논문 18-43-01-27 The Journal of Korean Institute of Communications and Information Sciences '18-01 Vol.43 No.01
https://doi.org/10.7840/kics.2018.43.1.201

바이오정보 활용 서비스 현황 및 GDPR 사례를 통한 바이오정보보호 법제 개선방안

정 부 금•, 권 헌 영°, 박 혜 숙*, 임 종 인**

Biometrics Service Trends and Improvement of Bio Data Protection Law referring to GDPR

Boo-geum Jung•, Hun-yeong Kwon°, Hea-sook Park*, Jong-in Lim**

요 약

센서 기반의 IoT 기술의 발달로 바이오정보 인식은 더욱 정확성을 띄게 되었고, 지문뿐만 아니라 얼굴, 홍채 인식이 스마트폰에 쓰이기 시작하고 있고, 인터넷 전문은행, 모바일 결재 등 비대면 금융 서비스의 활성화 등으로 바이오 정보는 본인 인증을 위한 수단으로서 다양한 분야에서 활용되고 확산되고 있다. 이를 지원하기 위해 각국에서는 바이오정보에 대한 법제의 정비를 시작하고 있다. 이에 본 논문에서는 최근의 바이오정보 활용 서비스와 EU GDPR에서의 바이오정보를 분석하였다. 이를 바탕으로 바이오정보보호를 위한 개선사항들을 도출하여, 안전한 바이오정보 활용 서비스를 위한 법제 및 정책 수립에 도움이 되고자 한다.

Key Words : biometircs, biometric data, genetic data, health data, GDPR

ABSTRACT

Due to the development of sensor based IoT technology, biometrics recognition has become more accurate, and face and iris recognition are starting to be used in smart phones as well as fingerprints. As a result of the activation of non-face financial services such as Internet banks and mobile payments, biometrics is being utilized and spread in various fields as a means of personal identification and authentication. To support this, the legal system of the biometrics is beginning to be established all over the world. Thus, in this paper, we analyze recent bio information service and bio information regulation in EU GDPR. And we'd like to assist in establishing legislation and policies for biometrics protection and utilization.

Ⅰ. 서 론

모든 것이 인터넷으로 연결되어 서로 정보가 생성・수집・공유・활용되는 초연결 시대의 도래[1] 로 온라인 상에서 본인임을 증명하고 비대면으로 재화를 이용하는 활동이 급격히 늘고 있다. 오프라인 상에서의 주민등록증, 실물 카드와 동일한 역활로 온라인 상에서는 주민등록 번호, 핸드폰 번호, 공인인증서 등이 사용되고 있다. 그러나 일련의 대형 개인정보 유출 사건들로 전 국민의 개인정보는 더 이상 개인정보가 아

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00282, 다매체 다중경로 적응적 네트워크 기술 개발)
◆ First Author : Korea University Department of Information Security & ETRI, bgjung@etri.re.kr, 정회원
° Corresponding Author : Korea University Department of Information Security, khy0@korea.ac.kr, 정회원
* ETRI Defense & Security ICT Convergence Center, parkhs@etri.re.kr, 정회원
** Korea University Department of Information Security, jilim@korea.ac.kr, 정회원
논문번호 : KICS2017-11-365, Received November 29, 2017; Revised January 4, 2018; Accepted January 4, 2018

닌 상황에 이르렀다. 또한, 글로벌 경제 시대를 맞이하여 복잡한 전자상거래 규제 구조를 개선하여 간편한 인증 및 결제 절차로 개선하고 있어 개인정보로서 바이오정보의 사용이 크게 확산되고 있는 추세이다.[2]

바이오 정보를 활용한 다양한 서비스에 있어서 기술과 법은 서로 상호 유기적인 관계로 작용하게 된다. 법제도는 신규 서비스 적용 및 확대를 위한 기반을 제공함으로써 새로운 기술 혁신을 견인할 수 있다. 즉, 정부가 정책적으로 지원할 수 있는 법제도적 근거를 제공함으로서 관련 기술 발전의 추진력으로 작용하게 된다. 그러나 기술의 발전을 지원하지 못하는 법제도는 규제가 되어 기술의 산업화에 장애로 작용할 수 있다.

특히 IT 관련 법제도는 급격한 기술변화와 세계적인 환경변화에 빠른 대응이 필요한 바 신규 서비스 활용에 장애물이 되는 직·간접적 규제를 개선하고 신기술과 서비스를 창출할 수 있는 촉매제로서 법제도의 기능을 강화할 필요가 있다.

