# 융합보안과 인권보장을 위한 법정책* **

양 천 수***

## I. 서 론

요즘 유행어가 되고 있는 '제4차 산업혁명'은 단순히 새로운 과학기술의 급격한 발전만을 뜻하는 것이 아니라, 현대사회의 패러다임을 근본적으로 바꾸고 있다. 동시에 법적 사고의 기본 틀 역시 바꾸고 있다.[1] 이와 더불어 제4차 산업혁명이 진행되면서 그 이전에는 경험하지 못하였던 새로운 법적 문제가 등장하고 있다. '융합보안' 문제 역시 그 가운데 한 예라 할 수 있다. '융합보안' 문제와 같이 제4차 산업혁명이 유발하는 새로운 법적 문제는 전통적인 법적 사고와 제도만으로는 적절하게 해결하기 어렵다. 이러한 문제를 해결하기 위해서는 새로운 법적 사고와 틀 위에서 법적 제도를 설계하고 이를 적용할 수 있어야 한다. 이 글에서는 어떤 측면에서 융합보안 문제가 새로운 법적 문제가 되는지, 이러한 융합보안 문제가 어떤 점에서 인권 문제가 되는지, 이를 해결하기 위해서는 어떤 법정책을 펼쳐야 하는지 살펴보도록 한다.

---

* 투고일자 : 2018. 12. 24. 심사일자 : 2018. 12. 26. 게재확정일자 : 2018. 12. 27.

** 이 글은 필자가 연구책임자로 참여한 연구보고서 『안전한 지능정보사회 구축을 위한 정보보호관련 법제도 개선방안 연구』(과학기술정보통신부, 2018)에서 필자가 집필한 부분을 대폭 수정 및 보완한 것입니다. 더불어 이 글은 필자가 이미 공간한 연구저서 『제4차 산업혁명과 법』(박영사, 2017)의 일부 내용을 포함하고 있습니다.

*** 영남대학교 법학전문대학원 교수・법학박사

1) 이에 관해서는 우선 양천수, 『제4차 산업혁명과 법』(박영사, 2017) 참고.

## II. 제4차 산업혁명과 사회구조의 변화

먼저 논의의 출발점으로서 제4차 산업혁명이 현대사회를 어떻게 바꾸고 있는지 살펴보도록 한다. 제4차 산업혁명에 관해서는 우선 두 가지 문제를 해결해야 한다. 첫째, 제3차 산업혁명과는 구분되는 제4차 산업혁명이 과연 존재하는가 하는 점이다. 둘째, 제4차 산업혁명에서 가장 본질적인 특성은 무엇인가 하는 점이다.

### 1. 제4차 산업혁명은 있는가?

현재 우리는 제4차 산업혁명을 기정사실로 받아들이고 있다. 이는 제4차 산업혁명을 제시한 클라우스 슈밥(Klaus Schwab)의 주장을 전적으로 수용한 것이다.[2] 그러나 슈밥 자신도 인정하고 있듯이, 제4차 산업혁명이 과연 존재하는지, 이미 진행 중인 제3차 산업혁명과 제4차 산업혁명 사이에 본질적인 패러다임 차이가 있는지 견해가 대립한다.

잘 알려져 있는 것처럼, 제1차 산업혁명은 증기기관에 기반을 둔 '본래 의미의 산업혁명', 제2차 산업혁명은 전기에 바탕을 둔 '대량생산혁명', 제3차 산업혁명은 컴퓨터와 인터넷이 초래한 '정보화혁명'을 의미한다. 이 중에서 제3차 산업혁명과 제4차 산업혁명 사이에 본질적인 차이가 있을지 의문을 제기할 수 있다. 왜냐하면 표면적으로 보면 제3차 산업혁명과 마찬가지로 제4차 산업혁명 역시 인터넷과 컴퓨터에 기반을 두고 있기 때문이다. 인터넷이 유선망에서 무선망으로 확대되고, 컴퓨터 역시 개인용 컴퓨터에서 스마트폰으로 다양해졌지만, 사회는 여전히 제3차 산업혁명이 야기한 '정보화사회'(information society)의 틀에서 벗어나고 있지는 않아 보이기 때문이다. 이 점에서 현대사회에서 진행되고 있는 과학기술의 발전은 제3차 산업혁명의 연장선상에 있다고 볼 여지도 있다. 그렇지만 필자는 슈밥이 주장하는 것처럼 제3차 산업혁명과 제4차 산업혁명 사이에는 본질적인 차이가 있다고 생각한다. 그 이유는 아래에서 살펴보는 것처럼, 제4차 산업혁명은 사회구조뿐만 아니라 우리의 사고 틀을 본질적으로 바꾸고 있기 때문이다.

---

2) 클라우스 슈밥, 송경진 (옮김), 『제4차 산업혁명』(새로운현재, 2016) 참고.

