정 보 보 호 학 회 지
제 30 권 제5호, 2020. 10

4차 산업혁명 시대 신기술 서비스의 개인정보 처리 실태 및 침해요인

봉 기 환*

요 약

초연결사회인 4차 산업혁명 시대가 들어서면서 AI, IoT, 블록체인 등 새로운 기술들에 대한 개발과 서비스 수요가 늘어나고 있다. 4차 산업혁명 시대에 데이터는 미래 산업의 원유이고 정부는 데이터 경제 활성화를 위한 투자를 아끼지 않고 있다. 반면 데이터를 활용한 서비스의 증가로 개인정보 침해 위험성이 증가한다는 우려도 있다. 본 논문에서는 4차 산업혁명 시대에 데이터를 활용하는 신기술과 서비스를 분류하고 분야별 서비스에서의 개인정보 처리 실태 및 침해가능 요소와 개선방향에 대하여 제시한다.

Ⅰ. 서 론

컴퓨터, 인터넷, GPS, 스마트폰 등으로 대표되는 3차 산업혁명을 지나 지금은 AI를 비롯한 빅데이터, 로봇, IoT, 블록체인, 드론 등의 기술이 주를 이루는 4차 산업혁명의 시대이다.

3차 산업혁명 시대 정보사회는 사람과 사람의 연결을 지향하며 시간과 공간의 제약을 허물었다[1]. 4차 산업혁명 시대는 초연결사회로 사람과 사람뿐만 아니라 사물과 사물간의 연결 그리고 사람과 사물간의 연결을 가능케 하고 있다. 온라인과 오프라인의 경계도 허물어지고 학습을 통한 빅데이터에서 스스로 생각하는 AI로 진화하고 있다.

인간, 사물, 기계가 연결되어 온라인을 통해 데이터가 수집되고 분석되어 스스로 생각하는 AI가 맞춤형 상품을 제공해 주는 초연결사회에서 이 모든 과정은 데이터에 의해 만들어지고 이 데이터들의 대부분은 사람이 만든 개인정보를 포함한다. 4차 산업혁명 시대의 원유는 데이터이고 이 데이터에 개인정보가 포함되어 있는 만큼 인권을 위한 자기정보결정권 확보와 처리과정의 투명성, 개인정보 유출 예방을 위한 차세대 기술 보호조치가 필요하다.

일각에서는 신기술 서비스에 대한 개인정보의 필요 이상 수집, 동의 없이 가능한 제공, 투명한 개인정보의 처리 공개와 열람, 정정·삭제 등 권리 행사 가능 여부 등에 대한 해결책이 미흡하다고 지적한다.

미국의 경우 개인정보 처리가 Opt-out으로 규정되어 사업자의 데이터 수집과 이용·제공이 상대적으로 원활한 반면 국내 사업자의 경우 사전동의 규정으로 인하여 데이터 활용에 아직 소극적이다. 가명정보의 도입과 일정 목적 내 동의 없이 가능한 가명정보의 처리, 결합 절차의 기준, 반출 기준을 개인정보보호법 개정을 통해 마련하였으나 가명처리 및 결합을 통해 개인정보가 재식별 될 가능성에 대한 우려는 계속되고 있다.

4차 산업혁명의 신기술 중 AI와 IoT를 활용한 자율주행자동차와 AI스피커 등 현재 상용화가 되었거나 사용화를 준비 중인 서비스에서 개인정보에 대한 문제점들이 지적되고 있으나 기타 다른 서비스들이 사업을 준비 중인 상황에서도 개인정보의 무분별한 처리 가능성에 대해서 예측만으로 정보주체가 인식하지 못하고 컨트롤할 수 없는 경우가 많다고 우려하고 있다. 이에 본 논문에서는 4차 산업혁명 시대에 활용될 수 있는 기술들을 자세히 분류해 보고 서비스 내 데이터 처리과정에서 개인정보보호의 원칙과 법률에 위반되는 사항들이 존재하는지 검증해보고자 한다.

