지식재산연구 제15권 제4호(2020. 12)
©한국지식재산연구원
The Journal of Intellectual Property
Vol.15 No.4 December 2020
https://doi.org/10.34122/jip.2020.15.4.191
Print ISSN 1975-5945 | Online ISSN 2733-8487

투고일자: 2020년 8월 3일
심사일자: 2020년 8월 20일(심사위원 1), 2020년 8월 12일(심사위원 2), 2020년 8월 20일(심사위원 3)
게재확정일자: 2020년 12월 4일

한국에서 사물인터넷과 관련한 빅데이터 보호제도의 현재와 그 방향

— 사물인터넷의 특성과 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 보호의 충분성에 중점을 두고

설민수*

Ⅰ. 서 론
Ⅱ. 사물인터넷 관련 빅데이터의 특성과 그 보호에 관한 쟁점
1. 사물인터넷의 기술적 기반과 그 빅데이터의 특징
2. 사물인터넷 관련 빅데이터 보호에 관한 쟁점
Ⅲ. 사물인터넷 관련 빅데이터에 대한 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 기존 보호와 그 구체적 적용
1. 부정경쟁방지 및 영업비밀보호에 관한 법률의 비공지 정보에 대한 보호 범위와 그 내용
2. 사물인터넷 관련 빅데이터에 대한 적용
Ⅳ. 한국에서 사물인터넷 관련 빅데이터 보호제도에 대한 대안의 필요성 여부
1. 사물인터넷 관련 빅데이터에 대한 현재 보호제도의 평가
2. 대안의 필요성에 대한 주장과 그 문제점
3. 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 보호제도의 장점
Ⅴ. 글을 마치며

* 서울남부지방법원 부장판사.

초 록

빅데이터의 보호는 사물인터넷이 활성화와 함께 일반인의 관심을 모으고 있는 영역이다. 자연스럽게 기존 보호제도의 문제점을 지적하면서 새로운 지식재산권에 의한 보호주장들이 분출되고 있다.

하지만 사물인터넷 관련 빅데이터는 다른 빅데이터와는 사물인터넷 기술의 특성에 따라 보안조치에 의한 비공지성, 추적가능성에 바탕을 둔 사용자의 개인정보와의 불가분성 등 여러 가지 다른 특징을 가지고 있고, 이러한 특성을 무시한 새로운 지식재산권에 의한 보호는 그 소유권 귀속과 같이 해결하기 어려운 여러 가지 법률적 쟁점을 야기할 뿐이다. 반면, 비공지성을 갖춘 정보를 보호하는 한국의 부정경쟁방지 및 영업비밀보호에 관한 법률과 그 보호범위에 관한 법원의 해석은 다른 국가와 다르게 영업비밀, 영업상 주요자산, 제2조 제1호 ㈐목의 부정경쟁행위라는 틀을 통해 이를 다양하게 분류해 보호하고 있다. 또한 그 정보의 독점력이 가진 가치에 따라 다양한 범위의 형사적 제재 및 민사적 보호를 폭넓게 제공하고 있다. 이에 따라 사물인터넷 관련 빅데이터 중 그 가치를 달리하는 사전처리를 거친 데이터세트, 비식별화 조치를 거친 데이터세트, 원시데이터 상태의 빅데이터에 관해서도 충분한 보호를 제공하며 사물인터넷 관련 빅데이터 거래에 있어 중요한 장애물인 개인정보 보호에 관련하여 재식별을 막아 빅데이터 거래 활성화를 가능하게 하는 장점도 가지고 있다.

주제어

사물인터넷, 빅데이터, 영업비밀, 영업상 주요자산, 개인정보 보호, 비공지성

Ⅰ. 서 론

사물인터넷(Internet of Things, 이하 IoT)은 각 기기에 설치된 센서(censor)들이 포착한 사용자와 주변 환경에 대한 정보와 기기의 작동과 기능에 대한 정보를 인터넷을 통해 저장장치로 전송·집적한 데이터를 활용해 상황에 맞추어 해당 기기 또는 인터넷에 연결된 다른 기기의 생산성이나 작동, 서비스를 조절하는 방식으로 작동하므로 다량의 데이터 발생과 보관, 그 활용은 IoT의 핵심이다.[1] 미국국립기술표준원이 "전통적인 관리도구 시스템의 저장공간과 관리능력을 벗어나는 센서, 인터넷 도구, 클릭, 이메일, 비디오 등 현재 · 미래의 모든 디지털 원천으로부터 나온 복잡하고 다양하며 분산된 데이터집합(data set, 이하 데이터세트)"으로 정의한 빅데이터(Big Data)에 대한 관심이 폭발한 것도 IoT의 발전이 본격화된 2010년대의 일이다.[2]

최근 데이터가 가진 내용이 아니라 그 수집되는 양(Volume), 데이터의 갱신 속도(Velocity), 여러 원천으로부터 나오는 다양성(Variety)으로 상징되는 방대함과 변동성을 특징으로 한 빅데이터의 중요성이 커지면서 빅데이터를 새로운 석유(new oil)로 비유한 관련산업 종사자들의 언급이 언론을 통해 전문가를 넘어 대중에게 널리 전파되고 있다.[3] 이에 따라 기존 보호제도의 한계를 지적하며 빅데이터를 현행의 지식재산권을 확장하거나 새로운 입법을 통해 보호하려는 논의들이 한국에서도 이루어지고 있으며 이러한 논의들은 IoT 관련 빅데이터를 다른 빅데이터와 구분하지 않는다.[4] 이러한 논의들에

---

1) Mauricio Paez, & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. Ky. L. Rev. 29(2016), p. 31.

2) Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 Pepp. L. Rev. 773(2015), p. 795.

3) *Id.* pp. 794-5; Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 Tenn. L. Rev. 863(2019), pp.866-8.

4) 박준석, "빅데이터 등 새로운 데이터에 대한 지적재산권법 차원의 보호가능성", 『산업재산권』, 제58호(2019), 78-83면; 차상육, "빅데이터의 지적재산법상 보호", 『법조』, 제728호(2018), 74-7면.

영향을 미치고 있는 것은 '데이터 주도 경제(data-driven economy)'를 표방하며 2014년부터 빅데이터 보호에 관한 논의를 진행하고 있는 유럽연합의 움직임과 2018년에 '한정제공데이터'라는 용어로 빅데이터를 보호하는 입법을 한 일본의 동향이다.[5)]

하지만 IoT 관련 빅데이터는 IoT의 기술적 특성에 따라 다른 빅데이터와 달리 외부로부터의 접근이 차단되는 비공지성을 가진다. 자연스럽게 현재 한국에서 IoT 관련 빅데이터는 영업비밀을 비롯해 비공지 정보를 보호하는 「부정경쟁방지 및 영업비밀보호」에 관한 법률(이하 '부정경쟁방지법')에 따른 보호를 받고 있는데 그 보호범위는 다른 그 어떤 국가보다 폭이 넓다.

이 글은 기존 논의들이 놓치고 있는 부분인 IoT 관련 빅데이터의 기술적 특성과 그에 따른 보호의 쟁점, 현재 IoT 관련 빅데이터를 보호하고 있는 부정경쟁방지법에 기초한 한국 제도의 보호범위와 그 충분성, 대안에 관한 논의들의 문제점을 통해 향후 한국이 IoT 관련 빅데이터 보호에 관해 취할 방향에 관해 살펴보고자 한다.

II. 사물인터넷 관련 빅데이터의 특성과 그 보호에 관한 쟁점

1. 사물인터넷의 기술적 기반과 그 빅데이터의 특징

(1) 사물인터넷의 기술적 기반

IoT의 기술적 뿌리는 1980년대 개발되어 현재 커피주문 시 대기자 확인 등 다양한 실생활 및 산업현장에서 쓰이는 무선인식기술인 RFID(Radio-Frequency Identification)나 그에 기초한 근거리 통신기술인 NFC 등 근거리 기기 간 통신기술이다.[6)] 이러한 근거리 기기 간 통신 기술이 2010년 대 스마

5) 박준석, 앞의 글, 88-92, 114-8면; 차상육, 앞의 글, 78-80면.

6) Katherine Britton, *Handling Privacy and Security in the Internet of Things*, 19 No. 10 J. Internet L. 3(2016), p.3.

트폰이나 태블릿 PC 등 이동전자기기의 범용화에 자극받은 시각이나 온도, 거리, 자기장, 방사선, 습도, 농도 등 다양한 형태의 환경 정보를 모으는 센서(censor)의 발전과 융합되면서 IoT의 기반이 마련된 것이다.[7] 여기에 인공위성으로부터의 거리를 삼변측량하는 GPS 기술의 발전과 2^{128}개의 인터넷 주소로 확장할 수 있는 IPv6의 2011년 채택은 개별기기의 정확한 위치추적 및 독자 인터넷 주소 부여를 통해 IoT가 가진 가치의 핵심인 사용자의 추적가능성(traceability)을 크게 향상시켰다.[8]

위와 같은 기반 환경과 함께 IoT의 발전에는 다음 두 가지 기술이 작용하고 있다. 우선 IoT가 작동하려면 실시간으로 각 기기에서 발생하는 대용량의 데이터를 저장할 공간과 그 기기와 연결된 다양한 관계자가 데이터에 접근할 수 있고 관련 데이터를 주고받을 수 있도록 관리하는 탄력적인 컴퓨팅 자원의 제공이 필수적이다. 통신망에서 집약적인 처리기능을 제공하는 컴퓨터인 서버(Server)를 활용해 서비스를 제공하는 사업자들이 개별 서버에 대한 작업요구량이 상이할 경우 이에 대응하기 위해 다수의 서버들을 하나의 가상망(virtual network)으로 묶어 유휴 서버에서 자원을 끌어다 쓰거나 다른 서버의 작업을 분산처리해 안정적인 서비스를 제공하는 기술에서 발전해 저장공간과 컴퓨팅 자원을 탄력적으로 제공하는 클라우드컴퓨팅(Cloud Computing)은 IoT에 가장 적합한 인프라로 2010년대 클라우드컴퓨팅의 보급은 IoT의 발전을 촉진시켰다.[9]

다음으로 IoT 기기를 기존의 전자기기와 구별하게 만드는 최대 특징은 마치 개별기기가 생각을 가진 것처럼(smart) 통신을 통해 스스로 작동을 조절하고 사용자와 상호작용을 하는 부분이다.[10] 이를 가능하게 하는 것은 2010년대 들어서 급속히 발전하고 있는 개별 IoT 기기에서 발생하는 데이터가 빅

---

7) Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 Berkeley Tech. L.J. 997(2016), pp.1003-4.

8) *Id.* p.1005.

