일감법학 | 제42호
2019년 2월 255-286쪽
건국대학교 법학연구소

Ilkam Law Review
Vol.42, Feb., 2019. pp.255-286
The Institute of Legal Studies, Konkuk Univ.

사물인터넷 환경과 개인정보보호의 법적 문제*

Legal Issues of the Personal Data Protection against Internet of Things

정 준 현**
Jeong, Jun-Hyeon

목 차

종래의 입법은 물리력을 전제로 어느 정도 정형화된 위험을 대상으로 하는 규제법이었다. 이러한 관계로 현재 진행되고 있는 사물통신시대에 내재된 비물리적이고 정형하기 어려운 고도화된 사이버위협으로부터 개인정보의 보호와 개인정보의 활용간에 'Positive-sum'의 결과를 유지할 수 있는 법제의 정비가 시급하다. 특히, 현행법제상 개인정보 유출사건이 발생하더라도, 정보주체인 개인이 정보처리자와 대등한 관계에서 배상책임을 받을 수 있을 것으로 기대하기 어렵다. 즉, 과실에 대한 입증책임이 전환되는 경우라 하더라도 개인의 입장에서는 정보처리자의 불법행위와 자신이 입은 피해간의 상당인과관계의 입증이나 피해액의 입증을 기대할 수 없고, 법정배상의 경우에는 정보처리자의 고의·과실 및 해당 불법행위와 자신이 입은 피해간의 상당인과관계 등을 입증할 것으로 기대하기 어려운 것이다.

이와 같이 개인과 개인정보처리자 사이에 존재하는 정보격차(Digital Divide)를 해소하기 위해서는 정보처리자에 대해 "설계에 의한 사생활보호"(Privacy by Design) 책임을 부여

투고일 : 2018. 12. 26. / 심사의뢰일 : 2019. 1. 16. / 게재확정일 : 2019. 2. 7.
* 이 연구는 2018학년도 단국대학교 대학연구비 지원으로 연구되었음
** 단국대학교 법과대학 법학과 교수
Professor, Law College of DanKook University

하는 한편, '구조화된 사이버 위협정보'를 표현하는 'STIX' 제도를 개인정보 보호분야에서도 적극 도입할 필요가 있다.

[주제어] 사물통신시대, 정보격차, 개인정보, 설계에 의한 프라이버시 보호, 구조화된 사이버위협 정보

Ⅰ. 처음에

오늘날의 정보화기술의 급속한 변화・발전은 입법의 능력한계를 초과한다고 평가할 수 있다. 즉, 전통적인 법제는 "$E=mc^2$"(즉, 유형물과 관리가능한 자연력으로서 무형물)에 기반을 두고 예측 가능한 정형화된 위험의 예방을 위한 규제와 발생된 위험상태나 장해에 대한 제재규정으로 만족할 수 있었다. 그러나, 관리가 가능하나 자연력이 없어 현행법상의 물건에 속하지 아니하는 무형의 '사이버'를 둘러싼 위험은 사전 예측・대응이 어려운 비정형성・첨단성을 갖는 점에서 뚜렷한 입법적 대응을 하지 못하고 있다. 그럼에도 소극적인 방어권으로서 프라이버시권(right to be alone)을 거쳐 '정보자기결정권'[1] 내지 정보프라이버시권(e-privacy)[2]'을 법적으로 도출하여 사물인터넷 사회를 맞이하게 된 것은 불행 중의 다행으로 보인다.

최근에는 이에 더 나아가 '잊힐 권리'가 판례[3]상 수용되고 2018년 5월부터 시행되는 유럽연합의 「개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 유럽의회와 유럽이사회 규칙」(이하 "GDPR"이라 한다)[4]에 의해 앞의 '잊힐 권리' 외에 '설계에 의한 프라이버시'(Privacy by Design) 내지 '기본사양으로서 프라이버시'(Privacy by Default) 등이 규정(제25조)되기에 이르렀다.

---

1) 김현철, "자기결정권에 대한 법철학적 고찰", 법학논집 제19권 제4호, 이화여자대학교 법학연구소, 2015, 365쪽; 자기결정권은 인간의 고유권으로서 시대에 따라 공동체가 승인한 규범에 합치하는 범위에서 자신에 관한 사항을 어느 누구의 간섭 없이 스스로 결정할 수 있는 권리로서 칸트의 "성년(Mündigkeit)" 개념에 상응한다(<https://de.wikipedia.org/wiki/Selbstbestimmungsrecht_der_V%C3%B6lker>).

2) Alan F. Westin. *Privacy and Freedom*, Atheneum, New York, 1967, p.7.

3) Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014. 5. 13.

4) 이 규칙은 별도의 전환입법을 기다리지 않고 유럽연합 내에 소재한 조직뿐만 아니라 상품・서비스를 제공하고자 하는 또는 유럽시민의 활동을 모니터링하고자 하는 유럽연합 밖에 소재한 조직에 대하여 적용된다는 점에서 그 파급효과는 매우 크다. <https://www.eugdpr.org/gdpr-faqs.html>, 검색일: 2018.5.17.

그렇다고 하더라도, 개인과 사회에 대해 가상이 아닌 실질적인 영향을 발하게 되는 사물인터넷사회 내지 '사이버기반의 물리적 사회'(Cyber-Physical System)에 접어든 이때, 개인 데이터(빅데이터)가 갖는 가치의 창출·활용과 이에 대립하는 개인정보에 대한 자기결정권 및 프라이버시의 보호문제 등의 갈등은 'Zero-Sum'의 관점이 아닌 'Positive-Sum'의 관점에서 법적으로 해소되어야 할 숙제임은 변명할 수 없다.[5]

Ⅱ. 사물인터넷 환경에서 수집·처리되는 정보와 위협

1. 사물인터넷 환경

사물인터넷[6]은 다양한 기능을 갖고 다양한 소프트웨어 플랫폼에 기반을 두고 있는 이종적인 웨어러블이나 센서 등 기기[7] 등이 인터넷을 매개로 통합적으로 정보를 소통할 수 있는 환경으로 일단 이해할 수 있으나[8], 이에 대한 기술적 내지 법적 정의[9]는 여전히 숙제로 남아 있다. 이와 관련하여, 사물통신의 개념을 정의함에 있어 장소적인 작은

5) 'Zero- Sum', 'Positive-Sum' 및 'Negative-Sum'은 논쟁이나 협상의 결과를 나타내는 게임이론으로, 이들은 각 당사자가 받는 富의 실질적인 크기(금전, 토지, 여가시간) 내지 측정이 가능한 보상을 의미한다. <http://www.amazon.com/Encyclopedia-Conflict-Resolution-Heidi-Burgess/dp/0874368391>, 검색일: 2018.5.15.

6) 1999년 "Internet of Things"를 처음으로 사용한 Kevin Ashton은 "우리가 모든 것을 알고 있는 컴퓨터를 갖게 되면 모든 것을 추적하고 계산할 수 있게 되어 낭비, 손실과 비용을 획기적으로 줄일 수 있게 된다. 즉, 사물인터넷은 인터넷이 그랬던 것처럼 세상을 변혁시킬 잠재력을 갖고 있다"고 한다. EY, "Cybersecurity and the Internet of Things" <http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of- things.pdf>, 검색일: 2018.6.21.

7) 미래창조과학부, "사물인터넷(Iot) 정보보호 로그맵", 2014.10.31, 2쪽.

8) 미국 상원이 2017년에 제출한 "Internet of Things Cybersecurity Improvement Act"에서는 사물인터넷의 개념을 '物을'을 중심으로 '① 인터넷과 연결이 가능하고 보통 인터넷과 연결되는 유체물과 ② 데이터를 수집, 전송, 수신할 수 있는 컴퓨터 프로세싱 유체물'로 확장하고 있다. 박성진, "[미국] 2017년 사물인터넷 사이버보안 개선 법안이 제출되다", <https://www.copyright.or.kr/mobile/gov/nuri/download.do?brdctsno=41501&brdctsfileno=12728>, 검색일: 2018.7.12.

9) 2014년 9월 유럽연합의 '데이터 보호지침(95/46) 제29조 실무연구반은' GDPR의 시행을 앞두고 기존법의 적용성이라는 관점에서 작성된 '사물 인터넷에 대한 의견서'를 통해 사물 인터넷 기기를 "사물인터넷 서비스의 제공이라는 맥락에서 개인의 데이터를 수집·추가·처리하는데 사용되는 모든 물체"로 정의하고 있다. Article 29 Data Protection Working Party, Opinion 8/2014 on 'Recent Developments on the Internet of Things'(14/EN WP 223) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>, 검색일: 2018.7.12.

것에서부터 분산되고 복합적인 거대한 시스템을 포함시키려고 하는 국제전기전자기술연구소(IEEE)가 '사물인터넷의 제안'(Internet of Things Initiative)을 통해 '사물인터넷을 구성하는 기기는 그것이 소형장치일지라도 적어도 하나의 시스템에 내장되어 있으면서 환경 속의 개인을 비롯하여 그 무엇인가를 끊임없이 감시・통제한다'고 지적[10]한다.

이러한 지적으로부터, 사물인터넷기기의 제작자나 사물인터넷서비스제공자 및 사물인터넷기기의 사용자 사이에 상존하는 '정보격차'(Digital Divide) 내지 '통제의 불평등성'과 이로 인하여 발생하는 프라이버시의 법적 문제를 도출할 수 있다.

2. 사물인터넷 환경과 수집・처리되는 정보

사물인터넷의 대상이 되는 사물은 개인 수요를 충족하기 위한 다양한 기능의 웨어러블에서부터 가정 내의 생활수요를 위한 '홈 오토메이션'을 비롯하여 자율주행자동차와 스마트 도시에 이르기까지 그 대상범위가 확대되어 가고 있고, 이들 기기를 통해 얻어지는 매년 두 배이상 늘어나는[11] 사용자 정보를 창의적으로 사용하려는 응용 프로그램 또한 사회적으로 보편화되어 있다.[12]

요컨대, 종래의 정보환경에서는 사람 중심의 정보통신에 기반을 둔 개인정보의 수집・처리가 근간을 이루었으나, 오늘날 사물인터넷 환경에서는 사물과 사물간에 소통되는 정보라고 하더라도 그 정보 속에는 사물의 식별정보(IP, Mac Adress, USIM 번호 등)를 매개로 해당 사물을 소유하거나 점유・관리하는 자의 모든 행태정보를 담고 있다. 이러한 점에서 볼 때, 사물인터넷 환경 속에서 수집・처리되는 정보는 특별한 사유가 없는 한 대부분이 개인정보의 영역에 해당함은 분명하나,[13] 개인정보가 프라이버시와 구별되는 것인지 여부는 좀 더 살펴볼 필요가 있다.

---

10) "IEEE Internet of Things Initiative is an IEEE(Institute od Electrical and Electronic Engineers) platform for the global community working on the IoT", <http://iot.ieee.org/>.

11) 오늘날 디지털 데이터의 규모는 데이터에 대한 무어의 법칙(Moore's Law)과 비슷하게 18개월에서 24개월을 단위로 두 배씩 증가하고 있다고 한다. Richard Kemp, *Legal Aspects of the Internet of Things*, Kemp IT Law, 2017, p.1

12) Juha K. Laurila / Daniel Gatica-Perez / Imad Aad / Jan Blom / Olivier Bornet / Trinh Minh Tri Do / Olivier Dousse / Julien Eberle, and Markus Miettinen, *From big smartphone data to worldwide research: The mobile data challenge* Volume 9 Issue 6, Pervasive Mob, Comput., 2013, pp.751-772.

