Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1269

정보통신보안법제의 문제점과 개선방안*

권 헌 영†‡
고려대학교 정보보호대학원

Information and Communication Security legal system's problems and improvement plan*

Hun-Yeong Kwon†‡
Graduate School for Information Security, Korea University

요 약

우리나라는 전 세계에서 정보화 능력이나 환경이 가장 앞선 나라로 평가 받는다. 그럼에도 불구하고 보안사고와 공격이 가장 빈번한 국가 중에 하나라는 것도 부인하기 어렵다. 이제는 정보화의 순기능을 위해 각종 물적 기반구축과 진흥에 방점을 두던 시기와는 다르게 정보화 성과를 공고히 하고, 그 성과를 보호하는 것이 중요한 시기가 되었다. 그러나 정보보안 법제의 체계화나 법령의 정비 문제는 늘 우선순위에서 밀려나 있다는 인상을 지우기 어렵다. 이제는 이런 틀에서 벗어나 변화의 중심에서 문제를 직시할 필요가 있다. 정보보안 법제의 체계를 바로 세우기 위하여 가장 시급한 일은 개념의 재검토와 체계의 재구성이고, 이후 공론화와 합의 과정을 거쳐 이를 법제화하는 문제이다. 이 글은 이러한 시론적 배경에 따라 우선 법제와 정책의 체계를 개선하기 위하여 필요한 조치가 무엇인가, 그리고 왜 그런 조치가 필요한가를 환기하기 위한 것이다. 아울러 그러한 구체적인 조치방안의 하나로 '정보보호정책기본법'이라는 신규입법을 이 글을 통해 제안하고자 한다.

ABSTRACT

Korea is recognized as the most advanced nation in regards to capabilities or environments of informatization throughout the world. Nevertheless, Korea brings on itself such stigmas as a nation vulnerable to information security. Now the globe ushered in an era requiring political balances. Yet, issues of legislative supports or system adjustments for information security policies are always pushed back on the priority list. There is a need to face problems at the center of changes departing from such frames. In order to establish a proper system for information security policies, the most urgent issues are reviews of concepts and reorganizations of systems, and then to legislate information security polities by being harmonious with public opinions. This paper is to remind what measures are needed to improve the system of priority policies depending on public backgrounds and why such measures are needed. Furthermore, the paper suggests a new legislation, 'Information Security Policy Act' as one of the specific measures.

Keywords: Adverse Effects of the Informatization, Information Protection, Information Security, Legal System for Information Security, Framework Act on Information Protection Policy

접수일(2015년 7월 16일), 수정일(2015년 8월 19일), 게재확정일(2015년 8월 20일)

* 이 논문은 서울대학교 공익산업법센터 제31회 세미나에서 발표한 발제문을 수정·보완한 것이며, 2014년도 정부(교육과학기술부)재원으로 마련된 한국연구재단의 지원(NRF-2014S1A3A2044645)으로 연구되었음.

† 주저자, khy0@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

I. 서 론

정보사회가 고도화되면서 일상에서 보안사고를 경험한다. 정부의 웹사이트가 공격을 받아 개인정보가 유출되기도 하고, 내 컴퓨터가 좀비 PC가 되기도 한다. 이런 보안사고는 정부 뿐 아니라 금융기관이나 온라인서비스기업을 가리지 않고 나타난다. 정보화를 통해 얻는 새로운 세상이 자칫 공포의 대상이 될 수도 있는 것이다. 세계 각 국은 자국의 정보보안 능력을 신장하기 위하여 다양한 노력을 경주하고 있다. 국가 행정체계를 정비하는가 하면 전문가를 전사로 양성하기도 한다. 정보보안은 이제 국가적 역량을 결집하여야 할 정책분야로 떠오르고 있는 것이다.

우리나라의 경우 전 세계에서 정보화 능력이나 환경이 가장 앞선 나라로 평가받는다. 그럼에도 불구하고 정보유출이나 보안사고가 비교적 빈번하게 일어나는 국가 중에 하나라는 것도 부인하기 어렵다. 이제는 정보화의 순기능을 위해 각종 물적 기반구축과 진흥에 방점을 두던 시기와는 다르게, 지금의 정보화 성과를 공고히 하고, 그 성과를 보호하는 것이 중요한 시기가 되었다.[1] 그러나 정보보안 법제의 체계화와 정비 등 제도 패러다임의 전환 문제는 그 시급성에 비해 다소 우선순위에서 밀려나 있다는 인상을 지우기 어렵다. 거시적 차원의 법체계 정립과 개선보다는 이슈에 단기적으로 대응하기 위한 분야별 강력한 대응입법이 이루어진 결과, 보호하려는 대상과 방법에 따라서 각종 법령이 산재해있고,[2] 일관된 원칙과 방향을 제시하고 있는 상위법의 부재도 아쉬운 실정이다.

이제는 이런 틀에서 벗어나서 변화의 중심에서 문제를 직시할 필요가 있다. 정보보안 법제의 체계를 바로 세우기 위하여 가장 먼저 필요한 일은 개념의 재검토와 체계의 재구성이다. 이를 위하여 차제에 관련법제의 의의와 연혁에 대하여 살펴보고 새로운 입법적 대응방안에 대한 생각을 정리해 보고자 한다.

1) 정보보호와 관련된 정책이 더 이상 정보화정책의 곁가지가 아니라 정보화정책의 새로운 패러다임 중에 하나로 인식되어야 한다는 것이 연구자의 생각이다.

2) 국가안보와 기밀·비밀에 관한 보호, 개인정보 보호, 통신망·시설이나 설비에 관한 보호, 전자정부 등 행정정보의 보호 등 분야별로 다양한 법령이 산재해 있고, 당국자나 업계가 준수해야할 규제도 분야별로 각기 다른 실정이다.

II. 정보통신보안법제의 의의와 체계

2.1 보안법제의 개념적 토대와 범주

보안법제는 '보안'을 어떤 의미로 이해하는가에 따라[3] 그 개념적 범주가 다양하게 설정될 수 있다. '보안'이라는 용어자체를 '무엇인가를 어떤 위험으로부터 안전하게 보호한다'는 의미로 이해하게 되면 그 '무엇인가'에 따라서, 또 '어떤 위험으로부터'에의 의미에 따라서 세부 범주가 결정될 것이다. 여기에 '어떻게'가 추가된다면 보안법제는 첫 번째로 그 대상으로서의 보호이익을 중심으로 구별 가능한 범주가 형성되고,[4] 두 번째는 위험요소의 속성에 따라서 구별 가능한 범주가 형성되는 데 이어 보호행위의 태양에 따른 범주도 형성될 수 있는 것이다.[5]

따라서 가장 넓은 개념적 범주에서의 보안법제는 그 대상과 방법을 가리지 않고 '무엇인가를 어떤 위험으로부터 안전하게 보호하는 인간활동에 관한 법규'로 설정할 수 있다. 'OO보안법제'에서 'OO'를 확정하지 않게 되면 가장 포괄적인 보안법제의 범주가 설정된다. 실정법상의 사례를 볼 때 '국가보안법'과 '국가안전보장을 위한 일련의 보안법령', '군사기밀의 보호 등과 같은 군사보안 관련 법령', '산업기밀보안 관련 법령', '정보통신보안 관련 법령', '영업비밀', '의료·법무·세무 등 서비스 정보', '수사 등 업무상 비

3) 정보보안, 정보보호, 사이버안보 등 우리가 관행적으로 사용하는 용어에 대한 명확한 개념정의가 연구의 출발점에 있어서 불필요한 오해나 혼란을 예방하는데 무척 중요한 것은 사실이지만, 이러한 사항을 모두 다루는 것이 지면의 한계와 더불어 본 연구의 논지와는 다소 관련이 없으므로 본 연구에서 그러한 논의를 출발점으로 삼지는 않는다. 이후 내용에 별도의 명확한 개념정의나 구분이 필요한 경우 따로 정리하기로 하되, 도리어 독자들께서는 최근 우리가 사용하는 '정보보안', '보안법제'의 관용적 정의나 용례는 잠시 잊고 연구자의 주장과 논지를 접해주시기를 부탁드린다.