본 논문은 2장과 3장에서 신기술 유형의 현황과 개인정보가 처리되는 서비스를 분석하고, 4장에서는 주요 신기술 서비스에서의 개인정보 처리 과정과 침해요인을

* 한국인터넷진흥원 (연구원, khbong@kisa.or.kr)

검증한다. 마지막으로 5장에서 개선방안을 제시하고 결론을 내린다.

Ⅱ. 4차 산업혁명 시대의 신기술 서비스

여기서는 신기술의 유형 구분 현황을 살펴보고 기초과학, 핵심기술, 응용기술 등을 정의하고 단계별 분류체계를 정한다.

2.1. 신기술 유형

신기술에 유형은 기초과학, 핵심기술, 응용기술 등의 기준에 따라 다양하게 분류되어 있다.

4차위 관계부처 합동으로 4차 산업혁명 대응 계획인 I-KOREA 4.0은 기초과학 기술로 AI, 빅데이터, 클라우드, IoT, Mobile을 분류하고 블록체인, 웨어러블, AR/VR, V2X 등을 응용기술로 분류하였다('17.11).

과학기술정보통신부는 '2018년 ICT R&D 기술로드맵'을 발표하면서 ICT연구개발 기술분류체계를 마련하였으며 미래통신·전파, SW·AI, 방송·콘텐츠, 차세대보안, 디바이스, 블록체인·융합을 대분류로 구분하였다. 인공지능, 빅데이터, 클라우드컴퓨팅, 웨어러블, 자율주행, 블록체인, IoT 등을 중분류로 구분하였다('18.10).

'19년 4월 관계부처 합동으로 발표한 5G플러스 전략에서는 활용성, 시장성, 국내 경쟁력, 정책지원 필요성 등을 종합 고려하여 5G Core, 5G+ Device, 5G+ Service로 구분하였다. 네트워크와 차세대 스마트폰을 5G Core로 분류하고, VR/AR, 웨어러블, 지능형CCTV, 드론, 로봇, V2X를 5G+ Device로 분류하였다. 관련 핵심서비스로는 실감콘텐츠, 스마트공장, 자율주행차, 스마트시티, 디지털 헬스케어를 선택하였다.

유럽의 특허청은 '17년 12월 4차 산업혁명 기술과 특허 보고서에서 7대 핵심기술을 빅데이터, VR/AR, 3D프린팅, AI, IoT, 에너지, 보안으로 정하고 관련 서비스를 영역으로 구분하여 개인, 가정, 교통수단, 사업, 생산, 인프라로 분류하였다.

영국의 컨설팅 기업인 PWC(Pricewaterhouse Coopers)는 비즈니스 관련 8가지 핵심 기술로 AI, 증강현실, 블록체인, 드론, IoT, 로보틱스, VR, 3D프린팅을 선정하여 사업을 추진하고 있다.

2.2. 신서비스 유형

4차위 I-KOREA 4.0에서는 신기술 관련 서비스를 14개로 분류하였으며, 스마트시티, 자율자동차, 스마트공장, 스마트에너지, 스마트환경, 맞춤형교육, 의료, 바이오 등으로 구분하고 있다. '16년 신산업 민관협의회에서 발표한 '4대 트렌드 변화에 대응한 신산업 발전방향 및 중점분야'에는 자율자동차, IoT가전, 로봇, 바이오헬스, 드론, AR/VR 등을 신산업 중점분야로 선정하였다.

과학기술정보통신부 ICT R&D 기술로드맵에서는 신기술 관련 서비스가 아닌 기술 세분류를 지정하였으며, 빅데이터 활용, 클라우드 기술, VR/AR, 바이오 인증, 웨어러블, 차량 V2X통신, 3D프린팅, 블록체인 네트워킹, IoT 디바이스 등으로 구분하고 있다.

2.3. 신기술 및 서비스 분류

본 논문에서는 신기술 유형을 핵심기술과 응용기술로 구분하고, 핵심기술은 AI, 빅데이터, IoT, 클라우드, 디바이스, 블록체인으로 구분한다. 그 외 VR/AR, V2X, 5G, 안면인식, 음성인식, 공간인식, 웨어러블, 3D 프린팅, 신소재, 신재생에너지 등 기술들은 응용기술로 구분하도록 한다.

