

사물인터넷과 개인정보보호

황 창 근*

차 례

I. 서 론

II. 사물인터넷과 개인정보의 관계

1. 사물인터넷의 법적 성격
2. 사물인터넷과 개인정보의 갈등·조화
3. 법제도 현황
4. 외국의 정책 동향

III. 사물인터넷을 위한 개인정보보호법 제의 문제점

1. 사물인터넷에서 정보의 법적 성격
2. 수집·이용·제공에서의 정보주체의 사전동의의 문제
3. 개인위치정보의 제3자제공시의 즉시통보의무의 문제
4. 위치정보법과 사물인터넷 사업의 규율 문제

IV. 사물인터넷의 활성화와 개인정보 보호를 위한 조화로운 방안

1. 사물인터넷의 전제조건으로서의 보안기술의 발달
2. 입법모형과 입법 방향
3. 구체적인 개선 내용

V. 결 론

* 홍익대학교 법과대학 교수

접수일자 : 2014. 5. 30. / 심사일자 : 2014. 6. 20. / 게재확정일자 : 2014. 6. 25.

I. 서 론

2014년 4월 세월호의 참사가 가슴을 짓누르고 있을 때, 국내의 한 주간 경제지는 “세월호가 스스로 위험 감지해 참사 막았다면 … 빅데이터·통신·센서 기술 발달로 사물이 인터넷으로 연결 … 2020년 1980조 시장 전망”이라는 제목으로 사물인터넷을 커버스토리로 실었다.¹⁾ 이 제목은 사물인터넷이 세월호의 참사까지 막을 수 있었을 것이라는 비유로 그 기대를 보여주고 있다. 사물인터넷(Internet of Things, IoT)^{2),³⁾라 함은 사람과 사물, 공간 등의 모든 것들이(Things)⁴⁾ 인터넷으로 서로 연결되어 모든 것들에 대한 정보가 수집·생성되고 활용되는 것을 의미하고,^{2),³⁾ 이 개념은 2005년 ITU가 1997년부터 진행된 레포트인 ‘네트워크의 도전(Challenges to the network)’이라는 시리즈물에서 사물인터넷을 다루면서 공식적으로 등장하였으며, 당시 사물인터넷을 언제, 어디서나 어느 것과 연결되는 통신환경이라고 정의하였다.⁴⁾}}

사물인터넷은 사물통신(Machine to Machine,, M2M), 싱터넷(Thingternet), 사물지능통신, 만물인터넷(Internet of Everything, IoE), Internet of objects라고도 불린다. 인터넷과 모바일 시대의 1차 디지털혁명에 이은 2차 디지털 혁명⁵⁾, 제3차 생산성혁명⁶⁾으로 불릴 정도로 경제적·기술적 변화의 시작이기도 하고, ICT환경을 포함한 사회문화적인 환경을 총칭하는 개념이기도 하다. 사물인터넷은 기술적으로 단말/센서, 유·무선 네트워크, 서비스 플랫폼, 애플리케이션으로 구성된다.⁷⁾ 사물인터넷의 발전은 클라우드컴퓨

1) 이코노미스트, 1235호, 2014.5.5, 30-41쪽

2) 정혁·이대호, “사물인터넷의 진화와 정책적 대안”, KISDI Premium Report, 14-3, 2014.4.23, 2쪽

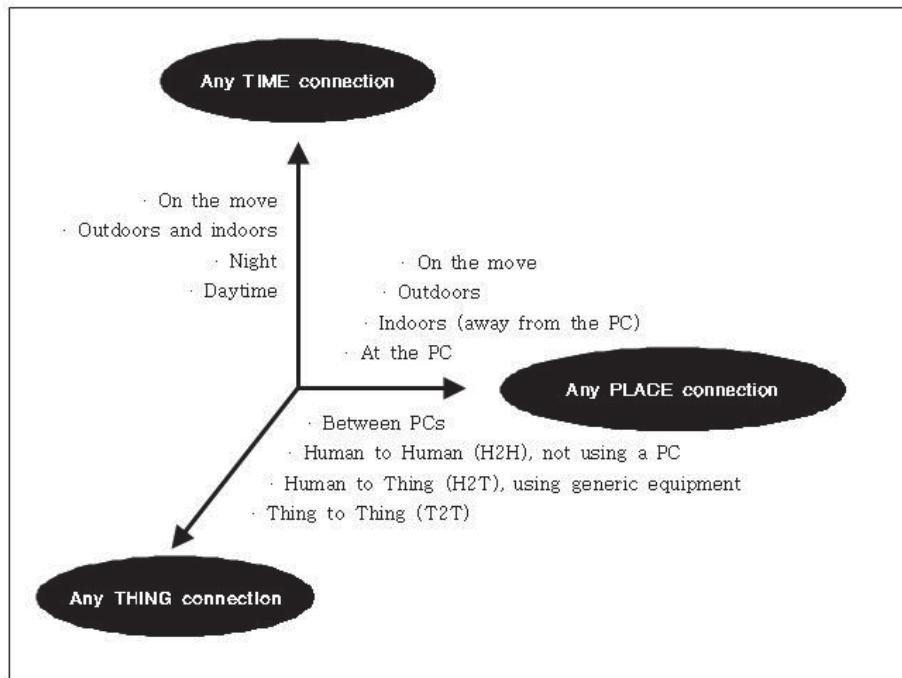
3) Internet of Things(IoT)라는 용어는 1998년 Kevin Ashton⁵⁾ 처음으로 사용하였다. Rolf H. Weber, “Internet of Things - New security and privacy challenges”, computer law and security review, 26, 2010, p.23

4) ITU, *ITU Internet Reports 2005 ; The Internet of Things*, November 2005, p.2

5) 매일경제 IoT 혁명 프로젝트팀, 「모든 것이 연결되는 세상 사물인터넷」, 매일경제신문사, 2014, 43쪽

6) 매일경제 IoT 혁명 프로젝트팀, 앞의 책, 171쪽

7) 강달천, “ICT산업의 발전과 개인정보 법제의 문제”, 인터넷법제도포럼 발표자료, 2014. 4. 30. 8쪽



<그림 1> ITU의 IoT 개념

출처 : ITU(2005)

팅, 미래인터넷(Future Internet), 빅데이터, 로봇공학, 시맨틱기술(semantic technology)과의 결합이 시너지를 발휘할 것으로 기대된다.⁸⁾

IoT는 민간, 공공 부문을 불문하고 사회 전영역에서 사용될 것으로 예상된다. IoT가 적용되는 분야로는 스마트 시티, 스마트 환경, 스마트 워터, 스마트 측정, 안전 및 에너지, 소매, 통계, 산업 통제, 스마트 농업, 스마트 동물농장, 스마트 홈, e헬스 등 다양하다.⁹⁾ 이를 통하여 IoT는 사회적 약자의 스마트한 일상생활을 보장하는 사회적 책임을 다할 것으로 전망된다.¹⁰⁾ 현재 100억개 정도의 인터넷 연결 사물수가 2020년에는 500억 개 정도로 늘어나고, 1인당 연결 사물 갯수가 2020년에 10개에서

8) Peter Friess, "Driving European Internet of Things Research", Ovidiu Vermesan and Peter Friess(ed.) *Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publisher, 2013, p.2

9) Ovidiu Vermesan, "Europe's IoT strategic research agenda 2012", Ian G Smith(ed.) *The Internet of Things 2012 New Horizons*, 2012, Halifax, p.36-39

10) Ovidiu Vermesan et el, "Internet of Things Strategic Research and Innovation Agenda", Ovidiu Vermesan and Peter Friess(ed.) *Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publisher, 2013, p.136

2030-2040년경에는 200개로 늘어날 것으로 예측하고 있다.¹¹⁾ 사물인터넷의 경제적 효과도 지대하다. 시스코의 예측에 의하면 사물인터넷은 향후 10년간 14조4천억달러의 시장을 형성할 것으로 추정되고,¹²⁾ 세계 각국은 이를 중요한 ICT산업으로서 다양한 정책을 추진하고 있다.¹³⁾ IoT에 대하여 독일에서는 18세기 후반의 1차 산업혁명, 20세기 초반의 전력을 도입한 2차 산업혁명, 1970년대 ICT 확산으로 인한 3차 산업혁명에 이은 4차 산업혁명(Industry 4.0)으로 추진되고 있다.¹⁴⁾ 우리나라에서도 2014년 「사물인터넷 기본계획」을 수립하였고, ICT R&D 중장기 전략의 10대 기술로 선정하고 있으며 사물인터넷의 국가표준 개발 및 세계 표준 채택을 위한 협의체를 구성하고 있다.¹⁵⁾

그런데, IoT에게 장밋빛 미래만 있는 것이 아니다. 모든 사물을 연결하고, 그 사물에 사람을 연결하는 사물인터넷의 발달에서 개인은 개인정보의 침해 내지 프라이버시 침해라는 새로운 도전을 받고 있다.¹⁶⁾ ITU는 2005년 IoT에 대한 레포트에서 정보보안, 정보보호 문제를 심각한 이슈로 받아들이고 있다.¹⁷⁾ 그런 관점에서 이 글은 우리 사회의 새로운 변화촉매 제가 될 사물인터넷의 발달을 위하여, 그리고 그로부터 발생될 개인정보의 침해와 보호 문제를 다루고자 한다. 아직 어느 나라에서도 이와 관련하여 직접적으로 입법화한 적은 없기 때문에 기존의 개인정보보호법리를 적용하여 장래 IoT의 진흥과 개인정보의 보호라는 양 측면에서 논리를 전개하고자 한다. 이를 위하여 IoT환경에서 개인정보의 침해 위험성과 그 특징을 알아보고, 개인정보보호와 관련된 이슈를 발굴하고, 외국의 정책

11) 매일경제 IoT 혁명 프로젝트팀, 앞의 책, 47쪽

12) 한국인터넷진흥원, “공공 부문 사물인터넷 도입 효과, 향후 10년간 4조 6,000억 달러 전망”, 「Internet & Security Bimonthly」, 2014년 1호, 34쪽

13) 자세한 내용은 민경식, “주요국의 사물인터넷 정책동향”. IT R&D 정책동향, 정보통신전파진흥연구원, 2012.9. 1-24쪽 참조

14) 매일경제 IoT 혁명 프로젝트팀, 앞의 책, 215쪽

15) 미래창조과학부, 사물인터넷 활성화를 위한 제도개선 및 정책협력 방안 연구, 연구보고서, 2013.11, 54쪽

16) Tobias Kowatsch and Wolfgang Maass, “Privacy concerns and acceptance of IoT services”, Ian G Smith(ed.) *The Internet of Things 2012 New Horizons*, 2012, Halifax, p.176

17) ITU, supra note 4, p.9

이나 논의동향을 정리한 후에 우리 법제에 대한 문제점을 분석하여 바람직한 개선방향을 도모하고자 한다. 우리 법제의 분석에서는 특히 사물인터넷과 밀접한 관련을 가지고 있는 위치정보법을 중심으로 사물인터넷의 활성화 및 개인정보보호를 위한 제반 문제점을 분석하고 개선방향을 도출하고자 한다. 아울러 최근 제정된 「정보통신 진흥 및 융합 활성화 등에 관한 법률」(이하 ICT 특별법이라 함)이 사물인터넷의 활성화에 어떤 역할을 할 것인지도 아울러 검토하기로 한다.