4) 1960년대부터 70년대를 문서보호의 시기, 1980년대를 컴퓨터 보호의 시기, 1990년대를 인터넷 등 통신네트워크의 보안의 시기로 구분하고 있는 것이 대표적인 예이다.

5) 정보보호의 개념을 협의(정보보안 등 기술적 요소)와 광의(프라이버시, 지적재산권 등 보호대상)로 구분하여 설명한 연구나[1], 보호대상에 대한 보호행위의 종류로서 물리적 정보보호, 조직·관리적·거버넌스적 정보보호를 구분하여 설명한 연구[2,3] 등 정보보호의 개념 범주에 관해 논했던 기존의 연구들도 결국 돌이켜보면 보호대상과 보호행위의 태양을 개념의 핵심요소로 삼고 있다는 것이다.

밀', '통신·금융 및 신용·위치·사생활비밀 등 개인정보' 등 대상에 따른 보안법제는 대상의 내용에 따라 범주가 포괄 또는 구분될 수 있다.

대상 내용별 범주에 이어서 중요한 개념적 요소는 대상 내용의 존재형식이다. 보호대상이 어떤 존재형식을 띠고 있느냐에 따라 그 보안활동이 결정되기 때문이다. 이는 전통적 방식과 현대적 방식의 차이를 결정짓게 되는 계기이기도 하다. 예를 들어 보호대상을 '국가안보'라고 설정하게 되면 국가안보에 위협이 되는 모든 위험으로부터 국가를 안전하게 보호하기 위한 일련의 활동이 정립될 수 있는데, 이러한 활동은 국가형성의 기초가 되는 요소 전체와 국가운영의 정치 및 사회, 경제질서를 포괄하는 개념과 함께 확장된다. 이런 개념의 확장을 수용하지 못할 바는 아니지만, 보다 구체적인 보안법제의 범위 식별을 위하여 대상의 존재형식에 따라 이를 '정보'로 한정하는 방법의 채용이 유용하다.

보안법제가 '정보보안법제'의 개념적 범주로 특정되고 나면 이제 '정보'의 매체적 특성에 따라 하위범주가 형성된다. 위에서 본 다양한 분야의 보안법제는 사실상 정보의 수직적 구분과 귀속분야에 따라 형성된 것이다. 그렇지만 이는 아직 정보의 매체적 특성은 반영되고 있지 못하다. 해당 정보가 어떤 매체에 체화되어 있는가에 따라 위험과 보호의 수준 및 방법이 달라지기 때문에 정보의 매체적 특성은 중요한 인식 요소가 된다. 고전적 매체로서의 구전(口傳), 문자와 종이인 문서를 비롯하여 특정한 시설, 방송·통신체계 등과 같이 정보의 존재형식과 소통형식에 주목하는 일련의 보안규범 또한 이 매체적 특성에 따라 이루어진 것이라 볼 수 있다.

현대의 매체적 특성은 역시 정보의 '디지털화'와 '온라인화'라고 할 수 있다. '정보화'라고 하는 사회변혁은 자연스럽게 보안법제의 관심을 '디지털화', '온라인화'로 이끌었고, 이에 따라 정보보안의 개념적 범주는 '디지털 정보'라고 하는 컴퓨팅 기술환경에서의 정보보안으로 특화되는 경향을 가져왔다. 컴퓨팅 기술환경에서의 정보보안은 급속한 온라인화와 더불어 더욱 기술적 영향을 많이 받게 되는데, 정보보안법의 관심도 이 정보통신기술환경에 따라 특화되고 진화하게 된다.

정리하자면, 보안법제는 그 보호대상 및 내용에 따라 수직적으로 구분되고, 또다시 그 존재형식에 따라 수평적으로 구분되는 개념적 범주를 설정할 수 있다. 매체적 특성에 주목하는 수평적 정보보안법제는 정보통신기술발달에 크게 영향을 받게 되지만, 다시 수직적 분화경향을 보이고 있다. 이러한 복잡한 개념적 틀과 환경이 정책경쟁과 보안법제의 체계적 정합성에 혼선을 가져오는 원인 중 하나가 될 수 있다.

2.2 보안법제의 연혁과 특성

2.2.1 전통적인 보안법제

우리나라가 독자적으로 현대적인 법체계를 수립하기 시작한 해방 이후, 우리나라의 보안법제는 국가안보적 측면에서 발달할 수밖에 없었고,[6] 정부와 입법부의 주된 관심은 '국가적 정보의 보호'에 집중되어 있었던 것이 사실이다.[7]

국가정보는 일종의 국가를 위한 지식이며 그러한 지식을 입수하는 행위(또는 상대방의 입수행위를 저지하는 것), 그리고 입수 또는 저지기능을 수행하는 조직 등을 포괄하는 개념으로[4], 정보와 매체의 통제가 특히 권력적 속성과 연결된다는 점을 고려할 때 국가적 관심은 해당 정치체제의 안정적인 보호와 권력의 유지·관리적 관점에서의 정보보안이 주된 관심사였다. 이어서 국가의 존립기반인 국토와 관련 시설의 보호, 사회·경제질서의 보호 등과 같은 공동체의 유지관리 역시 전통적 정보보안의 핵심 관심사가 아닐 수 없었다.

이런 전통적 의미에서의 보안법제는 국가안전보장, 국방, 공공질서의 보호 등과 같은 수직적 보호대상을 위해 정보보안활동과 법제가 수단적으로 중요시되어야 한다는 관념이 강하게 작용한다. 따라서 여기서의 정보활동은 정보의 수집과 분석 및 처리라고 하는 일련의 보호활동을 위하여 일반·추상적인 법규범

6) 해방 이후 남북이 분단된 상황에서 오랜 기간 동안 군사정권에 의한 통치가 진행되어 온 우리나라의 상황에서는 첩보나 방첩 등 국가안보가 가장 우선시 되는 가치 중에 하나일 수밖에 없었으며, 따라서 자연스럽게 사법적 성격보다는 강력한 공법적 경향이 두드러지게 나타나는 특성을 지닌다.

