사단법인 한국토지공법학회
토지공법연구 제77집 2017년 2월
Korea Public Land Law Association
Public Land Law Review
Vol. 77, February, 2017

제어국가에서 해킹 제어와 방식*

The Review on the Steering and Way of Hacking in Steering State

성 봉 근 (고려대학교 강사, 법학박사)
Sung, Bong-Geun / Korea University, The Department of Law. Ph.D. in Administrative Law

국문초록

해킹을 제어하기 위해서는 새로운 국가관과 행정의 패러다임이 필요하다.

해킹에 대한 방어와 대비를 국가기관이 일방적으로 전담하는 규제국가의 패러다임은 규범구조적인 면에서 민주주의와 헌법을 훼손할 위험성이 크며, 실효성면에서도 지나치게 국가에게 부담이 될 뿐만 아니라 전문성과 신속성 및 유연성이 떨어진다. 따라서 최근의 세계적인 흐름에 따라 보장국가의 국가관에 따라 국가와 민간이 함께 공동의 해킹 제어 책임을 지며, 시장에 대한 거리를 유연하게 조절하며 제어하는 제어국가의 방식으로 패러다임을 변화시키는 것이 필요하다.

과학기술적인 규범에 대한 특성을 고려하여 해킹에 대한 법이론적 논의를 의의, 성질과 피침해이익, 위험 등과 관련하여 논의하였다.

다음으로 최근의 해킹에 대한 제어를 적절하게 할 수 있도록 해킹에 대한 '새로운 분류체계'를 제시하여 보았다.

* 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2015S1A5B5A07041099)

제어하여야 할 해킹의 범위에 대하여도 주체별로 해커에 의한 침해 뿐만 아니라 국가에 의한 침해 등으로 확장하여 검토하여야 한다. 해커에 의한 침해도 외부적인 침해와 내부적인 침해. 통상적인 침해, 웹 해킹, 시스템 해킹 등으로 다양하게 이제는 제어하여야 한다. 국가에 의한 침해도 위법한 '온라인수색'(Online Durchsuchung, Online search) 등과 적법한 '전략적 해킹'(Tactical Hacking) 등으로 분류하여 연구할 필요가 있다.

해킹을 규제하는 법령들을 독일을 중심으로 유럽의 입법과 우리의 입법들을 비교하여 검토하여 보았다. 이와 관련된 판례도 살펴보았다.

제어국가에서의 해킹 제어를 위한 다양한 방식들을 살펴보았다.

구체적으로는 헌법·일반법·개별법의 체계적 입법을 하여 해킹에 대한 입법적 제어가 필요하다. 입법은 물론 행정에 있어서도 일방적으로 해킹을 처벌하고 규제하는 패러다임보다는 대화형 입법과 행정을 통한 해킹 제어가 바람직하다. 해킹에 대하여 책임지는 담당기관의 구축을 하여야 한다. 해킹 방지의무를 국가기관과 사회 및 기업체, 시민들에 대하여 전반적으로 강화하는 것이 필요하다. 제어국가에서 시장과의 자율성을 존중하면서도 해킹의 위험을 감소시키기 위해서는 지속적인 모니터링을 하고 보고체계를 갖추는 것이 필요하다. 과학기술규범의 특성상 과학기술의 발전을 반영하는 법제도를 정비해 나가야 한다. 해킹에 적합한 실효성 확보수단을 정비하고 강구하여야 한다. 그러나, 해킹 제어과정에서 발생할 수 있는 기본권 제한의 한계를 설정하고 조화되도록 하여야 한다. 해킹 피해를 개인의 문제로만 보지 아니하고, 권리구제를 철저히 함과 동시에 해킹에 대한 사회보험을 강구하는 것이 필요하다.

Abstract **

Now we need to get new paradigm and Ideological reflection on the nation so that we can control and steer of hacking effectively and properly.

The old paradigm is so called 'Regulatory State' which Government try to compulsively regulate hacking only by itself. But this is possible to infringe of democracy and constitution. In addition to it, this cannot be special, rapid and flexible to control hacking.

Therefore we can conclude that we shall change paradigm from Regulatory State to Steering State following global trend in also for hacking control.

At first, I've mentioned about concept, character of hacking, and related risk

** This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2015S1A5B5A07041099)

considering law of science and technology.

At second, I've suggested new classification of Hacking so that can properly steer in this Information Society.

So we can consider not only Hacking by Hackers but also Hacking by Government. And we can classify inner hacking and outer hacking, traditonal hacking for example ddos and web hacking, system hacking. There are also Online search and Tactical Hacking in way of hacking by government.

At third, I've researched about many laws especially including german law and court's decisions.

Finally I've try to suggest many ways for control and steering of Hacking.