9) *Id.* p.1006-7; 설민수, "한국 소프트웨어산업에서 형사처벌의 활성화를 통한 영업비밀의 지위 강화, 그 영향과 향후과제 — 미국과의 비교를 중심으로", 『사법』, 제52호(2020), 412-4면.

10) Paez & Marca, *supra,* pp.32-3.

데이터로 집적되는 클라우드 공간에서 실시간으로 분석해 각 IoT 기기의 기능과 작동을 실시간으로 조절하는 머신러닝(Machine Learning) 인공지능(Artificial Intelligence, 이하 'AI') 기술이다.[11]

(2) 사물인터넷 관련 빅데이터의 특징

IoT 관련 빅데이터도 빅데이터의 일부인 만큼 그 일반적 특징인 비경합적 성격(non-rivalrous nature)을 가진다. 그 성격의 변질 없이 복제될 수 있기 때문에 여러 사용자가 함께 사용할 수 있는 일반적 비경합성은 물론 같은 분석 목표로 사용하더라도 그 사용기법에 따라 수집하는 빅데이터의 원천이 서로 달라질 수 있어 단일한 형태나 범위를 가진 데이터세트가 존재할 수 없는 보다 광범위한 비경합성을 가진다.[12]

하지만 IoT 관련 빅데이터는 IoT의 기술적 특성에 의해 다른 빅데이터와는 다른 특징을 가진다. IoT 관련 빅데이터의 가장 큰 특징은 일종의 분절화(fragmentation) 현상이다. 현실의 IoT 환경은 하나의 거대한 시스템 안에 통합되어 연결된 유사한 수준의 다수의 기기들이 아닌 초기 기술에 가까운 RFID에 기반해 작동하는 커피기계부터 독자적 인터넷 주소를 가지고 5G로 상징되는 V2X 통신기술을 사용하며 고도의 머신러닝 AI로 작동되는 자율주행자동차(automated vehicle) 등 각기 다른 수준의 IoT 기기들이 상호작용을 하는 세계이다.[13] 개별 IoT 기기의 수준 차이만이 아니라 이러한 IoT 시장에서 플랫폼(platform)을 형성하려는 회사들도 새로운 기술을 통해 시장점유율을 높이려고 할 뿐 다른 IoT 회사들과의 데이터 교환이나 상호호환성(interoperability)을 통해 하나의 통일된 시장을 형성하려고 하지 않는다.[14] 자연스럽게 IoT 관련 빅데이터를 모았더라도 이를 실제로 사용하기 위해 서로 다른 구조로 형성된 데이터세트들을 하나의 일관성이 있는 데이터세트로

11) 설민수, 앞의 글, 414면.

12) Scholz, *supra*, p.875; Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 Ariz. L. Reb. 339(2017), p.346.

13) Paez & Marca, *supra,* p.34.

14) *Id.* pp.35-36; Poudel, *supra,* pp.1100-11.

사용하는 데는 상당한 노력과 시간이 필요하다.[15]

RFID, NFC 등 근거리 무선통신망을 비롯한 다양한 계층의 통신망으로 연결되면서도 분절화된 IoT가 직면하는 가장 큰 문제 중 하나는 보안(Security)이다. 일단 다양한 계층의 통신망으로 연결되는데다가 초기의 RFID를 사용한 단순한 기기부터 고도의 자율주행자동차까지 다양한 IoT 기기가 다양한 소프트웨어를 통해 연결되기 때문에 통일적인 보안체계를 갖추기가 아주 어려운 반면 전체 시스템으로의 연결점은 그만큼 많아지면서 외부에서의 침입 방지는 IoT 발전 초기부터 현재까지 극복이 어려운 중요한 난제이다.[16] 이러한 보안의 문제는 IoT 관련 빅데이터에 접근제한을 통한 비공지성이라는 특징을 그 탄생 시부터 갖게 만들고 있다.

또한 자연현상이나 사회현상과 같이 특정인에게 귀속시킬 수 없는 다른 데이터와 달리 IoT 관련 데이터는 사람에 의해 생성되거나 그 사람 자체 또는 관련 행위에 의해 생성되며 그 정보의 원천인 특정인이 추적가능한 데이터로서 이를 모은 IoT 관련 빅데이터의 가치 핵심 역시 특정인에 대한 추적가능성에서 나온다.[17] 가령, 건강관련 IoT 기기에서 사용자의 움직임이나 음성, 심박동, 혈압, 심전도 등의 빅데이터를 분석하는 이유는 이를 통해 향후 비상상황이나 특정질병의 발생을 예측하려는 것인데 위 빅데이터와 연관된 IoT 사용자에 대한 건강 상황 추적과 이를 반영한 빅데이터 연동이 불가능하다면 위 빅데이터는 그 가치를 거의 상실하게 된다.[18] 따라서 IoT 관련 빅데이터의 가치는 사용자 개인과 분리해서는 존재하기 어렵다.

마지막으로 IoT 관련 빅데이터는 다양한 단계에서 수집될 수 있고, 수집자가 아니더라도 그 전송 및 활용에 다양한 이해관계자가 발생한다. 우선 IoT의 작동을 위해서는 사용자의 행동이나 기기에 관련한 데이터를 모아 근

15) Liane Colonna, *Privacy, Risk, Anonymization and Data Sharing in the Internet of Health Things*, 20 U. Pitt. J. Tech. L. & Pol'y 147(2020), pp.152-3; Rubinfeld & Gal, *supra*, p.365.

16) Britton, *supra*, pp.4-5.

17) Scholz, *supra*, p.876.

18) Colonna, *supra*, p.161.

거리 통신을 통해 장거리 통신으로 연결할 관문(gateway) 역할을 하는 기기계층(device layer), 위 기기계층에서 발생하는 데이터를 클라우드 서버까지 연결하고 상호전송하는 네트워크계층(network service layer), 빅데이터를 저장하고 전송하며 최종 분석하는 소프트웨어가 위치하는 서비스계층(common service layer), IoT 사용자에게 빅데이터를 통해 IoT와 관련한 서비스를 제공하는 응용소프트웨어계층(application layer)과 같이 적어도 4개 계층이 상호작용을 이뤄야 한다.[19] 그 과정에서 각 IoT 기기의 수준과 각 계층 관련자의 능력과 자원에 따라 다양한 이해관계자가 발생한다. 가령, 스마트폰의 OS 운영자인 Google의 경우와 같이 스마트폰에서 발생하는 모든 데이터를 자신이 운영하는 클라우드 서버에 모아 분석하고 자신이 제공하는 Youtube 등 소프트웨어에 활용하는 경우와 같이 네트워크 계층을 제외한 기기단계부터 응용소프트웨어 단계까지 빅데이터의 수집, 전송, 활용 전체를 통제하는 경우도 있을 수 있지만, Amazon의 자동주문서비스(Dash Replenishment Service)처럼 각 가정의 가전제품들이 Amazon의 Echo 스피커 등을 통해 위 자동주문서비스의 관련기기로 등록되어 서비스를 제공하는 경우 그 가전제품들이 각각의 수준에 따라 별도로 빅데이터를 수집해 이를 활용하고 동시에 Amazon이 수집하는 빅데이터 중 일부를 구성할 수도 있다. 직접적으로 IoT 기기에서 발생하는 빅데이터 수집과정에 참여하지 않는 경우라도 이해관계를 가질 수 있는데 가령 자율주행자동차가 발생시키는 데이터에 대해서는 자율주행자동차의 운행에 영향을 받는 다른 교통운행자, 자동차 부품 제조자 및 관련 서비스 제공자, 보험회사, 지방자치단체, 경찰 등 다양한 이해관계자가 존재할 수 있다.

2. 사물인터넷 관련 빅데이터 보호에 관한 쟁점

(1) 사물인터넷 관련 보안 문제와 그 영향

앞서 살펴본 대로 IoT에서 보안은 가장 중요한 문제로 현재까지는 가정

19) Poudel, *supra,* pp.1002-3.

에 설치된 웹카메라의 허술한 보안을 틈타 제3자가 침입해 웹카메라에 찍힌 사용자의 은밀한 사생활에 관한 동영상을 공중에 노출시키는 경우와 같이 개인정보의 보호와 관련한 문제가 주로 제기되지만, IoT 기기가 발전할수록 해킹을 통해 침입해 건강관리에 사용되는 IoT 기기의 작동을 변경시켜 투약량을 조절하거나 자율주행자동차의 시스템에 접속해 원격작동 하는 것과 같이 개인의 신체, 생명에 직접 연관을 가진 IoT에 대한 조작가능성을 보여 주는 사례들이나 대중교통, 에너지 분야 공공기반시설에 대한 침투나 그 운행 방해의 문제가 제기되고 있다.[20] 더욱이 대부분의 IoT 기기는 저전력을 사용하는 소규모 기기 형태로 제조되어 암호화 같은 보안조치를 실행하기 힘들고 대부분의 제조사가 소비재 제조회사에서 출발해 소프트웨어 업데이트나 보안에 관한 경험이 부족하며 그 작동 과정에 관계된 앞서 본 4단계의 각 계층에 관련된 이해관계인들의 입장도 서로 대립되고 있어 보안에 관해 통일적 조치를 취하기도 쉽지 않다.[21]

이에 대해 IoT 기술 발전에 큰 영향을 미치는 미국과 유럽연합의 규제기관들은 아직 그 기술적 발전의 초기 단계에 불과한 IoT의 보안문제에 대해 직접 규제는 꺼리면서도 개인정보 보호와 관련한 형태의 간접적인 규제를 부과하고 있다.

유럽연합은 IoT 기기가 전통적인 전자기기와 다른 환경에서 발전하고 있어 그 기기의 효율성과 보안 사이의 균형을 찾아야 한다면서 초기 발전단계인 IoT의 사정을 고려해 특정 방향을 정해 보안을 규제하기보다는 IoT 기기가 창출하고 수집하는 개인정보 보호 체계의 일부로 다루고 있다.[22] 2018. 5. 25.부터 적용되면서 한국 내에서도 관심을 불러일으키고 있는 유럽연합의 「일반개인정보보호규정(General Data Protection Regulation, 이하 GDPR)」'은 IoT 기기 제조자를 정보처리자(controller)로 분류하고 제조자와 함께 정

20) Paez & Marca, *supra,* pp.46-9.

21) Poudel, *supra,* p.1012.

22) Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices*, 52 Suffolk U. L. Rev. 227(2019), p.262.