7) 그러나 다른 국가 대부분에 공통되는 보안법제의 초기 형태는 '타인의 비밀을 침해하여서는 아니된다'는 일반적이고 철학적인 법적 관념으로부터 출발한다. 지극히 사법적인 필요로부터 공법적 보호를 요구하는 과정으로 발전을 거듭하게 된 것이다. 보호이익을 가진 자의 입장에서 보면 '보호받아야 마땅할 나의 정보'를 위험으로부터 안전하게 보호하는 것이 중요한 관심의 대상이 된다. 이런 법적 관념의 발달은 다수 정보보안법제에서 국가의 적극적 개입의무를 규정하는 입법적 경향과 무관하지 않다.

을 마련하고, 이로부터 획득된 각종 정보를 체계적으로 보호하는 보안규범을 정립한다. 이에 따라 정보수집활동과 이에 수반하는 보안활동은 체계를 갖추게 되고, 정보의 수집활동에 관한 법제는 추상적 근거에 따라, 보안활동에 관한 법제는 그 하위개념이지만 내부를 강하게 통제하는 구체적 규범으로 설정된다.[8)]

정보수집활동을 법리적 관점에서만 보면 대외적으로는 국제법적 문제를 갖게 되고 대내적으로는 개인의 자유권적 기본권의 제한이라고 하는 문제를 갖게 된다. 따라서 추상적 근거에 따른 정보활동은 그것이 수집활동이든 보호활동이든 법적 논쟁의 대상이 된다. 대표적 사례가 바로 국가보안법 폐지론과 존치론의 대립[9)]이다[5-7].

이와 같이 전통적 보안법제에서는 정보의 수집 및 처리가 중요한 가치로 인식되면서 보안활동은 비교적 하위의 수준으로 자리 잡게 되었고, 자연스럽게 이 시기 보안관련 법제는 공무원, 군인 등과 특정한 신분적 속성을 가지고 해당 정보를 처리하는 자가 법제의 주된 규율의 대상이 되는 특성을 보인다. 일반 법률적 근거보다는 특별권력적 행정권발동의 근거만 확보하면 그들에 대한 일반징계권 등을 통해 원하는 목적을 달성할 수 있었던 것이다. 일반인을 다루는 형태의 규범은 간첩행위와 같은 범죄행위를 처벌하는 수준이면 족했다고 할 수 있다.

그러나 정보의 존재형태가 디지털화 및 온라인화하면서 전통적 정보보안의 범주가 변모하기 시작하였다. 구전, 문서, 시설 등과 같이 전통적 매체만 관리하면 되었던 보호대상이 정보통신매체로 전환되면서 보안 취약성도 그만큼 증가하였기 때문이다. 다양한 형태의 보안사고는 정보의 수집 및 처리에 못지않은 정책적 관심을 증폭시키기에 충분하였고, 위험의 진원지가 국제적으로 확대되면서 정보보안문제는 또다시 국가안전보장의 중요한 요소가 되었다. 전통적 첩보대응과는 다른 총체적 정보보안이 필요하게 되면서 정책적 틀을 재편하여야 할 상황에 이르게 된 것이다.

또한 인터넷을 활용한 전자상거래 등 산업적 측면의 정보화효과가 부각되면서,[10)] 정보화 초기 정보보안은 부인방지 및 해당정보의 위변조 방지 등 주로 전자서명 정책의 일환으로 추진되었다. 이후 온라인 정보활동의 일상화는 개인정보 및 사생활보호 정책에 대한 수요를 폭증시켰으며 특히 2000년 이후 전자정부, 전자금융 등 정보화정책효과가 전면적으로 구체화되면서 정보보안도 해당 분야별 상황에 따라 구체적으로 발전하기에 이르렀다. 법제적으로는 정보화촉진기본법, 전자서명법, 정보통신망법, 전자정부법, 전자금융거래법, 개인정보보호법[11)] 등 다양한 근거법규에 대한 입법이 이루어졌다.

2.2.2 정보화와 정보통신보안법제

정보화 시기 정보통신보안법제는 매체적 특성에 따라 수직적이던 정보보안법제에 대한 관심을 수평적으로 확대하는 역할을 하였다. 물론 정보통신이라고 하는 분야적 속성이 수직적 특성이 없는 것은 아니지만 '정보화'라고 하는 환경의 제공은 수평적 관점의 확산에 실질적으로 기여한 것을 부인하기 어렵다.

정보화가 본격적으로 시작되면서 정보통신보안법제는 정보화와 위험의 증가 및 그 대응이라고 하는 일련의 과정을 경험적으로 겪어 오면서 발전하였다. 따라서 전통적 보안법제가 군인이나 공무원에 대한 특수관계를 통해 문제를 해결하려고 하였던 것에 비해 이제 사회 전반을 두루 포괄하지 않을 수 없었다. 특별한 위험을 새롭게 사회에 도입하는 경우에 이에 대한 책임을 강화하는 형태의 입법과 그 구체적 의무사항 등은 모두 일반 국민을 다루는 것으로 엄격한 헌법적 통제를 받을 수밖에 없었던 것이다. 결과적으로 법제의 내용이 비교적 구체적이며 상세하고 전문적이게 변모하였다. 해당 분야에 대한 경험적 결과를 입법에 수시로 반영하면서 정보통신보안법제는 다른 분야에도 영향을 끼치게 되었고, 실질적으로는 정보보안에 관한 사회전반의 일반법적 기능을 수행하는 성과를 얻었다. 특히 보안범죄에 대한 특별형법적 규정 등과 위험에 대한 탐지 및 분석능력을 행정권에 의하여 확보하는 등의 규정은 다른 법령의 제정 과정에서도 그 방향성을 제시하는 역할을 하였다.[12)]

8) 대표적인 예로, 1961년 중앙정보부법에서 시작된 국가정보원법에서 이와 같은 흔적을 찾을 수 있다. 정보수집활동에 관한 사항은 대체로 법률에 따라 추상적 근거만을 갖추고, 보안활동에 관한 사항은 정보 및 보안업무기획·조정규정, 방첩 및 보안업무 규정 등 하위법령에서 매우 구체적이고도 강력한 내부통제장치를 마련하고 있다.

9) 최근 사이버위기관리법 입법 추진과정에서의 논란도 그와 유사한 논리구조를 가지고 있다.

10) 정보통신 관련 산업육성을 통해 국가경쟁력을 제고할 것을 내용으로 하는 정책방향도 이시기에 청사진이 그려졌다.

11) 신용정보의 이용 및 보호에 관한 법률 등 다양한 개별법규를 포함한다.

