https://doi.org/10.33778/kcsa.2019.19.5.063

4차 산업혁명기 인공지능과 빅데이터 운용을 위한 개인정보 보호와 이용에 관한 연구

최 원 상*, 이 종 용**, 신 진***

요 약

4차 산업혁명기에는 정보통신기술(ICT)의 비약적인 발전으로 사람과 사물로부터 정보를 수집하여 분석하고 가치를 창출하는 것이 가능하다. 그러나 사람을 대상으로 하는 정보의 수집은 법적으로나 제도적으로 많은 제한이 있다. 따라서 급변하는 사이버 안보환경에서 개인정보의 보호와 이용에 관한 심도 있는 연구가 필요하다. 본 연구의 목적은 4차 산업혁명기 인공지능(AI)과 빅데이터 운용을 위한 개인정보의 보호와 이용에 관한 패러다임의 전환을 모색하는 것이다. 이를 위한 연구의 구성은 제1장에서는 4차 산업혁명기 개인정보가 갖는 의미를 알아보고, 제2장에서는 선행연구 검토와 분석의 틀을 제시하였으며, 제3장에서는 주요 국가들의 개인정보의 보호와 이용을 위한 정책을 분석 한 후, 제4장에서는 4차 산업혁명기 개인정보 보호의 패러다임 변화 전망과 대응 방안을 고찰하였으며, 제5장에서는 개인정보의 보호와 이용을 위한 몇 가지 정책적 제언을 하였다.

A Study on the Protection and Utilization of Personal Information for the Operation of Artificial Intelligence and Big Data in the Fourth Industrial Revolution

Choi, Won Sang*, Lee, Jong Yong**, Shin, Jin***

ABSTRACT

In the 4th Industrial Revolution, information is collected and analyzed from people and objects through the rapid development of ICT. It is possible to create value. However, there are many legal and institutional restrictions on the collection of information aimed at people.Therefore, in-depth research on the protection and use of personal information in the rapidly changing cyber security environment is needed. The purpose of this study is to protect and utilize personal information for the operation of AI (Artificial Intelligence) and big data during the 4th Industrial Revolution. It is to seek a paradigm shift. The organization of the research for this is: Chapter 1 examines the meaning of personal information during the 4th Industrial Revolution, Chapter 2 presents the framework for the review and analysis of prior research. In Chapter 3, after analyzing policies for the protection and utilization of personal information in major countries, Chapter 4 looks at the paradigm shift in personal information protection during the 4th Industrial Revolution and how to respond. Chapter 5 made some policy suggestions for the protection and utilization of personal information.

Key words : **Fourth Industrial Revolution, Cybersecurity, Artificial Intelligence, Big Data, Protection of Personal Information,**

접수일(2019년 12월 9일), 게재확정일(2019년 12월 26일)

* 충남대학교 군사학과(제1저자)
** 국방과학연구소 소요기획연구실(제2저자)
*** 충남대학교 정치외교학과(교신저자)

1. 서 론

4차 산업혁명기 정보통신기술(ICT: Information Communications Technologies)의 발전은 국가 간에 사이버 안보에 대한 인식과 정보력에 현격한 격차를 만들고 있다. 또한 사이버 테러공격, 해커에 의한 정보유출 등 국가의 사이버 안보를 위협하는 요인과 현상은 다양한 형태로 나타나고 있다. 포괄적 안보 상황에서는 사이버 안보태세를 확립하기 위한 정보통신기술(ICT)이 필요하며 이러한 정보통신기술(ICT)의 발전은 사회적 비용의 투입을 적게 하여 국가안보의 유지를 가능하게 한다[1].

2016년 1월 다보스 포럼에서 '4차 산업혁명의 이해'라는 주제로 논의가 이루어지면서 주요 선진국들은 인공지능(AI: Artificial Intelligence), 사물인터넷(IoT: Internet of Things), 빅데이터(Big Data) 등 정보통신기술(ICT)에 관한 국가전략을 수립하여 추진하고 있으며, 한국도 국정기획자문위원회에서 국정운영 5개년계획을 발표하였으며, 2017년 8월에는 대통령 직속으로 '4차 산업혁명위원회'가 출범되었고, 정부도 '4차 산업혁명 대응 전자정부협의회'를 통하여 '지능형 정부 기본계획'을 수립하여 추진하고 있다[2].

지능형 정부는 정보통신기술(ICT)의 발전에 따라 지능정보사회의 구현을 위한 정부 정책이다. 이의 구현을 위해서는 인공지능(AI), 사물인터넷(IoT), 빅데이터(Big Data) 등 주요 정보통신기술(ICT)을 활용하는 것이 필수적이다.

도시 전체를 통신으로 연결하여 관리 및 운영하기 위해 지난 2008년에는 '유비쿼터스 도시의 건설 등에 관한 법률(일명, U시티건설지원법)'이 제정되었으며, 이후 정보통신기술(ICT)의 발전에 따라 사물인터넷(IoT) 기술을 적용하여 도시에서 생활하는 사람과 사물의 연결을 통한 생활편의 향상 등을 위해 2014년에는 '스마트도시 조성 및 산업진흥 등에 관한 법률(일명, 스마트도시법)'이 제정되었다. 이를 근거로 2018년 국토교통부의 국가스마트도시위원회에서는 스마트시티 국가시범사업으로서 세종시와 부산시에 시범도시 조성을 위한 국가시범도시시행계획을 의결하여 2019년부터 2021년까지 3년간 약 2조 4,000억원을 투자하여 인공지능(AI)·데이터 센터 구축, 데이터 연계를 위한 IoT망 구축, 국내 중소·스타트업의 창업 지원, 글로벌 혁신기업유치 등을 추진할 예정이다[3].

스마트 도시에서는 수집되는 방대한 데이터를 활용하고 가치 창출을 강조하고 있다. 스마트 도시에 거주하는 개인들에게 맞춤형 서비스를 제공하고 도시 기능의 안전성을 확보하기 위해서는 사람들의 시설물 이용 패턴, 개인별 활동 정보 등이 필요하다. 발전하는 도시 기능과 개인 삶의 편의성이 높아지는 반면, 개인정보의 노출과 유출의 위험도 동시에 같이 높아질 수밖에 없다.