Ⅱ. 바이오정보 서비스 현황

바이오 정보를 활용한 서비스는 본인 인증과 본인 확인의 2가지 범주로 구분할 수 있다. 본인 확인은 그 사람이 누구인가를 식별하는 것으로 데이터베이스에 저장된 여러 명의 사람들로부터 일치하는 사람이 있는지를 검색해서 식별해 내는 것이다. 예를 들면, 전자주민증과 같은 것으로 전자주민증에 있는 지문의 소유주를 지문 데이터베이스에서 검색하여 주민증 소지자의 얼굴과 이름 생년월일 등이 일치하는지를 조사하는 것이다.

본인 인증은 해당 사람이 권한이 있는 사람이 맞는지를 검증하는 것으로 입력된 바이오 정보와 시스템에 저장되어 있는 정보와 비교하여 신분을 증명하는 것이다.

범죄 수사나 보건 의료, 검역, 얼굴 이용 엔터테인먼트 서비스, 상업적 마케팅 같은 경우는 일반적으로 대상의 확인 기능이 우선이고, 금융결제나 출입통제, IT 보안과 같은 분야는 반드시 본임임을 확인함과 동시에 인증까지 하여야 하는 분야이다.

본 장에서는 바이오정보의 활용에 있어 확인과 인증으로 구분하고 현재 우리 실생활의 많은 분야에서 이루어지고 있는 주요한 최근 서비스 현황과 문제점 및 이슈들을 파악한다.

2.1 본인 인증 분야

전자상거래 규제 개선을 위한 전자결제 절차 간소화 추진으로 공인인증서 의무 사용이 폐지되었다. 이에 본인 인증을 위한 다양한 대체 수단이 도입되고 있는데, 가장 주목받고 있는 것이 바이오정보를 사용한 인증이다[3].

바이오 인증은 지문, 홍채, 얼굴 등 이용자 생체정보나 행위 정보를 이용하여 본임을 인증하는 것이다. 비밀번호를 암기하여 입력하거나 보안카드 등을 소지하지 않아도 되므로 편리하다. 본인만 인증이 가능하여 복제가 쉽지 않으며, 바이오 정보는 단말기 내부 보안 영역에 저장돼 유출 위험이 낮은 장점이 있다. 그러나 실리콘으로 제작한 지문이나 인터넷에 있는 사진을 이용한 위조 사고[1]와 악용 사례가 나타나고 있어 보안에 대한 대비가 필요하다[4].

2.1.1 금융 서비스

(1) 카카오뱅크

카카오뱅크는 2017년 7월 오픈한 인터넷 전문은행으로 SNS 기반의 비대면 채널에 바이오 인증을 접목한 간편 금융 서비스이다.

카카오뱅크가 바이오 인증을 도입한 이유는 비대면에 따른 보안성 강화 목적이 가장 크다. 금융위원회가 허용한 비대면 실명확인 방식을 준용하면 신분증 사진, 기존계좌를 이용한 이체, 영상통화, 카드, OTP[2] 등 접근 매체 확인, 생체인증 중 2가지를 이상으로 본인 확인을 하면 되므로, 휴대폰 본인 인증 후 지문, 패턴, 통장비밀번호를 등록하고, 신분증 사진을 찍어서 제출, 기존계좌를 활용하여 인증하고, 인증 비밀번호 등록한다. 신분증 사진은 신용평가사를 연계해서 확인을 한다.

(2) 삼성페이

삼성페이는 스마트폰에 신용카드를 등록하고 실물카드 없이 스마트폰과 지문인식으로 간편하게 결제할 수 있는 서비스이다. 오프라인 상점에서 NFC 단말기를 이용한 결제는 물론 예전의 마그네틱 카드 단말기에도 사용할 수 있다.

토큰화 기술을 이용, 일회용으로 발급되는 가상 카

1) Hacker News, "Hacker Clones German Defense Minister's Fingerprint Using Just her Photos," Dec.2014, http://thehackernews.com/2014/12/hacker-clone-fi

2) OPT(One Time Password) 높은 수준의 보안을 유지하며 사용자를 인증해야 할 필요가 있을 때 사용하는 일회성 발급 비밀번호

드 번호를 사용하고 MST[3] 방식을 적용하였다. 다른 결제 서비스는 NFC나 IC칩과 같은 접촉식 기술로 결제를 하는데 반해, 삼성페이는 이외 추가적으로 마그네틱 전송 기술을 제공하는 것이다.

서비스를 위해서는 모바일 기기에서 앱카드 실행 후 계정 로긴을 하고 지문을 등록한다. 이때 지문은 FIDO[4] 방식으로 개인의 모바일 기기에 지문이 저장된다. 휴대폰 본인 인증, 결재 비밀번호 입력, 서명 입력으로 등록이 이루어진다.