## 2. 제4차 산업혁명의 본질

### (1) '인간중심적 사고'에서 '탈인간중심적 사고'로

그러면 제4차 산업혁명의 본질적 특성은 무엇인가? 왜 우리는 제4차 산업혁명을 '혁명'으로 부를 수 있는 것일까? 필자는 제4차 산업혁명의 본질적 특성은 놀라운 속도로 발전하고 있는 최신 과학기술에서 찾을 수 있는 것은 아니라고 생각한다. ICT나 인공지능(AI), 생명공학(BT) 등과 같은 현대 과학기술의 정수가 제4차 산업혁명의 본질을 구성하는 것은 아니다. 그보다 더욱 중요한 것은 제4차 산업혁명이 우리 인간의 사고방식이나 사고 틀을 근본적으로 바꾸고 있다는 점이다. 이를 한 마디로 표현하면, 제4차 산업혁명은 기존의 '인간중심적 사고'를 '탈인간중심적 사고'로 바꾸고 있는 것이다.

### (2) 인간중심적 사고

그러면 '인간중심적 사고'란 무엇을 뜻하는가? '인간중심적 사고'란 말 그대로 생물학적 존재인 인간을 중심으로 하여 체계화된 사고방식을 말한다.[3] 따라서 인간이 아닌 존재, 가령 동물은 인간중심적 사고에서 주변적인 것으로 취급된다. 차별도 허용된다. 예를 들어, 인간이면 그 누구나 평등하게 누리는 '인권'(human rights)을 비인간적인 존재는 누릴 수 없다. 오히려 이들은 인권의 '대상'이자 수단이 될 뿐이다.

필자는 이러한 인간중심적 사고는 다음과 같은 사고로 구체화된다고 생각한다. '주체-객체 사고', '생명중심적 사고', '행위중심적 사고', '물리적 세계 중심적 사고'가 그것이다. 먼저 '주체-객체 사고'는 '주체'와 '객체'를 개념적·존재적으로 구분하면서 '주체'에 중심적인 지위를 부여하는 사고를 말한다.[4] 이때 '주체'는 당연히 인간이 되고, '객체'는 인간이 아닌 존재가 된다. 이러한 '주체-객체 사고'는 근대 이후에 형성된 법적 사고 및 법체계의 근간을 이룬다. 다음으로 '생명중심적 사고'는 이렇게 주체가 되는 인간은 생명을 갖고 있는 존재여야 한다는 사고를 말한다. 생명을 갖지 않은 존재, 가령 인공지능 로봇은 인간이 될 수 없기에 인간에게 부여되는 권리 역시 가질 수 없다. 여기서 말하는 생명은 탄소를

3) 인간중심적 사고에 관해서는 인간중심적 사고에 관해서는 양천수, "탈인간중심적 법학의 가능성: 과학기술의 도전에 대한 행정법학의 대응", 『행정법연구』 제46호(2016. 8), 1-24쪽 참고.
4) 이에 관해서는 우선 아르투어 카우프만, 김영환 (옮김), 『법철학』 (나남, 2007) 참고.

중심으로 하여 구성된 생명을 말한다. 나아가 '행위중심적 사고'는 탄소중심적인 생명으로 만들어진 인간이 주체로서 객체에 작용할 때 '행위'(Handlung)를 사용한다는 사고를 말한다. 다시 말해, 인간 주체는 행위를 통해서만 객체에 접근하거나 다른 인간 주체와 연결될 수 있다는 것이다. 바로 이 때문에 행위 개념은 전체 법질서에서 아주 중요한 개념으로 자리한다. 현행 법체계 및 법학에서 아주 중요한 지위를 차지하는 법률행위, 범죄행위, 행정행위, 소송행위 개념이 이를 잘 보여준다. 마지막으로 '물리적 세계 중심적 사고'는 인간 주체가 행위를 하는 공간은 물리적으로 실재하는 세계를 전제로 한다는 사고를 말한다. 물리적으로 실재하지 않는 세계는 인간 존재가 행위할 수 있는 공간이 아니기에 '인간중심적 사고'에서는 중요하지 않은 '가짜 세계'에 불과할 뿐이었다.

### (3) 탈인간중심적 사고

이렇게 오랫동안 우리의 법적 사고 및 법체계를 지탱하였던 인간중심적 사고는 최근 제4차 산업혁명이 진행되면서 '탈인간중심적 사고'로 대체되고 있다. 여기서 '탈인간중심적 사고'란 인간이 더 이상 중심적인 지위를 차지하지 못하는 사고를 말한다. 구체적으로 말하면, 인간중심적 사고를 구성하였던 '주체-객체 사고', '생명중심적 사고', '행위중심적 사고', '물리적 세계 중심적 사고'가 해체되는 사고를 뜻한다. 이를테면 인간이 아닌 존재, 즉 인공지능 로봇도 주체가 될 수 있는 가능성이 열리고 있다.[5] 생명 개념도 변화하여 기존의 탄소중심적 생명이 아닌 새로운 생명 개념이 출현할 수 있는 계기가 도래하고 있다.[6] '행위'를 대신하여 '소통'이 새로운 중심 개념으로 자리매김하고 있다.[7] 물리적 세계뿐만 아니라 비물리적 세계, 즉 사이버세계가 주체의 새로운 활동 영역으로서 그 중요성이 증대하고 있다. 마지막으로 '주체-객체 사고'를 대신하여 '체계-환경 사고'가 중심적인 지위를 차지하고 있다. 이처럼 제4차 산업혁명이 진행되면서 기존의 인간중심적 사고를 대신하는 탈인간중심적 사고가 사회 각 영역에서 우리의 전통적인 사고방식을 대체하고 있다.

