영남대학교 법학연구소
「영남법학」 제45호 (2017.12) 23~56면.
Yeungnam Univ. Law Journal
Vol.45 (December. 2017) pp.23~56.

4차 산업혁명 시대에서 범죄예방 및 정보인권 보장을 위한 법적 고찰
: 빅데이터 및 사물인터넷을 중심으로

이 준 복*

< 목 차 >

Ⅰ. 들어가며

현 정부는 사이버 보안에 대해 국민과 국가를 지키는 첨병이며 4차 산업혁명의 지속가능성을 뒷받침하는 핵심 분야이므로 국민의 안전을 정보보호정책의 최우선과제로 보고 있다. 특히 2017년 정보보호의 날을 맞아 국가 전반에 걸쳐 사이버 보안 취약지점을 철저히 점검하기 위해 스마트 기기, 자율주행차 등을 대상으로 한 해킹처럼 국민 안전을 위협하는 새로운 유형의 사이버 범죄 예방에도 적극적으로 대처하겠다는 입장을 표명한 바 있다.[1] 더 나아가 산업단지와 혁신도시에 특화된 정보보안인력을 양성하는 등 지역의 일자리 창출에도 관심을 기울일 것으로 예측된다. 그러나 정보보호의 날은 올해로 6주년을 맞지만

* 서경대학교 공공인적자원학부 법학전공 교수, 개인정보관리사(CPPG), 법학박사.
1) 디지털타임스, 문 대통령, “사이버보안, 4차 산업혁명 핵심 … 새유형 사이버범죄 예방 최우선”, 2017. 7. 12. 기사.

사이버 범죄는 해마다 증가하는 추세다. 경찰청에 따르면 사이버 범죄 건수는 2014년 11만 건에서 지난해 15만3000 건으로 2년 사이 40%가량 증가했다. 또 올해 5월까지 발생한 해킹 건수는 1200여 건으로 이미 지난해 전체 발생 건수(1847건)의 70% 수준에 달한다.[2] 따라서 각 관계부처는 현 정부의 방침을 구체화하기 위해 최근 랜섬웨어 등 정치적, 금전적 공격을 노린 사이버 공격이 뚜렷해지고 있기 때문에 각 기관과의 공조체계를 강화함은 물론, 신기술 활용을 통해 점차 고도화하는 공격에 대응해야 될 시점이다.[3]

이를 위해 범죄가 발생하면 피해 범위가 광범위하고 확산 속도가 빠른 사이버 공간 특성을 반영하여 가칭, '사이버범죄 예방기본법' 마련에 대한 논의가 활발히 이뤄지고 있다.[4] 4차 산업혁명 파장이 클수록 안전 위협은 더욱 커지며 나아가 국가 안보에 영향을 줄 뿐만 아니라, 온·오프라인 변화로 치안 패러다임 변화도 동시에 이뤄져야 한다. 사이버 공간에서 국민 안전을 확보할 수 있는 법체계 마련을 통해 4차 산업혁명을 범죄예방 수준을 높일 수 있는 기회로 활용해야 한다.

이에 본 연구는 4차 산업혁명시대에서 유의미한 도구로 제시되고 있는 사물인터넷, 빅데이터 등 신기술을 활용한 범죄예방마련 측면에 비중을 두어 진행한다. 특히 앞서 언급한 사례가 의미하듯 사이버 범죄가 증대되고 있는 것은 사실이나, 특정범죄 유형에 국한하여 진행하지 않고, 온·오프라인에서 다양하게 일어나고 있는 범죄에 대한 예방을 위해 빅데이터, 사물인터넷을 중심으로 진행한다. 다만, 여기에서는 양자에 대해 모두 접근하여 정리하겠지만, 데이터 수집 및 분석을 통해 범죄를 예측·예방, 분석·해결하는 사물인터넷은 빅데이터 기술을 전제로 하기 때문에 활용가능성 및 한계, 개선방향 제시 등에서는 빅데이터에 초점을 맞춰 비중 있게 다루어 진행함을 아울러 알려둔다.[5] 이를

---

2) 사이버경찰청 홈페이지(www.police.go.kr) 참조.
3) 매일신문, '랜섬웨어' 사태… "스파트폰 터치 겁나" 사이버공격 공포, 2017. 5. 18. 기사.
4) 전자신문, 4차 산업혁명 시대 '사이버범죄 예방기본법' 필요, 2016. 10. 19. 기사.
5) itworld, 마이크로소프트, "사물 인터넷과 빅데이터의 본질은 같다", 2015. 2. 27. 기사 발췌; 마이크로소프트에 따르면 사물 인터넷을 특별하게 만드는 것은 사물이 아닌 데이터다. 사물 인터넷은 센서와 인터넷 연결을 갖추고 있다면 어떤 사물이든 가능하며, 그 활용 범주가 거대한 만큼 정의하기도 어렵다. 실제로, 사물 인터넷은 때로는 M2M(machine-to-machine)이라고 불리기도 하며 시스코의 경우 사물 인터넷 대신 '만물 인터넷(Internet of Everything)이라는 용어를 쓰고 있다. 명칭은 다르지만, 사물 인터넷과 M2M, 그리고 만물 인터넷의 공통점은 바로 만질 수 있는 '사물'에 초점을 맞추고 있다는 것이다. 그러나 마이크로소프트는 사물 그 자체보다는 그 사물들이 생산하는 '데이터'를 주목하고 있다. 마이크

위해 제2장에서는 빅데이터 및 사물인터넷의 의의와 실태, 사례 등 현황에 대해서 정리하고, 제3장에서는 범죄예방을 위한 빅데이터의 활용가능성과 한계점에 대해 분석함으로써 활용가치 측면과 예측가능한 문제점 보완을 통해 결론을 도출하는데 근거자료로 활용한다. 끝으로 제4장에서는 본 연구의 핵심으로서 범죄예방을 위한 법·제도적 개선방향을 제시함으로써 결론을 이끌어내도록 한다. 특히, 법적 대책으로 제시가 되고 있는 개인영상정보보호법안 및 빅데이터 개인정보보호 가이드라인에 대한 의미도 살펴본다. 이러한 연구 진행을 위해 본 연구주제와 유사한 선행연구 자료를 활용한 문헌조사방법론과 결론을 도출함에 있어서는 귀납적 논증방식 및 비교법적 고찰방법을 병행한다.

Ⅱ. 빅데이터 및 사물인터넷의 의의와 현황

여기에서는 빅데이터와 사물인터넷의 의미에 대해서 살펴보고, 현재 실태와 사례 등을 통해 현황을 파악해 본다. 특히 범죄예방 측면에서 두 도구가 얼마나 기여할 수 있을지에 대한 활용 가능성 측면과 어떠한 방향으로 적용될 수 있을지에 대한 방법적 측면에서 구체적으로 정리한다.

1. 빅데이터 및 사물인터넷의 개념

1) 빅데이터의 개념

빅데이터의 출현은 인터넷 환경의 개선과 함께 인터넷 매체의 발달, 스마트기기의 광범위한 보급, SNS 이용자의 급속한 증가 등으로 인해 기하급수적으로 늘어난 데이터의 양적확보에 따른 것이다. 그러나 빅데이터가 단순히 데이터를 수집·축적하는 역할로 그치는 것이 아니라, 데이터 안에서 겉으로 드러나지 않은 규칙적인 흐름을 발견해 냄으로써 초현실을 감지할 수가 있기 때문에 곧 도래할 미래를 예견하여 현재 민간 분야 외에도 행정, 복지, 재난, 범죄

로소프트가 정의하는 사물 인터넷은 오히려 빅데이터의 정의에 가깝게 느껴진다. 사물 인터넷의 본질은 사물로부터 수집되는 수많은 데이터를 활용하는데 의의가 있는 것이기 때문에 빅데이터야말로 사물 인터넷의 가치를 나타낸다.

예측 등 공적 분야에서도 다양하게 활용되고 있는 것이 사실이다.[6] 이에 따라 이러한 빅데이터의 개념을 정리하면 아래 표와 같다.[7]

<빅데이터의 다양한 개념>

연구	개념
Mckinsey(2011)	기존의 데이터베이스 소프트웨어로 저장 · 관리 · 분석할 수 있는 능력을 벗어나는 규모의 데이터 셋으로 규정함
IDC(2011)	다양하고 거대한 규모의 데이터를 빠른 속도로 저장 · 발견 · 분석함으로써 경제적으로 가치를 창출하도록 고안된 새로운 기술
Body&Crawford (2012)	대규모의 데이터 셋을 모으고, 분석하고, 연결 및 비교하는 컴퓨터 기술의 정확성을 극대화 함
Wigan&Clarke (2013)	특정한 대량의 데이터 셋을 의미하는 것뿐만 아니라, 다양한 정보원에서 얻는 데이터를 통합하고, 나아가 데이터를 관리하고 분석하는 기술
국가정보화전략위원회 (2011)	대용량 데이터를 활용 · 분석하여 가치 있는 정보를 추출하고, 생성된 지식을 바탕으로 능동적으로 대응하거나 변화를 예측하기 위한 정보화기술

위에서 정리한 바와 같이 빅데이터에 대한 다양한 개념정의는 표현에서 차이가 있지만, 본질적인 내용상 차이는 없어 보인다. 다만, 2011년 국가정보화전략위원회의 개념 정의가 빅데이터의 의미를 명확하게 규정하고 있는 것으로 생각한다. 빅데이터에서 핵심적인 사항은 대용량 데이터에 의한 가치 있는 정보 추출과 이를 바탕으로 한 미래예측 기술 등이기 때문이다.

2) 사물인터넷의 개념

사물인터넷은 기존의 유선통신기반 인터넷 및 모바일 인터넷 보다 한층 더 진화된 단계의 인터넷을 의미하는데, 초기 유선통신 시대의 PC와 같은 사물간의 연결을 통해서만 데이터 교환이 발생했고, 매개체로서 사람의 개입이 요구되었다. 그러나 그 이후 무선통신기술의 발달로 인해 사람과 사람, 사람과 사물, 사물과 사물로 통신 가능 범위가 확대되었고, 나아가 사물 간의 자율적 통

6) 임상규, "빅 데이터를 활용한 스마트 재난관리전략", 「한국위기관리논집」 제10권 제2호, 위기관리 이론과실천, 2014 참조.
7) 오세연 · 이재영, "IOT와 Big Data의 연계를 통한 범죄예방 활용방안", 「한국콘텐츠학회지」 제13권 제1호, 한국콘텐츠학회, 2015, 44면 참조.

