글로벌 바이오정보 프라이버시 논점 분석을 기반으로 한 바이오정보 보호 가이드라인 개선 방안

정 부 금*, 권 헌 영**, 박 혜 숙***, 임 종 인****

요 약

프라이버시는 개인의 사생활이나 사적인 일이 타인에게 공개되지 않을 권리를 뜻한다. 바이오정보는 그 사람 자체에 대한 가장 사적인 개인정보로 기술이 발전함에 따라 개인 식별뿐만 아니라 개인에 대한 분석 및 판단까지도 가능하다. 개인정보보호법은 글로벌 프라이버시 원칙들을 기반으로 하여 만들어 졌으나 바이오정보보호를 위한 법제는 아직 제정되어 있지 않으며, 가이드라인으로 규정되어 있다. 이에 바이오정보를 일반 개인정보보다 더욱 민감한 정보로서 보호해야 할 시점에 이르러 바이오정보 보호를 위한 국제적인 프라이버시 논의들을 살펴보고 최근 개정된 바이오정보 보호 가이드라인을 개선할 수 있는 프라이버시 원칙들과 바이오정보의 활용을 위한 조치 사항을 제안하고자 한다.

Improvement Proposals for Biometric Information Protection Guideline based on the Analysis of Global Bio Information Privacy Issues

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

ABSTRACT

Privacy means the right not to interfere with the private life of an individual. Bio data is the most private personal information about the person itself, and according to advancement of technology, it is possible to analyze and judge individual as well as identify individual. The Personal Information Protection Act is based on global privacy principles, but the legislation for the protection of bio information has yet to be enacted. Therefore, it is time to protect biometric data as more sensitive information than general personal information. We will review the global privacy discussions for protecting biometric information and propose additional privacy principles and measures for utilization that should be defined in the biometric information protection guideline.

Key words : biometrics, 바이오정보, 개인정보보호, 프라이버시 원칙, 바이오 정보보호 가이드라인

접수일(2018년 8월 28일), 수정일(1차: 2018년 9월 23일), 게재확정일(2018년 9월 29일)

* 고려대학교 정보보호대학원 박사과정 & ETRI
** 고려대학교 정보보호대학원 교수
*** ETRI 국방신뢰인프라연구실 실장
**** 고려대학교 정보보호대학원 교수(교신저자)

1. 서 론

영화 쥬라기 월드 2018에서는 손바닥인증으로 비밀의 문이 열리고, 미션 임파스블 2018에서는 손가락의 혈액을 이용해 인증하는 시스템[1]이 등장한다. 영화에서 첨단 미래 기술로 예측하는 생체인식이 현재 스마트폰과 금융, 쇼핑 등 일상적인 생활에서 사용되고 있어 이제는 현실로 다가오게 되었다. 사람의 생체정보를 이용한 본인 확인 기능은 비밀번호나 보안카드처럼 암기하거나 소지할 필요가 없어 편리하기는 하지만 한번 유출되면 바꿀 수도 없으며 자신의 민감한 신체 정보가 유출되는 것으로 개인의 프라이버시 침해가 더욱 우려되는 상황이다.

최근 바이오정보와 프라이버시에 관한 가장 큰 논란을 불러일으킨 사건은 인도 정부의 인디아 스택이라는 일종의 생체주민증 제도이다[1]. 12억 국민 모두의 지문과 홍채 정보를 디지털화 하여 민간기업에서 상업적으로 활용이 가능하도록 추진하고자 하였는데, 인권단체는 자신의 정보가 개인의 동의 없이 정부에서 제공된다는 점에서 프라이버시 침해라고 주장했다. 오랜 공방 끝에 2017년 8월 인도 대법원은 프라이버시를 기본권으로 인정하는 판결을 내리게 되었다.

유럽연합(EU)은 1995년 발의된 '개인정보 지침'을 2016년 '개인정보보호규칙'으로 대체하면서 개인정보에 생체정보의 개념을 포함시켰다. 일본의 경우 생체정보를 법령에 도입하진 않았지만 개인정보의 하나로 인정해 개인 정보 보호체계를 적용하고 있다. 하지만 아직까지 세계적으로 생체정보의 유출 시 따로 마련된 보안책은 없다. 실리콘 위조지문 제작, 독일 해커단체 CCC의 푸틴 러시아 대통령 홍채 복사, 미국 에너지국 직원 정보 해킹 등 생체 정보 위조와 유출 사례는 국내외로 빈번하게 발생하고 있다[2]. 그러나 현재 국내에서 생체정보 보호에 대한 직접적 개별적으로 규율하는 법률은 없다. 정부의 '바이오정보 보호 가이드라인'은 2005년 제정되고 2007년 1회 개정된 상태로 지속되어 왔으나 최근 바이오정보 활용 서비스의 활성화로 인하여 바이오정보보호의 필요성이 대두되어 2017년 12월 개정안이 발표되었으며, 현재 바이오정보 보호의 필요성은 더욱 중요해지고 있다.