---

5) 이에 관해서는 양천수, "인공지능과 법체계의 변화: 형사사법을 예로 하여", 『법철학연구』 제20권 제2호(2017. 8), 45-76쪽; "현대 지능정보사회와 인격성의 확장", 『동북아법연구』 제12권 제1호(2018. 5), 1-26쪽 등 참고.

6) 이를 보여주는 클라우스 에메케, 오은아 (옮김), 『기계 속의 생명: 생명의 개념을 바꾸는 새로운 생물학의 탄생』 (이제이북스, 2004) 참고.

7) 이는 독일의 사회학자 루만(Niklas Luhmann)이 정립한 현대 체계이론에서 확인할 수 있다.

## 3. 사회구조의 변화

이처럼 제4차 산업혁명은 우리의 사고방식을 바꾸고 있을 뿐만 아니라, 동시에 사회구조 역시 바꾸고 있다. 제4차 산업혁명으로 인하여 새로운 사회 패러다임이 출현하고 있다.

### (1) 초연결사회

제4차 산업혁명은 현대사회를 '초연결사회'(hyper-connected society)로 변모시키고 있다.[8] 제4차 산업혁명을 통해 세상의 거의 모든 것이 연결되는 사회가 출현하고 있는 것이다. 이렇게 현대사회가 초연결사회로 변모하는 데는 크게 두 가지 원인이 작용한다. 첫째는 정보통신망, 즉 인터넷망이 확장되었다는 것이다. 제3차 산업혁명이 시작될 즈음의 인터넷망은 유선망을 기본으로 하였다. 그렇지만 무선인터넷망이 실용화되면서 인터넷을 통해 진행되는 '소통'(communication)의 가능영역이 비약적으로 확대되었다. 둘째는 사물인터넷(IoT)이 등장했다는 것이다. 사물인터넷이 인터넷을 통해 이루어지는 소통에 참여하면서 사람과 사람 사이의 연결뿐만 아니라 사람과 사물, 사물과 사물 사이의 연결이 가능해졌다. 이를 통해 초연결사회가 구현되고 있는 것이다.

이렇게 현대사회가 초연결사회로 변모하면서 이에 연계하여 '빅데이터 사회'라는 현상도 등장하고 있다.[9] 무선인터넷망과 사물인터넷 등으로 초연결사회가 구현되면서 인터넷을 통해 진행되는 소통이 비약적으로 증가하였고, 이에 발맞추어 데이터 역시 기하급수적으로 증대하고 있다. 이를 통해 사회의 거의 모든 영역에서 빅데이터가 축적되고 있다. 이러한 빅데이터는 단순히 데이터 그 자체만으로 그치는 것이 아니라, 빅데이터 과학을 통해 새로운 가치나 통찰을 창출하는 새로운 자원으로 활용되고 있다. 그 때문에 이제는 '데이터 경제학', '데이터 과학자'라는 용어가 등장하고 있다.[10] 이제는 어떻게 빅데이터를 축적해 활용하는지가 제4차 산업혁명 시대에 펼쳐지는 경제의 승패를 좌우하는 요소가 되었다.

---

8) 초연결사회에 관해서는 우선 유영성 외, 『초연결 사회의 도래와 우리의 미래』(한울, 2014); 금용찬, "디지털문명기 초연결사회, 창조경제논의", 『컴퓨터월드』 제363호(2014. 1), 124-131쪽; 선원진·김두현, "초연결사회로의 변화와 개인정보 보호", 『정보와 통신』 제31권 제4호(2014. 4), 53-58쪽; 양천수, "현대 초연결사회와 새로운 인격권 보호체계", 『영남법학』 제43집(2016. 12), 209-239쪽 등 참고.

9) 빅데이터에 관해서는 빅토르 마이어 쇤베르거·케네스 쿠키어, 이지연 (옮김), 『빅데이터가 만드는 세상』(21세기북스, 2013); 양천수, 『빅데이터와 인권』(영남대학교출판부, 2016) 등 참고.

10) 이를 보여주는 서울대 법과경제연구센터, 『데이터 이코노미』(한스미디어, 2017) 참고.