신서비스의 유형은 기술의 융합에 따라 한가지 서비스에서 다양한 기술이 적용될 수 있으므로 신기술의 유형과 일대일 매칭 또는 세분류를 하지 않고 분야별로 구분하도록 한다.

4차 산업의 서비스는 크게 공공 분야, 교통 분야, 금융 분야, 생활 분야, 의료 분야로 분류하였다. 공공 분야는 주로 인프라, 환경, 도시, 소재, 에너지 산업과 관련되며 O2O, 스마트 유통, 재난예측, 스마트 그리드 관련 서비스가 포함된다. 교통 분야는 물류, 유통, 제조, 교통, 이동체, 운송 산업과 관련되며 무인이동체, 지능형 교통체계, 자율주행 자동차 등과 관련된 서비스가 포함된다. 금융 분야는 대출, 거래, 투자, 보험 산업과 관련되며 핀테크, 스마트 금융, P2P 대출, 스마트 계약, 생체인증, 가상화폐 챗봇 등과 관련된 서비스가 포함된다. 생활 분야는 안전, 도시, 주거, 교육, 통신, 문화 산업과 관련되며 VR/AR, 맞춤형 교육, 스마트 홈 등과 관련된 서비스가 포함된다. 의료 분야는 건강, 보건, 복지, 바이

오 산업과 관련되며 원격의료, 헬스케어, 수술 로봇 등과 관련된 서비스가 포함될 수 있다.

Ⅲ. 신기술 서비스 내 개인정보가 처리 현황

여기서는 신기술 및 신서비스에서 처리되는 데이터 중 개인정보가 포함되어 수집・이용・제공 등 처리되는 유형을 분류하고 처리되는 개인정보의 유형과 침해요인이 될 수 있는 형태를 구분한다.

3.1. 개인정보 관련 신기술 및 신서비스 분류

프랑스의 개인정보보호 감독기구인 CNIL은 현재 개인정보와 관련한 신기술을 9개로 구분하여 사업을 추진하고 있으며, 생체인식, 쿠키, 사이버 보안, AI, IoT, 영상, 블록체인, 시민기술, 개발로 분류하고 있다. 영국의 개인정보보호 감독기구인 ICO는 '18년 'Technology Strategy'에서 개인정보와 관련한 중요 기술 3개를 선정하였으며, 사이버보안, AI와 빅데이터, IoT가 해당한다.

개인정보보호위원회 '2017 개인정보보호 연차보고서'에서는 개인정보 관련 주요 신기술 산업을 빅데이터, IoT・자율주행차, 핀테크, 스마트의료・헬스케어, 인공지능, 생체인식 기반 인증/보안, 드론으로 분류하였다.

3.2. 신기술서비스 내 처리되는 개인정보 유형

4차 산업혁명시대에는 데이터의 활용성이 높아짐으로써 디지털화된 개인정보 데이터가 대규모로 수집·집적되고 있다. 스마트 신고・구조 앱, 인공지능스피커, 항공 스마트 셀프체크인, 운전습관 연계보험 서비스 등 신서비스들은 개인정보 수집단계에서 많은 종류의 개인정보를 수집하고 있다.

'16년 행정안전부와 한국인터넷진흥원에서 발표한 '개인정보 영향평가 수행 안내서'[2]에서 제시하고 있는 개인정보 분류체계에 따른 12가지 유형 중 유출 시 심각한 문제를 야기할 가능성이 있어 법으로 특별하게 관리를 요구하는 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등 고유식별정보, 사상·신념, 정치적 견해, 병력, 생체인식정보, 인종・민족에 관한 정보 등 민감정보, 신용카드번호, 계좌번호 등 신용정보, 개인 또는 기기의 이동에 관한 정보 등 위치정보와 기타 중요정보도 수집되고 있다.

