 식별번호, 위치 정보, 온라인 식별자, 또는 해당 개인의 신체나 생리, 유전자, 정신, 경제, 문화 또는 사회적 정체성에 국한된 하나 이상의 요인을 참조하여 식별될 수 있는 자이다.
유전정보 (genetic data)	(13) “유전정보”란 자연인의 생리 또는 건강에 관한 고유의(unique) 정보를 제공하고 특히 해당 자연인의 생물 검체 분석에서 생성되는 선천적이거나 후천적인 유전 특성에 관한 개인정보를 말한다.
생체정보 (biometric data)	(14) “생체정보”란 안면 영상이나 지문 정보와 같이 자연인 고유의(unique) 식별을 허용 또는 확인하는 해당 자연인의 신체, 생리, 행동 특성에 관한 특정 기술 처리로 발생하는 모든 개인 정보를 말한다.
건강관련정보 (data concerning health)	(15) “건강관련정보”란 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보를 말한다.

GDPR이 선언하고 있는 개인정보처리의 원칙은 다음과 같다.

(a) 정보주체와 관련하여 합법적으로, 공정하게 그리고 투명한 방식으로 처리되어야 한다(적법성, 공정성, 투명성의 원칙).

(b) 명시적이며 적법한 특정 목적을 위해 수집되고 해당 목적과 양립하지 않는 방식으로 추가적 처리되어서는 안된다. 공익적인 기록보존 목적 또는 과학 및 역사 연구 또는 통계 목적을 위한 추가적 개인정보처리는 제89조(1)항에 따라 최초의 목적과 양립되지 않는다고 간주되지 않는다(목적 제한의 원칙).

(c) 개인정보가 처리되는 목적과 관련하여 적절하고 타당하고 필요한 범위로 제한되어야 한다(데이터 최소화의 원칙).

(d) 정확하고, 필요 시, 최신의 정보여야 한다. 처리 목적과 관련하여 부정확한 개인정보는 지체 없이 삭제 또는 정정되도록 합리적인 일체의 조치가 취해져야 한다(정확성의 원칙).

3. 특별한 유형의 개인정보 처리

GDPR은 우리나라의 “민감정보”와 유사한 규정으로서 “특별한 유형(special categories)의 개인정보 처리”로서 “인종이나 민족, 정치적 견해, 종교 또는 철학적 신념 또는 노동조합에의 가입 여부 및 특정한 자연인을 식별할 목적으로 이루어지는 유전정보 및 생체정보, 건강정보 또는 성생활이나 성적 취향에 관한 정보의 처리는 금지된다”고 선언한다(제9조제1항).

그리고 이러한 금지원칙에 대하여 그 예외로서 제9조제2항을 통하여 열거하고 있는 10가지 경우에는 이러한 특수한 유형의 정보를 취급할 수 있도록 예외를 두고 있다.

< 특별한 유형의 정보가 처리 가능한 경우 >

a) 당사자가 하나 또는 복수의 목적을 위해 개인 정보를 취급하는 것에 명시적으로 동의한 경우, 단, 유럽연합법 또는 회원국 법률이 당사자의 동의를 통한 금지 해제를 배제하고 있지 않는 경우에 한한다.
b) 정보의 취급이 노동기본권, 사회안전법 및 사회보호법상의 권리를 행사하고 의무를 수행하는 데에 필요한 경우, 단, 유럽법, 회원국 국내법 및 회원국 국내법에 따른 협정을 통해 당사자의 기본권 보장이 적절하게 보장되는 경우에 한한다.
c) 생존을 위해 중요한 당사자 또는 제3자의 이익을 보호하기 위해 필요하며, 당사자가 신체적 또는 법률상 이유로 의사 표명을 할 수 없을 때
d) 정보의 취급이 당사자의 적법한 행동을 통한 정치, 사상 종교 단체 또는

노같은 조합 기타 단체의 설립, 구성 및 기타 조작 과정에서 나타난 경우로서, 오직 단체의 전현 구성원 또는 단체의 목적을 달성하기 위한 적법한 계약의 수행을 위한 행위한 사람과 관련한 정보인 경우, 단, 당사자의 의사표시 없이 개인 정보가 외부에 공개되어서는 안된다.

e) 당사자가 명시적으로 외부에 공개한 정보의 취급

f) 청구권의 주장, 행사 또는 방어를 위해 필요한 경우 혹은 법원에서의 행위와 관련하여 필요한 정보의 취급

g) 정보의 취급이 유럽연합규범 또는 회원국 국내법에 근거하여, 정보의 중요한 부분에 대한 비밀은 유지하면서 당사자의 기본권 내지 이익을 보장하기 위한 적절하고 특수한 조치를 위한 것이거나, 현저한 공공의 이익을 위한 이유에서 필요한 경우

h) 정보의 취급이 건강 보호 또는 직업안전보건의 목적, 피고용인의 근로 능력 평가를 위한 목적, 보건사회영역에서의 의료상의 진단, 치료 또는 간호를 위한 목적 또는 보건사회 영역에서의 시스템 운영 또는 역무 수행을 위한 목적에서 유럽연합 규범, 회원국법 또는 구성원의 계약에 근거하여 필요한 경우

i) 정보의 취급이 공공 보건 영역에서 국경을 넘을 수 있는 보건상의 위험방지와 같은 공공의 이익을 위한 목적에서 이루어지거나, 보건 관리 및 의료품의 품질 및 안전 기준 유지를 위한 목적에서 이루어지면서 유럽연합 규범 또는 회원국법에 근거를 두고 있으며, 당사자의 권리와 자유, 특히 직무상의 비밀을 유지하기 위한 적절하고 특별한 조치가 보장되는 경우

j) 정보의 취급이 유럽연합 규범 또는 회원국법을 근거로 하여 당사자의 기본권 및 이익을 보장하는 조치를 수반하면서, 공공의 이익상의 목적, 학문 및 역사적 연구의 목적 또는 통계적 목적을 위해 필요한 경우. 유럽연합 내에서 활동하는 어떠한 주체이든 생체정보를 포함한 제9조 제1항의 정보는 위의 요건이 있을 때에만 취급이 가능하다.

특히 제9조제4항은 개인정보 중에서 유전자, 생체 및 건강 정보에 대해서는 회원국으로 하여금 더 엄격한 제한 기준을 추가적으로 설정할 수 있음을 명시하고 있다.

정보처리의 제한에 관한 규정은 이러한 특정범주의 정보뿐 아니라, 범죄경력 및 범죄행위에 관한 개인정보(제10조), 신원확인을 요하지 않는 개인정보(제11조) 등도 포함된다.

Ⅱ. OECD

1980년 OECD의 「사생활보호 및 개인정보의 국경없는 흐름에 관한 가이드라인」[73]은 프라이버시 보호만이 아니라 자유로운 정보의 흐름을 차단하지 않을 것을 목적으로 그 적용대상을 공공·민간부문을 넘어서 특정 개인과 관련한 모든 정보로 규정하고 있다.[74] 이 가이드라인에서는 생체정보에 대한 언급이 없기 때문에 개인정보에 포함시켜서 이해하는 것으로 충분할 것이다.

회원국이 지켜야 하는 가이드라인은 개인정보보보호의 일반적인 원리라 할 수 있는 다음의 8가지 원칙으로 명확하다.

< 개인정보보호 8원칙 >

① 수집제한의 원칙(Collection Limitation Principle), ② 정확성의 원칙(Data Quality Principle), ③ 수집목적 명확화의 원칙(Purpose Specification Priciple), ④ 이용제한의 원칙(Use Limitation Principle), ⑤ 안전확보의 원칙(Security Safeguards Principle), ⑥ 공개의 원칙(Open Principle), ⑦ 개인참여의 원칙(Individual Participation Principle), ⑧ 책임의 원칙(Accountability Principle)

이 가이드라인은 사생활의 효율적인 보호와 개인정보의 자유로운 유통을 가장 균형적으로 유지할 수 있는 방법에 대한 국제적인 합의를 나타내고, 기술중립적이고 융통성을 가진 다양한 방법의 준수사항을 허용하고, 글로벌 네트워크를 포함한 모든 환경에 적용되며, 많은

73) Guidelines on the Protection of Privacy and Transborder Flows of Personal Information.
74) 조규범, 앞의 "생체정보 보호를 위한 입법론적 고찰", 187면.

국내 또는 자기규제적인 기구들에서 사용되고 있다는 특징이 있다.[75] 다만, 법적 구속력이 없기 때문에 참고로 할 수 있을 뿐이다.[76]

제 3 절 미 국

Ⅰ. 생체정보의 활용

미국은 사실 9.11 테러 이전부터 생체인증을 이용한 개인인식기술이 개발되어 채택을 검토하고 있는 가운데 9.11 테러가 발생하였던 것이고, 그 후 대통령의 제안으로 생체인증을 이용한 개인인식기술을 실제로 채택하게 되었다. 이에 맞춰 어플리케이션에 대한 연구개발과 국가과학기술위원회(National Science Technology Council, NSTC)를 중심으로 정부부처 간 생체인식에 대한 정책을 실시하고 있다. 우리나라와 마찬가지로 미국 또한 생체인식정보를 활용하여 얼굴인식은 물론이거니와 헬스 및 피트니스와 같은 웰빙산업, 소비자・금융・전자상거래, 기업보안, 출입국관리시스템과 생체인식형 여권, 운전면허증, 복지연금 수급, 범죄수사, 귀 인식 스마트폰 등 매우 다양한 분야에서 이를 활용하고 있다.[77]

1. 공공분야에서의 활용

2015년 10월 6일 유럽연합의 유럽사법재판소가 미국의 개인정보보호수준이 미흡하므로 유럽연합의 각 국은 유럽연합 개인정보보호지침(Directive 95/46 EC) 제25조에 따라서 유럽연합 거주자의 개인정보가 미국으로 이전되는 것을 막는 조치를 취할 수 있다는 취지의 결정이

75) 이한주, 앞의 글, 192-193면.
76) 박미정, 앞의 논문, 83-84면.
77) Thomson Reuters, Biometric Litigation : An evolving landscape, April/May 2016, Practical Law, 2016.

내려지면서 구글, 페이스북 등 유럽인을 상대로 사업을 벌여 온 미국의 기업들에게 큰 충격을 안겨 준 바 있다.[78] 그럼에도 불구하고 미국의 경우 개인정보보호제도가 EU만큼 엄격하지 않다는 전반적인 분위기는 생체인식정보에 대해서도 마찬가지여서 아직은 EU에서와 같은 체계적·조직적인 움직임이 없는 것으로 보인다.[79] 미국의 생체정보 관련 법제를 전체적으로 살펴보면 다음과 같다.

연방차원에서는 생체인식정보의 수집이나 전달에 대한 법령의 정비보다는 다양한 부처 내지 공공기관에서 생체정보를 활용하기 위한 다양한 "정책 프로그램"을 추진하는 것에 집중하는 것으로 보인다. 그리하여 이하에서는 다양한 프로그램을 소개하기로 하는데, 이들 프로그램은 부처 간 "공동활용"을 증진하기 위한 것이라는 점에 관심을 둘 필요가 있다.

(1) 연방상무부 국가표준기술원

국가표준기술원(National Institute of Standards and Technology, NIST)은 1960년대부터 연방수사국의 법집행과 과학수사기술을 지원하기 위한 지문정보기술에 대한 연구 등 지난 50년간 생체정보 분야에서 ① 지문 및 얼굴인식의 일치여부와 호환, ② 형사사법정보체계, ③다양한 복합형태의 생체정보에 대한 측정, ④ 평가 및 표준화에 대한 연구를 수행해왔다. 특히 안보필요성에 따라 양질의 생체정보 수집을 증대시키는 광범위한 정부차원의 노력을 지원하게 되었고, 이로써 수집된 자료가 다른 기관에 의해 적절히 공유되도록 하며, 생체인식시스템의 정확성과 상호활용성이 보장될 수 있도록 노력하고 있다.[80]

---

78) http://www.boannews.com/media/view.asp?idx=51126&kind=6 (2016.10.6. 최종접속)

79) 이상경, "미국의 생체정보 관련 법제 동향", 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 워크숍 자료집」, 한국법제연구원, 2016, 221면.

80) http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)

(2) 국방부

국방부(Department of Defense)의 국방과학수사 및 생체인식국(Department of Defense Defense Forensics and Biometrics Agency)은 국방부의 생체인식활동과 과학수사에 공조하고 강화하는데 기여한다.[81)]

(3) 국토안보부

국토안보부(Department of Homeland Security)는 생체정보와 관련하여 특히 다음의 5가지 프로그램을 진행하고 있다.

① 진정신분증명(REAL ID.)

REAL ID.는 테러를 막고, 사기를 감소시키며, 연방정부가 발행한 신분증명서류의 정확도와 신뢰성을 제고하기 위한 것이다. 2007년 3월 1일, 국토안보부는 진정신분증명법 제정을 위한 60일간의 의견청취계획을 공지하였다. 이 계획에는 진정신분증명에 즉응하는 운전면허나 ID카드에 요구되는 특성으로서의 생체인식정보를 포함하지 않고 있었으나, 장래 추가적인 보안의 요소로서, 그리고 재발급기간 동안 개인을 확인하기 위한 요소로서 각 주가 이를 요청할 수 있는 가능성에 대한 의견 제출을 유도하였다.[82)]

② 생체인식관리사무국(OBIM) 설립

생체인식관리사무국(Office of Biometric Identity Management, OBIM)은 2000년 연방의회의 권고로 미 국방부산하에 바이오매트릭스기술을 도입할 목적으로 설립되어 2003년 9월 「바이오매트릭스 프라이버시에 관한 국방부 가이던스」를 공표한 바 있다[83)]. OBIM는 2013년 3월에

81) http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)
82) http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)
83) 이는 "① 프라이버시권의 보호에 관한 지침, ② 바이오매트릭스 정보의 수집권한에 관한 지침, ③ 바이오매트릭스정보 보호를 위한 국방부의 책임"이라는 세 가지 항목에 관한 기준을 제시하는 것으로 구성되어 있다. 이상경, 앞의 글, 201면 참조.

the United States Visitor and Immigration Status Indicator Technology, 즉 '유에스 비짓'(US-VISIT)[84]을 시행하였다. 이는 전자여권에 사진(필수), 지문(선택) 등 생체정보를 수록한 집적회로칩(IC Chip)을 탑재하도록 하였는데, 이러한 전자여권의 도입은 신체의 고유한 정보를 이용하는 것으로 위·변조가 불가능하다는 특징이 있다. 다만, 미국 국가차원에서의 생체정보 수집 행위는 개인의 인권, 사생활의 자유를 침해하는 것이 아닌지에 대한 우려의 목소리가 있다.[85]

③ 등록여행자(Registered Traveler)

운속안전국(The Transportation Security Administration, TSA)은 항공안전의 강화와 세관(customer service)의 증대를 위한 목적으로 민간영역과 더불어 등록여행자 프로그램을 개발 중이며, 이는 운송안전국의 감시와 더불어 민간영역에서 제공되는 자율적인 시장 주도 프로그램으로서 역할을 하게 될 것이다.[86]

(4) **법무부**

법무부(Department of Justice)는 주로 범죄수사와 관련된 생체정보 인식체계를 가지고 있다. 특히 ① 미연방수사국(FBI)은 생체인식표준

84) 미국 출입국관리의 핵심인 US-VISIT 프로그램은 입국 외국인의 생체정보를 채취하여 watch list 및 범법자 정보 등과 비교를 수행한다. US-VISIT은 1996년 IIRIRA(불법이민개혁법)에서 요청된 자동화 출입국관리시스템으로부터 시작되었으며, 2004년 '정보개혁 및 테러방지법'에서 US-VISIT을 자동화된 생체출입국데이터시스템으로 정의하였다. 2004년 입국 외국인의 2지 (양손 검지) 지문과 사진 수집을 시작하였으며, 2007년부터 정확도 향상과 호환성 지원을 위해 10지 지문과 사진 수집 방식으로 변경되었다. 미국 입국 외국인의 철저한 신원확인을 위해 비자 신청자에 대한 생체정보 수집 및 검증과 입국 시 생체정보 신원확인 과정을 거치고 있으며, 국토안보부 산하 이민관련기관들에서는 수집된 생체정보를 이용하여 위조문서를 사용하거나 신원 도용한 방문자를 막고, 수천의 범죄자와 출입국 사범들의 입국금지 판정에 활용하고 있다. http://consulting.skcc.com/39 (2016.6.15. 최종접속).

85) http://cis.org/EnhancedBorderSecurityVisaReformAct2002-HR3525 및 http://www.cnsnews.com/news/article/state-department-puts-biometric-chips-us-passports (2016.10.10 최종접속)

86) 이상경, 앞의 글, 202면.

으로서 전자지문전송명세서(Electronic Fingerprint Transmission Specification, EFTS) Version 8.0을 사용하고 있으며, ② 형사사법정보서비스부서(Criminal Justice Information Services Division)에 의해 전국적으로 운용되는 지문 및 범죄기록 시스템으로서 통합자동지문인식체계인 IAFIS(The Integrated Automated Fingerprint Identification System)를 보유하고 있고, ③ 연방수사국의 생체인식과 신원확인 운용의 핵심조직인 생체인식특성화센터(The Biometric Center of Excellence, BCOE)를 운영하고 있다.[87]

(5) **국무부**

국무부(Department of State)의 가장 큰 업무 중 하나는 미국전자여권(US Electronic Passport) 을 관리하는 것이다. 즉 일반 여권과 동일하나 뒷면 커버에 작은 비접촉성의 통합서킷(컴퓨터칩)이 부가된 것이다. 이 칩은 여권의 사진부착면에 시각적으로 인식될 수 있는 사항과 동일한 데이터를 저장하고 있으며, 디지털 사진을 내장하고 있다. 디지털 사진의 내장은 국경에서 얼굴(안면)인식기술을 통하여 생체인식 비교를 가능하게 한다. U.S. “e-passport”는 또한 새로운 모습을 갖고 있고, 추가적으로 위조방지와 보안을 위한 특성을 체화한 것이다.[88]

2. 민간분야에서의 활용

(1) **얼굴인식**(Facial Recognition)

미국 비디오 게임 업체에서는 최근 얼굴인식 기술을 빈번하게 이용한다. 예컨대, 최근 출시된 농구 시뮬레이션게임에서는 사용자에게 3D 얼굴 스캔에 기반한 인간화된 아바타(personalized Avatar)을 만들어 그 아바타가 NBA 선수들과 경기를 하는 것이다. 다만, 이러한 비디오

87) http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)
88) http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)

게임에서 얼굴인식 기능에 대한 법적 문제점을 지적한 재판이 있기는 하였다.[89]

한편, 애틀랜타시의 Trump marina casino에서는 9200명 정도의 사기 도박 전과자의 얼굴을 인식하는 카메라와 데이터베이스를 연결하는 시스템을 설치하였다. 이 제품은 카지노에 출입하는 모든 사람의 얼굴을 카메라로 스캔하여 전과자의 데이터베이스와 일치하는지를 검색한다. 체중이 10파운드가 증가하거나 나이가 10년 정도 들거나 수염을 길러도 90% 이상의 인식을 할 수가 있다고 한다.[90]

(2) **헬스 및 피트니스 추적**(Tracking health and fitness information)

생체정보는 웰빙 산업에서도 활용되고 있는데, 실제로 헬스 및 피트니스 추적(Health and Fitness Tracking) 업계에서는 생체정보 기술에 많은 투자를 하고 있는 것으로 보인다. 예를 들어, Fitbit, Jawbone, Nike와 같은 스포츠회사는 시계나 스마트폰, 피트니스 팔찌 같은 착용가능한 도구에 결합한 생체측정방식 기능을 도입하고 있다. 이 방식은 심장박동 수, 혈액의 산소포화도를 직접 측정할 수 있도록 하면서 자가 측정 가능성을 확대하고 있다. 이러한 자가 운동량 계량화 및 생체 측정 방식에 관심을 반영하여 일부 기업들은 직원들이 생체 스크린 진단을 후원하는 보험까지 후원하고 있는 상황이다.