2014년에 발생하였던 신용카드 3개사(KB, NH, 롯데)에서 약 1억여 건의 개인정보를 대출광고업체에 판매, 포스 단말기 관리업체의 서버에서 신용카드정보 유출, 농협생명에서의 정보유출 등은 금융회사의 대표적인 개인정보유출 사고이다[3].

또한 같은 해에 유통회사인 홈플러스가 경품행사시 수집한 개인정보를 보험회사 등에 판매하여 약 150억여 원의 부당 이득을 취득한 개인정보 판매에 이어 2019년에는 5만여 명의 개인정보가 유출되는 사고가 발생하였다. 국민건강보험공단의 직원들은 사적 이익을 위해 개인정보를 무단으로 열람하고 유출하여 파면 및 해임 등의 조치가 되었다. 이와 같이 개인정보의 노출과 유출은 정보주체인 개인은 물론이고 사회적으로도 많은 부작용과 후속처리비용을 요구한다.

4차 산업혁명 시대의 도래로 일상 활동의 전 영역에서 정보통신기술(ICT)에 대한 의존이 심화되고 있다. 사이버 공간에서는 사회관계망서비스(SNS), 클라우드 등에 해킹하여 개인정보 유출 등 사이버 범죄의 발생도 해마다 증가하여 정보통신기술(ICT)의 보안 위협에 대한 보안대책도 요구되고 있다[4].

지능정보기술의 고도화에 따라 이러한 위협은 미래사회에서 개인정보의 수집 및 활용의 필요성과 더욱 상충될 것이다.

2019년 12월에 국회 법제사법위원회 전체회의에서 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(일명, 정보통신망법), 신용정보의 이용 및 보호에 관한 법률(일명, 신용정보보호법) 등 이른바 데이터 3법이라 불리 우는 이 세 가지 법안이 국회와 정부 그리고 기업의 절실한 요구와 필요 속에서 처리되고, 본회의에 상정되었다. 개정안이 의결되

어 기술의 발전에 따른 법규의 뒷받침은 필수이다.

데이터 3법은 개인정보 사용자가 수집하고 이용 할 수 있는 개인정보의 범위를 확대하고 개인정보 데이터 보관 장소 이동 등에 관한 규제를 완화하는 것이 주요 내용이다. 이는 인공지능(AI)과 빅데이터의 활용을 위해서 위치정보의 보호 및 이용 등에 관한 법률(일명, 위치정보법)과 함께 개정이 필요한 법안들이다. 만약 이번 개정안이 의결되지 않는다면 기업이 보관중인 개인정보를 기업의 서버에서 클라우드 전문 업체로 옮기기 위해서 개인별로 연락을 하여 동의를 얻어야 해서 사실상 데이터를 옮기는 것은 불가하며 결국 서버를 증설해야 해서 비용증가로 인한 기업경쟁력 약화로 이어질 수밖에 없다. 구글과 페이스북이 네이버나 카카오보다 경쟁력이 월등하게 차이가 나는 원인은 바로 이러한 규제에 있다. 글로벌 업체인 이들은 개인정보 수집 시 한 번의 이용자 동의로 수집하는 개인정보의 항목이 50개가 넘으나, 국내 업체는 개인정보보호법, 온라인 개인정보 취급 가이드라인(정보통신위원회) 등의 규제 때문에 네이버는 18개, 카카오는 12개로 제한된다[5].

이러한 현상이 사이버 안보가 강조되는 지능정보사회에서 관심의 대상이 되는 것은 그 개인이 누구인가에 따라서 사안이 더욱 크게 확대 될 수도 있다는 것이다. 국가가 보호하는 주요 요인이나 과학기술자 등의 개인정보 노출과 유출은 국가 안보에도 영향을 줄 수 있다. 사이버 안보가 강조되는 이유 중 한 가지는 정보통신기술(ICT)이 급격하게 발전하는 환경에서 군사정보, 산업정보, 신호정보, 영상정보, 인간정보 등 다양하고 방대한 정보를 보호하여 국익을 지키기 위해서다. 따라서 개인정보를 보호하는 것은 곧 국가 안보를 보호하는 것이라 할 수 있다.

한국은 4차 산업혁명 시대의 도래에 따라 급격한 정보통신기술(ICT)의 변화를 겪고 있다. 무엇보다 인공지능기술과 데이터 활용기술이 융합되어 고도화된 정보처리를 하는 지능정보기술이 핵심적인 요소가 되었는데, 이의 발전을 위해서는 빅데이터가 필수적이며 인공지능(AI)도 빅데이터가 입력이 되어야만 신뢰도 높은 분석이 가능하다.

빅데이터 활용을 위한 대규모의 개인정보는 사물인터넷(IoT), 모바일 기기, 사회관계망서비스(SNS), 각종 센서 등 다양한 방식의 네트워크 접속을 통하여 수집되고, 향상된 데이터 분석 기술을 통한 개인 식별로 개인정보의 노출과 유출 등으로 사회문제화 되어가고 있다. 그러나 스마트 도시와 같이 도시 기능과 사람의 생활양식을 향상하기 위하여 정보통신시스템과 네트워크로 초연결된 지능정보사회에서는 인공지능(AI)과 빅데이터 운영을 통한 사회적 가치 창출을 위해서 개인정보의 이용은 필연적이다.

본 연구는 4차 산업혁명기 인공지능(AI)과 빅데이터 운영으로 사회적 가치를 창출하기 위한 개인정보의 보호와 이용에 관하여 연구한 것이다. 연구를 통해 인공지능(AI) 운영에 필수인 빅데이터의 원천이 되는 개인정보를 사이버 안보의 강화와 정보보호 측면에서 보호하고 이용하기 위한 법제적, 정책적, 기술적 방안을 마련하는데 기여하고자 한다.