II. 사물인터넷과 개인정보의 법률관계

1. 사물인터넷의 법적 성격

사물인터넷의 개념은 앞서 본 바와 같이 사람과 사물, 공간의 모든 것들이 인터넷에 연결되어 정보가 활용되는 것이라고 기술적으로 정의되지만, 이것이 법적인 의미를 가지기 위하여는 사물인터넷을 이용하는 사람의 법률관계를 형성할 수 있어야 한다. 단순히 사물간의 인터넷에서 정보가 교환되고 활용된다는 것은 기술적인 의미를 넘어 그 사물인터넷을 이용하는 사람에게 법적인 효과가 있어야 한다. 따라서 사물인터넷의 법적 성격은 사물인터넷의 이용에 따라 발생되는 각종 법률관계를 일컫는 것이 될 것이다.

전기통신사업법에 의하면, 사물인터넷은 통신을 매개로 사물과 사물, 사물과 사람간을 연결하는 것이므로 전기통신사업법상의 기간통신사업자의 지위를 가진다.¹⁸⁾ 동법에서는 기간통신사업을 “전기통신회선설비를 설치하고 그 전기통신회선설비를 이용하여 기간통신역무를 제공하는 사업”(제5조제2항)으로 정의하고 있으며, 기간통신역무는 “전화·인터넷접속 등과 같이 음성·데이터·영상 등을 그 내용이나 형태의 변경 없이 송신 또는 수신하게 하는 전기통신역무 및 음성·데이터·영상 등의 송신 또는 수신이 가능하도록 전기통신회선설비를 임대하는 전기통신역무를 말한다.

18) 미래창조과학부, 앞의 보고서, 24쪽

다만, 미래창조과학부장관이 정하여 고시하는 전기통신서비스(제6호의 전기통신역무의 세부적인 개별 서비스를 말한다. 이하 같다)는 제외한다”(제2조 11호)라고 정의하고 있다.

『위치정보의 보호 및 이용 등에 관한 법률』(이하 위치정보법이라 함)상으로는, 사물인터넷은 사물과 사물, 사물과 사람의 통신을 개념으로 하는 이상 사람의 위치정보를 수집하거나 이용하게 될 가능성이 높다고 할 것 이므로 위치정보사업자, 위치정보기반사업자의 지위를 가진다. 마찬가지로 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(이하 정보통신망법이라 함)을 이용한 위치정보 내지 개인정보의 이용과 관련하여 정보통신망법상의 정보통신서비스제공자의 지위를 가진다. 또한 개인정보보호의 수집과 이용을 하게 되므로 개인정보보호법상 개인정보처리자로서 개인정보보호법의 적용을 받게 된다.

또한, 2014. 2. 14.부터 시행되고 있는 ICT 특별법에 의하면 새로운 기술과 서비스가 기존의 법규에 의하여 허가 등을 받을 수 있는 근거가 없는 경우에는 정부에 신속처리를 요청하고, 신속처리를 하지 못하는 경우에는 임시허가를 통하여 조기에 사업화를 할 수 있는 규정을 마련하고 있다(제36조, 제37조). 이는 ICT를 기반으로 한 새로운 기술과 서비스가 기존의 법규에 의하여 제약을 받는 것을 피하기 위하여 새로운 진흥정책으로 고안된 것이다. 사물인터넷은 위 ICT 특별법상 새로운 기술이나 서비스에 해당되어 신속처리나 임시허가를 통하여 시장에서 사업화를 할 수 있게 된다. 다만 ICT 특별법에서는 동법이 정보통신 기술·서비스 등의 진흥 및 융합 활성화와 관련하여 우선하여 적용하도록 특별법의 성격을 가지는 것으로 규정하고 있으므로(제4조), 만일 사물인터넷이 이와 같이 정보통신 기술·서비스로서 진흥 및 융합 활성화를 위한 것이라면 다른 일반법규에 우선하여 적용되는 것으로 보이지만 실제 적용관계가 분명하게 해석할 수 있는 것이 아니다. 예를 들어 사물인터넷을 위 ICT 특별법 소정의 임시허가절차에 따라 사업화를 하더라도, 그와 관련된 개인정보 보호 이슈에 대하여는 여전히 개인정보보호법제의 적용을 피할 수 없는 것으로 보인다. 결국 ICT 특별법이 사물인터넷과 관련하여 의미를

가지는 것은 만일 다른 법에서 사업규제 방식을 가지고 있고 그것이 서비스의 진흥이나 융합의 활성화와 관련이 있다고 한다면 이 법에 의한 사업이 원활해 질 수 있다는 점일뿐이다.

그밖에 사물인터넷이 적용되는 개별법상의 지위를 가지는바, 예컨대 원격진료서비스의 경우에는 의료법을 사물인터넷과 관련하여 어떻게 해석하고 적용할 것인가의 법적 문제가 발생된다.

2. 사물인터넷과 개인정보의 갈등·조화

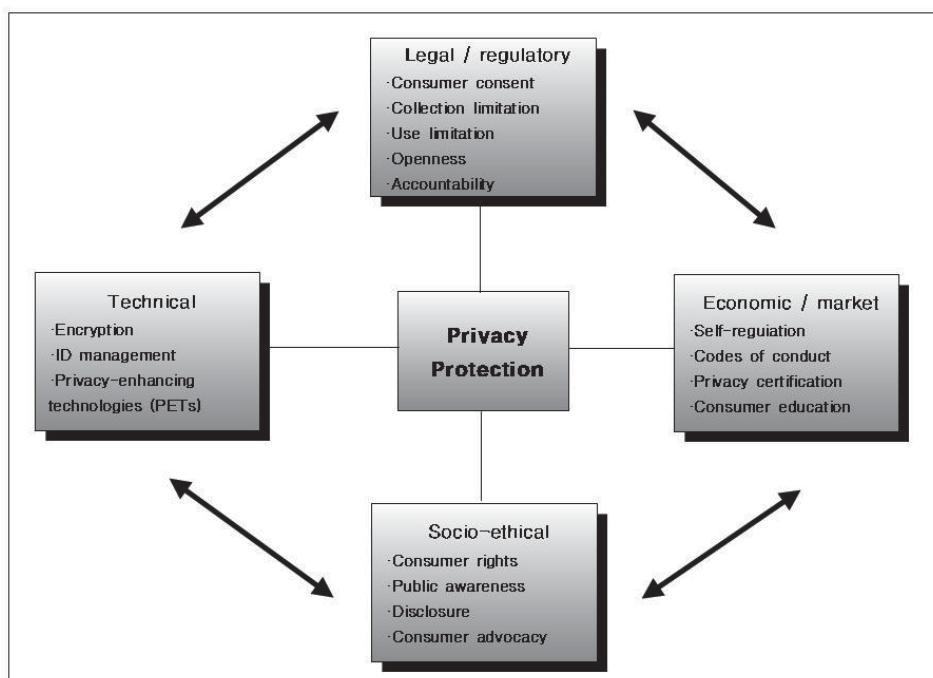
사물인터넷과 개인정보는 각 활성화와 보호라는 가치가 충돌하는 관계이다. 위치정보법을 포함한 개인정보보호법제가 사물인터넷 발달의 법적 장애가 될 수 있다는 것이 논의의 핵심이고, 양자의 갈등관계를 어떻게 풀어갈 것인가 하는 문제가 중심 과제이다. IoT에서의 개인정보보호문제는 사물인터넷을 보다 안전하게 하고, 이용자, 시장, 정부의 신뢰를 바탕으로 발전을 이루는 것을 목표로 한다. 사물인터넷의 개념을 처음으로 정립한 2005년 당시 ITU도 개인정보의 문제를 해결하지 않으면 사물인터넷의 발달의 장애가 될 것이라고 경고하였다.¹⁹⁾

IoT에서 개인정보와 프라이버시의 이슈는 새삼스러운 것이 아니다. 기존의 인터넷에서도 프라이버시, 보안문제, 개인정보보호문제 등은 계속적으로 제기되었다. 그러면 IoT에서는 어떤 차별성을 가지고 있는지 보면, IoT는 개인이나 사물이 인식하지 못한 상태에서 자동적으로 연결되고, 사람과 사물의 요구는 원격에서 이루어지는 것을 특징으로 한다.²⁰⁾ IoT에서의 개인정보 이슈는, 첫째 많은 디바이스가 방화벽(Firewall)과 같은 잘 알려진 체계로 더 이상 보호되지 않고 무선채널을 통하여 직접적인 공격을 받거나 또는 디바이스 자체가 절취당하는 등의 침해위협이 발생되며, 둘째 정보제공자와 정보이용자 사이에는 신뢰가 결여된 상태에서의 다양한 소스로부터 수집된 정보의 결합이 문제가 되며, 셋째 디바이스와 정보 이

19) ITU, *supra note 4*, p.9

20) Gianmarco Balini et el, “Internet of Things Privacy, Security and Governance”, Ovidiu Vermesan and Peter Friess(ed.) *Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publisher, 2013, p.208

용자 사이에 안전한 정보교환이 필요하다는 것이다.²¹⁾ ITU는 개인정보의 문제를 법제도적 측면 이외에도 시장의 측면, 사회윤리적 측면, 기술적 측면으로 나누어 자세한 관찰을 하고 있다(아래 <그림 2> 참조).²²⁾



<그림 2> 개인정보 보호의 다양한 측면

출처 : ITU

같은 맥락에서 침해 위협으로 유형화하면 기술적인 이슈(시스템위협과 데이터위협), 인적 이슈(서비스이용자와 서비스제공자 측면), 법·제도적 이슈(보안규제의 미비와 법제도내의 충돌상황)로 나눌 수 있다.²³⁾

-
- 21) Jens-Matthias Bohli, Peter Langendorfer and Antonio F.Skarmeta, "Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities", Ovidiu Vermesan and Peter Friess(ed.) *Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publisher, 2013, p.241
- 22) ITU, *supra note 4*, p.8 ; Bilel Jamoussi, "IoT Prospects of Worldwide Development and Current Global Circumstances", p.22 (www.itu.int/en/ITU-T/.../1010-B_Jamoussi_IoT.pdf. 2014.5.19. 검색)
- 23) 배진석·조우재·정윤혁, "Privacy Issues in IoT Communication", 2013년 한국경영정보학회 추계학술대회 자료집, 764-765쪽. <표 1>은 본문의 내용을 재구성하였음