또한, 일부 보험회사들은 직원들이 보험회사에 이런 피트니스 추적 생체정보를 공유할 경우, 보험 할인혜택을 제공하고 있다. 보험회사는 보험계약자의 중요한 생체정보를 획득할 수 있지만, 반면에 프라이버시 개인정보 침해에 대한 문제를 야기한다는 점에 주의할 필요가 있다.[91]

---

89) First Am. Class Action Compl., Vigil V. Take-Two Interactive Software, Inc., No. 15-8211 (S.D.N.Y. Dec. 4, 2015).

90) Simons John, Greed meets terror, Fortune v. 144, no. 8, Oct. 29 2001, pp. 145-146.

91) Michael P. Daly, Kathryn E. Deal, Matthew J. Fedor, Meredith C. Slawe, Biometrics Litigation : An evolving landscape, Practical Law, April/May 2016, p.40. http://www.drinkerbiddle.com/-/media/files/insights/publications/2016/04/biometricsfeature.pdf (2016.10.10.

(3) **소비자전자상거래신원확인**(Consumer Authentication for transactions)

수많은 소비자를 상대로 하는 금융 분야에서는 생체정보 인식기술을 활용하여 금융거래에서의 신원확인 수단으로 활용한다. 예를 들어 수많은 기업들은 손바닥 지문 인식 시스템을 활용하여 상점에서 결제의 진위여부를 확인하며, 지문인식기 활용하여 현금입출금기(ATM)에서 돈을 인출한다. 또한 휴대폰 사용에도 생체인식 기술이 적용되고 있다. 기존의 휴대폰은 비밀번호 입력을 통해 본인확인을 했지만, 현재는 지문 정보를 활용한 보인확인 시스템 기술로 대체되고 있다.

한편, 최근 미국 신용카드 회사에서는 생체정보를 활용한 '셀피 페이(selfie pay)' 기술을 시험하고 있다. 2016년에 미국에서 출시된 이 기술은 현재 실험 중이지만 점차 세계적으로 확장되고 있는 추세이다. 이 기술은 소비자로 하여금 그들의 지문이나 얼굴의 사진을 신원확인 수단으로 사용하도록 한다. 즉, 물건을 온라인 구매 시 비밀번호나 코드가 없어도 생체정보를 활용하여 신분을 확인 후 구매가 가능하다. 하지만 이런 편리성에도 불구하고, 스마트폰에서 소비자의 생체정보를 활용한 기술은 개인정보 침해와 데이터의 안정성에 문제가 있다는 지적이 있다.[92]

(4) **기업 보안**(Enhancing Corporate Security)

최근 회사 고용주들은 생체정보 인식기술을(예를 들어, 데이터센터에서 망막(Retina) 또는 손스캐너를 활용하여 백그라운드 체크에 지문을 수집) 보안 목적으로 활용한다. 다만, 이런 민감한 생체정보를 보유하는 기업은 정보유출 시 매우 큰 소송의 위험이 있는데, 가장 대

최종접속)

92) http://www.chicagotribune.com/business/ct-mastercard-selfie-pay-0224-biz-20160223-story.html (2016.10.10. 최종접속) 및 http://www.drinkerbiddle.com/-/media/files/insights/publications/2016/04/biometricsfeature.pdf (2016.10.10. 최종접속)

표적인 예로 최근 2015년 5월에 일어난 미국 인사국(U.S. Office of Personnel Management)에서 발생한 미국 연방정부 공무원의 신원조회와 비밀 취급 정보가 노출되었다. 이로 인해 5개 주에서 미국 인사국을 대상으로 20개의 소송이 제기된 바 있다.[93]

(5) **귀 인식 스마트폰**(Ear recognition Smartphone)

미국 기업 아마존은 귀를 활용한 스캔(ear-scanning security) 기능을 활용하여 귀로 스마트폰 잠금을 해제하는 생체정보 인식기술이 2015년 미국 특허청으로부터 승인받았다. 인간 개인마다 귀가 지문처럼 다르고 유니크함(uniqueness)을 가졌다는 점에 착안한 기술이다. 전화가 오는 경우 사용자가 스마트폰에 귀를 대면 스마트폰에 내장되어 있는 카메라센서가 귀 모양(ear shapes)을 스캔하여 잠금을 해제하는 기술이다.[94]

Ⅱ. 생체정보 관련 규범

1. 생체정보의 개념

미국 국가과학기술위원회(NSTC)는 생체정보라는 개념을 두 가지, 즉 (일반적인 의미의) “생체정보(Biometric Data)”와 “생체인식정보(Biometrics)”의 개념으로 구분한다.[95] 그리하여 양자를 구별하여 보면, 우선, 일반적인 의미의 “생체정보”(Biometric Data)는 생체정보 처리과정에서 생성된 컴퓨터 데이터들에 대한 포괄적 개념(자동인식 과정에서 발생하는 샘플, 모형, 템플릿, 유사성 점수를 포함하나, 이름 등은 포함되지 않

93) U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., No. 15-1394, MDL No. 2664 (D.D.C.)(Jackson, J.).

94) http://www.forbes.com/sites/amitchowdhry/2015/06/17/amazon-patents-a-system-that-unlocks-your-smartphone-with-your-ear/#3c317587a0d0 (2016.10.6. 최종접속)

95) http://www.biometrics.gov/ (2016.10.6. 최종접속)

는다)인 것으로 본다. 이와 구별하여 “생체인식정보”(Biometric Data)는 다시 2원적으로 이해한다. 즉, 생체정보가 가진 특성(Characteristic) 또는 절차(Process)에서의 의미 두 가지 모두를 생체정보로 보고 있는 것이다.[96]

< 생체정보의 개념 >

o **특성으로서** : 자동인식을 위해 이용할 수 있는 측정 가능한 생체적(해부학적 및 생리학적) 특성과 행동적 특성 o **절차로서** : 측정 가능한 생체적(해부학적 및 생리적) 특성과 행동적 특성에 기반하여 개인을 인식하는 자동화된 방법

그리하여 미국 연방정부는 생체정보의 민감성과 중요성을 인식하여 생체인식정보(biometric data)를 개인식별정보(personally identifiable information)인 것으로 파악하며, 특정한 자연인에게 **“유일함(uniqueness)”**을 갖는 본인만의 개인정보이기 때문에 이는 매우 신중한 취급이 요구된다고 평가한다.[97]

다만, 생체정보에 관한 대부분의 논의는 개인의 정보보호 및 프라이버시와 관련한 문제로서 지적되고 있다. 이에 국토안보부의 생체정보 수집 및 사용에 관한 보고서(2012-02) 중 생체정보의 위험(Risks)과 장점(Benefits)을 평가하는 부분에서는 생체정보의 배포(공개)에 있어서는 생체정보의 장점이 위험성 보다 커야 한다는 기준 등을 포함하는 가이드라인을 제시하고 있다.[98]

---

96) http://www.biometrics.gov/ (2016.10.6. 최종접속)

97) 그리하여 미국 의회는 2006년 생체인식정보를 도용하는 것에 대해 형사처벌을 하도록 입법하였다(18 U.S.C. section 1028(a)(1)(8))(Carmen Aguado, supra note 1, at 194-195).

98) Department of Homeland Security, Report 2012-02 of the Data Privacy and Integrity Advisory Committee(DPIAC) on Privacy and the Department's Collection and Use of Biometrics Nov 7, 2012, p.7.

2. 연 방

연방차원에서 생체정보에 관하여 별도로 제정된 개별법률은 존재하지 않는다. 다만 앞에서 언급한 바와 같이 9.11테러 이후 국가안보 등을 이유로 한 출입국이나 보안과 관련된 법에서 신분확인을 위한 목적으로 규정을 두고 있으며, 금융에 있어서도 본인확인을 위한 개인정보의 하나로 보아 일반적인 개인정보보호의 구조와 체계 속에서 이해하고 있는 것으로 보인다. 미국 연방법 차원에서 개인정보보호법제와 생체정보보호법제를 구분하여 보면 다음과 같다.

< 미국의 개인정보보호법제와 생체정보보호법제 >

법제현황			특 징
개인정보보호법제	공공부문	- 연방프라이버시법 - 전자통신프라이버시법(Electronic Communications Privacy Act) - 컴퓨터연결 및 프라이버시보호법 - 운전자프라이버시보호법(Driver's Privacy Protection Act of 1994) 등	개인정보를 포괄적으로 보호하는 법률의 제정 없이 특정 유형의 정보조사 및 사용기관만을 규율, 독립된 위원회 등을 통한 보호가 아닌 개개인의 사법적 구제책에 의존
	민간부문	- 공정신용기록법(Fair Credit Reporting Act) - 소비자신용기록개혁법(Consumer Credit Reporting Reform Act) - 금융기록프라이버시법(Financial Records Privacy Act) - 전자자금이체법(Electronic Funds Transfer Act) - 공정신용청구법(Fair Credit Billing Act) - 공정채무수집법(Fair Debt Collection Act) - 공정신용기회법(Equal Credit Opportunities) 등	

법제현황			특 징
생체정보보호법제	공공부문	- 신원절도법(Identity Theft and Assumption Act of 1998) - 국경보안강화 및 비자개혁법(Enhanced Border Security and Visa Entry Reform Act, 2002) - 애국법(USA-PATRIOT ACT) - 항공안전법(The Aviation Security Act Of 2001) - 연방첩보감시법(The Federal Intelligence Surveillance Act) 등	9.11테러 이후 국가적인 안보를 강화하기 위한 목적으로 테러리스트 등 범죄자 감시의 강화
	민간부문	- 금융프라이버시법 - 공정채무수집법(Faif Debt Collection Practices Act) - 금융현대화법 등	금융산업 관련 법률이 중심, 생체인식정보의 수집과 전달에 대한 포괄적 규율 미흡

출처 : 김일환, “생체정보보호법제 정비방안에 관한 고찰”, 「토지공법연구」, 제33집, 2006. 11, 361-362면.

3. 주

미국에서 개인정보의 보호가 주로 민간영역에서 “자율규제”(self-regulation)의 방식으로 이루어지고 있는 점을 감안할 때,[99] 현재 생체정보에 관한 법령을 가진 주 중에서 생체인식정보를 가장 엄격하게 보호하는 법률을 가진 일리노이 주법과 그러한 법률을 모델로 하여 제정을 시도하고 있는 뉴저지 주의 경우는 눈여겨 볼만하다.

(1) 텍사스: 상법전

텍사스 주 「상법전」(Texas Business and Commercial Code) 제503장은 생체정보식별자(TEX. BUS. & COM. CODE ANN. 503.001) (2009년 개정)에 관하여 다음과 같이 규정하고 있다(제503.001조).[100]

99) 박정훈, 앞의 글, 415면.

100) Sec. 503.001 of Capture or Use of Biometric Identifier, Texas Business and Com-

(a) 생체정보식별자는 눈동자 패턴 홍채 패턴, 지문, 음성, 손바닥 형상, 얼굴형을 대상으로 한다.
(b) 생체정보식별자의 정보는 다음의 경우를 제외하고는 상업적인 목적으로 사용해서는 안 된다. 즉, 생체정보를 수집하기 전에 개인에게 통보해야 하고, 정보를 수집하기 전에 생체정보식별자 개인의 동의를 받는다.
(C) 생체정보식별자 개인의 정보공개와 관련하여 상업적인 목적으로 획득한 개인의 생체정보식별자를 보유하는 정부기관은 본인의 동의 없이 생체정보식별자를 매매, 임대 또는 제3자에게 공개해서는 안 된다. 또한 생체정보식별자가 누설되지 않도록 동등한 혹은 다른 비밀정보를 보호하는 방법보다 더욱 주의하여 보관, 전송하여야 한다.
(d) 위에 언급한 규정을 위반하는 자는 각 위반행위마다 최대 $25,000의 민사벌금을 받을 수 있다.

(2) **일리노이: 생체정보 프라이시법**

일리노이 주는 2008년 「생체정보 프라이버시법」(Biometric Information Privacy Act of 2008)[101]을 통과시켰다. 이 법의 입법취지는 급격히 증가하는 생체정보인식기술을 활용한 금융거래 및 보안검사 기업으로부터 발생할 수 있는 신원도용의 위험으로부터 개인을 보호하기 위해서이다(740 ILCS 14/5).

이 법 제10조(정의)는 "생체정보식별자(Biometric Identifier)는 망막 혹은 홍채, 지문, 성문, 손과 얼굴모양을 대상으로 한다"고 규정한다. 이와 대조적으로 생체정보식별자에는 작성샘플(Writing sample), 서명, 사진, 타당한 과학적 실험에 사용된 인간생물학 샘플(Human Biological Sample), 인구통계(demographic data), 신장, 체중, 모발 색 또는 동공의 색과 같은 신체적 묘사는 포함하지 않는다(740 ILCS 14/10)고 하여 생체정보의 각 식별자에 대한 규범적 평가를 어느 정도 완결지었다.

---

mercial Code.
101) 740 ILCS 14/1 to 14/99 (2008 Supp.); P.A. 95-994, eff. 10-3-08.

또한, 제15조에서는 생체정보식별자나 생체정보를 보유한 민간기관은 그것의 보유, 수집, 공개, 파기에 있어서 대중에 공개할 수 있도록 정책을 문서화해야 하며, 초기의 보유목적이 만족되었거나 3년의 기간을 한계로 보유기관과 영구적 삭제일정에 대한 지침을 설정해 두어야 한다고 규정한다. 그리고 관할법원에서 발부한 유효한 영장(warranty)이나 소환장(subpoena)이 없는 한, 그 기관이 보유한 생체정보식별자나 생체정보는 설정된 보유기간과 파기지침을 준수하여 처리되어야 한다고 규정하고 있다(740 ILCS 14/15(a)).[102]

(3) **뉴저지**: **생체정보식별자 프라이버시법**

뉴저지 주에서는 「생체정보 식별자 프라이버시법」(Biometric Identifier Privacy Act)의 제정을 2002년과 2006년에 걸쳐 시도하였으나, 회기 만료에 의한 법안 자동폐기로 입법에 성공하지 못한 바 있다. 이 법안에 따르면, 생체정보 식별자의 정의와 보호에 관한 내용은 텍사스 주법과 같지만, 텍사스 주법이 정부기관만을 대상으로 하고 있음에 반해, 뉴저지 주법은 생체정보 식별자를 보유하는 "모든" 자를 대상으로 하고 있다는 점이 다르다.[103]

(4) **캘리포니아**, **노스다코타**, **위스콘신**, **미주리**

캘리포니아,[104] 노스다코타,[105] 위스콘신,[106] 미주리[107] 등 4개 주의 법률에서는 고용자들이 근로자들에게 피부 아래에 삽입하여 식별정보(identifying information)을 전송하는 마이크로 칩의 사용을 강제하지 못하도록 규정하고 있다.[108]

---

102) http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (2016.10.10. 최종접속)
103) http://www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM (2016.10.10. 최종접속)
104) California Acts Ch. 538, Section 52.7 (2009).
105) North Dakota Statutes 12.1-15-06 (2008).
106) Wisconsin Statutes 146.25 (2009).
107) Missouri Revised Statutes 285.035 (2008).
108) 그러나 근로자들이 "자발적으로" 장착하는 것까지 금지하는 것은 아니라고 한

제 4 절 독 일

Ⅰ. 생체정보의 활용

“생체정보(Biometrie 또는 Biometrische Daten)”는 일반적으로 사람을 식별할 수 있는 목소리, 행동 습관, 얼굴, 홍채, 지문, 손금, 필체 등을 망라한 개인적인 정보로서,[109] 최근 독일에서도 개인식별수단 혹은 비밀번호 등의 대용으로 생체정보를 사용하는 일이 활발해졌으며, 특히 2005년 11월부터는 지문 등의 생체정보 칩을 저장한 여권이 사용되고 있다.[110]

인간의 생체정보는 신체적, 심리적 요소와 행동 구조와 관련되어 있으므로, 독일 생체정보 산업은 이러한 관련성을 바탕으로 통신 및 정보기술 분야에서 생체상의 정보를 통해 신원을 인식하는 목적을 가진 특수한 보안 절차로서 발전해 왔다. 특히, 독일의 기업들은 신체적 요소로서 홍채 및 망막, 지문, 혈관, 안면, 손금, 귀의 형태, 목소리 및 조혈 구조에 대한 인식기술은 물론, 행동양식에 대한 정보인식기술로서 필체, 눈의 깜박임, 목소리, 입술의 움직임 및 걸음걸이 등이 인식 대상으로 개발되어 왔다.[111]

< 독일의 생체정보 기술 개발 분야>

생체정보요소	판독 기기	주요 해결 과제
손가락 지문	센서칩 / 시각 스캐너	손가락에 상처나 이물질이 있는 경우 해결방안 필요

다. Matthew W. Finkin, Some Further Thoughts on the Usefulness of Comparativism in the Law of Employee Privacy, 14 Employee Rts. & Emp. Pol’y j. 43, fn. 32, 2010.

109) Heumann, Björn, Whitepaper Biometrie, 2006, S. 3 f.

110) Spiegel Online, ePass: Biometrischer Reisepass kostet 59 Euro, 1. 6. 2005. http://www.spiegel.de/reise/aktuell/epass-biometrischer-reisepass-kostet-59-euro-a-358564.html(2016.10.6. 최종접속)

111) Lipinski, Klaus, Biometrie, IT Wissen, Dietersburg, 2009, S. 4.

생체정보요소	판독 기기	주요 해결 과제
손금	시각 스캐너	환자의 경우 해결 방안 필요
음성	마이크로폰	주변 소음, 목소리 변경, 병상에서의 이용 가능성 고려
안면	카메라	의상 및 날씨의 영향 고려
홍채	특수 카메라	환자의 경우 또는 손상된 홍채일 경우
망막	적외선 레이저	환자의 경우 또는 손상된 망막일 경우
서명	서명판	심리 또는 건강상태에 따른 영향 고려
키보드 사용 패턴	키보드	심리 또는 건강상태에 따른 영향 고려
행동 양식	카메라	변경 가능성 고려

출처 : Lipinski, Klaus, Biometrie, IT Wissen, Dietersburg 2009, S. 4.

현재 독일에서 생체정보는 주로 “공적 분야”에서 개인의 신분확인을 위해 여권, 체류허가 및 기타 신분증에 저장하여 활용하고 있으며, 특히 2005년 11월부터 지문 등의 생체정보 칩을 저장한 전자여권을 사용하기 시작하면서, 생체정보의 활용과 개인정보의 침해 및 보호의 문제가 대두되었다.[112)]

1. 내・외국인의 신분 증명

생체정보 관련 규정을 담고 있는 법령의 목록에서 보듯이, 독일에서 가장 널리 생체정보를 활용하고 있는 분야는 공적인 분야로서 특히 여권, 체류허가 및 기타 신분증에 생체정보를 저장하는 것이라고 할 수 있다.[113)] 출입국 시, 공적 부조의 신청 시 또는 체류 허가 시의 신

112) 김영미, “독일의 생체정보 관련 법제 동향”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 177면.

113) Meuth, Lotte, Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, Duncker & Humblot, Berlin 2005, S. 44.

원 확인을 위해 사용되며, 크게 내국인을 위한 여권 및 신분증과 외국인을 대상으로 하는 체류허가증에서의 사용으로 분류할 수 있다.

먼저, “내국인” 신분증에서의 생체정보는 「여권법」과 「개인신분증명법」에 그 근거를 두고 있다. 「연방기본법」 제1조제1항 내지 제2조제1항의 인간의 존엄 및 기본적 인격권의 원칙에 따라, 생체정보를 포함한 개인정보는 법률상 수권을 받은 행정청에 한해 수집할 수 있다. 이에 따라 여권법 제22조제1항 및 개인신분증명법 제7조 및 제8조는 개인 정보에 대한 작업과 이용 권한을 관련 행정청(여권 행정청, 신분증명 행정청)에 부여하고 있다.