2. 선행연구 검토와 분석의 틀

박국흠은 '수집된 정보'의 개념을 제시하여 그것이 개인정보보호, 공공재로서 공익성을 가지고 있으므로 정보 수집자의 전유물이 아님을 강조하였다. 그리고 현재와 같은 정보 제공 동의에 의한 데이터 이용체제는 데이터 거버넌스를 적용할 수 없으며, 이러한 현상을 개선할 수 있는 데이터 거버넌스를 위해서는 정보 제공 동의 체계 개선을 주장하였다. 그러나 정보 제공 동의 체계에 대한 구체적인 개선 방안을 제시하지 못했다[6].

오승환은 현행의 개인정보보호법에서 요구되는 사용자의 개인정보 이용을 위한 사전 동의 제도의 예외 범위를 더욱 확대하고, 빅데이터 기술에 의해 생산된 식별이 가능한 개인정보를 사후에 통제하는 사후통제권과 처음부터 비식별화 정보가 되는 것을 거부할 수 있는 개인정보통제권을 정보주체인 개인에게 부여할 것을 주장하였다. 사전 동의 제도의 예외를 확대하기 위해 정보처리 단계에서 비식별화 등 보안적인 조치를 제시하였으나 비식별화된 개인정보도 빅데이터 분석과정에서 다른 데이터와 결합하여 식별가능한 개인정보를 생산 할 수 있기 때문에 기술적 보완에 대한 심도 있는 연구가 필요하다[7].

김태오는 개인정보보호규제의 개선을 위한 단초를

찾고자 규범조화적인 개인정보보호 규제의 필요, 개인정보보호 규제의 초점을 이용 중심에서 리스크 관리 중심으로의 전환, 데이터 이용 상황과 중요성에 따라 사전 동의와 사후 거부에 따른 데이터 수집과 이용의 안분, 정보주체의 동의권 행사 행태를 고려하여 사전 동의제와 사후 거부제를 혼합하는 방안을 주장하였다. 이러한 주장은 헌법에 근거한 개인정보자기결정권의 본질에 비추어 볼 때 위헌의 소지가 있을 수 있으며, 정보통신기술(ICT)의 급격한 발전행태는 개인정보보호 규제의 초점을 리스크 관리 중심으로 할 수 있는 또 다른 관리기술의 개발을 필요로 하여 추가적인 사회적 비용이 발생 할 수 있다[8].

권헌영 등은 개인정보 가운데에는 프라이버시의 속성이 강한 것과 재산권의 속성이 강한 것이 혼재되어 있다는 점을 이해하고 다양한 상황별로 보호가 필요한 법익에 걸맞은 적확한 규제가 이루어지도록 하기 위하여 사전 동의와 같은 형식적인 절차의 준수 보다는 개인정보 제공 당시의 전후 상황 또는 정보주체의 합리적인 기대 범위 내에서의 개인정보 처리를 요구하는 실질적 사후적인 규제 체계로의 개편, 개인정보보호법을 일반법으로 하여 모든 상황에 대하여 규제하는 것은 사실상 제한되므로 산업 분야별 특성을 반영한 개별법을 중심으로 개인정보를 보호하는 체계를 마련할 것을 제시하였다. 그러나 사후적인 규제 체계로의 개편은 사전 동의 체계에 비하여 상대적으로 추가적인 시간과 비용이 발생할 수 있어 오히려 개인정보의 보호와 이용이 더욱 제한될 수 있다[9].

김용대 등은 데이터 거래의 활성을 위해 법률적 책임을 감면해주는 데이터거래소의 설립과 데이터를 제공하기 이전에 개인의 특성을 나타내는 정보를 보호하거나 제거하는 비밀보호 조치의 선행을 주장하였다. 그러나 법률적 책임을 감면해 주는 데이터거래소는 거래소 이외의 곳에서 위법적 거래를 발생 할 수 있으며, 개인의 특성을 제거한 정보라도 생산과정에서 다른 정보와 결합하여 식별이 가능한 개인정보가 생산될 수 있는 기술적 가능성이 있다[10].

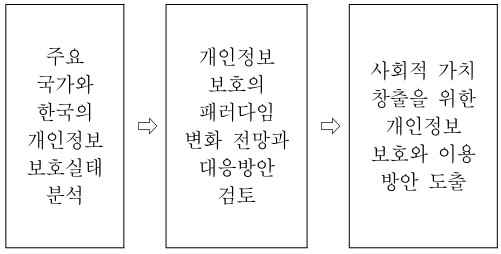
허성욱은 개인정보보호 법제의 정착을 통해 빅데이터에 의한 가치 창출에 기여하는 법규의 집행을 위해서는 개인정보보호 관련 법제의 전체적인 정비, 담당부서를 정비하여 법제도 간에 상호 중복이나 모순되는 내용의 정비, 빅데이터 산업의 성공적인 정착과 발전을 위한 개인정보의 개념 및 보호의 범위에 대한 재검토, 개인정보의 유형별로 보호의 방식을 사전 방식과 사후 거부 방식으로 달리하는 법제의 개선이 필요하다고 제시하였다. 이는 행정청마다 개인정보보호와 관련한 법률의 제개정을 소관하여 상호 중복되거나 모순되게 집행하는 경우가 있어 개선의 필요는 있겠으나 행정청 조직 개편의 측면보다는 법제적 측면에서 해결하는 것이 우선 필요하다[11].

윤상오는 개인정보보호를 통한 신뢰확보를 위해서 법·제도적 정비, 정책추진의 투명성 유지와 공개, 전자정부의 기능에 대한 예측 및 통제가능성, 개인정보 관련 업무를 담당하는 공무원의 마인드와 윤리의식, 개인정보와 사생활 보호에 대한 국민의 마인드와 철학 구비, 전자정부 정책 추진시 정부와 시민 간 상호 이해와 존중, 참여와 공유를 통한 거버넌스 형성을 하는 것이 필요하다고 주장하여 정부의 개인정보관련 정책 추진의 투명성 확보와 시민 참여, 전자정부 정책 추진에 대한 신뢰 형성, 공무원과 국민의 개인정보 보호에 대한 마인드 등에 대하여 강조하였다[12].