<표 1> IoT에서의 개인정보 침해요소

| 구 분 | 내 용 | |
|----------|-----------|--|
| 기술적 이슈 | 시스템 위협 | 전통적·물리적 위험(화재, 도난 등) 시스템의 오류 외부자의 공격(DDOS, 해킹 등) |
| | 데이터 위협 | 칩 저장 데이터와 서버(내장성)에 대한 공격 이동성 데이터 공격 |
| 인적 이슈 | 서비스 이용자 | 정보에 대한 책임, 통제권 |
| | 서비스 제공자 | 불필요한 수집과 저장 관리소홀로 인한 누출 |
| 법·제도적 이슈 | 보안규제 미비 | 표준의 미비 |
| | 법·제도내의 충돌 | 개인정보보호법제, 저작권법 등 |

예를 들어 RFID(Radio Frequency Identification)를 보면, 태그 내부에 저장된 사용자의 정보가 공개될 수 있고, 정보가 노출되지 않더라도 태그가 가지는 고유한 값을 통한 사용자의 위치추적이 문제가 될 수 있으며, 정보가 노출될 경우 그 태그와 관련된 사용자에 대한 이전의 모든 행적이 모두 노출될 위험이 있다.²⁴⁾

법적인 측면에서 이 문제를 해결하기 위하여는 IoT에서, 첫째 국가의 법적 규제 내지 시장규제가 필요한가, 둘째 만일 법적 규제가 예상된다면 전통적인 법적 규제로 충분한 것인지 아니면 새로운 법이 필요한 것인지, 셋째 새로운 법규제가 필요하다면 어떤 법률이 필요하고 그 시행 시점을 어떻게 설정할 것인가 하는 점으로 요약된다.²⁵⁾

3. 법제도 현황

우리나라에서 개인정보보호법제가 마련된 것은 1999. 2.8. 정보통신망이용촉진등에관한법률에서 최초로 개인정보보호 관련 규정을 도입하였고, 이후 위치정보법이 2005년에, 공공기관의 정보보호에 관한 법률이 1994년에 제정되었다가, 2011년 개인정보보호법이 제정되었다. 그 외에도 여러

24) 방송통신위원회, 사물통신(Machine-to-Machine)에서의 정보보호를 위한 효율적 인증시스템 연구, 연구보고서, 2010. 9. 30. 89쪽

25) Rolf H. Weber, *supra* note 3, p.26

분야에서 개인정보보호와 관련된 법률이 마련되기도 하였다.

현재 사물인터넷과 관련된 법제 현황을 보면 「전기통신사업법」, 정보통신망법, 위치정보법, ICT 특별법 등이 있다. 그러나 위 법들이 특정한 ICT서비스를 정의하고 규율하는 법이 아닌 이상 사물인터넷을 직접적으로 언급하고 있는 것은 아니다. 사물인터넷과 가장 밀접한 관련이 있는 개인정보보호법제가 위치정보법이다. 위치정보법은 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등의 보호와 이용 활성화라는 2가지 목적으로 입법되었는바(제1조), 사물인터넷은 필연적으로 위치정보의 활용과 관련이 있으므로 위치정보법의 제반 사항을 준수하는 것이 필수적이다. 그런데 위치정보법은 다른 나라에서 유례를 찾아볼 수 없는 입법이고, 개인정보보호법 보다도 먼저 생겼다. 당시 위치정보를 오·남용하는 것을 방지하기 위하여 위치정보를 규율하게 된 입법적 연혁이 있는데, 그 후 개인정보보호법도 제정되고 사물인터넷과 같은 새로운 서비스를 적용함에 있어서 법적 장애로 대두되고 있다. 사물인터넷상 개인정보는 위치정보법상 개인위치정보 내지 개인정보보호법상 개인정보에 해당된다. 개인정보보호법에 의한 개인정보는 생존하는 개인에 관한 정보로서 특정한 개인을 알아볼 수 있는 정보를 말하고, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 포함하기 때문에 사물인터넷에 수반된 개인위치정보는 개인정보일 수밖에 없다. 따라서 사물인터넷에는 개인정보보호법상 개인정보의 보호에 관련된 제반 규정이 적용되게 되는 것이다. 정보통신망법도 개인정보의 개념을 개인정보보호법과 동일하게 규정하고 있고, 개인정보의 수집·이용시에 사전동의방식을 취하고 있는 등 개인정보보호법과 유사하게 규정되어 있다. ICT 특별법은 신규 기술 및 서비스의 진흥 및 활성화를 다루고 있기 때문에, 사물인터넷의 진흥에 중요한 역할을 할 것으로 기대된다.

방송통신위원회는 2009년 ‘사물통신 기반 구축 기본계획’을 발표하여 법제도개선을 추진하였고, 미래창조과학부는 2014년 ‘사물인터넷 기본계획’을 수립하여 체계적인 사물인터넷의 진흥과 활성화를 도모하고 있다. 기본계획의 3대 추진과제로 ① 창의적 IoT 서비스 시장창출 및 확산, ②

글로벌 IoT 전문기업 육성, ③ 안전하고 역동적인 IoT 발전 인프라 조성을 정하였다. 기본계획에 따라 미래창조과학부는 5.13. 사물인터넷 혁신센터를 설치하고 본격적인 진흥정책을 시행하고 있다. 개인정보보호와 관련하여 기본계획은 사물인터넷 분야 보안기능·성능을 검증하는 보안 테스트 베드의 조성, 사물인터넷 제품·서비스에 보안 내재화를 위한 가전, 헬스케어 등 IoT 보안 분야 시범 사업의 추진, 사물인터넷 제품에 탑재되는 운영체제 등 보안기술 개발의 확대, 및 보안기술 문제해결 전문가인 ‘사물인터넷 정보보호 코디네이터’ 양성을 내용으로 하고 있다.²⁶⁾

4. 외국의 정책 동향

(1) EU

사물인터넷에서 프라이버시 내지 개인정보의 보호 문제를 가장 활발하게 논의하는 곳은 EU이다. EC(The European Commission)은 2009.5.12. 프라이버시 및 개인정보 보호원칙 (Prvacy and Data Protection Principles)에서 RFID를 합법적, 윤리적, 사회적, 그리고 정치적으로 적용할 수 있는 방법을 권고(recommendation)하였는데, 이는 EU가 처음부터 사물인터넷과 RFID에 있어서의 정보보안과 프라이버시 이슈를 인식함을 보여준다.²⁷⁾ 또한, EU Commission은 2009.6. 유럽을 위한 사물인터넷 액션 플랜 (Internet of Things-An action plan for Europe) 14개(Line of Action)²⁸⁾를 발표하였는데, 그 중에 개인정보의 오용가능성에 대한 적절한 보호방안이 사물인터넷에 대한 신뢰와 수용의 전제조건이 된다고 보고 있다. 2번째 액션에서 ‘개인정보보호를 위한 모니터링(Continuous monitoring of the privacy and the protection of personal data questions)’을 설정하고 프라이버시와 개인정보의 문제점에 대한 계속적인 모니터링을 주된 내용으로 하고 있다. 3번째 액션에서는 ‘silence of the chips’에 관한 권리에 법적,

26) 미래창조과학부, 사물인터넷 기본계획

27) Rolf H. Weber, *supra* note 3, p.25

28) Commision of the European Communities, Internet of Things – An action plan for Europe, 2009.6.18

기술적 논쟁을 예상하고 언제든지 네트워크를 끊을 수 있어야 한다는 것을 지적하고 있다.²⁹⁾ 또한 2013. 6.에는 사물인터넷포럼을 창설하여 개인정보보호, 윤리규범의 형성 등을 목표로 연구하고 있다. 또한 유럽의회는 자동차사고 시 응급상황을 자동으로 알려주는 eCall(emergency Call)을 모든 차량에 2015년까지 의무적으로 장착하도록 의무화하여 IoT를 실생활에 적용하고 있다. EU는 사물인터넷 활성화를 위하여 3가지 접근방법 즉 무조치(No Action), 연성법(Soft Law), 경성법(Hard Law)적 접근 중에서 가이드라인의 제정, 커뮤니케이션 형성 등 사물인터넷의 발달을 간접적으로 자극할 수 있는 준(準)법적 제도의 활용이 선호되고 있다.³⁰⁾ 사물인터넷 연구기관인 IERC(The European Research Cluster on the Internet of Things)는 많은 활동을 하고 있는데, 특히 프라이버시, 보안, 거버넌스에 대하여는 Activity Chain 05가 집중적인 연구를 수행하고 있다. 향후 전망에 의하면 2020년이 지나면 프라이버시와 보안에 대한 분명한 규범이 채택될 것으로 예상하고 있다.³¹⁾

(2) 미국

미국은 통일된 개인정보보호법제가 존재하지 아니하고 분야별 개인정보보호법제를 가지고 있는데, 사물인터넷 관련한 정보보호를 직접 다루는 법제는 물론이고 독자적인 위치정보를 다루는 법제도 존재하지 아니한다. 또한 과학기술의 발전에 따른 프라이버시 이슈를 다룬 연방법률이 존재하지 않는다. 마찬가지로 사물인터넷 관련한 개인정보보호 문제는 일반적인 개인정보보호문제로 접근하는 것이 타당하다. RFID가 본격적으로 이슈가 되던 2007년경에 미국 전역에서 RFID의 활용으로 인한 개인정보의 수집을 공개하는 입법을 몇 개주는 시도하였으나 연방 차원에서는 입법이 존재하지 않는다.³²⁾

29) Rolf H. Weber, *supra* note 3, p.26

30) 정보통신산업진흥원, “사물인터넷 발전을 위한 EU의 정책 제안”, 해외 ICT R&D 정책동향, 2013.6월, 52쪽

31) Ovidiu Vermesan, *supra* note 10, p.136. Table2.2

32) Mariko Yoshihara, *RFID and Privacy*, Public law Research Institute UC Hastings College

미국에서는 국가정보위원회(NIC)가 IoT를 2025년까지 미국의 국가경쟁력에 영향을 미칠 수 있는 6대 혁신적인 파괴적 기술(Disruptive Civil Technology) 중 하나로 지목하였다.³³⁾ 연방거래위원회(FTC)는 2013.11. 소비자보호 차원에서 사물인터넷으로 발생된 광범위한 프라이버시와 보안이슈를 주제로 업계, 학계 등이 참여하는 대규모의 워크샵을 개최하였는데, 동 워크샵에서는 프라이버시와 보안이슈의 한계, 새로운 디바이스의 통지와 동의문제, 새로운 환경에서의 프라이버시와 보안을 위한 바람직한 정책방향, 산업활성화를 위한 유인책 등이 논의되었다.³⁴⁾ 이러한 규제 움직임에 대하여 업계에서는 사물인터넷 활성화에 걸림돌이 될 수 있다는 반론이 제기되고 있다.³⁵⁾

(3) 일본

일본은 2009년 총무성이 주관하여 사물인터넷 사회 실현을 위한 워킹그룹을 결성하고 ‘사물인터넷 시대 실현을 위한 선결 과제’를 검토하였다. 선결과제에는 제도적 측면, 서비스 및 비즈니스 측면, 기술적 측면으로 나누었는데, 사생활 및 개인정보 보호와 센서 네트워크와 전자태그 이용에 따른 사생활침해 여부에 대한 검토가 제도적 측면에서 선정되었고, 또한 보안 확보를 위한 대책 추진이 서비스 측면의 과제로 선정되었다. 또한 2011년 8월 경제산업성은 ‘IT융합에 의한 신산업 창출 전략’에서 보안대책을 선결과제로 제시하고 있다.³⁶⁾

of Law, 2008, p.7(<http://gov.uchastings.edu/public-law/docs/plri/RFID.pdf>). 2014.5.29. 검색)

33) 민경식, 앞의 글, 5쪽

34) FTC, Internet of Things - Privacy and Security in a Connected World, 2013.11.19. (<http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>). 2014.6.26. 검색)

35) WSJ, “Setting Rules for the Internet of Things”, 2014.1.9.