Concretely speaking, we need to amend scattered laws for Hacking, especially make legislation better for example hierarchy which is arranged in order of constitution, general law, and individual law.

The Interactive structure in legislation and administration is better than one-sided for control and steering of Hacking.

We need to construct specialized and responsible Control Tower in executive for steering.

We shall raise the level of duty for protecting hacking in Government, Enterprise, and Society also through legal system including remedy.

(주제어) 해킹(hacking), 해킹의 분류(Classification of hacking), 해킹 제어 패러다임(hacking control paradigm), 거리(Distance), 보장국가(Steering State), 제어국가(Ensuring State), 온라인 수색(Online search), 전략적 해킹(Tactical Hacking), 해킹 제어 방식(the Way of Hacking Control)

Ⅰ. 머리말

정보화 사회에서 해킹을 통하여 시민들의 기본권이 침해되고, 사회질서가 교란되고 있다. 국가기관이 더 이상 사회에서 해킹으로부터 완벽하게 차단된 안전망을 제공해 주지 못하고 있다. 니더커트(Neithercutt)도 이로 인하여 대중들은 수많은 전투경기장(arenas)이나 다를 바 없는 사회에서 '법의 집행'(Law Enforcement)을 더 이상 신뢰하지 않는다고 지적한다.[1)]

해킹은 기존 사회에서 발생하던 기본권 침해 방법 내지 사회질서 교란 방법과 차이가 있다. 해킹의 주체는 해킹을 감행하는 자연인, 단체는 물론 최근 필요에 의하여 일부 국가에서 행하기도 한다는 점이 드러나고 있다. 해킹의 상대방 역시 자연인은 물론 각종 단체와 기업에만 국한되지 않고, 최근 국가의 각종 행정조직과 기간시설 등을 가리지 않는다. 해킹에 의하여 각종 기본권과 법익들이 침해되는데, 정보의 자기결정권과 프라이버시[2], 인간의 존엄성 등은 물론 구체적인 재산권의 침해, 생명·신체의 안전, 행동의 자유, 각종 위험으로부터의 안전, 국가안전보장과 사회질서, 국제 안보 등에 이르기까지 다양하다.

해킹의 방법과 유형은 법률의 제정이나 행정작용 보다 앞서 가면서 기존의 규제 및 방어를 무색하게 하고 있다. 이에 '과학기술규범'의 특성상 기술의 발전을 미처 따라가지 못해 규범의 실효성을 종종 잃어버리기가 쉽다. 이에 대비하기 위하여 첫 번째로, '해킹에 대한 새로운 분류체계'의 구성이 필요하다.

두 번째로, 해킹을 제어하기 위해서는 새로운 국가관과 행정의 패러다임이 필요하다.

해킹에 대한 방어와 대비를 국가기관이 일방적으로 전담하는 '규제국가'(Reguratory State)의 패러다임은 규범구조적인 면에서 민주주의와 헌법을 훼손할 위험성이 크며, 실효성면에서도 지나치게 국가에게 부담이 될 뿐만 아니라 전문성과 신속성 및 유연성이 떨어진다.

최근의 세계적인 흐름은 '보장국가'(Ensuring State)의 관점에서 국가의 책임을 사인 및 각종 단체와 분할하고 분담하여 국가의 기본권 의무와 각종 보장책임의 이행을 효과적으로 수행한다. 이를 위해서 '제어국가'(Steering State)의 관점에서 해킹에 대한 전문적인 규제도 시장의 자율규제를 활용하기도 하고, 규제된 자기규제를 활용하는 등의 약한 규제 방식을 취하기도 하고, 때로는 국가가 직접 개입하여 강하게 규제하는 방식을 취하는 등의 다양한 방식으로 접근하여야 한다.[3] 해킹에 대한 사전 대비와 사후 구제 모두 중요하다. 이와 관련된 입법과 이론 및 판례 등에 대한 다양한 연구를 통하여 해킹에 대한 제어와 방식에 대한 법적 고찰이 요구된다. 기술과 규범이 결합된 분야이어서 두 분야 간의 연결을 바탕으로 고찰하기로 한다.

---

1) Neithercutt, Introduction to Tactical Hacking : A Guide for Law Enforcement, Police Technical, 2015, at 7.

2) 프라이버시와 정보자기결정권을 실질적으로 구별하지 않는 입장과 여전히 구별의 실익이 있다는 입장으로 대립한다. 전자의 입장으로는 길준규, 통합개인정보보호법과 효과적인 개인정보의 보호, 토지공법연구, 제57집, 2012.5, 218면. 후자의 입장으로는 손형섭, 개인정보의 보호와 그 이용에 관한 법적 연구, 법학연구, 법학연구 제5집, 2014.6,11면.