보처리의 목적과 방법을 결정하는 자를 수탁자(processor)가 아닌 공동 정보처리자의 지위에 놓으면서 책임을 부담하도록 하는 동시에 정보처리자와 수탁자로 하여금 정보처리 과정에서 비밀유지를 포함해 위험에 상응한 적절한 보안조치의 채택을 의무화하고 있다.[23] 개인정보 침해의 위험에 대해 비구속적인 지침을 통해 시장의 발전방향을 유도하는 입장을 취하고 있는 미국에서도 연방공정거래위원회의 지침을 통해 IoT 기기의 개발단계부터 보안과 관련한 기술적 조치를 취하거나 데이터의 전송, 저장과정에서 암호화나 데이터 접근에 대한 제한 등의 보안 강화조치를 IoT 기기 제작자나 그 빅데이터 수집자에게 권고하고 있다.[24]

GDPR과 같이 보안조치를 그 개발과 정보처리의 구성단계마다 일정하게 요구하는 구속적인 법령이나 각국 규제기관의 개인정보 보호를 위한 정책방향, 그리고 IoT 기기 개발자들 사이의 소비자의 불안을 잠재우려는 경쟁으로 인해 IoT에서 발생하는 데이터에 대한 외부 접근이 제한되면서 IoT 관련 빅데이터는 어떠한 형태든 비공지성을 가질 수밖에 없다. 이 경우 기존 보호제도 중에서도 보안을 위한 통제에서 발생하는 비공지성에 기초한 독점력에 대하여 보호를 해 주는 제도가 자연스럽게 IoT 관련 보호제도로서 적합한 성격을 가질 수밖에 없다. 또한 기존제도에 대한 대안을 제시한다고 해도 그 대안이 IoT 관련 빅데이터의 비공지성을 무시하고 논의된다면 적절한 보호제도로서 기능하기 어렵다.

(2) 사물인터넷 관련 빅데이터의 존재 형태와 그 보호

IoT 관련 빅데이터는 하나의 형태로 존재하지 않는다. 현재 현실에서 가장 각광받는 IoT인 Amazon의 Alexa 등과 같이 사용자의 목소리를 인식하여 작동하며 TV, 전등, 스마트폰과 연동되는 장치인 스마트 스피커(Smart Speaker)가 수집하는 빅데이터인 사용자의 집안에서 발생하는 각종 음성(Voice)을 예로 들어 보기로 하자.

---

23) *Id.* pp. 261, 264.

24) Paez & Marca, *supra,* p.52.

스마트 스피커는 그 제조자가 정한 작동명령어(awake word)를 통해 그 작동을 시작하고 사용자의 음성을 녹음해 이를 그 저장장치에 저장하는 동시에 서버로 보내 Amazon 등 스마트 스피커 제조·판매사가 사용자들의 음성을 클라우드 서버에 저장한 뒤 이러한 음성을 일종의 빅데이터로 활용해 스마트 스피커를 비롯한 머신러닝 AI의 음성인식과 언어에 대한 이해능력을 향상시키는 데 활용하는 형태로 운영된다.[25] 물론 스마트 스피커의 제조·판매사가 모은 음성파일 그 자체인 원시데이터(raw data)는 그 크기가 클수록 그 자체로 일정한 가치를 가질 수 있다. 머신러닝 AI가 특정 패턴을 찾아내기 위해 적당한 빅데이터의 규모에 관한 답은 없지만 예측과 관련해 부분적 데이터는 아주 잘 반영할지 몰라도 전체 데이터 집단을 잘 반영하지 못하는 머신러닝 AI의 예측력의 중요한계 중 하나인 과적합 문제(overfitting)를 피하기 위해서도 상당한 규모의 데이터가 모였다는 것은 그 자체로 전체 데이터 집단을 대표할 수 있는 가치를 가지기 때문이다.[26]

하지만 스마트 스피커가 모은 음성파일은 인간의 목소리만이 아니고 다양한 형태로 발생하는 모든 소리를 포함한다. 통상 스마트 스피커는 거실, 침실, 욕실 등 다양한 장소에 위치하며 사람만이 아닌 전자제품, 동물 등 다양한 원천으로부터 나오는 소리를 모두 녹음하게 되는데 이러한 데이터를 인간의 언어 사용에 관한 예측능력을 향상시키는 데 사용하기 위해서는 무엇보다 데이터를 분류하고 정리해 머신러닝 AI의 훈련을 준비하는 일종의 사전처리(pre-processing)가 필수적이다. 이러한 사전처리는 오류값 등을 제거하는 클린징(cleansing), 머신러닝 AI가 입력받을 수 있도록 데이터를 바꾸는 변환(transformation), 모델의 예측력을 저해하는 독립 매개변수의 상관관계에 영향을 미치는 변수 등을 제거하는 필터링(filtering) 등 데이터를 정제하는(cleaning) 작업을 말하며 개발자가 그 학습목표를 지정하는 지도학습모델

25) Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 Cath. U. J. L. & Tech. 187(2018), pp. 191-2.

26) David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. Davis L. Rev. 653(2017), pp. 678-9, 684.

(supervised learning)에서는 목표에 따라 분류하는(labeling) 과정까지를 포함하므로 머신러닝 AI의 개발과정에서 가장 노력이 많이 들 수밖에 없으며, 사전처리를 거쳐 만들어진 데이터세트는 사실상 머신러닝 AI의 예측력을 좌우하게 된다.[27] 더욱이 이러한 사전처리를 거친 데이터세트는 빅데이터를 통해 그 머신러닝 AI 개발자가 해결하고자 하는 문제나 관련 방향까지를 담게 되므로 원시데이터와는 전혀 다른 가치를 가지게 된다.

여기서 빅데이터의 보호제도의 보호대상이 IoT 제조자 등이 수집한 원시데이터인가 아니면 최종적으로 사전처리를 거친 데이터세트인가와 함께 기존 보호제도는 위와 같은 사전처리나 기타 공정을 거친 다양한 형태의 빅데이터를 그 중요성에 따라 충분히 보호하고 있는지의 문제가 제기된다.

(3) 사물인터넷 관련 빅데이터의 소유자 문제

기존의 지식재산권에 의한 정보 보호제도는 그 정보의 소유자(ownership)가 누구인지를 일정한 기준에 의해 판단하고 그 소유자에게 어느 정도 배타적이고 독점적인 형태의 권리를 인정하는 형태를 취한다. 가령, 한국에서 빅데이터 이전 그와 가장 유사한 대상인 데이터를 체계적으로 배열 또는 구성한 편집물로서 그에 관해 접근하거나 검색할 수 있는 데이터베이스 보호의 경우 데이터베이스를 제작하거나 그 데이터의 갱신 · 검증 또는 보충에 인적 또는 물적으로 상당한 투자를 한 자를 데이터베이스제작자로 규정한 뒤 상당한 부분의 복제 · 배포 · 전송 등을 독점할 권리를 주는 방식을 취했다.[28]

문제는 데이터베이스의 경우 그 제작을 위해서는 데이터의 체계적 배열 또는 구성을 통한 편집이라는 별도의 행위와 이를 위한 자본투입이 필요해 이를 요건으로 해 독점권을 부여할 이해관계자가 뚜렷한 데 반해 IoT 관련 빅데이터에 관해서는 소유자나 그에 준해서 볼 독점권을 부여할 이해관계자가 뚜렷하지 않다는 점이다.

---

27) *Id.* pp. 682-3; Hyunjong Ryan Jin, *Think Big! The Need for Patent Rights in the Era of Big Data and Machine Learning*, 7 NYU J. Intell. Prop. & Ent. L. 78(2018), p. 90.

28) 저작권법 제2조 제20호, 제21호, 제93조.

우선 IoT 관련 빅데이터의 가치 대부분이 그 사용자인 개인에 대한 추적 가능성에서 나오므로 IoT 관련 빅데이터의 핵심은 그 사용자인 개인을 알아볼 수 있는 개인정보라고 볼 수 있다.[29] 개인정보가 포함된 IoT 관련 빅데이터의 경우 그 기기를 사용하는 개인의 사용을 통해 만들어지고 그 IoT 제작자 또는 Google, Amazon과 같이 관련 서비스를 제공하는 서비스제공자의 클라우드 서버에 축적되게 되므로 IoT 관련 빅데이터의 기본적인 창출자는 각 사용자이지만 수집자는 IoT 제작자 또는 서비스제공자로 데이터 창출자와 수집자가 별도로 존재한다.[30] 더욱이 IoT 사용자는 그 IoT 기기를 IoT 제작자로부터 구매한 물리적 소유자의 지위를 겸하고 있어 그 IoT 기기가 데이터를 클라우드 서버만이 아니라 IoT 기기에도 동시에 저장하는 형태로 운영된다면 자신의 IoT 관련 데이터에 관해서는 독자적인 수집자의 자격도 갖추고 있어 소유자로 볼 여지도 충분하다.[31]

IoT 기기가 아닌 클라우드 서버에만 데이터가 저장되는 IoT의 경우도 클라우드 서버를 통해 데이터를 수집하는 자를 빅데이터에 대한 유일한 독점권을 부여할 가치를 가진 이해관계자로 보기는 쉽지 않다. 만약 그 빅데이터 수집자가 IoT 사용자가 소유한 IoT 기기를 이용해 별도의 무상의 서비스를 제공하는 기업, 가령 스마트폰을 통한 무상의 차량내비게이션 서비스와 같은 형태의 서비스 제공기업의 경우라면 막대한 비용을 들여 별도의 서비스를 제공하고 소비자는 이를 무상으로 사용하는 대신 자신의 개인정보가 포함된 차량의 운행정보 데이터를 서비스 제공기업에 교환으로 제공하는 형태의 거래가 형성되므로 그 교환가치가 적절한지의 문제를 제외한다면 빅데이터를 수집하는 무상 서비스제공자를 데이터베이스제작자와 유사하게 볼 수도 있다.[32] 하지만 빅데이터 수집자가 IoT 기기의 판매자나 그와 동일시 할

29) 개인정보보호법 제2조 제1호.

30) Lars Smith, *Rfid and Other Embedded Technologies: Who Owns the Data?*, 22 Santa Clara Computer & High Tech. L.J. 695(2006), p.755.

31) *Id.* pp.738-9.

32) Noam Kolt, *Return On Data: Personalizing Consumer Guidance In Data Exchanges*, 38 Yale L. & Pol'y Rev. 77(2019), pp.83-4.

수 있는 지위에 있는 기업인 경우 그 빅데이터는 IoT 기기의 판매목적에 따른 작동과정에서 자동적으로 발생해 저장되는 결과일 뿐 수집자에게 독점적 권리를 부여할 만한 가치를 가진 별도의 행위와 자본의 투여가 있었다고 일반화할 수도 없다.