선행연구 검토를 통하여 4차 산업혁명기에 빅데이터의 활용을 통한 사회적 가치 창출과 개인정보보호를 위해서는 개인정보보호 관련 법규와 정책의 개선 그리고 개인정보가 식별 되지 않는 기술적 보완이 강조되고 있음을 알 수 있었다.

본 연구의 목적인 4차 산업혁명기 인공지능(AI)과 빅데이터의 운영으로 사회적 가치를 창출하기 위한 개인정보보호의 패러다임 전환을 모색하기 위하여 <표 1>과 같은 분석의 틀을 도출하였다.

<표 1> 분석의 틀



3. 주요 국가들의 개인정보보호 실태 분석

3.1 빅데이터의 특징과 개인정보 데이터

4차 산업혁명기에는 사물인터넷(IoT)에 의해 개인정보가 수집되고 빅데이터가 되어 인공지능(AI)이 이를 분석하고 예측하여 가치를 창출한다. 기술의 발전으로 기존에는 효율성이 없었던 비정형데이터 조차도 가치와 의미가 있는 정보를 생산하여 새로운 사회적 효율성과 가치를 창출한다. 그러나 가치 창출을 위한 분석의 토대가 개인정보인 경우에는 개인의 프라이버시를 침해할 우려가 있다. 따라서 빅데이터 이용에 따른 사회적 가치와 효율성의 창출을 위해서는 개인정보의 보호와 이용에 따른 상충의 해결이 필요하다.

인공지능(AI)의 신뢰도 높은 분석에 필요한 데이터는 대규모의 방대한 빅데이터로서 이의 사전적 의미는 현재의 정보관리와 분석체계의 적용이 제한되는 대용량의 데이터를 의미하며, 일반적인 데이터 베이스 소프트웨어의 정보처리능력을 초과하는 대규모의 데이터로 정의된다[13,14].

정보통신기술(ICT)이 발전 할수록 빅데이터 개념은 데이터 그 자체만이 아닌 방대하고 다양한 데이터를 분석하여 가치 있는 정보를 생산할 수 있는 기술과 시스템 설계 방식을 의미한다. 이는 구글, 페이스북, 아마존과 같이 빅데이터를 활용하는 인터넷 플랫폼 글로벌 기업들의 경쟁력과 관련하여 중요한 의미를 가진다[15,16].

빅데이터 분석기술은 기존의 정보처리 분석체계의 대상인 정형 데이터 이외에도 일정한 패턴과 형식이 없어 데이터 베이스에 분석되지 않은 사회관계망서비스(SNS)에 게시된 이미지, 동영상 등 비정형 형태의 데이터도 분석이 가능하다[17,18]

빅데이터와 관련하여 개인정보보호가 문제가 되는 것은 빅데이터의 개인정보 수집에 의미를 두는 것이 아니고, 수집된 정보를 분석하여 새로운 정보를 생산할 수 있는 능력을 갖추고 스스로 발전하는 것이 가능하기 때문이다. 이러한 빅데이터 기술의 특징에 따라 개인정보가 수집되고 생산되어 정보주체인 개인이 예상하지 못한 범위에서 그 정보가 이용될 수 있다는 것이다. 그러나 빅데이터 활용에 따른 한정된 자원의 효율성 증대와 사회적 가치의 창출로 인한 인간생활의 편익증진도 중요하기에 정보주체인 개인의 정보보호와 상충을 해결하여 균형 있고 조화로운 지능정보사회를 이루어야 할 필요성이 커지고 있다.

3.2 주요 국가들의 개인정보보호 실태 분석

유럽연합(EU)은 1980년대에 개인정보보호를 위한 법률을 제정하였으며, 프라이버시 보호의 일환으로 개인정보보호를 위한 회원국들의 입법 요구와 유럽연합(EU) 내에서 동일한 보호체제를 가동하여 원활환 디지털 거래를 촉진하기 위해 1995년에 '개인정보의 처리와 유통에 관한 개인정보보호 지침(Data Protection Directive)'을 제정하여 미국과 다르게 개인정보보호를 위한 통일된 법규범이 있는 것이 특징이다[19,20].

그러나 4차 산업혁명기 정보통신기술(ICT)이 발전되는 상황에서 효율적인 개인정보 이용의 필요성이 강조되자 기존 법규의 적용에 한계가 있어 2016년 4월 27일 유럽연합(EU)은 '일반개인정보보호규정(GDPR: General Data Protection Regulation)'을 제정·공표하였다. 이는 정보처리자의 정당한 이익을 위해 필수적인 경우에는 면책가능성을 열어두고, 추가적인 정보주체의 사후통제권을 강화한 것이다. 자연인의 관심사, 주관적 가치관, 행동의 특성 등을 분석하고 예측하는 정보처리를 '프로파일링(Profiling)'이라 정의하고, 프로파일링이 수행될 때 정보주체인 개인에게 이에 대하여 반대할 수 있는 권한을 부여하고 있다. 또한 개인정보가 판매 목적으로 처리되는 경우에도 마찬가지로 정보주체인 개인은 언제든지 반대할 수 있는 권한을 보유한다[21].

미국은 유럽연합(EU)과 다르게 국가적으로 적용되는 개인정보보호법은 두지 않고, 산업 분야별로 해당 법규가 개인정보보호를 위한 내용을 규정하고 있다. 2013년부터 연방거래위원회(FTC)는 소비자 동의 없이 모바일에서 개인정보를 수집하는 행위에 대하여 가이드 형식으로 주의를 주었다. 개인정보 중에서도

상대적으로 민감하다고 할 수 있는 위치정보에 관하여는 개인의 접근을 허용하고 명시적인 동의와 통지의 필요성을 강조한다. 또한 소비자가 인식하지 못한 상태에서 앱을 설치한 기기의 위치, 제3자에게 개인정보를 정보주체인 개인의 승인 없이 제공하는 행위에 대하여 규제한다. 1996년에 제정된 '건강보험 이전과 책임에 관한 법(HIPAA: Health Insurance Portability and Accountability Act)'에 따라 제정된 '개인의료정보 보호와 이용을 위한 규칙(HIPAA Privacy Rule)'은 개인의 의료정보 이용에 대한 가이드라인 역할을 한다. 이 규칙에 따라서 비식별 조치된 개인의 의료정보에 대한 보호규제를 제외하여 사용자가 자유롭게 이용 및 제공할 수 있어서 의료정보의 효율적인 이용이 가능하다. 이 규칙은 개인의 의료정보 이용을 목적으로 제정된 것은 아니지만, 비식별 조치된 개인의 의료정보 이용은 다른 분야에서의 개인정보 이용을 위한 가이드의 역할을 해준다[22].