3) 성봉근, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 239면.

Ⅱ. 해킹에 대한 법이론적 논의

1. 해킹의 의의

(1) 해킹의 개념

해킹(hacking)이라 함은 컴퓨터 네트워크의 취약한 보안망에 권한 없이 불법적으로 접근하거나 정보 시스템에 유해한 영향을 끼치는 행위이다. 앨빈 토플러에 의하면 정보통신 기술의 발전은 정부와 시민 이외의 제3의 세력들로서 해킹 세력들을 키워내게 되었다.[4] E 따라서 해킹과 관련된 법률관계는 '정부 대 시민'의 단순한 대립구조가 아니라. '정부와 시민 및 제3의 해킹 세력' 등으로 복잡하게 얽히게 되는 다극적인 구조로 파악하여야 한다.

해킹은 권한이 없는 경우뿐만 아니라 권한을 넘어서는 경우도 포함한다. 그러나 최근에는 예외적인 경우에는 정보주체의 동의 없이 침해하지만 국가 등의 허가를 받아 행하는 전략적 해킹 등의 개념도 논의되기 시작하고 있다.

'정보화 사회'(情報化社會; Informationsgesellschaft, Information Society)[5]에서 이해관계의 대립구조는 해킹 세력들로 인하여 복잡해지게 되었고, 해킹으로부터 전자정부와 시민을 보호하는 과제가 전자정부에게 부여되고 있다.

그리고 해킹은 국경이라는 경계가 무너지는 탈경계화'(脫境界化; Entgrenzung; De-bordering; Beyond)와 '네트워킹화'(網化; Vernetzung; Networking)[6], 국제화(Globalisieung) 등을 배경으로 종래의 국내법적 규율만으로는 법률관계를 제대로 제어할 수 없게 되었다.

(2) 해킹의 성격과 피침해이익

해킹이 침해하는 보호이익은 개인의 정보를 비롯한 각종 자유에 대한 '자기결정권'[7], 생명·신체의 안전과 재산권[8] 등이 있다. 기업의 영업의 활동과 관련하여 기업의 정당한 비

---

4) 최호진, 온라임게임 계정거래와 정보훼손죄 성립여부, 한국형사판례연구회 형사판례연구[21], 박영사,; 강동범, 사이버범죄와 형사법적 대책, 형사정책연구 제11권, 2000년, 80면; 박희영, 단순해킹의 가벌성에 관한 비교법적 연구 - 독일 형법 및 사이버범죄 방지조약을 중심으로-, 인터넷법률 통권 제34조, 2006.3, 23-24면 From 이관희 3면 각주 5 6 7

5) Hoffmann-Riem, Verwaltungsrecht in der Informationsgesellschaft - Einleitende Problemskizze, in Hoffmann-Riem/Schmidt-Aßmann(Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Nomos Verlagsgesellschaft, Baden-Baden, 1.Auflage, 2000, S.10.

6) Hoffmann-Riem, Das Recht des Gewährleistungsstaates, in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2005, S. 98. ; Hoffmann-Riem, Verwaltungsrecht in der Informationsgesellschaft - Einleitende Problemskizze, in Hoffmann-Riem/Schmidt-Aßmann(Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Nomos Verlagsgesellschaft, Baden-Baden, 1.Auflage, 2000, S. 37 - 38.

7) 공공기관의 정보공개에 관한 법률 제9조 제1항 제6호

8) 공공기관의 정보공개에 관한 법률 제9조 제1항 제3호

밀이 훼손될 수도 있으며[9], 국가의 안전보장 등 국가의 중대한 이익[10]과 사회의 안전을 심각하게 훼손시킬 수도 있는 장애와 위험 등에 이른다.

이 중에서도 특히 중대하게 침해되는 것은 '정보의 자기결정권'이다. 이는 오래전 독일 연방 헌법재판소의 '인구조사판결'[11]에 의하여 강조되기 시작한 개념이다. 인구조사판결은 정보의 자기결정권을 인정함과 동시에 이에 대한 침해는 법률유보의 원칙과 비례의 원칙에 따른 이익형량상의 위법성 판단 기준을 충족시켜야 한다고 판시하였다.[12] 이러한 인구조사판결의 시대적 상황이 오늘날과 다르지만, 해킹과 관련된 법이론적 기준으로서의 적용가능성은 여전히 유효하다고 생각한다.