(<http://blogs.wsj.com/digits/2014/01/09/setting-rules-for-the-internet-of-things/>). 2014.6.26. 검색)

36) 이상 일본의 정책동향은 민경식, 앞의 글, 12-14쪽 참조

III. 사물인터넷을 위한 개인정보보호법제의 문제점

1. 사물인터넷에서 정보의 법적 성격

(1) 사물인터넷상 사물정보의 성격

사물인터넷에서 제기되는 사물정보 또는 사물정보와 관련된 개인정보가 개인정보보호법제상 개인정보에 해당되는지 검토를 요한다. 사물인터넷은 사물과 사물, 공간, 사람의 연결을 전제로 하므로, 사물과 사람, 공간(위치)에 대한 다양한 정보를 기반으로 한다. 사람에 대한 정보는 그것이 특정인을 인식하는지 여부에 따라 개인정보가 되기도 하고 그렇지 아니하기도 한다. 통상 사물인터넷과 관련되는 정보는 사물에 대한 모니터링(monitor for products), 동물에 대한 모니터링(monitor for animals), 개인에 대한 모니터링(monitor for persons), 프로파일링 목적의 정보 수집(collect data for profiling purposes) 등의 4가지 목적으로 구분할 수 있다.³⁷⁾ 이에 따라 사물이나 동물에 대한 정보는 사물정보로, 개인에 대한 정보는 개인정보로 나눌 수 있다. 사물에 대한 정보는 “센서네트워크와 텔레메트리 등의 기술에서 사물을 이용하여 특정한 목적을 위하여 광 또는 전자적 방식으로 처리되어 부호, 문자, 음향 및 영상으로 표현된 모든 종류의 자료 또는 지식을 말하는 것”으로 정의된다.³⁸⁾ 문제는 이와 같은 사물정보가 개인정보가 될 수 있는가 하는 점이다.³⁹⁾ 사물정보는 그 자체로는 개인을 식별하는 개인정보가 되지 못하지만, 개인과 연계를 맺게 되는 경우에는 개인정보가 될 수도 있다.⁴⁰⁾ 사물정보 중에서 사물의 식별과 인증에 사용되는 정보는 개인정보로서 보호가치가 있다.⁴¹⁾ IP주소나

37) Viola Schmid, “radio frequency identification law beyond 2007”(http://tuprints.ulb.tu-darmstadt.de/1296/1/CylawReportXXIV_RFID_090106MB.pdf. 2014.5.29.)

38) 방송통신위원회, 앞의 보고서, 82쪽

39) Viola Schmid, *supra* note 34

40) RFID정보가 비록 개인을 직접적으로 식별할 수 있는 정보는 아니지만 다른 정보와 용이하게 결합하여 개인정보성을 가진다는 견해도 같은 취지이다. 배대현, “유비쿼터스 사회로의 발전추세에 따른 RFID 관련 법률문제 검토”, 법조, 제40호, 법무부, 2007.10, 15쪽

MAC주소가 사물식별정보의 대표적인 예이다. 또한 사물정보나 개인정보가 특정시간이나 위치와 결합할 때 즉 이동성을 가질 때에는 위치정보로서 위치정보법의 적용을 받는다. 위치정보법에 따른 위치정보를 분류하면 먼저 물건에 대한 위치정보와 개인에 대한 위치정보로 나누고, 개인에 대한 위치정보는 식별성이 있는 개인에 대한 위치정보(개인위치정보)와 식별성이 없는 개인에 대한 위치정보로 분류할 수 있다. 그 중에서 개인의 위치에 관한 정보를 개인위치정보라고 하여 위치정보법에서 개인정보보호법과 별도로 보호대상으로 한다. 개인정보보호법상의 개인정보와 위치정보법상의 개인위치정보의 개념은 상당한 차이를 보여준다. 위치정보는 개인의 식별성을 넘어서 특정시간대의 위치를 보여주는 것이므로 ‘민감정보’, 위치확인 서비스에 의하여 제작된 ‘제작정보’, 시간의 흐름에 따라 계속 변화하는 ‘동적정보’의 성격을 가지는 것으로 일반적으로 개인정보의 일종이지만 차이가 있다.⁴²⁾

(2) 위치정보의 개념 혼란과 보호범위의 문제점

사물인터넷과 관련된 정보는 사물에 관한 정보, 개인에 관한 정보 등이 포함되고, 특정 시간대의 위치에 관한 정보이면 현행 위치정보법상 위치정보가 된다. 위치정보법은 익명화된 개인정보나 단순 위치정보, 사물정보 등 일체의 위치정보를 규율대상으로 삼고 있고, 특히 개인을 특정할 수 없는 불특정다수에 대한 익명성 정보도 규율대상으로 삼는 만큼 사물인터넷의 장애요인이 될 수 있다. 현행 위치정보법상 위치정보는 ‘이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것’(제2조제1호)이라고 정의되어 있기 때문이다. 이 중 개인위치정보는 ‘특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와

41) 방송통신위원회, 앞의 보고서, 92쪽

42) 국가과학기술정보통신위원회, 위치정보의보호및이용등에관한법률안 검토보고서, 2004.12, 6~7쪽

용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다'(제2조제2호)고 규정하여 개인정보보호법상 개인정보의 성격을 가지고 있다.

그리고, 개인위치정보는 일반적인 개인정보의 개념과 동일하게 “다른 정보와 용이하게 결합”하는 경우에 개인정보성을 부여하고 있는데, 이러한 결합가능성으로 그 범위가 무한정 확대될 수 있다는 문제가 있다. 사물인터넷은 모든 사물이 센서 등 기기를 통하여 인터넷에 연결되는 것을 개념으로 하므로, 사물 그 자체가 정보를 가지는 것을 전제로 한다. 그런데 그 사물은 자체적으로 개인식별성을 가지고 있지 아니하나 다른 정보와 결합함으로써만 식별성을 가지게 되는 경우가 많이 발생하게 된다. 하급심판결이긴 하지만 스마트폰의 증권관련 앱의 로그인 절차를 간편하기 위하여 이용자의 동의없이 USIM 번호, 개인 이동전화번호, 국제단말기인증번호(IMEI)를 수집한 사안에서 IMEI와 USIM 일련번호는 기계적인 정보이긴 하지만 이동통신사가 보유하고 있는 다른 인적 정보와 결합하면 특정개인이 식별된다는 이유로 개인정보로 보고 있다.⁴³⁾ 이 판결을 적용한다면 사물식별정보가 인적 정보와 결합하여 개인정보성을 떨 수 있다는 것으로서 장래 사물인터넷 발전에 장애가 될 수 있다. 다만 위치정보법에서는 결합의 정도나 방법 등을 “용이하게” 결합하는 경우로 제한하고 있는데 어느 정도를 용이한 결합으로 볼 수 있는지 명확하지 않지만 이는 일반적으로 “합리적”인 결합을 의미하는 것으로 보고 있다.⁴⁴⁾ 결국 어떤 것을 합리적인 결합이라고 할 수 있을지 문제가 되는데, 이를테면 사물인터넷 시대에 사물과 사물의 결합, 사물과 개인의 결합은 무제한하게 나타날 것으로 보는데, 이러한 경우 그 결합의 합리성을 어떻게 판단할 것인지 쉽지 않을 것이다.⁴⁵⁾ 또한 애초부터 개인정보와 결합을 목적으로

43) 서울중앙지법 2011.2.23. 선고 2010고단5343 판결. 판결의 구체적인 내용은 전응준, “위치정보법의 규제 및 개선방안에 관한 연구”, 정보법학, 제18권 제1호, 2014.4, 214215 면 참조

44) 행정안전부, 개인정보 보호법령 및 지침·고시 해설, 2011, 9쪽 ; EU의 개인정보보호지침 제26조도 어떤 사람이 식별 가능한 상태인지 여부를 판단하기 위해서는 개인정보처리자나 그 밖의 사람들이 합리적으로 사용할 것으로 보이는 모든 수단을 고려하여야 한다고 해석기준을 제시하고 있다고 규정하고 있다.

로 생성되지 않는 정보에 대한 판단도 쉽지 않다. 결국 사물인터넷에서 생성되는 정보가 개인의 프라이버시를 침해하거나 영향을 미치지 않는 경우까지 개인정보성을 적극적으로 해석할 필요를 인정하기는 곤란하므로 이와 같은 경우까지 위치정보법의 규율을 끄집어 낼 필요는 없다. 검찰은 2011년 D사의 광고플랫폼과 관련하여 스마트폰 GPS정보와 접속IP 등은 동일한 IP주소에 다수 이용자가 접속한 상태가 될 것이라는 점을 고려하여 이를 이용자를 특정할 수 있는 개인위치정보가 아니라고 판단하기도 하였다.⁴⁶⁾ 이처럼 사물인터넷에서 생성 또는 수집되는 정보가 개인정보인지 여부에 대하여는 엄격한 해석이 필요하다.