더욱이 앞에서 살펴본 바와 같이 IoT 관련 빅데이터에 대하여는 IoT 기기를 운영하는 데 관여하는 적어도 4단계의 계층의 작동에 관계된 이해관계인들이 자신의 기기나 네트워크 운영과 관련해 직접적 이해관계를 가지며, 직접 운영과는 상관없는 이해관계인들도 다수 발생한다. 이러한 이해관계인 중 하나를 법률로 IoT 관련 빅데이터의 소유자로 지정하는 것은 아직 발전단계 초기에 있는 IoT에서 이해관계자들 사이의 갈등만 심화시킬 가능성이 크다.

여기에서 보호제도와 관련해 기존의 보호제도가 이러한 난제를 어떻게 해결하고 있는지, 기존의 보호제도와 다른 새로운 보호제도를 만들 때 이러한 난제를 해결할 수 있는지, 그리고 그로 인한 실익은 존재하는지가 문제된다.

Ⅲ. 사물인터넷 관련 빅데이터에 대한 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 기존 보호와 그 구체적 적용

빅데이터를 기존의 가장 유사한 정보형태인 데이터베이스와 비교할 때 체계적으로 배열 또는 구성한 편집물이라는 데이터베이스의 요건을 갖추지 못한다. 자연히 형식성을 요구하지 않고 정보를 보호하는 정보에 관한 기존 보호제도 중 창작성을 그 최소 요건으로 요구하는 저작권은 물론 데이터베이스에 관한 보호제도도 빅데이터 안의 개별 데이터나 데이터세트 중 요건을 갖춘 부분이 아닌 IoT 관련 빅데이터를 그 보호대상으로 하지 않는 것에 대하여는 대체로 이견이 없다.[33]

33) 박준석, 앞의 글, 105-109면; 차상육 앞의 글, 80-89면. 다만 사전처리를 거친 데이터세트를 데이터베이스보호제도의 보호대상으로 볼 수 있다는 입장도 있다. 이일호, "빅데

자연히 비공지성을 가진 정보인 IoT 관련 빅데이터의 보호는 비밀성을 특징으로 한 영업비밀과 그 밖의 각종 부정경쟁행위에 의한 침해에 대하여 제재를 통하여 관련정보를 보호하는 부정경쟁방지법이 담당하고 있다. 이에 대해 기존 논의들은 영업비밀을 중심으로 사전처리된 데이터세트를 제외하고 나머지는 영업비밀의 대상이 되기 어렵거나 그 침해태양이 영업비밀의 침해태양인 유출 또는 사용행위에 해당하지 않을 수 있다거나 부정경쟁방지법에 의한 보호는 일관성이 없고 영업비밀보다 보호가 약하다고 지적한다.[34]

그러나 한국의 부정경쟁방지법과 이에 관한 법원의 해석은 비공지 정보를 다른 나라와 다르게 단순히 영업비밀과 그 외의 정보로 구분하지 않고 적어도 3단계로 구분해 각각 가치에 따라 보호의 수단을 달리하고 있다.

1. 부정경쟁방지 및 영업비밀보호에 관한 법률의 비공지 정보에 대한 보호범위와 그 내용

(1) 영업비밀과 그 보호제도

부정경쟁방지법이 비공지성을 가진 정보 중 가장 강력하게 보호하는 것은 ① 실제 또는 잠재적인 독립된 경제적 가치, ② 일반에 알려져 있지 않거나 정상적 수단에 의하여 접근하기 어려운 비공지의 정보로서의 비밀성, ③ 보유자의 비밀성을 유지하기 위한 합리적 노력이 있을 때 인정되는 비밀관리성의 세 가지 요건을 갖춘 영업비밀이다.[35]

부정경쟁방지법은 절취, 기망, 협박과 같은 행위는 물론 포괄적인 부정한 수단으로 영업비밀을 보유자로부터 취득하는 행위나 사용, 특정인에게 노출하는 행위를 포함한 공개행위와 함께 계약관계 등에 따라 비밀유지의무가

이터의 법적보호문제 — 영업비밀보호법에 의한 보호가능성을 중심으로", 『법조』, 제727호(2018), 55-6면.

34) 이일호, 앞의 글, 88-89면(전자). 박준석, 앞의 글, 112-114면(후자).

35) 부정경쟁방지법은 2019. 1. 8. 개정되면서 제2조 제2호 영업비밀의 정의에서 '합리적 노력에 의해 비밀로 유지된'을 '비밀로 관리된'으로 변경하였으나 '관리'의 취지 자체에 비밀을 유지하기 위한 노력을 포함하므로 해석에 큰 변화가 있을 것으로 보기는 어렵다.

있는 자가 부정한 이익을 얻거나 보유자에게 손해를 입힐 목적으로 사용하거나 공개하는 행위까지를 모두 침해행위로 규정하고 있다(법률 제2조 제3호). 법원은 이렇게 광범위한 영업비밀의 침해태양에 더하여 그 구체적 범위를 제한할 수 있는 비밀유지의무(duty of confidentiality)를 신의칙 · 부수의무를 통해 최대한 폭넓게 인정하고, 부정한 이익을 얻거나 보유자에 손해를 가할 목적에 미필적 고의를 포함해 확장함으로써 영업비밀 보호의 범위를 끝없이 확장해 왔다.[36]

이렇게 비공지 정보가 영업비밀로 인정될 때 그 정보보유자는 침해행위에 대한 금지청구, 제공된 설비의 제거, 예방에 관한 청구를 할 수 있고(법률 제10조), 과실에 의한 영업비밀 침해행위에 대해서도 손해배상을 청구할 수 있으며(법률 제11조), 손해배상액의 산정 시 민법상의 불법행위와 달리 손해배상 산정방식에서 입증책임도 완화된다(법률 제14조의2 제1, 2, 3, 5항). 여기에 더해 2019. 1. 18. 법률 개정에 의해 영업비밀 침해행위가 고의적일 때에는 다른 비공지 정보에 대한 침해와 달리 3배까지 가중적 손해배상의 청구가 가능하다(법률 제14조의2 제6항).

하지만 한국에서 영업비밀이 특별히 강한 보호를 받는 것은 형사제재 때문이다. 부정경쟁방지법이 1991. 12. 31. 개정되면서 영업비밀이 처음으로 보호대상이 된 이래 영업비밀 침해에 대한 형사처벌은 그 대상을 기업의 임원 또는 직원으로 부정한 이익을 얻거나 기업에 손해를 가할 목적으로 특유한 생산기술에 관한 영업비밀을 제3자에게 누설한 자만을 처벌하는 제한적인 범위에서 2004. 1. 20. 부정경쟁방지법 개정 시 '임원 또는 직원'이라는 신분적 요소와 '생산기술에 대한 영업비밀'이라는 대상적 제한을 모두 삭제하면서 그 어느 국가보다 넓은 범위로 확장되었다.[37] 이에 따라 2010년대부터 영업비밀 침해에 대한 고소가 한해 1,200명 정도에 대하여 제기되고 있고,

---

36) 대법원 1996. 12. 23. 선고 96다16605 판결 및 대법원 2009. 10. 15. 선고 2008도9433 판결(비밀유지의무의 확장), 대법원 2003. 11. 14. 선고 2002도1739 판결(목적요건의 완화). 설민수, 앞의 글, 393-4면.

37) 설민수, 앞의 글, 392-3면.

기소되는 인원도 90여명 정도로 한국이 영업비밀 제도를 도입하는 과정에서 상당한 영향을 받은 미국의 영업비밀에 대한 형사처벌과는 비교가 어려울 정도로 활성화되어 있다.[38] 자연스럽게 1991년 형사제재와 함께 도입된 한국의 영업비밀에 대한 민사소송에 의한 보호는 형사제재에 후행하는 보조적 역할에 머물고 있다.[39]

(2) 영업상 주요한 자산과 그 보호제도

한국에서 영업비밀에 관한 형사제재는 영업비밀의 가장 큰 유출원인 근로자들의 이동성이 강화되고 경제의 디지털화가 일어난 2000년대 이후 또 다른 전기를 맞게 된다. 당시 부정경쟁방지법이 영업비밀 침해의 처벌대상을 기업의 영업비밀을 취득·사용, 제3자에게 누설한 경우로 제한하자 법원은 가장 광범위한 구성요건을 가진 범죄인 배임죄를 부정경쟁방지법에 정한 처벌대상을 넘는 행위에까지 확장해 적용하기 시작했다. 대법원 2003. 10. 30. 선고 2003도4382 판결은 회사 직원이 영업비밀을 무단으로 반출했을 때 실제 제3자에게 노출과 같은 재산적 손해를 가하지 않더라도 배임죄가 성립한다고 보았으며, 대법원 2008. 4. 24. 선고 2006도9089 판결은 근로자가 적법하게 취득하거나 그 사용에 허가를 받은 영업비밀이라도 퇴직 시에 이를 반환하거나 폐기할 의무가 고용계약에 의한 부수적 의무 또는 신의칙상 성립하므로 이를 반환·폐기하지 않은 부작위만으로도 업무상 배임이 성립한다고 판시해 부정경쟁방지법이 정한 영업비밀 침해를 넘는 행위를 처벌하기에 이른다. 2019. 1. 8. 개정 부정경쟁방지법은 위 행위들을 형사처벌의 대상이 되는 영업비밀 침해의 행위태양으로 추가함으로써 배임죄가 확장한 처벌범위를 흡수하였다(부정경쟁방지법 제18조 제1항 제1호 나, 다목).

배임죄의 영업비밀 외연 확장의 백미는 한국 외의 그 어느 국가에도 존재하지 않는 '영업상 주요한 자산'이라는 비공지 정보를 유출하는 행위를 배임죄로 처벌하는 부분이다. 이를 최초로 인정한 대법원 2005. 7. 14. 선고

38) 설민수, 앞의 글, 394-402면.
39) 설민수, 앞의 글, 401면.