### (2) 지능정보사회

초연결사회를 통해 사회 곳곳에서 빅데이터가 축적되면서 이러한 빅데이터를 통해 스스로 생각할 수 있는 탈인간적인 존재, 즉 인공지능이 가능해지고 있다. 다시 말해, 거대한 정보를 기반으로 한 인공지능이 출현하는 '지능정보사회'(intelligent information society)가 도래하고 있는 것이다.[11] 지능정보사회는 크게 세 가지 원인에 힘입고 있다. 첫째는 빅데이터의 출현, 둘째는 '무어의 법칙'으로 대변되는 컴퓨터 하드웨어의 급속한 발전,[12] 셋째는 머신러닝과 딥러닝의 개발이다. 첫째가 데이터에 관한 측면이라면, 둘째는 하드웨어에 관한 측면, 셋째는 소프트웨어에 관한 측면이다. 한편 이렇게 지능정보사회가 도래하면서 그 이전부터 성장하기 시작한 탈인간중심적 사고가 사회 전체적으로 확산되고 있다.[13] 알파고와 같은 인공지능에게 법적 인격성을 부여할 수 있는지, 법적 책임을 물을 수 있는지가 논의되고 있고, 인공지능의 윤리가 진지하게 논의되고 있다.[14] 더불어 인공지능이 우리 인간의 직업을 대체할 것이라는 두려움도 커지고 있다. 탈인간중심적 사회가 다가오고 있는 것이다.

### (3) 안전사회

안전사회 역시 제4차 산업혁명이 불러오고 있는 사회변화의 모습이라 할 수 있다. '안전사회'(Sicherheitsgesellschaft)란 안전을 최우선적인 사회적 목표로 설정하는 사회를 말한다.[15] 물론 안전사회는 제4차 산업혁명이 전적으로 유발한 것은 아니다. 현대사회가 위험사회로 접어들면서 안전사회에 관한 논의가 시작되었기 때문이다. 다만 제4차 산업혁명으로 초연결사회가 구현되고, 이로 인해 인터넷을

---

11) 지능정보사회에 관해서는 심우민, "지능정보사회 입법 동향과 과제", 『연세 공공거버넌스와 법』 제3권 제1호(2017. 2), 75-118쪽; 이원태 외, 『지능정보사회의 규범체계 정립을 위한 법·제도 연구』(정보통신정책연구원, 2016) 등 참고.

12) 다만 최근 반도체업계는 '무어의 법칙'을 폐기했다. 한동희, "[무어의 법칙 폐기]① 반도체 패러다임 대전환…IT융합 칩수요 다변화 시대", 『ChosunBiz』(2016. 4. 12) (http://biz.chosun.com/site/data/html_dir/2016/04/12/2016041201802.html#csidx28d1fc0c293c440b4ff3c01d6ef6552) 참고.

13) 탈인간중심적 사고에 관해서는 양천수, "탈인간중심적 법학의 가능성: 과학기술의 도전에 대한 행정법학의 대응", 『행정법연구』 제46호(2016. 8), 1-24쪽 참고.

14) 이에 관해서는 웬델 월러치·콜린 알렌, 노태복 (옮김), 『왜 로봇의 도덕인가』(메디치미디어, 2014) 참고.

15) 안전사회에 관해서는 토비아스 징엘슈타인·피어 슈톨레, 윤재왕 (역), 『안전사회: 21세기의 사회통제』(한국형사정책연구원, 2012); 양천수, "현대 안전사회와 법적 통제: 형사법을 예로 하여", 『안암법학』 제49호(2016. 1), 81-127쪽 참고.

통해 진행되는 소통의 안정성이 중요해지면서 정보보호에 관한 사회적 관심이 제고되고 있다. 특히 인터넷에 대한 침해수단이 급속도로 진화하고 이를 통해 개인정보를 포함한 각종 정보가 침해되는 사례가 빈번해지면서 정보보호의 중요성이 증대하고 있다. 이로 인해 안전사회, 더욱 정확하게 말해 안전한 정보사회를 구현하고자 하는 사회적 관심과 요청이 증대하고 있다. 정보보호 관련 법제도를 개선하고자 하는 최근의 움직임은 바로 이러한 사회적 흐름에 기인하는 것이다.

## III. 융합보안의 의의와 문제지점

### 1. 현실세계와 사이버세계의 융합

제4차 산업혁명이 진행되고 있는 오늘날 관찰할 수 있는 또 한 가지 현상으로서 현실세계와 사이버세계가 융합되고 있는 모습을 들 수 있다. 컴퓨터 하드웨어 기술이 급속하게 발전하고 인터넷이 등장하면서 사이버세계가 현실세계에 못지않은, 더 나아가 현실세계와 동등하거나 때로는 이를 넘어서는 의미와 중요성을 갖게 되었다. 이에 따라 사이버세계와 관련된 사이버경제가 비약적으로 성장하고 있다. 전 세계적으로 성장하고 있는 게임시장이 이를 예증한다. 더불어 최근에는 현실세계와 사이버세계가 융합하는 현상도 가속화되고 있다. 이에 따라 '증강현실'이 새로운 블루오션으로 자리 잡고 있다. 전 세계적인 열풍을 일으킨 '포켓몬 고'가 이를 잘 보여준다. 그런데 이렇게 현실세계와 사이버세계의 융합이 급속하게 진전되면서 '융합보안'이 새로운 이슈로 부각되고 있다. '융합보안'이 새로운 법적 문제로 등장하고 있는 것이다.