위 두 법은 모두 여권 및 신분증명에 저장하기 위해 수집할 수 있는 생체정보의 종류에 대해 제한 규정을 두고 있다. 다만, 그 범위와 규정 방식에 있어서는 양자 간에 차이가 있는데, 여권법의 경우 제4조제3항을 통하여 같은 조 제1항 및 제2항에서 규정하고 있는 여권의 기재 정보에 해당하는 일반적인 개인정보 외에도, 여권에 생체정보로서 사진, 지문, 지문이 어느 손가락의 것인지에 대한 정보 및 지문 날인 상태에 대한 진술이 포함된다고 규정하고 있다. 즉, 사진과 지문을 일반정보와 구별하여 생체정보로서 규정하고 있는 것이다.

반면, 개인신분증명법은 제5조에서 신분 증명에 포함되는 정보를 열거하면서, “생체정보”라는 용어의 사용 없이, 같은 조 제2항의 개인 신분 증명에 저장되어야 할 정보 가운데 하나로 “사진”을 제시하고 있다. 지문에 대해서는 같은 조 제9항에 따라 당사자의 신청이 있는 경우에만 신분 증명에 포함시킬 수 있다.

한편, 독일에 거주하는 외국인에게 부여하는 신분 증명(체류허가증) 상의 생체정보 사용에 대해서는 「외국인체류법」이 규정하고 있다. 동법 제3조에 따라 독일에 거주하는 외국인은 유효한 여권을 소지할 의무가 있으며, 제48조제1항제2호에 따라 체류허가증을 소지해야 하는

한편, 같은 조 제2항에 따라 체류허가증을 통해 신원을 확인할 수 있어야 한다. 여권법 등과 마찬가지로 외국인을 위한 신분 증명에도 일정한 생체정보의 요소들이 사용되며, 행정청은 체류 허가 시에 지문 및 안면 사진 등의 생체정보를 수집하게 된다.

그러나 내국인 신분 증명 시의 생체정보 사용과 외국인 신분 증명 시의 생체정보 사용에 대한 규정에 있어서는 규정 방식에 중요한 차이가 있다. 즉, 법률을 통해 생체정보의 수집 및 저장 범위와 그 권한을 규정하고 있는 내국인 신분 증명과는 달리, 외국인 신분 증명에 사용하는 생체정보의 수집 권한 및 범위는 법규명령을 통해 규정되어 있다는 점이다. 따라서 연방정부는 법적인 상황의 변화에 따라 연방참사원(Bundesrat)의 동의만 있으면, 외국인 등록에 필요한 생체정보 요소의 수집 범위를 달리 결정할 수 있을 것이다.[114] 한편, 난민수용법은 행정청이 수집 및 열람할 수 있는 생체정보의 범위를 지문, 사진 및 홍채로 규정함으로써, 일반적인 외국인 신분 증명 시에 사용하는 생체정보보다 더 넓은 범위를 인정하고 있다.

2. 형사절차에서의 활용

일반적인 수사절차에서 생체정보를 사용할 수 있는 근거는 법규명령인 "형사절차규칙(Strfprozeßordnung, StPO)" 제163조b가 제시하고 있다. 즉, 같은 조 제1항은 검찰 및 경찰공무원이 용의자에 대한 신원확인을 할 수 있다는 내용을 규정하고 있으며, 제2항은 피의자가 아닌 자에 대한 신원확인은 보다 엄격한 요건 하에서 이루어져야 한다는 점을 규정하고 있다. 제1항제1문이 용의자에 대한 신원 확인을 위해 필요한 모든 조치가 허용된다고 규정하고 있는 반면, 제2항에 따라 용의자 아닌 사람에 대한 신원 확인은 범죄 행위에 대한 명확한 수사

114) 이에 대해 Meuth, *op. cit.*, S. 62. 참조.

를 위한 목적에서만 가능하며, 당사자의 반대 의사가 있을 경우에는 허용되지 않는다. 따라서 용의자에 대해서는 우선 신분증에 대한 확인 절차를 거쳐, 의심스러울 경우 필요하다면 신분증에 저장된 생체정보 확인을 통한 신원 확인이 허용된다.[115] 그러나 용의자가 아닌 사람에 대해서는 신원 확인을 위한 조치가 필요하다 하더라도, 범행 수사의 목적에 따른 비례성 원칙이 준수되어야 한다. 즉, 용의자 아닌 사람에 대한 생체정보 조사는 신분증 제시에도 불구하고 당사자의 신원이 명확하지 않을 뿐만 아니라, 해당 범죄행위의 중대함이 생체정보 조치를 해야 할 정도로 클 경우에만 가능하다.[116]

형사소송규칙 제163조d는 이른바 "저인망식 수사(Schleppnetzfahndung)"[117]에 대해 규정하고 있으며, 엄격한 요건 하에 이를 허용하고 있다. 즉, 경계 검문 시에 필요한 단기간의 개인 정보를 수집할 수 있으며, 경우에 따라 생체정보가 포함될 수 있다. 단, 이를 위해서는 제2항제1문에 따라 법관의 명령을 받아야 하며, 그 명령은 정보와 관련된 조치의 시간적, 공간적, 방법상의 한계를 명확하게 담아야 한다.[118]

마지막으로, 컴퓨터를 이용한 범인 탐색(Rasterfahndung) 시에도 생체정보를 활용한다. 형사소송규칙 제98조a는 특정 수사영역[119]에서는 사

115) Meuth, *op. cit.*, S. 101.

116) Meuth, *op. cit.*, S. 102.

117) 이는 일정한 수사 영역에서 대량 검문 및 경계 검문 등을 통해 용의자를 색출하는 내용의 수사를 말한다.
http://www.rechtslexikon.net/d/schleppnetzfahndung/schleppnetzfahndung.htm. (2016.10.10. 최종접속)

118) 이에 대해 Meuth, *op. cit.*, S. 102 f. 참조.

119) 같은 조 제1항 제1문은 범죄가 다음과 같은 영역에서 중대한 의미를 갖는 사실상의 근거가 있을 경우에 컴퓨터 수사가 가능하다고 규정하고 있다.
1. 금지된 마취제 또는 무기 거래, 화폐 및 유가증권 위조 영역,
2. 국가 안보 영역,
3. 공공의 안전을 해치는 범죄 영역,
4. 생명 또는 신체, 성적 자기결정권 또는 개인의 자유에 대한 침해,
5. 직업상 또는 관습상의 의미에서 중대한 범죄일 때,
6. 범죄조직 또는 기타 방식으로 조직된 범죄.

실관계의 탐문이나 범인의 거처에 대한 수사 다른 방식으로는 불가능하거나 현저히 어려울 경우에 한해, 수사기관이 컴퓨터에 저장된 자료를 이용한 컴퓨터 범인 탐색을 할 수 있다고 규정하고 있다. 이 때 신분증명에 저장되었거나 비디오 관찰 또는 다른 방식으로 수집된 생체정보 역시 활용할 수 있다고 해석해야 할 것이다.[120] 또한 형사소송규칙 제98조c는 어떤 수사 절차에서 다른 수사 절차, 집행 절차 또는 방첩 절차를 통해 얻은 개인 정보를 기계를 이용해 대조할 수 있다고 규정하고 있다. 여기서 말하는 개인정보에는 생체정보 역시 포함된다고 해석할 수 있을 것이다.[121]

3. 생체정보 시스템의 연구

1999년에서 2000년 사이에 독일연방정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik, BSI)은 "생체정보 신원확인 시스템의 비교 연구"(Vergleichende Untersuchung biometrischer Identifikations-system, BioIS)라는 프로젝트를 통해 국내·외에서의 생체정보 활용의 필요성과 생체정보 활용을 위한 기기개발 기술에 대한 연구를 진행하였다.[122] 또한 연방의회는 2002년 생체정보 인식기술을 신분 증명 등에 활용하는 것에 대해 입법에 앞서 정보보호법 및 정책수요자 관점에서의 연구를 수행함으로써 생체정보 기술의 활용 범위를 설정하고자 하였다. 연방 의회는 2003년에 다시 생체정보 요소 중 어떤 것들을 신분 증명에 활용할 수 있을 것인지에 대한 연구를 수행했으며, 슐레스비히-홀스타인(Schleswig-Holstein)주 역시 독자적으로 생체정보를 신분증명에 포함시키도록 한 여권법 및 개인신분증명법의 변경을 개인정보 보호의 차원에서 평가하는 내용의 연구를 시행하였다.[123]

120) Meuth, *op. cit.*, S. 104.
121) Meuth, *op. cit.*, S. 103 f.
122) Gruner, Alexander, Biometrie und informationelle Selbstbestimmung – Rechtsfragen biometrischer Merkmale in Pass und Personalausweis, Dresden, 2005, S. 47.
123) Gruner, *op. cit.*, S. 50.

현재에도 연방정부 차원에서 일반적인 산업 진흥 내지 정책 개발 차원에서의 연구 지원은 일부 행하고 있다. 예컨대, 연방 교육 및 연구부(Bundesministerium für Bildung und Forschung, 이하 BMBF)는 생체정보 활용을 통한 공공 보안을 향상시키는 한편, 생체정보를 수집 및 이용하는 절차의 안전성을 높이기 위한 연구를 프랑스 정부와 공동으로 수행한 적이 있다.[124] 이 연구를 통해 연방정부는 경찰관청 내지 관세관청이 생체정보를 활용할 수 있는 가능성을 모색했으며, 이른바 "다중(복합) 생체정보(mulitmodale Biometrie)"라는 방식을 통해, 상이한 종류의 신원확인 수단을 "결합"시키는 방식에 대해 조사하였다. BMBF가 2016년 6월 현재 진행하고 있는 생체정보 관련 진흥 내용은 무선 생체정보시스템 모듈에 대한 연구이다.[125]

Ⅱ. 생체정보 관련 규범

독일법은 "개인정보(Personenbezogene Daten)"를 생체정보의 상위개념으로 간주하며, 두 개념을 명백히 분리하고 있다.[126] 그러나 독일의 연방 법률도 직접적으로 "생체정보(Biometrie)"라는 용어를 일반적으로 정의하거나 그 범위를 정하고 있지 아니하며,[127] 생체정보의 활용이나

---

124) Borchers, Detlef, Bundesregierung fördert Biometrie-Forschung, heise online, 3. 4. 2010. http://www.heise.de/newsticker/meldung/Bundesregierung-foerdert-Biometrie-Forschung-946316.html. (2016.10.13. 최종접속)

125) http://www.gesundheitsforschung-bmbf.de/de/2514.php (2016.10.13. 최종접속)

126) "개인정보"라는 용어에 대해서는 연방정보보호법(Bundesdatenschutzgesetz)이 제3조 제1항을 통해 "특정 또는 특정 가능한 자연인의 개인적 사실적 관계에 대한 개별적인 언급"이라고 정의하고 있다.

127) 단, 유럽연합이 기존의 지침을 폐지하고 지난 4월 발령한 "개인정보의 취급에 있어서의 자연인 보호와 자유로운 정보 교환 및 지침 95/46/EG의 폐지를 위한 유럽 규칙(Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG)"은 제4조 제14호에서 "생체정보상의 데이터(biometrische Daten)"에 대해 "특별한 기술적 절차를 통해 얻은 자연인의 신체적, 생리학적 또는 행동 약식과 관련한 요소를 담은 개

관리(보호)에 대하여도 그것을 일률적·통합적으로 규정하고 있는 법률이 아직은 존재하지 않는 것으로 보인다. 다만, 각종의 개별 법률 내지 법규명령 중에 생체정보의 수집 내지 사용과 관련된 내용을 규율하고 있는 경우가 있다. 따라서 생체정보가 독일법제 내에서 어떤 의미로 사용되고 있는지 살펴보기 위해서는 각 법령에 산재해 있는 위와 같은 내용을 규율하고 있는 규정의 내용을 검토하여 그 사용례를 정리해 보는 수밖에 없을 것이다.

독일법상의 생체정보 이용은 주로 공공분야에서의 내·외국인의 신분 확인과 관련한 규정을 통해 나타나고 있으며, 그 범위는 일반적으로 “사진”과 “지문”에 한하며, 경우에 따라서는 홍채까지도 포함하는 것으로 확인된다.

< 독일 법령상의 생체정보 관련 규정 >

법령명		관련 조문	생체정보의 범위 및 특징
테러방지법	외국인 체류법	제49조제1항 제99조제1항 (시행령제61조g제4항)	- 사진 및 지문 - 일반적인 개인정보와 구별
	여권법	제4조제3항	- 사진 및 지문 - 일반적인 개인정보와 구별 - 생체정보를 저장하는 정보은행 설립 금지
	난민법	제16조제1항a	- 사진, 지문 및 홍채
	개인신분 증명법	제17조 제20조제4항	- 사진, 당사자 동의시 지문 - 일반적인 개인정보와 구별 없음

인 정보로서 이를 통해 해당 자연인을 명백하게 식별하거나 확인할 수 있는, 안면 또는 지문 정보와 같은 것”이라고 정의하고 있다. 독일법상의 생체정보 역시 이러한 의미의 범위에서 쓰일 것이다.

법령명	관련 조문	생체정보의 범위 및 특징
전자서명기본법		- 생체정보의 범위에 대한 언급 없음

1. 테러방지법

2001년 9·11 테러가 발생한 후, 독일은 유럽연합이 테러행위에 대한 공동대처를 결정하는 데에 앞서 이미 신분증명에 대한 각종 법률을 개정하여 생체정보를 활용하기 시작하였다. 그 근거가 되는 법률은 2002년 1월 9일 전면 개정된「국제적인 테러리즘의 방지를 위한 법률(Gesetz zur Bekämpfung des intenationalen Terrorismus, Terrorismusbekämpfungs- gesetz, TBG)」, 즉「테러방지법」이다. 총 21개의 조문으로 구성된 테러방지법은 여권 및 개인신분증, 외국인을 위한 증명서류에 생체정보를 저장하는 것과 관련한 규정을 주요 내용으로 한다.

이들 규정을 통하여「여권법」과「개인신분증명법」상의 생체정보의 저장과 관련한 내용이 개정되었으며,「외국인체류법」과「난민법」에서도 외국인과 난민신청자들의 신분증에도 생체정보의 저장을 요구하게 되었다. 물론 이러한 생체정보에 관한 규정은 내용상 적정성, 필요성과 적절성을 전제로 한다.[128]

(1) 여권법

명령(Verordnung) (EG) Nr. 2252/2004을 근거로 한 테러방지법 제7조에 의해 여권법 제4조에 다음과 같은 2개의 추가조항이 신설되었는데, 이것이 생체정보에 관한 것이다. 즉, 제4조제3항제1문은 각종 여권에 "사진, 지문 등의 생체정보가 포함되어야 한다"고 규정하고 있으며, 제2문은 해당 정보를 권한 없이 열람, 변경 및 삭제해서는 안 된

128) 김영미, 앞의 글, 177-178면.

다고 규정하고 있다. 특히, 제3문은 연방 차원에서 제1문의 생체 정보를 저장하는 정보은행을 만들지 않는다고 규정한다.

그리고 이러한 생체정보의 활용은 기본권을 침해하지 않아야 하고, 행정청에 한하여 수집할 수 있으며, 작업 및 이용권한은 관련 행정청이 가지도록 하고 있다(제22조).

(2) 개인신분증명법

「개인신분증 및 전자신원증명에 관한 법률」(Gesetz über Personalausweise und den elektronischen Identitätsnachweis, PAuswG)은 2002년 1월 9일부터 생체정보의 저장을 허용되고 있었다.

특히, 2010년 전자개인신분증 관련 규정이 다수 포함되었는데, 여기에 저장되는 생체정보에는 “사진”과 “지문”이 있으며, 지문은 당사자의 신청이 있는 경우에만 저장할 수 있다(제5조제9항). 그리고 제17조에 따라 권한 있는 행정청은 역시 전자적으로 저장 및 작업된 신분 증명상의 생체정보 및 기타 정보를 열람하고, 필요한 생체정보를 수집할 수 있으며, 이 생체정보를 비교할 수 있다.

또한 제20조제4항에는 위의 AufenthV 제61조g제4항과 동일한 내용의 생체정보와 관련한 언급이 있다. 즉, 운송회사가 필요한 경우 신분증상의 개인정보를 열람할 수 있지만, 생체정보에 대한 열람은 불가능하다는 것이다.

(3) 외국인체류법

「외국인의 독일 내 체류, 직업활동 및 이민에 관한 법률」(Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet, AufenthG, 이하 외국인체류법)은 외국인의 신분증명, 즉 체류허가증에 생체정보를 저장할 수 있는 근거가 된다. 즉 외국인의 신원확인에는 “사진”과 “지문”이 가능한데, 제49조제1항제1문은 이 법

률에 따른 집행권한을 위임받은 행정청은 저장된 생체정보 및 기타 정보를 열람하고, 당사자로부터 필요한 생체정보를 입수할 수 있으며, 생체정보를 서로 비교할 수 있다고 규정하고 있다. 다만, 제3문은 이러한 생체정보는 “지문”과 “사진”에 국한한다고 규정하고 있다.

또한 같은 법 제99조 제1항 제13호a는 각종 유럽 규정 등에 따른 이국인, 난민 및 무국적자의 여행자증명과 관련한 규정을 제정할 권한을 연방내무부(Bundesministerium des Innern)에 부여하고 있다. 이 때 생체정보와 관련해서는 사진과 지문과 같은 정보의 수집, 분류, 저장 및 삭제 등에 관한 절차와 기술적 요건 등에 대한 규칙을 제정할 수 있도록 하는 것이다. 이 법 시행령(Aufenthaltsverordnung, AufenthV) 제61조g제4항제1문은 (앞서 언급한 개인신분증명법의 경우와 마찬가지로) 운송회사가 일정한 경우 여행자 증명을 열람할 수 있다고 규정하고 있지만, 제2문에서는 이 중 생체정보는 열람해서는 안 된다고 규정하고 있다.

(4) **난민법**

「난민법」(Asylgesetz, AsylG)은 2015년 10월 24일부터 난민법(AsylG)으로 명칭을 변경하여 적용한 것으로,「기본법」 제16조의 난민권을 실현하기 위한 법으로서 외국인체류법과 더불어 난민에 대한 기본적인 사항을 정한다. 이 법에 의하여 독일 연방정부는 연방참사원의 동의를 받아 난민에 대해서는 생체정보의 범위를 일반 외국인 등록의 경우와 다르게 정할 수 있다.

이 법 제16조제1항a제1문에 따르면, 행정청은 외국인의 서류 및 신원 확인을 위해 전자적으로 저장된 여권 기타 신분확인 서류의 생체정보 및 기타 개인정보를 열람할 수 있고, 필요한 생체정보를 수집할 수 있으며, 이 생체정보를 서로 비교할 수 있다. 제2문에서는 제1문이 의미하는 생체정보는 “지문, 사진 및 홍채에 한한다”고 정하고 있는

데, 이는 외국인체류법과 달리 난민법은 행정청이 수집, 열람할 수 있는 생체정보의 범위를 사진과 지문 외에 홍채까지 확대한 것이다.[129]

2. 전자서명기본법

「전자서명기본법」(Gesetz über Rahmenbedingungen für elektronische Signaturen, SigG)은 기존의 「서명법」을 2001년 5월 폐지하고 제정한 것이다. 2004년 개정된 전자서명기본법은 유효한 서명에 인증을 필수 요건으로 하였는데(제2조제9호), 이는 전자서명 기술의 진보로 생체서명시스템 공급자가 신원확인에 자필서명을 사용할 수 있게 한 것이다.

한편, "전자서명에 관한 명령"(Verordnung zur elektronischen Signatur, SigV)은 제15조제1항제1문에서 전자서명 신원확인 방법의 하나로 하나 또는 복수의 생체정보 확인을 들고 있다. 또한 제3문은 생체정보를 사용할 경우 권한 없는 사용을 배제하며 안전성이 확보된다는 점을 충분히 보장해야 한다고 규정하고 있다.

