「法과 政策」第22輯 第2號, 2016. 8. 30.
濟州大學校 法과政策硏究院

# 사물인터넷(IoT) 환경에서의 개인정보보호에 관한 규범적 고찰

## Normative Study on Personal Information Protection in IoT Era

신 혜 원* · 지 성 우**
Shin, Hye-Won · Ji, Seong-Woo

목 차



## 국문초록

사물인터넷은 주변 기술과 융합되어 하나의 생태계를 구성하며, 인터넷을 기반으로 한 융합의 중심에서 실제 생활영역으로 적용되면서 다양한 경제적 가치, 효율성 증대, 편의성 증대 등을 현실화할 것이란 기대가 높아지고 있다. 하지만 기술발전에 따른 편의성과 산업적으로 발생하는 많은 이익들이 밝은 미래만을 보여주는 것은 아니다. 기술의 발전 뒤에 사회는 해킹의 위협과 보

논문접수일 : 2016. 06. 30.
심사완료일 : 2016. 07. 25.
게재확정일 : 2016. 07. 25.
* 성균관대학교 법학전문대학원 박사과정(주저자)
** 성균관대학교 법학전문대학원 교수(공동저자)

안문제, 개인정보 침해문제 등 수 많은 위험에 직면해 있다. 정보기술의 발달로 자신의 개인정보가 노출된 정보주체는 원치 않는 광고와 스팸 등 기업 마케팅의 표적이 되었고 나아가 신용카드나 은행계좌의 불법도용으로 직접적인 재산적 침해가 발생하고 있다. 온라인 활동 증가, 광대역 연결의 확산, e커머스를 포함한 온라인 금융거래 증가, 컴퓨터보다 상대적으로 보안이 취약한 모바일 기기의 급속한 도입 등으로 인해 개인정보보안 위협은 지속적으로 증가할 것이다. 사물인터넷 시대에는 기기를 통해 수집된 정보에 의하여 특정 개인을 자동적으로 식별하고 개인의 습관, 위치, 관심사, 취향 등의 정보까지 파악할 수 있으며, 이용자 자신이 인지하지 못하는 상황에서 자신의 정보가 관찰·축적·공유될 수 있고 보건 및 의료분야 등의 민감한 정보가 수집·공유될 수 있다. 해킹사건이 잇따라 발생하며 여전히 개인정보 유출에 무방비하게 노출되어 있는 우리에게 사물인터넷의 밝은 미래만이 존재할 것인지에 대해서는 진지한 고민이 수반되어야 하며, 산업 활성화에 따른 이익을 따지기에 앞서 이용자의 정보보호를 위한 실질적인 보호방안과 진지한 법적성찰이 필요하다.

**주제어** : 사물인터넷, 개인정보보호, 개인정보자기결정권, 개인정보보호법, 개인정보유출

# Ⅰ. 서 론

세계적 수준의 국내외 IT기업들이 사물인터넷(Internet of Things)을 기반으로 한 제품 및 서비스에 주력하며 시장의 규모가 급증하고 있다. 사물인터넷은 홈·가전, 의료, 교통 등 다양한 산업분야에 적용되고 있으며, 본격적인 시장 활성화가 진행 중이다. 세계적으로 2020년까지 인터넷에 연결되는 사물의 수는 약 260억 개, IoT로 창출되는 부가가치는 약 1조 9천억 달러로 전망되고 있다. 나아가 최근 한 대형 국내통신업체는 사물인터넷 기기 개발에 필요한 필수 정보를 제공하여 개인 개발자나 소규모 회사가 이용할 수 있는 '기가 IoT 글루(Glue)'를 공개한 바 있다. 이와 같은 정보공개는 제작비용과 시

간을 획기적으로 줄이는데 도움을 주어 향후 사물인터넷 산업을 더욱 급격히 발전시킬 수 있게 만들 것이다.

사물인터넷은 통신망에서 사람과 사람, 사람과 사물, 사물과 사물 간을 자율적·지능적으로 시간·공간·대상의 제약 없이 연결함으로써 모든 정보들이 상호작용하게 만드는 방식을 지칭하는 개념으로 활용되고 있다.[1] 모든 것들이 통신망을 통해 연결된다는 점에서 사물인터넷은 현 단계에서 예측할 수 없을 정도의 편의성을 제공해 줄 것으로 예측되고 있는 반면, 활용분야가 우리 실생활의 모든 사물에 직접 접목되어 기존 사이버공간의 위험이 현실세계로 전이·확대되기 때문에 모든 사물을 연결하고 그 사물에 사람을 연결하는 사물인터넷의 발달에서 개인은 개인정보의 침해 내지 프라이버시 침해의 위협에 직면해 있다. 해킹사건이 잇따라 발생하며 여전히 개인정보 유출에 무방비하게 노출되어 있는 우리에게 사물인터넷의 밝은 미래만이 존재할 것인지에 대해서는 진지한 고민이 수반되어야 할 것이다.

본 논문에서는 우선 사물인터넷과 개인정보의 개념 및 관계, 헌법상 개인정보자기결정권의 의미와 근거, 사물인터넷의 개인정보침해 위험성에 대해 살펴보고자 한다. 다음으로 최근 개정된 EU와 일본의 법률에 대하여 알아본 후 우리나라 개인정보에 관련한 법률을 검토·분석하여 사물인터넷시대 개인정보보호를 위한 향후 개선방안에 대해 논의하고자 한다.

## Ⅱ. 사물인터넷과 개인정보

### 1. 사물인터넷의 의의 및 현황

#### 1) 의의

사물인터넷은 무선기술, 미세 전자·기계 시스템 및 인터넷이 융합됨으로써 발전된 것이다. 사물인터넷은 그동안 제조 산업이나 에너지 분야에서 활용되어

1) ITU Internet Reports, "The Internet of Things", 2005, p.3.

왔던 M2M(machine to machine)과 가장 밀접하게 연관되어 있다고 할 수 있는데, 초기의 사물인터넷이 산업장비를 연결시켰다고 한다면 이제는 일상생활의 모든 대상을 연결시키는 것으로 확대되었다. 이제 사물인터넷은 사람·장소·대상 및 물건을 포함하는 모든 것을 인터넷으로 연결시킨다는 의미에서, '모든 것의 인터넷(internet of everything, IoE)'이라는 단어까지 등장하고 있다.[2)]

우리 현행 법규에서 명확히 '사물인터넷'을 정의한 규정은 찾을 수 없고, '사물지능통신'의 개념 정의는 찾을 수 있다. 미래창조과학부 고시인 「전기통신번호관리세칙」 제3조 제21호에서 '사물지능통신'을 "정보통신망을 이용하여 사물과 사물 간 데이터 등을 송신하거나 수신하는 전기통신서비스"라고 규정하고 있는 것이 유일한 관련 정의 규정이다. 사물지능통신에 대하여는 협의로는 "방송통신망을 이용하여 사람이나 지능화된 기기가 사물의 상태를 제어하기 위한 통신"을, 광의로는 "통신과 ICT 기술을 결합하여 원격지의 사물의 상태나 상황정보를 확인할 수 있는 제반 솔루션"을 의미한다고도 한다.[3)] 한편 미래창조과학부의 보도자료에서는 사물인터넷을 "사람, 사물, 데이터 등 모든 것이 인터넷으로 서로 연결되어 정보가 생성·수집·공유·활용되는 기술·서비스를 통칭하는 개념"이라고 설명하고 있다.[4)]

### 2) 현황

사물인터넷은 특정 기관이나 기업, 개별적·폐쇄적인 형태에서 개방된 사물인터넷 서비스(Everything as a Service)로 진화되면서 주변 기술과 융합되어 하나의 생태계를 구성하며, 모든 것이 연결되는 과정에서 방대한 비정형 데이터의 처리·분석(빅데이터) 및 효과적인 정보처리(클라우드) 산업 또한 막대한 시장을 형성하고 있다.[5)]

---

2) 이대희, "사물인터넷 활용과 개인정보 보호", 「경영법률」 제25집 제3호, 2015, 366면.