(3) LG페이

LG전자는 페이 서비스에서 후발 주자로서 2017년 6월 지금까지 나온 '페이'의 단점을 보완하기 위해 노력한 'LG페이'를 내놓았다. LG페이는 기존의 마그네틱 방식과 NFC 방식에 추가적으로 IC칩 결제 기능까지 지원한다. 휴대전화의 앱으로만 동작하는 앱카드 형식의 기존 페이들과 달리 별도의 '화이트 카드'를 제공한다.

화이트 카드는 전자기기 성격의 카드 형태로 여러 카드 정보를 입력하여 카드 한 장으로 사용할 수 있도록 한 것이다. 결제를 위해서 해당 카드를 불러내고 생체 인증 과정을 거치는 방법은 다른 스마트폰 지불 방식과 동일하다. 삼성, LG 모두 페이앱을 실행하는 과정과 지문 기반의 바이오 인증을 하는 과정이 각각 따로 연속적으로 이뤄진다. 삼성페이와 마찬가지로 지문 인증에 FIDO방식을 사용한다.

2.1.2 ICT 보안 서비스

(1) 아이폰X 페이스 아이디

아이폰X의 페이스ID(2017년 9월 공개)는 기존의 지문인식을 완전히 대체하여, 아이폰 잠금 해제와 앱스토어 결제에 사용하는 새로운 바이오 인증 시스템으로 정확한 스캔과 인식을 위해 전면에 도트 프로젝터, 적외선 카메라, 투광 일루미네이터로 구성된 트루뎁스(TrueDepth) 카메라 시스템을 탑재했다.

얼굴은 비밀번호와 달리 새로 바꿀 수 있는 게 아니다. 누군가가 사용자의 얼굴을 똑같이 구현해 페이스아이디를 뚫을 수 있는 방법을 찾아낸다면 보안성에 큰 구멍이 생길 것이다. 같은 얼굴을 가진 일란성 쌍둥이에게 페이스아이디는 '완벽한' 인증 시스템이 아니다. 또 지문과 달리 우리의 얼굴은 SNS에 무수히 노출돼 있다. 미국 노스캐롤라이나대학은 페이스북에 올라온 얼굴 사진으로 3D 모델을 만들어 얼굴인식 애플리케이션을 해킹해 보였다. 성공률은 55%에서 85% 사이였다. 또한, 누군가 물리적 강제를 이용해 사용자가 페이스아이디를 잠금 해제하게 시킬 가능성도 있다. 경찰이 용의자의 아이폰을 강제로 잠금 해제하려는 상황에서 용의자의 얼굴을 아이폰X 앞에 놓기만 하면 되기 때문이다.

(2) 갤럭시 S8 홍채 인식

세계 최초로 갤럭시 스마트폰에 탑재된 홍채 인식은 스마트폰 전면에 표시되는 카메라를 바라보며 홍채로 본인임을 인증하는 방식으로 손을 대지 않는 비접촉 방식이다. 홍채 정보는 어릴 때 형성돼 변하지 않는 특징을 갖고 있다. 특히, 쌍둥이라 하더라도 홍채 정보는 각자 다르다. 전면 상단엔 홍채 인식을 위한 카메라와 적외선 LED가 있고, 홍채 인식을 위한 전용 카메라로 촬영한다. 촬영 정보에서 홍채 영역을 추출하여 디지털 정보로 바꾼 후 암호화 절차를 거쳐 하드웨어적으로 구분된 안전지역(trust zone)에 저장한다. 이후 스마트폰 기능을 실행할 때 등록된 정보와 비교해 인증이 이뤄진다.

2.2 본인 확인 분야

2.2.1 공공 서비스

(1) 인도 아드하르와 인디아 스택

인도 국민의 지문과 홍채 정보를 저장하기 위한 아드하르 시스템에는 현재 10억 명의 지문과 홍채 정보가 저장되어 있다[5]. 생체 인증으로 실시간 본인 확인을 위해 구축되었으며, 기업에서는 지문 또는 홍채 판독기를 통해 아드하르 시스템에 접속할 수 있다. 아드하르는 실시간 통신 회선 개통은 물론 통합결제시스템, 디지털 의료, 교육과 구직 활동 등 모든 분야에서 광범위하게 활용할 수 있는 복합 디지털 인프라인 인디아 스택의 데이터베이스로 사용되고 있다[5].

인디아 스택은 아드하르를 기반으로하여 디지털 카

3) Magnetic Secure Transmission, 마그네틱 보안전송

4) FIDO(Fast IDentity Online)는 비밀번호의 문제점을 해결하기 위한 목적으로 FIDO 얼라이언스에 의해 제안된 사용자 인증 프레임워크다. 인증 기법과 그 인증 정보를 주고 받기 위한 인증 프로토콜을 분리하는 것을 핵심 아이디어로 한다. FIDO Specification은 비밀번호 없이 인증을 하기 위한 Universal Authentication Framework (UAF) 프로토콜과 비밀번호를 보완해서 인증을 하기 위한 Universal 2nd Factor (U2F) 프로토콜로 구성된다.