### 2. 융합보안의 의의

#### (1) 개념

융합보안이란 지난 2008년 지식경제부에서 발표한 "Securing Knowledge Korea 2013"에서 제시한 개념이다. 그 당시 지식경제부는 보안 개념을 크게

‘물리보안’, ‘정보보안’으로 구분하면서 이러한 두 보안이 새롭게 융합되는 보안을 융합보안으로 지칭하였다. 요컨대 융합보안은 물리보안과 정보보안의 성격을 모두 갖고 있는 보안이라 할 수 있다. 오늘날 사물인터넷과 인공지능 기술이 급격하게 발전하면서 융합보안이 새로운 정보보안 문제로 각광을 받고 있다. 융합보안의 대표적인 예는 급속도로 전자화가 진행되고 있는 자동차에서 쉽게 발견할 수 있다. 요즘에는 고급차의 경우 스마트키를 이용해 문을 열고 닫는다. 그런데 스마트키를 해킹하면 자동차 소유자가 아니라도 손쉽게 자동차 문을 열고 안에 들어가 자동차를 절도할 수 있다. 요컨대, 스마트키의 정보보안을 침해함으로써 자동차에 대한 물리보안까지 침해하는 것이다. 이를 막기 위해서 정보보안과 물리보안을 모두 보장할 수 있는 융합보안이 요청되는 것이다.

### (2) 융합보안의 문제지점으로서 사물인터넷과 인공지능

융합보안은 특히 사물인터넷과 인공지능이 등장하면서 문제가 되기 시작하였다.[16] 오늘날 사물인터넷과 인공지능을 탑재한 다양한 제품이 상품으로 판매되면서 융합보안의 문제가 불거지고 있다. 무엇보다도 사물인터넷을 통해 초연결사회가 구현되면서, 융합보안을 침해함으로써 발생한 결과가 손쉽게 초연결망 전체로 확산되는 위험이 점증하고 있다.

사실 사물인터넷은 다음과 같은 점에서 융합적인 성격을 강하게 띤다. 첫째, 사물인터넷 그 자체는 다양한 기술의 융합체이다. 사물인터넷을 구현하기 위해서는 디바이스 기술, 네트워크 기술, 시스템 기술, 서비스 기술, 데이터 처리 기술 등 다양한 기술이 융합되어 적용되어야 한다. 둘째, 사물인터넷은 각기 상이한 산업을 융합시킨다. 예를 들어, 사물인터넷을 통해 전통적인 자동차산업과 ICT 산업이 자동차 안에서 구현된다. 셋째, 사물인터넷은 초연결사회를 가능하게 함으로써 세상의 모든 데이터가 융합될 수 있도록 한다. 이러한 근거에서 사물인터넷의 보안문제를 처리하기 위해서는 전통적인 방식의 보안이 아닌 새로운 보안, 즉 융합보안에 따른 접근방식이 필요한 것이다.

16) 이에 관해서는 최종석・박종규・김호원, “인공지능과 사물인터넷 융합 보안 기술 연구방안”, 『한국통신학회지』 제34권 제3호(2017. 2), 65-73쪽 참고.

## 3. 융합보안이 문제되는 지점

그러면 이러한 융합보안이 문제되는 지점은 무엇인가? 사물인터넷을 예로 보면, 다음과 같은 지점에서 융합보안이 문제된다.[17]

### (1) 사물인터넷 디바이스 보안

첫째, 사물인터넷 디바이스, 다시 말해 사물인터넷 기기 그 자체의 보안이 문제된다. 사물인터넷 기기가 해킹되면 본래 기능에 맞지 않게 오작동할 수 있기 때문이다.

### (2) 사물인터넷 네트워크 보안

둘째, 사물인터넷 네트워크 보안이 문제된다. 사물인터넷은 주로 무선인터넷망을 통해 다른 사물인터넷과 연결된다. 이 과정에서 네트워크 연결망을 통해 사물인터넷을 해킹할 수 있다. 따라서 사물인터넷 네트워크 보안을 구현할 필요가 있다.