3) 이규정 외 2명, "사물지능통신에 관한 법제도적 고찰", 2010, 6면.

4) 미래창조과학부 보도자료, "초연결 디지털 혁명의 선도국가 실현을 비전으로 사물인터넷 국가전략 수립", 2014.5.8

5) 한국정보화진흥원, "사물인터넷 수요와 시장동향", 「IT & Strategy Report」 제15호, 2015, 2면.

ICBM(IoT, Cloud, Big Data, Mobile)이 새로운 성장 동력으로 주목받는 가운데, 인터넷 기반의 융합의 중심에서 IoT가 실제 생활영역에 적용되면서 다양한 경제적 가치, 효율성 증대, 편의성 증대 등이 현실화될 전망이다. Business Insider Inc(2015)는 사물인터넷은 연결된 개체 및 임베디드 센서를 사용하여 데이터를 교환하는 광대한 성장 네트워크로, 생산성·효율성 및 혁신의 관점에서, 산업 혁명이후로 사회를 변형시킬 주요한 기술로 판단하고 있으며, 세계적으로 IoT 디바이스 산업의 경우, 2015년부터 2020년까지 연평균 성장률은 41%에 달할 것으로 전망하고 있다. 또한, 맥킨지(2015)는 사물인터넷 시장에 대해 2025년은 세계 GDP의 11%에 달하는 규모로 성장할 것으로 전망하고 있으며, 가트너(2015)는 2016년을 움직일 10대 기술 중 하나로, IoT 아키텍처와 플랫폼을 제시하여 향후 5~10년 사이에 안정화에 이를 것으로 예측하고 있다.

〈표 1〉 개인정보보호 10대 트렌드 전망[6)]

| 순위 | 2014년 | 2015년 | 순위변동 |
|---|---|---|---|
| 1위 | 빅데이터 분석 | 빅데이터 분석 | - |
| 2위 | 피싱, 스미싱, 파밍 | 피싱, 스미싱, 파밍 | - |
| 3위 | 공공데이터 개방 | SNS 개인정보보호 | ▲1 |
| 4위 | SNS | IoT(Internet of Things) | 신규 |
| 5위 | 모바일 앱 | 모바일 앱 | - |
| 6위 | 동의 만능주의 | 잊혀질 권리<br>(Right to be forgotten) | 신규 |
| 7위 | 모니터링 감시 | 징벌적, 법정 손해배상제도 도입 | 신규 |
| 8위 | 개인식별 인증 대체 수단 | 주민등록번호 수집 법정주의 | 신규 |
| 9위 | 개인정보 국외이전 | FDS<br>(Fraud Detection System) | 신규 |
| 10위 | 클라우드 컴퓨팅 | 공공데이터 개방 | ▼7 |

국내 사물인터넷 시장의 경우 2015년 3.8조원에서 2020년 22.9조원까지 성장할 것이며, 서비스 관련 매출의 비중이 52.6%까지 증가하며 성장을 주도할 것으로 전망하고 있다. 한국정보화진흥원(NIA)이 발간한 '2015년 개인정보보호

6) 출처: 한국정보화진흥원 「2015년 개인정보보호 10대 트렌드 전망」 보고서

10대 트렌드 전망' 보고서에서는 '빅데이터 분석'이 3년 연속으로 가장 큰 주목을 받을 것으로 전망됐으며, 신규 이슈로 IoT가 4위로 추가되었는데, 이는 모든 사물들이 연결될 수 있는 환경 도래에 따라 새로운 개인정보 침해에 대한 우려라고 볼 수 있다.

## 2. 사물인터넷과 개인정보 문제

IoT 기술발전에 따른 편의성과 산업적으로 발생하는 많은 이익들은 밝은 미래만 보여주는 것이 아니다. 기술의 발전 뒤에 해킹의 위협과 보안문제, 개인정보 침해문제 등 수 많은 위험에 직면해 있다. 온라인 활동 증가, 광대역 연결의 확산, e커머스를 포함한 온라인 금융거래 증가, 컴퓨터보다 상대적으로 보안이 취약한 모바일 기기의 급속한 도입 등으로 인해 개인정보보안 위협은 지속적으로 증가할 것이다.

사물인터넷 시대에는 기기를 통해 수집된 정보에 의하여 특정 개인을 자동적으로 식별하고 개인의 습관, 위치, 관심사, 취향 등의 정보까지 파악할 수 있으며, 이용자 자신이 인지하지 못하는 상황에서 자신의 정보가 관찰·축적·공유될 수 있고 보건 및 의료분야 등의 민감한 정보가 수집·공유될 수 있다. 미국 연방거래위원회(FTC, Federal Trade Commission)의 라미레즈 의장은 사물인터넷과 관련하여 광범위한 데이터 수집, 수집된 데이터의 예기치 않은 사용으로 인한 부정적 결과의 발생 가능성, 보안 위험 등의 문제점을 지적하고 있다. 사물인터넷에 사용되는 감시와 추적기술에 의하여 엄청난 양의 정보가 축적되고 데이터 분석에 의하여 개인정보나 민감정보가 새로이 생성되어 특정 개인을 파악할 뿐만 아니라, 연결된 많은 기기들이 해킹의 대상이 되어 심각한 규모의 해킹이 가능해질 수 있다는 것이다.

### 1) 사물인터넷 관련 개인정보

사물인터넷을 통해 얻어지는 정보에는 살아있는 개인에 관한 정보로서 성명, 주민등록번호, 영상 등을 통하여 식별가능한 일반적 개인정보, 다른 정보

와 쉽게 결합하여 식별할 수 있는 개인정보가 있을 수 있겠으나, 이외 민감정보와 위치정보도 포함할 수 있을 것이다.

〈표 2〉 개인정보의 유형과 종류[7)]

| 구분 | 개인정보의 종류 |
|---|---|
| 일반정보 | 이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적 |
| 가족정보 | 부모·배우자·부양가족의 이름 및 직업, 가족구성원의 출생지 및 생년월일, 주민등록번호, 직업 |
| 교육 및 훈련정보 | 학교 출석사항, 최종학력, 학교성적, 기술자격증 및 전문면허증, 이수한 훈련 프로그램, 서클활동, 상벌사항, 성격 및 형태 보고 |
| 병역정보 | 군번 및 계급, 제대유형, 주특기, 근무부대 |
| 부동산정보 | 소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등 |
| 동산정보 | 보유 현금, 저축현황, 현금카드, 주식·채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석 |
| 소득정보 | 현재 봉급액, 봉급경력, 보너스 및 수수료, 기타 소득의 원천, 이자소득, 사업소득 |
| 기타수익 정보 | 보험(건강·생명 등) 가입현황, 수익자, 회사차·회사의 관공비, 투자프로그램, 퇴직 프로그램, 휴가·병가 |
| 신용정보 | 대부 잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록 |
| 고용정보 | 현재의 고용주, 회사주소, 상관의 이름, 직무수행 평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트 결과, 직무태도 |
| 법적정보 | 전과기록, 자동차 교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록 |
| 의료정보 | 가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형 등 |
| 조직정보 | 노조 가입, 종교단체 가입, 정당 가입, 클럽 회원 |
| 습관 및 취미정보 | 흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여 기록, 도박성향 등 |

(1) 일반적 개인정보

개인정보보호법 제2조 제1호에서는 '개인정보'에 대하여 "살아있는 개인에

7) 성낙인 외 9인, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008, 222면 이하 참조한 김주영·손형섭, 「개인정보보호법의 이해」, 법문사, 2012, 161면 재인용

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)"고 규정하고 있다. 이러한 정의는 정보통신망법 제2조 제6호의 개인정보 정의와 같다고 볼 수 있다. 개인정보보호법과 정보통신망법은 개인정보의 정의에 대하여 일부 차이가 있을 뿐 동일한 내용을 규정하고 있다.