일본의 개인정보의 보호에 대한 법률 체계는 행정기관과 독립행정법인 등이 보유한 개인정보보호에 관한 법률, 각 지방공공단체에서 제정하는 개인정보보호조례 등으로 구성되어 있다. 또한, 정보통신, 의료, 금융 등 각 산업 분야에서 개인정보의 보호를 위한 가이드라인이 정해져 있다. 일본의 개인정보보호법에서는 개인정보를 '생존하는 개인의 식별할 수 있는 정보' 라고 규정하는데, 이는 유럽연합(EU)과 달리 상품의 검색, 열람, 구매 이력과 같은 행동 이력은 개인이 식별 되지만 않으면 개인정보로서 취급되지 않는다[23].

한국의 개인정보보호 법규는 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법), 신용정보의 이용 및 보호에 관한 법률(이하 신용정보보호법), 위치정보의 보호 및 이용 등에 관한 법률(이하 위치정보법) 등을 중심으로 개인정보보호에 중점을 두고 있어서 인공지능(AI)과 빅데이터의 활용을 위한 개인정보의 이용에 제한이 있다. 개인정보의 활용만을 강조하면 정보주체인 개인의 기본권을 침해할 우려가 있으나, 현행 개인정보보호 관련법들은 개인정보 활용의 비중이 점차 커지는 최근 정보통신기술(ICT)과 산업의 변화를 반영하기에는 제한이 있다. 반면에 2016년에 방송통신위원회 등 정부 관련부처가 정보통신기술(ICT) 관련 산업의 발전을 위해서 마련한 '개인정보 비식별 조치 가이드라인'은 정보산업의 활성화에만 치중하여 비식별 조치만 되면 개인정보의 이용과 양도를 허용하여 개인정보보호가 취약해 질 수 있다는 우려를 받고 있다. 가이드라인은 개인정보가 비식별 조치되면 식별이 될 가능성을 부정하여 빅데이터 기술력과도 맞지 않다. 이는 개인정보에 대한 식별의 가능성이 낮을수록 프라이버시가 침해 받을 가능성도 낮아지지만 상대적으로 활용 가치도 함께 떨어져서 산업계에서 개인정보 활용에 따른 가치를 높이거나 유지하기 위한 조치를 반영한 것으로 볼 수 있다. 따라서 개인정보의 비식별화 조치에 대한 현재의 가이드라인은 개인정보의 보호와 이용 모두에 적용하기에는 부적합하다. 반면 현행 개인정보보호법은 개인정보의 수집과 이용을 규제하기 위해 사용하는 '정보주체의 사전 동의' 요건은 어떠한 경우에도 동의 없는 정보사용을 금지시하여 과도하게 경직적이라는 의견이 있다. 현행 법제에 의하면 정보처리자가 빅데이터의 특성에 따라 부득이 식별가능한 개인정보를 생산한 경우에도 사전 동의 없는 개인정보의 수집행위가 되어 법률 위반이 될 수 있다[24].

한국은 개인정보보호를 위해 2013년에 행정자치부(현, 행정안전부)가 '공공정보 개방 및 공유에 따른 개인정보보호지침'을 마련하였으며, 2014년에는 '개인정보 비식별화에 대한 적정성 자율평가 안내서'를 마련하였다. 방송통신위원회도 2014년에 '빅데이터 개인정보보호 가이드라인'을 제정하였고, 2015년에는 미래창조과학부(현, 과학기술정보통신부)가 빅데이터 활용을 위한 '개인정보 비식별화 기술 활용 안내서'를 출간하였다. 특히 2016년에 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부 합동으로 개인정보를 비식별화 하여 이용 또는 제공하려는 사업자가 준수해야 할 '개인정보 비식별화 가이드라인'을 제정·발표하여 개인정보의 이용을 통해 정보통신기술(ICT) 관련 산업의 발전을 지원하고자 하였다. 이는 <표 2>와 같이 사전검토, 개인정보 비식별화 조치, 적정성 평가, 사후관리의 4단계로 구분되어 있다[25].

<표 2> 개인정보의 비식별 조치 및 사후관리 절차

1단계 (사전 검토)	⇨	2단계 (비식별 조치)	⇨	3단계 (적정성 평가)	⇨	4단계 (사후 관리)
개인 정보 (식별 정보)		개인 식별 요소 제거		부적정시 2단계로 이동		비식별 정보

이러한 가이드의 기본 취지는 '개인정보라 할지라도 정해진 4단계를 거쳐서 비식별 처리가 된 경우에는 개인정보로 취급하지 않으며 따라서 당사자의 동의 없이 사용할 수 있다'는 것으로 이는 이전과 달리 기술 환경의 변화에 따라 개인정보를 보호하는 것에서 이용하는 것으로 보호의 개념을 달리한 것으로 볼 수 있다[26].

4. 개인정보보호의 패러다임 변화 전망과 대응 방안

4.1 법제적 변화 전망과 대응 방안

주요 국가들은 자국의 개인정보보호를 정보통신기술(ICT)의 발전에 따라 데이터로서의 개념을 부여하여 이용의 대상으로서 범위를 넓혀나가고, 비식별되는 개인정보의 이용에 대하여는 규제하지 않는 쪽으로 법규를 마련하고 있다.