정보통신보안법제는 초기 단계에서는 해킹·바이러스나 컴퓨터 이용사기 등에 대한 대응과 같은 형사규제의 내용으로 출발하였지만, 이후 다양한 보안사고를 경험하면서 규정이 대폭 확대되고 구체화되었다. 특히, 미국의 2001년 9.11테러나 우리나라에서 발생한 2003년 1.25 인터넷 대란 등과 같은 미증유의 사건은 정보화를 통해 얻은 결실이 얼마나 소중한 보호의 대상인지를 일깨워주었다. 이후 '정보사회에서의 안전'이라고 하는 확대된 포괄적 의미의 정보보안이 정보통신보안법제의 중요한 이슈가 되고, 정보의 존재형태를 구체적으로 식별하고 그 중요성을 구분하는 한편, 위험을 탐지하고 취약성을 분석하는 등의 보안활동이 입법에 급속도로 반영되기 시작하였다. 위험책임을 강화하는 형태의 입법과 해당 서비스 등에 대한 국가개입의 근거가 확충되기도 하였다. 특히 국가 및 공동체를 유지·발전시키는 데 중요한 정보자원을 식별하고 그에 대한 대응은 특별하게 하는 노력이 경주되었다. 정보통신망법을 통해 운용되던 정보통신보안법제는 정보통신기반보호법을 통해 그 범위가 확장되고 다시 정보통신망법에 의하여 보다 구체화되는 과정을 거치면서 정보통신보안법제의 체계를 갖추었다.[13]

이러한 정보통신보안법제의 발전은 필연적으로 수직적으로 분화되어 있던 전통적 보안법제의 범주에도 영향을 끼치게 되었다. 수평적으로 연계된 통신망에서의 정보보안이 다른 인접한 분야에 영향을 끼치지 않을 수 없게 된 것이다. 일반인에 대한 행정권 발동을 필요로 하는 분야에서의 공조체제는 물론 기술기반이나 추진체계상의 전문기관 활용 등도 정보통신보안법제의 영향을 받은 분야 중에 하나이다.[14]

12) 전산망보급확장과 이용촉진에 관한 법률에서 일부 해당 내용이 포함되어 있었지만, 1999년 전부 개정된 통해 정보통신망법에는 본격적으로 망에 대한 각종 안정성확보와 행정조치권한, 준수 의무와 형벌규정이 대폭 추가·구체화되었다.

13) 2000년 2월 국무총리 주재로 열린 '사이버 테러방지 관계장관회의'에서 정부차원에서 사이버테러에 대한 대책을 적극 추진하기로 한 것이 정보통신기반보호법 제정의 시초로 거론되고 있다. 그러나 정보통신망법 등 보다 본격적인 입법적 대응은 2003년의 이른바 '1.25 인터넷 대란' 전후로 볼 수 있다. 인터넷이 보편화된 이후 보안사고가 빈번해지면서 비난 여론 또한 확산되었고, 정부당국과 국회는 뒤늦게 정보통신망법에 관련 내용을 대폭 추가하고, 2004년 1월 국가사이버안전센터를 설립하여 사이버공격에 대한 범국가적 대비태세를 구축하는 등으로 재발 방지를 위한 대책을 마련하였다.

2.2.3 정보화 이후의 특별분야 보안법제

정보통신 분야의 약진으로 인해 정보화는 일반적 현상이 되었다. 모든 분야의 정보가 정보통신 기기와 매체에 의하여 처리되면서 수직적 정보보안 요소는 특화의 길로 나아가게 된 것이다. 이 과정에서 정보통신보안법제 및 전통적 보안법제와의 협력과 경쟁은 불가피한 일이 되었다.

우선적으로 이루어진 분야는 전자정부분야이다. 전자정부분야는 행정정보화를 중심으로 발전하여 온 것으로, 공공분야의 모든 정보의 수집 및 처리가 디지털·온라인으로 처리되도록 하는 정책이다. 행정정보는 일반행정법적 관점과 근거를 가지고 수집 및 처리되지만, 그와는 별도로 일반적 규정으로서 전자정부법을 따로 두고 있는 것이 특징이다.

전자정부는 공공기관의 정보처리에 관한 사항을 다루고 있으므로 전통적 보안법제의 특성과 유사하게 일반국민에게 보다는 공공부문에 종사하는 공무원 등에 대해 특수하고 강력한 정보보안조치와 활동을 요구하게 된다. 그러나 전자정부는 일반 국민이 이용하는 통신서비스를 통해 제공되고 일반 국민의 참여도 중요한 몫이 되기 때문에, 일반국민에 대한 정보보안을 필요로 하는 요소도 존재한다. 전자정부분야에서의 정보보안은 이처럼 다면적 속성을 갖고 있기 때문에 정책경쟁이 불가피하다. 전자정부법상의 정보보안 규정과 전통적 정보보안의 문제가 서로 일반규정과 특별규정의 관계에서 얽혀서 경쟁을 하게 된다.[15] 나아가 정보통신 보안의 기술과 능력이 그대로 전자정부분야에 적용되면서 정보통신 정보보안과 전자정부 정보보안은 현장에서의 정책경쟁이 일어나고 있다. 특히 전문기술의 지원기관이 양 정책경쟁기관을 동시에 지원하는 과정에서 이런 일은 더욱 가중되게

14) 과거 정보통신부 등 정보화 소관부처의 협력은 물론, 현재의 한국정보화진흥원, 한국인터넷진흥원, 한국전자통신연구원 등 각종 정보화 전문기관이 당시 정보통신보안과 관련된 정책·기술지원을 시행하면서 전통적인 보안분야에도 기여한 점을 떠올려보면 이해가 쉽다.

15) 대표적 사례를 예로 들면, 국가정보원법을 근거로 존재하는 보안업무규정상 국정원은 국가보안시설 등에 대해 보안조사권을 가지면서 이와 동시에 전자정부법 제56조에서 정보통신망 보안대책과 조치의 이행여부 확인권한도 갖고 있다. 그런데 이와 별개로 전자정부법에서는 전자정부를 소관하는 행정자치부장관에게 국정원장과의 협의를 통해 중앙행정기관과 지자체가 준수하여야 하는 대민서비스 보안대책의 수립권한을 부여하고 있다.

마련이다. 모든 분야에 동일한 요소는 정보보안의 대상 및 관리주체 등에서는 구분이 가능하지만 위험의 요소와 대응이라고 하는 정책수단에서는 동일하거나 유사한 데에서 경쟁과 협력을 필요로 한다. 그러나 행정권의 발동과 정책수단의 활용이라고 하는 측면에서는 보다 근본적이면서도 효율적·효과적인 방법을 찾지 않을 수 없다.

이와 같은 특별분야의 정보보안문제는 아이러니컬하게도 정보화를 추진하면서 체계적으로 자원을 동원하고 배분하는 과정에 연유하여 발생한다. 우리나라는 정보화를 추진하면서 국가기간 전산망을 5대 분야로 구분하여 특화된 방식으로 추진하였는데 이에 해당하는 망이 국방·행정·교육·금융·공안 등의 분야이다. 결과적으로 해당 분야가 모두 특별 정보보안분야라고 해도 무방하다.[16]

국방 정보보안법제에 있어서는 최근에 괄목한 변화가 발생하였다. 국방정보화법을 필두로 사이버사령부 등 정보보안 관련 법규의 정비가 구체적으로 시행되었기 때문이다. 이는 전통적 정보보안법제가 정보통신과 연계되면서 하위개념으로부터 독자개념으로 진화하는 모델을 보여준다. 보다 적극적인 정보보안 활동의 하나로서 사이버전쟁에 대비하려는 관계기관의 노력은 정보보안의 개념이 국가안전보장이라고 하는 근본적 개념과 부합하는 수준으로 확대된다는 점을 의미한다.