(2) 개인위치정보

사물인터넷 기기의 상당수가 대상의 위치추적을 통해 사용되어진다. 센서가 부착된 자동차, 스마트폰의 위치 추적을 통한 서비스 제공 앱, 치매노인이나 어린이를 위한 위치추적 기기, 교통량 측정을 위한 CCTV를 통한 위치정보 등 방대한 위치정보가 본인도 모르는 사이 노출될 수 있다. 이러한 정보는 여러 개의 정보와 연계되어 특정 개인의 신원을 파악할 수 있다. 예컨대 건강관련 센서를 통하여 특정개인의 하루 동안의 움직임을 파악하여 데이터 세트를 확보한 후, 이러한 데이터 세트에서 특정인의 독특한 유형을 파악하고 이것과 해당 주체로부터 직접 얻었거나 일반적으로 획득할 수 있는 보조적 외부 정보를 연계시키면 특정 개인의 신원을 파악할 수 있다. 즉 위치정보에 의하여 특정 날짜에 특정행사에 참여하였거나 특정인을 만났는지 여부, 특정인의 집에 체류하였는지 여부, 민감한 의료정보 및 종교 활동에 대한 내용 등이 파악되어 위치 프라이버시가 상실될 수 있다.[8] 따라서 사물인터넷 시대에서 위치정보는 곧 개인을 식별할 수 있는 정보로서의 가능성을 가지고 있다.

위치정보는 위치정보 보호 및 이용 등에 관한 법률상 위치정보 내지 개인위치정보에 해당한다. 위치정보법 제2조에서 '위치정보'란 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조 제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것을 의미하며, '개인위치정보'는 특정 개인의 위치정보로서 위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게

8) Andrew J. Blumberg & Peter Eckersley, "On Locational Privacy and How to Avoid Losing it Forever", *Electronic Frontier Foundation*, 2009, pp.1-2.

결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다고 규정하고 있다. 위치정보의 수집에 대하여 위치정보법 제15조 제1항에서는 개인 또는 소유자의 동의 없이 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공을 금지하고 있다.

(3) 민감정보

개인정보보호법 제23조는 민감정보에 대하여 ① 사상·신념 ② 노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건강, 성생활 등에 관한 정보 ⑤ 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보라 규정하고 있다.[9] 사물인터넷 환경 속에서 정보통신서비스 제공자가 서비스를 안정적으로 제공하기 위해서는 기기 간 통신을 통해 다량의 정보를 자동으로 주고받게 되는데, 이러한 과정에서 본인의 민감한 정보가 해킹되거나 노출될 위험성이 높아질 것이다.

사물인터넷을 활용하는 여러 분야의 기기 중 특히 문제시 되는 것이 의료기기 분야이다. 모바일 헬스의 발전으로 환자들이 점차 집에서 의료기기를 사용하게 되고, 이에 따라 공용 네트워크에 의료기기가 연결된다거나 스마트폰과 같은 개인기기를 통해 의료 정보를 포함한 개인정보를 주고받게 될 것이다. 시만텍이 발표한 보고서는 2016년에는 IoT와 관련하여 의료기기, 스마트 TV, 자동차 등의 보안위협을 강조하였는데, 이중 의료기기의 경우 잠재적으로 매우 치명적인 취약점을 가지고 있다고 하며 그 위험성을 강조하고 있다.[10]

# Ⅲ. 개인정보의 보호법제 및 한계

## 1. 개인정보보호의 헌법적 의의

개인정보의 보호는 정보주체의 시각에서 볼 때 자신에 관한 정보의 생성과

9) 다만 공공기관이 개인정보보호법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 시행령이 규정하고 있는 민감정보를 처리하는 경우에는 민감정보에 해당하지 않는다(시행령 제18조).

10) Symantec, "Internet Security Threat Report", 2016, pp.16-17.

유통, 소멸 등에 주도적으로 관여할 법적 지위를 보장하는 것으로 파악될 수 있다. 이에 따라 개인에 관한 정보를 정보의 주체가 타인에게 알릴 것인지 말 것인지, 알린다면 언제 누구에게 어느 범위까지 알릴 것인가에 관하여 스스로 결정할 수 있는 권리를 보장할 필요가 있다. 이러한 정보주체의 권리를 우리 헌법재판소는 '개인정보자기결정권'이라는 이름으로 파악하고 있다.

### 1) 개인정보자기결정권

정보사회에서 특히 개인의 사생활침해가 우려되는 이유는 자동정보처리를 통하여 순식간에 개인정보를 무수히 많은 사람들이 전혀 다른 장소에서 한꺼번에 받아볼 수 있다는 것과, 컴퓨터를 통한 정보연결에 의하여 개인정보가 전혀 다른 목적으로 사용될 수 있다는 데에 있다.[11] 오늘날에는 정보통신기술의 비약적인 발달로 인하여 개인에 관한 정보를 저렴한 비용으로 손쉽게 수집·이용·보관·가공·처리하는 것이 가능해졌으며, 개인정보가 상업적인 거래의 대상이 되고 있다. 이에 자기 자신에 대한 정보를 보호받기 위하여 그 정보를 자율적으로 결정하고 관리할 수 있는 권리가 사생활의 비밀과 자유의 중요한 내용이 되고 있다.[12] 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리 즉, 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.[13] 이러한 개인정보자기결정권은 정보주체가 자신에 관한 정보의 수집·이용·제공 등에 대해 동의 또는 반대할 수 있는 권리를 핵심적 내용으로 하며, 경우에 따라 자신에 관한 정보에 통제력을 행사하기 위하여 자신의 개인정보에 접근하여 열람하거나 그 정보의 정정·삭제·차단·처리정지 등을 요구하는 권리로 발현될 수도 있다.[14]

---

11) 김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 「공법연구」 제29집 제3호, 2001, 111면

12) 정종섭, 「헌법학원론」, 박영사, 2008, 546면.

13) 헌법재판소 2005.5.26 선고 99헌마513, 판례집 제17권 제1집, 682면.

14) 개인정보보호의 법과 정책, "정보주체의 개인정보자기결정권" 고학수 편, 박영사, 2004, 5-7면.

### 2) 개인정보자기결정권의 근거

개인정보자기결정권의 헌법적 근거에 대하여 여러 가지 이론이 있으나, 우리 학계에서는 개인정보자기결정권의 근거와 관련하여 ① 헌법 제17조의 사생활의 비밀과 자유에서 찾는 견해, ② 헌법 제17조 및 헌법 제10조의 인간의 존엄과 가치에서 찾는 견해, ③ 자유로운 인격성의 보장을 위한 측면은 헌법 제10조의 인간의 존엄과 행복추구권에서, 권력통제권이라는 정치적 권리로서의 측면은 국민주권의 원리와 민주주의의 원칙에서 찾는 견해 등이 있다.