2004도7962 판결은 종업원이 자료를 유출한 경우 업무상배임죄가 성립하기 위해서 그 자료가 영업비밀에 해당하여야 할 필요는 없고, 그 자료가 불특정 다수의 사람에게 공개되지 않았고, 사용자가 상당한 시간, 노력 및 비용을 들여 제작한 설계도면 등을 담은 컴퓨터 파일과 같은 영업상 주요한 자산인 경우에는 이를 유출한 행위도 업무상배임죄를 구성한다고 보아야 한다고 판시하면서 배임죄의 성립을 인정하지 않은 원심판결을 파기한 바 있다. 그 후 일부 비판적 시각에도 불구하고 위 판결은 비밀관리성을 다른 요건보다 다소 엄격하게 해석하는 법원의 판례를 보완해 보호가치를 가진 기업의 비공지 정보 보호의 사각지대를 없앤다는 명분에 힘을 얻어 이제는 확고한 한국 법원의 입장으로 자리 잡고 있다.[40]

이에 따라 ① 불특정 다수에 공개되지 아니할 것, ② 사용자의 상당한 시간, 노력 및 비용이 투입되어 그 자료의 사용을 통해 경쟁자에 대하여 경쟁상의 이익을 얻을 수 있는 정도의 가치를 가질 것이라는 두 가지의 요건을 충족한 비공지의 정보는 영업상 주요한 자산으로 인정되고 실무적으로는 회사 내 비공지 정보에 대하여 영업비밀과 상호처벌을 보완하는 역할을 하고 있다.[41] 가령, 2015년부터 2019년까지 법원에서 선고된 소프트웨어의 소스코드에 관한 영업비밀침해가 쟁점이 된 형사단독 판결 39건을 보면 주된 범죄가 영업비밀침해인 사건이 30건, 영업상 주요자산 유용의 업무상 배임죄인 사건이 7건이고, 영업비밀침해를 주된 범죄로 기소하면서 부가적으로 영업상 주요자산의 업무상 배임죄도 함께 기소한 경우도 6건에 이른다.[42] 영업비밀 침해와 영업상 주요자산 유용행위가 함께 기소되어 처벌된 경우를 비교해 보면 비공지 정보 중 패스워드, 출입제한 등의 회사 내 개발집단 중

40) 김종석, “업무상 배임죄에 있어서 영업상 주요한 자산의 의미”, 대법원판례해설(제88호), 법원도서관, 2011, 524-530면. 헌법재판소 2019. 12. 27. 2017헌가17 결정(업무상 배임죄 처벌을 합헌으로 판시).

41) 대법원 2012. 6. 28. 선고 2011도3657 판결(영업상 주요자산을 정의). 대법원 2008. 4. 24. 선고 2006도9089 판결(반출 후 미반환, 미폐기 행위에 대하여 영업상 주요자산 역시 배임죄가 성립한다고 판시).

42) 법원판결문검색시스템에 ‘소스코드’와 ‘영업비밀’ 두 가지 검색어를 넣어 검색된 형사단독 판결문 중 무관한 판결문을 제외한 판결문으로 확인했다.

일부에 대해서만 명시적 접근을 허용하는 보안 조치를 취한 소스코드나 회로설계도, 개발 자료는 영업비밀로, 그러한 제한 없이 회사 내 개발 집단 전체에 대해서는 공유되지만 외부에는 공개되지 않는 개발계획서 등 정보나, 외부로부터 얻은 자료나 공개자료에 일부 변형을 가해 그 변형부분이 시판되거나 공개되지 아니한 소스코드, 시안자료 등은 영업상 주요자산으로 기소가 이루어진다.[43]

이렇게 영업상 주요자산으로 인정되는 비공지 정보의 경우 민사적 보호는 영업비밀보다 제한되는 것처럼 보일 수 있다. 부정경쟁방지법상 금지청구를 할 수도 없고, 과실행위자에 대한 손해배상, 손해배상 산정방식의 특례, 가중적 손해배상이 적용되지도 않는다. 하지만 비밀성을 핵심적 가치로 하는 영업비밀은 이미 경쟁자에게 그 자료가 노출된 이상 금지청구가 실효성을 가지지 못해 실제 금지청구가 특허권 침해에 비해 활발히 활용되지 않는 편이고, 손해배상 산정방식의 특례 또한 영업비밀침해의 손해배상 산정이 침해행위로 발생하지 아니한 손해를 손해배상 산정에 고려하는 기여분의 할당에 따른 공제 등 요인으로 인해 부정경쟁방지법이 정한 유리한 산정방식이 아닌 민사소송법 제202조의2에 따라 불법행위에 관해 법원의 일반적 권한으로 정할 수 있는 재량에 의한 산정방식으로 대부분 이루어지는 현실에 비추어 보면 그 민사적 보호의 차이는 크다고 볼 수는 없다.[44]

그 위에 영업상 주요자산의 경우 아래 부정경쟁방지법 제2조 제1호 ㈐목의 부정경쟁행위의 요건을 갖추고 있다.[45] 그렇다면 최근에 입법되어 그 활발한 적용여부도 불확실한 가중적 손해배상을 제외한 나머지 모든 민사적 보호에 대하여 영업비밀과의 차이는 존재하지 않는다고 보는 것이 더 적절하다.

---

43) 수원지방법원 2019. 9. 1. 선고 2018고단1088 판결, 인천지방법원 2017. 11. 30. 선고 2016고단7271 판결, 수원지방법원 2017. 10. 27. 선고 2015고단6362 판결.

44) 설민수, "영업비밀침해에 대한 손해배상의 실제와 개선 필요성 — 산정방식을 중심으로", 『지식재산연구』, 제13권 제2호(2018), 80-3, 85-8면.

45) 서울중앙지방법원 2020. 6. 26. 선고 2016가합540484 판결[영업상 주요자산에 대하여 부정경쟁방지법 제2조 제1호 ㈐목을 적용].

(3) 부정경쟁방지법 제2조 제1호 ㈎목의 부정경쟁행위와 그 보호제도

위 두 가지가 적어도 불특정 다수에 대해 공지되지 아니한 비밀성과 경쟁자에 대한 경제적 유용성을 요건으로 하는데 비하여 이러한 요건을 갖추지 못한 정보에 대해서도 부정경쟁방지법은 제2조 제1호 ㈎목의 부정경쟁행위를 통해 보호하고 있다. 위 보호제도는 대법원이 2010. 8. 25.자 2008마1541 결정을 통해 자신이 제공하는 소프트웨어를 설치할 경우 한국의 지배적 포탈인 네이버에 접속 시 네이버의 배너광고시스템에 의한 광고 대신 대체 또는 삽입형태의 별도 배너광고가 나타나도록 하는 영업을 하는 회사에 대하여 네이버가 신청한 광고행위 금지를 청구한 가처분을 인용한 원심을 유지하면서 경쟁자가 상당한 노력과 투자에 의하여 구축한 성과물을 상도덕이나 공정한 경쟁질서에 반하여 자신의 영업을 위하여 무단으로 이용함으로써 경쟁자의 노력과 투자에 편승하여 부당하게 이익을 얻고 경쟁자의 법률상 보호할 가치가 있는 이익을 침해하는 행위가 부정한 경쟁행위로서 민법상 불법행위에 해당한다고 판시한 데서 시작한다. 위 대법원의 판시 중 경쟁자를 '타인'으로 바꾸어 부정경쟁방지법의 기타 부정경쟁행위와 달리 포괄적 일반규정의 형식으로 2013. 7. 30. 부정경쟁방지법 개정과 함께 제2조 제1호 ㈐목으로 추가되었다가 2018. 4. 17. ㈎목으로 변경되어 현재에 이르고 있다.

위 조문을 법원에서는 주로 저작권 등 전통적 지식재산권에 의해 보호되지 않는 경쟁적 우위요소나 제품의 특성 등을 보호하는 데까지 폭넓게 사용하고 있다.[46] 그 요건과 관련해서는 민법상 불법행위로 존재하던 시점부터 현재까지 법원은 ① 행위대상이 보유자가 상당한 노력과 투자에 의하여 구축한 성과물이어야 하고, ② 공정한 경쟁질서에 반하여 그 성과물을 자신의 영업을 위하여 무단으로 이용해야 하며, ③ 결과적으로 노력과 투자에 편승하여 부당하게 이익을 얻고 경쟁자의 이익을 침해하는 행위로 인정되어야 한다는 세 가지

46) 대법원 2020. 3. 26. 선고 2016다276467 판결(조형 등을 포함한 골프장의 종합적 이미지), 대법원 2020. 3. 26. 자 2019마6525 결정(유명 아이돌 그룹의 이름과 이미지), 서울고법 2020. 2. 6. 선고 2019나2031649 판결(방송광고를 위한 브랜드 네이밍과 관련 콘티). 서울중앙지방법원 2015. 1. 29. 선고 2014가합552520 판결(가방의 디자인적 특징).

요건 중 통상 ①, ②요건을 중심으로 판단하고 있다.[47] 그중 노력과 투자에 의해 구축된 성과물의 판단과 관련해서는 그 대상의 명성이나 경제적 가치, 결과물에 화체된 고객흡인력, 해당 사업 분야에서 결과물이 차지하는 비중과 경쟁력과 함께 그 결과물이 공공의 영역(public domain)에 속하지 않아야 한다는 점이, 무단이용과 관련해서는 경쟁관계 여부, 잠재적 경쟁자로 등장할 가능성, 대체가능성, 수요자나 거래자들의 혼동가능성 등이 중시된다.[48]

정보나 데이터와 관련해 법원이 부정경쟁방지법 제2조 제1호 ㈐목의 부정경쟁행위로 인정한 사건을 보면 방송사가 상당한 비용을 투자한 선거출구조사결과를 사전에 입수한 뒤 이를 이용해 인용방송을 넘어 이를 활용한 경우, 유사 회사의 인터넷 쇼핑몰 홈페이지의 HTML 소스코드를 일부 가져와 거의 그대로 사용한 경우, 온라인백과사전 형식의 게시물 전체를 기계적으로 복제해 활용한 경우가 있다.[49] 반대로 인정하지 않은 경우는 공개되거나 인터넷을 통해 직접 열람이 가능한 공지의 정보, 공지된 회로도 등으로부터 통상 기술자가 얼마든지 만들어 낼 수 있는 회로도나 부품목록과 같은 정보를 무단사용한 경우를 들 수 있다.[50]

2. 사물인터넷 관련 빅데이터에 대한 적용

(1) 사전처리를 거친 데이터세트

IoT 관련 빅데이터 중 머신러닝 AI에 사용가능하도록 사전처리를 거친 데

47) 설민수, "저작권의 보호 한계와 그 대안: 비디오게임, 인터페이스 소프트웨어, 패션디자인에서의 도전과 한국 법원의 부정경쟁방지법 제2조 제1호 ㈑목의 확장적 적용을 중심으로", 『인권과 정의』, 제458호(2016), 45-6면.

48) 위 2016다276467 판결, 2019마6525 결정.

49) 대법원 2017. 6. 15. 선고 2017다200139 판결(방송사 선거출구조사결과), 서울중앙지방법원 2020. 2. 6. 선고 2018가합56840 판결(HTML 소스), 서울중앙지방법원 2015. 11. 27. 선고 2014가합44470 판결(게시물 전체 내용을 사용한 경우).

50) 서울중앙지방법원 2019. 6. 14. 선고 2018가합517389 판결(공공기관에 의해 공개된 정보), 서울중앙지방법원 2015. 5. 14. 선고 2013가합53187(공지된 회로도로부터 쉽게 고안이 가능한 기술자료).