Ⅲ. 판 례

독일 내에서 생체정보 활용을 허용할 것인가를 전면적으로 다룬 판례는 아직까지 찾아볼 수 없고, 연방헌재가 생체정보의 사용이 기본법에 위반하는지 여부도 판단한 바 없다.[130] 다만, 연방헌재는 2012년 12월 30일 여행자여권에 생체정보를 저장하는 것이 허용되는지에 대한 헌법소원을 각하한 바 있는데,[131] 이 결정에 의하면, 전자적 방식으로 저장된 생체정보가 정보은행 형식으로 저장되고 수사 등의 목적으로 이용된다면 기본법상의 정보적 자기결정권을 침해할 가능성이

129) 김영미, 앞의 글, 180면.
130) 김영미, 앞의 글, 185면.
131) BVerfG, Beschluss vom 30. 12. 2012 - 1 BvR 502/09 = BeckRS 2013, 47059.

있다고 하여 헌법소원을 제기하였으나 구체적으로 어떤 조치나 법규정이 권리를 침해하고 있는지 적시하지 않아 각하된 것이다.

반면에, 독일 여권법 제4조제3항에 따라 회원국가에서 발급된 여권과 여행증명서의 생체정보(지문)와 보안성 규범인 유럽규칙 VO(EG) Nr. 2252/2004에 대하여 2013년 독일 시민 미하엘 슈바르츠(Michael Schwarz)가 게젤키르헨 행정법원(VG Gelsenkirchen)에 유럽인권협약(EU-Grundrechtecharta) 제7조와 제8조 제1항에 근거하여 독일 여권법과 유럽법 규정에 의문을 제기한 것에 대하여 동 법원은 유럽법원에 그 판단을 의뢰하였고, 유럽법원이 제시한 정당화 사유는 다음과 같이 요약할 수 있다.[132)]

- 손가락 지문의 수집과 저장이 개인정보보호의 관점에서 개인의 권리를 일부 침해한다고 인정할 수 있으나, 여권 내지 여행자 서류 오남용에 대비할 필요가 있다.
- 개인정보보호는 '비례성(Verhältnismäßigkeit)'에 따라 판단되어야 함으로 지문의 저장이 오남용을 완전히 방지할 수는 없지만, '현저히 경감' 시킬 수는 있고, 현재로서는 지문의 수집 외에 다른 대안이 사실상 존재하지 않는다.
- 특히, 홍채 인식은 아직은 기술 및 비용적 측면에서 불가능한 상황이라고 할 수 있다.
- 더욱이 수집된 지문 정보의 오남용 방지를 위한 보호 장치가 충분히 되어 있다.

그러나 유럽법원은 이상의 정당화 사유 외에 다른 생체정보에 대한 저장 및 취급 요건에 대하여 언급하지 않았고, 게젤키르헨 행정법원(VG Gelsenkirchen)이 유럽법원에 판단을 의뢰 하면서 제기했던 중앙시스템에 저장하는 문제와 수집한 생체정보를 다른 목적을 위해 사용

132) EuGH, Urt. v. 17. 10. 2013 - C-291/12 = NVwZ 2014, 435.

할 수 있는 위험성에 대해서 언급하지 않아 판단을 회피하였다는 점에 대하여 비판을 받고 있다.[133]

한편, 2015년 네덜란드의 국내법이 유럽법에 따라 여권에 지문정보를 저장하도록 한 규정이 유효하다는 유럽법원의 판결이 있었는데, 특히 각 회원국들이 여권에 활용하기 위해 수집·저장한 생체정보를 다른 목적으로 사용하지 않을 것이라는 점을 국내법 규정을 통하여 보장할 의무는 없다고 판단하였다.[134] 이 판례 또한 개인정보보호의 관점에서 법적 판단을 회피하였다는 비판을 받고 있다.[135]

제 5 절 일 본

Ⅰ. 생체정보의 활용

1. 자동차 운행관리 솔루션

2015년 5월 14일 주식회사 Toshiba와 일본 IBM은 두 기업의 기술을 융합하여 drive recorder나 GPS 등의 종래의 정보에 운전자의 생체정보를 더하여 안심·안전·에너지절감 등의 실현을 위한 자동차운행관리 솔루션분야에서 협력하기로 하였다. drive recorder나 GPS 등의 정보에 운전자의 건강상태와 생체정보를 추가하고 수집된 데이터를 해석하여 그 결과를 보다 안전하고 에너지절감으로 이어지는 운행관리 솔루션 개발에 활용하려는 것이다. 개발된 서비스는 운송회사나 택시회사, 보험회사 등 다양한 기업들에 제공될 것이다.[136]

---

133) Pfeiffenbring, EuGH: Erfassung von Fingerabdrücken in Reisedokumenten, MMR-Aktuell 2013, 352719.

134) EuGH, Urt. v. 16. 4. 2015 - C-446/12 bis C-449/12 = BeckEuRS 2015, 431545.

135) Biselli, Urteil des Europäischen Gerichtshofes zu biometrischen Personalausweisen ignoriert Datenschutz, Netzpolitik, 21. 4. 2015.

136) http://www-03.ibm.com/press/jp/ja/pressrelease/48637.wss (2016.10.9. 최종접속)

2. 헬스케어 서비스

주식회사 핑크(FiNC)는 헬스케어의 예방영역에서 서비스를 제공하는 기업으로서 생활습관의 지도, 유전자검사 등을 이용한 여러 가지 헬스케어서비스의 기획과 개발을 통해 운영하고 있다. 2012년 4월 설립 당시 DNA와 혈액, 생활습관 등을 조사하는 유전자검사 서비스를 제공하였으나 검사만으로는 이용자에게 정보를 제공하는 것 이상의 support를 할 수 없다는 판단 아래, 이용자가 웹 사이트상에서 매일의 식사 동영상과 체중을 업로드 함으로써 영양사 등 전문가의 지도를 받을 수 있는 서비스를 제공하였는데, 대표적으로 유전자와 혈액정보 등 생체정보를 이용하여 각 이용자에게 헬스케어 콘텐츠를 추천하는 퍼스널 코치 애플리케이션을 들 수 있다. 또한, 이 기업은 2015년 10월 헬스케어서비스인 '퍼스널 신체 support'를 소프트뱅크와 공동개발하기로 한 내용을 발표하고 IBM의 인공지능 IBM Watson을 활용하여 퍼스널데이터에 기초한 고품질의 헬스케어서비스를 제공하였다.[137]

3. 익명화기술

빅 데이터 분석과 사물 인터넷(IoT)의 발전에 따라 데이터는 더욱 증가할 것이고 수집된 데이터를 개인정보로 활용함으로써 새로운 비즈니스 기회의 창출이 기대된다.[138] 이에 반하여, 사이버 공격과 내부 부정에 의한 대규모의 개인정보 유출, 프라이버시에 대한 배려가 없는 서비스의 중지 등의 사례도 발생하고 있어 각종 규범도 강화되는 경향에 있는데, 후지쯔 연구소에서는 이들 법안과 규제에 준거한 프라이버시 정보를 익명화・암호화하는 기술을 개발하고 있다. 여기서 개발한 것이 k-익명화 등 소위 "익명화 기술"이다.

137) https://jobs.forkwell.com/finc/jobs/558 (2016.10.9. 최종접속)

138) 강영기, "일본의 생체정보 관련 법제 동향", 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 233면.

2013년 7월 JR동일본 전철주식회사가 Suica의 승차이력 데이터를 익명화하여 판매하고자 한 사례가 있는데, 사업자에 대해 많은 이용자로부터 반대하는 의견이 많아서 사실상 서비스를 정지하였다. 이러한 영향으로 퍼스널데이터의 취급에 관한 규율을 명확히 하기 위해 내각 IT 종합전략본부는 '퍼스널데이터에 관한 검토회'를 설치하고 2014년 6월에 '퍼스널데이터의 활용에 관한 제도개정대강'을 만든 다음에, 2015년 개인정보보호법이 개정되어 2017년에 시행될 예정이다.

익명화 기술은 익명가공정보로 가공하는 데에는 여러 가지 수법이 사용되지만, 익명가공정보를 생성하는 수법에 요청되는 익명가공기준에 대해서는 분야마다 개인정보보호위원회가 향후 책정할 것이라고 한다. 익명화 기술로 불리는 개인을 특정할 수 없도록 데이터를 가공하는 기술이 유력한 후보로 떠오르고 있는데, 하나는 "가명화" 기술로서 실명을 가명으로 바꿈으로써 개인의 특정을 방지하는 것으로서, 가명화한 후에도 동일인물의 건강상태의 경과를 추적할 수 있는 장점이 있지만, 성별이나 연령 등 간접적으로 개인을 특정할 수 있는 속성의 조합으로 기록에 대응하는 개인을 특정할 가능성이 있다는 점이 단점이 있다.[139]

또 다른 하나는 "k-익명화"로서 간접적으로 개인의 특정가능한 속성을 준(準)식별인자(QI, Quasi-identifier)로 정의함으로써 동일한 QI의 조합이 반드시 k명 이상 존재하도록 데이터를 가공하고 기록에 대응하는 개인특정을 방지하는 방식이 있다.[140]

Ⅱ. 생체정보 관련 규범

일본에서도 생체정보에 관하여 직접적으로 그 개념이나 유형에 관하여 명문의 규정을 두고 있는 규범은 존재하지 않는 것으로 보인

139) 강영기, 앞의 글, 234면.
140) 이 방식의 자세한 내용은 강영기, 앞의 글, 234면.

다.[141] 다만, 개인정보와 관련하여 우리나라와 같이 「개인정보의 보호에 관한 법률」이 일반법적인 역할을 수행하는데, 최근 2015년에 개인정보보호법이 개정되면서, 개인정보의 정의를 명확히 한다는 취지에서 "개인식별부호" 및 "배려를 요하는 개인정보"라는 카테고리가 새로 마련되었다는 점에 주목할 필요가 있다. 2015년 개정 법률의 내용을 간단히 살펴본다.

< 일본 「개인정보의 보호에 관한 법률」의 체계 >

제1장 총칙
제2장 국가 및 지방공공단체의 책무 등
제3장 개인정보의 보호에 관한 시책 등
 제1절 개인정보의 보호에 관한 기본방침
 제2절 국가의 시책
 제3절 지방자치단체의 시책
 제4절 국가 및 지방자치단체의 협력
제4장 개인정보취급사업자의 의무 등
 제1절개인정보취급사업자의 의무
 제2절 익명가공정보취급사업자 등의 의무
 제3절 감독
 제4절 민간단체에 의한 개인정보보호의 추진
제5장 개인정보보호위원회
제6장 잡칙
제7장 벌칙

1. 개인정보의 개념

개정 법률 제2조(정의)에서 정하고 있는 개인정보의 유형인 "개인정보", "개인식별부호", "배려를 요하는 개인정보"의 개념을 살펴보면 다음과 같다.

141) 日本弁護士連合会, パーソナルデータの基本的枠組みについての意見書, 2014年11月20日, 7頁.

개인정보	① 이 법률에서 “개인정보”라 함은 생존하는 개인에 관한 정보로서 다음 각 호의 어느 하나에 해당하는 것을 말한다. 1. 당해 정보에 포함되어 있는 성명, 생년월일 및 그 밖의 기술 등[문서, 도화 혹은 전자적 기록 - 전자적 방식으로 작성된 기록 -에 기재 혹은 기록되거나 또는 음성, 동작 및 그 밖의 방법을 사용하여 표시된 일체의 사항(개인식별부호를 제외)]에 의해 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조하여 확인할 수 있고, 그로써 특정의 개인을 식별할 수 있도록 되어 있는 것을 포함한다) 2. 개인식별부호가 포함된 것
개인식별부호	② 이 법률에서 “ 개인식별부호”라 함은 다 음 각 호의 어느 하나에 해당하는 문자, 번호, 기호 및 그 밖의 부호 중 정령으로 정하는 것을 말한다. 1. 특정 개인의 신체의 일부의 특징을 전자계산기의 용도에 이용하기 위하여 변환한 문자, 번호, 기호 및 그 밖의 부호로서 당해 특정 개인을 식별할 수 있는 것 2. 개인에게 제공되는 서비스의 이용 혹은 개인에게 판매되는 상품의 구입과 관련하여 할당되거나 또는 개인에게 발행된 카드 및 그 밖의 서류에 기재되거나 혹은 전자적 방식에 의해 기록된 문자, 번호, 기호 및 그 밖의 부호로서 그 이용자 혹은 구입자 또는 발행을 받는 자마다 달라지도록 할당되거나 또는 기재 혹은 기록됨으로써 특정의 이용자 혹은 구입자 또는 발행을 받은 자를 식별할 수 있는 것
배려정보	③ 이 법률에서 “배려를 요하는 개인정보”(要配慮個人情報)라 함은 본인의 인종, 신조, 사회적 신분, 병력, 범죄의 경력, 범죄로 인해 피해를 입은 사실 및 그 밖에 본인에 대한 부당한 차별, 편견 및 그 밖의 불이익이 생기지 않도록 그 취급에 특별히 배려를 요하는 것으로서 정령으로 정하는 기술 등이 포함되는 개인정보를 말한다.

출처 : 일본 수상관저, 개정법 대비표, 9-10면, (번역-이인호 중앙대교수) 참조. http://www.kantei.go.jp/jp/singi/it2/pd/pdf/taihihyo.pdf (2016.10.20.최종접속)

이에 따르면 생체정보에 관한 정보는 “개인식별부호”에 포함되어 “개인정보”로서 법률의 보호를 받는다. 예컨대 “지문인증데이터”는 지문이라는 특정 개인의 신체 일부의 특징을 컴퓨터에서 이용하기 위해 변환시킨 문자, 번호, 기호 기타 부호로서 지문은 사람마다 다르기 때문에 당해 특정 개인을 식별할 수 있는 데이터라 할 수 있을 것이다. 여기서 “특정 개인을 식별”한다는 것은 “일반인의 판단력과 이해력을 가지고 생존하는 구체적인 인물과 정보와의 사이에 동일성을 인정하는 데 이르는 것”을 말한다.[142] 간단히 말해서 지문의 주인이 다른 사람이 아니고 특정의 누구인지 알 수 있는 상태가 되면 특정 개인을 식별한 것이 되는 것이다. 실제로 법률 개정의 논의가 중의원에서 이루어졌을 당시인 2015년 3월 25일 담당대신의 답변에서도 “개인식별부호”의 예로서 지문인식 데이터가 상정되어 된 바 있다.[143]

그리하여 개정법에 따르면, “개인식별부호”에 해당하는지 여부는 최종적으로 정령에서 정하도록 하고 있는데, 이에 포함되는 개인정보를 일정한 규칙에 따라 정리함으로써 특정한 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 정보의 집합물로 목차, 색인 기타 검색을 용이하게 하기 위한 것을 가진 것을 가리킨다고 하고 있다(개인정보의 보호에 관한 법률 시행령 제1조). 물론 개정 전의 법률에 의해서도 개인을 식별할 수 있는 귀모양 인증데이터는 개인정보에 포함될 수도 있다고 보았기 때문에 생체정보라는 개념이 처음으로 개인정보에 포함된 것으로 볼 것은 아니다.[144]

그러나 이번 개정으로 새로이 “개인식별부호”가 정의되고 이에 해당하는 정보가 개인정보라는 것이 명확해졌고, 이에 따라 생체정보의 개념도 포섭이 된 것이라 할 수 있다.[145] 다만, 개정법에서는 “정령으

142) 瓜生和久　編著,「一問一答　平成27年改正個人情報保護法」, 2015. 12, 12面.
143) http://www.gojo-partners.com/column-ps/1132/ (2016.10.9. 최종접속)
144) 宇賀克也,「個人情報保護法の逐条解説(第4版)」, 2013. 10, 28面.
145) 森田賢二, “個人情報保護法の改正概要と企業の対応”, Risk Solutions Report, No.41, 銀泉リスクソリューションズ株式会社, 2015. 12. 09. 4頁.

로 정하는 것을 말한다"고 되어 있고, 구체적인 확정은 정령의 내용에 따르지만, 제1호는 생체인증 등에 사용되는 지문, 홍채, 정맥인식 데이터 등 개인의 신체적 특징을 디지털화한 정보 등을, 제2호는 면허증 번호, 여권번호나 포인트 카드의 회원번호 등이 해당될 것이다.

특히, 제2조제3항은 "일정한 배려가 필요한 개인정보"에 관하여 규정을 두고 있는데, 본인에 대한 부당한 차별 또는 편견이 생겨나지 않도록 인종, 신조, 병력 등이 포함되는 개인정보에 대해서는 본인 동의를 얻어 취득하는 것을 원칙적으로 의무화하고, 본인동의를 얻지 않은 제3자 제공(opt-out)을 금지한다.

한편, "개인정보 데이터베이스 등"이란 개인정보를 포함하는 정보의 집합물로서 그 이용방법으로 보아 개인의 권리 이익을 해할 우려가 적은 것으로 정령이 정하는 것을 말한다(제2조4항). 이를 "준(準)개인정보"라 하는데, 이는 법률이 개정되기 전 생체정보에 관한 명확한 명문의 법 규정이 없어 법적용에 있어서 개인정보 등에 관한 정의가 애매한 상황에서 그 해석을 어떻게 할 것인가에 관한 "제7회 퍼스널 데이터에 관한 검토회"의 기술검토 워킹그룹에서 해석한 것으로서 자료에서 제시된 바에 따르면 다음과 같다.[146)]

< 준개인정보의 구체적 사례[147)] >

① 여권번호, 면허증번호, IP주소, 휴대단말기의 ID 등 개인 또는 개인의 정보통신단말기 등에 매겨져 계속적으로 공용되는 것

146) "준(準)개인정보에 포함되는 구체적 항목"에 관한 보다 구체적인 내용은 '퍼스널 데이터에 관한 검토회'의 '기술검토 Working Group 보고서' "(가칭) 準개인정보 및 개인특정성 저감 데이터에 관한 기술적 관점에서의 고찰에 대하여", 2014. 5.를 강영기, 앞의 글. 228-229면에서 재인용.

147) "준(準)개인정보에 포함되는 구체적 항목"에 관한 보다 상세한 내용은 パーソナルデータに関する検討会, 技術検討ワーキンググループ報告書～「(仮称) 準個人情報」及び 「(仮称) 個人特定性低減データ」に関する技術的観点からの考察について～, 技術検討ワーキンググループ, 2014年5月, 16-20頁.

② 얼굴인식데이터, 유전자정보, 음성의 특성, 지문 등 개인의 생체적・신체적 특성에 관한 정보로서 보편성이 있는 것 ③ 이동이력, 구매이력 등의 특징적인 행동의 이력

출처 : 日本弁護士連合会, パーソナルデータの基本的枠組みについての意見書, 2014年11月20日, 7頁.

이에 의하면, 특히 개인의 신체적 특성에 관한 것(대체로 생체정보에 해당하는 것으로 판단됨)에는 지문, 성문(聲紋), 정맥 패턴, 홍채, DNA, 얼굴인식 데이터, 손바닥 모양, 생체인증에서 사용되는 데이터(생체인증방식 고유의 방법으로 수치화한 데이터도 포함하고, 얼굴화상인식 데이터도 포함), 보행 패턴, 필적, 성별, 피부색, 인종, 가족구성, 혈액형, 머리카락색깔, 혈압, 맥박, 신장, 체중 등이 있다.[148] 다만, 이러한 "준개인정보"를 생체정보와 '동일한' 혹은 '동질적인' 개념이라고 보기에는 무리가 있었을 것이다. 이러한 논의는 법률의 개정으로 해소된 것으로 보인다.

2. 개인정보의 보호

이 법은 특정 개인을 식별할 수 없도록 개인정보를 가공한 것을 "익명가공정보"로 정의한다(제2조제9항).