헌법재판소는 개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권으로 보고 있다. 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장 장치로 보아야 한다는 것이다. 또한, 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다고 본다.[15]

## 2. 개인정보개념의 기준범위

우리나라의 개인정보 개념정의와 관련하여 규정이 매우 포괄적이라는 지적이 산업계를 중심으로 제시되고 있다. 개인정보보호법 제2조의 '해당정보만으로는 특정 개인을 알아볼 수 없더라도 쉽게 결합하여 알아볼 수 있는 것을 포함한다'는 부분에서 어느 정도를 쉽게 결합한 것으로 볼 것인가라는 식별가능성 판단기준이 불분명하다는 것이다. 그러나 각국의 개인정보 보호법제의 개념정의 규정들을 보았을 때 비단 우리나라만의 해당문제는 아니라고 보여진다. 기술의 발전상황과 데이터의 급증 그리고 분석기술의 고도화에 따라 식별가능의 명확한 기준정립은 어려우며 이에 따른 개인정보의 법적 보호체계는 한계에 봉착할 수밖에 없다.

〈표 3〉 각국의 개인정보 개념정의 규정[16]

| 국가 | 개인정보 개념정의 규정 |
|---|---|
| EU | 개인정보는 '식별되거나 식별가능한 자연인'(이하, '정보주체'라 한다)에 관한 정보를 말한다. |
| 영국 | 개인정보란 다음으로부터 식별될 수 있는 살아있는 개인에 관한 정보를 의미한다.<br>(a) 살아있는 개인을 식별할 수 있는 정보<br>(b) 살아있는 개인을 식별할 수 있는 정보 및 개인정보처리자가 보유하고 있거나 보유할 가능성이 있는 기타정보. 그리고 개인에 관한 의견, 개인정보처리자 또는 그 밖의 사람들의 개인에 관한 의사표현을 포함한다. |
| 독일 | 개인정보란 식별되거나 식별가능한 개인에 관한 인적 물리적 환경에 관한 모든 정보를 말한다. |
| 일본 | 이 법률에서 개인정보라 함은 생존하는 개인에 관한 정보로서, 해당 정보에 포함되는 성명, 생년월일 기타 기술 등에 의해 특정한 개인을 식별할 수 있는 것(다른 정보와 쉽게 조합될 수 있고, 그에 따라 특정한 개인을 식별하는 것이 가능하게 되는 것을 포함한다)을 말한다. |
| 호주 | 개인정보란, 진실여부 또는 기록된 형태에(데이터베이스를 구성하고 있는 정보 또는 의견을 포함한다) 상관없이, 개인에 관한 정보 또는 의견을 통하여 신원을 알 수 있거나 신원을 합리적으로 확인 가능한 경우, 그 정보 또는 의견을 말한다. |

15) 헌재 2005. 5. 26. 99헌마513 등, 판례집 17-1집, 668.

16) 심우민, "개인정보 비식별화 또는 익명화 쟁점", 오픈넷 포럼 발제문, 2016, 1-2면 인용.

개인 식별의 여부는 당해정보를 취급하는 자마다 다를 수 있는 상대적인 것으로 개인정보 해당여부는 정보처리자의 업무 환경 속에서 정보주체의 식별가능성, 다른 정보와의 결합가능성, 추적 가능성, 사생활 침해가능성 등을 종합적으로 고려하여 판단하여야 할 것이다.

결합의 용이성 판단기준과 관련하여 행정자치부는 식별을 위해 불합리할 정도의 시간, 노력, 비용이 투입되어야 한다면 그러한 정보들은 식별성이 없다고 판단하고 있으며, 특정 개인을 알아볼 수 없도록 가공되었거나 통계적으로 변환된 경우에는 특정 개인과의 관련성이 없고 식별이 어려우므로 개인정보에 해당하지 않다고 보고 있다.

해외의 경우 유럽연합 데이터 보호지침의 위임에 따라 개인정보의 개념에 대해 해설한 'Opinion 4/2007 on the concept of personal data'에서는 "개인을 식별가능한지 여부를 결정하기 위해서는, 개인을 식별하기 위해 관리자 또는 임의의 다른 사람에 의해 합리적으로 활용될 가능성이 있는 모든 수단을 고려하여야 한다"고 하면서 "해당 정보의 관리자 또는 임의의 다른 사람에 의해 합리적으로 활용될 가능성이 있는 모든 수단을 고려하였을 때 그러한 식별가능성이 존재하지 않거나 무시할 수 있는 수준이라면, 개인을 식별가능하다고 보기 어렵고, 따라서 그 정보도 개인정보에 해당하지 않다"라고 언급하고 있다. 미국의 경우 개인정보의 개념에 대해 식별 가능한 경우 외에도 특정 고객, 컴퓨터, 다른 기기에 합리적으로 연결되어 있는 정보도 포함하는 것으로 보고 있는데, 회사가 고객정보를 비식별화하는 합리적 조치를 취하거나, 대외적으로 비식별화 조치를 취하고 재식별화를 하지 않음을 공표하거나, 다른 회사에게 비식별화 정보를 이용하도록 하는 경우 재식별화를 계약상 금지하도록 할 경우 합리적으로 연결되어 있지 않는 것으로 본다.[17]

## 3. 정보주체의 동의

정보통신기술의 발달로 자신의 개인정보가 노출된 정보주체는 원치 않는

17) FTC, "Protecting Consumer Privacy in an Era of Rapid Change", *Federal Trade Commission*, 2012, pp.18-21.

광고와 스팸 등 기업 마케팅의 표적이 되었고 일상을 방해받는 수준까지 그 피해가 증가하기 시작하였다. 더 나아가 신용카드나 은행계좌의 불법도용으로 직접적인 재산적 침해가 발생하고 인터넷 해킹으로 신체에 대한 물리적 테러까지도 가능한 세상이 되었다.[18] 현행 법률에서는 이러한 정보통신서비스 이용 과정에서 이용자의 개인정보자기결정권을 보호하기 위해 사전 동의 제도를 두고 있다. 다시 말해, 사전 동의 제도는 개인정보자기결정권의 구현방법으로, 이러한 사전 동의를 규정하고 있는 법조항을 살펴보면 우선 개인정보보호법의 경우 제15조(개인정보의 수집·이용), 제17조(개인정보의 제공), 제18조(개인정보의 이용·제공 제한), 제22조(동의를 받는 방법)에서, 정보통신망법은 제22조(개인정보의 수집·이용 동의 등), 제23조(개인정보의 수집 제한 등), 제24조(개인정보의 이용 제한), 제24조의2(개인정보의 제공 동의 등), 제25조(개인정보의 취급위탁), 제26조의2(동의를 받는 방법)에서 규정하고 있고, 위치정보법 제15조(위치정보의 수집 등의 금지), 제18조(개인위치정보의 수집), 제19조(개인위치정보의 이용 또는 제공), 제21조(개인위치정보 등의 이용·제공의 제한 등)에서도 사전 동의 없는 정보 수집 및 이용 등을 금지하고 있다.

그러나 현행의 개인정보 사전 동의 제도가 정보주체를 보호하는데 실질적인 역할을 하고 있는지에 대해서는 의문이 있다. 동의서에 지나치게 많은 사항을 고지함으로서 이용자의 이해를 방해하고 오히려 사업자의 책임을 이용자에게 전가시키는 수단이 되고 있으며, 사전 동의를 하지 않을 시 해당 서비스를 이용할 수 없기 때문에 반드시 해당 서비스를 필요로 하는 이용자 입장에서는 내용에 관계없이 동의를 할 수 밖에 없다. 또한, 방대한 양의 정보를 처리하는 과정에서 실질적으로 정보주체의 동의를 받을 수 없는 경우가 증가하고 있는 상황이다.

## Ⅳ. 주요국 법제현황

### 1. EU

18) 김민호, "개인정보처리자에 관한 연구", 「성균관법학」 제26권 제4호, 2014, 247면.