### (3) 사물인터넷 시스템 및 서비스 보안

셋째, 사물인터넷 시스템 및 서비스 보안이 문제된다. 이는 사물인터넷을 구동하는 데 사용되는 프로그램과 관련된 보안문제에 해당한다. 사물인터넷 디바이스 보안 문제가 하드웨어에 관한 문제라면, 이는 소프트웨어에 관한 문제라 할 수 있는 것이다. 예를 들어, 해커는 사물인터넷의 구동프로그램을 공격하거나 사물인터넷에 연결된 응용프로그램을 공격함으로써 전체 초연결망을 혼란에 빠트릴 수 있다. 이 점에서 사물인터넷 시스템 및 서비스 보안이 문제된다.

### (4) 사물인터넷 데이터 보안

넷째, 사물인터넷 기기에 저장되어 있는 데이터 보안이 문제된다. 현대 초연결사회에서 사물인터넷 기기는 자연스럽게 방대한 데이터를 축적한다.

17) 이에 관해서는 배상태・김진경, "사물인터넷(IoT) 발전과 보안의 패러다임 변화", KISTEP R&D InI (2006) 49-51쪽 참고.

여기에는 당연히 민감한 개인정보도 포함된다. 따라서 만약 해킹에 의해 이러한 데이터가 유출되면, 이는 커다란 사회적 문제를 야기할 것이다. 융합보안 문제에서는 사물인터넷 데이터 보안 역시 중요하게 염두에 두어야 한다.

## IV. 융합보안과 인권

### 1. 공익으로서 융합보안

현대사회가 초연결사회로 변모하고 이로 인해 인터넷에 사회의 모든 정보가 빅데이터로 축적되면서 인터넷 보안, 즉 '사이버 보안'이 그 어느 때보다 중요해지고 있다. 해킹 등으로 보안이 침해되면 엄청난 양의 데이터가 유출될 뿐만 아니라 인터넷 서비스가 마비됨으로써 경제적으로도 크나큰 손실이 발생할 수 있기 때문이다. 이 때문에 물리보안이나 사이버 보안 및 융합보안을 포괄하는 보안 개념은 현대사회의 기능을 유지하는 데 필수적인 사회의 '공익'(public interest)으로 자리매김하고 있다. '정보통신망법' 등과 같은 법률은 바로 이렇게 공익에 해당하는 사이버 보안을 보장하기 위해 존재한다.

### 2. 인권으로서 융합보안

그런데 오늘날 보안은 단순히 공익으로만 머물러 있지 않다. 이를 넘어서 보안은 새로운 인권 혹은 기본권으로서 자리매김하고 있다.

#### (1) 공익과 인권의 분리

물론 전통적인 법적 사고에 따르면, 공익에 속하는 이익이 동시에 권리 또는 인권으로 규정되는 경우는 없다. 공익과 인권은 서로 구분되고 때로는 서로 대립하는 개념이자 이익이기 때문이다.[18] 이를테면 공익은 각 개인에게 귀속될 수 없는 집단적 이익으로 정의된다. 이에 반해 인권은 각 개인에게 분할되어

18) 이에 관해서는 양천수, "공익과 사익의 혼융현상을 통해 본 공익 개념: 공익 개념에 대한 법사회학적 분석", 『공익과 인권』 제5권 제1호(2008. 2), 3-29쪽 참고.

귀속될 수 있는 개별적 이익이다. 이러한 근거에서 인권과 공익은 개념적으로 뿐만 아니라 질적으로도 구분된다. 뿐만 아니라, 많은 경우 서로 대립하는 이익으로 취급된다. 헌법학에서 논의되는 기본권 제한 도그마틱이 이를 잘 보여준다.[19] 기본권 제한 도그마틱에서는 국가안전보장이나 질서유지 또는 공공복리를 위해 어떤 방법으로 그리고 어느 정도로 기본권을 제한할 수 있는지가 문제되는데, 여기서 알 수 있듯이 국가안전보장이나 질서유지 또는 공공복리와 같은 공익은 기본권과 대립하는 이익으로 설정된다.

### (2) 정보보안과 개인정보보호

이러한 맥락에서 정보보호법 영역에서는 '정보보안'(information security)과 '개인정보보호'(personal information protection)가 개념적으로 구분된다. '정보보안'은 전체 정보의 안전성을 보장하는 것으로서 일종의 공익에 해당한다. 이에 대해 '개인정보보호'는 개인정보 또는 개인정보 자기결정권이라는 개인적 권리를 보호하는 것으로서 권리 혹은 인권과 관련을 맺는다. 이러한 근거에서 우리 법체계는 양자를 규율하는 법률도 별도로 마련하고 있다. 가령 '정보보안'은 '정보통신망법'이 규율한다면, '개인정보보호'는 '개인정보보호법'이 실현하는 것을 목표로 한다. 거버넌스 역시 구분된다. 정보보안은 주로 과학기술정보통신부가 관할한다면, 개인정보보호는 방송통신위원회와 개인정보보호위원회가 관할한다. 이렇게 정보보안, 사이버 보안, 융합보안을 포괄하는 보안 개념은 인권이 아닌 공익과 관련을 맺는 것으로 이해되어 왔다.