5) 제4차 산업혁명시대, 혜성처럼 등장한 디지털 지도자 : http://www.ipnomics.co.kr/?p=59364&

드를 만들어 국민 12억 명의 지문과 홍채 정보의 디지털화를 시도하는 프로젝트다. 주민등록증에 지문과 홍채 정보를 담는 것과 동일하다고 보면 된다. 이를 통해서 단순히 본인 확인뿐만 아니라, 행정, 금융, 산업 등 모든 분야에 활용할 수 있도록 인프라를 구축하고 있는 것이다.

인도에는 포괄적인 개인정보보호법이 없기 때문에, 국민들의 데이터를 보호할 수 있는 개인정보 보호책이 마련되지 않은 채 기업에 의해 방대한 생태계가 구축되는 것은 문제가 있다는 의견이 제시되었다[6]. 이에 인도 대법원에서 국민들은 사생활을 보호받을 헌법의 기본권을 갖고 있다고 판결했고, 인도 대법원이 63년 동안 프라이버시 즉, 사생활 보호를 헌법상의 권리로 인정하지 않았던 판례를 변경해 기본권이라고 인정한 것에 큰 의미가 있는 판결로 볼 수 있다.[6)]

(2) 전자여권

전자여권이란, 국제민간항공기구(ICAO)와 국제표준화기구(ISO)에서 정한 국제표준에 의거 성명·여권번호와 같은 개인 신원정보와, 얼굴·지문과 같은 바이오인식정보를 전자적으로 수록한 비접촉식 전자 칩이 내장되어 있는 기계 판독식 여권이다[7)].

전자칩에는, 기존 여권의 신원정보면에 수록되어 있는 정보가 모두 전자적으로 수록된다. 즉, 동일한 정보를 여권의 앞쪽과 뒤쪽의 칩에 기록해 놓음으로써 동시에 변조하지 못하도록 하고, 어느 한 쪽이 변경되었을 경우 이를 구분해 낼 수 있도록 하는 것이다.

(3) CCTV

범죄예방, 주차단속 등 다양한 목적으로 설치된 CCTV는 매년 빠르게 증가하고 있는데, CCTV 통합관제센터를 통한 개인정보의 목적 외 이용 문제, 차량이나 얼굴 등을 자동 인식할 수 있는 지능형 CCTV 등이 논란이 되고 있다. 지능형 CCTV와 같이 영상정보 수집 장치와 얼굴인식 기술이 결합할 경우, 개인의 인권에 미치는 부정적 영향이 막대할 수 있고 국가 감시의 우려도 불러일으킬 수 있다. 이미 미국에서는 얼굴 인식 시스템이 수사 목적으로 광범위하게 사용되고 있는데, 이를 규제할 수 있는 법제는 미비한 상황이다[8)]. 현행 개인정보 보호법은 CCTV와 같은 영상정보처리기기에 대한 규정을 두고 있지만, 통합관제센터, 블랙박스, 바디캠, 드론 등 그 규제 대상에서 제외되어 있거나 수집된 영상정보를 얼굴인식 기술을 사용하여 분석하는 것에 대해서는 규율하고 있지 못하다.

2.2.2 출입 통제 서비스

(1) 인천 공항 출입국 관리

자동출입국은 사전 등록한 생체정보 또는 경찰청이 보유한 지문정보 데이터베이스와 연계를 통해 자동출입국심사대에서 여객이 출입국심사를 하는 것이다. 여권과 지문 및 안면 등을 스캔하면 비대면 으로 간단히 심사가 끝난다.

(2) 정부 청사 출입 통제

공무원 시험 준비중이었던 한 학생이 정부서울청사에 침입한 사건[9)] 이후 정부청사 출입을 위한 얼굴인식 시스템이 도입되었다. 얼굴인식을 도입하기로 한 것은 다른 바이오 인식 시스템에 비해 정확하고 처리 속도가 빠르며, 직접 접촉하지 않아도 되어 위생적인 것으로 판단했기 때문이다.

얼굴인식 출입통제 시스템은 각각 서울청사에 26대, 과천청사에 29대, 대전청사에 19대, 세종청사에 112대로 모두 186대가 도입됐다.[10)] 추후 다른 공공기관들로 확산되어 도입된다면 적용 규모가 크게 확장될 것으로 전망된다.