EU는 EU 회원국들 간 정보의 자유로운 이전과 EU의 공동시장의 발전을 위하여 EU 수준의 통일된 개인정보보호 법제를 마련해야 한다는 필요에 의해 1995년 10월 「EU 개인정보보호지침」을 채택하였고, 이후 현재까지 EU 차원의 개인정보보호에 대한 일반법으로서의 역할을 수행하였다.[19]

「EU 개인정보보호지침」은 다음의 기본원칙을 상정하고 있다. 첫째, 개인정보가 공정하고 합법적으로 처리될 것, 둘째, 개인정보가 특정되고 명확하며 정당한 목적을 위하여 수집되어야 하고, 그 목적과 양립할 수 없는 방식으로 더 이상 처리되지 말 것, 셋째, 개인정보가 수집되고 처리되는 목적과 관련하여 적절하고 타당하며 과도하지 않을 것, 넷째, 개인정보가 정확하고 필요한 경우에 최신성을 유지하여야 하며, 수집 또는 처리되는 정보의 목적과 관련하여 부정확하거나 불완전한 정보는 삭제 또는 정정될 것을 보장하는 모든 합리적인 조치가 강구될 것, 다섯째, 정보주체의 신원을 허용하는 형태로 그 정보가 수집되거나 처리된 목적을 위하여 필요기간 이상 보관되어서는 안 되며, 회원국은 역사적, 통계적 또는 과학적 사용을 위하여 장기간 저장된 개인정보에 대해 적절한 보호조치를 수립하여야 한다.[20]

「EU 개인정보보호지침」은 EU의 개인정보보호 규범을 하나의 법제로 조화시키려고 하였다는 점에서 가장 큰 의의가 있다. 그러나 클라우드 컴퓨팅, 빅데이터 분석기술 등 급속도로 발전하는 정보기술과 인터넷 사용자 수의 엄청난 증가, 정보수집의 복잡·다양화 등의 문제와 개별 회원국의 개인정보보호법의 내용이 통일되어 있지 않는 문제에 따라 개정의 필요성이 대두되었으며, 이러한 요구에 부응하여 유럽위원회는 2012년 1월 기존의 「EU 개인정보보호지침」을 대체하는 「EU 개인정보보호규칙안」(Proposal of General Data Protection Regulation)을 공표하였다. 이후 2013년 10월 유럽의회 Jan Philipp Albrecht 위원과 Dimitrios Droutsas 위원은 유럽위원회의 「EU 개인정보보호규칙안」을 수정한 절충개정안(Compromise Amendment)을 공표하였고 유럽의회는 2014

19) 함인선, "EU의 '1995년 개인정보지침'에 관한 법적 고찰", 「법학논총」 제33호 제1호, 전남대학교 법학연구소, 2013, 281면.

20) 방송통신위원회, "EU 및 일본의 개인정보보호법제 및 감독체계 개편내용 분석", 「방통융합정책연구」, 2014, 13면.

년 3월 이를 채택하였다. 그리고 최근 2015년 12월 14일, 4년의 논쟁 끝에 유럽의회는 2012년 1월에 작성한 GDPR을 최종 합의하여 2018년 초에는 1995년에 제정된 개인정보보호지침을 대체할 예정이다. 동 규정의 주요 내용을 살펴보면 △개인정보보호 위반 시 전체 매출액의 4% 벌금 △개인정보 유출 사고 발생시 72시간 내 감독기구에 보고 △16세 미만의 아동에 대한 개인정보 처리 시 부모나 법적 대리인의 동의 요구 △정보주체의 동의 없이 개인정보 이용 및 공개 금지 △민감 정보 취급 기업 개인정보영향평가 의무 수행 △개인정보처리 공공기관, 개인정보책임자 지정 △개인정보준수 인증 매커니즘 △개인정보 역외 이전(1. 적합성 판정에 의한 국외 이전 2. 적절한 보호조치를 갖춘 경우 국외이전 3. 다국적 기업에 적용되는 회사 내 개인정보 국외이전)등에 관한 사항이 있다.

우선 정보주체는 서비스 제공자가 보유하고 있는 자신의 개인정보를 다른 서비스 제공자에게 이전시킬 권리를 보유하며 자신의 정보가 유출되었는지 알 권리를 가진다. 또한 개인정보가 유출된 경우 72시간 이내에 통보받게 된다. 동 규정을 위반한 기업의 경우 전체 매출의 최대 4% 또는 2천만 유로의 벌금을 부과할 수 있으며, 기업에 의해 개인정보에 대한 침해가 발생할 경우 해당 기업의 주 사업장 소재지의 개인정보 보호당국이 동 사건을 처리하게 된다. 또한 EU 역외에 소재하는 기업에 의해 EU 시민의 개인정보가 침해되는 경우에도 적용된다. 따라서 회원국은 2년간 동 규정의 효과적인 적용을 위해 국내 제도를 개편하여야 한다.

이 새로운 법안은 유럽 전역에 걸쳐 개인정보 사용의 표준으로 더 큰 법적 확실성 제기 및 디지털 시장에 대한 신뢰 강화를 목적으로 하고 있다. 이 개인정보보호강화 안을 통해 유럽 IT정보산업 성장에 잠재적인 제약이 될 수 있을 거라는 우려와 함께 한편으로는 개인정보를 침해할 우려가 있는 요인을 파악하고 대처하기 위해 기업들이 개인정보 사용 과정을 위한 명확한 정책을 확립할 수 있는 기회도 될 수 있을 것이라는 의견도 있다.

### 1) 개인정보의 개념

개인정보에 관한 개념에 대하여 최근 통과된 GDPR 최종안에서는 식별된 또는 식별할 수 있는 개인이란 특히 이름, 식별번호, 위치정보, 온라인 식별자와 같은 식별자(identifier) 또는 그 사람의 물리적·심리적·유전적·정신적·경제적·문화적·사회적인 정체성(identity)에 특정된 하나 이상의 요소를 참조하여 직접 또는 간접으로(directly or indirectly) 식별될 수 있는 자라고 규정하고 있다.

즉, GDPR 이전의 개인정보지침에서 식별자에 관하여 식별번호만을 언급한 것과 달리 GDPR에서는 식별번호, 위치정보, 온라인 식별자, 이름으로 규정하고 있으며, 본 규정에는 식별범위에 관한 판단기준이 나와 있지 않지만 GDPR 리사이틀을 살펴보면 '개인이 식별가능한지 여부를 결정하기 위해서는, 그 개인을 식별하기 위해 개인정보처리자 또는 제3자에 의해 사용되는 합리적으로 가능하다고 생각되는 모든 수단을 고려하여야 한다'고 언급하고 있다.

### 2) 정보주체의 동의

「EU 개인정보보호규칙 절충개정안」은 '정보주체의 동의'에 대해 제4조 8항에서 '정보주체가 진술 또는 명확한 긍정적 행위를 통해 자신과 관련된 개인정보가 처리되는 것에 합의를 나타내는 정보주체의 자유롭게 주어진 특정되고 고지된 명시적(explicit) 표시'라고 규정하였다.[21] 그러나 최근 통과된 GDPR에서는 민감정보와 같은 특별한 경우를 제외하고 종전의 동의의 기준을 '명시적'(explicit)이라고 규정한 부분을 '명백한'(unambiruous)으로 수정했다. 이는 모든 경우에 있어서 명시적인 동의를 획득하는 것의 실질적 어려움을 해결하기 위한 것이라 볼 수 있다.[22]

## 2. 일본

일본은 최근 개인정보의 이용가치가 점차 높아짐에 따라 개인정보법 제정

21) 「EU 개인정보보호규칙 절충개정안」 제4조 8항.