### (3) 기본권으로서 안전

그러나 이러한 이해방식은 최근 변화를 맞고 있다. 최근 헌법학에서는 전통적으로 공익으로 평가되었던 이익을 기본권으로 새롭게 파악하는 이론적 시도가 전개되고 있기 때문이다. 이러한 예로서 '안전'(Sicherheit)을 들 수 있다. 안전은 우리 헌법에서 규정하는 국가안전보장이나 질서유지를 포괄하는 상위 개념으로서 가장 대표적인 공익에 해당한다. 안전은 흔히 개인적 권리를 대변하는 '자유'(Freiheit)의 대립 개념으로 논의된다. 이를테면 독일 법철학 전통에서는

19) 이에 관해서는 우선 김대환, 『기본권제한의 한계』(법영사, 2001) 참고.

안전을 중시하는 '홉스적 전통'과 자유를 중시하는 '로크적 전통'이 대립하는데, 이러한 이론적 대립을 영미철학에서 발전한 '자유주의-공동체주의 논쟁'과 대응시키기도 한다. 그런데 이렇게 공동체의 이익인 공익을 대변하는 개념으로 이해된 '안전'이 최근 독일의 몇몇 공법학자들에 의해 기본권으로 파악되고 있는 것이다. 요컨대, '기본권으로서 안전'(Sicherheit als Grundrechte)에 관한 논의가 이론적으로 힘을 얻고 있다.[20] 이러한 논의는 우리 공법학에서도 수용되어 안전을 기본권으로 파악하는 주장이 유력하게 주장되고 있다.[21]

### (4) 집단적 권리로서 융합보안

전통적으로 공익으로 파악되었던 안전을 개별적으로 귀속이 가능한 기본권으로 재설정할 수 있는가 하는 문제는 많은 논증을 필요로 하는 쉽지 않은 문제이다. 따라서 이 문제를 이 글에서 정면으로 다룰 수는 없다. 다만 결론만을 언급하면, 필자는 집단적 이익에 속하는 공익을 권리로 규정하는 것이 이론적으로 전혀 불가능하지는 않다고 생각한다. 공익을 집단적 권리로 파악하는 것이 바로 그것이다. 전통적으로 권리는 개인적 권리만을 염두에 두었지만, 최근 인권학 영역에서는 개인적 권리에 대비되는 집단적 권리가 새롭게 자리매김하였다. 이러한 집단적 권리는 특히 다양한 소수민족이 공존하는 다문화국가에서 중요한 인권으로 논의되고 있다. 소수민족의 자결권이 이러한 집단적 권리의 예로 언급된다. 사실이 그렇다면, 안전을 기본권으로 규정하고자 하는 시도가 전혀 불가능한 것은 아니라는 점을 알 수 있다. 안전을 개인적 기본권이 아닌 집단적 기본권으로 규정하는 것이다. 만약 그렇다면, 안전과 그 내용이 유사한 정보보안 역시 집단적 권리로 파악될 수 있을 것이다. 마찬가지 근거에서 정보보안의 하위 개념인 융합보안을 집단적 권리 또는 집단적 인권으로 새기는 것도 불가능한 일은 아니다. 요컨대, 안전을 집단적 권리로 파악할 수 있는 것처럼, 융합보안을 집단적 인권으로 규정할 수 있는 것이다. 이 점에서 융합보안은 인권과 무관하지 않은 개념이자 이익이라고 말할 수 있다. 융합보안을 침해하는 행위는 집단적 인권을 침해하는 행위로 새길 수 있는 것이다.

---

20) 예를 들어 Josef Isensee, *Das Grundrecht auf Sicherheit: Zu den Schutzpflichten des freiheitlichen Verfassungsstaates* (Vortrag gehalten vor der Berliner Juristischen Gesellschaft am 24. November 1982) (Walter de Gruyter, 2012) 참고.

21) 이를 보여주는 정문식, "안전에 관한 기본권의 헌법상 근거와 위헌심사 기준", 『법과 정책연구』 제7집 제1호(2007. 6), 217-239쪽 참고.

# V. 융합보안 관련 법제도의 쟁점 및 기본구상

그러면 이러한 융합보안을 보장하기 위해 법제도는 어떻게 대응하는 것이 바람직한가? 여기에는 어떤 법적 문제가 있는가? 이를 아래에서 간략하게 살펴보도록 한다.