Ⅲ. GDPR에서의 바이오정보보호

EU는 개인정보보호지침(1995년)을 전폭적으로 개정하여 최신 IT 기술을 반영한 GDPR[7]을 채택하였다(2016년 4월 27일). GDPR이 적용되기 시작하는 2018년 5월 5일이 되면, 28개 EU 회원국들의 개인정보보호법 제도가 보다 일관성 있게 시행될 것이다. 기존의 DPD[9]에서는 바이오정보에 대한 규정이 없었으나, GDPR에서는 바이오 정보를 특별한 범주의 개인정보로 정의하고 있다. 이에 본 장에서는 개인정보보호에서 글로벌 표준이 되고 있는 GDPR에서의 바이오정보 법제에 대해서 분석하고 시사점을 도출한다.

6) 인도에서는 신분증에 홍채, 지문 정보를 저장해야 한다 http://www.boannews.com/media/view.asp?idx=56612
7) http://www.passport.go.kr/digital/digital.php
8) <영구적인 라인업(The Perpetual Line-Up) - 미국에서 규제되지 않는 미국의 얼굴인식 시스템> 보고서
9) 2016년 4월 정부청사에 침입해 성적을 조작한 7급 공무원 수험생 송 모(26) 씨 사건
10) 공시생 침입사건이 쏘아올린 작은 공, http://www.securityworldmag.co.kr

3.1 바이오 정보의 개념

유럽전역의 공통적인 개인정보보호규정인 GDPR에서는 바이오정보를 유전정보, 바이오인식 정보 및 건강관련 정보로 명시하고 있다(제9조 특정 범주의 개인정보 처리).

유전정보(genetic data)는 개인의 유전적 또는 후천적으로 얻은 유전자 특성에 관한 개인정보로, 염색체 분석, DNA 분석 또는 RNA 분석 등 해당 개인으로부터 채취한 생물학적 샘플 분석에서 얻은 결과 또는 다른 요소 분석을 통해 이에 상응하는 정보를 획득하여 얻은 결과이다.

바이오인식 정보(biometric data)는 얼굴이나 지문 정보처럼 개인을 고유하게 식별하거나 확인할 목적으로, 개인의 신체, 생리, 행동 특성에 관하여 특수하게 기술적으로 처리한 결과 발생한 개인 정보를 의미한다.

건강관련 정보(data concerning health)는 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보를 의미한다(제4조 정의).

3.2 정보 주체 보호제도

기존의 개인정보에 대해서도 정보주체의 보호는 중요하지만 특히 민감정보인 바이오정보에 대한 정보주체의 보호는 더욱 중요한 사안이다. 이에, GDPR은 정보주체를 보호하기 위해 여러 가지 제도를 추가적으로 규정하였다. 그 중 제25조에서는 데이터 보호 중심설계 및 데이터 보호 설정[11]을 규정하고 있다. 개인정보 처리자는 개인정보의 처리 수단을 결정한 시점과 처리 당시 시점에서, 정보 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해, 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등, 적절한 기술 및 관리 조치를 이행해야 한다(by Design). 또한 개인정보 처리자는 기본설정을 통해, 처리의 개별 특정 목적에 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리 조치를 이행해야 한다(by Default). 이런 조항들은 개인정보에 대한 정보주체의 권리를 실질화하기 위하여 상품이나 서비스의 구상·기획 단계에서부터 적용할 것을 제안받고 있는 프라이버시 중심설정(Privacy by Default), 프라이버시 중심설계(Privacy by Design)의 원칙[12] 및 유럽네트워크정보보호원(ENISA)의 프라이버시 및 개인정보보호 중심설계의 공학적인 설계 방법[13]을 법으로 정의한 것이다.

3.3 바이오 정보 영향평가 적용

GDPR에서는 개인정보 영향평가를 적극적으로 도입하였다. 특히 제35조와 해설전문 91에서는 바이오인식 정보 등 민감 정보의 대규모 처리에 대해서는 개인정보 영향평가가 적용되어야 한다는 점을 명시하고 있다.

3.4 바이오 정보의 프로파일링

GDPR은 바이오정보를 포함하는 개인정보에 대해 '프로파일링'(profiling)을 규정하고 이를 제한하는 조항들을 도입하였다. 우선 '프로파일링'이란, "개인에 관한 특정한 개인적 측면을 평가하기 위해, 특히 개인의 업무능력, 경제 상황, 건강, 개인의 성향이나 관심사, 신뢰도, 행동, 위치, 이동에 관한 측면을 분석 및 예측하기 위해 개인정보를 사용하는 모든 개인정보의 자동처리 형태를 의미한다"(제4조(4)).

GDPR은 이러한 자동처리에 따라 정보주체에게 피해가 가지 않도록 규정하는데, 이러한 규정은 바이오정보 기반 서비스 제공에 대한 제한이 될 수 있어 프로파일링의 규정은 바이오인증 서비스 기술의 허용을 제한하게 될 수 있다.