13) 이애리/김범수/장재영, "사물인터넷(IoT)환경에서의 개인정보 위험분석 프레임워크", 한국IT서비스학회지 제15권 제4호, 한국IT서비스학회, 2016, 44쪽.

3. 개인정보와 사물인터넷의 위협

3.1 개인 데이터의 증가와 빅데이터

먼저, 사물인터넷환경에서 이렇게 실시간으로 수집되는 개개인 데이터는 해당 개인의 정치적・경제적・문화적・사회적 성향 등 망라적 데이터의 총체를 이루게 되며, 이와 같이 수집・처리・공유되는 데이터의 총체는 빅데이터[14]를 통해 공공과 민간영역을 아우르는 새로운 가치창출을 기다리는 잠재자원으로 존재하게 된다.[15]

반면에, 데이터의 홍수 속에서도 익명・비식별화된 개인 데이터로부터 정보주체를 식별・재식별할 수 있는 빅데이터의 능력은 우리 사회를 'Zero-privacy' 사회,[16] '자신을 감시자로 하려는 사회'(Self-Serveilence Society)[17] 내지 '전체주의 사회'[18]로 빠져들게 하는 지뢰가 될 수도 있다. 그럼에도 불구하고, 이미 우리 일상생활의 구성요소로 된 사물인터넷기기의 사용자 대부분은 자신에 관한 데이터의 수집・처리의 전체 과정에 대해 수동적인 지위를 가질 뿐만 아니라 자신이 실시간으로 감시・추적당하고 있다는 사실[19]도 제대로 인식하지 못하는 실정이다. 이러한 점에서 사물인터넷환경의 뜨거운 감자가 되고 있는 프라이버시의 문제[20][21]를 현행법령에 의한 정보자기결정권으로 대응

14) 빅데이터는 "클라우드 컴퓨팅과 사물인터넷을 배경으로 실시간 수집되는 방대한 양의 정형적 또는 비정형적인 데이터로부터 가치를 추출하고 분석하는 기술"을 의미한다. John Gantz / David Reinsel, "Extracting Value from Chaos", *IDC IVIEW*, IDC, 2011, p.6 of 12; 이와달리 '빅데이터'를 말 그대로 대량의 데이터에 수집과 관리 및 분석 등을 포함하는 개념으로 이해하기도 한다. 차상욱, "빅데이터(Big Data) 환경과 프라이버시 보호", IT와 법연구 제8권, 경북대학교 IT와 법 연구소, 2014, 198쪽.

15) 고대에는 땅이, 근대에는 기계가, 지금은 데이터가 가장 중요한 자산이 되고 있다('인공지능・빅데이터 파시즘 되살린다', <http://www.hani.co.kr/arti/science/future/847763.html>, 검색일: 2018.6.25.)고도 하고 빅데이터를 고갈되지 않는 '21세기의 석유'라고도 한다. 정준현, 빅데이터법제에 관한 비교법적 연구-영국-, 한국법제연구원, 2016, 58쪽.

16) Daniel J. Solove / Marc Rotenberg, *Information Privacy Law*, Aspen, 2003, p.507.

17) 개인이나 조직 등이 자신의 수요나 목적을 달성하기 위해 인터넷을 매개로 자신의 생활영역 또는 관리・감독하에 있는 모든 사람이나 물건을 통제하려는 현상을 의미한다. Scott McNealy, Polly Sprenger, "Sun on Privacy: 'Get Over it', WIRED", <http://archive.wired.com/politics/law/news/1990/01/17538>, 검색일: 2017.3.11.

18) Mark Weiser, *The computer for the 21st century*, Scientific American 제265권 제3호, Munn & Company, 1991, pp.94-104.

19) "사물인터넷에서는 'off-line'이나 기다림은 존재하지 않게 된다. 사물인터넷을 사용하지 않으려고 하여도 사물인터넷 내에서 살아가야 하기 때문에 어느 누구도 사물인터넷의 충격으로부터 벗어날 수 없다"고도 한다. <http://www.wired.com/insights/2015/02/say-goodbye-to-privacy/>, 검색일: 2018.5.7.

20) 1991년 '유비쿼터스 컴퓨팅'이라는 용어를 처음으로 사용한 Mark Weiser가 '프라이버시는 유비쿼터스 컴퓨팅

할 수 있는 것인지는 의문이 남는다.

3.2 이종적인 사물인터넷기기와 개인정보의 안전성 위협

다종・다양한 사물인터넷 기기의 증가는 보안적인 측면에서는 '서비스제공 거부공격'이나 스파이프로그램 등 악성코드에 의한 공격 대상의 증가와 함께 사이버 위협수단의 침입경로의 증가를 의미한다.[22] 개인이 자신이 소유・관리하는 웨어러블 등의 사물인터넷 기기에 의해 생성되는 개인 데이터를 각자의 능력으로 보호할 것을 기대할 수 없음은 당연하다. 데이터 주체가 아닌 공공서비스제공자 또는 민간서비스제공자에 의해 소유・관리되고 있는, 우리의 생활 곳곳에 존재하는 수많은 사물인터넷 기기로부터 생성・처리・공유되는 개인 데이터라고 하여 그 안전성 내지 보안성이 서비스제공자 등에 의해 당연히 담보되는 것은 아니다.[23]

기본적으로 기기의 제조자를 달리하고 응용프로그램에 따른 서비스별 소프트웨어 플랫폼도 달리하는 이종적인 센서나 모듈, 웨어러블 등으로 구성되는 사물인터넷환경은 '통제되지 아니하는 환경, 이종성 및 확장성의 요구를 기본적인 특징으로 한다.[24] 이러한 특징으로 인하여 사물인터넷을 위한 보안의 기본모델은 기밀성, 무결성 및 가용성을 기반으로 한 보안시스템으로 되어야 한다는 것이 일반적으로 승인되고 있다.[25] 그러나 이들 세 가지는 상호 배타적인 것으로 동시에 모든 것을 구현할 수 없다는 점에 문제의 심각성이 발견된다. 데이터에 대한 기밀성과 무결성에 대한 손상이나 변경이 없는 상태에서 자원으로서 데이터의 가용성만 제고하는 것은 기대하기 어렵다.[26]

의 핵심과제 중의 하나임을 이미 확인하였다. MarcLangheinrich, "Privacy in ubiquitous computing": John Krumm, *Ubiquitous Computing Fundamentals*, CRC Press, 2009, p.159.

21) Farzad Kamrani, Mikael Wedlin, Ioana Rodhe, *Internet of Things: Security and Privacy Issues*, FOI-R - 4362 - SE (https://www.foi.se/report-search/pdf?fileName), p.3 of 43.

22) Farzad Kamrani, Mikael Wedlin, Ioana Rodhe. *Ibid*., p. 40.

23) 'Georgia Institute of Technology'는 "2015년 출현하는 사이버위협에 관한 보고서"에서 사물인터넷과 관련된 위협으로서 다음을 제시하고 있다; ① 공격자는 사용자와 기계 사이의 신뢰관계를 표적으로 한다. ② 기술은 감시를 가능하게 하는데, 정책은 이를 따라가지 못하고 있다. ③ 모바일 기기는 점증하는 공격의 대상이 된다는 점에서 생태계 보안이 요구된다. Farzad Kamrani, Mikael Wedlin, Ioana Rodhe. *Ibid*., p.11

24) Emmanouil Vasilomanolakis, Jörg Daubert, Manisha Luthra, Vangelis Gazis, Alexander Wiesmaier and Panagiotis Kikiras, "On the security and privacy of Internet of Things architectures and systems", In International Workshop on Secure Internet of Things (SIoT 2015), 2015.

25) Farzad Kamrani, Mikael Wedlin, Ioana Rodhe. *Ibid*., p.12.

26) 2012년 수원의 여성 납치살해 당시 피해자가 112로 구조신고를 하였으나, 당시의 「위치정보의 보호 및 이용에

그렇다고, 가용성을 위해 기밀성을 제한하기도 어렵다. 왜냐하면, 악의적인 공격자는 물리적・사회공학적 접근을 통해 급증하고 있는 이종적인 사물인터넷 시스템의 취약점을 더 많이 악용할 수도 있다.[27] 그밖에, 사용자의 편의를 보장해 주는 스마트폰・CCTV 및 다양한 기능의 웨어러블이나 가정용 사물인터넷기기 등이 지능화되고 있는 악성코드에 감염되거나 백도어가 내장되어[28] 종국적으로는 악의자의 명령에 따라 개인을 감시하는 스파이로 전락할 가능성[29]도 있기 때문이다.

이러한 사정은 무결성에 대해서도 타당한다. 빅데이터를 통한 가치 있는 데이터세트・데이터베이스의 생산을 비롯하여 클라우드 컴퓨팅기술의 속성에 의해 분산화・암호화된 비식별 개인 데이터라고 할지라도 해당 개인을 특정화할 수 있는 빅데이터[30]를 통한 선제적 서비스 목적의 개인화 또는 위협데이터로부터 사회공동의 안전을 목적으로 공공 및 민간 보안기관 상호간에 이루어지는 데이터 공유[31] 등은 원 데이터의 손상을 통해 그 목적에 따른 유가치적인 데이터의 생산이 가능하기 때문이다. 이러한 과정에서 이들 데이터 세트나 개인화작업 등은 언제든지 정보주체에 대한 감시의 도구로 전락될 수 있어[32],

---

관한 법률」이 경찰에 대해 위치정보에 대한 접근권을 허용하지 아니한 결과 피해자가 살해당하는 결과를 막지 못하였다는 비판이 있자, 같은 해 5월 법 개정을 통해 경찰에 대해서도 긴급구조를 목적으로 개인위치정보에 접근할 수 있도록 하였다. 조용혁, 긴급구조를 위한 개인위치정보의 이용에 관한 법제개선방안, 한국법제연구원, 2014. 13쪽.

27) Farzad Kamrani, Mikael Wedlin, Ioana Rodhe. *Ibid*., p. 8.

28) 2015년 한국에 수출된 중국산 CCTV에서 제조사가 의도적으로 숨긴 Back door가 발견되어 보안 기기가 감시기기로 탈바꿈하는 사태가 발생하였다(“CCTV가 스파이?”, <http://www.etnews.com/20150531000071>, 검색일: 2016.6.1.). 기타 “The internet of things: how your TV, car and toys could spy on you”, <https://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys>.

29) “US intelligence chief:we might use the internet of things to spy on you”, <https://www.theguardian.com/technology/2016/feb/09/>, 검색일: 2018.3.21.

30) 이와 관련한 ‘Netflix’ 사건에 대하여는 정준현/권오민, “개인정보의 수집, 처리, 제3자제공과 가치창출에 관한 법적 문제 연구”, 홍익법학 제16권 제1호, 홍익대학교 법학연구소, 2015, 6쪽 참조. 그 외에 미국 매사추세츠州의 단체보험위원회(Group Insurance Commission)가 이름・사회보장번호 등 식별정보를 제거한 모든 주 공무원의 병원방문 기록을 무료로 관련 조사기관에게 제공하였던바, 삭제되지 아니한 성별・생년월일 및 우편 번호와 같이 남은 데이터를 유권자 데이터베이스에 연결하여 해당 개인을 식별할 수 있음이 증명되었다. Daniel C. Barth-Jones. The ‘re-identification’ of Governor William Weld’s medical information: A critical re-examination of health data identification risks and privacy protections, then and now. Available at SSRN <http://ssrn.com/abstract=2076397>, 검색일: 2018.2.5.