신도 가능한 사물통신(Machine to Machine, 이하 M2M으로 약칭함.)으로 발전하기에 이르렀다. 여기에서 M2M을 통해 주요 구성 요소 간 센싱, 제어, 정보 교환 및 처리 등이 가능한 지능적 관계가 형성되고, 이것이 서비스 형태로 변환되는데, 사물인터넷은 이러한 M2M의 개념이 무선통신을 넘어 인터넷 구조상에 적용됨으로써 현실과 가상세계의 모든 정보와 상호작용하는 개념으로 진화된 차세대 인터넷 환경인 것이다.[8][9]

따라서 본 연구에서는 사물인터넷의 정의와 범위파악을 위해서 기존 M2M과의 구분되는 특성을 정리하고자 개념 간 차이점을 개념의 '관계'와 연결의 '대상 및 방식'에 따라 정리했다. 먼저 '관계'란 M2M과 사물인터넷 개념의 선행성, 상하위성이 존재하는가 여부를 의미한다. 분석결과 이 부분은 연구자의 관점에 따라 상이한 태도를 보이고 있다. 다만, 어느 정도 간추려 보면 두 개념 간 관계의 선행성이 존재하기에 차이가 발생한다는 관점이 존재하는데, 이는 M2M은 단순히 사물인터넷이 나오기 전의 패러다임이기 때문에 상하위적 관계는 존재하지 않는 다는 것이다.[10] 한편, M2M을 사물인터넷의 기반기술로 파악하고, 그 관계에 상하위성이 존재한다고 파악하는 관점도 있는데 이들은 M2M에서 API[11]기술이 발전되어야 사물인터넷이 가능해지기 때문에 M2M은 사물인터넷의 선행기술이며, 그 결과 상하위적 관계도 존재한다는 입장도 있다.[12] 이러한 '대상 및 방식'은 M2M과 사물인터넷이 연결되는 대상과 방식이 어떻게 상이한가에 대한 관점으로 분류할 수 있는데, 이것은 연결의 주체, 연결의 능동성 여부, 연결의 정도, 연결방식으로 그 논의를 재정리할 수 있다.[13][14]

---

8) 주대영 · 김종기, 「초연결시대 사물인터넷(IOT)의 창조적 융합 활성화 방안」, 산업연구원, 2014, 22면.

9) 유상근 · 홍용근 · 김형준, "스마트모바일 서비스: M2M 기술 및 표준 동향", 「전자통신동향분석」 제26권 제2호, 전자통신연구원, 2011 참조.

10) Atzori, L., Antonio, I., Giacomo, M, "*The Internet of Things: ASurvey*", Computer Networks 54(15), 2011, pp,2787-2805.

11) API(Application Program Interface)란, 프로그램 또는 애플리케이션이 운영 체제에 어떤 처리를 위해서 호출할 수 있는 서브루틴 또는 함수의 집합이다. 윈도우 API의 경우 C, C++, 파스칼 등과 같은 언어에서 윈도우를 만들고, 파일을 여는 것과 같은 처리를 할 수 있도록 1,000여개 이상의 함수로 구성되어 있다. 명령어의 집합으로 애플리케이션 프로그램에서 오퍼레이팅 시스템의 기본적인 기능을 사용할 필요가 있을 때에 여기에서 명령어를 호출한다.

12) Ovidiu, V., Peter, F., Anthony, F, "*The Internet of Things 2012: New Horizons*", IERC 3rd edtion of cluster book; Zorzi, M., Gluhak, A., Lange, S., Bassi, A(2010), "*From Today's Intranet of Things to a Future Inter oh things*", Wireless Communications. IEEE 17(6), 2012.

2. 사물인터넷을 기반으로 한 빅데이터 기술

사물인터넷을 기반으로 한 빅데이터 기술은 센서 네트워크를 포함, Wi-Fi, 휴대전화망, 무선망 상에 수많은 물리적인 사물들의 연결을 전제로 한다. 이렇게 연결된 사물들은 서로 통신하고, 지능서비스를 위한 데이터를 생성해 내며 방대한 분량의 빅데이터를 통해 새로운 가치를 창출해내고 있는 것이다.[15] 기존의 시스템이 사실적 데이터를 수집하여 빅데이터화 하는 기초적 진단·분석에 국한되었다면 향후 시스템은 재난, 재해, 범죄 등이 일어난 사회적 문제를 빅데이터화 하여 미래에 일어날 가능성 있는 이슈를 사전에 예측하고, 더 나아가 해결 방법까지도 고민하고 대안을 제시할 수 있을 것으로 기대된다. 따라서 범죄의 예측과 예방 차원에서 사물인터넷을 통한 범죄나 범죄자를 색출하고, 이러한 사실을 빅데이터화 하여 발생할 범죄를 사전에 차단시킬 수 있다면, 적어도 완벽하지는 않더라도 사전에 차단할 수 있는 확률을 높일 수 있다면 범죄발생률을 감소시킬 수 있을 뿐만 아니라, 경제적 측면에서도 범죄피해에 대한 사회적 비용을 줄일 수 있을 것이다. 또한 근본적으로 국민들의 범죄에 대한 두려움 감소효과와 치안에 대한 신뢰도 상승, 궁극적으로는 삶의 질이 월등히 향상될 것으로 생각한다.

위와 같은 사항을 바탕으로 범죄예측에 대한 선행연구 자료들을 분석해보면, 범죄자와 피해자의 거주지 사이의 공간적인 분포패턴을 연구하여 특정패턴의 원인을 찾고, 도시공간구조의 특성을 파악하여 범죄발생 가능성을 평가한 연구가 수행되고 있다. 그리고 범행 위치의 공간적인 분포와 범죄발생의 시간적 분포 특성에 따라 시·공간 패턴을 유형화 하여 범죄패턴과 특징을 분석하여 범죄의 위치를 예측하는 연구도 수행되고 있는 것으로 파악된다. 이를 위해 범죄

---

13) 여기에 대한 보다 구체적인 내용은 미래창조과학부, 「사물인터넷 산업 실태조사 및 시장분석 연구」, 2014.10, 6면 이하 참조.

14) 일반론적으로 사물인터넷이라는 용어는 1999년 처음 사용되었고, 현재는 앞서 언급한 바와 같이 통신망을 이용하여 사람과 사물, 사물과 사물 간 지능통신을 할 수 있다는 사물지능통신(M2M) 개념을 인터넷으로 확장하여 현실과 가상세계의 모든 정보들이 상호작용하는 방식을 지칭하는 개념으로 사용된다. 다시 말해서 사물인터넷은 통신망에서 사람과 사람, 사람과 사물, 사물과 사물 간을 자율적·지능적으로 시간, 공간, 대상의 제약 없이 연결함으로서 모든 정보들이 상호 작용할 수 있도록 만드는 방식으로 이해되고 있다; ITU Internet Reports, *The Internet of Things*, November 2005, p.3.

15) 박현·김세한, "IoT 기반 Big Data 기술 동향", 「한국전자파학회지」 통권 제98호, 한국전자파학회, 2013, 44면.

자가 주로 활동하는 거점 지역과 이동하는 길 주변의 범죄 발생 현상에 대해 범죄자의 주된 거주지나 활동반경을 분석하는 지리학적 프로파일링이 활용되거나 컴퓨터 등을 사용하여 지표상의 다양한 지리정보를 종합적으로 처리하는 시스템을 활용하여 특별한 지역에서 행해진 범죄를 저장하고 이를 경찰의 탐색수단에 이용하는 GIS도 범죄예측 수단으로 활용되고 있다.[16][17]

3. 빅데이터 및 사물인터넷을 활용한 범죄예방 기대효과 및 해외 사례

1) 빅데이터를 활용한 범죄예방 기대효과 및 사례

(1) 산타 쿠로즈 경찰서의 프레드폴(PerdPol)

프레드폴 소프트웨어의 핵심은 특정 시간대에 범죄가 증가할 것으로 예상되는 지점을 지속적으로 찾아내는 것이다. 이를 위해 컴퓨터 알고리즘은 과거 범죄발생 데이터베이스를 이용해서 미래 발생확률을 150×150 미터 격자지도에 표시해 준다. 범죄 데이터베이스에는 범죄유형과 발생 장소·시간이 필요한데, 확률을 계산할 때 최근 범죄일수록 더 큰 가중치가 부여된다.[18] 프레드폴 예측기법의 특징은 순전히 범죄정보(유형, 위치, 시간)외에는 어떤 개인정보나 지역사회 데이터가 이용되지 않는다는 점이다. 따라서 분석과 이해가 비교적 용이할 뿐만 아니라 인권문제나 프라이버시 논란으로부터 자유로운 장점이 있다. SCPD 프레드폴은 침입절도에 있어 특히 효과적인 것으로 나타났다. 프로그램이 시행된 2011년 7월과 그 이전인 2010년 7월을 비교해보면 침입절도가 27% 감소했고, 시행 전후 6개월을 비교했을 때 305건에서 263건으로 14% 감소했다. 일반적으로 재산범죄가 폭력범죄에 비해 예측이 정확하고, 특히 침입범죄는 범행을 합리적으로 계획하기 때문에 예측과 예방이 효과적인 것으로 판단되었다.[19]

---

16) 오세연·이재영, 앞의 논문, 45면 참조.

17) 김경원, "빅 데이터를 활용한 경찰의 범죄예측 활성화 방안", 동국대 대학원, 석사학위논문, 2015 참조.

18) Bachner, J., *Predictive Policing: Preventing Crime with Data and Analytics*, IBM Center for The Business of Government, 2013, p.25.

19) Ibid, p.26.

(2) Shreveport 경찰서의 파일럿(PILOT)

산타 크루즈 경찰서의 프레드폴이 범죄정보만을 이용한 핫스팟 예측 및 예방 시스템인 반해, 루지애나 Shreveport 경찰서의 PILOT은 범죄 이외의 정보도 사용하고 있는 핫스팟 예측 및 예방 시스템이다. Shreveport 경찰서는 실험주제를 "정보기반개입대상 에측(PILOT: Predictive Intelligence-Led Operational Targeting)"으로 정하고, 범죄와 무질서에 관련된 최근 자료를 바탕으로 범죄 증가가 눈에 띄는 지역을 1개월 먼저 예측하고자 했다. 개입대상 범죄들에 대해서는 7일과 14일에 걸친 시차변수가 만들어졌고, 다른 예측변수(위험요인)들에 대해서는 한 달에 걸친 시차변수가 만들어졌으며, 911 신고전화와 경범죄에 대해서는 공간시차변수들도 만들어졌다. 이렇게 구축된 데이터를 이용해 두 가지 예측 기법을 적용했는데 이를 위해 실험지역을 약 37제곱미터 격자로 구분하였다. 첫 번째 기법은 로지스틱 회귀분석으로서 개입대상 범죄가 발생할 가능성을 각 셀별로 도출하였다. 두 번째 기법은 위험지역모델링으로서 먼저 각 셀에 분포하는 범죄와 관련이 큰 지리적·공간적 특성을 찾아냈다. 그런 다음 이러한 특성 하나 당 1점을 매기는 방식으로 각 셀의 점수를 합산함으로써 높은 점수가 부여된 셀이 고위험지역으로 결정되었다.[20]

(3) 뉴욕 경찰청(NYPD)의 Domain Awareness System(DAS)

앞의 두 사례가 예측을 위주로 하는 반면, DAS는 실기간 감시와 대응을 위주로 하는 특징이 있다. NYPD는 공공안전 및 보안을 유지하고 테러활동을 탐지하고 예방하기 위해 DAS 시스템을 개발하였다. 예측적 경찰활동이 미래를 예측하기 위해 데이터를 사용하는 반해, 컴퓨터 감시시스템은 도시 내의 수많은 데이터 소스를 이용해 현재를 보여준다. DAS는 이전의 개별적 분석과는 차원이 다르게 사람·사물·장소 간 연관성을 밝혀내수 있는 정보를 실시간으로 제공한다. 이것은 비디오 분석 소프트웨어를 이용한다. NYPD에 따르면, DAS를 이용해 용의자와 관련된 차량이 현재 어디에 있는지, 과거 수개월 동안 어디에 있었는지를 추적할수 있다고 한다. 또한 DAS는 자동차번호판을 용의자 정보와 비교해서 차량 소유자와 관계된 모든 범죄기록을 즉시 제공할수 있다.[21] NYPO는 공공안전 및 프라이버시 가이드라인을 제작해서 DAS의 합법적

20) 권양섭, "범죄예방과 수사에 있어서 빅데이터 활용과 한계에 관한 연구", 「법학연구」 제17권 제1호, 한국법학회, 2017.3, 3-4면.