유럽연합 역외의 개인정보처리자라 하더라도 정보주체에 대한 결정을 할 때나, 정보주체의 개인적 선호, 행동과 태도를 분석하거나 예상하는 프로파일링 기법 같은 개인정보처리 기술을 잠재적·계속적으로 사용하여 개인을 인터넷에서 추적하는 경우에는 이 법의 적용을 받는다(해설전문 24). 정보주체는 프로파일링 유

11) Data protection by design and by default

12) 프라이버시 중심설계란, 캐나다 온타리오 개인정보보호 감독관인 카부키안 박사가 1990년대 "미래의 프라이버시는 단지 법률이나 규제 체제 준수만으로 보장할 수 없다. 프라이버시 보장은 기관들이 시행 과정에서 기본설정으로 채택해야만 한다"는 취지로 고안한 개념이다. 프라이버시 중심설계의 실시는 7대 원칙에 따른다. 7대 원칙은 ① 사후 대응이 아니라 사전 대비, 문제점을 고치는 것이 아니라 사전 예방할 것 ② 프라이버시 보호를 시스템의 기본 설정값(default)으로 설정할 것 ③ 모든 활동계획에 프라이버시를 포함할 것 ④ 포괄적 기능성을 보장할 것, 즉 상호대체(Zero-Sum)가 아닌 상호보완(Positive-Sum)으로 전환 ⑤ 전체의 생명주기상에서 보안을 고려할 것 ⑥ 가시성과 투명성을 기반으로 이해당사자에게 항상 공개되도록 할 것 ⑦ 사용자 중심의 설계와 운영으로 개인의 프라이버시가 존중되도록 할 것 등이다(Ann Cavoukian, 2013).

13) ENISA 보고서에서 제시한 8가지 설계 전략은 ① 최소화(Minimize) ② 숨기기(Hide) ③ 분리(Separate) ④ 총계(Aggregate) ⑤ 통지(Inform) ⑥ 통제(Control) ⑦ 강화(Enforce) ⑧ 입증(Demonstrate) (ENISA, 2014)

무와 해당 프로파일링의 결과에 대해 고지 받아야 한다(해설전문 60). 구체적으로 정보주체는 프로파일링 등 자동 의사 결정의 유무, 관련 논리에 관한 유의미한 정보와 이러한 정보주체에 대한 처리의 유의성과 예상되는 결과에 대해 수집 시점에 정보를 제공받을 권리가 있으며(제13조 및 제14조), 같은 정보에 대해 열람권이 있고(제15조), 프로파일링에 대해 언제든지 반대할 권리를 갖는다(제21조). 무엇보다 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 발생시키거나 본인에게 지대한 영향력을 행사하는 자동 처리에만 의존하는 결정을 거부할 권리를 갖는다(제22조). 특히 바이오 정보를 비롯한 민감정보에 기반해서 판단이 이루어져서는 안 된다. 단, 제9조 (2)항의 (a)와 (g)가 적용되고 또한 정보주체의 권리와 자유, 정당한 이유를 보호하는 적절한 조치가 시행되는 경우는 예외로 한다.

3.5 익명처리와 가명처리

GDPR에서는 데이터의 보호에 가명처리의 개념을 새로이 도입하여 익명정보(anonymisation)와 가명처리(pseudonymisation)를 구분하여 다루고 있다. '가명처리'는 추가 정보를 사용하지 않고서는 정보주체를 식별할 수 없도록 개인정보를 처리한 것을 의미하며, 이 경우, 해당 추가정보는 별도로 보관되며 개인정보로 식별되거나 식별될 가능성이 있는 개인에게 해당되지 않도록 보장하기 위한 기술 및 관리조치가 적용된다(제4조(5)). 개인을 더 이상 식별될 수 없는 익명정보는 개인정보가 아니며, 통계를 위한 사용 및 연구를 위한 사용 등을 위한 익명정보의 처리에는 이 법이 적용되지 않는다. 가명 처리된 정보는 개인정보 식별에 대한 위험성을 줄일 수는 있지만, 다른 부가적인 정보를 사용하여 인식할 가능성이 존재하므로 여전히 개인정보로 간주한다. 즉, 연구나 통계 목적을 위해 민감정보의 처리가 필요한 경우, 앞서 살펴본 제9조 제2항 (j)에 명시되어 있다시피, 목적에 비례적이고 본질적인 권리를 존중하며 적절하고 구체적인 보호수단을 제공하는 경우 제89조 제1항에 따라 이를 처리할 수 있다. 그리고 '공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인 정보 처리에 적용되는 안전조치 및 적용의 일부 제외'를 규정하고(제89조 제1항) 이와 같은 목적에서 개인정보를 처리할 경우 가명처리 등 기술·관리적 보호수단을 적용해야 하고, 다만 '정보주체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보의 추가 처리', 즉 익명화를 우선적으로 적용해야 한다. 다만, 불가피한 경우 각국이 법률에 의해 동의권 행사 등 정보주체의 권리를 제한할 수 있도록 하였다.