31) 우리의 경우에는 정보를 공유에 따른 사건에 있어서 정보제공 업체에 대해 민사・형사사건에 대한 면책권을 규정한 입법(예: 미국의 사이버보안 정보 공유법(Cybersecurity Information Sharing Act))이 미비하여 위협정보의 공유는 형식적인 것에 그치고 있어 실시간의 공유를 통한 위협정보의 유형화도 쉽지 아니한 실정이다. 박상돈, “종합적 사이버보안 법률 제정에 관한 시론적 연구”, 입법과 정책 제6권 제2호, 국회입법조사처, 2014, 참조.

사물인터넷시대의 가장 중요한 화두는 개인 프라이버시의 문제로 귀결될 수밖에 없다.

4. 사물인터넷 환경과 국가의 과제

4.1 사물인터넷 환경과 국가의무

국가의무로서 국민의 안전에 대한 보장은 국가의 가장 기본적인 목적이며, 이러한 목적을 위해 헌법이 명한 민주주의원리・법치주의원리 및 사회국가원리에 입각하여[33] 입법을 수단으로 과소보호의 원칙에 따라 인간의 존엄과 가치에 대한 보호장치가 마련되어야 하며, 이러한 보호입법에서 요구되는 보호조치의 수준은 최소한 과소보호의 기준을 넘는 '효율적'이고 '충분한' 조치라야 한다.[34] - 후술하는 안전요건의 구비를 필수로 하되 보안요건을 부수적으로 하여야 할 것으로 생각된다.

이러한 보호조치에 근거한 입법에 의할 때 국가의 국민에 대한 명령・강제권한이 정당화될 수 있다.[35] 그리고, 그 정당화는 전방위적인 위험으로서 무질서 상태를 일반적 안전으로 발전시키고, 인간의 이기심을 사회조화적인 방향으로 이끌며, 갈등의 해결을 개인능력에 의한 자기사법(Selbstjustiz)에 맡기기 보다는 국가에 의한 권리보호의 공정한 절차로 전환시키는 것이라야 한다.[36]

요컨대, 인터넷에 연결되는 모든 기기가 스파이로 기능할 수 있는 사물인터넷환경하에서는 "현재의 정보기술혁명이 민주주의보다 독재에 보다 효율적이다"는 정부에 의한 감시우려[37]도 있지만, 국가기관 상호간의 견제와 균형의 원리에 대한 믿음을 바탕으로 국가에 의한 시대조화적인 개인정보 보호입법의 수립과 집행에 의존할 수밖에 없다.

---

32) 이창범, "개인정보보호법제 관점에서 본 빅데이터 활용과 보호 방안", 법학논총 제37권 제1호, 단국대학교 법학연구소, 2013, 518쪽; 허성욱, "한국에서 빅데이터를 둘러싼 법적 쟁점과 제도적 과제", 경제규제와 법 제7권 제2호, 서울대학교 공익산업센터, 2014, 16-17쪽.

33) 이러한 원리는 모두 궁극적으로는 개인의 인간존엄을 실현하기 위한 객관적인 조건들이자 제도적 장치이다. 방승주, "헌법 제10조", 헌법 주석서 Ⅰ, 한국헌법학회, 법제처, 2007, 250쪽.

34) 이부하, "비례성원칙과 과소보호금지원칙", 헌법학연구 제13권 제2호, 한국헌법학회, 2007, 10쪽.

35) 헌법재판소 2011. 8. 30. 선고 2008헌가22, 2009헌가7・24, 2010헌가16・37, 2008헌바103, 2009헌바3, 2011헌바16(병합) 결정; 헌법재판소 2011. 8. 30. 선고 2007헌가12, 2009헌바103(병합) 결정.

36) 小山 剛/上村 都/栗城壽夫, "3. 保護義務としての基本權", 保護義務としての基本權(ドイツ判例研究會), 信山社, 2003. 136頁.

37) 사물인터넷사회에서 정부에 대한 신뢰는 정부에 의한 개인의 프라이버시에 대한 보장을 전제로 한다. Robert Alexy, *A Theory of Constitutional Rights*, Oxford University Press, 2002, p.149.

4.2 국가의 과제

이러한 의무를 이행함에 있어서는 먼저 안전보장(Security)의 요소인 안전(Safety)과 보안(Security)을 구별[38]할 필요가 있다. 유형적이며 측정이 가능한 위험으로부터 개인 프라이버시를 보호하는 요건으로서 '안전'을 국가의 최소한의 의무로 삼되, 지속적 관찰・추적이 어렵고 비유형적이며 측정하기도 어려운 계획된 위협으로부터 개인 프라이버시의 보호를 내용으로 하는 '보안'을 사이버 위협의 속성에 비추어[39] 기대 가능한 합리적인 범위 내에서 국가의 최대한의 의무로 삼을 필요가 있다.[40]

다음으로, 고도화・지속화되어 사전탐지 및 유형화에 어려움이 있는 보안의 영역에 속하는 사물인터넷환경의 사이버위협을 지속적으로 구조화하는 작업을 통해 해당 위협을 공유화하면서 정형화하여 사전예측이 가능하도록 하는 안전의 영역으로 전환하려는 국가의 끊임없는 노력 또한 계속되어야 한다. 끝으로, 사물인터넷서비스의 제공자와 사용자 사이에 내재된 정보격차에서 비롯하는 '통제의 불평등'이라는 사회적 불평등[41]을 입법자가 확인・시정하여 헌법에 의해 보장되어 있는 정보자기결정권을 사적 자치의 원리에 따라 효과적으로 행사할 수 있도록 현실적인 조건을 입법적으로 형성해야 한다는 사회국가원리에 따른 과제 또한 배제해서는 아니된다.[42]

위에서 살펴본 인간존엄과 가치의 하나로서 프라이버시 보호에 대한 국가의무를 입법적・정책적으로 실현함에 있어서는 개인 데이터의 보호를 위해 요구되는 보안요소로서

---

38) 보안과 안전의 기본이념은 동일하나 법적인 분석을 위해서는 양자를 구별하고 있다. Jeremy J. Waldron/Eirik Albrechtsen, "Security vs safety", *Nebraska Law Review*, Volume 85, Issue 2, 2006, <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1118&context=nlr>, 검색일: 2018.7.5.

39) 지난 10년간 약 6억개 이상의 악성코드가 출현한 가운데 상위 6개 백신제품에서도 62.5%에 달하는 악성코드 파일은 탐지하지 못하는 것으로 조사됐다고 한다. <https://www.paloaltonetworks.com>, 검색일: 2018.7.21. 그밖에 상세한 내용은 정준현, "사물통신시대의 국가안보 위협으로서 간첩활동과 관련 법률의 부정합성", 미국헌법연구 제27권 제2호, 미국헌법학회, 2016, 341쪽 참조.

40) 이와 관련하여, "지금의 정치는 데이터 흐름을 통제하기 위한 투쟁이 되고 있다"면서 "현재의 정보기술혁명이 민주주의보다 독재에 보다 효율적이다"는 비판이 있다. '인공지능・빅데이터 파시즘 되살린다'. <http://www.hani.co.kr/arti/science/future/847763.html>, 검색일: 2018.6.25.

41) 배분적 정의의 관점에서 사물인터넷이 수집하는 정보에 따라 차별화된 서비스를 제공하고 또한 이에 기해 사용자에 대한 맞춤형 분류를 시도하는 것이 곧 사용자를 불합리하게 차별하는 것으로 사물인터넷의 정보수집기능이 평등정신을 구현하지 못한 정도의 위험성을 갖는다고 일률적으로 단정할 수 없다(김영진, "사물인터넷에 관한 공법상 쟁점과 입법정책소고", 경제법연구 제15권 제3호, 한국경제법학회, 2016, 310쪽.)고 하나, 차별화된 서비스의 사용자라 하여 정보격차에 따른 위험이 해소된 것으로 쉽게 판단할 문제는 아닐 것이다.

42) 같은 취지, 小山 剛/上村 都/栗城壽夫, 앞의 논문, 174頁.

상호배타적인 기밀성・무결성과 가용성에 대해 상쇄(Trade-off)관계를 통한 'Zero-Sum'을 기준으로 삼기 보다는 'Positive-Sum'의 사회적 이익을 얻을 수 있도록 하여야 한다.[43]

Ⅲ. 사물인터넷 환경에 있어서 개인정보와 사생활의 보호

1. 개인정보와 사생활

1.1 법제현황

공공과 민간영역에 걸쳐 모든 사람을 수범자로 하는 현행 「개인정보보호법」은 정보통신서비스제공자등과 사용자만을 수범자로 하는 2001년 7월 1일의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(정보통신망법) 제2조 제6호에 의한 입법정의에 따라 생존하는 개인의 직접식별정보 외에 '다른 정보와 쉽게 결합하여 해당 개인을 알아볼 수 있는 정보'를 개인정보로 정의(제2조 제1호)하여 시대적 변화에 적응하지 못하고 있다.[44][45]

---

43) 종래의 인터넷 환경에서의 보안위협과는 다른 새로운 사물인터넷환경에서의 위협이나 위험에 선제적으로 대응하지 못할 경우에는 현대 사회시스템 전반에 혼란이 발생할 우려가 높다고 경고한다. 德田 英幸, "IoT時代のセキュリティ課題", *SEC Journal Vo.12 No.13*, IPA, 2016, 1頁.

44) 대만의 個人資料保護法 제2조 제1호는 개인정보를 "자연인의 이름, 생년월일, 주민등록번호, … 개인을 직접 또는 간접적으로 식별하는 기타 정보"로 정의하여 우리와 유사한 태도를 취하고 있다, 翁清坤, "대만의 개인식별 번호법제 현황과 문제점", 한국법제연구원 학술대회 자료집, 한국법제연구원, 89쪽; 이기호/김계현, "대만 개인정보보호법의 주요 내용과 함의", 東北亞法研究 제11권 제2호, 전북대학교 동북아법연구소, 2007, 62쪽 등 참조.

45) 일본의 경우 2017년 5월30일부터 시행되는 개정된 個人情報の保護に関する法律 제2조에서는 종전법의 개인정보(제1호) 개념에 개인식별부호를 포함시키고 있다. 개인식별부호에 대하여 같은 법 제2조 제2항은 "특정 개인에 관한 신체의 일부 특징을 전자계산기용으로 제공하기 위해 변환된 글자, 번호, 기호 그밖의 부호로서 해당 특정 개인을 식별할 수 있는 것(제1호), 개인에게 제공되는 용역의 이용 또는 개인에게 판매되는 상품의 구입과 관련하여 할당되거나 개인에게 발급되는 카드 그밖의 서류에 기재된 또는 전자적 방식에 의해 기록된 글자, 번호, 기호 그밖의 부호로 그 이용자나 구입자 또는 발급을 받는 사람에게 별도로 할당되거나 기재 또는 기록됨으로써 특정 이용자 또는 구입자 또는 발행을 받을 자를 식별할 수 있는 것(제2호) 중 政令으로 정한 것으로 한다고 별도로 정의하여 우리와 차이를 보이고 있다. 참고로, 개인정보의 개념과 관련하여 우리법은 다른 정보와 '쉽게 결합'하여 알 수 있는 것으로 되어 있으나 일본법은 쉽게 '照合'하여 특정개인을 식별할 수 있는 정보를 포함한다고 한 점에서 차이가 있다. 그러나, '조회'를 'reference'로 표기하는 점(<http://www.cas.go.jp/jp/seisaku/hourei/data/APPI_2.pdf>)에 비추어 양자는 동일한 것으로 새길 수 있을 것으로

1.2 개인정보에 대한 자기결정권(E-프라이버시권)

"개인, 단체 또는 기관이 언제, 어떻게 어떠한 범위까지 자신에 대한 정보를 다른 사람과 소통할 것인가를 결정할 것을 주장할 수 있는 권리(Claim)"로 정의[46]되고 있는 영・미계통 국가의 E-프라이버시권 내지 정보 프라이버시권은 대륙법계의 국가에서 통용되는 정보자기결정권과 차이점을 보이지 아니한다.