인 이용과 데이터의 적절한 접근 및 관리에 대한 정책절차를 마련했다. 특히, 프라이버시에 대한 적절한 보호를 위해 기술, 운영, 법, 정책, 관리감독 등 안정장치를 마련했다. 가이드라인에 따르면 DAS는 뉴욕시 헌장 제18장 제435(a)조에 의거해서 개발되었다.

2) 사물인터넷을 활용한 범죄예방 기대효과 및 사례

사물인터넷 기술은 범죄예방에 국한하여 활용되지 않고, 필요한 경우 범죄수사, 범죄정보공유 등 치안분야의 다양한 영역에서 서비스 제공하는 것이 가능해졌다. 우선 범죄예방 분야에서 제공 가능한 서비스는 긴급연락망, 범죄예측, 범죄 발생 예측기반 순찰 강화, CCTV 설치 필요지역 도출 등이 있고, 범죄수사 분야에서는 이동 가능 경로 CCTV 자동분석, 상태 모니터링 등, 그리고 정보공유에서는 시간에 따른 범죄지도와 SNS 망을 활용한 범죄정보 공유 등의 서비스를 제공할 수 있다.[22]

특히, 앞서 정리한 DAS 사례[23]에서 볼 수 있듯이, 빅데이터 기술을 핵심으로 하고 있는 IoT 서비스는 제공되는 서비스 형태에 따라 수많은 기대효과를 가져올 수 있으며, 특히 급속하게 변화하는 미래치안환경의 변화에 적합한 솔루션을 제공할 수 있다. IoT 기술을 활용한 범죄예방 사례와 기대효과는 아래 표와 같다.

---

21) Joh, E.E., "*Policing by Numbers: Big Data and the Fourth Amendment*", Washington Law Review, 89:35, 2014, pp.48-49.

22) 아이뉴스, 범죄 예방에 나서는 IT 기술 기업들: 스웨덴서 '클릭뷰'로 살인범 검거, MS-뉴욕시 테러 감시 시스템 구축, 2014.10.16. 기사발췌.

23) IoT 기술의 도입을 통하여 가장 기대되는 치안분야는 범죄예방이며 IoT 기술을 활용한 대표적인 사례로는 뉴욕시의 DAS(Domain Awareness System)라는 대테러 감지시스템이다. DAS는 맨하탄 지역에 설치된 4천여 대 CCTV, 600여대 방사능 감지기, 100여 대의 자동차번호판 인식장치를 연계해 의심스런 사람이나 물품, 차량 관련 정보를 분석하는 시스템이다. 범죄나 테러 현장 주변 CCTV 영상을 통해 범죄용의 차량 정보를 포착하면 DAS를 통해 해당 도시 전역의 실시간 CCTV 영상을 분석해 용의 차량 위치를 파악하고, 현장경찰과 소방서 등 관련기관에 즉시 제공해 경찰이 이를 추적할 수 있도록 지원한다. 도로를 지나는 차량 중 수배차량이나 테러의심 차량이 있는 지도 번호판으로 확인한고, 보스턴테러사건처럼 건물 출입구에 가방을 내려놓는 식의 의심스런 행동도 판독한다. 무엇보다 CCTV화면, 신고전화, 용의자 체포기록, 자동차 번호판 추적 결과, 방사선 수치 등 방대한 데이터를 클릭 한 번에 확인할 수 있다는 점이 장점이다.

<IoT 기술을 활용한 범죄예방 사례와 기대효과>[24]

구분	활용방법	기대효과
범죄예방 정보공유 서비스	•안심태그와 GPS 등을 기반으로 보호대상자의 위치와 이동경로 정보를 확인하여 위험 알림 서비스를 제공 •기존 데이터들을 바탕으로 범죄분석을 실시하여 '범죄발생가능지역이나 시간대' 등에 대한 정보를 제공하여 범죄예방효과 극대화	•범죄에 노출되기 쉬운 어린이나 여성, 노인들의 안전을 보장하기 위해 다양한 방법으로 범죄예방정보 공유하여 도시안전 지수를 높임
112 영상제공 서비스	•긴급 출동하는 경찰관에게 U-City센터에서 확보한 CCTV영상을 바탕으로 현장사진이나 범인 도주경로 정보, 증거자료 등을 제공	•납치 · 강도 · 폭행 등 긴박한 강력사건 신고를 받고 출동하는 경찰관이 도착 전에 현장 상황을 전파 •미리 파악된 정보를 바탕으로 범인 검거, 위험방지 등 적절한 조치를 취할 수 있음
119 긴급출동 지원서비스	•화재 발생 시 화재지점의 실시간 CCTV 영상, 교통소통 정보 등제공 •재난상황 시 신속한 재난정보 제공	•화재 진압 및 인명 구조를 위한 골든타임 확보 •재난상황 전파와 상황복구에 신속한 대응을 지원
공중전화 안심부스	•범죄 위협을 받은 시민이 대피하면 자동으로 문이 닫혀 외부와 차단되고 싸이렌과 경광등이 작동	•공중전화 부스를 범죄로부터 대피 •CCTV녹화 및 스마트 미디어기능을 통해 범인 검거에도 활용
스마트 가로등	•에너지 절약형 LED 조명에 CCTV 기능으로 무선 인터넷 중계가 가능하며 거리미관 향상뿐만 아니라, 대민안전 방범 기능 강화와 에너지 절감을 통한 첨단디지털 공간을 조성	•조도가 증가하여 범죄자로 하여금 범행심리를 위축시키게 됨 •미관상 효과뿐 아니라 방범기능도 갖추고 있어서 시민들의 범죄두려움을 감소시키는 효과
미아방지 및 해상안전 서비스	•치매환자나 어린이 등에게 웨어러블 밴드 등을 보급하여 미아방지를 예방 •해상용 드론 등을 통해 해수욕장 및 해상지역에 실시간으로 응급구난 활동은 물론 선제적인 방제활동으로 안전사고 발생을 예방	•실종 및 조난, 구조에 필요한 인력과 시간을 절약할 수 있음 •실종자 수색에 드론을 활용할 경우 수색하기 힘든 범위까지 빠르고 신속하게 수색이 가능하여 실종자 및 조난자의 안전에 기여

(1) 미국의 샷스포터를 이용한 총기사건 범죄예측

개인총기사용이 불법인 우리나라와 달리 미국은 총기규제가 어느 정도 자유롭기 때문에 총기로 인한 사고와 범죄가 매년 증가하고 있다. 이에 미국 정부에서는 음향감지장치를 곳곳에 설치해 총소리를 바로 잡아내고 정확한 위치를 확인하는 시스템인 샷스포터를 개발하였고, 이 시스템은 공공장소에서 총이 발사된 시간을 인식하여 경찰이 발사한 총의 위치를 파악하는데 도움을 준다.

24) 김도우, "치안환경 변화에 따른 안전도시 도입방안 : 사물인터넷과 범죄예방환경설계를 중심으로",「한국셉티드학회지」제7권 제1호, 한국셉티드학회, 2016.5, 43면.

SST라는 기업이 개발한 이 시스템은 시내 마을 대학 캠퍼스 내에 설치되어 있는 커넥티드 마이크를 이용하였고, 마이크의 감지범위는 최대 10평방 마일로 '사실상 폭발하는 소리'의 범위를 측정하도록 개발되었다. 마이크는 총성이 들리면 기록한 데이터를 경찰서의 컴퓨터로 전송하여 소리가 마이크에 도달한 시간을 측정하여 데이터화하여 총의 위치를 추정한다.[25] 이러한 미국의 사례를 면밀히 검토하여 우리도 사물인터넷을 활용한 범죄예방 방안을 마련하는 것이 필요하다.

(2) 런던경찰청의 오아시스(OASYS) 범죄예측시스템

영국 런던경찰은 5년간 범죄를 저지른 전력이 있는 조직폭력범죄자의 범죄기록과 이들이SNS에 올리는 글 등을 분석해 범죄가능성을 예측하는 오아시스(OASYS)' 프로그램을22시간 시범 운용 중이다. 우범자가 선동적 글을 올리면 이들과 온라인 상에서 연결된 사람들의범죄기록 등을 추적해 추가 범행가능성을 분석하여 범죄자에 대한 데이터베이스를 기초로 사회관계망 서비스(SNS) 동향까지 분석해 우범자를 사전에 가려내는 빅데이터 분석능력까지 갖추고 있다. 이 시스템의 목적은 특정인 검거보다는 재범가능성이 큰 범죄자를 파악하여 범죄를 사전에 예방하는 것이다.[26]

Ⅲ. 범죄예방을 위한 빅데이터의 활용가능성과 한계

여기에서는 범죄예방을 위해 빅데이터의 활용 가능성 측면과 그 한계점에 대해서 살펴보도록 한다. 범죄예방 도구로서 사물인터넷에 대한 의의와 현황 등에 대해서는 앞서 정리했는데, 이는 필연적으로 빅데이터를 기반으로 하기 때문에 서론부분에서 미리 밝힌 바와 같이 본 장에서는 빅데이터 활용 측면과 한계에 대해서 살펴보는 것으로 그 범위를 한정하여 진행한다.[27]

---

25) 오세연 · 이재영, 앞의 논문, 45면 참조.

26) 위의 논문, 46면 참조.

27) 디지털 데일리, 빅데이터와 IoT는 한몸, 2014. 2. 12. 기사 발췌; 빅데이터를 정의할 때 3V라고 말한다. 데이터의 크기(Volume), 데이터가 새로 생성되는 속도(Velocity), 데이터 종류의 다양성(Variety) 면에서 기존과 차원이 다른 모습을 보여주는 것을 빅데이터라고 부른다. 이같은 빅데이터는 사물인터넷(IoT) 시대에 더욱 중요한 요소가 됐다. 센서네트

1. 빅데이터의 활용 가능성 검토

범죄예방을 위해 빅데이터 활용이 어떠한 의미를 갖는지 검토해보는 것이 우선적 과제일 것이다. 빅데이터 기술이 범죄예방 및 해결을 위한 대안적 수단으로서 가치가 있는지 파악하기 위해서는 우리 현행법 체계에서 개인정보에 대한 분명한 확인이 선행되어야 하고, 빅데이터를 활용하는데 있어서 목적과 정보주체를 구별하여 이에 부합할 수 있는 합리적인 활용방안 모색이 뒤따라야 할 것이다.

기술의 활용과 그 효율성은 그 토대가 되는 현실 내지 상황에 대한 정확한 인식을 전제로 할 때 담보된다. 따라서 빅데이터 기술의 활용을 논하기 위해서는 현재 우리나라의 정보현실 내지 상황을 고려해야 한다. 실제로 빅데이터 기술이 먼저 활용되기 시작한 영미권 및 유럽의 경우에는 개인을 식별할 수 있는 고유식별정보 또는 민감정보 등 개인정보가 우리나라와 같이 국가에 의해 집약적으로 생성 · 수집 · 관리되지 않았기 때문에 산재(散在)해 있는 다양한 정보들을 한데 모아서 그 속에서 유의미한 정보가치를 창출 · 이용해야 하는 현실적 필요성이 있었고, 그로 인해 정보수집 및 분석기술로서 빅데이터기술이 등장하였다. 그러나 빅데이터 기술의 발달로 방대한 정보의 수집 · 통합 · 분석이 가능하게 됨에 따라 일반적인 경향 내지 성향을 파악하는 것을 넘어 특정 개인을 식별할 수 있는 수준이 되고, 개인정보의 보호 필요성에 대한 인식이 점차 확립됨에 따라, 최근에는 오히려 빅데이터의 활용을 제한하는 방향으로 입법이 이루어지고 있다.