이터세트는 빅데이터 활용과 머신러닝 AI 기술이 가장 발전했고 오픈소스 소프트웨어(Open Source Software) 커뮤니티를 중심으로 관련 기술의 공유를 기초로 한 기술습득, 개발역량 강화 노력이 활발한 미국에서도 실무상 영업비밀로 관리되며 관련 산업에서 거래되거나 공유되지 않는다.[51] 어떻게 보면 당연한 것이 머신러닝 AI 학습을 위해 사전처리를 거친 데이터세트는 구체적인 머신러닝 AI 등의 설계과정에서 가장 많은 시간과 인적자원을 투입해야 하는 작업으로 머신러닝 AI가 도출한 결과나 그 관련 기법에 관한 지식만으로는 도저히 역설계를 통해 추출할 수 없기 때문이다.

이러한 관행은 향후에도 지속될 가능성이 크다. 우선 위 분야는 소프트웨어산업을 주도하고 있는 미국에서도 가장 급속히 발전하는 분야로 개발인력에 대한 수요가 커 개발자들에 대한 구인경쟁이나 그에 따른 이직이 활발하고 그에 관한 지식이나 관련 자료의 공유나 전파가 왕성하여 상대적으로 특정 기업이 경쟁자에 대하여 개발우위를 유지할 수 있는 부분은 시간과 인적자원의 투입이 필요한 사전처리된 데이터세트이다.[52] 따라서 학문적 연구목적이 아닌 한 이를 영업비밀로 하지 않고 공표하거나 공개한 상태에서 이용하는 경우 자체를 상상하기 어렵다. 다음으로 최근 머신러닝 AI의 기술 자체가 대규모의 데이터를 사용해 그 예측의 정확성을 향상시키는 쪽에서 기존에 다른 분야에 활용된 데이터세트나 제한된 데이터세트를 활용해서도 예측가능성을 향상시키는 기술 쪽으로 그 방향이 옮겨가고 있어 사전처리를 거친 데이터세트는 일회적인 용도가 아닌 계속적 경쟁력의 원천으로 작용할 가능성이 커 이에 관해 영업비밀로 유지할 필요성도 커지고 있다.[53]

따라서 이렇게 IoT 관련 빅데이터 중 사전처리를 거친 데이터세트는 ① 경제적 가치, ② 비공지의 정보로서의 비밀성의 요건을 완전하게 갖추고 있으므로, ③ 보유자가 비밀관리성을 갖추고 있는지에 따라 한국에서 영업비밀 또는 영업상 주요자산으로서 부정경쟁방지법에 의해 보호될 수

51) Hyunjong Ryan Jin, *supra*, pp. 95-6; 설민수, 앞의 글(주12), 417면.
52) 설민수, 앞의 글(주12), 418면.
53) 설민수, 앞의 글(주12), 418면.

있다. 사전처리 과정에 있는 IoT 관련 빅데이터의 경우는 그 과정에서 구체적으로 투입된 비용, 노력, 사전처리의 진행과 비밀성의 유지 정도, 침해자가 취득하거나 사용한 데이터의 양에 따라 판단될 것이지만, 완전한 상태로 공개되거나 누구나 쉽게 접근할 수 있는 경우가 아닌 한 위 두 가지나 적어도 부정경쟁방지법 제2조 제1호 ㈐목의 적용에 대한 기존 법원의 입장에 의하면 그 상당부분을 그대로 무단으로 취득하거나 사용한 경우에는 위 규정에 의한 보호대상이 될 가능성이 크다.

(2) 비식별화 조치를 거친 데이터세트

비식별화 조치(de-identification)란 개인정보 중 개인을 특정짓거나 밀접한 관계를 가지고 있어 직·간접적으로 개인을 식별할 수 있는 개인식별지표(personal identifier)와 그 정보주체(data subject) 사이의 연관관계를 감소시키는 모든 조치를 의미한다.[54] 종래 이러한 비식별화 조치는 정보처리자 단독 또는 제3자와 협업을 통해서도 정보주체가 직·간접적으로 더 이상 식별될 수 없을 정도로 개인정보를 불가역적(irreversible)으로 변환하는 조치를 의미하는 익명화 조치(anonymization)와 동일시되거나 불가역한 상태에 이른 것을 익명화로 보고 비식별화 조치는 이를 포함한 광의의 개념으로 이해하는 것이 보통이었다.[55] 여기에 GDPR이나 그 영향을 받아 2020. 2. 4. 개정된 개인정보보호법은 분리 보관되는 추가정보를 사용하지 않고는 특정 개인의 정보임을 알 수 없도록 처리하고, 추가 정보 보관에 대한 기술적, 조직적인 조치를 취할 것을 요구하는 가명처리(pseudonymisation)란 개념을 별도 설정하고 있어 관련논의는 더 복잡화되고 있다.[56]

그 개념과 관계없이 비식별화 조치를 거친 IoT 관련 빅데이터는 원시데이터에서 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 가

54) Colonna, *supra,* p.155; 김나루, "빅데이터 환경에서 개인정보의 익명화 또는 비식별화에 관한 비교법적 연구", 『세계헌법연구』, 제25권 제2호(2019), 138면.

55) Colonna, *supra*, pp.154-5; 김나루, 앞의 글, 134-140면.

56) 개인정보보호법 제2조 제1, 1의2호. Colonna, *supra*, pp.156-8; 김나루, 앞의 글, 146-7면.

공행위를 통해 정보주체인 IoT 사용자의 식별이 원시데이터보다 어려워지게 된다. 식별의 곤란성 정도가 불가역한 정도에 이를수록 IoT 사용자에 대한 추적가능성이 떨어지고 자연스럽게 비식별화 조치를 거친 데이터세트는 개인정보 보호에 관한 규제를 벗어나 정보처리자가 제3자에게 이를 판매하거나 사용하게 할수 있는 거래의 대상이 될 수도 있다. 실제 유럽연합은 불가역한 수준에 이른 익명화 조치를 거친 개인정보는 GDPR 규제의 대상에서 제외하고 있다.[57] 결과적으로 비식별화 조치를 거친 IoT 관련 데이터세트는 원시데이터에 비식별화 조치라는 별개의 공정이 추가 투입되고 거래의 대상으로서 규제의 제한에서 어느 정도 벗어나게 됨으로써 별개의 가치를 가지게 된다.

이러한 비식별화 조치를 거친 IoT 관련 데이터세트에 관해 부정경쟁방지법의 보호 논의는 현실에서 거래가 아직 실체화되지 않았기 때문에 어떤 형태로 거래될지에 관해서는 가정을 필요로 한다. 다만 기존 판례에 비추어 보면 어느 정도 비공지성을 가지고 거래대상이 될 정도로 비식별화가 이루어졌다면 부정경쟁방지법에 의한 보호대상이 되기에 충분하다. 거래의 대상이 될 정도로 비식별화 조치가 이루어졌다면 그 과정에서 IoT 관련 원시데이터와 달리 비식별화 과정과 그 거래를 위한 준비과정에서 그 데이터세트의 보유자는 상당한 비용과 별도의 투자를 할 가능성이 높고 거래대상으로 위 데이터세트는 원시데이터와는 구별되는 별도의 가치를 가지고 있는 이상 누구나 쉽게 접근할 수 있는 공지의 대상이 아닌 한 적어도 영업상 주요자산 또는 부정경쟁방지법 제2조 제1호 ㈐목의 보호대상으로 인정되기에 충분하다.

만약 비식별화 조치를 거친 IoT 관련 데이터세트를 누구나 접근할 수 있는 공개된 상태로 거래를 한다면 어떻게 될까? 그와 같은 거래가 현실에서 발생하기 위해서는 위와 같은 상태로 거래할 경우에도 관련 데이터세트에 관해 일정한 시장가격이 형성될 지와 같은 문제에 달려 있다. 다만 아래에서 언급할 개인정보의 재식별 위험성 때문에 위와 같은 상태로 거래될 가능성

57) Colonna, *supra*, p.153.

은 거의 존재하지 않을 것이다.

(3) 원시데이터 상태의 빅데이터

마지막으로 원시데이터 상태로 보유자의 클라우드 서버에 일체 가공을 하지 않은 상태로 존재하는 IoT 관련 빅데이터의 경우는 영업비밀이나 영업상 주요자산, 부정경쟁방지법에 의한 보호 자체가 모호한 편이다. 대체로 보안목적에서 내부자 외에는 접근을 제한하는 형태로 보관될 가능성이 높지만 분절화가 심한 IoT 기기의 성격상 이는 회사 규모나 그 정책에 따라 각기 그 보관 형태가 달라질 가능성이 높아 일괄적으로 언급하기 어렵다.

다만, 그 경제적 가치 자체가 보유자에게는 모호하더라도 그 보관형태가 소수의 내부자 외에는 접근을 불허하는 형태가 될수록 영업상 주요자산이나 적어도 부정경쟁방지법 제2조 제1호 ㈏목의 대상으로 인정받을 가능성이 크다. 우선 빅데이터는 그 방대함과 변동성을 특징으로 하는 것인 이상 IoT 관련 빅데이터 중 일체 가공을 하지 않은 원시데이터라도 그 양이 막대하고 다른 대체적 수단이 없을 경우 그것만으로 상당한 경제적 가치를 가질 가능성이 크다. 무엇보다 한국 법원의 실무에서 영업비밀 등과 관련해 경제적 유용성 자체를 심리하는 것은 드물고, 침해자가 일상의 수단이 아닌 내부자의 매수나 공모 등의 수단으로 유출해 활용하려는 것 자체가 일정한 경제적 유용성을 가지고 있다고 판단할 가능성이 높다. 두 번째로 보관의 형태가 소수의 내부자 외에는 접근을 제한하기 위해서는 그만큼 노력과 투자가 필요하고 이러한 과정이나 관련 비용 자체가 IoT 관련 빅데이터의 생성과 별도의 투자 또는 노력으로 인정받을 가능성이 커진다. 또한 클라우드 서버에 저장되고 접근이 제한되는 보안조치를 취하는 이상 내부자와 공모 등이 없이는 정보통신망에 대한 침입 외에는 접근이 불가능한 것이 통상적이며 그 경우 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조를 위반하는 별도의 불법행위를 구성하게 될 것이며 이때 행위 자체가 부당성의 요건을 상당부분 충족하게 된다.

반대로 클라우드 서버에 보관한다고 하더라도 보안조치를 취하지 않아 누

구나 접근할 수 있는 공개상태로 놓아둔다면 부정경쟁방지법의 보호대상이 되지 않는 것은 명확하다.