어쨌든, 현행 개인정보보호법은 OECD의 개인정보보호 8원칙에 입각하여(법 제3조), 개인정보에 대한 정보주체의 통제권을 주된 내용으로 하는 정보자기결정권을 인정하고 있다.[47] 이들 권리의 세부적인 사항은 제15조부터 제39조의2까지 29개의 조문에 걸쳐 규정하고 있는데, 그 중에서 민감정보[48]・고유식별정보에 대한 안전성 확보에 필요한 조치의무(제23조 제2항・제24조제3항), 주민등록번호에 대한 암호화조치(제24조의2 제2항) 및 개인정보 보호인증제도(제32조의2)는 정보통신환경의 변화에 순응하기 위해 새롭게 신설한 제도이다.

이와 관련, 우리의 개인정보보호법제가 최근에 개정・시행된 일본의 個人情報の保護に関する法律 제2조 제9항의 '익명가공정보'[49]와 같은 규정을 마련하지 못함으로써 익명화된 개인정보를 정보주체의 통제를 받지 않고 활용할 수 있도록 하는[50] 빅데이터의 활로를 개척하지는 못한 점은 아쉬움으로 남는다.

보인다.

46) Alan F. Westin, *Privacy and Freedom*, p. 7.

47) 이영준 교수는 민법개정시안으로서 "민법은 모든 사람이 자기의사에 의하여 자신의 생활관계를 형성함으로써 자신의 존엄과 가치를 실현하고 생활을 할 수 있게 하는 것을 목적으로 한다"는 내용을 민법 제1조에 명시할 것을 주장하고 있다. 이영준, "민법의 지도원리로서 사적 자치- 민법개정안에 언급하여", 법조 통권 제527호, 법조협회, 2000, 47쪽.

48) 개정된 일본의 個人情報の保護に関する法律 제2조 제3항은 우리 법이 민감정보로 분류하고 있는 "본인의 인종, 신조, 사회적 신분, 병력, 범죄경력, 범죄피해를 당한 사실과 그밖에 본인에 대한 부당한 차별・편견이나 그밖의 불이익이 발생하지 않도록 취급에 특별한 배려가 필요한 것으로 정령이 정하는 사항을 포함하는 개인정보"를 '要配慮個人情報'로 규정하고 있다(제2조 제3항).

49) 이에 의하면, 제1항 제1호에 해당하는 개인정보의 경우에는 해당 개인정보에 포함된 記述 등의 일부를 삭제(해당 일부 記述 등을 복원할 수 있는 규칙성을 갖지 않는 방법으로 그밖의 다른 記述 등으로 대체하는 것을 포함)하여, 그리고 제1항 제2호에 해당하는 개인정보의 경우에는 해당 개인정보에 포함되는 개인식별부호 전부를 삭제(해당 개인식별 부호를 복원할 수 있는 규칙성을 가지지 않는 방법으로 다른 記述 등으로 대체한 것을 포함)하여 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻는 개인에 관한 정보로서 해당 개인정보를 복원할 수 없게 한 것을 익명가공정보로 정의하고 있다.

50) 菅原貴与志, "改正個人情報保護法の問題", 慶應法學 第34號, 慶應法学 法務研究科, 2016, 36頁.

1.3 정보주체의 동의권과 통제능력의 한계

‘지구촌 프라이버시 집행 네트워크’(Global Privacy Enforcement Network; GPEN)의 2016년 9월의 연구보고서[51]에 의하면, 조사의 대상이 된 기기의 약 2/3는 개인정보가 어떻게 수집・이용・저장・공개되는지에 관하여 그리고 기기의 3/4는 개인정보에 대한 삭제의 방법에 관하여 기기의 사용자에게 적절한 정보를 제공하지 못한 것으로 밝혀졌다고 한다. 이로 인하여 다음과 같은 결과가 야기될 수 있다.[52]

즉, ① 사용자는 자신이 사용하는 웨어러블 등의 기기가 인터넷과 연결될 때 야기되는 개인정보의 생성・저장에 대해 적절한 통제능력을 갖지 못하게 된다. ② 자신이 사용하는 기기에 의해 생성되는 데이터의 처리와 관련하여 정보주체의 동의가 불완전하게 이루어질 수 있다. ③ 빅데이터에 의하여 사용자가 동의한 바 없는 다른 용도로 개인에 관한 정보가 사용될 가능성을 배제할 수 없다. 그밖에 ④ 서로 다른 기기로부터 획득한 데이터의 집합은 서비스제공자의 ‘디지털 우선’(Digital First)[53]과 관련하여 개인의 특정한 측면을 부당하게 침해할 수 있다.

위와 같은 문제의 해소를 위해서는 정보주체에 대하여 진정한 선택과 통제가 가능할 수 있도록 보다 높은 수준의 정보주체의 동의를 요건으로 하면서 개인에 관한 정보의 처리를 계약이행에 엄격하게 한정시킬 필요가 있다.

2. 개인정보와 프라이버시의 동일성 여부

현행의 개인정보보호법제는 앞에서 살펴본 바와 같이 정보주체의 이름이나 주민등록번호 등 직접식별정보 뿐만 아니라 개인의 형태정보라고 할지라도 다른 정보와 쉽게 결합하여 해당 개인을 알 수 있는 정보에 속하면 그 간접정보 또한 개인정보의 범주에

51) GPEN Privacy Sweep, Internet of Things: Participating Authorities’ Press Release, <https://www.privacyenforcement.net/node/717>, 검색일: 2018.3.12.

52) Richard Kemp, *Ibid*., p.3.

53) 2014년 뉴욕타임스 ‘혁신 보고서’에 처음 등장한 ‘디지털 퍼스트’ 개념은 보고서 발표 이후 신문을 비롯한 미디어 업계는 물론 일반 소비자와 관련된 비즈니스 대부분의 영역에 걸쳐 미래 전략의 핵심 키워드 중 하나로 거론되고 있다(한국경제매거진, 2016.12.14.). 일본에서는 기업과 개인이 스마트 폰 등을 통해 주소변경이나 법인설립절차 등 행정민원을 전자적으로 수행할 수 있도록 하는 내용의 “디지털 퍼스트 法案”이 국회에 제출될 것으로 보도되고 있다. 日本経済新聞　電子版, “デジタルファースト法案次期国会に提出へ　行政手続き、電子申請に統一”, 2018. 6. 7.

포함시키고 있다. 따라서, 식별정보로서의 개인정보와 프라이버시의 영역에 속하는 개인정보가 혼재된 것으로 읽혀지고, 그 점에서 개인정보자기결정권은 프라이버시권과 동일하게 보아도 되는 것인지가 문제될 수 있다.

참고로, 개인정보의 보호법익과 관련하여서는 '개인정보의 수집・처리 및 활용을 통해 사회질서 및 행정효율을 향상시킴으로써 궁극적으로 공익을 증대한다'고 하는 사회적 법익설, '개인정보를 기업의 이윤증대를 위한 기업자산 또는 자원'으로 파악하는 경제적 법익설, 그리고 '개인정보는 사적 거래의 대상이 되지 아니하는 것으로 개인의 인격을 형성하는 요소'로 이해하는 개인적 법익설의 대립이 있다.[54] 생각하건데, 사물인터넷 환경 하에서 수집・처리되는 개인정보는 국가와 사회를 구성하는 자연인에 대한 정보인 동시에 해당 자연인이 사물인터넷 사회를 살아가면서 수인하여야 할 정치・경제・문화 등 모든 영역에 대한 수요정보라는 점에 비추어 볼 때, 개인정보가 갖는 사회적 및 경제적 법익으로서의 부수적 특성을 배제할 수는 없다.

2.1 개인정보와 프라이버시

우리 판례[55]는 일관되게 정보자기결정권의 헌법적 배경을 헌법 제10조의 인간의 존엄・가치 및 행복추구권과 헌법 제17조의 사생활의 비밀・자유권에서 도출되는 것으로 전제하면서, 개인정보자기결정권의 보호대상이 되는 개인정보를 개인의 신체・신념・사회적 지위와 신분 등과 같이 인격주체성을 특징짓는 사항으로서 개인의 동일성을 식별할 수 있게 하는 일체의 정보로서 개인의 내밀한 영역에 속하는 정보는 물론 공적 생활에서 형성되었거나 이미 공개된 개인정보까지도 포함하는 것으로 새기고 있다.[56]

이와 달리, 사생활의 비밀・자유의 불가침권은 제3자가 사생활 영역을 들여다보는 것에 대한 보호를 제공하는 기본권으로서 사생활의 자유는 국가가 사생활의 자유로운 형성을 방해하거나 금지하는 것에 대한 보호를 의미한다.[57] 이러한 사생활권은 자연인

54) 정준현, "개인정보의 통합관리에 따른 법적 문제", 외법논집 제36권 제3호, 한국외국어대학교 법학연구소, 2012, 152-153쪽 참조.

55) 헌법재판소 2010. 2. 25. 선고 2008헌마324, 2009헌바31 전원재판부 결정; 대법원 2014. 7. 24. 선고 2012다49933 판결; 대법원 2016. 3. 10. 선고 2012다105482 판결 등; 열거되지 아니한 기본권을 본 경우(헌법재판소 2005.5.26. 99헌마513)도 있다.

56) 유럽사법재판소도 유럽인권재판소의 판례에서 언급하고 있는 '사생활'을 식별되거나 식별가능한 개인과 관련된 모든 정보로 정의되는 개인데이터에 대한 보호를 포함하는 의미로 해석하고 있다. CJEU, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, para. 52.

이나 법인이 자신에 관한 정보를 스스로 관리・통제할 수 있는 인격권적인 권리로서 제3자의 알권리에 우선함을 명백히 하고 있다.[58]

위의 판례입장에 의할 때, 개인정보와 프라이버시(사생활)는 권리주체와 데이터의 내용면에서 구별된다. 즉, 개인정보는 자연인을 주체로 삼아 사적 영역 및 공적 영역과 관련된 일체의 정보를 대상으로 하나 프라이버시는 자연인 및 법인을 주체로 삼지만 그 데이터의 영역은 사적 영역에 한정된다는 점에서 양자는 구별된다. 이러한 점에서 개인데이터의 보호범위는 프라이버시 보다 넓다.[59] 그밖에, 허용되는 침해와 관련하여서도 양자는 구별된다. 즉. 개인정보보호법제가 허용하고 있는 합법적인 사유에 근거하여 개인데이터를 수집・처리・제3자 제공하는 것은 개인정보에 대한 침해를 구성하지 않지만, 프라이버시에 대한 침해를 구성할 수는 있다는[60] 점에서 구별된다.