한편 우리나라의 경우는 고유식별정보 및 민감정보를 포함한 개인정보가 국가의 주도로 생성 · 수집 · 처리되어온 역사적 사실과 현재까지도 광범위한 생활영역에서 개인정보의 요청과 그에 따른 제공 · 이용 등이 빈번히 이루어지고 있다는 점에서 영미 또는 유럽의 정보현실과는 그 토대부터 전혀 다른 상황에 놓여 있다. 특히 방대한 정보의 집적을 전제로 하는 빅데이터의 특성상 수집과정에서 개인정보가 포함될 가능성이 매우 높고, 설사 수집과정에서 개인정보를 기술적 수단을 통해 배제하여 비식별 정보만을 수집대상으로 설정한다고 하더라도 통합 및 분석과정에서 비식별정보간 또는 비식별정보와 식별정보간의 결

워크에서 쏟아지는 실시간 데이터들은 V3의 특징을 고스란히 갖고 있기 때문이다. 이 데이터들은 끊임없이 빠른 속도로 쏟아지고, 기존의 정형 데이터의 모습을 갖추고 있지 않다. 데이터의 크기는 두말할 나위도 없다.

합에 의한 '정보의 개인화' 가능성이 상당히 존재한다. 또한 빅데이터 기술의 도입과 활용이 본격화되기 이전에 개인정보보호를 위한 개별 법제를 이미 마련해 놓은 우리나라의 법 현실 또한 고려되어야 한다. 이는 비록 공공의 이익 내지 공익적 목적, 즉 범죄예방을 위해 개인정보를 활용할 필요성이 인정되는 경우에도 마찬가지로 직면할 수 있다.[28]

1) 범죄예방 차원에서 불특정 다수에 대한 빅데이터의 활용 가능성

빅데이터 기술을 활용함에 있어서는 데이터의 분석결과를 어떠한 영역에서 무슨 목적과 용도로 활용할 것인지 그 방향성이 중요한 의미를 갖는다. 특히 빅데이터를 형성하는 자료의 성격과 내용이 고려되어야 하는데, 만약 이에 개인정보가 포함될 가능성이 있는 경우에는 더욱 목적과 용도에 따라 빅데이터 활용의 폭과 범위 그리고 한계를 달리 설정할 필요성이 있다.

비록 치안유지 혹은 일반예방 목적이라 하더라도 구체적인 혐의 없이 불특정 일반인의 정보를 대량으로 수집ㆍ보관ㆍ관리하고, 빅데이터 기술 통해서 개인화의 수준까지 분석하는 것은 정보차원에서의 '사찰' 내지 '감시'에 해당하고, 이는 개인의 정보자기결정권[29]은 물론 프라이버시에 대한 심각한 침해라는 점에서 허용될 수 없다.[30][31] 이러한 이유에서 불특정 다수를 대상으로 한 범죄예방 목적의 정보 활용에 있어서는 각 단계별로 엄격한 제한과 규범통제가 필요하다고 생각한다.

---

28) 김봉수, "빅데이터의 범죄예방 목적 활용과 규범적 한계", 「법학논총」 제36권 제4호, 전남대학교 법학연구소, 2016.12, 308면 이하 참조.

29) 김일환, 「초연결사회에서 개인정보보호법제 정비방안에 관한 연구」, 2017 한국법제연구원ㆍ법제처ㆍ한국공법학회ㆍ한국헌법학회 공동학술대회(4차 산업혁명에 따른 입법 대응 전략 모색)자료집, 2017.4.7, 60-61면 참조; 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체 스스로 결정할 수 있는 권리이다. 즉 정보 주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리이므로 개인정보자기결정권은 개인관련정보의 사용과 공개에 대하여 원칙적으로 개인 스스로 결정할 권리이다. 따라서 누가, 무엇을, 언제 그리고 어떠한 경우에 자기에 관하여 아는지를 시민들이 더 이상 알 수 없는 사회질서 및 이를 가능하게 하는 법질서는 개인정보자기결정권과 조화되지 못한다. 이것이 곧 개인정보자기결정권의 헌법상 의의와 내용이다.

30) 헌재 1998.5.28. 96헌가5; 헌재 2003.10.30. 2002헌마518; 헌재 1990.9.10. 89헌마82; 헌재 2013. 5.30. 2011헌바360, 2012헌바56(병합); 헌재 2004.6.24. 2002헌가27; 헌재 2005.5.26. 2004헌마190.

31) 김봉수, 앞의 논문, 309면.

먼저 첫째, 정보수집과 관련하여 수집대상정보의 범위는 '비식별정보'로 제한될 필요가 있다. 다시 말해 식별가능한 개인정보, 예컨대 고유식별정보, 민감정보, 식별가능정보 등은 수집을 제한해야 되고, 둘째, 수집된 정보를 저장하고 보관하는데 있어서는 일정한 제한 기간을 설정하되, 3개월 이내의 단기간으로 하고 그 기간이 도래하거나 목적을 달성하게 되면 자동적으로 소멸될 수 있도록 강행규정을 명확히 마련하는 것이 요구된다. 왜냐하면 구체적인 범죄 관련성이 없음에도 불구하고 불특정 다수의 정보를 향후 있을지도 모를, 즉 없을 수도 있는 범죄발생을 대비하여 무분별하게 대량으로 수집하고 저장·보관하여 정보화하는 것은 정보 활용 원칙 중 비례원칙 등에 명백히 위반되므로 아무리 범죄예방이라는 공익적 목적범위 이내라고 할지라도 용인될 수 있는 한계점을 이탈한 것이라고 생각한다. 셋째, 정보를 활용하고 처리하는데 있어서는 비록 수집대상이 비식별정보로 제한된다고 하더라도 대량의 정보를 집적시키고 정보화하게 되면 결합가능성이 커질 수 있기 때문에 이로 인해 수집정보의 가공 및 처리 단계에서 개인정보성을 취득하는 것이 가능해진다. 이러한 이유에서 빅데이터 기술을 활용하기 이전 및 이후, 즉 빅데이터 분석 이전의 자료상태에서 뿐만 아니라 분석 후의 결과물에 대해서도 반드시 암호화 내지는 익명화 과정을 적용시켜야 할 것이다. 또한 빅데이터 기술을 통한 분석수준 역시 규범적·기술적으로 제한하여 범죄 관련한 다중의 행태 내지 경향성을 분석·파악하는 정도로 그 활용의 한계를 명시함으로써 개인화되지 않도록 주의하는 것도 뒷받침되어야 한다. 넷째, 이 경우에 있어서는 수집·저장·활용(가공)·분석된 정보를 목적 외 이용하거나 제3자에게 제공·이전하거나, 공유하는 일체의 행위를 엄격하게 금지하고 위반 시에는 엄중한 벌칙적용 규정의 마련도 필요할 것이다.[32]

이상과 같은 내용을 요약하자면, 범죄예방을 목적으로 한 불특정 다수에 대한 빅데이터의 활용은 공익적 차원에서 이뤄지는 것일지라도 정보주체의 정보인권 보장과의 법익균형성을 최대한 고려해야 되고, 이를 위해 형평성에 맞는 적절한 통제가 필요할 것이다. 다만 너무 과도한 제한 및 통제가 가해질 경우에는 공익적 목적을 달성할 수 없으므로 이 또한 간과해서는 안 될 사항이다. 그리고 빅데이터 기술을 활용한 분석결과물 역시 암호화 과정을 통해 가능한 개인을 식별할 수 있는 도구로 사용되지 않도록 해야 되고, 그 용도 역시 범죄

32) 김봉수, 앞의 논문, 309-301면 참조.

예방을 위한 대책 수립 등에만 활용되도록 그 범위를 명확하게 규율할 필요가 있다. 또한 비식별정보의 수집이라 하더라도 그 수집 및 활용에 대한 별도의 강행규정을 두어 그 실효성(實效性)을 확보하는 것이 중요할 것이다.

2) 범죄수사 과정에서 특정인에 대한 빅데이터의 활용 가능성

(1) 수사 및 재판절차에서 특정인의 특수성

앞서 살펴본 불특정 다수와는 달리, 피의자 내지 피고인과 같은 특정인은 구체적인 사건과 관련하여 범죄혐의가 의심 또는 인정되는 자라는 점에서 일반인과 구별되고, 형사법 영역에서 피의자 및 피고인은 헌법 제27조 제4항 및 형사소송법 제275조의 2에서 명시하고 있는 무죄추정원칙에 따라 보호된다는 점에서 재판을 통해 형이 확정되어 수감된 수형인과도 그 지위가 다른 것이 사실이다. 한편 피의자 및 피고인은 구체적 사건에서 범죄혐의가 있는 자이고, 향후 재판부의 판결에 의해 형이 확정이 될 가능성이 항상 존재하고 있다는 점에서 앞서 언급한 불특정 다수인 일반인 수준에서 취급하는 것도 범죄수사 및 예방 차원에서 볼 때, 불합리한 것임에 틀림없다.

이에 따라 수사 및 재판절차에서 특정인의 정보를 수집·보관·처리함에 있어서는 실질적 조화에 기여할 수 있도록 빅데이터의 활용 가능성 및 범위를 달리해야 될 것이다. 이에 여기에서는 피의자·피고인이 형사절차의 당사자로서 당해 범죄를 구성하는 요건 및 성질 등에 주목할 필요가 있다.

(2) 범죄유형에 따른 개인정보 활용범위 구별

먼저 관련된 범죄의 성격이 최근 국가적·사회적 문제가 되고 있는 '테러범죄'처럼 예방의 필요성이 크고, 피의자 및 피고인의 법익과 비교하여 월등하게 우월한 공익성을 가지고 있을 때에는 비록 무죄추정을 받고 있는 피의자·피고인의 개인정보라 하더라도 수집 및 처리가 허용되어야 한다. 단, 저장기간을 정하여 일정한 기간이 경과된 후에는 자동적으로 파기토록 제한을 둠으로써 정보인권 보장적 측면을 고려해야만 한다. 그리고 행위자의 특정한 소질 및 성향이 발현되어 발생하는 범죄군, 예컨대 살인, 아동학대, 강간 등의 경우에는 대부분 동종 범죄경력자에 의해서 범죄가 재발할 가능성이 상당하고, 그 성향에 따라 범죄의 수법 및 태양 등에서 개인화된 특성을 보이는 경우가 많기 때문에 동종

범죄의 예방 및 신속한 수사 차원에서 피의자·피고인의 정보를 수집 및 처리할 수 있도록 해야 한다.[33]

한편 앞서 언급한 범죄 행위자의 성향에서 비롯된 범죄는 아니나, 강도, 절도, 사기, 공갈, 약취·유인, 방화 등과 같이 수법과 방식에 있어서 특정화된 패턴이 발견되는 범죄군에 대한 범죄예방 및 수사 차원에서 개인정보의 수집·보관·처리가 제한된 범위 내에서 활용될 여지가 충분하다고 생각한다.