이와 같이 개념상의 혼란에서 사물인터넷을 적용할 경우의 문제점을 고찰하면 다음과 같다. 첫째 위치정보법이 2005년 제정 당시는 물론이고 현 시점에서 과연 입법목적에 부합하는 정당한 규율범위를 설정하고 있는가 하는 점에 대한 검토이다. 위치정보법은 제1조 목적에서 천명하고 있듯이 위치정보를 보호하고 이용하기 위한 목적으로 제정되었다. 그에 따라 위치정보의 개념을 정의하고, 그에 따른 정책수단을 다양하게 구성하고 있고, 위치정보를 이용한 사업에 대한 규제방식까지 다루고 있다. 그런데 이 법에서 정의하고 있는 위치정보는 모든 이동성 있는 물건 또는 개인에 대한 위치정보를 포함하므로, 그 정보가 개인을 식별할 수 있는 정보인지 여부를 불문하고, 사람과 사물도 구분하지 않는다. 다만 사물 중에서는 이동성이 있는 물건만을 대상으로 하기 때문에 이동성이 없는 물건은 대상에서 제외된다. 물건에 대한 위치정보는 그 자체로서 개인정보보호와 특별한 관련이 없고, 개인에 대한 위치정보 중에서도 식별성이 없는 개인에 대한 위치정보 또한 개인정보의 보호 필요성이 있다고 하기 어렵다. 그럼에도 불구하고 현행법은 이를 구별하지 아니하고 일체의 규제를 하고 있는바 이는 규율범위에 있어서 지나치게 광범위하게 규

45) 결합의 용이성과 관련하여 정보의 보유주체의 동일성 여부, 다른 정보를 획득할 수 있는 가능성의 정도, 결합의 용이성 판단주체 등 3가지 논점을 제시하는 견해가 있다. 영국이나 일본에서는 정보의 보유주체를 동일한 것으로 보고 있으며, 결합의 용이성은 정보처리자의 사정에서 판단하여야 한다. 전웅준, 앞의 글, 217-219쪽

46) 구태언, 개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구, 고려대 정보보호대학원 석사학위논문, 2013.12. 77-81쪽 참조

정한 것이라고 하겠다. 위치정보법은 개인정보가 아닌 위치정보에 대하여도 수집·이용·제공에 당사자의 동의를 요하는 등 일반적인 규율을 받게 됨에 따라 개인정보법보다 보호범위가 넓다는 특징이 있다.⁴⁷⁾ 둘째, 위와 같은 위치정보 개념의 불명확성과 광범위성으로 인하여 새로운 서비스의 등장에 장애 요인이 될 수 있다는 점이 문제가 된다. 사물인터넷에서 가장 첨예한 문제가 되는 점이 이 부분이다. 사물인터넷은 물건의 정보를 인터넷을 통하여 연결하여 수집하고 이용하는 것을 그 기본 구조로 하기 때문에, 대부분의 사물정보가 현행법상 위치정보에 해당됨이 분명하다. 현행 위치정보법에 의하면 이동성이 있는 물건에 대한 특정 시간과 장소에 관한 정보는 위치정보가 되어 동법의 규율대상이 되기 때문이다. 이를 테면 자동차의 이동정보, 휴대폰의 이동정보, 각종 휴대용 기기의 이동정보는 그 자체로 위치정보가 된다. 위치정보에 해당하면 수집, 이용 등에 있어서 사전에 정보주체의 동의를 받도록 되어 있는데, 동의의 대상이 되는 소유자나 주체를 파악하기도 어렵고 그 많은 사물에 대하여 사전의 동의를 획득하게 하는 것은 사실상 불가능하다. 실현불가능한 의무를 부과하는 법은 정당성을 가지기 어려우므로 현행법을 사물인터넷에 적용하는 것은 근본적인 한계가 있다고 할 것이다.

2. 수집·이용·제공에서의 정보주체의 사전동의의 문제

사물인터넷은 각종 사물에 달린 센서에 따라 부지불식간에 데이터가 수집되고, 그 데이터가 다른 정보와 결합되어 식별성이 있는 개인위치정보가 된다. 그런데 위치정보법에 의하면 위치정보 또는 개인위치정보의 수집·이용·제공 등에 있어서 정보주체의 일체의 동의를 원칙으로 하고 있다(제15조제1항, 제18조, 제19조). 만일 동의를 얻지 않고 수집하는 경우에는 개인위치정보의 경우에는 형벌(제39조, 제40조)로 처벌하고, 물건의 위치정보의 경우에는 과태료(제43조제2항)의 제재를 가하고 있다. 이러한 사전동의의 규제방식은 개인정보보호법 및 정보통신망법 등 우리나라

47) 박경신, “개인정보의 정의와 위치정보보호법의 개선방안”, 법학연구, 전북대학교, 2012. 213쪽

라 일체의 개인정보보호법제에 공통되는 방식이다. 이러한 방식이 이른바 원칙적인 것 즉 동의기반 방식인지 이론이 없는 것은 아니지만, 입법연혁상 사전동의를 위치정보법의 원칙이라고 하지 아니할 수 없다. 그리고 정보통신망법에 있어서도 동의를 원칙으로 하는 ‘동의기반’이라고 보인다. 즉 정보통신망법 제22조에 의하면 개인정보처리자가 개인정보를 이용하려고 수집하는 경우에는 정보주체의 동의를 받도록 하고, 제2항에서 동의 없이 수집할 수 있는 예외를 두고 있다. 그런데 이 조문은 1998년 정보통신망법 제정시에 최초로 도입된 개인정보보호의 규정⁴⁸⁾취지와 크게 다르지 않다. 당시의 입법취지에서 “개인정보의 오·남용을 방지하기 위하여 정보통신서비스제공자가 정보통신서비스 이용자의 개인정보를 수집하는 경우에는 그 이용자의 동의를 받도록 하고”⁴⁹⁾라고 규정하여 동의기반의 개인정보 수집원칙을 채택한 것이 인정된다.

개인정보의 수집 등에 있어서 사전동의방식을 일반적으로 부당하다거나 불합리한 것으로 보기는 어렵다. 개인정보의 수집시에 정보주체의 동의를 얻도록 하는 이유는 정보주체의 정보자기결정권에 터잡은 것이므로, 그것이 사전동의 방식이든 사후동의방식이든 정보주체가 해당 사물이 인터넷으로 연결되어 정보가 수집될 수 있음을 알 수 있게 하는 것을 전제로 하여야 한다. 이는 개인정보주체의 정보자기결정권의 기반이 되는 것 이므로 헌법적인 가치가 분명하다. 그런데, 이동성이 있는 사물의 정보가 주된 데이터로 작용하는 사물인터넷에 있어서 이와 같은 위치정보법상의 규제방식은 기존의 개인정보의 수집 등의 경우보다 훨씬 심각한 문제를 야기할 수 있다는 것이다.⁵⁰⁾ 즉 부지불식간에 일어나는 사물의 이용에 있어서 매번 이용자의 개인정보 수집에 관하여 사전동의를 받는 것이 용이

48) [구정보통신망이용촉진등에관한법률] 제6조(개인정보의 수집 및 취급) ① <생략>
②정보통신서비스제공자가 이용자의 개인정보를 수집하는 때에는 당해이용자의 동의를 받아야 한다. 다만, 다음 각호의 1에 해당하는 경우에는 그러하지 아니하다.

1. 이 법 또는 다른 법률에 특별한 규정이 있는 경우
2. 정보통신서비스 이용계약의 이행을 위하여 필요한 경우
3. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우

49) 과학기술정보통신위원회, 전산망보급확장과이용촉진에관한법률개정법률안 심사보고서, 1998.12. 2-3쪽

50) 배진석·조우제·정윤혁, 앞의 글, 765쪽

하지 않고,⁵¹⁾ 만일 사전동의를 받는 것이 사실상 불가능하다고 하다면 이 사전동의 규정은 실효성이 있다고 하기 어려우며,⁵²⁾ 사전동의방식을 관철 할 경우에는 빅데이터의 이용이 어렵게 되어 사물인터넷 등 관련 산업에 진입장벽으로 작용할 수 있게 될 것이다.⁵³⁾ 더구나, 위치정보법에 의하면 “누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이 동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니”되는 것으로 규정하여(제15조) 개인식별성이 없는 위치정보에 대하여도 사전동의를 요구하고 있는데, 이와 같이 개인정보의 성격을 가지지 아니하는 사물의 위치정보까지도 규율하게 되면 사실상 사물인터넷은 활성화가 상당히 어려워지게 된다. 이는 최초 위치정보법 제정 당시에 당사자의 동의요건을 도입한 취지는 동의가 개인정보주체의 개인정보에 대한 통제의 가장 기본의 되는 것이라는 취지⁵⁴⁾를 보더라도 분명하다. 그런 점에서 보면 현행법과 같은 사전동의방식은 사물인터넷 발전에 큰 장애가 될 수 있고, 반대로 정보주체가 사물인터넷의 정보수집 등에 대하여 아무런 관여도 하지 못하게 하는 것도 정보권의 침해라고 할 것이므로, 이를 조화시킬 수 있는 방법을 강구하여야 한다.

3. 개인정보의 제3자제공시의 즉시통보의무의 문제

위치정보법에 의하면 위치기반서비스사업자는 개인정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인정보

51) 구태언, 앞의 글, 46쪽 ; 박정훈, “우리나라 개인정보보호법제상의 추적가능 시스템에 관한 연구”, 토지공법연구, 제52집, 2011.2. 296쪽

52) 다만 교통량 측정 등을 위한 영상정보처리기기의 경우는 개인정보보호법에서 법상으로 허용하는 규정을 두고 있고(제25조제1항제5호), 위치정보법에서 다른 법률에 특별한 규정을 두고 있는 경우는 다른 법률을 적용하도록 하고 있으므로(제15조), 이 경우 개인정보법이 적용될 것이므로 별다른 문제는 없다. 그런데 개인정보보호법은 ‘교통정보의 수집·분석 및 제공을 위하여 필요한 경우’로 제한하고 있으므로 개인정보에 대한 일반적인 수집 및 이용을 허용하는 것은 아니라고 한다. 미래창조과학부, 앞의 연구보고서, 64쪽

53) 구태언, 앞의 글, 2013.12. 45쪽

54) 조용혁, “개인위치정보의 보호에 관한 법률적 고찰”, 정보화정책, 제12권 제2호, 2005년 여름, 한국전산원, 130쪽

주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하여야 한하는 것으로 규정하고 있다.(제19조제3항). 위치기반서비스사업자의 지위를 가지는 사물인터넷 사업자에게 이를 적용하게 되면, 매번 이와 같은 법적 의무를 이행하는 것은 매우 불편할 뿐만 아니라 매회 통보를 통하여 많은 비용이 발생하는 문제가 있으며, 실제로도 위치정보가 계속적으로 변하고 정보주체의 위치가 변함에 따라 이를 통보하는 것도 쉬운 일이 아니다. 이와 같은 장애를 해결하지 못하면 사물인터넷의 정착에 큰 장애가 될 것임이 충분히 예상이 된다.

4. 위치정보법과 사물인터넷 사업의 규율 문제

사물인터넷은 위치정보법상의 위치정보사업 및 위치기반서비스사업과 상당한 관련이 있다. 즉 위치정보사업이라 함은 ‘위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것’(제2조제6호)을 말하고, 위치기반서비스사업이란 ‘위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위하는 것’(제2조제7호)을 말한다. 위치정보사업자는 방송통신위원회의 허가를 받아야 하고(제5조), 위치기반서비스사업자는 방송통신위원회에 신고하여야 한다(제9조). 그런데 사물인터넷 시대는 위치정보법이 최초 제정된 2005년의 상황과 비교하여 현저한 변화가 있다.⁵⁵⁾ 당시에는 이동통신사 기지국을 기반으로 위치정보의 수집을 규율하는 것을 전제로 하였고, 실제 위치정보법에 의하여 허가 또는 신고를 받은 사업자는 이동통신사, 물류회사가 주종을 이루었으나,⁵⁶⁾ 사물인터넷 시대에는 모든 사물의 위치정보가 수집되는 상황이기 때문에 위치정보의

55) 당시 위치정보법 제정이유를 “이동통신기술의 급속한 발달로 물류, 보안, 상거래 등에 위치정보를 이용하는 다양한 서비스가 등장하면서 개인위치정보가 유출, 남용되는 등 개인의 사생활이 침해될 우려가 커지고 있는 바, 위치정보를 수집하는 사업에 대하여 허가제도, 위치정보기반서비스를 제공하는 사업에 대하여 신고제도를 도입하고, 위치정보의 수집·제공 등에 관한 절차를 정함으로써 위치정보의 유출로 인한 사생활 침해의 방지를 도모하는 한편, 위치정보와 관련된 기술개발, 표준화 등을 지원함으로써 위치정보의 이용을 활성화하고 국민생활의 향상과 공공복리의 증진에 이바지하려는 것”이라고 밝히고 있다. 2004.9. 정부 제출 법률안

56) 전응준, 앞의 글, 205쪽

양이나 질의 증대로 인하여 동법의 규율대상이 폭발적으로 확대될 것으로 예측된다. 그런 점에서 관련 사업자도 폭증하게 되어 정부의 규율 능력과 범위를 벗어날 수도 있다. 이와 같은 허가 또는 신고를 통한 위치정보 사업은 새로운 인터넷서비스의 등장에 장애가 될 가능성이 높고 일체의 사업에 대하여 진입장벽을 두는 것은 불필요한 규제라고 하겠다. 특히 개인을 식별하지 않는 위치정보에 대하여까지 영업규제를 하는 것은 지양하여야 한다. 19대 국회에서 정부는 이와 같은 내용으로 위치정보산업의 진입규제를 완화하는 내용의 위치정보법개정안을 제출하고 있다.