이에 본 논문에서는 바이오정보의 개념에 대해서 고찰하며 국제적으로 논의되고 있는 바이보정보 프라이버시 논의들을 분석하여 최근 개정된 바이오정보 보호 가이드라인에서 규정하고 있는 보호 원칙들에 추가적으로 정의되어야할 프라이버시 원칙들과 바이오정보의 활용을 위한 조치사항을 제안하고자 한다.

1) 본인임을 인증하기 위한 수단으로 기존에는 지문, 걸음걸이, 홍채 등을 이용하는 장면이 등장했으나, 손가락을 찔러 피를 내어 본인 인증을 하는 더욱 강력한 생체 인증을 보여주는 장면이 등장함

2) 2016년 3월 금융보안원 자료

2. 바이오정보의 개념

바이오정보에 해당하는 영어의 biometrics는 biometric data라는 용어에 대응되는 것으로 bio와 측정을 뜻하는 metrics의 합성어로 살아있는 개인의 신체적인 특징을 자동화 처리에 의하여 측정 및 인식하여 데이터화한 것을 의미한다. 즉, 바이오정보는 바이오인식 데이터의 의미로 사용한다.

Biometrics는 선천적인 특징과 후천적인 특징으로 구분할 수 있다. 인간이 태어나면서부터 갖게 되는 선천적인 생리학적 특징들로 DNA 샘플, 지문, 손바닥 정맥, 지정맥, 손모양, 홍채, 망막, 얼굴 영상 등이 있으며 이러한 생리학적 특징은 대부분 일생동안 변하지 않는다는 특징을 갖는다. 행동적, 후천적인 특징들로 필체, 키보드 타이핑 리듬, 걸음걸이 패턴, 음성 패턴 등이 있으며, 이러한 행동적인 특징은 살아가면서 의식적 혹은 무의식적으로 바뀔 수 있다.

2.1 국제규범에서 바이오정보의 개념

OECD Biometrics 보고서[2]에서는 biometrics를 개인을 알아내거나 확인하기 위하여 신체적, 행동적 특징을 자동화된 방법으로 측정하여야 하며, 자동화된 방법으로 인식 혹은 검증을 할 수 있는 개인의 유일하고 측정 가능한 특징이라고 정의하고 있다. 수동으로 사진을 비교하는 것은 포함되지 않는다.

IBIA[3]에서는 biometrics와 biometric data를 구분해서 정의하고 있다. Biometrics는 자동인식에 사용되어 질 수 있는 측정 가능한 신체적(해부학적, 생리학적), 행동적 특징을 말하며, 이는 반드시 자동화된 방법으로 인식해야 한다. Biometric data는 이러한

자동인식 과정에서 생성되는 모든 데이터로 정의하고 있다. 자동인식 과정에서 생성되는 데이터란 원본 바이오정보와 관련되어 파생 혹은 추출된 샘플, 모델, 템플릿, 유사도 등을 포함한다.

EU GDPR[4]에서는 Article4(14)에서 biometric data를 살아있는 개인의 신체적, 생리적, 행동적 특성과 관련되어 기술적 처리로부터 도출된 개인정보로 정의하고 있다. 이러한 바이오정보를 사용하여 얼굴 영상이나 지문검사 정보처럼 자연인을 유일하게 확인하거나 접근이나 출입을 허용할 수 있다. 즉, 유일하고 변함없어야 한다는 개인정보로서 바이오정보의 조건, 자동 처리되어야 한다는 처리조건, 얼굴, 지문 등의 특징을 사용한다는 점, 인식과 허용 등의 용도에 사용할 수 있다는 것을 정의하고 있다.

2.2 국내규범에서 바이오정보의 개념

방송통신위원회와 한국인터넷진흥원의 바이오정보 가이드라인[5]에서는 바이오정보는 지문, 홍채, 음성, 필적 등 개인의 신체와 행동의 특징적인 정보로서 본인임을 판단하기 위하여 기술적 처리[3]가 되는 개인정보를 말하고, 바이오정보는 '원본정보'와 원본 정보로부터 특징 값을 추출하여 생성된 템플릿이라 부르는 '특징정보'로 구분하여 정의하고 있다.