Ⅳ. 한국에서 사물인터넷 관련 빅데이터 보호제도에 대한 대안의 필요성 여부

1. 사물인터넷 관련 빅데이터에 대한 현재 보호제도의 평가

앞에서 살펴본 쟁점과 관련해 부정경쟁방지법에 의한 보호를 평가해 보기로 한다.

영업비밀과 기타 정보로만 구별하는 다른 국가와 달리 한국의 부정경쟁방지법과 법원의 해석은 공개된 비식별화 조치를 거친 데이터세트와 별다른 보안조치 없이 클라우드 서버에 보관된 사실상 공지 상태의 원시데이터를 제외한 나머지 IoT 관련 빅데이터에 대해 그 침해가 있을 경우 영업비밀, 영업상 주요자산 또는 부정경쟁방지법 제2조 제1호 ㈋목의 보호대상으로 보고 형사처벌 또는 민사상 구제조치 등 다양한 보호제도를 제공하고 있다. 보유자가 투자한 비용과 관리를 위한 노력에 따라 그 가치와 중요성이 달라질 수밖에 없는 IoT 관련 빅데이터인 사전처리를 거친 데이터세트, 비식별화 조치를 거친 데이터세트, 원시데이터에 관해 영업비밀, 영업상 주요자산, 경쟁방지법 제2조 제1호 ㈋목의 보호대상으로 보호수단과 그 보호강도도 달리하고 있다. 그 위에 IoT 기기의 향후 발전과정에서 보안이 점점 중요시되고, 개인정보 보호가 강조될수록 IoT 관련 빅데이터 전반이 원천적으로 비공지성을 강하게 가질 수밖에 없다는 점까지를 감안해 보면 사회적 요구에 따라 보안의 강화를 통해 IoT 관련 빅데이터를 관리하는 사업자에게 필요한 전반적 보호를 추가적 비용의 요구 없이 제공하는 점도 부정경쟁방지법의 장점이다.

또 다른 쟁점이었던 IoT 관련 빅데이터에 관해 그 근원적인 소유자의 문제 역시 부정경쟁방지법에서는 크게 제기되지 않는다. 해당 정보의 저자나

창작자로의 소유나 처분권 귀속을 전제로 하는 다른 지식재산권과 달리 정보를 관리하는 자의 노력에 의한 비공지성에 따른 독점을 그 보호대상으로 평가하는 부정경쟁방지법의 특성은 IoT 관련 빅데이터가 제기하는 난제 하나를 큰 어려움 없이 돌파할 수 있게 해 준다. 가령, 현재 대법원은 영업비밀과 관련하여 제3자로부터 일정한 조건으로 무상취득해 보유자가 가공한 정보에 관하여 정보보유자가 제3자가 부과한 조건을 위반해 독점적으로 활용한 경우에도 영업비밀로 인정하고 있다.[58] 즉, 다른 지식재산권과 달리 IoT 관련 빅데이터에 관해서 부정경쟁방지법에 의한 보호는 그 진정한 소유자가 누구인지를 묻지 않는다.

2. 대안의 필요성에 대한 주장과 그 문제점

(1) 대안의 필요성에 대한 주장

대안의 필요성을 주장하는 논의들이 비밀성을 그 전제로 하는 영업비밀이나 그와 유사한 보호방식에 부정적인 가장 큰 이유는 침해의 두려움으로 빅데이터를 비공지 상태로 유지하는 것이 빅데이터 유통과 활성화의 가장 큰 장애이므로 새로운 보호제도를 도입해 빅데이터를 보유한 기업들이 두려움 없이 경쟁자들에게 관련 데이터를 공개할 수 있도록 하여 빅데이터의 공개 및 유통을 활성화한다는 데 있다.[59]

반면 그 대안에 관해서 구체적으로 언급하는 논의는 드문 편이다. 기존의 지식재산권법의 어디에서도 보호를 제공하지 않고 있고, 한국에서 새로운 입법을 주장할 때 주로 참작하는 미국이나 유럽연합에서 관련 논의나 입법이 이루어지지 않는 상황이 영향을 주고 있다고 할 수 있다. 이에 따라 가장 많이 대안의 하나로 논의되는 것이 일본이 2018. 5. 30. 부정경쟁방지법을

58) 대법원 2009. 2. 12. 선고 2006도8369 판결(개작해 활용할 경우에도 소스코드 공개를 요구하며 가장 강한 사유화에 대한 제한을 부과하는 General Public License 조건의 소스코드를 개작한 소스코드를 보유자의 영업비밀로 인정).

59) 박준석, 앞의 글, 109-110면; 차상육, 앞의 글, 126-127면; 이일호, 앞의 글, 88-89면.

개정해 제2조 제11호 내지 16호에 신설한 한정제공데이터라는 이름으로 빅데이터를 보호하는 제도나 그와 유사한 보호제도이다.[60]

(2) 문제점

대안의 필요성에 관한 주장들의 가장 큰 문제점은 현재 IoT 관련 빅데이터의 거래가 활성화되지 않는 이유가 비공지성을 기초로 한 보호방식 때문이라는 전제가 틀렸다는 것이다.

우선 IoT 관련 빅데이터 중 사전처리된 데이터세트는 앞에서 살펴보았듯이 향후 빅데이터 거래시장이 활성화가 되더라도 관련 기업이 경쟁자에 대하여 가질 수 있는 경쟁력의 원천으로서 비밀로 둘수록 그 가치가 증가하는 이상 일상적인 거래대상, 특히 공개를 전제로 하는 거래의 대상이 되기 어렵다. 머신러닝 AI가 만들어 낸 결과물만으로 그 학습의 원천이 되는 데이터세트의 추론 자체가 불가능해 침해가 있더라도 침해를 인정받기 어렵다는 점에서 위 사전처리된 데이터세트는 거래에 아무런 장애가 없더라도 영업비밀에 그 보호를 의존할 가능성이 높다.

영업비밀로 남을 필요가 크지 않은 비식별화 조치를 거친 데이터세트나 클라우드 서버에 보관되어 있는 원시데이터 역시 새로운 보호제도가 나타난다고 해서 바로 거래가 활성화될 수 없다. 현재 IoT 관련 빅데이터의 거래가 활성화되지 않는 가장 큰 이유는 그 정보주체에 대한 추적가능성이 큰 IoT 관련 빅데이터에 대해 개인정보 보호와 보안상의 이유로 그 거래나 재이용을 엄격히 제한하는 각국의 법률이나 관련 규제 때문이다.[61] IoT 관련 빅데이터의 거래가 활성화되지 않는 또 다른 사유인 IoT 관련시장이 분절화된 시장으로 관련 빅데이터의 표준화가 이루어지지 않아 기존 시장에 진입해 있는 머신러닝 AI 관련 기업들도 이를 모아 실제 분석에 활용할 정도까지에는 상당한 정도의 별도 노력을 필요로 한다는 점도 보호제도의 도입 여부와는 무관한 사유이다.

---

60) 박준석, 앞의 글, 114-118면.

61) Colonna, *supra*, p.153; Rubinfeld & Gal, *supra*, pp.367-8.

대안의 필요성에 관한 주장의 또 다른 문제점은 그 대안이 현재 영업비밀, 영업상 주요자산, 부정경쟁방지법 제2조 제1호 ㈐목으로 IoT 관련 빅데이터를 다양한 형태와 종류에 따라 보호하는 현행 한국의 보호제도와 다른 형태로 IoT 관련 빅데이터를 보호할 가능성이 크지 않다는 것이다.

방대함과 변동성을 특징과 가치로 하는 데이터세트인 빅데이터의 성격상 그 보호는 자신의 데이터세트 중 극히 일부를 사용했다고 해 바로 침해를 주장할 수 있는 것이 아니고 그 대부분 또는 그와 유사하다고 볼 수 있을 정도의 상당한 분량을 그대로 사용한 경우가 아니라면 이를 침해행위로 보기 어려울 수밖에 없다. 또한 공개 또는 어느 정도 외부인의 접근이 허용된 상태로 거래될 경우 이를 그 거래대상자가 아닌 자가 이를 취득하거나 사용할 때는 공공의 영역에 속한 데이터세트로 보고 취득·사용할 가능성이 높으므로 이러한 행위는 침해행위에서 제외하거나 행위가 통상의 허용된 행위가 아닐 경우에만 침해행위로 규정하는 방법으로 보호할 수밖에 없다.

그 경우 보호제도 자체가 한국에서 영업비밀의 외연을 확장하는 영업상 주요자산, 부정경쟁방지법 제2조 제1호 ㈐목과 구별할 수 없는 내용이 될 가능성이 아주 크며, 영업비밀 외에는 비공지 정보를 보호하지 않는 국가라면 모르겠지만 한국과 같이 다양한 형태의 보호제도를 갖춘 국가가 이를 도입할 필요성은 거의 없다. 실제 일본이 도입한 한정제공데이터 제도는 현재 한국의 위 보호제도들과 비교해 거의 구별실익이 없다.[62]

3. 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 보호제도의 장점

(1) 사물인터넷 관련 빅데이터에서 비식별화 조치의 한계

앞서 살펴본 바와 같이 IoT 관련 빅데이터 가치의 대부분은 그 사용자에 대한 추적가능성이다. 반면에 빅데이터 거래를 위한 전제조건인 비식별화

62) 박준석, 앞의 글, 116-7면; 차상육, 앞의 글, 135-6면.

조치는 이러한 추적가능성을 단절 또는 감소시키는 데 목적이 있다. 여기에서 IoT 관련 빅데이터의 활용에서 일상적으로 제기되는 문제인 빅데이터의 유용성과 사용자의 사생활 침해가능성 사이에는 역상관관계(negative correlation)가 발생하게 되고 유용한 IoT 관련 빅데이터는 비식별화 조치에도 불구하고 늘 추적가능성의 위험을 안을 수밖에 없다.[63]

실제로 IoT 관련 빅데이터 중에는 비식별화 자체가 불완전한 경우도 얼마든지 있다. 앞에서 살펴본 스마트 스피커를 통해 수집된 일상의 대화에 관한 음성데이터의 예로 돌아가 보자. 비록 음성데이터와 관련된 사용자의 이름, 주소, IP 주소 등 관련 개인식별지표를 모두 삭제한다고 해도 사용자의 독특한 음색이나 성문의 분석을 통해 개인을 식별할 가능성은 남게 된다.