정보보호는 전자행정의 고유한 문제는 아니고 전체 행정의 문제이기는 하지만, 마우러(Maurer)가 지적하듯이 전자 행정작용과 관련하여 정보보호는 특별히 논란이 되므로 논의가 필요하다. 왜냐하면, 전자정보처리시설을 통하여 무한정한 개인의 정보들이 저장되고 처리될 수 있기 때문이고, 또한 제3자에 의한 해킹을 확실하게 막을 수 없기 때문이다. [13]

최근에는 독일연방헌법재판소는 '온라인수색판결[14]'을 통하여 정보의 '시스템'에 대한 무결성과 기밀성 등을 이른바 'IT 기본권'으로 인정하는 판시를 하고 있다. 국민들에게 정보기술시스템상의 보안이 유지되어야 한다는 '기밀성'(機密性; Vertraulichkeit, Confidentiality)과 정보의 내용이 변경되지 않아야 한다는 '무결성'(無缺性; Integrität, Integrity) 등이 'IT 기본권'이라는 새로운 기본권으로 인정되어야 한다는 것이므로 우리의 경우에도 제3의 기본권으로서 받아들여질 수 있다.

해킹은 전술한 여러 가지 개인적, 국가적, 사회적 이익들을 위법하게 침해하는 행위이지만, 특히 정보와 관련하여서 독일연방헌법재판소의 판시에서 인정된 정보 자체에 대한 '정보의 자기결정권'은 물론 정보시스템에 대한 'IT 기본권'도 함께 침해하는 행위로 성격이 추가하여 규정되어야 할 것이다.

2. 해킹과 관련한 행정법상 위험의 범위

해킹이 야기하는 위험은 전통적 위험과 구별되는 현대형 위험에 속하게 된다. 절충설에 따라 위험을 이해한다면, 위험은 그 특성을 고려하여 개연성의 판단시기를 이른바 "Je-desto-Regel"에 따라 다르게 적용하게 될 것이다.[15] 해킹은 피해를 당하는 시기에 인지하기가 어려울

9) 공공기관의 정보공개에 관한 법률 제9조 제1항 제7호
10) 공공기관의 정보공개에 관한 법률 제9조 제1항 제2호
11) BVerfGE 6, 1 (46)
12) BVerfGE 65, 1 (46).
13) Maurer, Allgemeines Verwaltungsrecht, 18. Aufl., Verlag C.H. Beck,, 2011. S.483-484 Rn.20.
14) BVerfG, 1BvR 370/07 vom 28.2, 2008
15) 성봉근, 보장국가에서의 위험에 대한 대응 - 전자정부를 통한 보장국가의 관점에서 본 위험-, 법과 정책연구, 제15권 제3호, 2015.9, 1050면.

뿐만 아니라, 피해가 발생한 이후에도 이를 인지하지 못하는 경우도 많다. 해킹은 컴퓨터와 정보통신기술을 활용하는 정보화 사회에 있다는 것만으로도 잔존위험성(Restrisiko)가 존재하면서, 위험의 가능성 단계인 '리지코(Risiko, Risk)로서의 위험'에서 위험의 개연성 단계로 발전한 '게파(Gefahr, Danger)로서의 위험' 사이의 시간적 간격이나 발전 속도가 매우 빠르다. 또한 가능성 단계의 위험에서 출발하여 개연성 단계의 위험을 거쳐, 장해(Störung, Accident) 단계로 도달하는 것이 순식간인 특징이 있다. 또한 해킹은 손해가 발생하여 장해가 이미 존재하는 경우에도 2차 해킹의 위험이 잠복하거나 동시에 공존할 수 있다.[16]

헌법 제10조상 국가는 국민에 대한 기본권 보호의무를 진다. 따라서 국가는 해킹으로부터도 국민을 보호하여야 할 헌법상의 의무가 있다.

제3의 해킹 세력이 기본권을 침해하거나 국가의 안전보장과 사회질서를 침해하는 경우에는 기본권의 대사인적 효력에 의하여 기본권을 보호할 의무가 있다. 전자정부에서 기본권을 침해하는 해킹 세력들에 대한 규제는 민사상의 책임, 형사상의 책임, 행정상의 책임 등으로 분류할 수 있다. 이들 책임이나 구제가 병행되는 경우도 가능하다.

정부가 리바이어던이 되어 개인의 사생활을 침해하거나 사상을 검열하는 경우에는 기본권의 대국가적 효력과 관련하여 기본권 보호의무를 진다.

국가가 국민의 기본권을 보호할 의무를 수행하고 사회의 안녕과 질서를 유지하여야 할 의무가 존재한다는 것은 당위(Sollen)에 해당한다. 그러나, 해킹에 대한 제어는 그 어떤 위험이나 장애 원인들보다도 사실상 제대로 수행하기에는 많은 어려움과 제약이 따르는 현실(Sein)과 크게 괴리가 된다.