< "익명가공정보"의 개념 >

⑨ 이 법률에서 "익명가공정보"라 함은 다음 각 호에 열거된 개인정보의 구분에 따라 당해 각 호에서 정하는 조치를 취하여 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻어지는 개인에 관한 정보로서, 당해 개인정보를

148) パーソナルデータに関する検討会, 技術検討ワーキンググループ報告書～「(仮称)準個人情報」及び「(仮称) 個人特定性低減データ」に関する技術的観点からの考察について～, 技術検討ワーキンググループ, 2014年5月, 17頁.

복원할 수 없도록 한 것을 말한다.
1. 제1항제1호에 해당하는 개인정보 – 당해 개인정보에 포함되는 기술 등의 일부를 삭제하는 것(당해 일부의 기술 등을 복원할 수 있는 규칙성을 갖지 않는 방법에 의해 다른 기술 등으로 치환하는 것을 포함한다)
2. 제1항제2호에 해당하는 개인정보 – 당해 개인정보에 포함되는 개인식별부호의 전부를 삭제하는 것(당해 개인식별부호를 복원할 수 있는 규칙성을 갖지 않는 방법에 의해 다른 기술 등으로 치환하는 것을 포함한다)

출처 : 일본 수상관저, 개정법 대비표, 11면, (번역-이인호 중앙대교수) 참조. http://www.kantei.go.jp/jp/singi/it2/pd/pdf/taihihyo.pdf (2016.10.20.최종접속)

그리하여 개인정보취급사업자의 의무로서 이용목적의 특정(제15조), 이용목적에 의한 제한(제16조), 적정한 취득(제17조), 취득 시 이용목적의 통지(제18조), 데이터내용의 정확성 확보(제19조), 안전관리조치(제20조), 종업원・수탁자에 대한 감독(제21,22조), 제3자제공의 제한(제23조), 외국에 있는 제3자제공 제한(제24조), 제3자제공에 관한 기록의 작성(제25조), 제3자제공을 받는 시점의 확인(제26조), 보유개인데이터에 관한 사항의 공표(제27조) 등에 관한 규정을 두고 있다.

또한, 정보주체의 권리를 개인정보취급사업자의 의무와 같은 부분에서 규정을 하고 있는데, 정보개시청구(제28조), 정정청구(제29조), 이용정지(제30조)가 그것이다.

한편, 법률 개정으로 새로 신설된 “익명가공정보취급사업자” 등의 의무에 관한 규정으로, 익명가공정보의 작성 등(제36조), 익명가공정보의 제공(제37조), 식별행위의 금지(제38조), 안전관리조치(제39조) 등이 추가되었다.

마지막으로 민간단체에 의한 개인정보보호에 관한 규정으로서, 개인정보취급사업자 등이 인정을 받은 “인정개인정보보호단체”는 대상 사업자의 개인정보 등의 적정한 취급을 확보하기 ㄱ하여 개인정보와 관련된 이용목적의 특정, 안전관리를 위한 조치, 개시 등의 청구 등에

응하는 절차 및 그 밖의 사항에 관하여 이 법률의 취지에 입각한 지침, 즉 “개인정보보호지침”을 작성하고 공표하도록 노력하여야 한다(제53조).

제 6 절 시사점

생체정보의 활용은 거의 모든 문명국가에서 일상적으로 이루어지고 있는 현상이 되었다. 특히 개인을 식별하기 위한 목적으로 “지문”을 활용해 왔다는 점에서는 어느 정도 공통된다. 다만, 그것을 개인정보와는 다른 개념으로 인정하고 그것을 독립적인 규범으로 체계화한 국가는 아직 찾아보기 힘들다. 그나마 생체정보로서 “사진”이나 “지문”을 다양한 법령 등에 규정되어 있으며 이를 직접적으로 언급할 수 있게 된 계기는 역시 9.11테러에 의한 것이었고, 개인의 신분을 확인하기 위한 공적 활용에서의 규범화가 두드러진 현상이라 할 수 있다. 국가마다 생체정보에 관한 관심을 두는 분야가 다른데 특히 독일의 경우 공적 분야에서, 미국의 경우 사적 분야에 더 관심을 두는 것 같다. 그럼에도 아직은 어느 나라도 생체정보의 개념이나 유형, 보호 등에 관하여 법 제도 등을 완결적인 형태로 갖추고 있기 못하고 있는 것으로 결론내릴 수 있다.[149] 생체정보의 개념을 생체인식정보로 인정하고 있는 미국의 경우는 주목할 만하지만, 미국 또한 연방차원에서는 생체정보를 개인정보의 체계 속에 포함시켜서 이해하며, 독자적인 규범적 지위를 가진 개념으로 인정하고 있는 것으로 보이지 않는다.

다만, 주목할 만한 것은 유럽의 통합개인정보보호규정(GDPR)이 기존의 개인정보 외에 유전정보라든가 생체정보를 명시함으로써 앞으로 유럽을 비롯한 다양한 국가에서도 개인정보와 생체정보의 원칙적 차

149) 김일환, 앞의 “생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안 연구”, 83면.

이에 입각한 법령을 제정하고 그에 따른 보호조치를 정비해 나갈 것으로 예상할 수 있다.

이 규정은 종전의 지침이 가졌던 한계로서 개인정보보호에 관한 일관성 부족, 규범적 불확실성, 온라인 개인정보보호에 대한 리스크를 해결하고, 각 회원국마다 보호수준이 달랐던 점을 인식함으로써 개인정보의 국외이동 및 제공에 관한 보호수준을 원칙적으로 정하였다는 점에 의의가 있다. 이러한 원칙과 기준은 우리 법제에서 생체정보의 개념이나 범위, 활용 및 보호의 수준 등을 정할 때에 참고할 수 있을 것이다.

또한 최근 일본「개인정보보호에 관한 법률」의 개정에 따른 개인정보 개념의 분화와 정보보호에 대한 동의요건의 강화, 새로 신설된 개인정보보호위원회의 설치 등에 관한 규정 등은 아직은 우리 법제와 비교하기에는 미치지 못하는 면이 있지만, 보수적인 일본에서의 변화 추구를 엿볼 수 있는 부분이기도 하다.

제 5 장 결론: 생체정보 관련 법제의 정비 방향

제 1 절 생체정보의 규율 체계

Ⅰ. 규율 필요성

생체정보라는 것은 사실 새롭게 등장한 개념도 아니며 현행의 법제로 해결될 수 없는 문제들이 발생하여 큰 사회문제가 대두된 상황도 아니다. 이미 오래 전부터 자연인이 자신의 존재와 권한을 알리기 위한 수단으로 "지문"을 사용해 왔고, 대부분 공공분야에서 일정하게 통제된 환경 하에 사용되던 것이, 점차 민간영역에서 급속도로 전자적이고 개방적으로 활용되면서 점차 다양한 방면과의 접촉이 발생하고 결과가 다변화하여 그에 대한 규율이 보다 세밀하고 체계적으로 이루어져야 할 필요성이 보다 크게 증가한 것이다.[150]

이러한 현실적인 "필요성"에 기초하여 우리 법제는 생체정보에 대한 규율을 구체화하고자 다수의 법령과 정부 문서에서 생체정보의 개념과 유형을 정하는 시도를 하였다. 즉,「전자금융거래법」상의 "생체정보",「전자통신망법」시행령 상의 "바이오정보",「전자서명법」상의 "생체특성에 관한 정보"는 생체정보라는 용어를 법령이 직접적으로 포섭한 예이며, 그 밖에 행정자치부에서 마련 중인「바이오정보 보호 가이드라인(안)」(2015.12)은 물론 일찍이 정보통신부에서 수립한 바 있는「생체정보 보호 가이드라인」(2005.12)이나 국회사무처 법제실에서 작성된 보고서「생체인식정보 보호에 관한 연구」(2005) 등에서도 생체정보의 개념을 명시적으로 사용하여 왔다.

150) 이러한 이유로 개인정보가 이미 "식별성"을 전제로 하기 때문에 개인정보의 개념 속에 생체정보를 포함시켜 현재의 법제를 유지하는 것도 무방할 수 있다는 의견이 있을 수 있지만, 이미 개별법령에서 개인정보와 생체정보 간의 개념 분화(분리)가 시작되었기 때문에 개인정보의 하나로 다시 통합하는 것도 어렵게 되었다.

그러나 아직 우리 법제는 “생체정보법”이라는 명칭을 가진 법률이 존재하지 않고, 그렇다고 개인정보 처리활동의 전반에 적용될 수 있는 일반법도 없으며[151] 생체정보에 관한 개별 규정을 가지고 있는 일부 법령들도 그것이 일정한 규범적 체계를 형성하고 생체정보의 보호에 필요한 고유의 보호조치 체계를 구축하기 위한 의도에 기초한 것이라기보다는 동일한 사건이나 유사한 이슈에 대하여 그때그때의 필요에 따라 동일 또는 유사한 처리원칙으로 중복 적용하거나 합리적인 이유없이 처리기준을 다르게 규정하여 혼선을 빚을 가능성이 높다.

또한, 관계 부처들이 마련한 가이드라인들도 법적 강제력 내지 구속력을 가지지 않고 공공 및 민간영역의 사업자가 자율적으로 규제하기 위한 지침 내지 기준으로서의 역할을 한정적으로 수행할 뿐이고 기존 「개인정보보호법」 상의 개인정보의 수집・이용・제공・파기 등의 규정을 옮겨놓은 것과 별반 다르지 않게 규정되어 있어[152] 생체정보만의 특수성을 제대로 반영하지 못하고 있다는 비판에 직면한다.[153]

따라서 각 법령에서 존재하는 용어를 통일하는 것은 물론이고 무엇보다도 생체정보 내지 바이오정보와 개인정보 및 민감정보와의 관계를 명확히 하면서 생체정보의 특성이 반영된 고유의 보호조치 체계가 구축될 필요가 있다. 이러한 연구는 법령 정비라는 실무적인 관점에서 뿐만 아니라 이론적인 관점에서도 검토가 병행되어야 할 것이다.

---

151) 박정훈, 앞의 글, 405-406면 각주10)에 의하면, 우리나라는 2005년 생체정보에 관한 권장지침으로서 (구)정보통신부가 제정한 「생체정보보호 가이드라인」을 확정하였으나, 곧바로 이 시스템을 초보적인 단계로 이용하고 있는 중・대기업과 공공기관의 반대로 유명무실하게 되었으며, 그 후에는 생체정보를 포함한 개인정보보호나 프라이버시에 관하여 특별한 대응조치를 취하고 있지 않다.

152) 심우민, 앞의 글, 3-4면.

153) 예를 들어 유일한 식별자로서의 이용금지, 본인확인 수단으로만 이용제한, 생체정보를 근거로 한 차별금지, 프라이버시 영향평가 등에 관한 규정이 미비하며, 공공기관의 무분별한 생체정보 오남용의 위험성이 점차 증가하는 상황에서 공공기관에 대해서는 적용하기 어렵다는 점 등이 가이드라인의 한계점으로 평가된다. 박정훈・김행문, 앞의 글, 89-90면; 오길영, 앞의 글, 236-237면.

그리하여 생체정보의 통일적이고 체계적인 법제 정비방안을 위하여 어떠한 개선방안이 논의가 될 수 있는지 살펴본다.

Ⅱ. 규범 제정의 필요성

첫 번째로 검토할 것은 생체정보의 규율을 과연 "법령"의 형식으로 정비할 것인지, 아니면 현행 행정자치부나 정보통신부가 노력하는 바와 같이 "가이드라인" 등의 형식으로 정비할 것인지에 관한 것이다.

가이드라인은 기술도입기나 기술확산기와 같이 아직 법을 제·개정하기에는 이르지만 규율이 필요한 영역에서, 행위자에게 모범적인 구체적 행위지침을 제시하여 그에 따른 행위를 유도하지만 그 행위를 법적으로 강제하지는 않는다는 점에서 일종의 연성법(soft law)이라 할 수 있다. 이러한 가이드라인은 시간이 흐름에 따라 실정법(경성법; hard law)으로 발전하여 그 분야에서 중요한 규범으로 작용할 개연성이 높다.[154] 때문에 잠정적으로는 기술발전기인 현 상황에서는 가이드라인과 같은 연성법을 구체적인 행동(보호)지침으로 삼고 추후 실정법령으로 전환하는 것이 타당하다는 의견이 있다.[155] 그러나 이러한 연성법으로 해결하자는 견해는 생체정보의 유출이나 도용 등에 관하여 현실적인 대응으로서는 부족하다고 판단되며 적어도 생체정보의 보호와 관련하여서는 법적 구속력이 있는 법령에 근거를 둘 필요가 있다.

---

154) 이러한 연성법의 증가추세를 부정적으로 평가할 것이 아니라 시대적 필요의 산물로 긍정적으로 인식할 필요가 있다. Pierre-Marrie Dupuy, "Soft Law and the International Law of the Environment", *Michigan Journal of International Law*, 12, 1991, p.422.

155) 이러한 의견에 따르면 정보통신부가 지난 2005년 당시 기술도입기에 있었던 RFID기술이 개인정보보호의 측면에서 많은 문제가 있어 이에 대한 구체적 행위지침을 제시하기 위하여 'RFID 프라이버시보호 가이드라인'을 채택한 바 있는데, 입법형식의 측면에서 RFID 기술의 도입확산기인 2005년에 실정법형식보다 가이드라인이라는 연성법 형식을 채택한 것은 바람직하다고 본다. 이원태 외, 「사이버세상의 새로운 규범체계 정립방안 연구」, 방송통신정책연구 14-진흥-009, 2014, 44면.

Ⅲ. 실정법적 체계

두 번째로 검토할 것은 실정법적 체계의 관점에서 생체정보에 관한 사항을 ①「개인정보보호법」내에 개인정보에 대한 특례로서 민감정보나 고유식별정보와 같은 '제3의 형태'로서 규정을 따로 둘 것인지,[156] 아니면 ② 현행 법령의 체제와 같이 각 개별 법규에서 필요에 따라 생체정보에 관한 사항(단, 용어와 보호조치에 관하여는 전반적으로 통일할 필요가 있다)을 개별적으로 둘 것인지를 결정하는 것이다. 아니면, 더 나아가 ③ 생체정보의 활용 및 보호에 관한 자기완결적 법률로서 소위 "생체정보보호법" 등과 같은 개별법을 제정하는 방안[157]도 생각할 수 있다.[158]

어떠한 방안에 대해서도 찬반의견은 있을 수 있으며 최종적인 결론은 다양한 전문가의 의견을 반영하여 입법자가 결정할 문제이다. 다만, 본 연구에서는 생체정보가 특수한 성격을 가지고는 있지만 개인정보로부터 동떨어진 별개의 정보가 아니기 때문에, 법체계적 통일성과 안전성을 기한다는 측면에서, 개인정보 전반에 통용되는 공통적인 기준과 원칙은 가능한 한「개인정보보호법」에서 규정하고, 개별법은 그 분야만의 특수성이 충분히 드러나도록 보충성의 원칙에 따라 규정할 필요가 있음을 확인한다.[159] 이러한 다양한 의견에 기초하여 생체

156) 오길영, 앞의 글, 241면.

157) 조규범, 앞의 "생체정보 보호를 위한 입법론적 고찰", 198면은 개인정보보호법에 대한 특별법으로서 "생체정보보호법"의 제정을 통하여 생체정보의 수집 및 처리에 관한 법적 근거를 마련해야 한다는 입장을 취하고 있다.

158) 연광석, 앞의 보고서, 62면은 생체인식정보도 개인정보의 일종으로서 다만 일신전속성 및 인격과의 불가분성이라는 특성이 있을 뿐이라는 점을 고려하면 통일된 데이터보호법의 제정을 기다려 그 안에 별도의 장을 마련하는 정도가 바람직하다고 판단한다.

159) 이창범, "비교법적 관점에서 본 개인정보 보호법의 문제점과 개정방향: 한국·EU·일본을 중심으로",「Internet and Information Security」, 제3권제2호, 2012. 2, 76면.

정보에 대한 근거 규범의 정비방안에 대한 틀을 구상하여 보면 다음과 같다.

1. 특별법으로 제정하는 경우

생체정보에 관하여 자기완결적 법률을 제정하는 경우이다. 이에 관하여는 그 필요성과 한계에 관하여 의견이 매우 다양할 것이며, 그러한 법률 속에 담아야 하는 규율의 내용과 수준 또한 기존 법체계, 특히 개인정보보호법과의 관계 등을 통하여 정해져야 할 것이기에 아직은 그 틀을 설계하는 것이 쉽지 않다. 이러한 개별법의 제정 필요성과 구체적인 입법 실천에 관하여는 "의료정보" 내지 "건강정보"의 보호와 관련하여 보다 적극적인 논의가 추진 중인데, 특히 보건복지부에서 2005년부터 법률안 상정을 추진한 것으로부터 국회에 제출된 '건강정보보호법(안)'(2006, 윤호중 의원), '건강정보보호법(안)'(2008, 백원우 의원), '개인건강정보보호법(안)'(2008, 전현희 의원 및 유일호 의원), '개인의료정보보호법(안)'(2012, 신경림 의원) 등의 경우를 참고할 수 있을 것이다.[160]

무엇보다도 생체정보의 활용과 보호에 관하여 개별법으로 제정하고자 하는 경우 그 기반은 현행 가이드라인 또는 가이드라인(안)이 될 수 있다. 정보통신부 및 KISA에서 작성한 2007년의 '바이오 정보보호 가이드라인'과 행정자치부가 2015년 현재 수립을 추진하고 있는 '바이오정보 보호 가이드라인(안)'이 그것이다. 두 가이드라인의 내용은 하나의 규범이라고 하기에는 부족한 면이 있고 규범적 효력에 관하여는 앞에서 언급한 바와 같이 한계가 있지만, 추후 입법을 추진하는 데에 있어서는 중요한 참고자료가 될 것이기에 언급을 하지 않을 수 없다.

두 가이드라인의 체계를 비교하여 보면 다음과 같다. 다만, 2015년의 바이오정보보호가이드라인(안)은 아직 그 체계와 내용을 정하고 있

160) 이한주, 앞의 글, 196면. 주요 법안의 내용에 관하여는 같은 글, 196-199면 참조.

는 과정 중에 있기 때문에 2007년의 완성된 가이드라인과 비교하는 것은 무리가 있기에 이를 참작할 필요가 있다.

< 2007년 및 2015년 바이오 정보보호 가이드라인(안) 비교 >

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	**바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)**
제 1 장 총 칙	
제 1 조(목적) 이 가이드라인은 바이오인식시스템을 운영하는 자가 개인식별에 이용하는 바이오정보를 보호하기 위하여 준수하여야 할 사항을 정함으로써 바이오정보의 안전한 이용환경을 조성함을 목적으로 한다.	제 1 조(목적) 이 가이드라인은 바이오정보의 처리 및 보호에 관한 사항을 정함으로써 바이오정보의 안전한 이용환경을 조성함을 목적으로 한다.
제 2 조(정의) 이 가이드라인에서 사용하는 용어의 정의는 다음과 같다. 1. “바이오정보”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. 2. “바이오인식시스템”이라 함은 바이오정보를 이용하여 개인을 식별하는 정보시스템을 말한다. 3. “운영자”라 함은 바이오인식시스템을 운영하는 자를 말한다. 학술연구 또는 기술개발을 목적으로 바이오정보를 수집·이용하는 자도 운영자로 본다.	제 2 조(정의) 이 가이드라인에서 사용하는 용어의 뜻은 다음과 같다. 1. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특정에 관한 정보를 말한다. 2. “바이오인식정보”라 함은 식별 및 인증 등의 고유기능에 사용하기 위하여 개인의 바이오정보로부터 특징을 전자적으로 추출하였을 경우에 생성되는 특징정보와 그 추출 대상이 되는 원본정보(바이오정보)를 말한다. 다만, 추출 과정을 거치지 아니하여 특징정보가 존재하지 않는 원본정보는 제외한다.