2.2 관련 사례

양자는 다음과 같은 점에서 구별이 필요하다. 구체적인 예를 들자면, 체납된 사회보장분담금의 강제징수를 위해 체납자의 주택을 경매하는 절차의 일환으로서 국가가 관련 법령이 정한 바에 따라 소유자의 신원과 대상 주택을 일간지에 공고하였고, 경매가 종료된 이후에 구글의 검색엔진을 통해 제3자가 체납자에 관한 위와 같은 정보에 접근할 수 있게 되어 야기된 'Google Spain 사건[61]'에서는 두 가지의 관점이 가능하다. 즉, 프라이버시의 관점에서는 해당 일간지에 합법적으로 게재된 해당 정보가 사생활에 영향을 미친다면, 제3자와 해당 정보를 일간지에 게재한 국가에게 관련된 법적 책임이 귀속된다. 반면, 개인정보의 관점에서는 관련 정보를 삭제하거나 접근차단의 조치를 취하지 않고 인터넷 검색엔진에 의한 처리를 가능하도록 방치한 해당 일간지가 관련된 법적 책임을

57) 헌법재판소 2011. 10. 25. 선고 2009헌마691 결정; 헌법재판소 2011. 8. 30. 선고 2009헌바42 결정 등; 프라이버시권은 개인에게 근본적인 영향을 미치는 문제에 대하여 부당한 정부의 간섭으로부터 자유로울 개인의 권리이다. Eisenstadt v. Baird 405 U.S. 438(1972), p.34.

58) 서울고등법원 1995. 8. 24. 선고 94구39262 판결: 확정 [정보공개청구거부처분취소].

59) Juliane Kokott and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Volume 3, Issue 4, Oxford Academic, 2013, p.225.

60) CJEU, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, para. 49.

61) CJEU, Case C-131/12 [2012] OJ C165/11. Please note that the authors are not responsible for this case at the Court of Justice and that the following remarks are not based on any internal information. The Opinion of Advocate General Jääskinen of 25 June 2013 was not yet available when the article was written.

부담하여야 한다는 추론이 가능하다.[62]

그밖에, 행정규제의 대상인 개인정보는 그 대부분이 프라이버시의 성격을 갖는다는 사실을 인정하면서도 공개・비공개, 민감성・프라이버시성 유무나 정보의 가치정도에 관계없이 '특정개인의 식별정보'를 개인정보로 정의하고, 주로 민사규제에 의존하게 되는 프라이버시는 '자신에 관한 정보가 함부로 제3자에게 공개되지 아니할 자유'라는 일본최고재판소의 정의에 따라 특정개인을 식별할 수 없는 정보라고 하더라도 프라이버시를 침해할 수 있다는 견해도[63] 양자의 구별필요성을 인정한다. 현재 일본은 특정성과 식별성만을 요건[64]으로 특정개인을 식별할 수 있는 것을 모두 개인정보로 정의하는 것이 일반적인 것으로 보인다.[65]

2.3 구별의 필요성

프라이버시와 개인정보는 그 대상이나 사항적인 범위 및 실체적인 권리의 내용면에서 차이가 상존한다. 자연인으로서의 개인의 관점에서는 개인정보의 보호범위가 보다 포괄적이고 실체법상의 접근・차단・정정・삭제권 등을 통해 보다 적극적이고 예방적인 수준의 추상적 보호가 가능하다. 이에 반하여 프라이버시권은 사적 영역에 대한 침해의 구체성이 인정되어 민사법상의 분쟁으로 되는 경우에 한하여 소극적 내지 사후구제적인 대상이 될 뿐이다. 그밖에, 공정하고 목적에 맞게 처리되어야 한다는 개인정보의 보호요건은 프라이버시 침해를 정당화할 수 있는 사유인 '법질서와 합치성'[66], '목적의 정당

62) Juliane Kokott and Christoph Sobotta, *Ibid.*, pp.227-228.

63) 鈴木正朝, プライバシ-の權利と個人情報保護法, 平成 24年11月, <https://www.cas.go.jp/jp/seisaku/mynumber/symposium/iwate/siryou5.pdf>, 검색일: 2018.7.15.

64) 이와 관련하여 개정전의 個人情報の保護に関する法律에 대해 일본의 '기술검토 워킹그룹'은 현행법상 개인정보에 대한 용어정의는 기술적 관점에서 명확하지 않다고 하면서 "① 현행법의 '照合의 용이성'에 대해 ㉠ 현행법의 해석이 명확하지 않다는 것과 ㉡ 현행법의 제정 당시보다 기술진전에 의해 프라이버시 침해를 유발할 수 있는 다른 정보와의 照合 가능성이 높아져 현행법의 '照合의 용이성'의 요건에 대해 별도의 검토가 필요하다. ② 개인정보 여부에 대한 판단기준으로서 개인식별성을 '특정'과 '식별'로 나누고, 해당 정보가 누구 것인지를 알 수 있는 것을 '특정'으로, 해당 정보가 누구의 것인지는 특정할 수 없으나 어느 집단에 소속한 사람에 대한 것임을 알 수 있는 상태를 '식별'로 구별할 필요가 있다고 제안하여 식별의 경우에는 정보주체의 동의대상이 되지 아니하는 것으로 해야 한다는 뉘앙스를 남기고 있다. 技術検討ワーキンググループ, 報告書<http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf>, 1/37쪽 참조.

65) 이에 대하여 정보의 종류나 이미 공지된 정보인지 여부 또는 일반적으로 다른 사람에게 알리고 싶지 않는 정보인지 여부 등에 대한 구별 없이 법률이 광범위한 개인정보개념을 취함으로서 정보의 활용을 위축하는 부작용을 낳게 되었다고 비판한다. 菅原貴与志, 앞의 논문, 29頁.

성'[67] 및 '민주사회의 필요성'[68] 등을 포섭한다는 점[69]에도 주목해야 한다.

아무튼, 개인정보에 대해 인정되고 있는 정보주체의 정보자기결정권은 자기정보에 대한 정보주체의 자유의지에 의한 통제권을 보호하는 것으로서, 개인정보자기결정권에 대한 침해는 사적 영역에 대한 현실적·구체적 침해로서의 프라이버시 침해를 구성하지는 아니함을 알 수 있다.[70] 말하자면, "정보주체의 정보자기결정권에 대한 침해 = 프라이버시권에 대한 침해"의 공식은 성립되지 아니한다.

3. 개인정보 내지 프라이버시에 대한 현행 보호수단과 대안

3.1 현행법상의 수단

앞에서 살펴본 바와 같이 개인생활의 수요를 실시간으로 충족할 다양한 기능을 가진 모든 이종적인 기기가 연결되어 개인감시의 도구 작용할 우려가 높은 사물인터넷시대에서는 정보약자인 정보주체의 정보자기결정권을 헌법의 기본질서인 민주원리·법치주의원리 및 사회국가원리와 조화를 이룰 수 있도록 하는 입법적 대안이 강구되어야 함은 당연하다.

현행 개인정보보호법 상 위와 같은 취지를 반영한 것으로 볼 수 있는 제도로는 '고유식별정보 및 주민등록번호의 처리제한'(법 제24조, 제24조의2) 및 '개인정보 유출통지'(제

66) 북아일랜드에 사는 여성(원고)이 자신의 손자를 데리고 하루 동안 잠적하였다. 해당 여성을 아동납치범으로 오인한 경찰은 수사를 개시하였고, 그 수사기록으로 인하여 해당 여성은 취업상의 불이익을 받게 되었다. 해당 여성이 영국을 상대로 제소한 사건에서 유럽인권재판소는 "원고의 사생활과 관련한 데이터가 원고의 사생활권에 반하여 공개되지 아니하도록 보장할 수 있는 충분한 안전장치가 마련되어 있지 않았다"고 하면서 인권침해를 인정하였다. ECtHR, M.M. v UK App no. 24029/07 (13 November 2012), para. 200.

67) 유럽사법재판소는 공공기금의 사용공개는 공공기금의 적절한 사용에 기여하고 농업정책에 대한 시민의 공개토론을 가능하게 한다는 사실을 전제로, 농부에 대한 농업 보조금의 공개는 공공기금 사용의 투명성을 보장하는 합법적인 목적을 위한 것으로 본다. CJEU, Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, paras 67-71.

68) 유럽인권재판소는 30년 전에 있었던 정치활동과 관련한 정보를 '비밀경찰 등록부'에 보관·관리하는 것은 비례원칙에 반한다고 판단하였다. ECtHR, Segerstedt-Wiberg and Others v Sweden App no 62332/00, ECHR 2006-VII, para. 90.

69) Juliane Kokott and Christoph Sobotta, *Ibid*., p. 228.

70) 개인정보 유출로 인하여 원고에게 신원확인, 명의도용이나 추가적인 개인정보 유출 등 후속 피해가 발생하였음을 추지할 만한 상황이 발견되지 아니하는 점 등에 비추어 볼 때, 개인정보 유출로 인하여 원고에게 위자료로 배상할 만한 정신적 손해가 발생하였다고 보기는 어렵다. 대법원 2012. 12. 26. 선고 2011다59834, 59858, 59841 판결.

34조) 등의 제도를 비롯하여 사물인터넷 서비스제공자의 책임에 초점[71]을 둔 '법정 과징금제'(제34조의 2)와 손해배상책임에 있어서의 '과실입증의 전환제'(제39조제1항) 및 손해액의 3배를 초과하지 아니하는 범위 내의 '징벌적 배상제'(제39조), '집단분쟁조정'(제49조) 및 '단체소송'(제51조) 등이 있다.

3.2 문제점

개인의 능력상 상론은 할 수 없지만, 다음과 같은 문제점을 안고 있는 이들 수단은 불평등한 사물인터넷 환경 하에서 정보주체의 개인정보의 보호 내지 프라이버시의 포괄적 보호수단으로서는 부적합한 것으로 생각된다. 새로운 제도에 대한 적극적인 검토가 필요하다.

3.2.1 손해배상과의 관계에서 과징금

불법이익의 환수수단인 과징금은 주민등록번호가 분실・도난・유출・위조・변조 또는 훼손된 경우를 대상(제34조의2)으로 하는 점에서 개인식별정보에 대한 사물인터넷 서비스자의 보호책임을 담보하는 행정수단으로 될 수는 있다. 그러나, 해당 정보주체가 이로 인하여 입은 실질적인 피해를 입증하지 못하면[72], 피해자인 정보주체는 아무런 손해배상을 받지 못하는데 국가만 과징금을 취득하게 되는 결과적 불균형이 발생하게 된다.[73] 이러한 점에서 위의 과징금 그 자체는 손해배상책임 및 빅데이터[74]의 관계에서 볼 경우 사물인터넷 환경에 있어서 보호되어야 할 정보주체의 프라이버시권 보다는 정보자기결정권의 외형보호에 치우친 제도로 폄하될 수 있다.[75]

---

71) 정보보호법제는 기존의 동의 위주에서 책임성 위주로 변경할 것이 제안되기도 한다. 박종수, 빅데이터법제에 관한 비교법적 연구-독일-, 한국법제연구원, 2016, 65쪽.