최근의 해킹의 기술의 발전과 관련하여 행정청은 비참하게도 예산상의 제약, 각종 규제상의 제한 및 훈련·교육·기술 등의 부족으로 인한 각종 방해를 받아 제대로 따라 잡을 수가 없다.[17]

Ⅲ. 해킹의 유형과 사례

1. 해킹에 대한 새로운 분류체계의 구상

해킹에 대한 유형을 최근의 사이버상의 위험과 관련하여 새로운 분류체계를 다음과 같이 수립해 보고자 한다. 과학과 기술에 대한 법 분야이므로 기술적인 사실관계를 함께 고

16) Kugelmann, Polizei- und Ordnungsrecht, 2. Aufl., Springer-Verlag Berlin Heidelberg, 2012, § 5, Rn. 107.

17) Neithercutt, *Id.* (Fn. 1), at 8.

려하여 이 글에서 '새로운 분류체계'를 처음으로 시도해 보고자 한다. 이는 해킹에 대한 규범들이 실효성을 잃지 않도록 현실적인 과학과 기술의 발전을 반영하기 위한 것이기도 하다.

2. 침해 주체에 의한 유형분류

(1) 해커에 의한 침해 유형

사이버 안전을 침해하는 각종 행위를 하거나 유해한 환경을 조성하는 자가 해커인 경우이다.

해킹 세력들은 국내에 국한되지 않으며 국제적인 활동을 하는 경우들이 많다. 또한 해커들은 사이버 상으로는 국가와 전력이 비대칭이지 않고 대등하거나 심지어 우월한 정보통신 기술력을 보유하기도 한다. 이러한 해커들[18]은 사이버상으로는 종래의 국가와 시민의 대립구조에 큰 변화를 가져오는 제3의 축이 된다. 해킹 세력들도 의도에 따라 시스템을 뚫는 해커와 악의적인 침입자인 크래커를 구분기도 한다. 크래커에는 정보 획득을 위한 단순 침입자인 '인트루더(Intruder)'와, 시스템의 서비스를 막는 '어태커(Attacker)', 시스템을 파괴하고 상용 프로그램의 복사 방지장치를 풀거나 바이러스를 전파하는 '디스트로이어(Destroyer)' 등이 있다.[19]

해킹 세력들은 금융정보를 탈취하여 금융사기를 의도하는 자들로부터 위키리크스 같이 정치적인 이해관계를 가지고 움직이는 경우들도 있다.[20] 해킹 세력들은 국내에 국한되지 않으며 국제적인 활동을 하는 경우들이 많다. 또한 해커들은 사이버 상으로는 국가와 전력이 비대칭이지 않고 대등하거나 심지어 우월한 정보통신 기술력을 보유하기도 한다. 이러한 해커들은 사이버상으로는 종래의 국가와 시민의 대립구조에 큰 변화를 가져오는 제3의 축이 된다.

(2) 기업에 의한 침해 유형

사이버 안전을 위협하는 또 다른 침해의 주체는 기업이다. 기업은 이윤의 창출과 이윤극대화를 위하여 행동한다. 라리유(Larrieu)에 의하면 개인정보에 접근하는 방식에 있어서 옵트인(opt-in) 방식과 옵트아웃(opt-out) 등 두 가지가 강구된다.[21]

고객의 정보에 대한 접근을 제한하여 정보의 자기결정권과 프라이버시를 보호하는데 비중을 두는 각종 옵트인(opt-in) 규제 법령이 마련되어 있지만,[22] 기업은 이에 대하여 각종

18) http://terms.naver.com/entry.nhn?docId=3432462&cid=58445&categoryId=58445 최종 방문일 2016.10.19.
19) http://terms.naver.com/entry.nhn?docId=3432462&cid=58445&categoryId=58445 최종 방문일 2016.10.19.
20) 성봉근, 전자정부에서 행정작용의 변화에 대한 연구, 고려대학교 박사학위논문, 2014, 71면.
21) Larrieu, Droit de I'nternet, ellipses, 2e édition, 2010, 189 p.
22) 성봉근. 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 60면.

혜택을 미끼로 하여 고객들의 사전동의를 매우 용이하게 받아냄으로써 성공적으로 규제법령을 우회적으로 피해가면서 영업을 수행하고 있다.

사이버 상에서 고객의 정보는 재산적 가치를 크게 가지게 되며, 기업에서 적극적으로 고객의 정보를 해킹에 의하여 취득하려하거나, 고객 정보에 대한 매매를 정보주체인 시민들의 동의 없이 하기도 한다.