다양한 보안사고를 통해 일반 국민의 관심을 증폭시켰던 금융분야는 정보보안 분야가 앞으로 더욱 발전하여야 할 분야로 꼽힌다. 금융기관은 공공성도 존재하지만 본질적으로 사익을 추구하는 기업이기 때문에 발생하는 특성이 존재한다. 개별 금융기관의 정보화는 해당 금융기관의 이윤극대화에 초점이 맞추어져 있기 때문에 효율성을 가장 우위에 두고 정보화를 추진하게 된다. 금융망은 모든 금융기관을 연동하여 일반 금융소비자에게 제공되기 때문에 정보보안에 대한 대응은 연합하여 이루어질 필요가 있다. 그러나 시장의 대응을 일의적으로 강제하거나 유도하기는 어려우므로, 현재로서는 결과적으로 금융감독 기능의 강화를 통해 보안수준을 격상하는 방법에 의존할 수밖에 없을 것이다. 결국 금융소비자 보호와 국가 정보통신 기반으로서의 금융정보망의 안전한 보호라고 하는 관념에 입각한 정보보안 입법과, 정책체계의 협력과 효과적 집행을 위하여 근거를 구체화하는 노력이 요구되는 분야이다.

공안망은 전통적 정보보안 체계에 의하여 운용되는 데 문제점이 없을 것으로 전망된다. 교육망의 경우에는 전국단위의 교육행정정보시스템의 운영상 문제를 다루고 있기 때문에 관련 법규에서 일관되게 정책을 집행할 수 있는 체계만 갖추면 된다. 물론 일반 국민인 학생과 학부모의 이용관계에서 발생하는 보안의무규정 등은 구체적으로 입법에 반영하는 것이 필요할 것이다.

III. 현행 보안법제의 한계와 과제

3.1 개념적 혼동과 정책의 충돌

현행 보안법제는 위에서 본 바와 같이 다양한 개념이 중첩적으로 산재하여 경쟁하고 있는 상황이다. 발전과정에서 생긴 불가피한 측면도 없지 않지만, 공론이 부족한 상태에서 경험적 대응에 따라 입법이 이루어진 탓으로 볼 수도 있다. 하지만 근본적으로는 전통적 보안법제와 정보통신 및 분야별 보안법제 간의 역할구분이 불명한 것이 가장 큰 원인이라고 생각된다. 나아가 '보안'의 개념을 수직·수평적으로 분명하게 정립하고 역할분담을 하지 못함으로써 불필요한 정책경쟁을 유발한 것도 중요한 원인 중 하나이다.

이렇듯 국가안보적 정보보안의 개념과 범위가 불분명하게 획정되고, 정보통신분야의 일반법적 정보보안활동과 능력이 혼용되면서 수직 및 수평 관계가 논리적으로는 틀어지게 되었다. 즉, 정보통신 분야는 정보통신사업자를 규율하는 수직적 체계를 가장 큰 기반으로 하면서도, 정보통신망에서의 정보보안이라고 하는 수평적 체계 대부분을 모두 수용하는 일반법적 내용을 갖게 된 것이다.[17] 이러한 상태에서 개별

16) 국가 5대 전산망의 구축경과와 상세설명에 대해서는 대통령자문정부혁신지방분권위의 연차별 발간자료나, 2000년을 전후하여 정부가 발간한 정보화백서 또는 정보화촉진기본계획 등을 참고하기 바란다.
정보통신보안법제가 정보화법제의 제개정과정에서 단계별로 마련되어 온 연혁적 특성을 고려하면 정보화 추진과정에서 중요시 되어온 분야를 우선 특별분야로 고려하는 것이 합리적일 것이다. 그러나 이 분야 외에도 보안활동이 중요시 되는 특수분야는 무수히 많다. 여기서는 지면의 한계를 고려하여 몇 가지 분야만을 다룬다는 점을 분명히 하고자 한다.

17) 부연하면, 현행 정보통신망법은 사업자의 정보보안 관련 규제를 골자로 하고 있으면서도, 망과 시설에 대한 보호, 그리고 일반국민에 대한 특별형법적 규정은 물론, 개인정보보호와 정보통신 내용규제까지 모두 다루

분야별 정보보안과 개념적 혼동을 가져오는 것이 불가피함은 물론, 전문기술이나 추진체계의 확보 등에서 어떤 특정 분야나 기관이 우위를 점하고 있는 상황에서는 정책 간 경쟁이나 혼선이 발생하기에 용이한 구조이다.

이런 문제를 해결하기 위해서는 정보보안의 요소를 구체적으로 식별하고, 같은 것과 다른 것을 구분해 내는 개념적 접근이 선행되어야 한다. 예를 들어 정보보안은 수평적으로 모든 분야에 해당하는 내용으로 정하되, 개별법에서 정하고자 하는 수직적 정보보안을 구별해 내고 역할 분담을 시도하는 것이다. 이런 접근 방법은 정책의 틀을 짜는 것과 정책 수단의 동원과 집행에서의 일반관계와 특수관계를 분별하는 데 도움이 된다.

3.2 보호이익의 체계적 보호

개념적으로 구분된 수평적 정보보안과 수직적 정보보안은 분야별 정보보안이 보호이익에 집중할 수 있도록 해주는 효과가 있다. 정보보안에 관한 일반적 원칙을 천명하고 특별분야를 따로 정하여 분리하되, 해당 특별분야의 입법사항과 규제의 과학적 근거를 강화한다면 분야별로 건전한 경쟁도 촉진할 수 있다. 여기서 건전한 경쟁이라 함은 특별한 보안입법을 위하여 개별 정책기관이 신규제도를 도입하는 경우 일반적 보안입법 체계에서 그 효과성을 검증하거나 혹은 반대적 논의를 촉발하는 것을 말한다. 현재로서는 분야별로 지나치게 규제경쟁이 강하게 나타나면서 규제과잉 또는 공백분야가 발생할 수 있다고 생각한다.

3.3 사전위험예방행정의 근거

정보보안은 위험입법의 한 분야라 할 수 있다. 최근 들어 정보보안 사고는 위험의 전면성, 사고피해의 광범위성, 완전한 복구나 구제의 불가능성 등을 보여주고 있다. 위험책임을 개별 당사자에게 맡겨둘 수만은 없는 분야 특성이 존재한다.[18] 이런 문제점에 대응하기 위하여 가장 좋은 방법은 사전적으로 위험을 방지하기 위한 노력을 강화하는 것이다.

그러나 현재로서는 이런 종합적 대응을 추구하려는 능력과 노력은 여러모로 부족해 보인다. 공공과 민간부문을 막론하고 보안활동을 수행하여야 하는 당사자와 책임자에 대한 규제법규가 체계적이고 현실적이지 못할 경우 당사자는 규범적 수용능력을 갖추지 못할 가능성이 높다. 이렇게 되면 실제로 사고책임자가 운이 안 좋은 경우로 인식하게 되는 경우가 자연스러울 것이다. "하필 그 사고가 우리 회사에서 일어나거나 내가 재임하는 동안에 일어날 게 뭐람"이라고 하는 형태의 인식이 일반화되고, 사고 이후에 발생하는 손해배상이 기업의 현존가치를 넘어서는 경우, 또는 징계나 처벌과정에서 '사정을 참작한 판결'을 법률적으로나 사회적·정치적으로 용인하는 일이 반복되면 규범은 사실상 사문화되는 것이다.