또한, 행정자치부의 개인정보의 안전성 확보조치 기준[6] 및 방통위의 개인정보의 기술적·관리적 보호조치 기준[7]에서는 바이오정보라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다고 정의하고 있다.

전자금융거래법[8]에서는 생체정보를 접근매체의 한 유형으로 정의하고 있으며, 한국인터넷진흥원(KISA) 정보보호산업지원센터[9]에서는 바이오인식 정보라는 용어로 정의하고 있고, DNA보호법[10]에서는 디엔에이신원확인정보란 개인 식별을 목적으로 디엔에이감식을 통하여 취득한 정보로서 일련의 숫자 또는 부호의 조합으로 표기된 것으로 정의하고 있다.

2.3 바이오정보의 법적 지위

바이오정보는 특정인으로 판단할 수 있는 정보로서 개인정보로서의 법적인 지위를 갖는다. EU GDPR Article9[4]에 따르면 인종 또는 민족의 기원 데이터, 유전자 데이터, 생체 인식 데이터, 건강 관련 데이터를 특별한 범주의 개인정보로 정의하고 있어 GDPR에서의 개인정보 처리에 관한 모든 규정을 적용받는다. 국내 개인정보보호법에서도 제23조에서 바이오정보를 자연인에 관한 개인의 민감정보로 정의하고 있다.

3. 글로벌 바이오정보 프라이버시 논의 분석

바이오정보는 개인정보로서의 법적인 지위를 가지며 이에 따라 예외적인 경우를 제외하고는 원칙적으로 처리가 금지된다. 이러한 개인정보보호 원칙과 관련한 국제적인 논의에는 OECD 프라이버시 8원칙[11], ISO/IEC 29100 프라이버시 11원칙[13], APEC 프라이버시 9원칙[12] 등이 있으며, 이러한 원칙들에 기반을 두어 각국의 개인정보보호법 등이 제정되었다[14]. 이와 더불어 본 장에서는 일반 개인정보보다 민감하고 유출시 더욱 심각한 피해를 가져올 수 있어 더욱 신중히 다루어야 할 바이오정보의 프라이버시에 관한 특별한 국제적인 논의들에 대하여 분석한다.

3.1 IBIA 바이오정보 프라이버시 권장 사항

IBIA[5]는 미국에서 설립된 국제 바이오정보 산업 연합으로 바이오인식정보를 상업적으로 사용하고자 할 때 필요한 바이오정보 프라이버시 보호 권장 사항들을 제시하고 있다[3]. 주요 내용은 다음과 같다.

바이오인식 기술이 개인 식별 외의 목적으로 사용되는 경우에는 개인에게 이를 통지하여야 한다. 바이오인식 정보에 대한 여러 상황-자발적 혹은 비자발적으로 바이오인식 정보를 등록할 경우, 캡쳐 및 저장하는 비 바이오인식 정보의 종류를 지정할 경우, 그 데이터가 어떻게 사용될 것인가를 결정하는 경우, 데이

3) '기술적 처리'란 IoT 센서, 입력단말을 사용하여 생체정보를 입력받고, 원본 정보로부터 특징점을 추출하기 위해 전자적으로 처리되는 전 과정을 말함

4) special categories of personal data

5) International Biometrics & Identification Association (국제 바이오인식 산업 연합)

터가 제공될 개인에 대한 고지 범위를 결정하는 경우, 등록자에게 부과 될 수 있는 위험 요소와 위해 요소가 존재하여 이를 알려야 할 경우-에 따라 개인에게 옵트인[6] 또는 옵트아웃[7] 기회를 제공하여야 한다.

바이오인식 기술의 구현자와 운영자는 개인 정보 보호 정책을 게시하고 개인 정보 보호 원칙을 열거하여 포함하여야 하며, 캡처/저장되는 바이오인식 데이터 유형과 목적을 특정해야 한다. 수집한 바이오인식 정보는 합리적으로 결정된 보유 기간을 명시하고 보유 기간 결정 정책이 합리적임을 명시해야 한다. 정의된 바이오인식 정보만을 수집하고, 정의된 목적에 해당하는 사유로만 수집해야 한다.