비록 비식별화 조치를 통해 이러한 추적가능성의 위험을 낮춘다고 하더라도 재식별(re-identification)의 가능성이 존재한다. 종전에는 개인정보를 불가역적으로 비식별화한 익명화 조치를 거친 정보를 외부의 보조적인 정보와 결합하여 정보주체를 다시 식별한다고 해 익명화 해제(deanonymization) 또는 연결공격(linkage attack)이라고 불리기도 하는 재식별 주장의 핵심은 원시데이터의 일부 삭제 또는 대체와 같은 방식으로 원시데이터를 유통시키지 않는 비식별화 조치로도 외부 정보와 비교대조가 용이해짐에 따라 재식별될 가능성이 상존한다는 것이다.[64] 이에 따라 GDPR의 경우 일정한 비식별화 조치를 취하면 빅데이터의 유통에 제한을 두지 않고 허용하자는 일부 주장과 달리 각 비식별화 조치에 내재한 위험성을 평가하는 위험성 관리를 비식별화 조치에 수반하는 과정으로 내재화하는 방식을 취해 가명처리와 그 과정에서 재식별 가능성을 줄일 수 있는 기술적 조치들을 통한 지속적인 합리적 위험성 관리를 대안으로 제시하고 있다.[65]

---

63) Colonna, *supra*, p.161.

64) Elizabeth A. Brasher, *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, 2018 Colum. Bus. L. Rev. 209(2018), pp. 227, 231-33.

65) *Id.* pp.247-250; Colonna, *supra*, pp.163-6.

(2) 부정경쟁방지 및 영업비밀보호에 관한 법률에 의한 보호의 장점

부정경쟁방지법에 의한 IoT 관련 빅데이터 보호는 앞에서 살펴보았듯이 어디까지나 비공지성을 전제로 하며, 비공지성은 최종적인 소비자를 대상으로 하는 정보상품의 거래에서는 확실히 거래활성화의 결정적인 장애물이다. 소비자로서는 비공지 상태를 유지해가면서 소비를 하고 거래를 할 유인이 없기 때문이다.

하지만 IoT 관련 빅데이터와 같이 그 수요자가 이를 일종의 개발을 위한 소재로서 활용하는 기업이라면 비공지 상태의 유지는 거래에 있어서 큰 장애물이 되지 못한다. 실제 기업 간 기술거래에 있어서 영업비밀을 포함한 기술지원이나 공동개발기술에 관해 수수료를 받고 거래를 하는 경우가 종종 있다.[66] 물론 비공지 상태 정보의 거래이므로 그 거래 활성화를 위해서는 거래당사자를 연결시켜주고 신뢰를 담보할 거래 중개자가 필요하겠지만 이러한 문제는 결정적 장애로 보기 어렵다.

반면 비공지 상태로 거래될 때 가장 큰 장점은 재식별의 위험성을 낮추어 IoT 관련 빅데이터를 제공하는 원천인 사용자의 IoT 기기 사용, 그리고 IoT 관련 빅데이터 거래에 대한 거부감을 낮출 수 있다는 것이다. 비식별화 조치를 거친 데이터세트의 재식별의 핵심은 해당 데이터를 외부의 보조적 정보나 다른 데이터세트와 결합시키는 방식을 통해서이며 자연스럽게 데이터세트가 공개될수록 그 재식별의 가능성은 커지는 반면 비공지의 상태로 거래될 경우 상대적으로 불완전한 상태의 비식별화 조치를 거친 데이터세트라도 거래를 허용해도 그 위험성을 낮출 수 있게 된다.[67] 따라서 민감한 개인정보가 담긴 IoT 관련 빅데이터의 거래에서 데이터의 비공개, 접근제한 조치, 취급자에 대한 자격제한과 같은 공개를 막는 조치는 상대적으로 개인정보 침해에 대한 인식이 강한 유럽연합 국가들 사이에서 법률로 의무화되거나 거래를 허용하는 기준으로 일반화되고 있다.[68] 실제 현재 한국에서 가명처리 조치를 거쳐 거래하고 있는 금융권 데이터

66) 수원지방법원 2019. 7. 17. 선고 2016가합82382(영어비밀 포함한 기술의 라이선스계약). 대전지방법원 2019. 9. 26. 선고 2018가합102984 판결(영업비밀을 포함한 공동 생산기술개발계약).

67) Colonna, *supra*, pp.169-170.

68) *Id.*, pp.171-172.

도 어디까지나 인증을 거친 기업회원을 중심으로 거래하며 공개된 상태로 거래하는 행위는 금지하고 데이터의 결합은 엄격한 허가 사항으로 하고 있다.[69]

Ⅴ. 글을 마치며

IoT 관련 빅데이터는 자동차의 가격보다 자동차 관련 빅데이터의 가치가 훨씬 비싼 시대가 도래할 것이라는 장밋빛 미래와 이러한 기대와는 달리 IoT가 급속히 확산되지 않는 현실 사이에 끼어 있다. 장밋빛 미래가 현실이 되지 않은 데에는 기술적 문제 등 다양한 이유가 있지만 IoT 기기 사용자들이 자신의 사용으로 만들어지는 데이터에 관하여 IoT 기기 제조자 등이 해당 IoT 기기 개선을 넘어 이를 임의로 판매하거나 활용하는 데 강한 저항감을 보이고 이에 따라 IoT 기기 제조자들도 그 활용에 조심스러운 태도를 취하고 있는 것도 그중 하나이다.

그 위에 IoT 관련 빅데이터의 진정한 소유자가 누구인지는 현재의 IoT 발전 단계에서 쉽게 확정짓기 어려운 문제로 IoT 관련 빅데이터에 대해 다양한 이해관계자까지 존재하는 현실까지를 더해 보면 IoT 관련 빅데이터의 비공지성을 바탕으로 한 독점력을 다양한 형태로 보호하는 한국의 부정경쟁방지법에 의한 보호는 여러 가지 장점을 가지고 있다. 이에 반해 어떤 설익은 형태의 결론을 전제로 할 수밖에 없는 새로운 보호제도의 도입은 오히려 IoT 관련 빅데이터의 발전에 장애물이 될 여지가 훨씬 크다. 실제 IoT 관련 빅데이터의 거래 활성화에는 IoT 기기의 분절화 현상으로 인한 표준성 등의 부족, 개인정보 침해에 대한 규제 문제 등이 앞에서 보았듯이 훨씬 큰 현실적 장애이므로, 금융권 데이터에 관해 금융데이터거래소를 통해 그 거래활성화를 꾀하듯이 그 거래를 중개하고 관련 규제에 대하여 거래자에 대하여 일정한 보증을 할 수 있는 거래기관의 조성이 한국에서는 보다 현실적 문제로 논의를 필요로 하는 부분이다.

---

69) 금융보안원, “금융권데이터 유통가이드”, 2020, 35면.

참고문헌

〈단행본(국내)〉

김종석, "업무상 배임죄에 있어서 영업상 주요한 자산의 의미", 대법원판례해설(제88호), 법원도서관, 2011.

〈학술지(국내)〉

김나루, "빅데이터 환경에서 개인정보의 익명화 또는 비식별화에 관한 비교법적 연구", 『세계헌법연구』, 제25권 제2호(2019).

박준석, "빅데이터 등 새로운 데이터에 대한 지적재산권법 차원의 보호가능성", 『산업재산권』, 제58호(2019).

설민수, "영업비밀침해에 대한 손해배상의 실제와 개선 필요성 — 산정방식을 중심으로", 『지식재산연구』, 제13권 제2호(2018).

_____, "저작권의 보호 한계와 그 대안: 비디오게임, 인터페이스 소프트웨어, 패션디자인에서의 도전과 한국 법원의 부정경쟁방지법 제2조 제1호 ㈐목의 확장적 적용을 중심으로", 『인권과 정의』, 제458호(2016).

_____, "한국 소프트웨어산업에서 형사처벌의 활성화를 통한 영업비밀의 지위 강화, 그 영향과 향후과제-미국과의 비교를 중심으로", 『사법』, 제52호(2020).

이일호, "빅데이터의 법적보호문제 — 영업비밀보호법에 의한 보호가능성을 중심으로", 『법조』, 제727호(2018).

차상육, "빅데이터의 지적재산법상 보호", 『법조』, 제728호(2018).

〈학술지(서양)〉

Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 Cath. U. J. L. & Tech. 187(2018).

Daniel L. Rubinfeld & Michal S. Gal, *Access Barriers to Big Data*, 59 Ariz. L. Reb. 339(2017).

David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. Davis L. Rev. 653(2017).

Elizabeth A. Brasher, *Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation*, 2018 Colum. Bus. L.

Rev. 209(2018).

Hu Margaret, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 Pepp. L. Rev. 773(2015).

Hyunjong Ryan Jin, *Think Big! The Need for Patent Rights in the Era of Big Data and Machine Learning*, 7 NYU J. Intell. Prop. & Ent. L. 78(2018).

Katherine Britton, *Handling Privacy and Security in the Internet of Things*, 19 No. 10 J. Internet L. 3(2016).

Lars Smith, *Rfid and Other Embedded Technologies: Who Owns the Data?*, 22 Santa Clara Computer & High Tech. L.J. 695(2006).

Lauren Henry Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, 86 Tenn. L. Rev. 863(2019).

Liane Colonna, *Privacy, Risk, Anonymization and Data Sharing in the Internet of Health Things*, 20 U. Pitt. J. Tech. L. & Pol'y 147(2020).

Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. Ky. L. Rev. 29(2016).

Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices*, 52 Suffolk U. L. Rev. 227(2019).

Noam Kolt, *Return On Data: Personalizing Consumer Guidance In Data Exchanges*, 38 Yale L. & Pol'y Rev. 77(2019).

Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 Berkeley Tech. L.J. 997(2016).

Korea's Protection to Internet of Things related Big Data and Its Direction — Focusing Features of Internet of Things and Sufficiency of Protection by the Unfair Competition Prevention and Trade Secret Protection Act

Seul, Minsoo

Protection of Big Data draws attention of general public beyond related experts as Internet of Things(hereafter 'IoT') spreads. Naturally, discussions of introduction of new intellectual property protection measures that points out the fault of existing protections are erupting.

However, IoT related Big Data has many distinct features from other Big Data including non-publicity originated from security measures, inseparability of user's personal information by traceability. Accordingly, new protection measures by intellectual property to IoT related Big Data bring out unsolvable numerous legal issues like attribution of ownership. The Unfair Competition Prevention and Trade Secret Protection Act and court's interpretation(hereafter 'the Act') protects non-public information in Korea by utilizing frames of trade secret, major assets in business and unfair competitory acts by section 2.1(Ka) unlike other countries. The Act provides various and wide range of criminal sanctions and civil protection measures according to the value of the information by monopoly powers. It sufficiently protects pre-processed dataset, de-

identified dataset, Big Data in raw data status among IoT related Big Data and has the advantage of helping active trading of Big Data by discouraging re-identification of personal information which is one of main barriers to trading of IoT related Big Data.

Keyword

Internet of Things, Big Data, Trade Secret, Major Asset in Business, Protection of Personal Information, Non-Publicity