3.3. 자동처리를 통한 개인정보의 수집・이용

신기술 서비스들은 기기 간의 연결로 다양한 정보를 대량으로 수집하여 빅데이터 분석을 통해 비즈니스를 창출하고 있다. 쿠키정보, IP주소정보, 서비스 이용 내역, MAC주소, 영상 촬영정보, 음성명령 로그기록, 차량 운행정보 등이 자동으로 수집되고 타 정보와 결합하여 상당히 민감해 질 수 있는 정보가 자동 생성되기도 한다. 자동으로 수집되는 정보들은 정보주체가 그 수집 여부를 실시간으로 인지하기 어려우며, 해당 정보들이 어떻게 사용되는지를 파악하기 힘들기에 상당한 위험성을 가지고 있다.

3.4. 서비스별 개인정보 접근권한 요구

IoT 기술을 활용한 신서비스들의 대다수는 어플리케이션 등을 통해 스마트폰, 태블릿 PC, 스마트 워치 등 기기와 연동되어 서비스되고 있는데, 최근 앱 서비스 제공자가 이용자의 기기 내에 저장되어 있는 정보 및 설치된 기능에 무분별하게 접근함으로써 개인정보 침해 우려가 커지고 있다.

위치정보 수집 권한, 연락처 정보 열람・검색 권한, 카메라 촬영 권한, 전화연결 권한, 오디오 녹음 권한을 요청하는 서비스가 다수 있으며, 캘린더 정보 열람・수정 권한, SMS 메시지 열람 권한 등도 요청하고 있다.

3.5. 개인정보 제3자 제공 및 업무 위탁

최근 서비스 가입 시 정보주체가 무심코 동의하게 되는 개인정보 제3자 제공 동의가 대규모 개인정보 유출 사고를 촉발하고 있어 문제가 되고 있다. 그럼에도 불구하고 대다수 서비스에서 개인정보 수집 및 활용에 동의하지 않으면 회원 가입이나 필수 서비스를 진행할 수 없는 경우가 많은 것이 현실이다. 개인정보를 제공하는 주요 이유로는 서비스 개선 및 통계분석, 홍보 및 마케팅, 상품 배송, 요금 결제 및 정산 등이 해당한다.

4차 산업혁명의 도래로 비용절감, 업무 효율화, 서비스 개선 등 다양한 목적의 개인정보 처리 업무가 늘어났고 이에 대한 관리 비용과 책임을 단일 개인정보처리

가 모두 감당할 수 없게 되었다. 때문에 각종 업무를 외부 기업이나 개인에게 위탁하는 사례가 증가하고 있으며, 데이터 시대에 있어 업무의 위탁은 개인정보 처리 업무의 위탁과 병행되는 경우가 많다.

신기술 서비스들은 상당수가 개인정보를 위탁하고 있으며 동시에 해외기관에 개인정보를 위탁하고 있는 업체도 많다. 위탁을 하는 주요 이유는 서비스 및 시스템 운영, 회원관리 및 상담, 안내 메일 및 메시지 발송, 상품 배송 등이 있다.

Ⅳ. 주요 신기술 서비스의 개인정보 처리 실태

여기서는 본 논문에서 정의한 신기술 유형 중 핵심기술에 해당하는 IoT, 블록체인, AI 기술을 활용한 서비스에서의 개인정보 처리에 관해 조사한 실태를 설명한다.

4.1. IoT 기기에서의 자동으로 처리되는 개인정보 실태

스마트홈 서비스는 도어락/도어벨, 홈 영상기기, 스피커, TV/로봇청소기, 허브 등 다양한 IoT 기기가 연결되어 제공된다. 그 중 스마트TV와 웨어러블 기기의 수집부터 저장・이용・제공 및 파기까지의 단계별 처리과정과 개인정보 침해요인을 살펴본다.