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
4. “제공자”라 함은 운영자에게 자신의 바이오정보를 제공하는 개인을 말한다.	
제 3 조(적용범위 등) ① 이 가이드라인은 개인식별에 이용하는 바이오정보 및 바이오인식시스템에 대해 적용한다. ② 바이오정보 및 바이오인식시스템에 관해 법령의 규정이 있는 경우에는 그에 따른다.	
제 4 조(기본원칙) ① 운영자는 제공자의 동의를 얻고 바이오정보를 수집하여야 하며, 수집목적에 필요한 최소한의 정보를 수집하여야 한다. ② 운영자는 제공자에게 바이오정보의 수집목적을 명확히 알려야 하며, 그 목적범위 내에서 바이오정보를 이용하여야 한다. ③ 운영자는 이 가이드라인이 정하는 방법과 절차에 의하여 바이오정보를 수집・보관・이용 또는 파기하여야 한다. ④ 운영자는 제공자에게 바이오정보의 수집・이용・제3자제공 또는 파기와 관련하여 알 필요가 있는 정보를 제공하고, 제공자가 언제든지 이를 확인할 수 있도록 하여야 한다. ⑤ 운영자는 바이오정보의 도난・멸실・훼손・유출 등 각종 위험을	제 3 조(바이오정보 보호 원칙) ① 개인정보처리자는 바이오정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 바이오정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 바이오정보의 처리 목적에 필요한 범위에서 적합하게 바이오정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. ③ 개인정보처리자는 바이오정보의 처리 목적에 필요한 범위에서 바이오정보의 정확성, 완전성 및 고유성이 보장되도록 하여야 한다. ④ 개인정보처리자는 바이오정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 바이오정보를 안전하게 관리하여야 한다.

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
방지하기 위하여 적절한 보호조치를 취하여야 한다.	⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 바이오정보를 처리하여야 한다. ⑦ 개인정보처리자는 바이오정보의 익명처리가 가능한 정우에는 익명에 의하여 처리될 수 있도록 하여야 한다. ⑧ 개인정보처리자는 바이오정보를 인종, 민족, 건강상태 등을 식별하여 개인을 차별하려는 목적으로 이용하지 말아야 한다.
제2장 바이오정보의 수집・이용・파기	
제 5 조(수집) ① 운영자는 바이오정보를 수집하는 경우 제공자의 동의를 얻어야 한다. 다만, 법령에서 달리 규정하는 경우에는 그러하지 아니하다. ② 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각 호의 사항을 제공자에게 알리고, 이를 충분히 설명하여야 한다. 1. 수집하고자 하는 바이오정보의 종류 2. 바이오정보의 수집목적 및 보유기간 3. 바이오정보의 구체적인 처리방법 4. 바이오정보관리책임자의 성명・소속부서・직위・연락처 등의 인적사항 5. 바이오정보의 수집, 고지한 수집목적외 이용이나 제3자제공에	제 4 조(바이오정보의 수집・이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 바이오정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 다만, 건강정보, 유전정보 등 민감정보는「개인정보 보호법」제23조에 따른다. l. 정보주체의 동의를 받은 정우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
대한 동의의 철회 또는 바이오정보의 열람, 이용내역의 조회나 오류정정의 요구 등 제공자의 권리 및 그 행사방법 6. 그 밖에 제공자의 권익을 보호하기 위하여 필요한 사항 ③ 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에 법령에서 달리 규정하는 경우를 제외하고는 제공자가 만18세 미만인 자, 심신박약으로 인하여 한정치산 선고를 받은 자 또는 금치산 선고를 받은 자(이하 “만18세 미만인 자 등”이라 한다)인 때에는 제공자의 동의 외에 그의 법정대리인의 동의를 얻어야 한다. 이 경우 운영자는 제공자의 법정대리인에게 제2항의 규정에 의한 고지 및 설명을 하여야 한다. ④ 운영자는 제공자의 신체적·행동적 특징에 관한 원본정보에서 특징정보를 생성할 경우 수집 목적 상 필수불가결한 정보만을 생성하도록 하여야 한다.	에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다. ② 개인정보처리자는 제l항제l호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. l. 바이오정보의 수집·이용 목적 2. 수집하려는 바이오정보 3. 바이오정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 ③ 제l항에 따라 수집한 바이오정보에서 바이오인식정보를 이용할 경우에는 제2항 각 호의 사항을 알리고 바이오정보 처리에 대한

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
	동의와 별도로 정보주체의 동의를 받아야 한다. 다만, 다른 법령에서 바이오인식정보의 처리를 요구하거나 허용하는 경우에는 그러하지 아니하다. ④ 개인정보처리자는 바이오정보 또는 바이오인식정보만으로 중요정보에 대한 접근권한 부여 등의 인증 수단으로 사용하지 않아야 한다.
제 6 조(보관) 운영자는 수집한 원본정보를 보관하는 경우에는 성명·주민등록번호·주소 등 제공자를 알 수 있는 정보와 별도로 분리하여야 한다.	
제 7 조(이용) ① 운영자는 수집한 바이오정보를 제공자에게 고지한 수집목적 이외의 다른 목적으로 이용하고자 하는 경우에는 제공자의 동의를 얻어야 한다. ② 운영자가 제1항의 규정에 의하여 제공자의 동의를 얻고자 하는 경우에는 제공자에게 미리 다음 각 호의 사항을 알리고, 이를 충분히 설명하여야 한다. 1. 바이오정보의 새로운 이용목적 및 보유기간 2. 제5조제2항 제3호 내지 제6호에서 규정한 사항 ③ 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에 법령	제 6 조(바이오정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 바이오정보를 제4조제l항에 따른 범위를 초과하여 이용하거나 제6조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다. ② 제l항에도 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 경우

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
에서 달리 규정하는 경우를 제외하고는 제공자가 만18세 미만인 자 등인 때에는 제공자의 동의 외에 그의 법정대리인의 동의를 얻어야 한다. 이 경우 운영자는 제공자의 법정대리인에게 제2항의 규정에 의한 고지 및 설명을 하여야 한다.	로 한정한다. 1. 정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 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 4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 바이오정보를 제공하는 경우 5. 바이오정보를 수집하지 않으면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 6. 조약, 그 밖의 국제 협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 8. 법원의 재판업무 수행을 위하여 필요한 경우 9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
제 8 조(제3자 제공) ① 운영자는 보유하는 바이오정보를 제3자에게 제공하는 경우에는 제공자의 동의를 얻어야 한다. ② 운영자가 제1항의 규정에 의하여 제공자의 동의를 얻고자 하는 경우에는 제공자에게 미리 다음 각 호의 사항을 알리고, 이를 충분히 설명하여야 한다. 1. 바이오정보를 제공받는 제3자의 성명・주소・연락처(법인의 경우에는 명칭, 주된 사무소의 소재지, 연락처) 등의 인적사항 2. 제공하고자 하는 바이오정보의 종류 3. 바이오정보의 제공목적 및 보유기간 4. 제5조제2항 제3호 내지 제6호에서 규정한 사항 ③ 운영자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에 법령에서 달리 규정하는 경우를 제외하고는 제공자가 만18세 미만인 자 등인 때에는 제공자의 동의 외에 그의 법정대리인의 동의를 얻어야 한다. 이 경우 운영자는 제공자의 법정대리인에게 제2항의 규정에 의한 고지 및 설명을 하여야 한다.	제 5 조(바이오정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 바이오정보를 제3자에게 제공(공유를 포함한다. 이하 같다.)할 수 있다. l. 정보주체의 동의를 받은 경우 2. 제4조제1항제2호・제3호 및 제5호에 따라 바이오정보를 수집한 목적 범위에서 바이오정보를 제공하는 경우 ② 개인정보처리자는 제l항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다. l. 바이오정보를 제공받는 자 2. 바이오정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 바이오정보의 항목 4. 바이오정보를 제공받는 자의 개인정보 보유 및 이용 기간 5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
제 9 조(파기) ① 운영자 또는 바이오정보를 제공받은 제3자는 다음	제 7 조(바이오정보의 파기) ① 개인정보처리자는 보유기간의 경과, 바

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
각 호의 어느 하나에 해당하는 사유가 발생한 때에는 지체 없이 보유하는 제공자의 바이오정보를 복원할 수 없도록 파기하여야 한다. 1. 바이오정보의 수집·이용 목적 또는 제공받은 목적을 달성하거나 달성할 수 없게 된 경우. 단, 제공자의 별도 동의나 법률의 규정이 없는 한 원본정보는 특징정보 생성시 수집목적 등을 달성한 것으로 본다. 2. 바이오정보의 보유기간이 만료한 경우 3. 제공자 또는 법정대리인이 제10조의 규정에 의하여 바이오정보의 수집, 수집목적 외의 이용 또는 제3자 제공에 대한 동의를 철회한 경우 4. 기타 바이오정보의 보유가 더 이상 필요하지 않게 된 경우 ② 운영자는 제1항 제3호의 규정에 의하여 바이오정보를 파기한 경우에는 제공자에게 그 사실을 알려야 한다. 다만, 제공자가 만18세 미만인 자 등인 경우에는 제공자 외에 그의 법정대리인에게 그 사실을 알려야 한다.	이오정보의 처리 목적 달성 등 그 바이오정보가 불필요하게 되었을 때에는 지체없이 그 바이오정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다. ② 개인정보처리자가 제l항에 따라 바이오정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
제3장 제공자 등의 권리	
제10조(동의의 철회) ① 제공자는 언제든지 운영자 또는 바이오정보를 제공받은 제3자에 대하여 제5조제	제11조(바이오정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 바이오정보 또는 바이

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
1항 본문, 제7조제1항 또는 제8조제1항의 규정에 의한 동의를 철회할 수 있다. 다만, 법령에서 달리 규정하는 경우에는 그러하지 아니하다. ② 제공자가 만18세 미만인 자 등인 경우에는 제공자 외에 그의 법정대리인이 제1항 본문의 규정에 의한 동의철회를 할 수 있다.	오인식정보 처리의 정지를 요구할 수 있다. ② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 바이오정보 또는 바이오인식정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다. l. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 3. 공공기관이 바이오정보 또는 바이오인식정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우 4. 바이오정보 또는 바이오인식정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우 ③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
	였을 때에 는 정보주제에게 지체 없이 그 사유를 알려야 한다. ④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 바이오정보 또는 바이오인식정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.
제11조(열람・내역조회・오류정정 요구) ① 제공자는 언제든지 운영자 또는 바이오정보를 제공받은 제3자에게 자신의 바이오정보에 대한 열람을 요구하거나, 바이오정보를 이용한 내역 또는 제3자에게 제공한 내역의 조회를 요구할 수 있고, 오류가 있는 경우에는 이의 정정을 요구할 수 있다. ② 제공자가 만18세 미만인 자 등인 경우에는 제공자 외에 그의 법정대리인도 제1항의 권한을 행사할 수 있다. ③ 운영자 또는 바이오정보를 제공받은 제3자는 제공자 또는 그의 법정대리인으로부터 제1항 또는 제2항의 규정에 의한 열람・내역조회 또는 오류정정 요구를 받은 경우에는 지체없이 이에 응하여야 한다.	제 9 조(바이오정보의 열람) ① 정보주제는 개인정보처리자가 처리하는 자신의 바이오정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다. 다만, 바이오인식정보 중 특정정보에 한해서는 보유여부 확인으로 대체한다. ② 개인정보처리자는 제l항에 따른 열람을 요구받았을 때에는 10일 이내에 정보주체가 해당 바이오정보를 열람할 수 있도록 하여야 한다. ③ 개인정보처리자는 제2항에 따른 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다. ④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
	l. 법률에 따라 열람이 금지되거나 제한되는 경우 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 3. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우 4. 바이오정보의 보관기간이 경과하여 파기한 경우 ⑤ 개인정보처리자는 제1항에 따른 열람을 요구한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서 및 관계증명 자료를 제출받아 확인하여야 한다. 제10조(바이오정보의 정정·삭제) ① 제9조에 따라 자신의 바이오정보 또는 바이오인식정보를 열람하거나 존재 확인한 정보주체는 개인정보처리자에게 그 정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다. ② 개인정보처리자는 제l항에 따른 정보주체의 요구를 받았을 때에는 바이오정보 또는 바이오인식정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
	정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다. ③ 개인정보처리자가 제2항에 따라 바이오정보 또는 바이오인식정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다. ④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다. ⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.
제4장 바이오정보의 보호조치	
제12조(바이오정보관리책임자) ① 운영자는 제공자의 바이오정보를 보호하고 바이오정보와 관련한 제공자의 권리행사를 보장하기 위하여 바이오정보관리책임자를 지정하여야 한다. ② 바이오정보관리책임자는 다음 각 호의 업무를 수행한다. 1. 바이오정보의 수집·이용·제3자제공 기타 바이오정보 취급에 관한 업무의 총괄 2. 제13조 및 제14조의 규정에 의	

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
한 바이오정보 보호조치 이행 및 침해사고의 통지 3. 제공자로부터 제기되는 불만이나 의견의 처리 4. 기타 바이오정보 및 바이오인식시스템의 보호에 필요한 사항	
제13조(보호조치) ① 운영자는 바이오정보 및 바이오인식시스템을 보호하기 위하여 필요한 기술적·관리적 보호조치를 취하여야 하며, 보호조치의 구체적인 사항은 <별표>와 같다. ② 운영자는 제1항의 규정에 의한 보호조치를 취하기 위하여 필요한 경우 정보통신기반보호법 제17조의 규정에 의한 정보보호컨설팅전문업체 등 외부전문기관을 이용할 수 있다.	제 8 조(바이오정보의 안전성 확보 조치) ① 개인정보처리자는 바이오인식정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보 안전성 확보 조치 기준 고시에 따른 기술적·관리적 및 물리적 조치를 하여야 한다. 다만, 개인정보처리자는 바이오인식정보에 해당하지 않는 바이오정보의 경우에는 유출 시 위험도 등을 고려하여 암호화 적용여부를 정할 수 있다. ② 개인정보처리자는 바이오인식정보를 내·외부망을 통해 전송하거나 저장(내·외부망, 업무용 컴퓨터·모바일 기기 등)할 경우 원본정보와 특정정보를 모두 암호화하여야 한다. ③ 개인정보처리자는 제3항에 따른 바이오인식정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. ④ 개인정보처리자는 바이오인식정보를 저장할 경우 원본정보와 특정정보를 분리하여 저장·관리

바이오 정보보호 가이드라인 (정보통신부, 2007.9)	바이오 정보보호 가이드라인(안) (행정자치부, 2015.12)
	하여야 한다. ⑤ 개인정보처리자는 바이오인식정보를 저장할 경우 다른 개인정보와 분리하여서 저장·관리하여야 한다.
제14조(침해사고의 통지) ① 운영자는 바이오정보의 도난·멸실·훼손·유출 등 침해사고가 발생한 것을 안 때에는 지체없이 제공자에게 그 사실을 알려야 한다. ② 운영자는 제1항의 규정에 의한 통지를 하여야 하는 경우에 제공자가 만18세 미만인 자 등인 때에는 제공자 외에 그의 법정대리인에게 알려야 한다.	

2.「개인정보보호법」내에 규정을 두는 경우

생체정보의 개인정보로서의 성격을 확고히 하고 각종 개인정보와의 관계를 정하기 위하여 일반법적 성격을 가진 현행「개인정보보호법」내에 생체정보를 포함시키는 경우를 상정할 수 있다. 이는 본 연구에서 가장 적절한 방법으로 평가한 것으로서, 이하 세부적인 개선방안을 제안하는 경우에도 이 법에 포함시키는 것을 전제로 제안하는 것임을 언급하고자 한다. 다만, 생체정보를 이렇게「개인정보보호법」에 편입시키는 경우에도 어떠한 체계로 포함할 것인가에 대하여는 다음과 같이 세분하여 살펴볼 수 있다.

(1) 개인정보의 개념을 세분하여 정의규정에 두는 경우

생체정보를 개인정보의 하나의 유형으로 보아 개인정보 또는 그밖의 개념을 정의하는 규정에서 다른 구별개념과 함께 개별적으로 정의하는 방법을 생각할 수 있다. 유럽의 GDPR이나 일본의 개인정보의 보호에 관한 법률과 같은 방식을 예로 들 수 있다.

GDPR 유형	일본 개인정보보호법 유형
제*조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다 1. 개인정보 2. 유전자정보 3. 생체정보 :	제*조(정의) 이 법에서 '개인정보'라 함은 생존하는 개인에 관한 정보로서 다음 각 호의 어느 하나에 해당되는 정보를 말한다. 1. 생체정보 2. 위치정보 3. 신용정보 :

이러한 유형에 해당하는 대표적인 경우로서 19대 국회 2015년 강은희 의원 등 21인이 발의한 개인정보보호법 전부개정법률안(의안번호 1913932)을 들 수 있다.[161]

> 제 2 조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
> 1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보(해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 식별할 수 있는 것을 포함한다)를 말하며, 다음 각 목에서 정의된 정보를 포함한다.
> 가. 개인위치정보: 생략
> 나. 개인신용정보: 생략
> 다. 개인금융거래정보: 생략

161) http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T1B5B0W2V0C5K1X7Q4Z0V4X4U4X9O2 (2016.10.24. 최종접속)

라. 개인보건의료정보: 생략 마. 학생교육정보: 생략 **바. 바이오인식정보: 생략**

(2) 민감정보의 규정 속에 포함하여 규정하는 경우

생체정보의 성격은 규범적인 의미를 떠나 누구나 매우 민감한 정보라고 생각할 것이다. 그러나 규범적인 관점에서는 그것이 당연히 민감정보라고 말하기에 어려움이 있음은 앞에서 언급한 바와 같다. 때문에 「개인정보보호법」상 민감정보의 개념을 수정하여 생체정보를 민감정보의 개념 속에 포함시키고자 하는 경우로서 이 경우도 아래와 같이 두 가지의 방식 또는 그 두 가지를 모두 채택하는 방식을 생각할 수 있다. 즉, ① 법률 제23조의 본문인 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보" 속에 직접적으로 생체정보를 포함시키는 방법 또는 ② 법률 제23조에 따라 대통령령으로 정하는 정보로서 시행령 제18조에 규정되어 있는 유전정보와 범죄경력정보 외에 "개인을 식별하기 위한 생체정보"를 추가하는 방법이 그것이다.

< ① 법률을 개정하는 경우 >

개인정보보호법	개정시안
제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로	제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, **건강정보 및 생체정보**, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가

개인정보보호법	개정시안
서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 이하 생략	있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 이하 생략

< ② 시행령을 개정하는 경우 >

시행령	개정시안
제18조(민감정보의 범위) 법 제23조제1항 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	제18조(민감정보의 범위) —————— —————— —————— —————— —————— ——————— (생 략) ——————— —————— —————— —————— —————— —————— —————— —————— **3. 개인을 식별하기 위한 생체정보**

(3) 민감정보나 고유식별정보와 같이 처리제한 규정으로 두는 경우

「개인정보보호법」은 제3장(개인정보의 처리)에서 그것을 개인정보의 수집, 이용, 제공 등에 관한 사항(제1절)과 개인정보의 처리 제한에 관한

사항(제2절)로 구분하고 있다. 특히 개인정보의 처리 제한에 있어서는 일반적인 개인정보처리에 대한 처리제한의 특례로서 “민감정보”, “고유식별정보”, “주민등록번호”, “영상정보” 등에 관하여 규정하고 있다. 따라서 생체정보를 이러한 처리제한 특례의 체계 속에 편입하여 다음과 같이 생체정보의 처리제한에 관한 규정을 두는 방식을 생각해볼 수 있다.