(3) 엄격한 규범통제 하에서의 활용

앞서 언급한 것처럼, 비록 범죄예방 및 범죄수사에 있어서의 현실적 필요성 내지 효율성이 인정되어 피의자·피고인의 정보에 대한 수집 및 처리가 허용될 수 있다고 할지라도 보다 엄격한 과잉금지의 원칙 내지는 비례의 원칙에 따른 심사에 근거하여 이뤄져야 한다.[34] 다시 말해서 법률적 근거 없이 검·경 등 수사기관 차원의 내부규칙 내지 훈령 차원에서 수권이 이루어지는 것은 개인정보를 침해할 가능성이 짙은 것이 사실이다. 이에 피의자 및 피고인의 정보수집 및 처리에 관한 명확한 법적 근거를 마련할 필요성가 있다. 예를 들면, 수집정보의 범위 및 보관기간, 공유 및 이전, 목적과 용도 등에 관한 구체적 사항을 명문으로 나타내야 할 것이다. 각 범죄별 정보보유기간은 단기와 장기로 구분하여 설정하고, 수집된 정보의 목적 및 용도도 유사 내지는 동종 범죄가 발생하면 피의자와의 동일성 여부를 파악하는 확인목적으로만 활용될 수 있도록 그 활용범위를 한정함으로써 정보의 공유 및 이전 등을 금지하고, 프로파일링에 의한 감시 및 사찰의 도구로 전락되지 않도록 빅데이터를 통해 달성하고자 하는 본래의 목적을 분명히 해야 될 것이다.

2. 빅데이터 활용의 한계점

1) 빅데이터를 분석하는 행위의 형사절차상 한계점

여기에서는 앞서 정리한 내용을 바탕으로 빅데이터 분석을 활용하여 범죄를

33) 김봉수, 앞의 논문, 313면.
34) 헌재 1996.4.25. 92헌바47.

예방하고 수사를 진행하기 위한 절차에서 사용하는 것이 어떠한 한계점을 갖게 되는지 확인해보도록 한다.

먼저 범죄자 검거를 위해 빅데이터 분석 시스템을 통해 정보를 분석하는 행위는 내사에 해당되고, 내사 단계에서는 강제수사가 인정되지 않으므로 강제수사와 임의수사의 구분이 본 시스템의 적법과 불법을 구분 짓는 기준이 될 수 있을 것이다.[35] 아래에서는 강제수사와 임의수사의 판단기준이 무엇인지 분석해보고, 빅데이터 분석 시스템에 의한 데이터 분석행위가 강제수사 성격을 가지고 있는지 판단해 보기로 한다.[36]

임의수사와 강제수사에 대한 구별기준에 대해서는 다양한 학자들의 견해가 전개되어왔다. 특히 최근에는 사회의 변화와 과학기술의 발달로 인하여 입법자가 법을 제정할 당시에는 생각할 수 없었던 다양한 수사방법들이 등장하고, 발전하면서 이러한 것들을 어떤 범위 내에서 어떤 절차에 따라 허용할 것인가 하는 문제가 새롭게 제기되고 있다. 이러한 학자들의 견해를 요약·정리하자면, 형식설은 형사소송법이 명시적으로 강제처분으로 규정한 것만 강제수사에 해당하고 나머지는 임의수사로서 허용된다는 입장이나, 이와 같이 임의수사의 범위를 지나치게 넓게 보는 견해는 현재 찾아보기 어렵다. 이에 반해 실질설은 형식적인 법률을 기준으로 하지 않고 다른 실질적인 표준에 따라 양자를 구별하려는 견해이다. 과거에는 물리적 강제력의 행사 유무에 따라 구별하는 견해도 있었지만 현재로는 상대방의 의사에 반하는가 여부를 기준으로 하는 견해가 일반적이다. 이에 따르면 강제수사란 상대방의 의사에 반하여 실질적으로 그의 법익을 침해하는 처분을 말하며, 반대로 상대방의 법익침해를 수반하지 않는 수사는 임의수사라고 본다. 적법절차기준설은 헌법이 정한 적법절차의 원리에서 파생되는 기본권존중의 관점에서 수사기관의 처분이 법공동체가 인정하는 최저한도의 기본적 인권마저 침해할 우려가 있는 때에는 강제처분으로 보아 영장주의를 비롯한 법적 규율을 받게 된다는 견해이다.[37]

수사기관에 의한 기본권침해의 유무를 기준으로 하면서 상대방이 동의하면 기본권을 침해하더라도 임의수사에 해당한다는 견해인 기본권기준설도 기본적

35) 신양균·조기영, “내사의 개념과 허용범위”, 「형사법연구」 제23권 제3호, 한국형사법학회, 2011, 194면 참조.
36) 권양섭, 앞의 논문, 11면.
37) 위의 논문, 10-12면 참조.

으로 이 견해와 유사하다고 할 수 있다. 실질설은 법익침해에 중점을 두어 상대방의 의사에 반하였는가를 기준으로 강제수사와 임의수사를 구분하고 있다. 반면 적법절차기준설은 실질설에서 한 걸음 더 나아가 수사기관의 처분이 헌법상 개별적으로 명시된 기본권을 침해하거나, 또는 명시되지 아니하였더라도 법공동체가 공유하고 있는 최저한도의 기본권 인권마저도 침해할 우려가 있는 것인 때에는 강제수사에 해당되고 그와 같은 최소한도의 요구범위에 들지 않는다면 임의수사에 해당된다고 보고 있다. 실질설보다 적법절차기준설이 강제수사의 범위를 보다 넓게 인정하고 있다는 점에서 기본권 보호에 더욱 충실하다고 볼 수 있다. 빅데이터 분석 시스템에 의한 데이터 분석행위를 적법절차기준설에 의하여 판단하더라도 강제수사의 영역보다는 임의수사에 포함된다고 보아야 한다. 앞서 언급한 바와 같이 빅데이터 분석 시스템은 국가기관이 정당하게 보유하고 있는 데이터베이스를 대상으로 시스템 구축이 이루어져야 하며, 데이터 분석을 위한 원자료의 활용도 실정법에 위배되면 안 된다. 물론 현행 디엔에이 신원확인정보의 이용 및 보호에 관한 법률과 같은 개별적인 법적 근거가 존재한다면 발생가능한 문제점을 최소화시킬 수 있겠지만, 이와 같은 법적 근거가 존재하지 않은 경우, 식별 개인정보를 활용할 경우에는 반드시 현행 개인정보보호법을 준수해야 한다. 이와 같은 요건에 부합할 경우에는 빅데이터 분석 시스템을 활용한 데이터 분석행위는 임의수사에 해당된다고 봄이 상당하다.

2) 개인정보보호법제 위반에 따른 정보인권 침해 여부

현행 개인정보보호법 제2조 제1호에서는 “개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.” 규정하고 있다. 동법 제15조 제1항에서는 개인정보를 수집할 수 있는 경우를 1호부터 6호까지 나열하고 있으며, 이 경우가 아니면 개인정보를 수집하지 못하도록 규정하고 있다. 국가기관이 보유하고 있는 데이터베이스를 활용할 경우, 활용되는 데이터베이스의 성격에 따라 원자료가 개인정보에 해당될 수 있다. 식별 가능한 개인정보를 빅데이터 분석시스템에 활용할 경우에는 반드시 개인정보보호법을 준수해야 한다. 다만, 비식별 정보의 경우에는 경찰관직무집행법에 근거하여 빅데이터 분석 시

스템을 통해 분석될 수도 있을 것이다.

한편 4차 산업혁명에 의한 지능정보사회에서 인간의 도움 없이 스스로 생각하고, 판단하고, 결정하여 행동하는 물질들의 세상이 구현될 경우 정보주체인 인간의 의사결정이 배제된 사물들의 연결, 빅데이터에 의존한 정보주체의 생활방식과 형태가 결정된다. 이는 곧 범죄예방 및 수사절차에서도 그대로 적용될 수 있고, 일상생활에서 정보인권 침해문제로 이어질 가능성 또한 존재하는 것이다. 그렇다면 이제 우리는 우리가 통제할 수 없는 '모든 것이 완벽하게 연결된' 초연결사회에서 살고 싶은가, 아니면 불완전하게 연결되고 나 스스로 연결여부를 결정할 수 있는 on off 스위치가 있고, '일정부분' 끊어진 초연결사회에서 살고 싶은지를 판단해야 한다. 이처럼 개인정보자기결정권으로 비롯되는 정보인권을 진지하게 논의하는 이유는 과거나 지금처럼 향후, 민주법치국가의 존립근거인 인간의 존엄성과 자율을 보호하기 위해서이다. 이제 중요한 것은 두려움의 대상인 정보처리를 가능한 한 투명화함으로써 기술적 발전에 관하여 규범적으로 판단하고 예측함으로써 인간의 존엄성과 자율을 계속해서 보호해야만 한다는 것이다.[38]

따라서 정보인권 보장의 본질적인 내용은 4차 산업혁명 시대에서 아무리 문명의 이기가 발전하더라도 인간의 자율적 의사소통 내지는 판단을 확보할 필요가 있다는 것이다. 즉, 분명하게 짚고 넘어가야 될 것은 지능정보사회에서 정보인권의 보장을 단순한 개인의 권리보장 측면에서만 바라봐서는 안 된다. 왜냐하면 이 문제는 국민의 기본권인 정보인권을 침해하지 않도록 빅데이터, 사물인터넷 등의 기술체계가 헌법이 보장하고 있는 영역 이내인 것인지 확인하고 판단해봐야 될 문제인 것이다. 범죄예방 및 수사절차라는 공익상 목적이라고 할지라도 개인정보주체가 자신의 정보수집 및 처리 등의 절차를 인식하고 있고, 어떻게 활용되고 어떠한 의미를 갖는지 파악하고 스스로 판단할 수 있는 환경조성이 필요하다.

38) 김일환, 앞의 논문, 79면.

Ⅳ. 범죄예방을 위한 법·제도적 개선방향

본 장에서는 본 연구의 핵심적인 사항으로서 앞서 제3장에서 살펴본 바와 같이 빅데이터의 활용의 한계점을 벗어나지 않는 법적 개선방향을 제시하고 한다. 즉 지금까지 정리한 내용을 종합적으로 고찰하여 빅데이터 등을 활용하여 범죄예방 및 수사 절차에서 활용할 경우, 정보인권 침해 등 법적인 문제점을 최소화할 수 있는 법·제도적 개선방향에 대해 모색해보고자 한다. 구체적으로 먼저, 현재에 이르기까지 논의가 되고 있는 법안과 가이드라인에 대해 면밀히 분석해본다. 그리고 향후 입법을 추진하는 과정에서 빅데이터의 활용이 법적 테두리 안에서 정보인권 보장 및 범죄예방, 수사절차 등에게 가치상승을 위해 반드시 고려되어야 할 사항을 아래와 같이 구분하여 언급한다. 이를 위해 정보인권 보장을 위한 프라이버시 침해방지 측면에서 살펴보고, 현행 법률들 간의 체계적인 해석 및 정합성 등을 고려한 입법내용 및 체계의 개선방향을 중심으로 정리함으로써 본 연구의 결론을 이끌어 내도록 한다.

1. 개인영상정보보호법안의 의미

최근 로봇, 인공지능(AI) 등 지능정보기술 보급의 확산으로 기존의 CCTV, 네트워크 카메라 등의 고정식 영상촬영기기가 점차 지능화되고 있으며, 다양한 형태로 개발 및 보급되면서 이를 통해 대규모의 개인영상정보가 수집·처리·유통되고 있다. 앞서 언급한 바와 같이 이러한 영상정보기기를 통해 수집되는 영상정보가 범죄 행위의 입증과 범인 검거에 결정적인 공헌을 하는 등의 사회적 유용성이 점차 증대되고 있지만, 한편으로는 자동화된 기기를 통해 수집되는 개인영상정보의 개인 식별성 및 사생활 침해 위험성도 함께 증가하고 있다. 이에 행정안전부에서는 개인영상정보보호법안[39]을 입법예고[40]했는데, 동 법안

39) 동 법안은 제1장 총칙: 개인영상정보 보호의 범위 등, 제2장 영상정보처리기기: 고정형 및 이동형 영상촬영기기의 설치·운영에 대한 기준 등, 제3장 개인영상정보의 처리: 개인영상정보 처리 단계별 보호기준 등, 제4장 개인영상정보의 안전한 관리: 개인영상정보의 안전한 관리를 위한 조치사항 등, 제5장 영상정보주체의 권리 보장: 영상정보주체 등의 권리 보장 등, 제6장 보칙, 제7장 벌칙으로 구성되어 있다.