72) 정보통신서비스 제공자의 보호조치 미이행과 해킹사고의 발생 사이에 상당인과관계가 인정되지 아니하여 갑회사의 손해배상책임이 인정되지 않는다. 대법원 2018. 1. 25. 선고 2015다24904, 24911, 24928, 24935 판결.

73) 송동수/성기만, "개인정보유출에 대한 구제방안으로서 징벌적 손해배상", 토지공법연구 제67집, 한국토지공법학회, 2014, 177쪽.

74) 익명화된 개인정보의 재식별은 이미 입증되었다. 박종수, 앞의 연구보고서, 61쪽.

75) 최희경, "미국 헌법상 정보 프라이버시권", 법학논집 제19권 제2호, 이화여자대학교법학연구소, 2014, 32쪽; 미국 판례상으로서 보상가능한 실질적인 손해가 없으면 청구를 기각하고 있다. 이원우, "개인정보 보호를 위한 공법적 규제와 손해배상책임", 행정법연구 제30호, 행정법이론실무학회, 2011, 247쪽.

3.2.2 '3배 범위 내의 징벌적 배상'

위의 징벌적 배상은 "가해자의 악의적인 동기나 무모한 무관심에 기인한 터무니 없는 불법적인 행위에 대해 부과되는 손해"로 정의된다는 점[76]에서 사물통신서비스 제공자에 대한 책임을 강조하는 제도임을 부인할 수는 없다. 이러한 제도에 대하여는 정보주체에게 기대하기 어려운 손해발생의 입증에 더하여 고의・중대한 과실의 입증을 법정요건으로 하고 있다는 점[77]과 징벌적 배상의 수준을 보다 높여야 한다는 주장은 그 실효성을 떠나, 외국법원이 우리의 글로벌 기업에 대해 행한 천문학적 금액의 징벌적 배상판결에 대한 방어막인「민사소송법」제217조 제1항 제3호(선량한 풍속이나 그 밖의 사회질서에 어긋나지 아니할 것)를 [78] 우리 스스로가 제거하는 결과를 야기할 수 있다는 점에서 각각 쉽게 판단할 것은 아니다.

3.2.3 집단분쟁조정・단체소송

재판외 분쟁해결제도로서 집단분쟁조정은 세계적으로 유례없는 제도[79]라는 점은 별론으로 조정신청자의 상대방에 대해 조정절차에 응하는 것과 조정안에 대한 수락이 법상 강제되어 있지 않다(위의 법률 제43조・제49조)는 점에서 그 실효성에 의문이다. 그리고, 단체소송은 일반 공공의 이익보호를 위한 소송제도로, 권리보호의 조기화가 가능하다는 점[80]에서 사물인터넷 환경에서 정보격차의 해소를 위한 제도라고는 할 수 있다.

그러나, 위의 법률 제7장에 의한 단체소송은 소비자기본법에 의한 '한국소비자원' 이외에 비영리민간단체지원법 상의 요건을 갖춘 '경제정의실천시민연합 등의 단체를 통한 소송의 수행을 기대할 수는 있으나[81] 집단분쟁조정을 거부하거나 집단분쟁조정의 결과를 수락하지 아니한 경우에 침해행위의 금지・중지를 구하는 소송기능에만 머물고

76) 이종구, "전보배상과 징벌적 손해배상 및 3배 배상제도에 관한 연구", 경영법률 제26권 제1호, 한국경영법률학회, 2015, 451쪽.

77) 대법원 2012. 12. 26. 선고 2011다59834 판결 등 참조.

78) 미국판결에서 인정된 원고의 손해액은 모두 전보적 손해배상액에 해당하고 제재적 성격의 손해액이 포함되어 있지 않은데, 민사소송법 제217조의2의 입법 취지가 징벌적 손해배상이 아닌 전보적 손해배상의 경우에도 손해액이 과다하다는 이유만으로 외국판결의 승인을 제한할 수 있도록 한 것이라고 볼 수 없다. 대법원 2015. 10. 15. 선고 2015다1284, 판결

79) 서희석, "우리나라 집단분쟁조정제도의 현황과 과제", 비교사법 제23권 제4호, 한국비교사법학회, 2016, 1444쪽.

80) 권혁재, "독일의 단체소송제도", 민사법의 이론과 실무 제14권 제1호, 민사법의 이론과 실무학회, 2010, 126쪽; 전병서, "한국과 일본에서의 소비자단체소송제도의 도입", 법조 제56권 제4호, 법조협회, 2007, 50쪽.

81) 정혜운, "소비자 권익을 지키기 위한 법적 제도들", 한국소비자보호원 보도자료, 2008.

있어서 사물인터넷 서비스제공자의 책임의 강화를 통한 정보주체 보호의 실효성을 기대하기 어려울 것으로 보인다.

3.3 새로운 대안

사물인터넷 사회에 내재된 사물통신제어자・서비스제공자와 사용자 사이에 상존하는 다양한 불평등성에도 불구하고 사물인터넷 환경을 살아갈 수밖에 없는 정보주체의 개인정보를 보호하기 위해서는 정보주체의 정보자기결정권에 초점을 두는 방식은 지양되어야 한다. 아래에서는 이러한 목적을 위해 미국 FTC의 '사물인터넷 보고서'에 의한 '설계에 의한 보안'[82]에 상응하는 것으로서 'EU의 제29조 작업반 의견서'가 제시하여,[83] 현행 유럽연합의 'GDPR' 제25조로 수용된 '설계에 의한 프라이버시'(Privacy by Design)'을 중심으로 살펴볼 필요가 있다.

이와 관련하여 미국의 과학연구단체인 'MITRE' 등이 제안한 것으로서 비정형적인 위험의 구조화라는 점에서 '설계에 의한 프라이버시'와 상호보완적인 관계에 있는 것으로 보여지는 'STIX'(Structured Threat Information eXpression)[84]에 대해서도 살펴보기로 한다.

Ⅳ. 대안으로서 '설계에 의한 사생활 보호' 등

1. '설계에 의한 프라이버시'의 의의

1.1 의미

'설계에 의한 프라이버시'는 차용된 개념으로, 인공위성으로부터 위치정보를 송수신할 때 본인확인을 거치지 아니하듯이 '통상인은 식별이 불가능하거나 인식할 수 없는

82) '설계에 의한 보안'은 지속적인 테스트, 인증보호 및 최상의 프로그래밍 관행에 대한 준수 등의 방법을 통해 가능한 한 취약성이 없고 공격에 영향을 받지 않도록 시스템을 만드는 소프트웨어 및 하드웨어의 개발방식을 의미한다. <https://whatis.techtarget.com/definition/security-by-design>

83) Richard Kemp, *Ibid*., pp. 8-9; 심우민, "사물인터넷 개인정보보호의 입법정책", 헌법학연구 제21권 제2호, 한국헌법학회, 2015.

84) "Need for IT sharing standard", <https://www.anomali.com/platform/what-are-stix-taxii>; "Introduction to STIX", <https://oasis-open.github.io/cti-documentation/stix/intro>, 검색일: 2018.5.17.

상태로 IoT 서비스를 제공하도록 하는 소위 '개인데이터에 대한 보호가 필요 없도록 하는 설계'로 설명되고 있다.[85]

1.2 배경

인간의 수요의 실시간 충족이라고 하는 사물인터넷 사회 내지 '산업 4.0'의 요구로부터 실시간으로 수집・처리・공유되는 정보에 대한 가치와 책임 있는 정보관리의 필요성이 급격하게 증가하고 있다. 이와 동시에, 급속한 혁신, 글로벌 경쟁 및 증가하는 사물인터넷 기기와 시스템 복잡성 등은 개인정보로 인한 프라이버시 침해를 해소해야 한다는 과제를 남기고 있다.

바꾸어 말하자면, 사물인터넷이 제공하는 새로운 편의성과 효율성을 누리는 반면, 헌법 제10조가 규정한 국가의무로서 개인정보의 흐름에 대한 정보주체의 선택의 자유와 통제권을 보존해야 한다.[86] 사물인터넷 시대의 사회규범은 형식적인 준법의 요건을 넘어 정보사회에 대한 신뢰와 자유가 보장될 수 있도록 '기본사양'(by default)으로 프라이버시가 보호되는 사물인터넷 사회를 구축하는 것이 국가의 기본의무인 동시에 시장존립의 필수요건으로 요구되고 있다.

1.3 'GDPR'의 규정 내용

'GDPR' 제25조는 제1항에서 "최신 기술과 실행 비용, 처리의 성격과 범위, 상황 및 목적뿐만 아니라 처리로 인하여 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험을 고려하여, 정보처리자는 처리의 수단을 결정한 시점과 처리의 시점에서 데이터의 최소화 등 개인정보보호원칙을 이행하고 이 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해 처리에 필요한 안전조치를 포함하기 위해 고안된 익명처리 등 적절한 기술 및 관리적 조치를 이행하여야 한다"고 규정하고, 같은 조 제2항에서는 "정보처리자는 기본사양을 통해 처리의 특정한 개별목적에 필요한 범위에 한하여 개인정보가 처리되는 것을 보장하는 적절한 기술 및 관리조치를 이행하여야 한다.

85) <https://en.wikipedia.org/wiki/Privacy_by_design>, 검색일: 2018.6.22.

86) 모든 권리 가운데에서 가장 포괄적이고 문명인에게 가장 가치가 있다고 하는 권리가 있다면 그것이 바로 프라이버시권이다. 藤原靜雄, 逐條個人情報保護法, 弘文堂, 平成 15年, 1頁.

이러한 의무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기관 및 접근용이성에 적용된다. 특히, 이러한 조치는 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 기본사양을 통해 보장한다"고 규정하여 기본사양으로서 '설계에 의한 프라이버시'제도를 도입하고 있다.

2. '설계에 의한 프라이버시'의 7대 원칙

'설계에 의한 프라이버시'에 대한 7대 기본원칙은 아래와 같으며, 이들 원칙 각각은 공정한 정보원칙(The Fair Information Principles)[87]과 연결된다. 즉, ① 지구촌 법령에 의한 일반기준보다 높은 수준의 사생활 보호기준의 설정・집행에 대한 명시적 약속을 바탕으로 사생활침해의 가능성을 사전 예방적이고 혁신적으로 배제해야 한다는 '반응적이 아닌 사전적이며 사후구제가 아닌 예방이어야 한다는 원칙', ② 정보주체에 의한 별도의 조치가 없더라도, 목적의 명시, 수집 제한, 데이터 최소화[88] 및 사용・보유・공개의 제한, 불명확한 경우에는 프라이버시 추정 등과 같은 '공정한 정보원칙'(FIPs)을 기본사항으로 보장하여야 한다는 '기본사양으로서 사생활보호', ③ 사생활의 보호는 총체적(추가적이고 폭넓은 맥락에 대한 상시적 고려)・통합적(모든 이해 관계자의 의사반영)・창조적(내장된 프라이버시가 대안이 될 수 없다면 기존의 선택을 버리고 새로운 설계의 도입)인 방식으로 기술・운영 및 정보아키텍처에 포함되어야 한다는 '설계에 의해 내장된 사생활보호', ④ 대립되는 이익의 상쇄(trade-off)에 기반을 둔 시대낙후적인 'Zero-Sum'이 아니라 'Positive -Sum'이 될 수 있도록[89] 모든 합법적인 이해와 목표가

87) 이 원칙은 사용자에 대한 '고지/인식', '선택/동의', '접근/참여', '무결성/보안성', '시행/구제' 등으로 이들 공정한 정보원칙은 캐나다의 개인정보보호 및 전자문서법 (Personal Information Protection and Electronic Documents Act)의 프라이버시보호원칙으로 입법화되어 있기도 하다. "The Fair Information Principles", <https://www.privacyfirst.nl/acties-3/item/154-the-fair-information-principles-canada.html>, 검색일: 2018.7.19.