기업에 의한 침해는 입법적인 로비나 활동으로까지 이어지고 있다. 최근 기업들은 4차 산업혁명(4th Industrial Revolution)[23]을 기치로 내걸면서, 사물인터넷(Internet of Things; IOTs)과 빅데이터(Big Data) 등을 보다 적극적으로 활용하기 위하여 종래의 옵트인(Opt-in) 원칙에서 옵트아웃(Opt-out)원칙으로의 전환을 하자는 주장들[24]을 지지해 왔다. 기업들은 이러한 방향으로 입법청원을 해 왔으며, 그러한 압력과 노력들이 '옵트인 원칙의 완화'를 거쳐서 '옵트아웃 원칙으로 변화'하는 것이 현실적인 법령으로 입안되어 나갈 추세이다. 최근의 예로서 '개인정보 비식별 조치 가이드라인'이 2016.7.에 제정되었다.

이러한 변화가 프라이버시와 기본권 등을 약화시킨다면 위법한 침해뿐만 아니라 적법한 침해도 사이버 상에서 발생한다.

(3) 국가에 의한 침해 유형

1) 분리의 원칙과 예외

(가) 정보기관에 의한 침해

국가정보원이나 사이버 수사대 등 정보 수집을 담당업무로 하는 국가기관에서 국가안전보장이나 질서유지 등은 물론 산업기밀 유출방지, 테러방지, 범죄발생 가능성 등의 파악, 정치적인 동향 파악이나 여론 형성의 통제 등을 목적으로 해킹을 하는 경우들이 있다. 이에는 후술하듯이 정당한 목적 하에 적법한 절차를 밟아서 행하는 적법한 침해와 '빅 브라더'로서 정당하지 못한 목적을 가지고 적법절차를 위반하고 행하는 위법한 침해가 있다. 특히 정치적인 목적으로 행해지는 사이버 검열도 사이버상의 기본권의 안전과 보장을 침해하는 유형 중의 하나로 포함시킬 수 있다.

23) 4차 산업혁명은 기업들이 제조업과 정보통신기술(ICT)을 융합해 작업 경쟁력을 높이기 위한 차세대 산업혁명을 의미한다. http://terms.naver.com/entry.nhn?docId=2805211&cid=43659&categoryId=43659 최종 방문일 2016.10.19. 4차 산업혁명이 3차 산업혁명인 정보통신기술의 활용을 넘어선 성격을 가지는 이유는 사물 인터넷(internet of things)을 통해 생산기기와 생산품 간 상호 소통 체계를 구축하고 전체 생산과정을 최적화를 구축하려는 것이기 때문이다. http://terms.naver.com/entry.nhn?docId=3403455&cid=42107&categoryId=42107 최종 방문일 2016.10.19.

24) 최경진, 미래 ICT 환경에 맞는 바람직한 개인정보보호 법과 정책의 개선방향, in 제4차 산업혁명 물결, ICT 법제 개선방향, 국회 제4차 산업혁명포럼, 2016.7, 66면.

(나) 집행기관에 의한 침해

경찰기관과 정보기관의 '분리의 원칙'(Trennungsgebot)이 고전적인 구조이었지만, 사이버상에서는 이 역시 탈경계화의 대상이 될 수 있다. 사이버 상에서는 수사와 단속의 대상이 되는 범죄 행위가 정보에 대한 무권한 접근과 탈취, 정보사기 등의 모습으로 나타나게 되므로, 사이버상에서 수사기관과 정보기관의 분리의 원칙을 고수하는 것은 정보화 사회에서 더 이상 통용될 수 없다는 점을 충분히 헤아리지 못한 것이다. 테러방지 등 각종 현대형 위험에서 보듯이 수사기관과 정보기관, 일선 행정기관과 정보기관 등이 정보교환을 위하여 '협력의 원칙'이 함께 적용될 수 있어야 할 것이다.[25]

2) 위법성에 따른 분류

(가) 온라인 수색

국가에 의하여 필요에 따라 행해지게 되는 온라인 수색(Online-Durchsuchung)은 정보기술시스템에 은밀하게 접근하는 것이다.[26] 온라인 수색은 '진행 중인 전화통신'을 대상으로 하는 것은 법률유보와 영장주의를 충족하는 한 문제되지 않는다. 이 경우는 방문한 인터넷 사이트나 전화통화에 관한 정보는 인터넷 통신업자(Provider)의 서버에도 대부분 저장되어 있기 때문이다. 반면에 온라인 수색의 대상이 당사자의 컴퓨터, 특히 하드디스크인 경우는 해킹에 의하여 기본권이 침해되는지를 의식하지 못한 채 수색을 당하게 된다. 국가기관은 소프트웨어를 심어 둠으로써 꺼져 있는 국민의 컴퓨터의 시스템에 접근하고 정보를 전송하게 할 수 있다.[27]