수집된 바이오인식 데이터의 정확성과 완전성을 유지해야 한다. 스스로 초기 등록 혹은 재등록은 위조에 취약할 수 있으므로, 바이오인식 데이터 등록, 삭제를 위한 대면 컨택 포인트를 포함한 데이터 수정 매커니즘을 제공해야 한다. 바이오인식 데이터에 대한 접근은 지정된 사람과 응용프로그램에 의해서만 가능해야 한다. 유용한 사이버보안 활동을 통하여 수집되어 보관 중인 바이오인식 혹은 그 외 관련된 정보를 보호해야 한다. 사이버 또는 기타 프라이버시 침해가 발생하는 경우 정보 유출을 막기 위해 응용 프로그램에서 허용하는 범위 내에서 데이터의 연결을 끊어야 한다. 저장된 데이터와 전송되는 데이터는 암호화하여야 한다.

바이오인식 데이터를 제공한 사용자에게 저장되고 있는 현재의 데이터 내용을 요청할 수 있는 메커니즘을 제공하여야 하고, 게시된 목적에 충분한 감사 로그를 유지함으로써 권장 사항을 준수해야 하며, 독립적인 바이오인식 정보보호 정기 감사를 실시해야 한다.

바이오인식 정보를 포함한 개인의 사적인 정보가 침해당했다고 생각하는 경우 소비자의 대응 절차 대한 매뉴얼이 있어야 하며, 개인정보 침해 우려가 제기되었을 때를 위한 연락처 정보가 공개되어 있어야 한다. 또한 신원 확인을 위해 사용된 바이오인식 정보의 취소, 삭제 또는 변경을 포함하여 가능한 구제책이 제공되어야 한다.

3.2 OECD 바이오정보 프라이버시 이슈

개인정보보호에서 가장 기본이 되는 프라이버시 8원칙을 제시한 OECD에서는 추가적으로 바이오정보를 위한 프라이버시 침해 위험이 발생할 수 있는 주요한 이슈들을 제기하고 있다[2].

펑션 크리프(목적 크리프)는 하나의 특정 목적을 위해 수집된 데이터가 연속적으로 의도하지 않거나 허가되지 않은 다른 목적으로 사용되기 위한 프로세스 또는 시스템으로 확장되는 것을 말하는 용어이다. 프라이버시 원칙의 용어로, 목적 크리프는 최종성 원칙을 위반하는 것으로 생각할 수 있다. 즉, 개인의 동의와 합의 없이 데이터 수집 시 정한 목적과 다르게 데이터의 보유, 공개 등으로 사용하는 것을 말한다.

생체 인식 기술이 감시 및 사회 통제의 기술이 될 것이라는 우려가 가능하다. 생체 인식 정보는 아마도 궁극적인 개인 식별자로서 정보 사회의 불길하고 비인도적인 측면, 즉 비교할 수 없는 양의 개인 정보가 체계적으로 수집되고 사용될 수 있는 사회를 촉진시킬 가능성이 있는 것으로 보일 수 있다.

생체 인식 식별자를 사용하면 데이터 사용 시 또는 데이터베일런스[8]를 통해 감시가 쉽게 수행 될 수 있다. 모든 전자 거래가 생체 인식 인증을 필요로 하는 곳에서 거래 데이터에 액세스 할 수 있는 사람도 개인에 대한 자세한 정보를 알게 된다[15]. 개인의 생체 정보만 알고 있으면 암호, 주민번호 등 개인에 관한 정보가 없어도 또한 데이터 주체의 동의와 상관없이 거래 데이터에 연결이 가능하다는 위험이 있다.

또한, 식별 또는 확인의 토큰으로 사용되는 생체 인식 템플릿이 현재 대부분의 생체 인식 공급 업체에 의해 판매되는 경우 개인 정보를 침해하고 개인의 자유를 위태롭게 할 수 있다. 또한 저장된 템플릿과 비교하여 확인 또는 식별을 기반으로 할 때 국가 응급 상황 발생 시 등 필요 시 기업이나 정부가 개인 정보를 침해 할 위험이 존재한다[16].