우리 사회에서 정보보안에 관한 인식상의 문제는 예방을 위한 투자비 규모라는 지적이 많다. 정부부문의 정보보안 투자활성화를 비롯하여 위험예방을 위한 사전 점검, 감독 등 정보보안에 적합한 새로운 행정수단을 광범위하게 도입하는 것이 필요하다. 정보보안사고 예방 투자활동이나 노력에 대해 다양한 형태의 인센티브를 도입하는 것도 고려해 볼 수 있다. 규제조치를 수반하는 긴급한 대응체계를 정립하는 것이 예방행정의 중요한 내용임은 물론이다.

3.4 통합적 대응

정보보안 사고가 발생하였을 경우 단일 부처에서 개별적으로 대응하기도 하고 다양한 부처가 연계하여 통합적으로 대응하기도 한다. 그렇지만 법적 대응체계가 조직법적으로 잘 정비되어 있지 못한 점은 아쉬운 일이다.[19] 정보보안은 대상이 다양하고 개별적이라는 점을 앞에서 보았다. 그러나 위험요소나 대응방안이 유사하다는 점도 간과해서는 안된다. 고도 정보사회에서의 정보보안은 우리가 사회를 구성하면서 잘 구분한 개념의 융통적 통합을 요구한다. 공공과 민간, 수직과 수평, 국내와 국외, 수직 개별분야, 공급자와 이용자 등의 구분은 대응에 효율적인가를 기준으로 통합과 협력체계로 운영하여야 한다.

고 있다.

18) 그런 의미에서 정보통신보안에 있어서 기존 위험책임론이 갖는 의미는 새롭다. 위험책임론에 관한 논의는 상당한 역사를 가지고 있으나, 특히 공법분야에 관한 최근의 연구들을 참고하길 권한다[8,9].

19) 다부처에 권한과 업무가 분산되어 있고, 그 대응체계가 효율화 되어 있지 못한 부작용은 최근 우리사회가 경험한 일련의 안전사고에서 충분히 경험한바 있다. 개인정보, 행정정보, 국가기밀 등 보호의 대상이 되는 정보별로 소관부처와 지원·전문기관도 각기 다른 상황에서의 사고처리와 수습과정의 혼선은 우려를 넘어 시급히 개선이 필요한 사항이다.

이런 통합적 대응은 국가자원의 효율적 동원과 배분이라고 하는 전통적 정치 및 행정체계의 관념이 정보보안에 대해서도 잘 작동하여야 한다는 것을 의미한다. 국가권력의 구성요소와 조직체계를 정한 헌법과 정부조직법에 의하는 전통적 체계에 덧붙여 정보보안에 관계되는 각종 조직법과 작용법을 운용하기 위한 입법적 조치가 있어야 한다. 이때에는 정부 뿐 아니라 민간의 전문가 등도 함께 대응하는 민관군 총합대응체계에 관한 근거가 포함되어야 한다. 경우에 따라서는 국제적 자원동원이나 협력도 긴요하다.

3.5 입법원칙의 준수

입법원칙은 정보보안법제에서도 준수되어야 한다. 법률유보의 원칙, 명확성의 원칙, 비례 및 과잉금지의 원칙이 대표적 원칙이라 생각된다.

법률유보의 원칙은 대통령령이나 훈령 등에 의하여 관리되고 있는 정보보안활동에 대해, 보다 근본적인 법규범으로 이의 근거를 명확히 하는 노력이 요구된다. 특히, 과거 전통적인 보안법제에 있어서 군인이나 공무원 등에 요구되었던 특수하고 강력한 정보보안규제행위에 있어서도 이에 대한 구체적 근거를 확보하여야 할 것이다. 아울러 정보보안기술이나 산업이 간접적으로 영향을 받는 분야에 대해 보다 구체적 근거와 민간 참여를 보장하는 형태의 발전이 이루어진다면 좋겠다.

명확성의 원칙도 근거의 법률화 못지않게 중요하다. 전통적 정보보안법제에서의 추상성은 지속적으로 문제가 될 수 있다. 어떤 행위가 어떤 형태에 규제의 대상이 되는지를 명확히 하는 노력이 필요하다. '안전보장에 관한 정보' 등과 같은 불확정 개념을 보다 구체화하는 것부터 '공공질서' 등과 같이 헌법재판소가 이미 정하여 둔 불명확한 법규 기준 등을 우선 참고할 수 있을 것이다.[20]

20) 소위 '불온통신' 사건이다(헌재 2002. 6. 27. 선고 99헌마480). 당시 헌재는 모호한 의미의 불온통신으로 인정되는 대상을 대통령령으로 위임한 사항이 포괄위임금지 원칙에 반하고 있다고 판단하였는데, 이러한 흠결있는 규정으로 말미암아 정보통신부장관이 처리하게 되는 명령 또한 위헌으로 귀결된다고 판시한 바 있다. 아울러 헌재는 전기통신사업법상의 허위통신의 죄를 인터넷상의 표현행위에 적용하고자 한 소위 '미네르바 사건'에서도 해당 조항 중 '공익을 해할 목적'이라는 부분이 형벌의 명확성의 원칙에 반하여 위헌이라고 결정하였다(헌재 2010. 12. 28. 선고 2008헌바157, 2009헌바88(병합)).

규제과잉의 문제와 처벌위주의 실효성 확보수단도 차제에 재고되어야 한다. 과학적으로 정보보안에 기여하는 규제가 어떤 것인지 식별해 내고, 이를 평가하여 규제의 실효성을 검증하는 제도를 도입하는 것도 고려해 볼 수 있다. 일반법적 규정을 통해 이런 과잉규제에 대한 심사권한을 갖는 추진체계를 정립하는 것도 방법이다.

IV. 가칭 정보보호정책기본법의 구상[21]

4.1 필요성과 의의

정보보안에 관한 행정 및 정책관할은 연혁적으로나 내용적으로 특수한 분야로 인식되어 왔다. 특히, 정보보안에 관한 개념적 접근의 다양성과 정책환경의 특수성에 기인한 인식의 차이가 상존하여 왔다. 대체로 1990년대 중반 이후 정보화정책의 집중적 추진은 개념의 분화와 인식의 격차를 가중하는 결과를 초래하였다고 할 수 있다.