22) Hunton & Williams Privacy&Information Security Law Blog, Council of the European Union Releases Draft Compromise Text on the Proposed EU Data Protection Regulation, June 4, 2013. www.huntonprivacyblog.com/tag/council-of-the-european-union

당시 예상하지 못했던 개인정보 및 프라이버시에 관한 사회적 상황이 현행법 제정 당시와는 다르게 변화하고 있는 환경변화를 수용하여 2003년 제정된 개인정보보호법을 2015년 9월 3일 개정하였고, 2017년 전면적인 시행을 앞두고 있다.

개정안의 핵심골자는 우선 정부가 독립적인 개인정보보호 전문기관을 설치하여 일본의 개인정보보호제도를 국제수준에 맞추고, 기업의 자율규제 규칙을 지지하고 기술이 발전함에 따라 확대된 개인정보의 회색지대를 해소하는 것을 목표로 한다. 그리고 개인 식별을 어렵게 한 후 그 데이터를 타사에 전달하여 활용할 수 있도록 규제를 완화하고, 정부는 개인과 관련된 데이터이면서도 특정 개인을 식별할 수 없도록 하여 그 권리와 이익을 침해하지 않는 데이터(개인 데이터)를 활용한 새로운 사업의 창출을 목표로 한다.[23]

개정 법률에는 개인이 특정되지 않도록 하는 '익명가공정보화'를 의무화하고 제3자에게 개인정보를 제공하는 규정을 명확히 하는 등 개인정보보호를 도모하면서도 그 이용과 활용을 촉진하여 신산업·신서비스의 창출과 국가안전·안심 향상을 실현할 수 있도록 규정을 정비하고자 하는 노력이 담겨 있다.[24]

### 1) 개인정보의 개념

일본 개인정보보호법 제2조에서는 개인정보를 '개인정보', '개인데이터' 및 '보유개인데이터'의 3가지로 분류하고 있다. '개인정보'란 생존하는 개인에 관한 정보로서, 해당 정보에 포함되는 성명, 생년월일 그 밖의 기록 등에 의하여 특정 개인을 식별할 수 있는 것(다른 정보와 용이하게 조합할 수 있으며, 그에 의하여 특정 개인을 식별할 수 있게 되는 것을 포함한다)을 말한다.[25] '개인데이터'란 개인정보데이터베이스 등을 구성하는 개인정보이며,[26] 여기에서 '개인정보데이터베이스 등'이란 개인정보를 포함하는 정보의 집합물로서 특정

23) 한은영, "일본 개인정보보호법 개정의 배경 및 개정안의 주요 내용", 「정보통신정책연구 동향」 제26권 13호, 2014, 21면.

24) 한은영, "일본 개인정보보호법의 개정 내용 및 평가", 「정보통신정책연구 동향」 제27권 제17호, 2015, 41-42면 참조.

25) 「일본 개인정보보호법」 제2조 제1항.

26) 「일본 개인정보보호법」 제2조 제4항.

개인정보를 전자기기를 사용하여 검색할 수 있도록 체계적으로 구성한 것 및 그 밖에 특정 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것이다.[27] 그리고 '보유개인데이터'란 개인정보취급사업자가 공개, 내용의 정정, 추가 또는 삭제, 이용정지, 소거 및 제3자에 대한 제공의 정지를 할 수 있는 권한을 갖는 개인데이터이다. 단, 그 존부가 명확해지면 공익 그 밖의 이익을 해할 수 있다고 정령(政令)으로 정한 것 또는 정령에 따라 1년 이내의 기간 내에 소거하도록 정한 것은 제외한다고 규정되어 있다.[28]

개인정보의 정의와 관련하여 이번 개정 법률에서는 특정 개인을 식별하는 정보(개인식별부호)가 담긴 것을 개인정보로 명확히 하였으며, 개인식별부호는 다음 두 가지로 분류된다. i) 특정 개인의 신체 일부 특징을 전자적으로 제공하기 위해 변환한 글자·숫자·기호·기타의 부호 ii) 서비스 이용·제품구입과 관련하여 개인에게 할당되거나 개인에게 발급되는 카드·기타 서류에 기재되거나 전자적 방식에 의해 기록되는 글자·숫자·기호·기타 부호가 그 이용자(구입자)마다 다르도록 할당·기재·기록됨으로써 특정 이용자(구입자)를 식별할 수 있는 것이다. 여기서 첫 번째 항목은 생체인식 등에 사용되는 지문이나 홍채, 정맥 등 개인의 신체적 특징을 디지털화한 정보를 나타내며, 두 번째 항목의 경우 포인트 카드 회원번호나 온라인 서비스의 이용자 ID 등이 좋은 예시가 될 수 있다. 휴대폰 번호와 기기에 할당된 단말ID 등의 정보가 개인정보에 해당되는가의 의문이 제기되고 있지만, 개정 법률에서는 세부 사항을 정령으로 정하도록 되어있기 때문에 구체적인 확정은 향후 정령을 통해 이루어지게 된다. 나아가 민감정보(인종, 신앙, 사회적 신분, 병력, 범죄 경력, 범죄 피해 사실 등)가 포함된 개인정보의 경우 본인 동의를 얻어 취득하는 것을 원칙으로 의무화하고 본인 동의 없는 제3자 제공의 특례(opt-out)를 금지한다.[29]

### 2) 정보주체의 동의

27) 「일본 개인정보보호법」 제2조 제2항.
28) 「일본 개인정보보호법」 제2조 제5항.
29) 한은영, 전게논문, 2015, 42-43면.

기존 일본 개인정보보호법은 개인정보취급사업자가 특정된 이용목적 달성에 필요한 범위를 초과하여 개인정보를 취급하는 경우에는 정보주체의 동의를 얻어야 하며,[30] 개인데이터를 제3자에게 제공하는 경우에는 본인의 동의를 필요로 한다. 하지만 개정 법률에서는 개인을 특정할 수 있는 정보를 가공에 의해 익명화한 후 본인의 동의 없이도 데이터를 제공할 수 있는 '익명가공정보' 조항이 신설되었다. 이는 개인정보 활용을 통한 산업진흥의 발전을 위한 것으로 데이터 활용을 위한 법률의 규제를 완화한 것으로 볼 수 있다.

익명가공정보는 '특정 개인을 식별할 수 없도록 개인정보를 가공해 얻을 수 있는 개인에 관한 정보로서 당해 개인정보를 복원할 수 없도록 한 것'으로 정의된다.[31] 익명가공 정보를 취급하는 경우 '익명가공정보 취급사업자'[32]는 제3자 제공시 공표 및 명시의무(제37조), 식별행위 금지의무(제38조), 안전관리 조치의무 등(제39조)을 준수해야 한다. 즉 익명가공정보를 제3자에게 제공할 때는 익명가공정보에 포함된 개인에 관한 정보 항목 및 그 제공방법에 대하여 공표하는 동시에 해당 제3자에게 제공하는 정보가 익명가공정보라는 사실을 명시하여야 하며, 해당 익명가공정보를 다른 정보와 조합(照合)하거나 개인식별부호, 가공방법에 관한 정보를 취득하는 등의 방법으로 재식별하여서는 안 된다.

이번 개정에서는 익명가공정보 취급 이외에도 제3자 제공에 대한 규정이 늘었다. 개인정보를 제3자에게 제공하는 자는 개인정보보호위원회 규칙에 따라 해당 개인정보를 제공한 날짜, 제3자의 성명 또는 명칭, 기타 개인정보보호위원회 규칙으로 정하는 사항에 관한 기록을 작성하고 동 규칙에서 정하는 일정 기간 동안 보존하여야 한다. 제3자로부터 개인정보를 제공받는 자는 공급자의 성명 또는 명칭, 주소, 법인일 경우 그 대표자의 성명, 해당 개인정보의

30) 「일본 개인정보보호법」 제16조 1항.