40) 행정안전부는 개인영상정보의 보호와 영상정보처리기기의 설치·운영 및 개인 영상정보의 처리 등에 관하여 규율하는 개인영상정보 보호법 제정안을 2016년 12월 16일 최초 입법예고(행정자치부 공고 제2016-370호)하고, 같은 해 12월 21일 입법 공청회를 개최한

은 최근 영상정보 처리 기술의 고도화 및 사회적 유용성 증대로 사회 모든 영역에 걸쳐 영상정보처리기기의 설치·운영이 크게 증가하고 있으나, 국가 사회 전반을 규율하는 개인영상정보 보호 원칙과 기준이 마련되지 못해 개인영상정보의 오·남용 및 사생활 침해 등에 대한 우려가 증가하고 있어 국민의 권리와 이익을 보장하려는 것이 주된 제정목적이라고 할 수 있다.

한편, 현행 개인정보보호법에서도 영상정보처리기기의 설치 및 운영과 관하여 규율하고 있으나 일정한 공간에 지속적으로 설치되어 있는 CCTV, 네트워크 카메라와 같은 고정형 영상촬영기기만을 규율대상으로 한다는 점에서, 개인영상정보보호법의 제정을 통해 최근 인공지능(AI) 기술이 접목된 지능형 기기, 드론, 웨어러블 카메라, 블랙박스 등 다양한 형태의 이동형 영상촬영기기에서 촬영되는 개인영상정보의 규율에 대한 법적 사각지대를 해소할 수 있을 것이다. 또한 개인영상정보의 처리 및 관리, 영상정보주체 권리보호에 관한 사항 등을 규율하고 있을 뿐만 아니라 행정안전부장관의 허가를 받은 경우에는 통계작성, 학술연구 및 연구개발 등 필요 시 개인영상정보를 촬영할 수 있으며 나아가 비식별 조치를 위한 개인영상정보의 목적 외 이용 등에 관한 규정도 함께 포함되어 있어 개인영상정보의 '보호'와 '활용'의 균형을 통한 관련 신산업 발전과 경제 활성화에도 기여할 수 있을 것으로 기대된다.[41]

그러나 개인정보 보호의 효율성 및 법체계의 정합성 유지, 개인영상정보 분야의 규범이 추가됨으로 인한 수범자의 혼란 방지, 개인정보 보호 수준의 약화에 따른 정보주체의 자기정보결정권 침해 방지 등의 측면에서 개인영상정보 관련 별도입법을 추진하기 보다는 현행 개인정보보호법과 하위법령에 편입시키는 것이 보다 효율적이고 타당하다고 생각한다. 또한 향후 동 법안을 입법 추진한다면, 그 과정에서 개인영상정보 보호를 규율할 법의 형식과 체계뿐만 아니라 개인영상정보의 개념 및 보호 원칙, 생애주기(Life-cycle)별 보호기준, 기술적·관리적 보호조치, 영상정보주체의 권리 보장방안 등으로 구성되는 법률의 구체적인 내용에 대한 각계의 심도 깊은 논의를 통해 입법에 대한 사회적 합의와 공감대 형성을 위한 노력이 무엇보다 요구될 것이다.

데 이어 기관, 단체, 개인으로부터 제출받은 의견들을 분석·검토하여 2017년 9월 13일 일부 수정된 「개인영상정보 보호법」법률제정안을 재입법예고(행정안전부 공고 제2017-77호)하였다.

41) 이시직, "개인영상정보보호법 제정법률(안) 재입법예고", 「정보통신방송정책 동향」 제29권 제17호, 정보통신정책연구원, 2017.9.18, 9-16면.

2. 빅데이터 개인정보보호 가이드라인의 의미

현행 개인정보보호법이나 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법이라 칭함.)은 개인정보를 수집·이용·제공하기 위해서는 정보주체로부터 이에 대한 동의를 요구하고 있다. 그러나 개인정보의 활용은 상당히 광범위하게 이뤄지고 있기 때문에 정보주체가 아닌 자로부터 입수한 개인정보를 제공하거나 처리하게 되는 경우가 다양하게 발생하고 있는 것이 사실이다. 단적인 예로 빅데이터 분석과 활용이라고 볼 수 있는데, 현행 개인정보보호법 제20조는 정보주체 이외로부터의 개인정보 수집에 대해서 규율하고 있다. 즉 정보주체의 요구가 있을 경우, 수집출처와 처리 목적, 정보주체에게 자신의 개인정보 처리를 중지할 권리가 있다는 사실을 고지하도록 명시되어 있다. 그러나 이러한 규정이 존재하고 있음에도 불구하고 현행 개인정보보호법제는 이러한 경우에도 일반적인 개인정보와 마찬가지로 개인정보의 수집·활용 등을 위해 정보주체의 동의권이 전제되어 있는 것인지에 관해서는 구체적으로 규정하고 있지 않은 입법적 미비점이 존재한다.[42]

이에 따라 현재 빅데이터를 범죄예방 및 수사 절차에서 활용하기 위해서는 개인정보보호법제와의 상충부분을 따져보고, 정보주체의 사전 동의를 받기가 사실상 곤란한 경우에 어떻게 처리하는 것이 합리적일지의 문제일 것이다. 방송통신위원회가 제시한 동 가이드라인의 대강의 내용을 살펴보면, 이에 대한 사항을 담고 있는데, 이는 법률상 규정이 미비되어 있는 사항들을 구체화여 문제점을 최소화시키겠다는 의지로 판단된다. 특히 가이드라인 제1조는 공개된 개인정보[43] 또는 이용내역 정보[44] 등을 전자적으로 설정된 체계에 의해 조합, 분석 또는 처리하여 새로운 정보를 생성함에 있어서 이용자의 프라이버시 등을 보호하고 안전한 이용환경을 조성하는 것을 목적으로 한다고 규정하고 있는데, 이 규정에서 방송통신위원회의 의도가 엿보인다.

---

42) 심우민, "빅데이터 개인정보보호 가이드라인과 입법과제", 「이슈와 논점」 제866호, 국회입법조사처, 2014.6.12, 1-2면 참조.

43) 공개된 개인정보: 정보주체 등에 의해 제한 없이 일반 공중에게 공개된 정보로서 생존하는 개인을 식별할 수 있거나 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보.

44) 이용내역정보: 이용자가 서비스를 이용하는 과정에서 자동으로 발생되는 인터넷 접속정보파일, 거래기록 등의 정보로서 생존하는 개인을 식별할 수 있거나 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보.

한편, 동 가이드라인의 주요내용을 확인해보면, 우리나라 개인정보보호법제의 개인정보의 수집 · 이용 · 제공 등을 행할 때 엄격한 사전동의 방식(Pot-in)을 취하고 있는 것과는 달리, 엄격한 요건이 아니라 상당부분 그 요건을 완화하고 있는 조항을 발견할 수 있다.[45] 다만 개인정보자기결정권 등 정보인권을 보장하가 위해 공개된 개인정보, 이용내역정보, 개인정보를 활용하여 생성된 새로운 개인정보에 관한 출처, 처리사실 및 목적 등을 정보주체가 원할 경우에는 쉽게 확인할 수 있도록 보완규정을 마련해 놓고는 있다.[46] 그러나 대부분의 규정들은 정보주체로부터의 동의 요건을 완화하는 것을 기본 원칙으로 두고 있으므로 다음과 같이 개편이 필요해 보인다. 먼저 빅데이터 관련 산업의 활성화 측면에서 볼 때, 이를 이용자와 국민들의 편의를 위해 활용되게끔 하기 위해서는 필연적으로 최소한의 범위 내에서 개인정보 활용을 용인할 수밖에 없다. 이러한 과정을 통해 최적화된 유용한 정보와 서비스들이 제공될 수 있기 때문에 일방적으로 정보인권의 보장 측면만을 고집하는 것은 오히려 타당하지 못할 수 있다.[47] 이에 따라 개인정보의 수집 및 활용을 제한된 범위 내에서 허용하되, 허용된 정보에 대한 정보주체의 자기통제권을 보장하기 위해 개인정보자기결정권을 헌법상으로 인정하게 된 것이다.[48] 결론적으로 헌법재판소가 인정한 정보인권의 구체적인 권리로서 개인정보자기결정권을 어떻게 현실적으로 보장할 수 있을지에 대한 문제로서 가이드라인을 재고(再考)해봐야 된다는 것이다.

3. 입법내용상 정보인권과의 관계 검토

현재까지 빅데이터 등을 활용한 범죄예방 및 수사 절차에 대한 법 · 제도가

45) 빅데이터 개인정보보호 가이드라인은 제3조 공개된 개인정보, 제4조 이용내역정보의 수집, 제5조 새로운 개인정보의 생성, 제6조 비식별화, 제8조 민감정보의 생성금지, 제11조 공개된 개인정보 등의 제3자 제공 등의 조항에서 보면, 개인정보주체의 동의요건을 상당히 완화하여 규율하고 있음을 확인할 수 있다. 보다 구체적인 사항은, 심우민, 앞의 글, 2면 참조.

46) 심우민, 앞의 글, 2면.

47) 심우민, “빅데이터의 활용과 개인정보 보호”, 「이슈와 논점」 제724호, 국회입법조사처, 2013.10.11. 참조; 우리나라의 법제들은 상당히 엄격한 사전동의 원칙을 취하고 있는데, 언제 어떠한 방식으로 개인 식별 가능성을 가질지 알 수 없는 모든 정보들에 관하여 사전에 이용자들의 동의를 구하는 것은 현실적으로 불가능하다고 할 수 있으며, 만일 그렇게 될 경우 사실상 빅데이터의 활용을 저하하는 결과를 불러일으킬 수 있다.

48) 헌재 2005.5.26. 99헌마513, 2004헌마190(병합); 헌법재판소는 개인정보자기결정권을 헌법상 열거되지 않은 기본권으로 인정한 바 있다.

미미한 것이 사실이므로 이는 곧 향후 입법론적으로 주요 쟁점사항이 될 것이다. 또한 형사상 범죄수사 측면에서가 아니라 범죄예방 목적 차원에서 빅데이터 등을 활용하는 것을 특정한 법적 근거로 마련하는 것은 간단한 문제가 아니다. 따라서 여기에서는 범죄예방 등에 기여하기 위한 법·제도적 근거를 마련하는데 있어서 빅데이터의 활용과 정보인권과의 관계에 대해 검토한다. 이는 곧 입법을 하는 과정에서 정보인권을 침해하지 않는 범위 내에서의 빅데이터의 활용을 통해 범죄예방 등의 효과를 추구할 수 있는 방안이 될 것이다. 본 연구에서 중점적으로 다루고 있는 빅데이터의 활용은 개인정보와 관련성이 밀접하기 때문이다.