(나) 전략적 해킹

해킹은 반대로 사용되는 목적의 정당성에 따라 사람을 살리거나 위험을 축소하며, 테러를 사전에 방지하기도 하고, 테러의 위험이나 장애를 축소시키는데 사용될 수도 있다. 이러한 정당한 목적의 해킹[28]을 '전략적 해킹'(Tactical Hacking)이라고 한다.[29]

전략적 해킹으로 예를 들면 인질극이 벌어지는 상황에서 현장의 전화기가 꺼진 상황이라고 하더라도 와이파이를 통해 범인이 두려움에 처해 있는지, 항복하기를 원하는지, 언제 어떻게 폭탄을 감행하려고 하는지 등에 대한 범죄 상황 정보를 정확하게 실시간으로 파악할 수 있다.[30] 따라서 이러한 정확한 정보를 바탕으로 위험의 변화에 대응하면서 탄력적인 행정을 수행할 수 있게 된다.

25) 박재윤, 사이버안보의 복합적 특성과 국가사이버안보기본법(안)에 관한 토론문, in 국가사이버안보법제의 제정필요성과 법적 쟁점, 한국행정법학회 등 공동학술대회, 2016.10, 71면; 성봉근. 앞의 논문 (주 15), 1062면.
26) Kugelmann, a.a.O., (Fn 16), § 7, Rn. 190.
27) Kugelmann, a.a.O., (Fn 16), § 7, Rn. 188.
28) Neithercutt, *Id.* (Fn. 1), at 7.
29) Neithercutt, *Id.* (Fn. 1), at 8.
30) Neithercutt, *Id.* (Fn. 1), at 10.

온라인 수색과 유사하지만, 목적의 정당성이나 적법절차의 원칙, 법률유보 등을 엄격하게 충족하는 국가 해킹 기술이므로 엄밀하게는 구별이 될 수 있다. 그러나 이러한 요건들을 어기게 된다면 위법한 온라인 수색과 다를 바가 없게 되는 매우 위험한 기술이므로 신중한 주의를 요한다. 니더커트(Neithercutt)는 이러한 전략적 해킹이 조지 오웰의 '빅 브러더'(Big Brother)에 비유될 만한 기술이라고 한다.[31]

3. 외부적 유형과 내부적 유형 분류

(1) 외부적인 침해 유형

해킹을 당하는 조직 내부나 사회 내부와 외부를 구별할 때, 사이버 안전에 대한 침해 행위의 주체와 행위가 외부에서 발생하는 경우이다. 해커에 의한 침해, 기업에 의한 침해, 국가에 의한 침해 등 사이버 안전의 침해에 대한 대부분의 경우는 외부적인 침해에 해당한다.

(2) 내부적인 침해 유형

1) 내부 구성원의 고의・과실에 의한 경우

기업은 고객의 정보를 엄격하게 관리하는 비용을 충분히 지불하기 보다는 절감하기 위하여 높은 수준의 보안에 대한 투자를 제대로 하지 않는다.

해킹은 아무리 외부적인 방화벽이나 보안기술이 높은 수준으로 구비된다고 하더라도 내부 구성원의 부주의한 심리와 행동이 결합되면, 사이버 안전은 도저히 확보할 수 없다. 내부적으로 현대캐피탈 해킹 사건에서 보듯이 첫째 아이디와 비밀번호 관리에 대한 주의의무 준수, 둘째, 보안시스템 관리를 위한 해킹 방지・차단・통보 등 각종 주의의무 준수, 셋째 해킹 프로그램 업로드 필터링과 차단 등의 주의의무, 넷째, 데이터 베이스에 있는 정보는 물론 로그파일 등에 남아 있는 정보 등에 이르기까지 정보 암호화 실시에 대한 주의의무 등[32]이 내부적으로 제대로 준수되어야 한다.

최근에는 SQL 인젝션 공격이나 크로스 사이트 스크립팅(XSS) 공격 등[33]에서 보듯이, 웹이나 어플리케이션 개발자의 부주의로 해킹을 용이하게 하는 경우들도 늘어나고 있다.

2) 담당 공무원의 고의・과실에 의한 경우

고객정보 유출사건들의 발단이 정보를 보관하는 각종 공공기관 공무원들의 고의나 과실에 의하여 해킹이 용이하게 이루어지기도 한다.

---

31) Neithercutt, *Id.* (Fn. 1), at 7.

32) http://navercast.naver.com/contents.nhn?rid=2871&contents_id=83992 최종 방문일 2016.10.9.

33) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19.; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

3) 시민의 고의・과실에 의한 경우

보이스 피싱(Voice Phishing)이나 스미싱(smishing) 등 전통적인 해킹 기법, 그리고 자료실에서 자주 발생하는 파일 업로드(File Upload)나 인증 우회 등 웹 해킹 등에서 시민인 사용자(User)에 의한 고의・과실로 해킹이 용이하게 일어나는 경우도 많다. 그러나 최근에는 파밍(Pharming)처럼 사용자가 아무리 주의를 해도 해킹을 당하여 금융피해로 이어지는 경우들이 발생하고 있다.