31) i) 해당 개인정보에 포함된 기술 등의 일부를 제거한 것 ii) 해당 개인정보에 포함된 개인식별 부호의 전부를 제거한 것

32) 익명가공정보를 포함한 정보의 집합물이나 특정의 익명가공정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것, 그 외 특정 익명가공정보를 쉽게 검색할 수 있도록 체계적으로 구성한 것으로서 정령(政令, 시행령)으로 정하는 것을 사업에 이용하는 자를 말한다(제2조 제10항).

취득 경위를 확인해야 한다. 또한 해당 개인정보를 제공받은 날짜, 확인된 해당사항 등을 기록해야 한다. 이것은 불법으로 반출된 개인정보를 대상으로 본인이 의도하지 않은 유통이 일어나는 것을 방지하기 위한 것이다.

나아가 개인정보 취급사업자 또는 그 종업원(과거 종업원이었던 자 포함)이 그 업무와 관련하여 다룬 개인정보 데이터베이스 등(그 전부 또는 일부를 복제하거나 가공한 것을 포함)을 본인이나 제3자의 부정한 이익을 도모할 목적으로 제공하거나 도용한 경우 1년 이하의 징역 또는 50만 엔 이하의 벌금에 처하도록 규정한 조항도 신설되었다.[33]

## Ⅴ. 사물인터넷 개인정보보호를 위한 개선방향

사물인터넷의 경우 기기에 의하여 수집되어 송신되는 데이터에 제3자가 접근하여 이용할 수 있고, 이에 의하여 네트워크에 연결되어 있는 특정 사물인터넷 기기가 취약할 경우 서비스거부공격과 같이 그 기기가 연결되어 있는 네트워크와 다른 외부 시스템에 대하여 공격을 가하거나 신체적·물리적 위험을 야기할 수 있다.[34] 따라서 정보보호의 강화와 기기의 보안성 강화는 사물인터넷에 대한 소비자의 신뢰성 확보 및 사물인터넷을 활성화시키기 위한 중요한 요건 중 하나라고 할 수 있다. 이를 위한 방법에는 여러 가지 있겠으나 그 중 데이터의 비식별화 처리 및 이용자의 형식적 동의제도를 보다 실질적으로 개선하는 방법을 고려해 볼 수 있다. 이와 함께 정보처리자의 정보 활용의 활로를 열어주는 대신 이에 상응하는 엄격한 법적책임을 적용하여 개인정보가 침해되는 위험을 최소화 시키는 방법을 생각해 볼 수 있다. 나아가 국가적·개인적 차원에서의 이용자의 정보보호에 대한 중요성과 개인정보 침해 시 발생할 수 있는 위험성을 인식시키는 노력 또한 중요한 문제라 할 수 있다.

33) 한은영, 전게논문, 2015, 45면.
34) FTC, "Internet of Things", 2015, pp.10-14.

## 1. 비식별화 정보처리 및 동의요건 개선

앞서 살펴본 EU 및 일본의 경우 불과 몇 년 사이에 급변하고 있는 네트워크 초연결 사회에 대응하여 최근 개정안을 내놓는 등 개인정보보호 법제에 대하여 진지한 논의를 이어가고 있으며 이러한 세계적인 추세는 우리나라에도 많은 영향을 미칠 것으로 예상하고 있다. 빅데이터를 활용한 사물인터넷 기기의 증가, 데이터 급증, 분석 및 예측 기술의 고도화 등을 고려할 때 개인정보의 개념 범주를 명확히 하여 법제를 적용하는 것보다 현 시점에서 예측 가능한 식별과 비식별 정보의 범주를 기준으로 비식별 정보에 대한 조치와 동의규정을 논의하는 것이 적절하다고 보여진다.

현재 우리나라 대부분의 부처들은 비식별화 조치를 전제로 법률상 규정된 동의요건을 면제하는 데 초점을 두고 있다. 2014년 12월 방송통신위원회가 공표한 「빅데이터 개인정보보호 가이드라인」은 개인정보의 비식별화를 거친 정보 활용에 관해 법률상 정보주체의 동의요건을 면제해 주는 것이었으며 이후 미래창조과학부, 행정자치부 등은 이 가이드라인 내용과 거의 동일한 가이드라인을 출간해 오고 있다.[35] 하지만 실질적으로 사전 동의권은 추상적이고 방대한 양의 약관과 서비스 이용제한을 통해 형식적으로 행해지고 있으며, 이는 개인에 대한 보호라기보다 기업이 규제를 피해 정보 수집을 합리화시키고 피해에 대한 책임은 소비자가 떠안게 되면서 결국 정보주체의 권리를 실질적으로 보장 할 수 없는 문제가 발생할 수 있다.

빅데이터 분석기술의 발전으로 비식별 정보라고 하더라도 잠재적 식별 가능성은 언제나 존재한다. 즉 현재의 비식별정보가 영원한 비식별 정보는 아닌 것이다. 사전 동의 제도에서 반드시 동의를 거쳐야하는 개인정보는 식별이 가능한 정보에 한정하여 규제하고, 다른 정보와의 결합을 통해 식별 가능성은 있지만 그 범위가 포괄적인 경우 사후적 통제를 통해 해결하는 것이 형식적 사전 동의를 통한 위험성을 낮추고 개인정보자기결정권을 실질적으로 보장받을 수 있을 것이다.

35) 심우민, 전게논문, 2016, 2-3면.

사후통제와 관련하여 처리정지 등을 들 수 있는데, 미국연방거래위원회(FTC)의 경우 급속한 변화의 시대에 맞춘 소비자 개인정보 보호 보고서에서 구글, 페이스북, 마이크로소프트 등이 회원으로 있는 온라인 광고기업단체인 디지털 광고연합(DAA)에 올해 말까지 웹브라우저나 웹사이트에 이용자가 자신의 개인정보가 수집되는 것을 거부할 수 있는 '추적 금지 시스템'을 마련하라고 요구하였다. 추적금지 시스템은 웹사이트가 이용자의 인터넷 이용정보 등을 추적하는 것을 방지하도록 하여 이용자가 이를 클릭하면 정보 추적이 불가능하도록 한다. 또한 '데이터 브로커' 기업들을 관리할 수 있는 중앙통제 웹사이트를 통해 데이터 브로커들이 중앙통제 웹사이트에 개인정보 수집방법과 수집된 개인정보를 모두 공개할 것을 요구한바 있다.

## 2. 정보처리자의 정보활용 및 법적책임

개인정보보호의 실현을 위해서는 우선 정보처리자에 대한 법적책임을 강화할 필요가 있다. 최근 EU와 일본의 개정 법률을 보면 산업진흥을 위한 규제완화 측면의 차이는 있지만 정보처리자의 법적책임에 대해서 보다 엄격하게 적용하고 있다.

우리나라 역시 최근 법률개정을 통해 정보주체의 요구가 없더라도 수집출처 및 처리목적을 공지하도록 하거나, 특별한 경우를 제외하고 주민등록번호 처리를 제한하였으며, 징벌적 손해배상 도입 등을 통해 처벌 규정을 강화하였다. 그러나 처벌 규정을 강화한다 하더라고 개인정보 범주의 불명확성이라는 명분하에 개인정보는 유출되고 침해받게 될 것이다. 그렇다고 개인정보를 포괄적으로 적용시켜 처벌할 수는 없다. 개인정보보호 만큼 산업진흥 측면도 간과할 수 없는 중요한 부분이기 때문이다. 따라서 일본의 경우와 같이 특정 개인을 식별할 수 없도록 익명정보로 가공하여 활용할 수 있도록 함과 동시에 정보이동의 투명성과 법적책임을 엄격히 적용시켜 정보침해를 최소화 하는 것도 하나의 방안이라고 할 수 있을 것이다.