현 행	개정시안
제23조(민감정보의 처리 제한) 제24조(고유식별정보의 처리 제한) 제24조의2(주민등록번호 처리의 제한) 제25조(영상정보처리기기의 설치·운영 제한) 제26조(업무위탁에 따른 개인정보의 처리 제한) 제27조(영업양도 등에 따른 개인정보의 이전 제한)	제23조(민감정보의 처리 제한) 제24조(고유식별정보의 처리 제한) 제24조의2(주민등록번호의 처리 제한) **제24조의3(생체정보의 처리 제한)** 제25조(영상정보처리기기의 설치·운영 제한) 제26조(업무위탁에 따른 개인정보의 처리 제한) 제27조(영업양도 등에 따른 개인정보의 이전 제한)

3. 각 개별법에서 규정을 두는 경우

「개인정보보호법」은 개인정보보호에 관하여 다른 법률에 특별한 규정이 있는 경우가 아닌 경우에 적용되는(제6조) 일반법으로서, 생체정보의 특별한 보호필요성에 기하여 “다른 법률”에 직접 그 근거를 두는 것이다. 이는 현행 법령에서 특별한 영역으로 볼 수 있는 「정보통신망법」, 「전자금융거래법」, 「전자서명법」 등에서 생체적 특성이나 바이오정보라는 용어로 적용되고 있는 체계를 그대로 유지하고는 것이다.

다만, 현행의 상태를 유지하고자 하는 안이기는 하지만, 그 용어가 매우 상이하기 때문에 개념과 의미를 통일하고 보호체계를 보다 강화하여 개별 법률에서 규정을 두는 것은 어느 경우에나 필요하다.

제 2 절 생체원본정보와 생체인식정보의 구분

생체정보는 일반적으로 “생체원본정보”와 그 원본정보로부터 특징값을 추출해낸 “생체인식정보”로 구분된다. 생체원본정보는 우리가 생각하는 생체정보의 원형(原形)을 가진 것으로서 생체원본정보가 도난・위조되는 경우 회복이 불가능하며 더 이상 그 식별자를 사용할 수 없다는 점은 앞에서 언급한 바와 같다. 따라서 일반적으로 생체정보라 할 때에는 이러한 생체원본정보가 아닌 생체인식정보로 의미를 파악하여야 할 뿐 아니라 실제로 수집하고 활용하는 생체정보 또한 생체인식정보여야 한다는 점도 앞에서 지적하였다.

일상적으로 활용하고 있는 대부분의 분야, 즉 금융이나 정보통신분야에서 이용되는 생체정보는 생체인식정보로 저장하고 활용하는 것으로 충분하며 생체원본정보는 필요로 할 이유가 없다. 생체원본정보가 필요할 수 있는 경우는 생체인식기술 또는 생체인증기술의 연구・개발 단계에서 기술적 구성이나 검증을 위하여 필요하거나 또는 생체인식정보를 분실・도난・유출・훼손당하거나 생체인식시스템에 장애가 발생하여 생체인식정보를 재발급하는 등의 일정한 문제가 발생한 경우 등 매우 제한적인 정도로만 인정될 수 있는 것이다.

그러나 우리나라에서는 각종 법령에서 생체원본정보와 생체인식정보를 구분하지 않고 사용하고 있는데, 예컨대 「정보통신망법」 시행령에서 정하고 있는 바이오정보가 생체원본정보인지 생체인식정보인지 어떠한 유권해석 없이 수집・이용되고 관리되고 있다(여기서 바이오정보는 보안조치로서 암호화 저장을 하여야 한다고 하고 있으므로 법문 그 자체만으로 보면 원본정보를 의미하는 것이라 해석할 수 있다). 업계에서 원본정보와 인식정보의 개념을 구별하는지, 원본정보를 수집하여 암호화 저장을 하고 있는지는 현황 파악이 된 바도 없다.

< 정부부처에서 인식하고 있는 생체정보의 개념 >

개인정보의 안전성 확보조치 기준 (행자부 고시, 2016)	개인정보의 기술적 · 관리적 보호조치 기준 (방통위 고시, 2015)
제 2 조(정의) 16. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.	제 2 조(정의) 8. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

생체정보가 모바일 등에서 본격적으로 그리고 보편적으로 활용되기 시작한 현 상황에서 각종의 단말기들이 생체정보를 저장할 수 있는 획기적인 기능을 갖추었는데, 그 생체정보라는 것이 생체원본정보인지 생체인식정보인지 사용자는 아직 구별하지 않는 상황이다. 그런데 생체원본정보를 그대로 저장한 채로 생활하는 경우, 이들 단말기들은 대부분 융합 네트워킹이 가능한 장비들이기 때문에[162] 그 도난이나 유출 등의 부작용은 매우 큰 사회적 파장을 야기할 수 있는 것이다.

그리하여 앞으로 법령에서는 생체원본정보와 생체인식정보의 개념을 구분하고 그 처리기준도 달리 정하여야 할 필요가 있으며, 이러한 의미에서 행정자치부에서 마련하고 있는 바이오정보보호 가이드라인(안)(2015)이나 강은희의원 의원발의(안)의 제안한 정의규정은 참고할 만하다.

< 생체(인식)정보의 정의규정(안) 비교 >

바이오 정보보호 가이드라인(안) (2015.12)	개인정보보호법 전부개정 의원발의(안) (2015.2)
제 2 조(정의) 이 가이드라인에서 사용하는 용어의 뜻은 다음과 같다.	제 2 조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

162) 오길영, 앞의 글, 244면.

바이오 정보보호 가이드라인(안) (2015.12)	개인정보보호법 전부개정 의원발의(안) (2015.2)
1. “**바이오정보**”라 함은 지문, 얼굴, 홍채, 정액, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특정에 관한 정보를 말한다. 2. “**바이오인식정보**”라 함은 식별 및 인증 등의 고유기능에 사용하기 위하여 개인의 바이오정보로부터 특징을 전자적으로 추출하였을 경우에 생성되는 특징정보와 그 추출 대상이 되는 원본정보(바이오정보)를 말한다. 다만, 추출 과정을 거치지 아니하여 특징정보가 존재하지 않는 원본정보는 제외한다.	1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 식별할 수 있는 정보(해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 식별할 수 있는 것을 포함한다)를 말하며, 다음 각 목에서 정의된 정보를 포함한다. 가. ~ 마. (생 략) 바. **바이오인식정보:** 얼굴·지문·홍채·정맥·동작·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보(해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 식별할 수 있는 것을 포함한다)를 말하며, 가공되지 않은 원본정보와 그로부터 추출되어 생성된 특징정보를 포함한다. 다만, 추출 과정을 거치지 아니하여 특징정보가 존재하지 않는 원본정보는 제외한다.

또한 양자의 개념을 구분하는 경우에도 혼동을 배제하기 위하여 “생체정보를 저장하거나 송수신할 때에는 그 원본정보와 이름·주민번호 등의 식별자를 반드시 구분하도록 하고, 이를 암호화(비식별화)하여 저장하여야 한다”는 내용도 명문으로 두어야 할 것이다.[163]

163) 이창범, 앞의 “생체정보의 분야별 활용현황 – 금융, 의료, 수사 분야”, 116면은 구분저장은 권장하나 필수적 요구사항은 아닌 것으로 보고 있다.

제 3 절 생체정보 수집 · 이용 및 처리에 관한 보호장치의 확충

생체정보는 그 사람만이 가진 불법의 특징을 나타내기 때문에 다수의 식별자에는 그 사람의 건상상태는 물론 가족의 유전적 병력이나 인종적 특성까지 알 수 있는 정보가 포함되어 있는 경우가 많다. 때문에 그것이 생체원본정보로서 유출되는 경우 다시는 해당 정보를 활용한 본인확인서비스를 이용할 수 없게 되는 위험이 따른다. 따라서 생체정보는 생체인식정보로 파악할 필요가 있으며, 그에 대한 보호도 일반적인 개인정보와는 다른, 더 강화된 보호장치가 필요하다. 이에 대하여는 「개인정보보호법」의 체계에 따라 생체정보를 "수집 · 이용 · 제공"하는 경우와, 생체정보를 "처리"하는 경우로 나누어 살펴보기로 한다.

Ⅰ. "수집 · 이용 · 제공"에 있어서의 보호장치

1. 목적 제한

「개인정보보호법」에 따르면 개인정보의 수집 · 이용은 "목적"(제15조제1항)과 "동의"(제15조제2항)에 결부된 조건에 따른다. 따라서 개인정보처리자는 수집 목적에 필요한 최소한의 개인정보를 수집하여야 하고 동의를 받지 않는 한 목적의 범위를 벗어난 수집이나 제3자제공은 원칙적으로 금지된다(제18조). 그리고 개인정보는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 파기되어야 한다(제21조).

생체정보의 수집과 이용 또한 일반적인 개인정보의 경우와 마찬가지로 "목적"이나 "동의"에 엄격하게 결부될 필요가 있다. 우선, "목적"과 관련하여, 앞에서 언급한 바와 같이 생체원본정보와 생체인식정보를 구별하는 전제 하에, 생체원본정보는 원칙적으로 수집 및 이용이

불가능한 것으로 하고, 통계작성 및 학술연구의 목적이나 생체정보의 분실로 인한 재발급 등 기술적으로 생체원본정보의 수집이 불가피한 경우에 한하여 생체인식정보를 확보함과 동시에 원본정보는 즉시 삭제하도록 정하는 것이 필요하다. 생체인식정보는 특징값을 바꾸어 얼마든지 새로 생성하여 활용할 수 있지만, 생체원본정보는 분실·도난·유출되는 경우 더 이상 생체인식기술(본인확인수단)로 활용할 수 없게 되는 상황이 발생하기 때문이다.

같은 취지에서 생체정보의 상업적인 이용 또한 정보주체의 동의를 불문하고 원칙적으로 금지될 필요가 있다. 생체정보는 지문, 홍채, 정맥, 얼굴윤곽, 유전자 등과 같이 "살아있는" 사람의 신체(생체)를 통해서 얻어지는 정보이기 때문에, 연구 또는 기술개발의 목적이든 본인확인의 목적이든 생체정보를 "거래"의 대상으로 허용할 경우 어떠한 형태로든 윤리적 문제를 낳을 수 있는 소지가 있기 때문이다.[164]

다만, 생체원본정보의 수집과 활용이 예외적으로 허용되어야 하는 경우가 있을 수 있다. 예컨대 생체인식정보의 도난이나 위조 등을 이유로 재발급 등에 필요한 경우 또는 통계작성이나 학술연구 등의 제한적 목적을 위하여 불가피하게 허용되어야 하는 경우가 그것이다. 현행「개인정보보호법」또한 수집목적의 범위를 초과하는 경우에 대하여 예정하고 있는데, 원칙적으로 수집목적의 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공할 수 없으나(제1항), 일정한 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다(제2항)고 규정하고 있다. 그러한 예외로 9가지의 경우를 열거하고 있는데, 이를 생체정보의 경우에도 그대로 적용할 수 있는지는 개별적으로 따져볼 필요가 있다.

164) 이창범, 앞의 "생체정보의 분야별 활용현황 - 금융, 의료, 수사 분야", 116면.

< 개인정보의 목적 외 이용・제공의 예외와 생체정보에의 적용가능성 >

개인정보의 목적 외 이용・제공	생체정보에의 적용가능성	
	원본정보	인식정보
1. 정보주체로부터 별도의 동의를 받은 경우	가능	가능
2. 다른 법률에 특별한 규정이 있는 경우	가능	가능
3. 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	불가능	가능
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우	가능	가능
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의・의결을 거친 경우	불가능	가능
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우	불가능	가능
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우	불가능	가능
8. 법원의 재판업무 수행을 위하여 필요한 경우	불가능	가능
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우	불가능	가능

생체원본정보의 경우 그 고유한(unique) 성격으로 인하여 현행 예외사유보다 제한되어야 하며, 정보주체의 명시적인 동의가 없는 한 원칙적으로 목적 외 이용이나 제3자제공이 금지되어야 한다. 다만, 「개인정보보호법」이 "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우"(제4호) 예외사유로 인정하고 있는 데에 대하여, 이러한 통계작성이나 학술연구 목적의 개인정보에 대하여 까지 식별성을 제거하도록 하는 것은 과도한 개인정보보호라고 보는 견해도 있다.[165] 통계작성이나 의료, 학문적 연구・개발을 위한 생체원본정보의 수집・활용을 일반적으로 금지하는 경우 과학기술발전을 저해할 수 있기 때문에, 질병치료나 연구・개발을 위한 목적 외에는 어떤 경우에도 "법률에 의하지 아니하고는" 원칙적으로 처리될 수 없어야 한다는 것이다.

2. 동의 방식

개인정보의 수집이나 제3자제공을 위하여는 정보주체의 동의가 필요한데, 동의를 받기 위해 개인정보처리자가 정보주체에게 미리 알려야 하는 사항으로는 "① 개인정보를 제공받는 자, ② 개인정보를 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목, ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용"이 있다(제15조 및 제17조). 또한 정보주체 이외로부터 수집한 개인정보를 처리하려는 때에는 그 수집출처나 처리 목적 등에 대하여 고지하여야 한다(제20조). 개인정보처리자가 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알려야 하며, 정보주체와의 계약 체결

165) 이창범, 앞의 "비교법적 관점에서 본 개인정보 보호법의 문제점과 개정방향: 한국・EU・일본을 중심으로", 90-91면.

등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다(제22조).

이러한 "동의를 받는 방법"과 관련하여 생체정보의 경우에는 다음과 같은 몇 가지의 사항을 추가하여 명문화하여야 할 필요가 있다. 우선, ① 동의의 방식과 관련하여 "명확하게 인지할 수 있도록 알리는" 방식으로서 반드시 "**서면**"에 의하도록 한다. 그리고 ② 동의의 내용과 관련하여 생체정보가 유일한 수집정보가 아니며 대체수단으로서의 정보가 고지됨으로서 제공할 수 있는 정보에 대한 "**선택가능성**"이 포함되어야 한다. 마지막으로 ③ 정보주체의 동의 없이는 원칙적으로 생체정보는 처리될 수 없다는 "**처리금지**" 원칙이 포함되도록 하는 것이다.

< 생체정보에 있어서의 동의를 받는 방법에 대한 제안 >

	현행(개인정보보호법)	개정시안
방식	개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.	(생 략) 각각 **서면으로** 동의를 받아야 한다.
내용	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	**① 생체정보의 수집・이용 목적** **② 수집하려는 생체정보의 식별자 및 수집 방식** **③ 생체정보의 보유 및 이용 기간** **④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 대체수단의 내용**

	현행(개인정보보호법)	개정시안
한계	개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1항제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.	**생체정보처리자는 생체정보의 처리에 대하여 제**조에 따른 정보주체의 동의없이는 생체정보를 처리할 수 없다.**

Ⅱ. "처리"에 있어서의 보호장치

「개인정보보호법」 제23조는 "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"를 "민감정보"라 칭하고, 정보주체의 별도 동의나 법령에 의하지 않고는 원칙적으로 그 처리를 금지하고 있다. 이를 엄격하게 해석하는 경우 대표적인 생체정보인 "지문" 조차도 "민감정보"라 할 수 없는 결과가 발생한다. 또한 생체정보를 통해서 건강상태를 분석할 수 있다고 해도 생체정보가 건강정보 그 자체는 아니기 때문에 현행법상 생체정보는 민감정보로 보기도 어려울뿐더러 그 규정에 의한 보호도 받기 힘들게 된다는 결론에 이를 수 있다.[166]

166) 이은우, "생체인식 정보의 처리에 관한 개인정보 보호법제의 현황과 개선방향", 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016, 286면.

이렇게 개인정보 및 민감정보와 생체정보의 관계를 어떻게 설정할 것인가에 관한 문제에 있어서 가장 이상적인 방법은 생체정보만의 정보보호를 위한 보호체계를 구축하는 것이라고 할 수 있다. 이는 곧 개인정보의 자기결정권을 어떻게 구현하는가의 문제이며 현행 법제에서 생체정보를 어떠한 체계 속에 포함시키느냐의 문제라 할 수 있다. 다만, 생체정보에 관한 특별법으로 설계하는 것보다는 가급적 현행 법체계의 틀 속에 포함시키는 것이 입법적 부담을 경감하는 방식이 될 것이다. 이러한 현행 법체계의 틀 속에서 생체정보의 특성을 가장 잘 반영하는 것은 결국 "동의제도"를 어떻게 설계할 것인가로 귀결된다고 할 수 있다.

앞에서 생체정보의 성격을 보다 명확하게 하기 위한 입법 개선방안으로「개인정보보호법」제23조(민감정보의 범위) 또는 동법 시행령 제18조(민감정보의 처리제한)에 규정되어 있는 바와는 별도로 생체정보의 범위 및 생체정보의 처리제한에 관한 규정을 따로 두거나, 아니면 위 민감정보 규정 안에 생체정보를 포함시키는 방안을 제시하였다. 다만, 어느 경우를 선택하더라도 생체정보는 민감정보 보다 더 엄격한 보호장치가 필요하다는 점을 강조하여야 한다. 즉,「개인정보보호법」상 민감정보는 개인정보의 처리에 대한 동의와는 "별도의" 동의를 받아야 하고, 별도의 기술적・관리적 보호조치를 취해야 한다.

민감정보의 처리제한	생체정보의 처리제한(안)
제23조(민감정보의 처리 제한) ① 개인정보처리자는 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	제23조의2(생체정보의 처리 제한) ① 개인정보처리자는 식별 및 인증 등의 고유기능에 사용하기 위하여 개인의 생체적 특징을 전자적으로 추출한 생체인식정보로서 대통령령으로 정하는 정보(이하 "생체정보"라 한다)를 처리할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는

민감정보의 처리제한	생체정보의 처리제한(안)
처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 **별도로 동의**를 받은 경우 2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.	경우에는 그러하지 아니하다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 **별도로 서면으로 동의**를 받은 경우 2. 법령에서 생체정보의 처리를 요구하거나 허용하는 경우 **3. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우. 단, 특정 개인을 알아볼 수 없는 형태로 생체정보를 처리하는 경우에 한한다.** ② 개인정보처리자가 제1항 각 호에 따라 생체정보를 처리하는 경우에는 그 생체정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 **기술적·관리적 및 물리적 조치**를 하여야 한다.

중요한 것은 「개인정보보호법」에서 민감정보를 비롯하여 특별히 보호가 필요한 정보로서 고유식별정보, 주민등록번호, 영상정보에 관한 처리제한 규정을 두고 있고, 개인정보처리자는 그러한 정보의 "안전성 확보에 필요한 조치"의 의무를 지는데, 과연 이러한 의무가 어느 정도 실효적으로 적용되고 있는지에 대해서 살펴볼 필요가 있다. 즉, 위의 정보에 대한 처리제한 규정에는 공통으로 개인정보처리자로 하여금 개인정보를 처리함에 있어 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하도록 하고 있다. 그리

고 이를 위하여「개인정보의 안전성 확보조치 기준」(행자부 고시 제 2016-35호)이 수립되어 있다. 그러나 이 지침에 규정된 안전조치가 추상적이고 일반적인데다가, 각 개인정보의 식별자의 특성이 반영되지 않은 한계가 있고, 무엇보다도 개인정보처리자의 유형 및 개인정보 보유량에 따라 적용대상과 안전조치 기준이 달라 과연 안정성 확보가 어느 정도 달성될 수 있을지에 관하여는 의문이 생기는 것이다.

< 행정자치부「개인정보의 안전성 확보조치 기준」의 체계 >

제1조(목적)
제2조(정의)
제3조(안전조치 기준 적용)
제4조(내부 관리계획의 수립・시행)
제5조(접근권한의 관리)
제6조(접근통제)
제7조(개인정보의 암호화)
제8조(접속기록의 보관 및 점검)
제9조(악성프로그램 등 방지)
제10조(관리용 단말기의 안전조치)
제11조(물리적 안전조치)
제12조(재해・재난 대비 안전조치)
제13조(개인정보의 파기)

제23조부터 제25조까지의 처리제한 규정에 따른 각 개인정보의 안전성 확보에 관하여는 정보의 식별자가 가진 특성과 위험성에 따라 보다 구체적이고 현실적으로 정해져야 할 것이다. 이러한 의미에서 행정자치부의 바이오정보보호 가이드라인(안)의 경우도「개인정보보호법」에서 개인정보를 바이오정보로 대체하는 정도에 그치고 있다는 한계를 인정하고, 보다 밀도 있게 규정될 필요가 있다.