스마트TV는 기기 내 마이크와 카메라를 통해 음성정보와 영상정보를 수집하고 IPTV, OTT(Over the Top) 등과 연결을 통해 시청내역, 콘텐츠 구매내역, 상품 구매내역 등을 수집하여 이용자에게 맞춤형 서비스를 제공한다. 마이크를 통한 음성정보는 주로 TV 전원 on/off, 콘텐츠 선택, 음성출력량 조절 등의 명령어 인식정보가 수집된다. 인식된 정보는 DB에 저장된 음성 명령어 정보와 비교하여 정확한 명령어를 구분하게 되는데 정확도 향상을 위해서 이용자의 음성을 수집하여 비식별처리 및 특징정보 추출 후 수집정보는 파기하게 된다. 이 경우 음성 원본정보는 인식 즉시 비식별처리를 하여 개인정보 보관기간을 최소화 해야한다. 그러나 특징정보를 추출하기까지 일정시간 원본정보를 보관해야 하고 특히 화자를 인식하는 서비스를 제공하는 경우 식별이 가능한 정보를 보관해야한다는 문제는 기술적으로 해결이 필요한 부분이다. 콘텐츠 추천의 경우 시청내역 및 콘텐츠 구매내역을 수집하여 이용자의 성향을 범주화한 DB와 이용자가 시청하는 콘텐츠를 비교하여 기존 이용자들이 추가로 시청했던 콘텐츠들을 추천하게 된다. 최근 콘텐츠 내 패션, 식품 등도 추천해주는 서비스가 제공되면서 이용자가 스마트TV를 통해 이용하는 모든 내역이 감시받고 있다는 우려를 낳고 있다. 콘텐츠 추천은 개인이 식별되지 않은 일련번호로 이용자를 구별하고 이용내역만을 빅데이터를 통해 분석한 결과를 추천하지만 스마트TV와 연결된 IPTV의 구매자 정보, 카메라 또는 마이크의 오작동을 통한 필요 이상의 정보들이 수집되고 저장될 수 있어 기술적 보호조치가 이루어지지 않으면 식별된 개인정보가 유출될 가능성이 높다.

IoT를 활용한 웨어러블 기기는 스마트워치, 바디캠, 가정용 로봇, 스마트팔찌 등 다양하며 스마트폰 또는 PC・서버 등에 연결되어 개인의 위치정보, 행태정보, 신체정보, 건강정보, 가정 및 주변의 영상정보, 통화 및 명령어 인식을 통한 음성정보 등이 수집된다. 이들 기기들이 다양한 형태로 정보를 수집하고 서버와 연결하여 빅데이터 분석 및 AI를 활용하여 새로운 서비스들을 창출해 내고 있는 반면 기기에서 전송하는 정보의 저장, 파기 등의 보호조치에 소홀할 경우 개인정보의 유출로 인한 피해가 확대될 수 있다. 특히 새로운 기기들이 출시되면서 기존 기기의 정보를 이동하거나 통신사 등을 통한 정보의 이동 형태가 빈번해 지면서 이용하지 않는 개인정보의 명확한 파기 조치가 이루어지고 있는지 확인하기 어렵다. 또한 사업자의 인수합병 및 등으로 인한 개인정보처리자의 변경 시 영업 양도 안내 등을 통한 서비스 선택권 보장과 개인정보의 제3자 제공 또는 위탁의 여부가 명확하게 정보주체에게 전달되지 못하는 경우도 있다.

4.2. 블록체인에서의 개인정보 처리 실태

블록체인 기반 온라인투표시스템은 유권자 인증, 투표 결과 저장 및 검증 과정 등 블록체인 기술을 적용하여 위변조가 불가능하도록 하는 것을 목표로 하고 투표/개표의 위변조가 불가능하고 이해관계자가 결과 검증이 가능한 시스템으로, 이해관계자가 투표/개표 과정에 직접 참관할 수 없던 기존 시스템과 달리 노드에 직접 접근할 수 있는 권한을 부여하고 있다[3]. 블록체인은 기존의 공인인증서 시스템과 마찬가지로 비대칭키 암호체계를 활용하여 블록체인에 트랜잭션을 올릴 때 본인의 개인키로 전자서명을 하고 있는데 투표시스템에서도 선

거인이 본인이 투표한 것이 맞다는 것을 증명하기 위해 선거인의 개인키를 이용한다. 투표할 때 사용하는 암호키를 생성하는 과정이나 제공하는 과정에서 키 관리에 대한 이슈가 존재한다.