정보통신기술(ICT)이 급격하게 발전하는 지능정보사회에서 개인정보보호 법제는 개인정보보호를 위한 획일적인 기준을 제시하기 보다는 규제로 인해 얻어지는 법익(개인정보보호 강화 등)과 규제로 인해 제한되는 법익(개인정보를 데이터로 하는 산업 등)간 균형이 되도록 하는 방안을 모색하는 것이 필요하다. 또한 개인정보보호법은 개인정보를 수집할 때에는 법률에 명시된 예외사유가 없는 한 반드시 사전에 정보주체인 개인의 명시적 동의를 받아야 한다고 규정하고 있다. 그러나 개인정보보호와 관련된 일부 판례에 비추어 볼 때, 현행 법조문에 규정되어 있는 사전 동의라는 법적 기준이 정보통신기술(ICT)의 발전 현실에 비추어 볼 때 법 개정의 필요성이 있겠다[27].

데이터 통합 시 발생하는 개인정보 식별의 위험을 해결하는 기술적 방법론이 아무리 발달하여도 개인정보의 유출에 따르는 법률적 위험은 상존한다. 이러한 법률적 위험은 실제 데이터를 통합하여 새로운 가치를 창출하려고 시도하는 관련 산업의 성장은 물론이고 인공지능(AI)의 운용을 제한하고 있다. 따라서 데이터 결합에 의한 가치 창출을 통해 국가 경쟁력 향상을 위해서 법률적 위험을 제거하거나 약화시킬 수 있는 법제적 장치가 필요하다.

4.2 정책적 변화 전망과 대응 방안

정보통신기술(ICT)의 급격한 발전은 과거에 사회적 가치가 없었던 개인에 관한 정보와 분석 결과물을 가치 있는 수익을 창출하는 자원으로 만들고 있어 개인정보를 이용하기 위한 수요가 상시 존재한다. 따라서 개인정보의 노출과 유출에 대처하는 단기적 정책이 아닌 개인정보에 대한 수요를 사회적으로 용인되고 보편타당하고 합리적인 범위에서 허용되는 개인정보의 이용기준을 정보통신기술(ICT)의 발전 추세에 부합하게끔 마련할 필요가 있다. 헌법상 기본권 원칙과 개인정보보호법에 의거하여 공기관과 사기업의 기업 활동간 의도하지 않게 습득되거나 생산된 개인정보는 정보주체인 개인이 소유권을 보유하고 원칙적으로 동의가 없는 정보의 사용은 제한되어야 한다는 강조는 빅데이터의 원천이 되는 개인정보의 이용이 통제되어 사회적 효율성을 증대하고 가치를 창출하는 분석 도구로서의 이용을 제한하게 되어 개인은 물론이고 국가마저 사회적 가치를 공유하지 못하는 결과를 초래 할 수 있다. 특히, 빅데이터를 이용한 분석결과를 이용하는 정보주체인 개인의 기대와 만족도를 향상 시킬 수 있는 경우에는 개인정보의 이용을 허용하는 법제적, 정책적 시스템의 구축이 반드시 사업자만을 위한 것이라고 볼 수는 없다.

데이터 경제의 등장과 함께 데이터 구매자와 판매자의 정보를 중개하는 한국데이터진흥원의 데이터스토어 같은 데이터 장터가 온라인에서 운영되고 있다. 이곳에서는 데이터 제공자가 판매하는 데이터 만을 거래하여 데이터 거래에 따른 공익성의 확대에 한계가 있다. 수집된 개인 정보의 공익성을 극대화 할 수 있도록 데이터 거래를 연결 하여 더욱 큰 가치를

창출할 수 있는 인프라 구축과 플랫폼 마련이 필 요하다[28].

이를 위해, 수집된 정보의 활용에 대한 결정을 대표할 조직권과 이들 대표들에 의한 대표선출이나 위원회 구성, 정보 활용 동의, 비식별화 조치, 개인정보보호 및 정보보안, 정보주체들의 기여도 평가 및 이에 대한 보상, 정보의 판매에 관한 사항 등의 결정에 참여 하여 개인정보의 사용자와 교섭하는 권한과 데이터 이용에 따른 이용수익권 등을 검토해 볼 수 있다. 이는 개인정보를 데이터로서 합당하게 규정하여, 데이터의 공익적·합리적 이용을 증진시킬 것이다[29].

지능정보사회에서 개인정보는 정보주체인 개인은 물론이고 사회적 가치를 더욱 향상 시키는 자원으로서 활용되도록 정책이 디자인 되어야 한다.

4.3 기술적 변화 전망과 대응 방안

개인정보의 보호와 이용을 위해 유럽연합(EU), 미국, 일본, 한국 등 주요 국가들은 비식별화, 익명화, 가명화에 대한 개념과 관 규정을 마련하였다. 안전하고 효율적으로 개인정보를 이용할 수 있는 여건을 마련하기 위해 많은 국가들이 개인정보의 비식별 조치와 관련한 정책을 마련하고 법규를 정비하였다. 국가마다 개인정보의 보호와 이용에 대한 접근방식과 해결 방안은 다르지만, 개인을 식별할 수 없는 정보는 이용 가능한 정보로 분류한다. 개인정보에서 개인 에 관한 식별 가능성을 제거하는 기술적 처리와 일련의 과정을 비식별화로 정의하며, 비식별화와 익명화의 개념이 동의어처럼 사용되기도 한다.

가명화된 개인정보는 비식별 정보로서 최초 수집된 목적 이외로도 이용이 가능하지만, 재식별 될 기술적 가능성이 있어 개인정보보호 규제의 적용을 받는다. 이는 추가적인 정보와 결합되어 재식별이 가능할 수가 있어서 재식별이 불가한 익명화와는 구분된다. 유럽연합(EU)은 가명정보라는 개념을 마련하여 빅데이터의 이용과 개인정보의 보호를 동시에 추진하는 융통적인 방법을 선택한 것이다[30].

국제전기통신연합 전기통신표준화 부문(ITU-T)의 비식별 처리 표준 개발에 의하면 익명화는 식별이 가능한 데이터와 개인정보 주체 간의 연관성을 제거하는 과정이고, 가명화는 식별된 데이터를 대체하는 개인정보에 적용하는 과정이다. 비식별화는 일련의 식별된 데이터와 개인정보 주체 간의 연관성을 제거하는 모든 과정에 대한 일반적인 용어이다[31].