IT를 중심으로 하는 정보화정책을 추진하는 과정에서 전통적 정보보안의 관념과 정보화환경에서의 정보보안을 효과적으로 접목하는 데 어려움을 겪으면서 국가적 차원의 통합적·유기적 정보보안정책을 요구하는 의견은 점증하고 있다. 따라서 현 상황을 효과적으로 극복하기 위한 제도적 대응방안을 모색하는 것은 정보보안 정책환경의 개선은 물론 다가올 고도정보사회에서 국가 정책의 효율적 집행을 위하여 바

21) 지금까지 정보통신보안법제의 연혁과 쟁점에 관해 다루면서 그 대안으로 '정보보호'정책기본법을 제시하는 것이 다소 용어적·개념적 혼란을 야기할 수 있다고 생각된다. 우선 학계와 실무계는 물론이고, 관계법령에서 조차 정보보호, 정보보안, 사이버보안, 사이버안보 등의 다양한 용어가 명확한 의미 구분이 없이 혼재되어 사용되고 있고, 여전히 어느 정도의 통일된 견해의 합치는 이루지 못한 것으로 보인다(이와 관련된 자세한 사항은 정필운 교수의 연구[13]에 잘 정리되어 있으며, 일독을 권한다). 그러나 이러한 논쟁의 문제는 차치하고, 연구자는 정보통신보안법제 특수성과 해당 분야의 전문성이 전통적인 보안법제와 녹아들면서 우리 사회 모든 분야를 아우를 수 있는 상위의 기본법이 존재하여야 한다는 생각을 가지고 있다. 이 기본법의 명칭은 그간 우리 실무계에서 개인정보보호나 정보보안 등 다양한 보안대상과 활동의 상위개념으로서 '정보보호'라는 용어를 사용한 관행과 익숙함에 비추어(예컨대 '정보통신망의 이용촉진 및 정보보호' 등에 관한 법률의 용어 사용을 보더라도) 다른 용어보다는 정보보호정책기본법이 가장 적당한 명칭이 아닌가 생각한다.

람직한 일이 될 것이다.

앞서 살펴본 바와 같이 전통적 보안법제와 정책의 특색은 국가안보에 방점을 둔 견지로 대표되는 바, 냉전체제에서 출발하여 군사정부 등 권위주의 행정체제를 이어받은 한국의 경우 이 특수성이 행정전반에 유효한 상황이다. 법제적으로도 국가보안법, 국가정보원법, 군사기밀보호법 등 다양한 전통적 정보보안 정책 근거 법규가 존재하며 각기 실효적 수단을 보유한 것으로 평가할 수 있다.

2001년 9.11 테러사건 이후 정보자원 전반에 대한 보안정책은 전통적 국가안보적 관점에서 재구성되고 있으며 특히 국가 및 사회기반시설에 대한 보호가 중요한 정책이슈로 부상하였다[7,10]. 법제적으로는 정보통신기반보호법[22]을 비롯한 다양한 하위법규 등의 입법이 존재한다. 분야별 특성과 발전상황에 따라 정보보안에 관한 정책도 구체적으로 변모하고 있으며 이를 국가적 차원에서 유기적으로 운영하는 것이 숙제라 할 수 있다.

2010년 전후로는 정보화정책의 전면화와 스마트 환경이 전개되면서 정보보안은 분야별로 더욱 구체적으로 진화하는 단계에 와 있다. 지능형전력망(스마트그리드), 국방정보화, 행정정보 공유 및 보호 등 개별 분야의 보안정책은 기존 정보화정책과 더욱 밀접한 관계를 맺으며 전개되고 있으며, 이에 따라 분야별 사이버안전센터의 확충 등 침해대응 정책도 구체화되고 있다.

우리나라의 경우 다양한 형태의 수직적 내용에 대한 정책구체화와 입법적 대응은 활발한 것으로 평가된다. 특히, 정보통신망, 전자정부, 국가안보, 국방, 전력망, 금융 등 개별 분야가 편차는 있으나 해당 분야의 정책관할부처에서 경쟁적으로 법제를 구비하고 이를 지속적으로 보완·발전시키고 있다. 그러나 이러한 모든 분야의 입법·정책의 수준과 대응능력 등에서는 편차가 점증할 가능성이 있어 국가적 차원에서의 대응이 필요한 것도 사실이다. 수평적 내용으로서의 정보보안 정책이 경쟁적으로 추진되면서 추진체계, 연구개발지원, 정책수단 혼동 등이 우려되고 국가적 차원에서의 종합·조정을 통한 통합적 보안정책의 추진을 기대하는 데에는 아쉬움이 있다. 이제는 보안법제와 정책의 수평적·수직적 특성을 충분히 이해하고 이에 대한 개선방안을 제도적으로 도출하는 것이 향후 고도 정보사회의 구현을 위하여 바람직한 일이다.[23][24]

이런 차원에서 정보보호정책기본법은 보안정책의 수평적·수직적 특성을 기반으로 하여 이를 구체적으로 실현하기 위한 정책입법적인 성격이 크다. 다양한 분야에 걸쳐 존재하는 수직적 정보보안의 개념과 정책의 내용을 인정하면서도, 정보보안의 개념적 범위를 설정·구체화하고 이에 대응하기 위한 범정부수준의 통합적 정책체계를 확립함은 물론 국가적 차원에서 정보보안을 위한 자원동원의 효율성과 효과성을 보장하는 근거 입법으로서의 위상도 가진다.

또한 개별분야의 특수한 규율을 위한 입법 내용은 개별법에 두고 정책체계 효율화를 위하여 필요한 공통사항은 기본법에 두는 법제 간 역할분담을 가능하게 하는 입법으로서의 의의도 가진다. 이렇게 되면 장기적으로 해당 정책이 경쟁과 협력을 지속하면서 일반법과 특별법의 관계 또는 기본법과 개별법의 관계를 발전시키는 정책환경을 제공할 수 있을 것이다.

4.2 정보보호정책기본법의 주요 내용

정보보호정책기본법은 기본법적 내용을 제공하기 위하여 정책의 대상을 명확히 확정할 필요가 있다. 이를 위하여 목적과 정의 및 적용범위를 총칙에 규정하되 ① 온라인과 오프라인 정보보안을 모두 포괄, ② 국가안보와 정보화분야를 포괄, ③ 적용우선순위와 규범경쟁의 해결방안 등에 관한 사항을 포함하는 것이 필요하다.

정책의 집행체계로서의 추진체계를 구체적으로 규정하되 ① 국가전체적 차원에서 집행체계의 협의·조정 기능을 확보, ② 모든 정보보안정책을 총괄하는 기구의 설치 또는 전임 행정기관(주무관청)의 지정,

22) 2001. 1. 26. 제정, 법률 제6383호.

23) 같은 맥락에서 강경근 교수도 일관된 법제도가 없는 상태에서의 정보에 대한 침해는 사회적 수고와 경제적 비용의 증가로 이어지므로, 정보보호 관련 법제를 체계적으로 분류하여 그 일관된 법원리와 헌법원리에 입각한 통일성 있는 정보보호 법제를 마련하여야 한다고 주장한다[11].

24) 이런 차원에서 최근 일본이 사이버보안기본법의 입법에 성공한 것은 우리에게 큰 시사점을 준다. 일본은 2014. 11. 12. 총4장(제1장 총칙, 제2장 사이버보안전략, 제3장 기본적 시책, 제4장 사이버보안전략본부)에 35개 조문, 부칙 3개 조문으로 구성된 기본법의 입법에 성공하였으며, 관련추진체계 정비와 더불어 대규모 예산투입을 준비하고 있다. 법안 원문은〈http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm〉 참고.