IV. 사물인터넷의 활성화와 개인정보 보호를 위한 조화로운 방안

1. 사물인터넷의 전제조건으로서의 보안기술의 발달

사물인터넷의 발달은 사업자·이용자·정부의 사물인터넷에 대한 신뢰를 전제로 하고, 그 신뢰는 사물인터넷의 보안기술에 대한 신뢰를 바탕으로 한다. 사물인터넷은 사물, 사람, 공간 등 모든 곳에서 용이하게 개인정보의 수집이 이루어지고 이를 빅데이터로 활용하고 있는 만큼, 다양한 활용을 위한 정보의 질적 보장 및 신뢰, IoT 디바이스와 정보이용자 사이의 정보의 안전한 교환, 취약한 디바이스에 대한 보호체계의 보장이 필수적이다.⁵⁷⁾ 여기에는 암호화기술(cryptographic techniques), 데이터 최소화, 신원 확인, 인증, 익명화기술이 중요하게 된다.⁵⁸⁾ 장래 IoT에서의 정보 보호 및 보안기술의 전망에 의하면 2015년까지는 이용자 중심의 프라이버시 기술 및 정책이, 2020년까지는 보안과 프라이버시의 자체적 필요에서 기술이 선택되고, 2020년 이후에는 자가적응(self adaptive) 보안기술로 발전할 것으로 기대되고 있다.⁵⁹⁾ 정부에서도 이러한 목표 하에 권한 없는 접근을 차단하기 위한 암호화, 인증 등 기술적 보호조치를 강구하여야 하고, 개

57) Jens-Matthias Bohli, *supra* note 19, p.225

58) Ovidiu Vermesan, *supra* note 10, p.95

59) Ovidiu Vermesan, *supra* note 10, p.129. Table2.1

인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템, 정보접근기록(로그)에 대한 안전한 관리, 바이러스 침투 방지를 위한 백신프로그램 등의 설치 등을 종합적으로 강구하고 있다.⁶⁰⁾ 이와 같은 기술적 보호조치에 대한 개발에는 많은 비용이 소요되므로 국가가 이를 적극적으로 지원해주는 방식이 필요하므로 관련법제에서 그 근거를 신설하여야 한다. 미래창조과학부는 2014년 ‘사물인터넷 기본계획’에서 사물인터넷 분야 보안기능·성능을 검증하는 보안 테스트 베드의 조성과 운영체제 등 보안기술 개발의 확대 등을 중요 시책으로 하고 있는 것도 이러한 이유 때문이다.

2. 입법모형과 입법 방향

사물인터넷과 개인정보보호 관련한 입법론은 두 가지 측면에서 검토가 필요하다. 첫째 입법목적에 따라 어떤 내용의 입법을 할 것인가의 문제이고, 둘째는 입법방식으로서 개별입법, 기존법제의 개선 및 가이드라인 등 자율규제방식 등의 선택문제가 있다.

(1) 입법모형의 선택

먼저 입법의 목적과 관련하여 어떠한 내용의 입법을 하는 것이 타당할 것인가에 대하여 보면, 미국에서 RFID와 관련한 입법에서 분류한 방식을 참고할 수 있는데, 이는 향후 사물인터넷 관련 입법에서 입법의 주된 목적이나 방향을 어떻게 설정할 것인지와 관련이 있다. 즉 1) 알권리입법(Right-to-know-legislation), 2) 금지입법(Prohibition-legislation), 3) 보안입법(IT-security-legislation), 4) 활용입법(Utilization-legislation), 5) 태스크포스입법(Task-force-legislation)으로 분류된다. 알권리입법은 소비자가 RFID의 존재 사실을 알고 제거 등을 선택할 수 있도록 하는 입법으로서 미국의 상당수의 주에서 사용되고 있으며 EU에서도 법률안(The European Article 29 Data Protection Working Party)으로 상정된 사실이 있다. 금지입법은 RFID의 사용을 금지하거나 제한하는 것으로서 전통적인 입법방식이며, 보안

60) 정보통신부, RFID 프라이버시 보호 가이드라인 해설서, 2007.9

입법은 RFID의 보안 표준을 설정하는 것을 내용으로 하고, 활용입법은 금지 입법의 대응방식으로서 RFID의 활용을 지원하는 입법이며, 마지막으로 태스크포스입법은 RFID의 관련 연구를 하는 기술단체 지원 등을 내용으로 한다.⁶¹⁾ 위의 입법모형은 일반적으로 규제와 진흥의 양 측면과 개인정보보호의 목적까지 고려된다면 어느 하나만이 아니라 여러 목적이 종합적으로 반영되는 것이 바람직하다고 하겠다.

(2) 입법 및 규제방식의 선택

다음으로, 입법방식에 대한 논의이다. 위와 같이 사물인터넷에서의 개인정보 보호를 위한 구체적인 개선방안이 있지만, 현재의 법령 즉 개인정보보호법 또는 위치정보법, 정보통신망법을 개정하여 문제를 해결할 수 있다면 가장 바람직하다. 또한 ICT 특별법에 따라 새로운 규제들이 생기기전에 신규 기술 및 서비스로 사업화의 정책적 도움(신속처리 내지 임시허가제도)을 받을 수도 있다. 이와 관련하여 사물인터넷에 특화한 개별법을 제정할 것인가 하는 문제가 있는데, 이전에 사물정보통신과 관련하여 개별법의 입법 움직임이 그와 같은 사례이다. 사물인터넷 활성화를 위하여 단일법 형태의 입법이 필요하다는 방식은, 기존의 법률의 개정만으로는 이와 같은 효과를 달성하기 어렵다는 것을 전제로 한다. 그 내용으로는 사물인터넷 진흥 기본계획의 수립과 시행, 전파사용료 감면을 내용으로 하는 국가적 지원체계, 정부의 기술개발 지원의무 규정 도입과 사물인터넷 환경의 조성, 전문인력 양성 등 기반조성, 시범사업의 실시, 국제 협력 등을 내용으로 한다.⁶²⁾ 그러나 사물인터넷을 아직 독자적인 서비스 영역으로 확정하기 곤란하고, 사물인터넷은 국제간에 발생되는 거래라는 관점에서 국제적인 적용이 불리한 개별법의 제정은 바람직하지 않으며,⁶³⁾

61) 이상 입법모형에 대한 설명은 Viola Schmid, cylaw - Report x x iv- cnference Speechers to the “internet of Thimgs” in 2008.
(http://tuprints.ulb.tu-darmstadt.de/1296/1/CylawReportXXIV_RFID_090106MB.pdf.
2014.5.29.검색); Rolf H. Weber, supra note 3, p.29

62) 미래창조과학부, 전계 연구보고서, 152-153쪽 ; 한국정보화진흥원의 가칭 ‘사물통신기 반구축 및 사물정보 이용활성화에 관한 법률(안)’도 같은 취지이다. 한국정보화진흥원, 사물지능통신에 관한 법제도적 고찰, 연구보고서, 2010.12, 44쪽 이하

다른 인터넷서비스와의 뚜렷한 차별성을 가진 것도 아니고, 특히 단지 특정기술을 위한 개별법을 제정하는 것도 바람직한 것이 아니라는 점⁶⁴⁾에서 개별법의 제정은 바람직하지만 한 것은 아니다. 따라서, 사물인터넷의 발전 속도에 따라 시장에 적용할 수 있는 가이드라인을 제정하여 시행하는 방식이 바람직하다. 사물인터넷은 아직 기술적으로 완전히 정착된 것이 아니며 그 서비스의 양과 질도 예측하기 곤란하고, 섣부른 규제가 가지고 오는 서비스에 대한 예측의 잘못은 실효성이 없을 뿐만 아니라, 해당 서비스 발전의 발목을 잡는 상황으로 변질될 가능성도 없지 않다. 우리나라가 ICT 분야의 선진적인 도래에 맞추어 그동안 많은 규제대책을 세웠지만 상당수가 초기에 실패로 돌아간 것에서 교훈을 얻어야 한다.⁶⁵⁾ 사물인터넷의 경우에도 현행 법제에서 적용가능한 방향으로 개선을 하는 정도로 속도를 조절할 필요가 있다.⁶⁶⁾ 사물인터넷 시대에 있어서 개인정보 보호를 위한 각국의 입법정책동향에 대하여는 앞서 본바와 같지만, 대체로 유럽에서는 적어도 개인정보보호만을 위한 입법은 불필요하다고 보는 입장이 있는데 그 이유는 현재의 다양한 개인정보보호법제의 수준이 충분히 만족스럽다는 것을 전제로 하고 있으며, 이와 달리 미국에서는 캘리포니아, 위스콘신 등 몇 개주에서 RFID 관련 입법을 시도하고 있는 다른 사례가 있다.⁶⁷⁾ EU는 사물인터넷의 정책방향에 대하여 경성, 연성 등의 여러 방법 중에서 연성법(Soft Law)⁶⁸⁾적인 접근방식을 택하고 있고,⁶⁹⁾

63) Rolf H. Weber, *supra note 3*, p.27

64) Viola Schmid, “radio frequency identification law beyond 2007”(http://tuprints.ulb.tu-darmstadt.de/1296/1/CylawReportXXIV_RFID_090106MB.pdf. 2014.5.29. 검색)

65) 게시판 본인확인제에 대한 위헌결정이 대표적인 사례이다. 건전한 인터넷환경 조성이라는 입법목적에도 불구하고 결과적으로 예정하였던 기대효과를 달성하지 못하는 등 섣부른 규제로 판명되었다. 황창근, “제한적 본인확인제 위헌 결정과 인터넷윤리 법제에서의 시사점”, 정보처리학회지 제20권 제2호, 2013.3, 1-7쪽

66) 스마트 사회에서 획일적 규제를 피하고 이용자 선택권이 가능한 유연한 규제를 강구하여야 한다는 취지도 같은 의견이다. 이기주, “스마트 사회의 보안위협과 정보보호 추진정책에 관한 제언”, 2013년 정보통신 기술과 정책, 31쪽