6) 개인이 먼저 자신의 데이터 수집을 허용해야만 데이터 수집을 할수있는 방식으로 기업, 단체가 광고성 메일을 보낼 때, 사전에 동의를 한 사람에게만 메일을 발송하는 방식

7) 옵트인과 반대되는 개념으로, 자신의 데이터 수집을 허용하지 않는다고 표명할때 정보수집이 금지되는 방식으로 기업, 단체는 광고성 메일을 모든 수신자에게 일단 보내고 난 후, 수신자가 발송자에게 수신거부 의사를 밝히면 이후부터는 메일을 발송하지 않는 방식

8) (신조어) 데이터 감시능력. 신용카드 구매, 휴대전화 통화, 인터넷 사용으로 인해 생겨난 개인정보의 흔적을 연구하여 개인의 생활을 감시하는 능력

특정 생체 인식은 개인의 동의 또는 적극적인 참여없이 또는 알지 못하는 사이에 사용될 수 있다. 영국에서는 폐쇄 회로 TV (CCTV) 기술이 도시 거리에서 범죄자의 인식을 자동화하는 안면 인식 기술과 결합되고 있다. 구매자가 얼굴 인식을 사용하여 구매 습관을 추적하도록 하는 안면 인식 시스템이 가능하며, 이 경우 각각 피사체 개인은 안면 인식이 수행되고 있는지도 모를 것이다. 홍채 스캐닝은 이미 피사체로부터 상당한 거리 (18 ~ 24 인치 범위)에서 수행 할 수 있다. 기술이 향상됨에 따라 홍채 획득은 사용자가 개입하지 않아도 훨씬 먼 거리에서 이루어질 수 있다. 프라이버시 관점에서 이러한 상황은 수집 제한, 공개 및 목적 지정 원칙과 충돌 한다.

DNA에 의한 식별의 가장 큰 위험 중 하나는 개인 식별 외의 목적으로 DNA 신원 정보를 사용하는 목적 크리프를 범하는 경우이다. 개인의 DNA 구성에 기초하여 건강 관련 결론을 도출할 수 있기 때문이다. 대규모 DNA 기반 신원 확인 시스템이 구축되면 이 정보를 보험 회사, 금융 기관 등 유망한 사용자들이 위험 분석 및 연구 목적으로 DNA 프로필에 액세스해야 한다는 상당한 압력이 있을 것이다.

3.3 IBG BioPrivacy Best Practices

국제바이오 정보그룹[9]은 “바이오 프라이버시 계획의 모범 사례[10]”로서 다음과 같은 4가지 범주 내 25개 항목을 제시하였다.[17]

범위와 기능 범주에서는 원래 의도한 것보다 넓은 범위의 검증・식별 기능 수행을 금지하고, 바이오인식 정보를 범용 식별기준으로 사용 금지, 시스템에 특정 용도로만 보관하고, 종료 시 폐기하여야 하며, 시스템의 원래 용도뿐만 아니라 잠재적 용도까지 고려하여 프라이버시 리스크 평가, 바이오인식 정보 외의 다른 정보의 수집・보관은 식별・검증 목적에 필요한 최소한으로 제한하여야 하며, 템플릿을 보관하고, 원칙적으로 원본 데이터 보관은 금지하고 있다.

데이터의 보호 범주에서는 대조 이후의 데이터 전송의 보호, 바이오인식시스템 및 데이터에 대한 접근 제어, 바이오인식 정보의 개인정보와의 분리 보관 (논리적・물리적), 프라이버시를 침해하는 시스템의 종결 수단 마련하도록 되어있다.

정보주체의 통제 범주에서는 정보주체의 바이오인식 정보 제어권 및 폐기 요청권 보장, 정보주체의 바이오인식 정보와 관련하여 수집한 정보의 수정권 및 열람권 보장, 정보주체가 익명 등록이 가능하도록 설계하여야 한다고 정의하고 있다.

공개·감사·책임·감독 범주에서는 운영자로서의 책임 부담, 독립된 감사기관의 시스템 감사 및 감독, 감사 데이터의 완전 공개, 바이오인식 시스템 구현목적의 완전 공개, 정보주체가 바이오인식 시스템에 등록한 경우 그 사실의 공개 의무, 명시적인 허가 없이 바이오인식 대조가 이루어지는 경우 그 사실을 정보주체에게 공개하여야 하며, 바이오인식 시스템 등록이 필수인지 선택인지의 공개 의무, 선택인 경우 대안의 마련 의무, 시스템 운영 및 감독을 책임지는 사람이나 단체의 공개, 등록・인증 및 식별 과정의 공개, 바이오인식 정보 보호 방법 및 인식 시스템의 보호 체계 공개, 대체 인증 프로세스의 공개 및 대체 인증자에 대한 차별 없는 서비스를 제공해야 함을 명시하였다.

3.4 EU GDPR

EU GDPR[4]에서는 원칙적으로 유전자 정보, 생체정보, 건강 관련 정보 등 민감 정보 처리를 금지하면서, 정보주체의 명백한 동의, 방어권 행사, 공개된 개인정보 등의 경우에는 예외적으로 허용한다.