제 4 절 기 타

Ⅰ. 생체정보 기반 본인확인서비스 인증제도의 도입

생체정보를 활용함에 있어 지금까지는 기술수준과 비용 등 이용자 불편이 주된 것이었으나, 최근 생체정보의 활용이 빈번해지면서 보안 문제와 이용자 불신이 커지고 있다. 핀테크, 간편결제, 인터넷뱅킹 등의 이용이 급격히 증가하고 일상화 되면서 본인확인을 요구하는 사이트와 서비스, 앱, 기기 등이 증가하고 있는데, 이는 생체정보를 기반으로 하는 본인확인서비스를 통하여 더욱 확대될 것이다. 그러나 현행법상 본인 확인을 위해 사용되는 생체정보 기반의 본인확인서비스를 관리·감독할 수 있는 통일적인 감독 체계가 마련되어 있지 않고, 생체정보 기반의 본인확인서비스의 안전성과 신뢰성을 사전 검증하거나 사후 관리할 수 있는 인증체계도 마련되어 있지 않아 충분히 안전성이 확보되지 않은 채 생체정보 기반 본인확인서비스가 유통될 가능성이 없지 않다.

「정보통신망법」 제23조의3은 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법 즉 “대체수단”의 개발·제공·관리 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있게 하고 있다. 이에 따라 방송통신위원회는 본인확인기관의 지정에 관한 절차를 마련하여 일정한 심사절차를 거쳐 본인확인기관을 지정하고 매년 사후관리를 하고 있다. 한편, 「신용정보법」 제4조제1항은 신용조회업의 업무 중 하나로서 “본인인증 및 신용정보주체의 식별확인업무로서 금융위원회가 승인한 업무”를 규정하고 있다. 그러나 방송통신위원회와 달리 금융위원회는 생체인식 정보를 이용한 본인확인서비스의 안전성을 검증하거나 사후 관리하기 위한 장치를 운용하고 있지 않다. 그럼에도 불구하고 금융위원회는 신용조회업자의

경우에는 금융위원회의 승인만 있으면 본인확인서비스가 가능한 것으로 해석될 수 있어 보안상 심각한 허점이 생길 수 있는 것이다.

< 현행 본인확인서비스 관련 규정 >

정보통신망법	신용정보법
제23조의3(본인확인기관의 지정 등) ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 **안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.** 1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획 2. 본인확인업무의 수행을 위한 기술적·재정적 능력 3. 본인확인업무 관련 설비규모의 적정성 ② 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다. ③ 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신	제4조(신용정보업의 종류 및 영업의 허가) ① 신용정보업의 종류 및 그 업무는 다음 각 호와 같다. 이 경우 제2호 및 제3호의 딸린 업무는 대통령령으로 정한다. 1. 신용조회업: 신용조회업무 및 다음 각 목의 업무 **가. 본인인증 및 신용정보주체의 식별확인업무로서 금융위원회가 승인한 업무** 나. 신용평가모형 및 위험관리모형의 개발 및 판매 업무 2. 신용조사업: 신용조사업무 및 그에 딸린 업무 3. 채권추심업: 채권추심업무 및 그에 딸린 업무 4. 삭제 ② 신용정보업을 하려는 자는 제1항 각 호에 따른 업무의 종류별로 금융위원회의 허가를 받아야 한다. ③ 제2항에 따른 허가를 받으려는 자는 대통령령으로 정하는 바에 따라 금융위원회에 신청서를 제출하여야 한다. ④ 금융위원회는 제2항에 따른 허가에 조건을 붙일 수 있다. ⑤ 제2항에 따른 허가와 관련된

정보통신망법	신용정보법
위원회에 신고하여야 한다. ④ 제1항부터 제3항까지의 규정에 따른 심사사항별 세부 심사기준·지정절차 및 휴지·폐지 등에 관하여 필요한 사항은 대통령령으로 정한다.	허가신청서의 작성 방법 등 허가신청에 관한 사항, 허가심사의 절차 및 기준에 관한 사항, 그 밖에 필요한 사항은 총리령으로 정한다.

이에 양법을 개정하여 생체인식 기반 본인확인서비스의 안전성과 신뢰성 확보를 위해 일원화된 관리·감독 체계와 인증제도를 도입할 필요가 있다.

Ⅱ. 유전자정보 등 생체정보의 국외유출 금지 강화

「생명윤리법」은 가장 본질적인 생체정보라 할 수 있는 유전자정보에 관한 규율을 담고 있는 법률로서 개인정보의 수집 및 이용에 대해서 제한을 두고 있지만, 이 법의 목적과 주된 내용은 주로 인간대상연구와 인체유래물연구 및 유전자 치료 및 검사에 초점이 맞춰져 있다.

그런데 이 규정과「개인정보보호법」제23조의 관계에 관하여 살펴볼 필요가 있다. 즉, 개인정보보호법 제23조에 따르면 "유전자검사 등의 결과로 얻어진 유전정보"는 당연히 민감정보이기 때문에 정보주체의 별도의 동의가 있거나 법령에 의한 경우가 아니면 유전자정보의 처리가 금지된다.

< 민감정보인 유전정보의 처리 및 제3자 제공 관련 규정 >

생명윤리법	개인정보보호법
제18조(개인정보의 제공) ① 인간대상연구자는 제16조제1항에 따라	제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노

생명윤리법	개인정보보호법
연구대상자로부터 개인정보를 제공하는 것에 대하여 **서면동의를 받은 경우**에는 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.**	동조합·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. 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 ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

그러나 본인확인서비스 목적으로 수집한 유전정보도 민감정보에 포함되는지 여부가 분명하지 아니하고, 유전자정보를 비식별조치한 경우에는 유통에 아무런 제한이 없게 된다. 이러한 경우 본인확인서비스 등의 명분으로 국내 이용자의 유전자정보가 대량으로 수집되어 해외로 유출되거나 해외에서 오·남용될 가능성이 없지 않다.

오늘날과 같이 정보주권이 강조되는 빅데이터 시대에 국내 유전자정보가 함부로 해외로 대량 유출될 경우, 국내 의료산업 및 제약업계

는 물론 개인에 대하여도 막대한 피해를 줄 수 있다. 따라서 유전자정보가 대량으로 해외로 유출되는 것을 막기 위한 예방적 조치가 필요하며, 유전자정보는 비식별조치(익명화)가 되더라도 원칙적으로 국외 이전을 금지하거나 엄격히 제한하여야 한다.

참 고 문 헌

Ⅰ. 국내문헌

강영기, “일본의 생체정보 관련 법제 동향”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

국가인권위원회, “동의절차 및 대체수단 없는 지문인식기 도입은 개인정보자기결정권 침해”, 2015. 3. 1. 보도자료.

금융위원회, “전자금융사기 예방서비스”, 2013. 9. 16. 보도자료.

_____, “비대면 실명확인 운영 현황 및 향후 계획”, 2016. 5. 26. 보도자료.

김민호, “개인정보처리자에 관한 연구”, 「성균관법학」, 제26권제4호, 2014. 12.

김영미, “독일의 생체정보 관련 법제 동향”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

김일환, “생체인식기술 등 첨단정보보호기술의 이용촉진을 위한 법제도적 방안연구”, 「법과정책」, 제주대학교 사회과학연구소, 제13집제2호, 2007. 8.

_____, “생체정보보호법제 정비방안에 관한 고찰”, 「토지공법연구」, 제33집, 2006. 11.

_____, “주민등록법상 지문정보의 목적 외 이용에 대한 헌법적 고찰”, 「공법연구」, 제41집제1호, 2012. 10.

김재성, “바이오인식시스템 보안위협과 차세대 Medical biometrics”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

문기영, “생체인식 기술현황 및 전망”, 「TTA Journal」, No. 98, 한국정보통신기술협회, 2005, 39면.

박미정, 「공공정보의 이차 활용을 위한 법제도에 관한 연구 - 생체·의료정보의 이차 활용을 중심으로-」, 연세대학교대학원 박사학위논문, 2014. 12.

박정훈, “바이오매트릭스의 이용에 따른 법적 과제”, 「경희법학」, 제47권제2호, 2012.

박정훈·김행문, “생체정보 프라이버시의 쟁점 및 정책 시사점-전자여권 사례를 중심으로-”, 「정보화정책」, 제15권제3호, 2008 가을호.

배현아, “생체정보의 분야별 활용현황 - 의료분야”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

송영관, 「기술표준화, 정부개입, 그리고 공인인증서」, 「한국개발연구」, 제37권 특별호(통권제127호), 2014. 8.

심우민, “스마트 시대의 생체정보 보호를 위한 입법과제”, 「이슈와 논점」, 국회입법조사처, 제1129호, 2016. 3. 3.

연광석, “생체인식정보 보호에 관한 연구(비교법적 검토를 중심으로)”, 「법제현안」, 제2005-4호(통권제173호), 국회사무처 법제실, 2005. 9.

연구성과실용화진흥원, “생체인식 기술 및 시장동향”, S&T Market Report, vol. 39, 2016. 2.

염홍열 외, 「전자인증수단 이용기반 확대를 위한 안전성 기준 연구」, 한국인터넷진흥원, 2011. 12.

오길영, “개인정보 보호 법제의 법적 문제 - 금융개인정보와 생체개인정보를 중심으로”, 「민주법학」, 제53호, 2013. 11.

유장희 · 조현숙, “바이오인식기술의 현황 및 진화”, 「정보처리학회지」, 제20권제3호, 2013. 5.

윤재호 · 홍진실, 「바이오인증기술 최신 동향 및 정책과제」, 지급결제조사자료 2006-7, 한국은행, 2016. 8.

이민영, “생체정보의 보호에 관한 법제도적 정책방향”, 「정보통신정책」, 제16권제21호(통권359호), 2004. 11. 16.

_____, “아이오티 관련 개인정보보호법제 조망”, 「신산업 활성화와 개인정보보호」, 개인정보보호법학회 · 한국인터넷진흥원 공동학술대회 자료집, 2016. 6.

이상경, “미국의 생체정보 관련 법제 동향”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

이상명, “주민등록 지문날인제도의 위헌성”, 「한양법학」, 제22권제4집(통권제36집), 2011. 11.

이승재, “생체인증(바이오인식인증)을 이용한 인증기술 및 시장현황”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

이원상, “빅데이터 환경에서 생체정보의 형사정책적 활용에 대한 고찰”, 「비교형사법연구」, 제17권제1호(통권제32호), 2015.

이원태 외, 「사이버세상의 새로운 규범체계 정립방안 연구」, 방송통신정책연구 14-진흥-009, 2014.

이은우, “생체인식 정보의 처리에 관한 개인정보 보호법제의 현황과 개선방향”, 생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

이인호, “「개인정보보호법」상의 ‘개인정보’ 개념에 대한 해석론 – 익명화한 처방전 정보를 중심으로 -”, 「정보법학」, 제19권제1호, 2015. 4.

_____, 일본「개인정보의 보호에 관한 법률」번역문.

이재득, “바이오인식기술의 금융서비스 적용현황 및 발전과제”, 「지급결제와 정보기술」, 제57호, 2014. 7.

이정현, “스마트환경에서의 공인인증서 활용과 문제점”, 「Internet & Security Focus」, 한국인터넷진흥원, 2013. 3.

이창범, “비교법적 관점에서 본 개인정보 보호법의 문제점과 개정방향: 한국・EU・일본을 중심으로”, 「Internet and Information Security」, 제3권제2호, 2012. 2.

_____, “생체정보의 분야별 활용현황 - 금융, 의료, 수사분야”, 「생체정보의 활용 및 보호를 위한 법제 정비방안 연구 - 워크숍 자료집」, 한국법제연구원, 2016.

이한주, “개인의료정보보호법 제정의 필요성과 입법방향”, 「한국의료법학회지」, 제22권제1호, 2014. 6.

한국인터넷진흥원, “KISA, 바이오인식 기술 연계한 공인인증 활용 기술 개발 추진”, 2015. 5. 21 보도자료.

전동훈, “바이오인식 기술의 종류와 활용현황”, 「생체정보의 활용 및 보호를 위한 법제정비방안 연구 : 워크숍 자료집」, 2016.

정소영, “생체정보의 분야별 활용현황 - 범죄수사 분야”,「생체정보의 활용 및 보호를 위한 법제정비방안 연구 : 워크숍 자료집」, 2016.

조규범, “생체정보 보호를 위한 입법론적 고찰”,「공법연구」, 제37집 제1-2호, 2008. 10.

_____, “생체정보보호를 위한 입법론적 대응방안”,「국회도서관회보」, 제45권제9호(통권352호), 2008. 10.

최윤섭, “How the Implement Digital Healthcare in the Future”, 2016.

한국정보보호산업협회,「2015 국내정보보호산업 실태조사」, 2015. 12.

Ⅱ. 외국문헌

1. 미 국

Department of Homeland Security, Report 2012-02 of the Data Privacy and Integrity Advisory Committee(DPIAC) on Privacy and the Department's Collection and Use of Biometrics Nov 7, 2012.

John D. Woodward Jr., Biometrics: Identifying Law and Policy Concerns, in biometrics: Personal Identification in Networked Society, Chapter 19 (Anil K. Jain et al. eds., 1998), at 385-405.

Marie-Helen Maras, Internet of Things : Security and Privacy Implications, International Data Privacy Law, Vol.5, Iss. 2, 2015.

Matthew W. Finkin, Some Further Thoughts on the Usefulness of Comparativism in the Law of Employee Privacy, 14 Employee Rts. & Emp. Pol’y j. 43, fn. 32, 2010.

Michael P. Daly, Kathryn E. Deal, Matthew J. Fedor, Meredith C. Slawe, Biometrics Litigation : An evolving landscape, Practical Law, April/May 2016.

Pierre-Marrie Dupuy, “Soft Law and the International Law of the Environment”, Michigan Journal of International Law, 12, 1991.

Simons John, Greed meets terror, Fortune v. 144, no. 8, Oct. 29 2001.

U.S. Office of Personnel Mgmt. Data Sec. Breach Litig., No. 15-1394, MDL No. 2664(D.D.C.)(Jackson, J.).

Thomson Reuters, Biometric Litigation : An evolving landscape, April/May 2016, Practical Law, 2016.

2. 독 일

Borchers, Detlef, Bundesregierung fördert Biometrie-Forschung, heise online, 3. 4. 2010.

BFDI, Datenschutz-Grundverordnung, 2016. 5.

Biselli, Urteil des Europäischen Gerichtshofes zu biometrischen Personalausweisen ignoriert Datenschutz, Netzpolitik, 21. 4. 2015.

Gruner, Alexander, Biometrie und informationelle Selbstbestimmung – Rechtsfragen biometrischer Merkmale in Pass und Personalausweis, Dresden, 2005.

Heumann, Björn, Whitepaper Biometrie, 2006.

Lipinski, Klaus, Biometrie, IT Wissen, Dietersburg 2009.

Meuth, Lotte, Zulässigkeit von Identitätsfeststellungen mittels biome-

trischer Systeme durch öffentliche Stellen, Duncker & Humblot, Berlin 2005.

Oppermann/Classen/Nettesheim, Europarecht 5. Auflage, C.H.Beck, München 2011, Rn. 71 ff.

Pfeiffenbring, EuGH: Erfassung von Fingerabdrücken in Reisedokumenten, MMR-Aktuell 2013

Spiegel Online, ePass: Biometrischer Reisepass kostet 59 Euro, 1. 6. 2005.

3. 일 본

パーソナルデータに関する検討会, 技術検討ワーキンググループ報告書～「(仮称) 準個人情報」 及び 「(仮称) 個人特定性低減データ」に関する技術的観点からの考察について～, 技術検討ワーキンググループ, 2014年5月.

瓜生和久 編著,「一問一答 平成27年改正個人情報保護法」, 2015.

森田賢二, “個人情報保護法の改正概要と企業の対応”, Risk Solutions Report, No.41, 銀泉リスクソリューションズ株式会社, 2015. 12. 09.

宇賀克也,「個人情報保護法の逐条解説(第4版)」, 2013.

日本弁護士連合会, パーソナルデータの基本的枠組みについての意見書, 2014年11月20日.

Ⅲ. 웹페이지

http://cis.org/EnhancedBorderSecurityVisaReformAct2002-HR3525 (2016.10.10 최종접속)

http://consulting.skcc.com/39 (2016.6.15. 최종접속).

http://news.joins.com/article/18217655 (2016.6.20. 최종접속)

http://science.ytn.co.kr/program/program_view.php?s_mcd=0082&s_hcd=&key=201312041631167881 (2016.9.20 최종접속)

http://www.biometrics.gov/ (2016.10.6. 최종접속)

http://www.biometrics.gov/referenceroom/federalprograms.aspx (2016.10.6. 최종접속)

http://www.boannews.com/media/view.asp?idx=50952&kind=6 (2016.10.13. 최종접속)

http://www.boannews.com/media/view.asp?idx=51126&kind=6 (2016.10.13. 최종접속)

http://www.boannews.com/media/view.asp?idx=51126&kind=6 (2016.10.6. 최종접속)

http://www.chicagotribune.com/business/ct-mastercard-selfie-pay-0224-biz-20160223-story.html (2016.10.10 최종접속)

http://www.cnsnews.com/news/article/state-department-puts-biometric-chips-us-passports (2016.10.10 최종접속)

http://www.drinkerbiddle.com/-/media/files/insights/publications/2016/04/biometricsfeature.pdf (2016.10.10. 최종접속)

http://www.dt.co.kr/contents.html?article_no=2014112002100260800001 (2016.6.20 최종접속)

http://www.fnnews.com/news/201508071657143432 (2016.6.20. 최종접속)

http://www.forbes.com/sites/amitchowdhry/2015/06/17/amazon-patents-a-sys

tem-that-unlocks-your-smartphone-with-your-ear/#3c317587a0d0 (2016.10.6. 최종접속)

http://www.gesundheitsforschung-bmbf.de/de/2514.php (2016.10.13. 최종접속)

http://www.gojo-partners.com/column-ps/1132/ (2016.10.9. 최종접속)

https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap7-subchapXI-partC-sec1320d-6.pdf (2016.10.20. 최종접속)

http://www.heise.de/newsticker/meldung/Bundesregierung-foerdert-Biometrie-Forschung-946316.html. (2016.10.13. 최종접속)

http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (2016.10.10. 최종접속)

http://news.joins.com/article/18217655 (2016.6.20. 최종접속)

http://www.kantei.go.jp/jp/singi/it2/pd/pdf/taihihyo.pdf (2016.10.20.최종접속)

http://www.law.go.kr/lsInfoP.do?lsiSeq=111327&ancYd=20110329&ancNo=10465&efYd=20110930&nwJoYnInfo=N&efGubun=Y&chrClsCd=010202#0000 (2016.10.10. 최종접속)

http://www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM (2016.10.10. 최종접속)

http://www.rechtslexikon.net/d/schleppnetzfahndung/schleppnetzfahndung.htm. (2016.10.10. 최종접속)

http://www.spiegel.de/reise/aktuell/epass-biometrischer-reisepass-kostet-59-euro-a-358564.html (2016.10.6. 최종접속)

http://www-03.ibm.com/press/jp/ja/pressrelease/48637.wss

http://www.edaily.co.kr/news/NewsRead.edy?SCD=JC21&newsid=01659686612647608&DCD=A00302&OutLnkChk=Y (2016.10.9. 최종접속)

https://jobs.forkwell.com/finc/jobs/558 (2016.10.9. 최종접속)

http://terms.naver.com/entry.nhn?docId=1222567&cid=40942&categoryId=31819 (2016.10.24. 최종접속)

http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T1B5B0W2V0C5K1X7Q4Z0V4X4U4X9O2 (2016.10.24. 최종접속)