블록체인 기반 의료 융합서비스 시스템은 개인 중심 진료정보 교류 서비스를 위한 것으로 환자 편의 서비스를 이용할 수 있는 환자용 모바일 앱을 개발하여 블록체인 기반의 전자처방전, 제증명 발급, 실손보험 청구 등을 제공하는 스마트 간편 서비스이다. 건강정보 관리 능력 증대, 보험청구 및 심사 프로세스 효율화, 의료기기 및 약물 유통채널 추적, 연구 데이터의 공유 및 활용성 증대, 개인 의료 건강 정보의 보호 강화, 의료정보 무결성 확보 및 책임추적성 강화의 효과를 기대할 수 있다[4]. 서비스가 구현되기 위해서는 개인정보인 전자처방전이 약국이나 보험사 등으로 제공되고 개인의료정보들을 블록체인 위에 올려 위변조가 불가능하게 하지만 정보주체의 자기결정권과 관련하여 삭제권을 행사할 수 없게 된다.

4.3. AI에서의 개인정보 처리 실태

의료분야에서 AI를 적용할 경우 신체정보, 유전자정보, 환자고유번호, 인적정보, 의료증상 기초 정보, 진료정보 등 개인정보를 활용하게 된다. 예방/예측 단계에서 유전체 정보, 의료정보, 생활습관, 식습관 등이 활용되고, 진단 단계에서 이미지, 영상 데이터 등 환자의 의료정보, 치료/처방 단계에서는 딥러닝에 환자의 치료정보를 활용하게 된다. AI 맞춤형 의료서비스 분야에서 활용되는 유전자 데이터 처리 과정은 먼저 유전적 소인 등을 토대로 질병 발병의 위험도를 예측하는 위험평가(Risk Assesment)가 진행이 되고, 질병 발병 위험도 등을 토대로 질병 예방을 위한 생활 방식 등을 제안하는 예방 단계(Prevention), 유전체 분석 등을 토대로 분자 수준에서 질병을 조기에 찾아내는 발견 단계(Detection), 유전자이상/변이 등의 분석 결과를 토대로 질병에 대한 정확한 진단을 하는 진단 단계(Diagnosis), 유전적 특징에 따른 진단 및 약물감수성 파악으로 효과적 치료를 하는 치료 단계(Treatment), 질병 치료에 대한 반응 및 질병의 예후를 모니터링 하는 관리 단계(Management)로 되어 있다[4]. 유전자 처리 과정에서 개인의 식별된 정보는 필요하지 않으며 비식별처리된 유전자 정보와 진단정보, 치료정보 등을 빅데이터로 분석하고 발병 위험도, 생활방식, 질병 초기 발견, 병명 진단, 치료 방법, 예후 관리 등을 AI를 통해 제안한다. 비록 환자 정보가 비식별처리되어 분석이 진행되더라도 정보주체의 자기정보 통제권을 가지기는 어렵다. 가명처리된 정보는 개인정보이고 자기정보 중 어떤 정보가 분석에 활용이 되는지, 어떤 목적으로 활용이 되고 정보가 제3자에게 제공되거나 위탁이 되는지 알 수 있도록 기술적 조치를 취해야 한다. 의료 서비스제공자 또한 AI 분석에 있어 투명성, 책임성, 통제성에 대한 의무를 다해야 한다.