유럽연합(EU)은 1995년에 제정한 개인정보의 처리와 유통에 관한 개인정보보호 지침(Data Protection Directive)상의 가명 처리된 정보와 익명화 정보는 강제력을 갖추지 못했으나, 2016년에 제정된 일반개인정보보호규정(GDPR)에는 가명정보 규정을 익명처리와 구분되게 명시하였다[32].

미국 연방거래위원회(FTC)는 2012년에 모든 분야에 적용이 되는 개인정보 비식별 조치 및 규정에 관한 권고문을 발표하였다. 이 규정은 개인, 컴퓨터, 기타 기기로부터 개인에 관한 정보를 수집하거나 이용하는 상업적 실체 전부에 적용 된다[33,34].

일본은 2003년 개인정보를 포괄적으로 규율하는 개인정보의 보호에 관한 법률을 제정한 후, 2015년 전면 개정하여 2017년부터 시행중이다. 민간영역만 규율하여 하나의 법률로 공공과 민간을 모두 규율하는 한국과 다르다. 이 법률의 중점은 개인정보의 범위가 불명확하여 이용이 제한되었던 것을 해결하고 빅데이터 관련 산업을 활성화 하는 것이다. 또한 익명가공정보라는 새로운 개념을 정의하였는데 이는 개인정보를 식별이 가능하게끔 복원 할 수 없도록 가공된 정보를 말한다. 비식별화된 정보는 복원이 불가능하다는 전제하에 개인정보로서 보호 대상이 아닌 것으로 분류하고, 정보주체인 개인의 사전 동의 없이 최초 수집한 목적 이외의 용도로 이용할 수 있다. 다수의 익명가공정보를 결합하여 통계정보를 생산하거나, 개인과 관련이 없는 정보와 결합하여 통계적인 경향을 분석하는 것은 허용되나 익명가공정보를 다른 정보와 대조하는 재식별은 불가하다[35].

일본의 익명가공정보가 유럽연합(EU)의 일반개인정보보호규정(GDPR)의 가명화 정보와 유사한 개념인 것 같으나, 그 법적규제는 미국법에 따라 비식별 개인정보와 같이 개인정보가 아니기에 자유로운 이용이 가능하다.

한국 정부가 2016년에 발표한 '개인정보 비식별화 가이드라인'은 비식별화 조치 및 그 사후 사용을 <표 3>과 같이 가명처리, 총계처리, 데이터 삭제, 데이터

범주화, 데이터 마스킹 등의 기법을 이용하도록 규정하며 재식별이 되지 않도록 관리적·기술적 보호조치를 필수적으로 이행하도록 하고 있다[36].

<표 3> 비식별 조치 방법(예시)

처리기법	처리 전	처리 후
가명처리	홍길동, 35세	임꺽정, 30대
총계처리	홍길동 180cm, 임꺽정 170cm	물리학과 학생들의 키 합 : 350cm, 평균키 : 175cm
데이터 삭제	주민등록번호 900101-1234564	90년대생, 남자
데이터 범주화	홍길동, 35세	홍씨, 30~40대
데이터 마스킹	홍길동, 35세, 한국대 재학	홍OO, 35세, OO대학 재학

가이드라인에서는 비식별 조치를 유럽연합(EU)의 일반개인정보보호규정(GDPR)에 명시된 익명화와 동일한 개념으로 간주한다. 가명정보의 이용은 개인정보보호법에 의해서 불가하며 비식별 조치를 한 경우에는 개인정보에 해당되지 않는다. 그러나 이 가이드라인은 법적 지위가 불명확하다. 이에 의하면 비식별 정보는 수집 목적 외의 이용이 가능한 것 같아 보이나 개인정보보호법에 의해서 수집 목적 외 이용은 허용되지 않는다. 그래서 개인에 관한 식별이 가능한 요소를 정해 놓고 불필요한 요소는 삭제하며 비식별화가 필요한 경우에는 전문가의 검증을 받도록 하고 있다[37].

5. 결론 및 제언

4차 산업혁명기에는 사물인터넷(IoT) 기술로 디지털화된 대량의 정보를 수집하여 알고리즘에 의한 인공지능(AI) 분석으로 사회적 가치를 창출하기 위해서 개인정보의 보호와 이용의 조화가 필요하다.

포괄안보시대에서 사이버 안보가 강조되고 정보통신기술(ICT)이 급격하게 발전되어 지능정보사회가 구현될수록 사회적 가치 창출을 위한 개인정보의 보호와 이용에 대한 요구는 더욱 커질 것이다. 이러한 변화에 대비하기 위한 몇 가지 정책적 제언을 하고자 한다. 첫째, 국가사이버안보전략에 개인정보의 보호와 이용에 관한 내용을 명시하여 정부 기관별로 소관업무와 관련된 계획을 수립하고 추진해야 한다. 포괄안보시대에서는 사이버 안보의 중요성이 강조된다. 따라서 정부 기관별 소관업무와 관련된 개인정보의 보호와 이용에 관한 계획을 수립하여 추진한다면 관련 법률과 연계성을 유지하고 국가사이버안보의 강화와 확립이 가능하다.

둘째, 개인정보의 이용에 관한 정책과 제도를 4차 산업혁명기에 부합하게끔 개방적으로 정비해야 한다. 정보통신기술(ICT)이 발전하면서 지능정보사회의 구현을 정책적으로 추진하는 상황에서 개인정보는 빅데이터의 원천이 된다. 인공지능(AI)은 이를 분석하여 다양한 현안 문제에 대한 해결방안을 제시한다. 따라서 유럽연합(EU)의 일반개인정보보호규정(GDPR)과 같이 환경변화가 반영되는 정책과 제도의 정비가 필요하다.

셋째, 정보주체인 개인의 사전 동의에 관하여 폭넓게 법적 권한을 부여해서 합리적인 개인정보의 보호와 이용 여건을 보장해야 한다. 본인의 의사에 따라 이루어지는 개인정보에 관한 사전 동의를 하는 시점에서 제공되는 개인정보의 종류, 이용범위와 기간, 상업적 이용, 목적 외 이용, 타 기관으로의 제공 등을 다양한 항목별로 당사자가 직접 선택하도록 법률로서 정한다면 동의에 따른 개인의 기본권을 포기하는 것이 아닌 법률로 보호할 수 있으며, 개인정보 사용자도 다양한 정보를 추가 또는 사후 동의를 받고자 하는 노력의 낭비 없이 이용 또는 제공 할 수 있다.