## 1. 독자적인 법규범의 필요성

먼저 융합보안을 실현하기 위해서는 이에 관한 독자적인 법규범을 마련하는 것이 필요해 보인다. 현재 융합보안을 규율하는 법적 규제, 특히 사물인터넷이나 인공지능의 보안문제를 규율하는 법적 장치는 보이지 않는다. 물론 사물인터넷이나 인공지능에 사용되는 보안 프로그램을 정보보호제품으로 보고 국가정보화 기본법이 규율하는 CC인증을 여기에 적용할 수 있을지 모른다. 그러나 이는 융합보안이 갖고 있는 독특한 성격을 충분히 고려하지 못한 것이다. 위에서도 살펴본 것처럼, 사물인터넷 보안에 관해서는 크게 네 가지의 보안, 즉 디바이스 보안, 네트워크 보안, 시스템 보안, 데이터 보안이 문제된다. 따라서 이러한 보안을 모두 충분하게 실현하려면, 복합적인 규제장치가 투입될 필요가 있다. 이 점에서 기존의 정보보호 관련 법제도는 융합보안 문제를 적절하게 규율하기 어렵다. 그 때문에 융합보안에 관한 독자적인 법규범을 제정할 필요가 있다.

## 2. 사전예방을 통한 보안

융합보안 문제는 철저한 사전예방을 통해 구현하는 것이 필요하다. 왜냐하면 이미 정보침해가 발생한 시점이나 그 직후에 개입하는 것은 융합보안을 구현하는 데 실패할 가능성이 높기 때문이다. 현대 초연결사회에서는 사물인터넷 기기 한 개의 보안만 침해되어도 그 결과가 초연결망을 통해 사회 전체적으로 파급될 수 있다. 또한 융합보안이 문제되는 경우에는 융합보안이 침해된 경우 그 결과가 사이버세계에만 머무는 것이 아니라, 실제세계에도 악영향을 미치는 경우가 많다. 따라서 융합보안은 철저한 사전예방 중심의 규제로 구현하는 것이 바람직하다.

## 3. 설계를 통한 보안(security by design)

이러한 사전예방 지향의 규제로서 가장 대표적인 것으로 '설계를 통한 보안'(security by design)을 들 수 있다.[22] 설계를 통한 보안은 제품을 설계하는 단계부터 보안을 고려해야 한다는 것을 말한다. 따라서 융합보안을 적절하게 구현하려면, 융합보안 관련 제품, 즉 사물인터넷 기기나 인공기능 기기를 설계하는 단계부터 보안문제를 고려해야 한다. 물론 이 과정에서 경제적 비용이 증가할 테지만, 이를 상쇄할 수 있는 법적 규제를 마련할 필요가 있다.

## 4. 독자적인 인증제도 마련

'설계를 통한 보안'의 연장선상에 있는 제도가 바로 보안인증제도이다. 현행 정보보안 관련 법체계는 ISMS, PIMS, CC 등과 같은 다양한 인증제도를 갖추고 있다. 이외에도 준비도 평가나 성능평가와 같이 인증제도와 유사한 기능을 수행하는 제도를 갖추고 있다. 그렇지만 이들 제도들은 사물인터넷 기기나 인공지능처럼 융합보안과 관련된 제품의 보안상태를 인증하는 데 적합하지 않다. 이들 기기가 갖고 있는 융합적·복합적 성격을 고려하면, 이들에게 적합한 독자적인 인증제도를 마련하는 것이 바람직하다.

## 5. 융합보안에 관한 거버넌스

마지막으로 융합보안을 관할하는 거버넌스를 어떻게 구축하는 것이 바람직한지 검토해야 한다. 이를 위해서는 우선 융합보안을 관할하는 주무부처를 어떻게 결정해야 하는 것이 바람직한지 판단해야 한다. 현행 정보보안 관련 법체계는 정보보안에 관한 거버넌스를 다음과 같이 체계화하고 있다. 공공영역은 국가정보원이, 민간영역은 과학기술정보통신부가 그리고 개인정보보호에 관해서는 행정안전부와 대통령 직속의 개인정보보호위원회가 관할하는 것이다. 하지만 앞에서 살펴본 것처럼, 국가정보원이 국내 공공기관의 정보보안 문제를 다루는 것에 관해서는 비판이 제기되고 있다. 이의 연장선상에서 국가정보원법 개정안도

22) 이에 관해서는 Hyunmin Kim, *Side-channel security by design: hardware level countermeasures* (고려대 정보보호대학원 박사학위논문, 2018) 참고.

발의되고 있다. 국가정보원의 관할영역을 기본적으로 해외에 대한 정보보안으로 한정하는 것이 그것이다. 이러한 맥락에서 보면, 공공영역의 정보보안 문제를 국가정보원이 관할하는 현행 거버넌스 체계는 근원적으로 되돌아볼 필요가 있을 것이다.

한편 이와는 상관없이 융합보안 문제는 기본적으로 과학기술정보통신부가 관할하는 것이 타당하다. 왜냐하면 융합보안 문제는 주로 사물인터넷 기기나 인공지능과 같은 제품과 관련을 맺는데, 이는 시장에서 판매되는 것으로서 민간영역에 속한다고 볼 수 있기 때문이다. 그러므로 융합보안에 관한 거버넌스는 과학기술정보통신부가 관할하는 것을 기본 축으로 하여 설계하고 운용하는 것이 바람직하다.