67) Viola Schmid, “radio frequency identification law beyond 2007”(http://tuprints.ulb.tu-darmstadt.de/1296/1/CylawReportXXIV_RFID_090106MB.pdf. 2014.5.29. 검색)

68) 여기서 ‘soft law’라는 개념은 사업자의 자율규제(self-regulation)와 정부의 가이드라인의 제정 등을 통한 사업자 감독 등의 협력규제(co-regulation)를 의미하고, 협력규제 내지 자율규제방식은 온라인상 프라이버시 내지 개인정보보호의 가장 효과적인 시

과거 정보통신부도 RFID와 관련하여 프라이버시 보호 가이드라인을 제정하여 업계의 기준으로 삼은 사실이 있다.⁷⁰⁾

<표 2> EU의 사물인터넷 정책 방향과 기대 효과

| 정책옵션 | 특징 | 기대 효과 |
|--------------------|---|--|
| 무조치 (No Action) | · 현재의 정책을 유지 | <ul style="list-style-type: none"> 관련 사업자들은 완전히 자유로운 경쟁환경에서 활동 EU의 정책 목표와 부합하는 방향으로 사물인터넷 발전을 유도하는 것은 불가 |
| 연성법 (Soft Law) | · 커뮤니케이션의 형성, 개인정보의 제정 등 사물인터넷의 발전을 간접적으로 자극할 수 있는 준(準) 법적 제도(quasi legal institution) 활용 | <ul style="list-style-type: none"> 사업자들이 스스로 가장 효율적인 시장규제 방법을 결정함으로써 자유로운 사업 활동 영위가 가능 인센티브가 확인될 경우 EU의 정책 목표에 부합하는 사물인터넷 산업 발전 유도가 가능 |
| 경성법 (Hard Law) | · 기존 법과 규제를 사물인터넷에 적합하도록 완전히 수정하고 이를 기반으로 실제 정책을 집행 | <ul style="list-style-type: none"> 정책 집행 기관 및 집행 방식에 따라 발전 효율성을 극대화 하는 것이 가능 사물인터넷이 발전 초기 단계에 있는 만큼 정책 집행에 따른 부정적 외부 효과의 예측이 불가 |

출처 : 정보통신산업진흥원

3. 구체적인 개선 내용

장래의 사물인터넷의 도래에 맞추어 보면 그 법적인 장애로 작용할 위치정보법을 그대로 존속시킬 것인지에 대하여는 근본적인 의문이 없지 않지만,⁷¹⁾ 폐지 여부는 별론으로 하고 사물인터넷 시대에 위치정보법을

행방법으로 인정되고 있다. Rolf H. Weber, *supra* note 3, p.27-28

69) 정보통신산업진흥원, 앞의 글, 52쪽

70) 정보통신부, 앞의 책, 2007.9

71) 사물인터넷을 활성화하기 위하여 또는 정착시키기 위하여 현행 위치정보법에 대한 손질이 필요하다는 논의는 가능하지만, 그에 더 나아가 위치정보법을 폐지할 것인지에 대하여는 신중한 검토를 요한다. 원래 위치정보법이 입법하게 된 배경이 2005년 경 위치정보를 이용한 물류산업 등의 진흥에도 그 목적이 있다고 할 것이므로, 진흥

어떻게 개선할 것인가 하는 점으로 초점을 맞추어 개선 내용을 제시하고자 한다. 이하 정부가 2013. 12. 27. 국회에 제출한 위치정보의 보호 및 이용 등에 관한 법률일부개정안을 함께 검토하기로 한다.⁷²⁾

(1) 첫째, 위치정보법의 규율대상이 되는 위치정보의 개념정의를 다시 할 필요가 있다. 사물의 단순 위치정보는 개인을 식별할 수 있는 정보가 아니므로 개인정보보호의 취지상 보호의 가치가 없다고 할 것이다.

(2) 둘째, 위치정보에 대한 사전동의방식을 개선하여야 한다. 이동성이 있는 사물인터넷의 경우에는 매번 사물의 소유자 또는 관리자로부터 동의를 받는 것이 불가능하므로 동의를 전제로 한 수집, 이용 등의 개인정보보호체계에 대한 근본적인 재고가 필요하다.⁷³⁾ 그 개선방안으로는, 인터넷에 연결된 모든 사물에 해당 사물이 개인정보를 수집할 수 있음을 쉽게 알아볼 수 있도록 표시하거나 센서가 작동함을 알려주는 사실의 통지로 대체하는 방안,⁷⁴⁾ 단순위치정보 즉 개인식별성이 없는 사물에 대한 위치정보에 대한 사전동의제도를 삭제하는 방안,⁷⁵⁾ 사전동의방식을 opt-out 방식으로 변경하는 방안 등이 가능하다. 이는 IoT를 통하여 수집되는 정보에 대하여 사물의 이용자 또는 소유자가 개인정보자기결정권을 실질적으로 행사할 수 있도록 RFID 또는 센서의 유무를 알 수 있도록 하는 것이다. 이는 사물 또는 개인에 대한 추적시스템은 쉽게 사물에 장착되는 반면, 프라이버시 및 보안솔루션은 장치되지 못함으로 빚어지는 불균형을 해소하는 것이기도 하다.⁷⁶⁾ 이에 따라 해당 사물을 이용하는 정보주체가 이용 여부를 선택하게 하여 궁극적으로 정보권행사를 할 수 있게

의 측면을 완전히 도외시하고 폐지로 가는 것은 성급한 결론이다.

72) 정부의 2013.12.27.자 위치정보의 보호 및 이용에 관한 일부개정법률안 참조

73) 미래창조과학부, 앞의 보고서, 130쪽 ; 박경신, 앞의 글, 216-217쪽 ; 전용준, 앞의 글, 227쪽

74) 구정보통신부의 'RFID 프라이버시 보호 가이드라인'에서는 RFID 태그를 통한 개인정보의 수집사실을 이용자에게 통지하거나 쉽게 알아볼 수 있는 방법으로 표시하도록 하고 있다(제5조). 정보통신부, 앞의 책, 2007.9 ; Viola Schmid, cylaw - Report x x iv - cnference Speechers to the "internet of Thimbs" in 2008.(http://tuprints.ulb.tu-darmstadt.de/1296/1/CylawReportXXIV_RFID_090106MB.pdf. 2014.5.29.검색) ; 박정훈, 앞의 글, 296쪽

75) 전용준, 앞의 글, 219쪽

76) Gianmarco Balini, supra note 18, p.210

하면 될 것이다.

(3) 셋째, 개인위치정보의 제3자제공시의 즉시통보의무를 개선하여야 한다. 개정안에 의하면 위치기반서비스사업자가 개인위치정보를 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 통보하도록 되어 있으나 위치기반서비스사업자는 물론 개인위치정보주체에게도 불필요한 통보가 많아, 정보주체가 자신의 개인위치정보를 제공하는 경우에는 통보를 하지 않아도 되고 개인위치정보주체의 동의를 받은 경우에는 대통령령으로 정하는 바에 따라 모아서 통보할 수 있도록 개선을 하였다(동제19조). 즉시통보 규정은 그동안 사업자에게 많은 부담과 비용을 발생케 하고 정보주체에게도 매번 통보를 받느라 불편을 초래한 것인만큼 이를 개선하여 상당한 기간을 통하여 한 번 통보토록 하는 것은 바람직하다고 할 것이다. 이에 반하여 개인정보에 대한 사전동의가 형식적으로 이루어지고 있는 사정에서 불편해소를 위하여 통보제도를 약화시키는 것은 바람직하지 않다는 반론도 제기되고 있다.⁷⁷⁾

(4) 넷째, 위치정보 관련 사업자 규제방식의 변화가 필요하다. 정부의 개정안에 의하면 위치정보산업의 진입규제를 완화하는 내용으로서 개인 위치정보를 대상으로 하지 아니하는 위치정보사업 또는 위치기반서비스 사업에 대하여 허가 또는 신고대상에서 제외하고 있으며, 위치정보사업에 대하여 허가, 양수 등에 대한 인가 및 휴지·폐지 승인에 대하여 원칙적 허용의 네거티브 규제방식을 채택하고 있다. 이는 개인위치정보를 대상으로 하지 않은 위치정보 내지 기반사업은 개인정보 침해 위협이 없기 때문에 이를 인정한 것이므로, 위치정보법이 단순위치정보에까지 규율범위가 지나치게 확장되어 있다는 점을 반영한 것이고, 이는 궁극적으로 위치정보 산업의 활성화에 기여할 것으로 기대되고 있다.⁷⁸⁾ 다만 단순위치정보에 대한 사업에 대한 진입규제를 완화한 이외에 나머지 위치정보에 대한 각종 규제의 대상에서는 제외하고 있지 아니하여(개정안 제38조의3), 단순위치정보를 위치정보법의 주된 규율대상으로 보고 있는 근본적인 한

77) 미래창조과학방송통신위원회, 위치정보의 보호 및 이용 등에 관한 법률 일부개정법률안 검토보고서, 2014.2, 15쪽

78) 미래창조과학방송통신위원회, 앞의 검토보고서, 8쪽

계를 벗어난 것은 아니라고 하겠다.

(5) 마지막으로 그동안의 개인정보보호의 쟁점은 수집, 관리, 폐기 등 다양한 측면에서 전개되었고, 특히 최소수집의 원칙으로 대변되는 수집상의 사전동의 등 규제가 집중된 측면이 있었다. 그런데 사물인터넷에서는 정보는 시간, 공간, 사물의 제한 없이 수집되고 활용되는 것을 그 핵심구조로 하는 것이므로 기존의 최소수집의 원칙 등 수집기반의 규제체계와는 부합되기 어렵다. 따라서 사물인터넷에서는 수집 보다는 이용 단계에서 개인정보보호의 규제체계를 집중하는 발상의 전환이 요청된다. 이를테면 불법적인 유출이나 제공 등이 발생할 경우에는 집단소송제도, 징벌적 손해배상, 법정손해금, 과징금, 영업취소 등 강력한 규제체계를 집중하여 이용단계를 강화하는 것이 필요하다.

V. 결 론

사물인터넷은 새로운 산업혁명에 비견될 정도로 우리의 생활방식의 변화를 예고하고 있다. 이는 생활의 편의를 증대시킬 뿐만 아니라, 산업구조의 변화를 가져와 생산성의 획기적 증대도 예상된다. 사물인터넷 시대에는 개인의 모든 행동, 정보가 사물을 통하여 부지불식간 수집되고, 빅데이터를 통하여 활용되게 되는 것이므로 개인정보의 침해위험성이 보다 높아진다. 수집과 이용, 파기에 이르는 일련의 과정에서 개인정보를 어떻게 보호할 것인가는 매우 중요하다.

이 글은 사물인터넷에서 개인정보보호의 쟁점이 어떻게 전개되는지 관련하여, 국내외 정책 방향을 살펴보고, 그 문제점은 무엇이고 이를 어떻게 해결할 것인지 등에 대하여 살펴보았다.