GDPR의 가명처리, 익명정보의 구분을 적용해 보면, 공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인정보 처리라 하더라도 가명처리는 개인정보로서 정보주체의 동의 등 절차에 따라 처리해야 하고, 익명정보는 개인정보가 아니므로 이 법의 적용이 배제된다.

Ⅳ. 바이오정보보호 법제 개선 방향

바이오정보는 살아있는 개인을 인식할 수 있는 정보이므로 기본적으로 개인정보에 관한 일반법인 개인정보보호법[8]을 따르게 된다, GDPR이 개인정보의 활용과 보호의 균형에 초점이 맞추어져 있다면 개인정보보호법은 보호가 좀 더 높은 비중을 차지하고 있다[14]. 즉, 개인정보를 활용하기에 규제가 되고 있는 부분이 존재한다. 본 장에서는 앞서 GDPR의 분석을 사례로 하여 바이오정보 보호를 위한 법제 개선 방향을 제시한다.

4.1 통합적 개념 및 기준 규정

개인정보보호법에서 바이오 정보가 정의되어 있는 부분은 민감정보 관련 조항이다. 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보나 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 정보로서 개인정보보호법 시행령에 의해 규정된 유전정보, 범죄경력자료 등이 민감정보에 해당되어 그 처리가 제한된다.

그러나 「개인정보 보호법」은 모든 바이오인식 정보를 민감정보로서 포함하고 있지 않다. 지문은 개인의 고유성, 동일성을 나타내고 정보주체를 타인으로부터 식별가능하게 하는 가장 보편적이고 중요한 개인정보이지만, 현행 개인정보 보호법에서는 민감정보로 규율되고 있지 않다.

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

전자서명 및 전자거래 관련 법률들에서는 '생체특성정보'를 개인정보에 포함하여 규정하고 있다. 「전자금융거래법」, 「전자서명법」, 정보통신망법 시행령 외

14) Graham Greenleaf, "Asian Data Privacy Laws: Trade & Human Rights Perspectives," (2014), p. 122

에도, 지문의 경우 「주민등록법」, 「여권법」, 「인감증명법」, 「형의 실효 등에 관한 법률」, 「경범죄 처벌법」, 「실종아동등의 보호 및 지원에 관한 법률」에 따라 국가 행정에서 요구되는 때가 있으며, 유전정보의 경우 「DNA법률[15]」, 「실종아동등의 보호 및 지원에 관한 법률」에서 규율되는 때가 있다.

이처럼 여러 법률이 바이오인식 정보를 '생체정보' 혹은 '바이오 정보'로 서로 다르게 규정하여 흩어져서 규율하고 있다는 사실은 통합적 개념 정립 및 기준 규정이 필요하다는 점을 역설한다.

4.2 합리적인 사전 동의 규제

개인정보보호법 제3조에서는 바이오정보가 포함된 개인정보의 주체를 보호하기 위하여 정보 처리 목적을 명확하게 하고 그 목적에 필요한 범위에서 최소한의 정보만을 처리해야함을 원칙으로 규정하고 있다.

개인정보의 수집과 제공에 관해서는 제15조와 제17조의 범위를 넘어서는 이용 및 제공은 원칙적으로 금지된다. 단, '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공'하는 경우 예외가 허용된다. 즉, 이 경우 개인정보 처리자는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 이렇게 개인정보보호법은 목적 외 이용·제공에 대한 예외사유를 한정적으로 명시한다. GDPR에서는 최초 수집 목적에 부합되는 목적에 대해서는 정보주체의 동의나 별도의 법적인 근거 없이도 허용하도로 되어 있어 대조되는 부분이다. 초연결 사회의 도래로 어디에나 있는 IoT 기기 간 통신을 통해 수집·이용되는 수많은 실시간 정보에 대해 개별적인 사전 동의는 현실적으로 어려운 실정이다. 이에 합리적인 사전 동의 규제가 이루어질 수 있는 방향으로 개선해야 할 것이다.

4.3 비식별화 세분화 및 기준 필요

개인정보보호법은 GDPR에서 새로이 정의한 가명처리를 명시하고 있지 않다. 동 법 제2조는 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'을 개인정보로 포함시키는데, 이는 GDPR 내에서 규정하고 있는 가명처리정보에 해당된다고 볼 수 있다. 즉, GDPR의 가명처리는 '추가적인 정보를 사용하지 않고는 특정 정보주체를 알아볼 수 없도록 처리하는 것'을 의미한다.

개인정보보호법은 제3조 제7항에서 "개인정보 처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다"라고 규정하고 있다. 그러나, 익명처리에 대해서 구체적 내용이나 방법에 대하여 정의하지 않는다.