88) 개인식별정보의 수집은 최소한으로 유지하되, 정보・통신기술 및 시스템 등의 설계는 상호작용과 전송에 있어서의 비식별성을 기본사양으로 해야 하고, 어디에서나 개인정보에 대한 식별가능성, 관찰가능성 및 연결가능성이 최소화되어야 함을 의미한다. Ann Cavoukian, Privacy by Design *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices,* Information and Privacy Commissioner of Ontario, 2010, p.3.

89) 프라이버시가 주어진 범위 내에 있는 다른 합법적인 이해, 설계 목표 및 기술적 능력과 경쟁하여야 하는 'Zero-Sum'의 방식에 위치하는 경우가 있을 수 있다. 그러나, '설계에 의한 프라이버시'는 이러한 접근방식을 거부하고, 혁신적인 'Positive-Sum'의 방식으로 합법적인 非프라이버시 목표(non-privacy objectives)을 포용・수용해야 한다고 한다. Ann Cavoukian, *Ibid*., p.4.

설정되어야 한다는 '완전한 기능성', ⑤ 수집・처리된 개인정보를 안전하게 보존하고 목적이 달성된 경우에는 적시에 안전하게 삭제되는 것이 보장되어야 한다는 '종단간 보안' 내지 '수명주기에 걸친 보호', ⑥ 모든 이해 관계자는 제3자의 독립적인 검증을 전제조건으로 명시된 약속과 목적에 따라 움직여야 하며, 개인은 언제든지 개인정보의 관리와 관련된 정책과 관행에 관한 정보에 접근・이용할 수 있어야 한다는 '가시성 및 투명성' 그리고 ⑦ 인간과 기계간의 인터페이스를 인간중심의 인터페이스 내지 사용자 친화적인 인터페이스로 전환하여야 한다는 '사용자의 사생활 존중' 등 7가지를 기본원칙으로 삼고 있다.

3. 개인정보 위협의 구조화(STIX)

랜섬웨어 및 악성코드를 비롯한 각종 사이버 위협이 고도화되고 지속되고 있을 뿐 아니라 사물인테넷 환경에 있어서의 다양한 웨어러블과 소프트 플랫폼 등 사이버 위협대상의 증가는 필연적으로 위협정보의 구조화・표준화 작업과 이를 통한 위협정보의 공유를 요구하게 된다.[90] 이러한 노력의 대표적인 것이 비정형적인 사이버위협 정보를 표시하는 국제표준어가 'STIX'(Structured Threat Information Expression)이다(이러한 위협정보를 재전송하는 수단은 'TAXI'라 한다).[91]

이러한 'STIX'를 사용하게 되면, 사이버 정보 중 의심스러운 속성정보와 손상시키는 속성정보 등 모든 면을 대상과 대상에 대한 설명적인 관계로 명확하게 표현할 수 있고 사물인터넷의 제어자 등 이해관계인이 쉽게 접근할 수 있는 표현 형태('JSON')[92]로 저장될 수 있다. 'STIX'의 위와 같은 역할은 첫째, 비정형적인 사이버 위험을 최대한 정형화・

90) 미래창조과학부・한국인터넷진흥원, "사이버 위협정보 분석・공유시스템 리플렛.pdf", <https://www.boho.or.kr/data/noticeView.do?bulletin_writing_sequence=25824>, 검색일: 2018.1.14.

91) 우리나라에서는 과학기술정보통신부 산하의 KISA가 "C-TAS"를 통해 실시간이 아닌 정적인 상태로 이러한 업무를 수행하며(https://www.krcert.or.kr/data/noticeView.do?bulletin_writing_sequence=25824), 미국에서는 국토안보부소속의 MITRE가, 일본에서는 경제산업부 소속하의 독립법인인 IPA가 각각 이 업무를 수행하고 있다. 박철민/조정식, "국외사이버 위협정보공유의 체계조사", INTERNET & SECURITY FOCUS, 한국인터넷진흥원, 2014, 49,54,55쪽 등 참고.

92) JSON(JavaScript Object Notation)은 속성-값 쌍으로 이루어진 데이터 객체를 전달하기 위해 인간이 읽을 수 있는 텍스트를 사용하는 개방형 표준 포맷을 의미한다. 비동기 브라우저/서버 통신 (AJAX)을 위해, 넓게는 XML(AJAX가 사용)을 대체하는 주요 데이터 포맷이라고 한다. 특히, 인터넷에서 자료를 주고 받을 때 그 자료를 표현하는 방법으로 특히, 컴퓨터 프로그램의 변수 값을 표현하는데 적합하다고 한다. "JSON", <https://ko.wikipedia.org/wiki/JSON>.

표준화하여 IoT기기의 안전을 위한 조건으로 입법화할 수 있고(예컨대, 정보통신 진흥 및 융합활성화 등에 관한 특별법 제36조에 의한 임시조건), 두 번째로 정형화되지 아니한 첨단의 새로운 위협정보에 대하여는 보안기관 상호간 위협정보의 공유에 의한 보안성의 제고를 통해 개인정보를 지속적으로 탈취・감사하는 스파이 기능을 가진 각종 악성 프로그램으로부터 개인정보를 보호하는데 매우 유용할 것으로 판단된다.

뉴질랜드의 프라이버시 커미셔너가 2017년에 발표한 "침해신고와 관련하여 선정된 개인정보기관의 통계관행에 대한 조사결과"[93]에서 개인정보의 침해의 신고 및 통계작성과 프라이버시의 제도개선 등을 위해 구조화된 정보표시인 'STIX'의 사용을 권고하고 있는 것도 위와 같은 유용성을 인정한 것으로 볼 수 있다.[94]

Ⅴ. 맺는 말

IoT 사회는 물리적으로 작동되는 사회가 아니라 비물리적인 디지털 정보에 의해 제어되는 물리적 시스템에 의해 개인과 사회의 수요가 실시간 충족되는 'Cyber -Physical System' 사회이다. 이러한 사회에서 개인정보의 제공이 없는 개인수요의 충족이나 공공복리의 증진은 상정할 수 없다. 이러한 점에서 IoT환경에서 실시간으로 생성되는 무수한 개인정보의 집합에 내재된 무한의 가치를 현실화하려는 공공과 민간의 요구와 개인정보를 지키려고 하는 정보주체의 요구는 상호 충돌하게 된다. 이러한 충돌 국면에서는 정보주체의 자기결정권이 정보격차로 인하여 사실상 형해화되었다는 사실과 개인정보를 탈취하는 수법과 수단은 사전탐지가 어렵고 개인정보침해사고가 발생한 경우라 하더라도 입증이 어렵다는 현실이 각각 고려되어야 한다. 이러한 고려를 전제로 다음과 같은 제언을 하고자 한다.

첫째, 개인의 식별정보를 제외한 형태정보에 대한 합리적 수준의 익명화는 IoT사회의 구성원이 공동체 이익을 위해 수인해야 할 사회적 제약의 한계치로 새롭게 관념될 필요가 있다. 둘째, 개인정보를 활용하여 새로운 가치를 창출하려는 정보처리자와 그 혜택만 누리고자 하는 단순한 사용자 사이에 존재하는 정보격차의 해소를 하고, 정보처리자의

93) <http://icdppc.org/wp-content/uploads/2017/04/Breach-notification-statics-survey-repoer-18-April-2017.pdf>

94) 이에 관한 내용은 정준현 외 6인, 개인정보 침해 신고센터 업무처리 절차 개선방안 연구 최종보고서, 한국인터넷 진흥원, 2017 참조.

책임을 보다 제고하는 'PbD'과 같은 법적 제도의 개발에 집중할 필요가 있다. 셋째, 개인정보에 대한 불법접근이나 개인정보의 오·남용에 대한 사회공동체적 감시가 실시간으로 가능할 수 있도록 위협정보의 구조화·표시화에 대한 국가 노력이 강화되어야 한다. 끝으로, 각국의 '디지털 우선'을 향한 입법정책이 지구촌 공동체 차원의 'Positive-Sum'을 위한 지혜의 경쟁무대로 되길 희망한다.

참고문헌

1. 단행본

정준현, 빅데이터법제에 관한 비교법적 연구-영국-, 한국법제연구원, 2016.

정준현 외 6인, 개인정보 침해 신고센터 업무처리 절차 개선방안 연구 최종보고서, 한국인터넷 진흥원, 2017.

박종수, 빅데이터법제에 관한 비교법적 연구-독일-, 한국법제연구원, 2016.

Alan F. Westin, *Privacy and Freedom*, Atheneum, New York, 1967.

Ann Cavoukian, Privacy by Design *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices,* Information and Privacy Commissioner of Ontario, 2010.

Daniel J. Solove / Marc Rotenberg, *Information Privacy Law*, Aspen, 2003.

MarcLangheinrich, "Privacy in ubiquitous computing": John Krumm, *Ubiquitous Computing Fundamentals*, CRC Press, 2009.

Richard Kemp, *Legal Aspects of the Internet of Things*, Kemp IT Law, 2017.

Robert Alexy, *A Theory of Constitutional Rights*, Oxford University Press, 2002.

藤原靜雄, 逐條個人情報保護法, 弘文堂, 平成 15年.

小山 剛/上村 都/栗城壽夫, 保護義務としての基本權(ドイツ判例研究會), 信山社, 2003.

2. 학술지

권건보, "개인정보자기결정권의 보호범위에 대한 분석", 공법학연구 제18권 제3호, 한국비교공법학회, 2017, 199-224쪽.

권혁재, "독일의 단체소송제도", 민사법의 이론과 실무 제14권 제1호, 민사법의 이론과 실무학회, 2010, 121-160쪽.

김미리(역)/박세진(역)/권헌영(역), "사물인터넷: 규제의 새로운 패러다임", 경제규제와 법 제9권 제1호, 서울대학교 공익산업법센터, 2016, 189-214쪽.

김영진, "사물인터넷에 관한 공법상 쟁점과 입법정책소고", 경제법연구 제15권 제3호, 한국경제법학회, 2016, 305-319쪽.

김진영, “사물인터넷 활성화를 위한 입법과제 및 개선방안 연구”, 과학기술법연구 제24권 제1호, 한남대학교 과학기술연구원, 2018, 43-92쪽.

김현철, “자기결정권에 대한 법철학적 고찰”, 법학논집 제19권 제4호, 이화여자대학교 법학연구소, 2015, 357-372쪽.

박상돈, “종합적 사이버보안 법률 제정에 관한 시론적 연구”, 입법과 정책 제6권 제2호, 국회입법조사처, 2014, 5-36쪽.

박철민/조정식, “국외사이버 위협정보공유의 체계조사”, INTERNET & SECURITY FOCUS, 한국인터넷진흥원, 2014, 49-55쪽.

방승주, “헌법 제10조”, 헌법 주석서 Ⅰ, 한국헌법학회, 법제처, 2007, 250쪽.

서희석, “우리나라 집단분쟁조정제도의 현황과 과제”, 비교사법 제23권 제4호, 한국비교사법학회, 2016, 1439-1476쪽.