자율주행차의 경우 현행 법률에서 차량과 관련된 정보는 개인에게 귀속되어 있으며 차량과 관련된 정보라 함은 차량의 속도 정보, 주행 기록, 배터리 사용 및 관리 정보 등을 말한다[5]. 자율주행차의 원활한 운행을 위해서는 앞에서 언급한 정보가 수집되고 활용되어야 하며 주행단계에서 개인정보수집이 불가피하다. 자율주행이 원활하게 이루어지기 위해서 주변 차량과의 커뮤니케이션이 중요한데 주변 차량 및 환경과 커뮤니케이션을 가지고 자율적인 판단을 하기 위해서는 자율주행차의 주행에 활용되는 기본 입출력 정보가 중요하다. 또한 외부환경을 인식해야하므로 거리상의 행인 정보도 수집하게 된다. 활용 단계에서는 차량 운행정보에 사용자의 개인정보가 저장되고, 차량 운행 중 통화정보, 이동정보, 주행습관, 음성인식 명령 정보, V2X 통신에 의한 주행정보 등의 개인정보가 처리된다. 이렇게 처리되는 개인정보들은 유출과 침해 예방을 위해 비식별조치되어 처리해야함은 물론 정보주체가 자기정보의 처리상황을 인지할 수 있도록 안내해 주어야 한다. 그러나 단시간 내에 예측할 수 없는 다량의 개인정보를 수집할 수 밖에 없는 서비스 구조에서 기기에 수집되는 모든 개인정보에 대하여 동의하기 어려우며 이용자의 음성정보, 신체정보, 금융정보, 운전습관 행태정보 등의 개인정보들을 수집·이용하고 있어 투명성과 신뢰성 보장을 위한 보호조치가 마련되어야 한다.

Ⅴ. 결 론

본 논문에서 4차 산업혁명 시대의 신기술을 분류하고 주요 기술별 개인정보 처리 실태 조사 결과를 살펴보았다. 개인정보보호법 개정으로 동의 없이 가명처리

및 결합이 가능한 범위가 신설되어 데이터 활용을 통한 데이터 경제 활성화를 기대하고 있다. 그러나 가명정보도 개인정보인 이상 수집부터 파기까지 개인정보 보호 원칙을 준수해야 한다. 기계적으로 자동으로 수집되고 스스로 학습되는 알고리즘을 통해 출력된 정보는 개인정보가 될 가능성이 있다. 법률 개정 지연으로 데이터의 활용도 지연되고 데이터를 안전하게 처리할 수 있는 보호조치 개발도 지연되었다. 사업자와 개발자는 최소한 사전예방과 투명성, 프라이버시 보호를 원칙으로 하는 PbD(Privacy by Design)[6]를 반영한 기획·설계 단계를 거칠 수 있도록 설정해야 하고 이는 분야와 서비스별로 각기 다른 보호 수칙으로 만들어질 수 있다. 또한 이용자의 경우에도 정보주체로써 스스로 개인정보를 보호하고 자기정보결정권을 행사할 수 있도록 보호수칙을 만들 필요가 있다. 그동안 데이터 활용의 법적 제약으로 개인정보를 포함한 데이터를 처리하는 활용 사례가 많지 않았으나 데이터 경제 활성화에 따라 다양한 신기술 서비스 증가가 기대되는 한편 개인정보 보호조치 마련을 위한 서비스별 연구가 필요하다.

참 고 문 헌

[1] 김일환, “초연결사회에서 개인정보 보호법제 정비 방안에 관한 연구”, 성균관법학 제29권 제3호, 2017.
[2] 행정안전부·한국인터넷진흥원, “개인정보 영향평가 수행 안내서”, 2016.
[3] 과학기술정보통신부, “블록체인 기반 온라인 투표시스템 시범사업 개요”, 2018.
[4] 한국인터넷진흥원, 서울의료원, “블록체인 기반 Smart Hospital 서비스개발 시범사업”, 2019.
[5] 장성재, “보건의료 빅데이터 관리시스템 최신 동향”, BRIC View 동향리포트, 한국원자력의학원, 2017.
[6] 안경환 외 3인, “자율주행 자동차 기술 동향”, 한국전자통신연구원, 2013.
[7] Ann Cavoukian, “Privacy by design the 7 foundational principles”, 2011.

〈저 자 소 개〉

봉 기 환 (Kihwan Bong)
2006년 2월 : 서강대학교 경영학과 졸업
2017년 2월 : 고려대학교 정보보호대학원 금융보안학과 석사수료
2006년 3월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 정보보호, 개인정보