개인정보보호법 제18조 제2항 제4호의 '특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우'라는 문구가 그 자체로서는 가명처리를 의미하는 것인지 익명처리를 의미하는 것인지 명확히 구분되지 않는다. 또한, 개인정보 비식별화는 주민번호 이름, 나이 등 정형 데이터에 대한 방법만을 다루고 있다. 따라서, 개인정보보호법에 바이오정보와 같은 비정형데이터를 포함하여 비식별화에 대해 명확한 정의와 규범을 추가할 필요가 있다.

V. 결 론

온라인에서의 경제생활이 일상화되어 안전하고 쉽고 간편한 바이오정보를 활용한 금융, 인터넷, 건강 등의 서비스 활성화는 피하거나 제한할 수 없는 것이지만, 동시에 인권을 가진 개인의 정보보호도 결코 양보될 수 없다. 이 점에서 바이오정보의 활용과 개인바이오 정보보호는 함께 추구하여야 할 것이고, 이러한 개인바이오정보의 활용은 개인정보보호를 내재하면서 허용되어야 할 것이다.

EU GDPR을 사례로 살펴보았을 때, 급격히 확산되고 있는 바이오정보 서비스를 안전하게 규제하고 보호하기 위한 법제의 정비를 위해서는 현재의 서비스 형태를 반영하여 바이오정보에 대한 명확하고 일관된 정의가 필요하며, IoT 시대의 도래에 따라 본인이 인식하지 못하는 사이에 이루어질 수 있는 바이오정보의 본인 인증 목적 외 사용에 대해서는 구체적인 절차와 규정 정의가 필요하다. 또한 바이오정보에 대한 영향 평가 및 프로파일링 정의, 바이오정보와 같은 비정형 데이터의 비식별화에 대한 구체적인 정의가 추가되어야 함을 개선점으로 도출하였다. 본 논문에서 도출한 이러한 개선 방향은 바이오 정보를 활용하는 서비스의 활성화와 민감한 개인정보로서의 바이오정보의 보호에 대한 균형 확보를 위한 법제 및 정책 수립에 도움이 될 수 있을 것이다.

References

[1] J. Shim, *Korea's 4th Industrial Revolution*,

15) 디엔에이 신원확인정보의 이용 및 보호에 관한 법률

ETRI-easy IT, 2017.
[2] J. Yoon, *Latest Trends in Biotech Technology Policy task*, Bank of Korea, 2016.
[3] H. S. Jin, "A study on improvement for a means of access to electronic financial service," *Convergence Secur. J.*, vol. 15, no. 5, 2015.
[4] Financial security officer, *Investigation of cases of bio information accidents and countermeasures*, 2016.
[5] P. Chatterjee and A. Nath, "Biometric authentication for UID-based smart and ubiquitous services in india," *Fifth Int. Conf. Commun. Syst. and Network Technol.*, pp. 662-667, 2015.
[6] P. Dixon, "A failure to "Do No Harm" India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.," *Health Technol.*, vol. 7, no. 4, pp. 539-567, Dec. 2017.
[7] EU GDPR (General Data Protection Regulation) (Regulation (EU) 2016/679)
[8] EU Data Protection Directive (Directive 95/46/EC)
[9] Personal data Protection Act (Enforcement 2016.9.30.)

정 부 금 (Boo-geum Jung)

1986년 2월 : 부산대학교 계산통계학과 졸업
1991년 8월 : 숙명대학교 전자계산학과 석사
2012년 2월 : 고려대학교 정보보호학과 박사과정 수료
1986년 1월~현재 : 한국전자통신연구원 책임연구원
<관심분야> 개인정보보호, 바이오정보보호, 신뢰네트워크, 사이버국방

권 헌 영 (Hun-yeong Kwon)

1992년 2월 : 연세대학교 법학과 졸업
1998년 2월 : 연세대학교 법학과 석사
2005년 2월 : 연세대학교 법학과 박사
2015년 9월~현재 : 고려대학교 정보보호대학원 부교수
<관심분야> 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부

박 혜 숙 (Hea-sook Park)

1992년 2월 : 경성대학교 전산통계학과 졸업
1994년 2월 : 부산대학교 이학석사
2005년 8월 : 충남대학교 이학박사
1994년 2월~현재 : 한국전자통신연구원 실장
<관심분야> 고신뢰네트워킹, 특수목적망 설계

임 종 인 (Jong-in Im)

1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
현재 : 고려대학교 정보보호대학원 및 사이버국방학과 교수, 대검찰청 디지털수사자문위원회 위원장, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
<관심분야> 사이버안보, 사이버국방, 정보법학, 디지털포렌식, 개인정보보호 등