프로파일링(개인정보 자동처리 형태)의 개념을 정의하고, 정보주체에게 프로파일링 처리 필요성 및 처리 후 예상 결과 등 고지의무를 규정하고, 프로파일링을 받지 않을 권리 명시한다. 프로파일링은 개인정보를 분석하여 개인의 특정한 측면(업무능력, 건강, 관심사, 행동, 위치 등)을 예측하기 위한 개인정보의 자동처리 형태를 의미한다.

개인정보에서 식별성을 제거하는 것을 익명화와 가명화로 구분하고, 익명화된 데이터는 더 이상 개인정보가 아니며, 가명화된 정보는 공공기록 보존, 과학·역사 연구, 통계 목적으로 하는 경우 정보주체 동의없이 이용할 수 있으나 여전히 개인정보이므로 보호조치가 필요하다. 가명화란 추가 정보의 사용 없이는 특정 정보주체를 식별할 수 없도록 처리된 개인정보로

9) International Biometric Group: IBG
10) Bio Privacy Initiative – Bio Privacy Best Practices

정의하였다.(GDPR 제4조)

시스템 최초 설계 시점부터 개인정보보호를 고려하도록 하고, 기본 설정으로 필요한 목적 하에서만 데이터의 처리가 가능하도록 하는 방식으로 시스템을 운영해야 한다고 제시하였다.

4. 바이오정보 보호 가이드라인의 주요 내용

행정자치부에서 2017년 12월 개정한 바이오정보 보호 가이드라인[5]에서는 바이오정보의 안전한 활용을 위해 다음과 같은 6대 보호원칙을 제시하고 있다.

비례성의 원칙에서는, 바이오정보를 사용하는 사업자는 위험과 편익을 비교하여 수집 및 이용 여부를 판단하고, 바이오정보의 종류에 따른 특징을 반영하여 침해 위험이 최소화되도록 서비스하여야 한다.

수집·이용제한의 원칙은 사업자는 바이오정보의 이용 목적, 수집 정보, 유지기간을 사용자에게 고지하고 동의를 받아야 하며, 템플릿 생성 후 원본정보는 파기해야 한다. 원본정보를 보존하려면 그 이유 및 보존기간을 고지 후 동의를 받아야 한다.

목적제한의 원칙은 바이오정보의 활용은 고지한 목적에 대해서만 사용해야 한다는 것이다. 예를 들면, 식별 목적으로 이용자에게 동의를 받고 질병 분석 등의 용도로 활용해서는 안 된다. 다른 목적으로 활용하려면 사전 동의를 받는 등 법적인 근거가 있어야 한다.

통제권 보장의 원칙은 자신의 바이오정보를 스스로 수정하거나 삭제할 수 있도록 어렵지 않은 방법을 제공해야 한다는 것이다. 특히, 아동이나 신체적 장애가 있는 경우 본인이 원하지 않을 경우 등을 대비하여 다른 정보를 사용할 수 있도록 하는 것도 필요하다.

투명성 원칙으로 바이오정보 보호에 관한 사항을 알기 쉽게 안내하고 문의를 접수하기 위한 기능을 운영해야한다는 것이다.

바이오정보 중심 설계 및 운영 원칙은 서비스의 초기 설계부터 바이오정보 보호를 위한 기본 값 선택 등의 방안을 포함해야 하고, 바이오정보를 서버로 모아서 일괄 처리를 하려면 개인정보 영향평가를 실시해야 한다는 것이다.

또한 추가적으로 기술적 관리적 보호 조치에서는 바이오정보의 보안에 관한 내용으로 안전성 확보 및 정보보안 원칙에 해당하는 내용들을 정의하고 있다.

5. 바이오정보 보호 가이드라인 개선 방안

본 장에서는 국제적인 바이오정보 프라이버시 논의들을 기반으로, 가이드라인에서 명시하고 있는 보호원칙들에 추가적으로 규정이 필요한 프라이버시 원칙들과 바이오정보의 활용을 위하여 익명화 및 가명화 조치 정의가 필요함을 제시한다.