아직 국내외 정책동향을 보더라도 사물인터넷에서의 개인정보보호의 특유한 점을 발견하기 어렵다. 국내의 개인정보보호법제 중 사물인터넷과 가장 관련이 많은 법제는 위치정보법이다. 기존의 개인정보보호법제에 있어서는 개인정보의 수집, 이용 등의 경우에는 정보주체의 사전동의를 원칙으로 하고 있다. 그러나 부지불식간에 일어나는 사물정보 및 개인정보

의 수집이 이루어지고 활용되는 사물인터넷시대에 이와 같은 원칙을 고수하는 것이 어렵게 되었다. 또한 기존의 개인정보 내지 위치정보의 개념은 사물정보와 결합가능성을 매개로 상당 부분 개념정의 및 보호범위를 달리하여야 하는 문제가 발생되었다. 그 외에도 사물인터넷 사업을 위하여 위치정보법상 사업자규제 방식의 변화가 필요하다.

사물인터넷은 장래형이 아니라 현재진행형이고, 그로부터 발생되는 개인정보 침해에 대한 위협이나 보안 문제 또한 충분히 예상이 되는 부분이다. 개인정보 보호를 위하여 사물인터넷의 활성화를 규제하는 것은 바람직하지 않고, 반대로 사물인터넷의 활성화를 목적으로 개인정보 보호를 방기하는 것도 바람직하지 않다. 그렇다면 어떻게 하면 개인정보 침해 가능성을 줄이면서 사물인터넷의 활성화를 도모할 것인가의 균형 잡힌 시각이 필요하다. 인터넷으로 연결된 사물이 가지고 있는 정보의 수집과 이용을 피할 수 없는 현실에서는 수집은 용이하게, 이용은 엄격하게 통제하는 수집에서 이용으로의 발상의 전환이 무엇보다도 필요하다.

사물인터넷과 개인정보의 보호문제는 균형을 가지고 조화롭게 풀어야 하고, 사물인터넷은 국제적으로 표준이 설정되고 거래가 이루어지는 것을 감안하여 국제적인 규범의 형성을 따라가는 것이 필요하다고 하겠다.

참 고 문 헌

- 강달천, “ICT산업의 발전과 개인정보 법제의 문제”, 인터넷법제도포럼 발표자료, 2014. 4. 30
- 구태언, 개인정보 정의조항, 동의제도 및 형사처벌의 합리화에 관한 연구, 고려대 정보보호대학원 석사학위논문, 2013.12.
- 매일경제 IoT 혁명 프로젝트팀, 「모든 것이 연결되는 세상 사물인터넷」, 매일경제신문사, 2014
- 민경식, 주요국의 사물인터넷 정책동향. IT R&D 정책동향, 정보통신산업 진흥원, 2012.9.
- 박경신, “개인정보의 정의와 위치정보보호법의 개선방안”, 법학연구, 전북대학교, 2012
- 박정훈, “우리나라 개인정보보호법제상의 추적가능 시스템에 관한 연구”, 토지공법연구, 제52집, 2011.2
- 배대현, 유비쿼터스 사회로의 발전추세에 따른 RFID 관련 법률문제 검토, 법조, 제40호, 법무부, 2007.10
- 배진석·조우제·정윤혁, “Privacy Issues in IoT Communication”, 2013년 한국경영정보학회 추계학술대회
- 이기주, “스마트 사회의 보안위협과 정보보호 추진정책에 관한 제언”, 2013년 정보통신 기술과 정책
- 이코노미스트, 막 오른 사물인터넷 시대, 2014. 5. 5. 1235호
- 전웅준, “위치정보법의 규제 및 개선방안에 관한 연구”, 정보법학, 제18권 제1호, 2014.4.
- 정 혁·이대호, “사물인터넷의 진화와 정책적 대안”, KISDI Premium Report, 14-3, 2014.4.23.
- 조용혁, “개인위치정보의 보호에 관한 법률적 고찰”, 정보화정책, 제12권 제2호, 2005년 여름, 한국전산원
- 주대영·김종기, 초연결시대 사물인터넷(IoT)의 창조적 융합 활성화 방안, 산업연구원, 2014
- 황창근, “제한적 본인확인제 위헌 결정과 인터넷윤리법제에서의 시사점”, 정보처리학회지 제20권 제2호, 2013.3
- 국가과학기술정보통신위원회, 위치정보의 보호 및 이용 등에 관한 법률안 검토

- 보고서, 2004.12,
과학기술정보통신위원회, 전산망보급확장과이용촉진에관한법률개정법률안
심사보고서, 1998.12.
- 미래창조과학방송통신위원회, 위치정보의 보호 및 이용 등에 관한 법률
일부개정법률안 검토보고서, 2014.2
- 미래창조과학부, 사물인터넷 활성화를 위한 제도개선 및 정책협력 방안
연구, 연구보고서, 2013.11.
- 방송통신위원회, 사물통신(Machine-to-Machine)에서의 정보보호를 위한 효
율적 인증시스템 연구, 연구보고서, 2010. 9. 30.
- 정보통신부, RFID 프라이버시 보호 가이드라인 해설서, 2007.9
- 정보통신산업흥원, “사물인터넷 발전을 위한 EU의 정책 제안”, 해외 ICT
R&D 정책동향, 2013.6월
- 한국인터넷진흥원, “미국 연방거래위원회, 연방정부 차원의 사물인터넷
균형 발전 모색”, 「Internet & Security Bimonthly」, 2014년 1호
_____, “공공 부문 사물인터넷 도입 효과, 향후 10년간 4조
6,000억 달러 전망”, 「Internet & Security Bimonthly」, 2014년 1호
- 한국정보화진흥원, 사물지능통신에 관한 법제도적 고찰, 연구보고서,
2010.12
- 행정안전부, 개인정보 보호법령 및 지침·고시 해설, 2011.

A Juels, “RFID Security and Privacy: A Research Survey”, IEEE journal om
Selected Areas in Communications, Vol.24, 2006

Bilel Jamoussi, “IoT Prospects of Worldwide Development and Current Global
Circumstances”

Commision of the European Communities, Internet of Things – An action plan
for Europe, 2009.6.18

Gianmarco Balini, Trevor Pierce, Marcus Handte, Domenico Rotondi, Sergio
Gusmeroli, Salvatore Piccione, Bertrand Copigneaux, Frank Le Gall,
Foued Melakessou, Philippe Smadja, Alexanandru Serbanati and Julinda
Stefa, “Internet of Things Privacy, Security and Governance”, Ovidiu
Vermesan and Peter Friess(ed.) Internet of things: Converging
Technologies for Smart Environments and Integrated Ecosystems, River

Publisher, 2013

ITU, ITU Internet Reports 2005 ; The Internet of Things, November 2005.

Jens-Matthias Bohli, Peter Langendorfer and Antonio F.Skarmeta, “Security and Privacy Challenge in Data Aggregation for the IoT in Smart Cities”, Ovidiu Vermesan and Peter Friess(ed.) Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publisher, 2013

Mariko Yoshihara, RFID and Privacy, Public law Research Institute UC Hastings College of Law, 2008

Ovidio Vermesan, “Europe’s IoT strategic research agenda 2012”, Ian G Smith(ed.) The Internet of Things 2012 New Horizons, 2012, Halifax

Ovidiu Vermesan, Peter Friess, Patrik Guillemin, Harald Sundmaeker, Marcus Eisenhauer, Klaus Moessner, Frank Le Gall and Philippe Cousin, “Internet of Things Strategic Research and Innovation Agenda”, Ovidiu Vermesan and Peter Friess(ed.) Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publisher, 2013

Peter Friess, “Driving European Internet of Things Research”, Ovidiu Vermesan and Peter Friess(ed.) Internet of things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publisher, 2013

Rolf H. Weber, “Internet of Things - New security and privacy challenges”, computer law and security review, 26, 2010

Viola Schmid, “radio frequency identification law beyond 2007”

⟨web-page⟩

<http://www.internet-of-things-research.eu>

<http://www.itu.int/en/publications/Pages/default.aspx>

<국문초록>

사물인터넷 시대에는 개인의 모든 행동, 정보가 사물을 통하여 부지불
식간 수집되고, 빅데이터를 통하여 활용되게 되는 것이므로 개인정보의
침해위험성이 보다 높아진다.

아직 국내외 정책동향을 보더라도 사물인터넷에서의 개인정보보호의
문제를 직접적으로 다룬 것은 발견하기 어렵다. 국내의 개인정보보호법제
중 사물인터넷과 가장 관련이 많은 법제는 위치정보법이다. 기존의 개인
정보보호법제에 있어서는 개인정보의 수집, 이용 등의 경우에는 정보주체
의 사전동의원칙, 개인정보 내지 위치정보의 개념 및 보호범위, 위치정보
법상 사업자 등에 대한 재검토가 필요하다.

개인정보 보호를 위하여 사물인터넷의 활성화를 규제하는 것은 바람직
하지 않고, 반대로 사물인터넷의 활성화를 목적으로 개인정보 보호를 포
기하는 것도 바람직하지 않다. 어떻게 하면 개인정보 침해 가능성을 줄이
면서 사물인터넷의 활성화를 도모할 것인가의 균형 잡힌 대책이 필요하
다. 인터넷으로 연결된 사물이 가지고 있는 정보의 수집과 이용을 피할
수 없는 현실에서는 수집은 용이하게, 이용은 엄격하게 통제하는 수집에
서 이용으로의 발상의 전환이 무엇보다도 필요하다. 또한 사물인터넷은
국제적으로 표준이 설정되고 거래가 이루어지는 것을 감안하여 성급한
입법 보다는 국제적인 규범의 형성을 따라가는 것이 필요하다.

주제어 : 사물인터넷, 위치정보, 개인정보보호, 개인정보, 사전동의

The Internet of Things and Protection of Personal Data

Hwang, Chang-Geun*

In the age of Internet of Things(IoT), every behaviors and data of individuals is unnoticeably collected by things and exploited by big data. Consequently, a risk of infringement on personal data increases.

There are hardly any policies at home and abroad which directly dealing with personal data protection issues related to Internet of Things. Amongst domestic personal data protection laws, Location data law is the most closely related law to Internet of Things. About existing personal data protection law, it is necessary to reconsider the opt-in rule, a notion and protection extent of personal data and location data and the business regulation regarding personal data collecting and exploiting.

It is neither desirable regulating Internet of Things in order to protect personal data nor giving up personal data protection for the purpose of revitalizing Internet of Things. What is required is a balanced measure to reduce riskiness of invasion of personal data and also to revitalize Internet of Things. It is inevitable consequence that data within things connected by internet are collected and utilized. Thus, the highest importance lies in a switchover to that data are easily collected but not exploited with strict control. Moreover, taking into account establishment of international norms and transactions, Internet of Things needs to follow a formation of international standards rather than to be legislated hastily.

Key Words : Internet of Things(IoT), Location Data, Personal Data Protection, Personal Data, Opt-In

* Professor of Hongik University college of law