송동수/성기만, “개인정보유출에 대한 구제방안으로서 징벌적 손해배상”, 토지공법연구 제67집, 한국토지공법학회, 2014, 175-200쪽.

심우민, “사물인터넷 개인정보호보의 입법정책”, 헌법학연구 제21권 제2호, 한국헌법학회, 2015, 1-36쪽.

오승한, “빅데이터 산업의 활성화와 개인정보 보호를 위한 법제도 개선의 연구”, 아주법학 제11권 제4호, 아주대학교 법학연구소, 2018, 369-412쪽.

이기호/김계현, “대만 개인정보보호법의 주요 내용과 함의”, 東北亞法硏究 제11권 제2호, 전북대학교 동북아법연구소, 2007, 51-77쪽.

이부하, “비례성원칙과 과소보호금지원칙”, 헌법학연구 제13권 제2호, 한국헌법학회, 2007, 275-303쪽.

이순환/박종수, “개인정보 비식별조치 가이드라인의 법적 문제와 개인정보보호법제 개선방향”, 공법연구 제45권 제2호, 한국공법학회, 2016, 257-287쪽.

이애리/김범수/장재영, “사물인터넷(IoT)환경에서의 개인정보 위험분석 프레임워크”, 한국IT서비스학회지 제15권 제4호, 한국IT서비스학회, 2016, 41-62쪽.

이영준, “민법의 지도원리로서 사적 자치- 망법개정안에 언급하여”, 법조 통권 제527조, 법조협회, 2000, 5-47쪽.

이원우, “개인정보 보호를 위한 공법적 규제와 손해배상책임”, 행정법연구 제30호, 행정법이론실무학회, 2011, 237-275쪽.

이제희, “4차산업혁명시대, 개인정보자기결정권 보장을 위한 법적 논의”, 토지공법연구

제80집, 한국토지공법학회, 2017, 143-165쪽.

이종구, “전보배상과 징벌적 손해배상 및 3배 배상제도에 관한 연구”, 경영법률 제26권 제1호, 한국경영법률학회, 2015, 447-486쪽.

이준복, “사물인터넷시대에서 정보인권 보장을 위한 법적 고찰”, 홍익법학 제16권 제3호, 홍익대학교 법학연구소, 2015, 85-114쪽.

이창범, “개인정보보호법제 관점에서 본 빅데이터 활용과 보호 방안”, 법학논총 제37권 제1호, 단국대학교 법학연구소, 2013, 509-559쪽.

장철하, “한국의 개인정보보호법제 현황과 개선 시사점”, 법학논집 제22권 제3호, 이화여자대학교 법학연구소, 2018, 163-199쪽.

전병서, “한국과 일본에서의 소비자단체소송제도의 도입”, 법조 제56권 제4호, 법조협회, 2007, 47-79쪽.

정원준, “사물인터넷 활성화를 위한 법제도적 개선방안 연구”, 법과 정책연구 제4권 제4호, 한국법정책학회, 2014, 1835-1867쪽.

정준현, “개인정보의 통합관리에 따른 법적 문제”, 외법논집 제36권 제3호, 한국외국어대학교 법학연구소, 2012, 152-153쪽.

_____, “사물통신시대의 국가안보 위협으로서 간첩활동과 관련 법률의 부정합성”, 미국헌법연구 제27권 제2호, 미국헌법학회, 2016, 331-366쪽.

정준현/권오민, “개인정보의 수집, 처리, 제3자제공과 가치창출에 관한 법적 문제 연구”, 홍익법학 제16권 제1호, 홍익대학교 법학연구소, 2015, 937-960쪽.

차상욱, “빅데이터(Big Data) 환경과 프라이버시 보호”, IT와 법연구 제8권, 경북대학교 IT와 법 연구소, 2014, 193-259쪽.

최희경, “미국 헌법상 정보 프라이버시권”, 법학논집 제19권 제2호, 이화여자대학교법학연구소, 2014, 29-58쪽.

허성욱, “한국에서 빅데이터를 둘러싼 법적 쟁점과 제도적 과제”, 경제규제와 법 제7권 제2호, 서울대학교 공익산업센터, 2014, 16-17쪽.

Hans-Heinrich(김태오 역), “The Internet of Things : Remarks from the German Perspective” 경제규제와 법 제9권 제1호, 서울대학교 공익산업법센터, 2016, 140-159쪽.

John Gantz / David Reinsel, “Extracting Value from Chaos”, *IDC IVIEW*, IDC, 2011, p.6 of 12.

Juha K. Laurila / Daniel Gatica-Perez / Imad Aad / Jan Blom / Olivier Bornet / Trinh Minh

Tri Do / Olivier Dousse / Julien Eberle, and Markus Miettinen, *From big smartphone data to worldwide research: The mobile data challenge* Volume 9 Issue 6, Pervasive Mob, Comput., 2013, pp.751-772.

Juliane Kokott and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Volume 3, Issue 4, Oxford Academic, 2013, pp.222-228.

Mark Weiser, *The computer for the 21st century*, Scientific American 제265권 제3호, Munn & Company, 1991, pp.94-104.

菅原貴与志, "改正個人情報保護法の問題", 慶應法學 第34號, 慶應法学 法務研究科, 2016, pp.27-48.

3. 기타 (인터넷자료 or 전자문헌)

미래창조과학부・한국인터넷진흥원, "사이버 위협정보 분석・공유시스템 리플렛.pdf" <https://www.boho.or.kr/data/noticeView.do?bulletin_writing_sequence=25824>, 검색일: 2018.1.14.

박성진, "[미국] 2017년 사물인터넷 사이버보안 개선 법안이 제출되다", <https://www.copyright.or.kr/mobile/gov/nuri/download.do?brdctsno=41501&brdctsfileno=12728>, 검색일: 2018.7.12.

정혜운, "소비자 권익을 지키기 위한 법적 제도들", 한국소비자보호원 보도자료, 2008.

技術検討ワーキンググループ, 報告書<http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf>, 1/37쪽 참조.

徳田 英幸, "IoT時代のセキュリティ課題", *SEC Journal Vo.12 No.13*, IPA, 2016, 1頁.

鈴木正朝, プライバシ-の權利と個人情報保護法, 平成 24年11月, <https://www.cas.go.jp/jp/seisaku/mynumber/symposium/iwate/siryou5.pdf>, 검색일: 2018.7.15.

翁清坤, "대만의 개인식별 번호법제 현황과 문제점", 한국법제연구원 학술대회 자료집, 한국법제연구원.

日本経済新聞 電子版, "デジタルファースト法案次期国会に提出へ 行政手続き、電子申請に統一", 검색일: 2018.6.7.

"IEEE Internet of Things Initiative is an IEEE(Institute od Electrical and Electronic Engineers)

platform for the global community working on the IoT", <http://iot.ieee.org/>.

"Introduction to STIX", <https://oasis-open.github.io/cti-documentation/stix/intro>, 검색일: 2018.5.17.

"JSON", <https//ko.wikipedia.org/wiki/JSON"https://ko.wikipedia.org/wiki/JSON>.

"Need for IT sharing standard", <https://www.anomali.com/platform/what-are-stix-taxii>.

"The Fair Information Principles", <https://www.privacyfirst.nl/acties-3/item/154-the-fair-information-principles-canada.html>, 검색일: 2018.7.19.

"The internet of things: how your TV, car and toys could spy on you", <https://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys>.

"US intelligence chief:we might use the internet of things to spy on you", <https://www.theguardian.com/technology/2016/feb/09/>, 검색일: 2018.3.21.

<http//icdppc.org/wp-content/uploads/2017/04/Breach-notification-statics-survey-repoer-18-April-2017.pdf"http://icdppc.org/wp-content/uploads/2017/04/Breach-notification-statics-survey-repoer-18-April-2017.pdf>.

<http://ssrn.com/abstract=2076397>, 검색일: 2018.2.5.

<http://www.amazon.com/Encyclopedia-Conflict-Resolution-Heidi-Burgess/dp/0874368391>, 검색일: 2018.5.15.

<http://www.amazon.com/Encyclopedia-Conflict-Resolution-Heidi-Burgess/dp/0874368391>, 검색일: 2018.5.15.

<http://www.etnews. com/ 20150531000071>, 검색일: 2016.6.1.

<http://www.hani.co.kr/arti/science/future/847763.html>, 검색일: 2018.6.25.

<http://www.wired.com/insights/2015/02/say-goodbye-to-privacy/>, 검색일: 2018.5.7.

<https://en.wikipedia.org/wiki/Privacy_by_design>, 검색일: 2018.6.22.

<https://www.eugdpr.org/gdpr-faqs.html>, 검색일: 2018.5.17.

<https://www.paloaltonetworks.com>, 검색일: 2018.7.21.

Article 29 Data Protection Working Party, Opinion 8/2014 on 'Recent Developments on the Internet of Things'(14/EN WP 223) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf>, 검색일: 2018.7.12.

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos,

Mario Costeja González, 검색일: 2014.5.13.

EY, “Cybersecurity and the Internet of Things” <http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things.pdf>, 검색일: 2018.6.21.

Farzad Kamrani, Mikael Wedlin, Ioana Rodhe. “Internet of Things: Security and Privacy Issues”, FOI-R - 4362 - SE (https://www.foi.se/report-search/pdf?fileName), p.3 of 43.

GPEN Privacy Sweep, Internet of Things: Participating Authorities’ Press Release, <https://www.privacyenforcement.net/node/717>, 검색일: 2018.3.12.

Jeremy J. Waldron / Eirik Albrechtsen, “Security vs safety”, Nebraska Law Review, Volume 85, Issue 2, 2006, <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1118&context=nlr>, 검색일: 2018.7.5.

Scott McNealy, Polly Sprenger, “Sun on Privacy: ‘Get Over it’, WIRED”, <http://archive.wired.com/politics/law/news/1990/01/17538>, 검색일: 2017.3.11.

[Abstract]

Legal Issues of the Personal Data Protection against Internet of Things

Jeong, Jun-Hyeon*

'Internet of Things(IoT) society' is not a physically active society but a 'Cyber-Physical System' society in which the demands of individuals and society are met in real time by physical systems controlled by non-physical digital data. In these societies, the fulfillment of individual needs without the provision of personal data or the promotion of public welfare can not be assumed. In this regard, the demands of the public and private parties to realize the infinite value inherent in a myriad of personal data generated in real time in the IOT environment and the data subject to protect personal data are in conflict with one another.

In this conflict phase, the fact that the self-determination authority of the data subject has become virtually defective due to the data gap and the methods and means of seizing personal data are considered to be difficult to prove, even if personal data infringement occurs do. Based on these considerations, the following suggestions are made.

First, a reasonable level of anonymization of personal data should be accepted as a social constraint that members of IoT society should recognize for the benefit of the community. Secondly, it is necessary to solve the digital divide existing between data processors who want to create new value by using personal data and simple users who want to enjoy the benefits, and to improve the responsibility of data processors by using legal system such as 'PbD'.

Third, national effort to institutionalize 'STIX'(Structured Threat Information eXpression) should be strengthened so that illegal access to personal data and social community monitoring of misuse and abuse of personal data can be realized in real time. Finally, I hope that the legislative policy toward 'Digital First' in each country will become a competition stage of

* Professor, Law College of DanKook University

wisdom for ‘Positive-Sum’ at global community level.

[Key Words] Internet of Things, Digital Divide, Personal data, Positive-sum, Privacy by Design, STIX’(Structured Threat Information eXpression)