넷째, 개인정보 비식별 조치 가이드라인의 내용 중에서 개인정보보호법과 상충되는 내용을 정비하고 법제화해서 실효성을 갖춰야 한다. 개인정보의 이용을 넓게 해석하는 가이드라인의 내용을 법제화 한다면 개인정보 이용 시 발생 할 수 있는 위법적 행위를 제거하여 이를 이용하고자 하는 사용자의 법적 부담을 줄이거나 제거 할 수 있으며, 개인정보의 이용 범위가 더욱 확대되어 이에 따른 사회적 가치 창출도 한층 커질 것이다.

참 고 문 헌

[1] 신진, “한국의 국방정책과 안보”, 국제정치논집, 제40권, 제2호, p. 125, 2000.

[2] 최원상, 신진, “4차 산업혁명기 정부 비상대비정책의 패러다임 전환에 관한 연구”, Crisisonomy, 제15권, 제7호, p. 34, 2019.

[3] 정기석, “금융사 개인정보 유출 방지 방안에 관한 연구”, 융합보안논문지, 제14권, 제4호, p. 110, 2014.

[4] 김연수, “치안분야의 정보통신기술 활용방안 연구”, 융합보안논문지, 제16권, 제2호, p. 24, 2016.

[5] 전자신문, https://www.etnews.com/201910010002 67.

[6] 전자신문, https://www.etnews.com/201909260001 85

[7,28,29] 박국흠, “수집된 정보의 공익성에 관한 고찰”, 정보화정책, 제26권, 제1호, pp. 31-42, 2019 (봄).

[8,21,22,24] 오승환, “빅데이터 산업의 활성화와 개인정보 보호를 위한 법제도 개선의 연구”, 아주법학, 제11권, 제4호, pp. 392-407, 2018.

[9] 김태오, “데이터 주도 혁신 시대의 개인정보자기결정권”, 행정법연구, 제55호, pp. 48-51, 2018.

[10,27] 권헌영, 윤상필, 전승재, “4차 산업혁명시대 개인정보권의 법리적 재검토”, 저스티스, 제7권 제42호, pp. 24-37, 2017.

[11,23,26] 김용대, 장원철, “인공지능 산업 육성을 위한 개인정보보호 규제 발전 방향”, 경제규제와 법, 제9권 제2호, pp. 171-174, 2016.

[12] 허성욱, “한국에서 빅데이터를 둘러싼 법적 쟁점과 제도적 과제”, 경제규제와 법, 제7권 제2호, pp. 18-19, 2014.

[13] 윤상오, “전자정부 구현을 위한 개인정보보호 정책에 관한 연구”, 한국지역정보화학회지, 제12권 제2호, pp. 22-26, 2009.

[14] 김수연, “빅데이터 산업 활성화를 위한 개인정보 보호규제 개선 검토”, 한국경제연구원, KERI Brief 15-28, pp. 5-6, 2015.

[15] McKinsey Global Institute, Big data: The next frontier for innovation, competition, and productivity, 2011.

[16] Philip Carter, ‘빅데이터 분석: CIO를 위한 미래 지형적 아키텍처, 기술 그리고 로드맵’, IDC 백서, p. 5, 2011.

[17] Xavier Boutin & Georg Clemens, Defining ‘Big Data’ in Antitrust, Antitrust Chronicle, August, Vol. 2, 2017(summer).

[18] 이경규, ‘정보권력의 견제와 균형-빅데이터 환경의 함의를 중심으로‘, 법학연구, 제17권 제4호, pp. 51-52. 2014.

[19] Jason A. Kotzker, ‘The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad’, 15 St. Thomas L. Rev. 727, 748, 2003.

[20] ‘Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data’, Official Journal L 281, 1995.

[25,36] 정부부처합동, ‘개인정보 비식별 조치 가이드라인’, 방송통신위원회, 2016, https://kcc.go.kr/tsi/etc/search/search/ASC_integrationsearch.jsp?page=A10010000.

[30,37] 강혜영, 권헌영, “국내외 비식별화 현황분석을 통한 개인정보 활용정책 제언”, 융합보안논문지, 제19권, 제1호, pp. 42-45, 2018.

[31] 임형진, “빅데이터 환경에서의 개인정보 비식별 처리 방법 분석”, 전자금융과 금융보안, 제8호, pp. 10-37, 2017.

[32] 차상육, “EU 개인정보보호법제의 최근 입법과 시사점”, 정보법학, 제21권, 제1호, pp. 141-171, 2017.

[33] FTC, Protecting Consumer Privacy in an Era Rapid Change, Recommendation for Business and Policymakers, 2012

[34] 이대희, “개인정보 보호 및 활용방안으로서의 가명·비식별정보 개념의 연구”, 정보법학, 제21권 제3호, pp. 1-36, 2017.

[35] 이창범, “4차 산업혁명과 ICT법의 선진화 방향”, 정보과학회지, pp. 22-33, 2018.

[저 자 소 개]

최 원 상 (Choi, Won Sang)
1994년 2월 충남대학교 학사
2006년 8월 한성대학교 석사
現, 충남대학교 박사과정(군사학)
행정안전부 비상계획전문경력관
email : cws0314@korea.kr

이 종 용 (Lee, Jong Yong)
1983년 2월 육군사관학교 학사
1991년 12월 국방대학교 석사
2018년 2월 한남대학교 박사
現, 국방과학연구소 정책기획부
소요기획연구실 책임연구원
email : im2343@add.re.kr

신 진 (Shin, Jin)
1981년 2월 성균관대학교 학사
1984년 2월 서울대학교 석사
1992년 2월 서울대학교 박사
現, 충남대학교 정치외교학과 교수
email : jinshin@cnu.ac.kr