한편, 빅데이터 활용의 문제는 범죄예방 측면에서 다뤄지는 것에 그치는 것이 아니라, 산업 측면에서도 그 수요가 증대되고 있다. 실제로 지난 19대 국회에서는 '빅데이터의 이용 및 산업 진흥에 관한 법률'이 발의된 바 있는데, 해당 법률안에서는 비식별화 된 공개정보를 이용하고 처리하는 절차와 빅데이터에 관련된 개인정보 처리절차 등을 규정했다. 동 법안은 제안자의 임기만료로 폐기되었고, 현 20대 국회에서 같은 취지의 법률안이 발의되어 계류 중이다. 현재 빅데이터산업은 사물인터넷·클라우드 컴퓨팅 산업 등과 함께 정보통신산업의 성장을 이끌 한 축으로서 성장 가능성이 높으나, 국내에서는 개인정보 보호와 관련된 규제의 경직성으로 인하여 많은 기업들이 빅데이터 사업에 적극적으로 나서지 못하고 있는 현실적인 문제와 빅데이터 등 정보통신산업에서의 개인정보 활용 형태는 기존의 '개인정보처리자-정보주체'라는 양자적 구조의 범위를 이미 넘어선 상태인 반면, 개인정보에 관한 현행법은 이와 관련된 규정이 마련되어 있은 법체계상 문제점이 제기된다.[49]

이렇듯 산업 수요 측면에서도 중요한 빅데이터는 범죄예방 등의 측면에서 살펴볼 때, 활용 가능한 범위를 명시하고 있는 근거법률로 '공공데이터법'이 있는데, 공공데이터법에서는 다른 법률에서 금지하지 않는 한 개인정보가 포함되어 있지 않은 정보는 제공이 가능하도록 되어 있다. 그러나 다른 법률에 속하는

49) 이에 빅데이터산업의 가치 제고를 위하여 현행 개인정보 보호 법제에서 공백으로 남겨두고 있는 비식별화된 개인정보의 취급에 관한 사항을 규정함으로써 법률의 명확성을 제고하는 한편, 신성장 산업인 빅데이터산업의 진흥과 그 이용의 활성화에 관한 사항을 규정하여 개인정보의 침해를 방지하고 국민경제의 발전에 이바지하려는 제정목적·취지가 있는 것이 발의된 법률안의 특성이라고 할 수 있다; 국회 의안정보시스템 홈페이지 (http://likms.assembly.go.kr) 참조.

정보공개법 제9조나 개인정보보호법 등을 살펴보면 개인정보의 범위가 불명확한 실정이다.[50] 이러한 이유에서 범죄예방을 위한 빅데이터 활용 가능성의 결정은 정보의 범위를 어떻게 설정하는 지에 달려있다. 현행 개인정보보호법에 의할 경우, 개인정보의 범위를 광범위하게 설정하고 있으므로 빅데이터 분석의 범위는 줄어들 수밖에 없다. 즉 개인정보의 범위를 명확하게 규정하는 것이 필요한데, 여기에서 범죄예방 측면과 정보인권 보장 측면인 양자를 고려한 합리적인 개인정보 범위 설정이 중요해진다. 더 나아가 현행 기상법, 통계법, 저작권법 등 다양한 개별 법률들이 공공데이터 사용을 제한하고 있는 근거가 많으므로 개별 법률들 간의 조화를 이룰 수 있는 전체적인 시각에서의 법률적 정비 작업도 요구된다고 할 것이다.[51] 그러나 개인정보의 범위가 명확하게 되었다고 하더라도 개인정보가 완전히 제거된 정보만을 사용할 수 있는 것은 아니기 때문에 개인정보가 포함된 정보를 사용하게 되는 경우, 그 처리방안에 대해 고민할 필요가 있다.

4. 입법체계상 합리적 개선방향

지금까지 정리한 개선해야 될 쟁점사항을 바탕으로 현행 개인정보 관련 법률들 간의 체계적인 해석 및 정합성 등을 고려하여 입법체계의 개선방향을 모색하는 것이 순서일 것이다. 따라서 여기에서는 입법체계상 합리적인 개선방향을 제시함으로써 본 연구의 결론을 이끌어내고자 한다.

현행 개인정보보호 법제들이 빅데이터 활용을 저해한다는 의견이 빈번하게 제기되면서 현행 법제에 규정되어 있는 개인 식별 가능성 요건을 완화해야 한다는 주장 또한 제기되고 있는 것이 현실이다. 이러한 요건 완화의 필요성에 따라 앞서 정리한 빅데이터 개인정보보호 가이드라인도 마련된 것이지만, 이에 대해 중·장기적인 차원에서 조금 더 시간을 두고 고민해봐야 될 사안이라고 생각한다. 왜냐하면 개인정보 주체 동의에 대한 요건완화가 전반적으로 개인정보보호 법체계에 예상치 못한 혼란을 야기시킬 수도 있기 때문이다. 이러한 식

50) 이원상, "범죄예방을 위한 첨단과학기술 활용에 따른 법제도적 쟁점 고찰", 「형사정책연구」 제27권 제2호, 한국형사정책연구원, 2016, 248-251면; 이상윤, 「빅데이터법제에 관한 비교법적 연구 - 종합보고서」, 한국법제연구원 지역법제 연구, 2014, 109면.

51) 이상윤, 앞의 논문, 109-110면.

별 가능성 문제는 이용자들에게 법적으로 부여된 동의권 행사방식의 문제와도 연관되는데, 이 문제에 대해서는 단계적 접근을 통해 공감대 형성 및 사회적 신뢰성을 확보하는 것이 중요하다. 또한 일반법인 개인정보보호법을 통해 개인정보보호위원회[52]의 역할을 기대해볼 수도 있겠지만, 형식적인 기구가 아닌 분산된 개별 정보보호 법률들의 소관 부처들의 감독 및 규제 기능을 통합·일원화하여 운영될 수 있는 감독기구의 체계정비가 필요하다. 그리고 빅데이터 활용기술 뿐만 아니라, 최근 정보 기술의 양태를 고려해볼 때, 개인정보보호 문제를 효율적으로 해결하기 위해서는 경제·사회적 측면에서 전문성이 뒷받침되어야 한다.[53] 이러한 현실에서 정부 규제당국의 과거와 동일한 일방적 규제기준을 강요하는 것은 비효율적이고 무리가 뒤따른다고 볼 수 있다. 따라서 민간영역의 자율규제(self regulations)를 활성화시키고, 이러한 과정에서 축적된 법적 기준을 면밀히 분석하여 법·제도적 개선안에 반영될 수 있도록 조치해야 될 것이다.[54]

한편, 범죄예방을 위해 빅데이터 및 사물인터넷을 활용하는 것의 가장 큰 걸림돌이 입법의 부재이기도 하지만, 미흡한 입법을 통해 관련 법률 간에 상충문제가 발생하거나 관련 법률들에 충분한 내용이 입법되지 못하는 문제도 있다. 이는 우리나라의 입법방식과 법률을 주관하는 주관부처간의 구획화 된 입법으로 인해서 발생하게 된다. 4차 산업혁명에서 거론되고 있는 빅데이터, 사물인터넷 외에 드론, 자율 주행자동차 등에 대한 규정들은 개인정보보호법, 정보통신망법, 도로교통법, 건축법 등 다양한 법률들에 산재되어 있으며, 해당 법률의 주무부처는 행정안전부, 과학기술정보통신부 방송통신위원회, 국토교통부 등 여러 부처들로 산재되어 있기 때문에 따라서 해당 기술과 관련된 체계적이고 유기적인 규율이 어려운 상황이다. 예컨대, 일본의 경우에는 관련 사안에 대해서 기본법을 제정하고, 기본법을 기준으로 다양한 개별 법률을 제정하는 방식을 택하고 있다. 또한 독일은 Artikelgesetz[55]를 통해서 법률들 간의 유기적인 관

52) 개인정보보호법 제7조 이하 참조.
53) 개인정보보호 감독기구의 권한 및 위상강화를 위해 개인정보보호기구의 헌법상 의의와 근거에 따른 개인정보의 효율적 보호를 위한 통제의 필요성이 요구된다. 김일환, 앞의 논문, 84-86면 참조.
54) 심우민, 앞의 이슈와 논점 (제724호), 4면.
55) 이원상, 앞의 논문, 256면; 독일의 'Artikelgesetz'또는 'Mantelgesetz'라는 입법방식은 많은 법률 또는 다양한 법률내용들을 동시에 개정하는 방식이다.

계가 유지되는 방식을 취하기도 한다.[56] 그러나 우리나라는 개별입법을 통해 각 사안에 대응하는 법률을 규정하기 때문에 법률들 간의 체계적이고 유기적인 모습이 미흡한 실정이다. 더욱이 최근 들어 새로 규정되는 법률들을 더욱 그러하다.[57] 그러므로 체계적인 입법이 가능할 수 있도록 빅데이터 및 사물인터넷 등 관련 기술과 관련된 입법 가이드라인을 만들 필요가 있다. 이를 통해 앞서 언급한 문제점들을 최소화시키고, 개선방향에서 꼭 적용되어야 될 사항을 포함시킴으로써 범죄예방 · 수사절차 등에서 빅데이터 등의 활용이 정보주체의 정보인권도 함께 보장하는 방향으로 나아가는 것이 핵심이라고 볼 수 있다.

Ⅴ. 나가며

본 연구에서는 4차 산업혁명 시대에서 빈번하게 거론되고 있는 빅데이터, 사물인터넷을 중심으로 범죄예방 및 정보인권 보장 측면에서 활용가능성과 그 한계점, 한계점 극복을 위한 여러 측면에서의 개선방향을 이끌어냄을 목표로 진행했다. 이를 위해 우선 빅데이터 및 사물인터넷에 대해 의의와 실태, 사례 등 현황에 대해 전반적으로 살펴보고, 범죄예방을 위해 빅데이터와 사물인터넷의 활용가능성 측면을 살펴보았다. 물론 이런 과정에서 선행연구된 문헌을 통해 문헌조사방법론을 접목하여 진행했지만, 이에 대한 평가와 한계점 측면에서는 향후 제시될 수 있는 사항에 대해서 충분히 언급했다.

그러나 본 연구의 가장 핵심적인 사항은 제4장으로서 범죄예방을 위한 법 · 제도적 개선방향이라고 할 수 있다. 지금까지 정리한 사항을 토대로 여기에서는 프라이버시 등 정보인권 침해방지와 개인영상정보보호법안 및 빅데이터 개인정보보호 가이드라인에 대한 분석을 통해 나아가야 될 방향에 대해 제시했고, 보안강화와 사회적 신뢰성 확보 측면에서는 빅데이터 활용에 대한 국민의

56) 강석구 · 이원상, 「사이버범죄 관련 법령정비 방안」, 형사정책연구원 연구총서, 2013, 185면.
57) 예를 들어, 「개인정보보호법」이 제정되어 「정보통신망법」에서 개인정보보호 관련 규정인 제33조-제40조 규정이 삭제되었음에도 「정보통신망법」 제44조의10 제3항은 여전히 제33조의2 제2항 규정 및 제35조-제39조의 규정을 준용하고 있다. 이 문제는 이미 「개인정보보호법」이 제정된 이후 계속해서 지적하고 있지만, 아직도 존치되고 있다. 이는 입법오류를 넘어서서 입법방치가 되는 상황이라고 할 것이다; 강석구 · 이원상, 앞의 책, 183면(이원상, 앞의 논문, 256면에서 재인용).

신뢰가 전제조건이 되어야 함을 강조했다. 당연히 기술적 측면에서 보안이 강화되는 것이 필수요건이지만, 본 연구에서는 기술적 측면에 대한 언급은 최소화하고 법리적 검토 부분과 방향제시에 초점을 맞췄다. 끝으로 입법체계상 개선방향 제시에서는 먼저, 개인정보보호법제에 대한 세부정비를 위해 빅데이터를 활용하는 과정에서 개인정보 주체에 대한 사전동의 부분에 대한 개선방향, 개인정보 감독기구에 대한 체계정비 방안, 자율규제 적용방안 모색, 법·제도적 개선안 마련에 따른 기존 현행 법률들 간의 상충문제 해결과 보다 합리적인 입법 가이드라인 마련 등에 대해 구체적으로 제시했다.