③ 정보보호기술・집행관리・사업관리 등의 전문기관 및 전문가 집단의 효율적 관리방안, ④ 개별 정책의 추진기관과의 역할분담 방안 등을 규정하여야 한다.

또한 기본법의 구체적 정책수단으로서 ① 정보보호 기본계획 및 시행계획, ② 연구개발・인력개발・민관협력・국제협력 등 다양한 조성행정기능, ③ 조성행정을 위한 기금 등 재원의 확보방안, ④ 정보보호정책을 위한 고권적 행정수단으로서 긴급대응・조사・위험예방활동・신고대응 등 다양한 규정과 그에 상응하는 보상제도의 도입, ⑤ 실효적 수단으로서의 금지행위와 형벌규정[25] 등의 규정을 둘 수 있을 것이다.[26]

나아가 일반민사적 상황에서 적용 가능한 환경조성을 위한 사항으로써 ① 정보보호산업, ② 정보보호 서비스 및 기관인증, ③ 전문자격제도의 도입, ④ 공제・부조 및 보험제도 등에 대한 규정도 주된 입법의 내용이 될 것이다.

4.3 정보보호정책기본법의 입법 전략

정보보호정책기본법에는 다양한 규정의 도입이 가능하겠으나, 정책기본법은 정책의 추진체계와 자원동원의 효율적 관리라고 하는 근본 목적에 충실하게 입법을 추진하는 것이 바람직하다. 복잡하지 않은 내용을 설정하는 것은 조기 입법의 완료에 도움이 된다. 또한 필요한 제도이나 기본법에 반영하지 못한 경우에는 개별 분야별 입법을 통해 구체화하면 된다.

기본법과 더불어 제・개정하여야 할 개별 법률안의 로드맵을 동시에 마련하여 입법을 추진하여야 한다. 결국 이 로드맵이 정보보안법제가 전체적으로 체계성 있게 발전할 수 있는 모델이기 때문이다. 정보보호정책기본법의 제정은 우선적으로 기존의 법률인 정보통신망법, 정보통신기반보호법, 전자정부법, 지능형전력망법, 국방정보화법, 전자금융관계법 등의 개정소요를 수반하게 될 것이다. 현재 법률이 없는 다양한 행정분야에서 특별입법의 소요를 발굴하여 제정안을 마련하여야 하며 암호관리 등 수평적 행정분야에 관한 개선소요도 추가로 검토할 수 있을 것이다.

25) 경우에 따라서는 형법이나 개별법규에 규정이 가능하나 일반적 조항에 대한 규정을 추진하는 것이 보다 바람직할 것이다.

26) 입법기술적 관점에서 벗어나 정책학적 범주로 나아가면 정책성공을 위한 보다 다양한 논의와 아이디어를 얻을 수 있다. 참고로 황종성 외의 연구[12]에서는 정보화 관련 법령정비를 위한 기초적인 고려요소로 ① 헌법적 요청의 존중, ② 상위 정책목표와 하위 정책목표 사이의 정합성 유지, ③ 정당한 정책목표가 가장 적확하게 가능한 한 최소한의 비용으로(경제적, 사회적, 기술적 총비용) 달성될 수 있는 방안 모색, ④ 적절한 제재수단의 선택, ⑤ 집행의 수월성 문제 등을 거론하고 있다.

V. 맺음말

우리는 역사적·상황적 특성에 따라 보안법제의 체계적 발전을 도모하지 못하고 있다. 다행히 최근 들어 정보보안 대한 인식이 개선되고 중요성이 부각됨에 따라 법제적 노력을 기울여야 한다는 논의가 정부 내외부로부터 확산되고 있다. 이에 우선 정책의 체계를 개선하기 위하여 필요한 조치가 무엇인지, 그리고 왜 그런 조치가 필요한 지에 대한 생각을 정리하여 보았다.

아직 정보통신보안법제에 대한 체계적 연구가 부족한 상황에서 시론적 논의를 보태는 것도 무척 조심스러운 것이 사실이다. 더구나 수년 동안 부처 간 정책경쟁이 있어 왔던 분야에서 생각을 내어 놓는 것이 새로운 분란의 씨앗이 될 수도 있다고 생각하니 더욱 우려스럽다. 그럼에도 불구하고 우리가 입법적 노력을 기울이고 정책을 체계적으로 운용하지 않으면 애써 마련한 정보통신 강국이 사상누각이 될 수도 있다고 생각하니 어떤 모양으로든지 논의를 촉발하는 것이 이 분야 연구자로서의 사명이란 생각도 갖게 된다. 모쪼록 정부와 의회가 국민적 뜻을 결집하고 기존의 정책을 반성하면서 새로운 차원의 정보사회를 구현하는 데 도움이 되길 바라면서 글을 맺고자 한다.

References

[1] Gil-Hyun Nam, "E-Government Implementation and necessity of information protection", Korea National Defense University, 2000.

[2] Banks.S., "Security Policy", Computer & Security, Vol. 9., 1990.

[3] B. Von Solms., "Information Security-The Fourth Wave", Computer & Society, Vol.25., 2006.

[4] Abram N. Shulsky, Silent Wafare: Understanding the World of Intelligence,

Virginia: Brassey's, Inc, pp.1-3, 2002.
〔5〕 Intelligence Committee, "Presentation source book of Public hearing for enactment of national cyber crisis management act", Republic of Korea National Assembly, 2013.
〔6〕 Intelligence Committee Senior Professional Advisor, "Bill of national cyber terrorism prevention, Bill Review Report of national cyber safety administration", Republic of Korea National Assembly, 2013.
〔7〕 So-Young Yook, "The Necessity of Enacting Cyber Security Act", Journal of Korean Comparative Public Law Association, 11(2), 2010.
〔8〕 Peter Baumeister, "Staatshaftungsrechtliche Fragen in der Risikogesellschaft ", Korea Public Land Law Association Public Land Law Review, 32(2), Trans. Seung-Pil Choi, Korean Public land law Association, 2006.
〔9〕 Gi-Jin Kim, "The Study on the Theory of Risk Liability", Korea Public Land Law Association Public Land Law Review, 43(2), 2009.
〔10〕 Do-Seung Kim, "Legal Challenge for Cyber Crisis Response", Journal of Korea Information Society Development Institute, 21(17), Korea Information Society Development Institute, pp.38, 2009.
〔11〕 Kyung-Keun Kang, "Legal Perspectives and Prospects of Information Security", Journal of Korean Comparative Public Law Association, 6(2), pp.204, 2005.
〔12〕 Jong-Sung Hwang and others, A Theoretical Study on the Policies for Information Legislations Reform, National Information Society Agency, pp.9-11, 2007.
〔13〕 Pil-woon Jung, "A Critical Analysis on the Concept of 'Cyber Security'", Yonsei Journal of Mediccal and Science Technology Law, 2(2), 2011.

〈저자소개〉

권 헌 영 (Hun-Yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 졸업
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2015년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부