### 3. 정보보호에 대한 이용자의 의식 개선

법률개정도 중요한 사안이지만 정보보호를 위한 정보주체의 인식개선이 필요하다. 우리나라의 경우 몇 번의 정보유출 사고가 있었지만 이에 대해 많은 피해자들은 개인적인 사후대책마련의 어려움으로 문제를 회피해버리거나 어차피 어디선가 유출된 정보라는 식의 반응을 보이는 등 정보유출의 위험성에 대해 크게 문제의식을 가지고 있지 않는다는 것이다. 이러한 정보보호에 대한 안전 불감은 결국 사업자가 정보보호에 대한 의무감을 경감시키게 만드는 요인 중에 하나일수 있다는 것이다. 자신의 정보를 보호하기 위해 보다 적극적으로 인식하고 행동하는 것이 필요하며, 이를 위해 국가적 차원의 노력이 필요하다. 정보보안에 대한 위험의식이 낮다는 것은 그 위험성에 대해 잘 모른다는 것이고 이용자의 입장에서 빠르게 변하는 기술발전과 끊임없이 쏟아져 나오는 정보기기와 서비스들을 모두 비판적으로 판단하고 선택하기에 한계가 있을 수 있다. 따라서 현 시점에서 이용자의 인식개선을 위해 정부차원의 노력이 필요하다.

## Ⅵ. 결 론

사물인터넷은 새로운 산업혁명에 비견될 정도로 우리의 생활방식의 변화를 예고하고 있다. 사물인터넷은 보건·의료, 개인 및 공공의 안전, 자원관리, 물류 및 교육 등의 분야에서 개인과 사회에 많은 혜택을 가져다주는 등 생활의 편의를 증대시킬 뿐만 아니라, 산업구조의 변화를 가져와 생산성의 획기적 증대도 예상된다. 하지만 이로 인하여 개인의 모든 행동, 정보가 사물을 통하여 부지불식간에 수집되고 프라이버시 내지 개인정보의 보호와 보안에 대한 심각한 문제를 야기할 수 있다.

사물인터넷에 대한 논의의 핵심은 사물인터넷이 제공하는 혜택을 희생시키지 않으면서도 개인정보를 적절하게 보호하는 것이다. 이를 위해서는 다양한 의견이나 주장이 있을 수 있으나 하나의 방안이 모든 문제를 해결해 주는 것

은 아니며, 특정분야에 적절한 방안이 다른 분야에 대해서도 적절하다고 할 수도 없다. 그러나 사물인터넷 이용자의 신뢰가 곧 산업의 발전으로 이어짐은 부동한 사실이므로 개인정보 보호규범 및 보호원칙이 적용되어야 할 것이다. 신뢰를 획득하지 않으면 사물인터넷 기기의 광범위한 활용을 기대할 수 없고 따라서 기술의 진보에 따른 혜택을 누리지 못하게 된다. 따라서 산업 활성화에 따른 이익을 따지기에 앞서 이용자의 정보보호를 위한 실질적인 보호방안과 진지한 법적성찰이 필요하다.

## 참고문헌

□ 국내문헌

1. 단행본

권영성, 「헌법학원론」, 법문사, 2010.

김주영·손형섭, 「개인정보보호법의 이해」, 법문사, 2012.

성낙인 외 9인, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008.

성낙인, 「헌법학」, 법문사, 2014.

정종섭, 「헌법학원론」, 박영사, 2014.

한수웅, 「헌법학」, 법문사, 2014.

허 영, 「한국헌법론」, 박영사, 2014.

2. 논문

김민호, “개인정보처리자에 관한 연구”, 「성균관법학」 제26권 제4호, 2014, 241-266면.

김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 「공법연구」 제29집 제3호, 2001, 87-112면.

김승한, “사물인터넷 활성화를 위한 법제도 개선방향에 관한 연구”, 「한국경영정보학회 추계학술대회」, 2014, 545-555면.

권건보, “개인정보보호의 헌법적 기초와 과제”, 「저스티스」, 2014, 7-42면.
심우민, “사물인터넷 개인정보보호의 입법정책”, 「헌법학연구」 제21권 제2호, 2015, 1-36면.
이대희, “사물인터넷 활용과 개인정보보호”, 「경영법률」 제25집 제3호, 2015, 365-397면.
한은영, “일본 개인정보보호법 개정의 배경 및 개정안의 주요 내용”, 「정보통신정책연구 동향」 제26권 13호, 2014, 18-26면.
_____, “일본 개인정보보호법의 개정 내용 및 평가”, 「정보통신정책연구 동향」 제27권 제17호, 2015, 41-51면.
황창근, “사물인터넷과 개인정보보호”, 「외국법제정보」 통권 제46호, 2014, 79-113면.

3. 기관보고서

미래창조과학부, “사물인터넷(IoT) 정보보호 로드맵 3개년 시행계획”, 2015.
방송통신위원회, “비식별개인정보의 보호 및 활용에 관한 연구”, 「방송통신정책연구」, 2010.
_____, “EU 및 일본의 개인정보보호법제 및 감독체계 개편내용 분석”, 「방통융합정책연구」, 2014.
한국인터넷진흥원, “사물인터넷 보안 위협 동향”, 「Internet & Security Bimonthly」 제5호, 2014.
한국정보화진흥원, “사물인터넷 수요 및 시장동향”, 「IT & Future Strategy」 제15호, 2015.

□ 해외문헌

Adam Thierer, “The Internet of Things and Wearable Technology”, *21 RICH J. L. & TECH,* 2014.
Andrew J. Blumberg & Peter Eckersley, “On Locational Privacy and How to Avoid Losing it Forever”, *Electronic Frontier Foundation*, 2009.

FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change", *Federal Trade Commission*, 2012.
ITU Internet Reports, "The Internet of Things", 2005.
Rolf H. Weber, "Internet of Things-New security and privacy challenges", *Computer law and security review*, 2010.
Symantec, "Internet Security Threat Report", 2012.

[Abstract]

# Normative Study on Personal Information Protection in IoT Era

Shin, Hye-Won
*Ph.D. Student in Law at Sungkyunkwan University*
Ji, Seong-Woo
*Professor of Law at Sungkyunkwan University, Ph.D. in Law*

Internet of everything (IoT) has evolved from the individual and closed form within specific organizations or companies to an 'Everything as a Service', forming a kind of ecosystem by combining with surrounding technology, and ass it is applied to the actual living territory at the center of internet-based convergence, various economical value, increase in efficiency and increase in convenience are expected to become real. But because of this, individual's all behaviors and information may be collected involuntarily through objects, and cause serious problems regarding the protection and security of privacy or personal information using big data. In other words, it is directly applied to all objects in the real life and extends the threats in cyber space to real

life, individuals are facing the threat of personal information invasion or privacy invasion in the midst of the development of IoT that connects all objects and those objects to humans. To people that are defenselessly exposed to the leakage of personal information due to continuous hacking incidents, a serious consideration on whether there is only a bright future in IoT or not should be accompanied, and before calculating the profit due to revitalization of industry, practical protection plans and serious legal consideration for the protection of user information are needed.

**Key words** : Internet of Things, Personal information security, Right to informational self-determination, Personal information protection act, Data breach