이미 유럽이나 미국, 일본 등에서는 새로운 첨단과학기술들의 등장과 관련해서 다양한 연구들이 수행되어 왔고, 그를 지원해 주기 위해서 다양한 법제도들이 마련되고 있다. 그런데 우리나라는 이제 겨우 관련 문제들을 인식하는 수준에 머물러 있으며, 규범적으로 논의되는 영역이 가이드라인이나 시행규칙, 시행령에 머물러 있는 것이 사실이다. 이와 함께 법적 효력이 상당히 낮은 단계에서 마련된 것이기 때문에 규범력에서도 한계를 갖게 된다. 이처럼 빅데이터, 사물인터넷 등 관련된 일반적인 법률들도 미흡한 상황에서 범죄예방과 관련된 근거규정을 마련하기는 더욱 쉽지 않은 상황이다. 특히 해당 기술들은 개인정보와 매우 밀접한 관련성이 있으므로 범죄에 대한 수사목적과는 달리 범죄예방을 위해 해당 기술들을 사용하는 것은 그리 쉽지 않은 상황이다.[58] 더욱이 해당기술을 활용하는 것이 기술적이나 법적으로 가능하더라도 경우에 따라서는 오히려 국가에 의한 감시 내지는 사찰로 오인될 가능성이 농후하므로 국민들의 감정에 반하는 결과가 초래될 수도 있다. 따라서 범죄예방을 위해 빅데이터 등을 사용하는 문제는 앞서 제시한 개선방향을 충분히 고려하여 법·제도적 개선방안을 마련함에 있어서 종합적이고 단계적으로 접근해야 될 것이다.

투고일 : 2017.11.15 / 심사완료일 : 2017.12.11 / 게재확정일 : 2017.12.18

58) 연합뉴스, 트위터, 美 정보당국에는 데이터 분석자료 안 판다, 2016.5.10. 기사; 실제로 미국에서도 트윗을 분석해 정보를 판매하는 '데이터마이너(Dataminer)'가 정보당국에 제공하던 서비스를 중단하였다.

[참고문헌]

강석구 · 이원상, 「사이버범죄 관련 법령정비 방안」, 형사정책연구원 연구총서, 2013.

권양섭, “범죄예방과 수사에 있어서 빅데이터 활용과 한계에 관한 연구”, 「법학연구」 제17권 제1호, 한국법학회, 2017.3.

김경원, “빅 데이터를 활용한 경찰의 범죄예측 활성화 방안”, 동국대 대학원, 석사학위논문, 2015.

김도우, “치안환경 변화에 따른 안전도시 도입방안 : 사물인터넷과 범죄예방환경설계를 중심으로”, 「한국셉티드학회지」 제7권 제1호, 한국셉티드학회, 2016.5.

김봉수, “빅데이터의 범죄예방 목적 활용과 규범적 한계”, 「법학논총」 제36권 제4호, 전남대학교 법학연구소, 2016.12.

김일환, 「초연결사회에서 개인정보보호법제 정비방안에 관한 연구」, 2017 한국법제연구원 · 법제처 · 한국공법학회 · 한국헌법학회 공동학술대회(4차 산업혁명에 따른 입법 대응 전략 모색)자료집, 2017.4.7.

미래창조과학부, 「사물인터넷 산업 실태조사 및 시장분석 연구」, 2014.10.

박 현 · 김세한, “IoT 기반 Big Data 기술 동향”, 「한국전자파학회지」 통권 제98호, 한국전자파학회, 2013.

성욱준, 「빅데이터 분석을 적용한 정책 사례 연구」, 국회입법조사처 정책연구용역 보고서, 2015.12.

신양균 · 조기영, “내사의 개념과 허용범위”, 「형사법연구」 제23권 제3호, 한국형사법학회, 2011.

심우민, “빅데이터 개인정보보호 가이드라인과 입법과제”, 「이슈와 논점」 제866호, 국회입법조사처, 2014.6.12.

_____, “빅데이터의 활용과 개인정보 보호”, 「이슈와 논점」 제724호, 국회입법조사처, 2013.10.11.

오세연 · 이재영, “IOT와 Big Data의 연계를 통한 범죄예방 활용방안”, 「한국콘텐츠학회지」 제13권 제1호, 한국콘텐츠학회, 2015.

유상근 · 홍용근 · 김형준, “스마트모바일 서비스: M2M 기술 및 표준 동향”, 「전자통신동향분석」 제26권 제2호, 전자통신연구원, 2011.

이상윤, 「빅데이터법제에 관한 비교법적 연구 - 종합보고서」, 한국법제연구원 지역법제 연구, 2014.

이시직, “개인영상정보보호법 제정법률(안) 재입법예고”, 「정보통신방송정책 동향」

제29권 제17호, 정보통신정책연구원, 2017.9.18.
이원상, “범죄예방을 위한 첨단과학기술 활용에 따른 법제도적 쟁점 고찰”, 「형사정책연구」 제27권 제2호, 한국형사정책연구원, 2016.
이준복, “사물인터넷시대에서 정보인권 보장을 위한 법적 고찰”, 「홍익법학」 제16권 제3호, 홍익대학교 법학연구소, 2015.9.
임상규, “빅 데이터를 활용한 스마트 재난관리전략”, 「한국위기관리논집」 제10권 제2호, 위기관리 이론과실천, 2014.
주대영 · 김종기, 「초연결시대 사물인터넷(IOT)의 창조적 융합 활성화 방안」, 산업연구원, 2014.
한승욱, “범죄예방 환경조성을 통한 생활안전 증진 방안”, 「정책포커스」 제309호, 부산발전연구원, 2016.7.

Atzori, L., Antonio, I., Giacomo, M, “*The Internet of Things: ASurvey*”, Computer Networks 54(15), 2011.
Bachner, J., *Predictive Policing: Preventing Crime with Data and Analytics*, IBM Center for The Business of Government, 2013.
ITU Internet Reports, *The Internet of Things,* November 2005.
Joh, E.E., “*Policing by Numbers: Big Data and the Fourth Amendment*”, Washington Law Review, 89:35, 2014.
Ovidiu, V., Peter, F., Anthony, F, “*The Internet of Things 2012: New Horizons*”, IERC 3rd edtion of cluster book, 2012.
Zorzi, M., Gluhak, A., Lange, S., Bassi, A, “*From Today's Intranet of Things to a Future Inter oh things*”, Wireless Communications. IEEE 17(6), 2010.

국회 의안정보시스템 홈페이지(http://likms.assembly.go.kr).
사이버경찰청 홈페이지(www.police.go.kr).

itworld, 마이크로소프트, “사물 인터넷과 빅데이터의 본질은 같다”, 2015.2.27. 기사.
디지털 데일리, 빅데이터와 IoT는 한몸, 2014.2.12. 기사.
디지털타임스, 문 대통령, “사이버보안, 4차 산업혁명 핵심 … 새유형 사이버범죄 예방 최우선”, 2017.7.12. 기사.
매일신문, ‘랜섬웨어’ 사태… “스파트폰 터치 겁나” 사이버공격 공포, 2017.5.18. 기사.

아이뉴스, 범죄 예방에 나서는 IT 기술 기업들: 스웨덴서 '클릭뷰'로 살인범 검거, MS-뉴욕시 테러 감시 시스템 구축, 2014.10.16. 기사.
연합뉴스, 트위터, 美 정보당국에는 데이터 분석자료 안 판다, 2016.5.10. 기사.
전자신문, 4차 산업혁명 시대 '사이버범죄 예방기본법' 필요, 2016.10.19. 기사.

[국문초록]

4차 산업혁명 시대에서 범죄예방 및 정보인권 보장을 위한 법적 고찰 : 빅데이터 및 사물인터넷을 중심으로

이 준 복*

4차 산업혁명 파장이 클수록 안전 위협은 더욱 커지며 나아가 국가 안보에 영향을 줄 뿐만 아니라, 온·오프라인 변화로 치안 패러다임 변화도 동시에 이뤄져야 한다. 사이버 공간에서 국민 안전을 확보할 수 있는 법체계 마련을 통해 4차 산업혁명을 범죄예방 수준을 높일 수 있는 기회로 활용해야 한다.

이에 본 연구는 4차 산업혁명시대에서 유의미한 도구로 제시되고 있는 사물인터넷, 빅데이터 등 신기술을 활용한 범죄예방마련 측면에 비중을 두어 진행했다. 특히 본 연구에서는 온·오프라인에서 일어나고 있는 범죄 예방을 위해 빅데이터, 사물인터넷을 중심으로 진행한다. 다만, 여기에서는 양자에 대해 모두 접근하여 정리하겠지만, 사물인터넷은 빅데이터 기술을 전제로 하기 때문에 활용가능성 및 한계, 개선방향 제시 등에서는 빅데이터에 초점을 맞춰 비중 있게 다루어 진행함을 아울러 알려둔다.

이를 위해 제2장에서는 빅데이터 및 사물인터넷의 의의와 실태, 사례 등 현황에 대해서 정리하고, 제3장에서는 범죄예방을 위한 빅데이터의 활용가능성과 한계점에 대해 분석함으로써 활용가치 측면과 예측가능한 문제점 보완을 통해 결론을 도출하는데 근거자료로 활용한다. 끝으로 제4장에서는 본 연구의 핵심으로서 범죄예방을 위한 법·제도적 개선방향을 제시함으로써 결론을 이끌어내도록 한다. 특히, 법적 대책으로 제시가 되고 있는 개인영상정보보호법안 및 빅데이터 개인정보보호 가이드라인에 대해서도 살펴보았다.

주제어 : 4차 산업혁명, 빅데이터, 사물인터넷, 범죄예방, 정보인권보장

* 서경대학교 공공인적자원학부 법학전공 교수, 개인정보관리사(CPPG), 법학박사.

[Abstract]

Legal Study on the 4th industrial revolution era for the crime prevention and the information human rights protection
: Focused on Big Data and Internet Of Things

Lee, Joon-bok*

The bigger the wave of the fourth industrial revolution becomes, the greater the security threats are, which affects the National Security. Thus. the change in security paradigm must be made at the same time by on-line and off-line changes. The fourth industrial revolution should be utilized as an opportunity to raise the level of crime prevention through the establishment of a legal system to security in cyberspace.

Therefore, this study is conducted by placing emphasis on the aspect of the crime prevention using new technology such as Inter Of Things, Big data which are suggested as meaningful tools. In particular, the present study for the crime prevention happening in the on line and off line goes around big data and Internet Of Things. We will also deal with all of things in every case. However, since the Internet of things is premised on the big data technology, it is also informed that it focuses on the big data in terms of utilization possibility, limit and improvement direction.

For this, In Chapter 2, we summarize the significance, realities, and cases of Big Data and Internet of Things. and In Chapter 3, by analyzing the possibility and limitations of big data for crime prevention, It is used as a basis to draw conclusions. Finally, In Chapter 4 we make the conclusions by presenting the legal and institutional improvement directions for crime prevention as the core of this study. In particular, we have reviewed the Personal Video Information Protection Act and the Big Data Privacy Protection Guidelines, which are

* Professor in SeoKyeong University, Division of Public Human Resources, Certified Privacy Protection General(CPPG), Doctor of laws.

presented as legal measures.

Key words : Fourth industrial revolution, Big Data, Internet Of Things, Crime prevention, Information human rights protection.