5.1 바이오정보 책임성 원칙

프라이버시에서 책임성이란 정보 관리자가 다른 원칙들을 효과적으로 준수 할 수 있도록 기반을 마련해야 함을 의미하며[2], 책임성의 원칙은 최근 사용기관의 의무를 강화하기 위해 새롭게 주목 받고 있다. 2014년 개정된 OECD 가이드라인은 새로 추가된 “책임성 이행” 항목에서 책임의 원칙을 실현하기 위한 세부 방안으로 프라이버시 관리 프로그램을 수립하도록 하고 있다[18]. 바이오정보는 일반 개인정보보다 민감도가 높은 개인정보로 높은 프라이버시 위험평가와 보호조치가 필요하다. 따라서 급속히 바뀌는 환경에 따라 주기적으로 검토 및 갱신되어야 하며 내부관리계획의 수립 의무를 부과하여야 하며, 기업 내 개인정보보호 책임자에 바이오정보의 보호에 대한 책임을 추가하여야 할 것이며 특히 바이오정보의 위탁이나 제3자 제공시 바이오정보 처리자의 법적 책임 등 통합적인 바이오정보 프라이버시 관리 체계를 수립으로 바이오정보 책임성을 명확히 지키도록 규정하여야 할 것이다.

5.2 바이오정보의 정확성 유지 원칙

바이오정보에 있어서 정확성은 일반 개인정보의 정확성보다 더욱 중요시 되어야 하는 원칙이다. 일반 개인정보의 경우 수정이나 변경이 가능하지만 바이오정보가 잘못될 경우 본인이 본임임을 인증 받지 못하는 결과를 초래하기 때문이다.

데이터 처리의 모든 과정에서 위·변조되는 것을 방지하여 데이터의 정확성과 완전성을 유지해야 한다. 바이오인식 데이터 등록 및 삭제 시 본인임을 인증한 데이터 수정 체계를 제공해야 한다. 또한 바이오정보의 처리과정에서 데이터는 하드웨어, 데이터베이스, 처리자 등의 여러 요소가 개입되며 각 요소에서의 처리과정에서 데이터가 통합, 재분류되는 경우 처리 프로그램의 내재적 문제, 하드웨어 오동작 처리자의 실수 등에 의해 복합적인 이유로 왜곡이 일어날 수 있다. 이러한 데이터 모든 처리 과정이 고려된 정확성 유지 원칙이 지켜져야 함을 명시할 필요가 있다.

5.3 바이오정보의 프로파일링 금지 원칙

바이오정보의 프로파일링은 개인의 성향적, 행동적 특성을 분석 및 예측하기 위해 바이오정보를 자동 처리하는 것을 의미한다. 기존의 일반 개인정보의 프로파일링으로서는 개인의 관심사, 위치 등을 분석하여 광고나 마케팅 등을 위해 사용될 수 있으나 바이오정보의 자동처리를 통해서는 개인의 내적인 건강, 유전적인 특징을 노출하게 되는 위험이 있다. 가장 정밀한 바이오정보로 볼 수 있는 DNA에 의한 프로파일링의 가장 큰 위험 중 하나는 개인 식별 외의 목적으로 DNA 정보를 사용하게 되는 경우이다. 인간 게놈에 대한 연구와 함께 DNA 프로파일링은 개인의 DNA 구성에 기초하여 잠재적 건강 관련 결론을 도출할 수 있기 때문이다. 입사 시험, 보험 가입 등에서 이러한 DNA 정보에 기반으로 미래의 질병 및 잠재된 성향을 판단하여 입사를 거부당하거나 보험 가입이 취소될 수 있을 것이다. 바이오정보 프라이버시를 위해서는 이러한 프로파일링이 금지되어야 하며 프로파일링에 대한 거부권이 보장되어야 한다.

5.4 바이오정보의 익명화, 가명화 조치

바이오정보의 보호를 위한 프라이버시 원칙 및 기술적 관리적 보호 조치 외에 가이드라인에서는 활용을 위한 조치 사항을 담아서 보호와 활용의 균형을 이룰 수 있도록 해야 할 것이다. 이에 바이오정보의 활용을 위해서는 바이오 정보에서 개인 식별 정보를 제거한 익명화, 가명화 조치가 필요한데 구체적인 방법 및 활용에 대해서는 개인정보 비식별화 가이드라인 등에서 다룰 수 있으며 원본정보나 특징정보에 대해 공공, 통계 목적으로 데이터를 이용 또는 보존할 경우에 대해 익명화 및 가명화에 관한 기본 원칙에 해당하는 내용들이 정의되어야 할 것이다.

6. 결 론

본 논문에서는 바이오정보 보호 가이드라인에 대해 검토하고 국제적인 논의를 기반으로 추가적으로 규정되어야 하는 보호 원칙들과, 보호와 더불어 활용을 위한 조치가 필요함을 제시하였다. 바이오정보는 단순히 본인임을 확인하는 인증 수단을 넘어서 개인에 관한 모든 정보 - 금융, 신용, 취향, 특성, 뿐만 아니라 신상, 건강, 유전력, 잠재력 등 그 사람에 관한 알 수 있는 모든 것 그리고 발생할 수 있는 모든 가능성까지를 담고 있는 방대한 데이터베이스의 압축판이라고 할 수 있다. 바이오정보에는 단순히 지문, 얼굴 뿐만 아니라 걸음걸이, 홍채, 음성, 혈액, DNA까지 신체적, 행동적, 유전적, 모든 특징들이 포함된다. 개인에 관한 모든 정보를 끌어낼 수 있는 핵심 키를 다 가지고 있다고 해도 과언이 아니다. 사물인터넷 및 모바일 기기가 확산되고 4차 산업혁명으로 모든 산업에 지능화에 따른 생체인식은 더욱 확산될 것으로 예상되는바 그만큼 적용되고 수집되고 처리, 분석되는 데이터의 절대량도 크게 증가할 것이다. 그런 관점에서 보면 특히, 프라이버시의 관점에서 보면 바이오정보는 개인의 과거와 미래를 알 수 있는 '개인정보의 지도'로 불러야 할지도 모른다. 바이오정보에 대해 프라이버시의 원칙이 더욱 구체적으로 정의되고 정책과 기술을 통해 시행되고 준수되어야 할 것이다.

참고문헌

[1] Parag Chatterjee Asoke Nath, "Biometric Authentication for UID-based Smart and

Ubiquitous Services in India," Fifth International Conference on Communication Systems and Network Technologies (2015).
[2] OECD, "Biometric-based Technologies," DSTI/ICCP/REG(2003)2/FINAL , 2004.
[3] IBIA, "Privacy Best Practice Recommendations For Commercial Biometric Use." Aug. 2014.
[4] EU GDPR (General Data Protection Regulation) (Regulation (EU) 2016/679).
[5] 방송통신위원회, 한국인터넷진흥원, "바이오정보보호 가이드라인," 2017.12.
[6] http://www.law.go.kr/법령/행정자치부의개인정보의안전성확보조치기준
[7] http://www.law.go.kr/법령/개인정보의기술적·관리적보호조치기준
[8] http://www.law.go.kr/법령/전자금융거래법
[9] https://www.kisis.or.kr/kisis/index.do
[10] http://www.law.go.kr/법령/디엔에이신원확인정보의이용및보호에관한법률
[11] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980.
[12] APEC, "APEC privacy framework," APEC, 2004.
[13] ISO/IEC 29100, "Information technology - Security techniques - Privacy framework," 2011.
[14] 염흥열, 고재남. "글로벌 프라이버시 원칙 비교분석." 정보보호학회지, 2013.
[15] O'Connor, "Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification", Stanford Technology Law Review, April 2004.
[16] Tomko, George, "The Fundamental Problem with Template-based Biometrics", presentation at the 12th Conference on Computers, Freedom and Privacy, San Francisco, 2002.
[17] Liu, N.Y., "Bio-privacy: Privacy regulations and the challenge of biometrics." 10.4324/9780203804087. 2013.
[18] The OECD Privacy Framework, OECD, 2013.

[저 자 소 개]

정 부 금 (Boo-geum Jung)
1986년 2월 부산대학교 계산통계학 학사
1991년 8월 숙명여자대학교 전자계산학 석사
2012년 2월 고려대학교 정보보호대학원 박사 수료
현재 한국전자통신연구원 책임연구원
email : bgjung@etri.re.kr

권 헌 영 (Hun-yeong Kwon)
1992년 2월 연세대학교 법학과 학사
1998년 2월 연세대학교 법학과 석사
2005년 2월 연세대학교 법학과 박사
현재 고려대학교 정보보호대학원 교수
email : khy0@korea.ac.kr

박 혜 숙 (Hea-sook Park)
1992년 2월 경성대학교 전산통계학과 학사
1994년 2월 부산대학교 이학석사
2005년 8월 충남대학교 이학박사
현재 한국전자통신연구원 국방신뢰인프라연구실 실장
email : parkhs@etri.re.kr

임 종 인 (Jong-in Lim)
1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 수학과 석사
1986년 2월 고려대학교 수학과 박사
현재 고려대학교 정보보호대학원 및 사이버국방학과 교수
email : jilim@korea.ac.kr