(3) 결합된 유형

가해자인 해킹 세력에 의하여 순수하게 외부적이고 기술적인 요인으로만 발생하는 유형들도 있다. 그러나 최근 해킹들은 내부적으로 담당하는 관리자나 사용자의 고의・과실과 결합하여 발생하는 유형들이 더욱 많아지고 있다. 따라서 이에 대한 종합적인 접근을 하지 않으면 안 된다.

4. 해킹의 기술적 방법에 의한 유형

(1) 각종 서비스 공격 유형

1) D DOS공격

먼저 DDoS 공격에 대하여 전자정부는 국가와 사회 및 시민들의 안전을 방어해 낼 수 있는 시스템과 정보통신기술 및 법적 장치들을 보유하고 있어야 한다. 디도스(DDoS ; Distributed Denial of Service)는 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부 공격(Denial of Service attack ; DoS)'을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것이다.[34]

최근에 '농협 DDoS 공격 사례'가 발생하여 은행고객들의 각종 자료와 내용이 해킹당하고 농협의 서버가 파괴당하는 일이 발생하였는데, 전자정부차원의 대책들이 깊이 있게 논의하게 되는 계기가 되었다.[35] '현대캐피탈 고객정보 유출사건' 역시 사회적인 반향을 크게 불러 일으켰다.[36] 독일에서도 최근 우리나라의 현대캐피탈 고객정보유출사건과 매우 유사한 '뒤셀도르프 디도스 공격 사건'사례가 판례에 의해 등장하고 있다.[37] 독일의 뒤셀

34) http://terms.naver.com/entry.nhn?docId=68779&cid=43667&categoryId=43667 최종 방문일 2016.10.29.

35) 동아일보,2011.01.18 사건의 구체적인 경과와 피해 및 보상 유형에 대하여는 http://blog.naver.com/saxobank?Redirect=Log&logNo=80187444159

36) 2011년 4월 현대캐피탈 서버를 해킹해 빼낸 개인정보로 거액을 요구한 해킹범이 검찰에 구속 기소됐다. 2011년 4월 14일 서울중앙지검은 현대캐피탈 서버를 해킹해 개인정보를 빼돌린 혐의를 적용하여 '정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반'으로 기소하였다. 스포츠서울,2013.01.14 기사; 지디넷, 2013.01.14 기사 ; 아이뉴스, 2013.01.14 기사 등

37) LG Düsseldorf, Urteil vom 22.3.2011 – 3 KLs 1/11; 박희영, DDoS 공격은 공갈죄 및 컴퓨터업무방해죄에 해당, 독일 막스 플랑크 국제 형법 연구소 연구원, 최신 독일 판례 연구, 로앤비(www.lawnb.com),

도로프 지방법원[38]은 이 사건의 DDoS공격은 공갈죄 및 컴퓨터 업무방해죄에 해당한다고 판시하였다.(DDoSAttacken als Erpressung und Computersabotage)[39]

2) 악성코드 공격

최근에는 로마보병 선봉부대 HASTATI 악성코드와 APT 등 '악성코드'공격사례가 역시 사회적인 주목을 받았다.[40] 2013년 3월 20일 주요 방송사·금융기관에 대한 대규모 해킹 사건이 발생하였는데, 이는 디도스(DDoS·분산 서비스 거부) 공격보다 한층 진화한 최신 수법을 사용한 것이다. 이러한 로마군 보병대 악성코드와 같은 경우는 해킹 피해가 발생하여 장해가 있는 경우라도 제2차 해킹, 제3차 해킹 등의 위험이 병존하게 된다. 따라서 행정청은 이미 발생한 장해제거의무와 앞으로 발생하게 될 위험에 대비한 개입의무가 동시에 발생한다.[41]

3) 보이스 피싱, 스미싱, 파밍 등

최근 우리 사회구성원들이나 주변 지인들 중 누구나가 한두 번은 경험하였을 수 있을 정도로 보이스 피싱 사례도 빈번하게 발생하고 있다.

'보이스 피싱'(Voice Phishing)은 전화를 통하여 신용카드 번호 등의 개인정보를 알아낸 뒤 이를 범죄에 이용하는 전화금융사기 수법을 말한다.[42] '스미싱'(smishing)은 다수인에게 핸드폰의 문자메시지를 이용하여 핸드폰에서 트로이목마를 주입하는 해킹 기법인데 맥아피가 'SMS + Phishing'이라고 분석하여 호칭하였다. 해커가 핸드폰 사용자에게 웹사이트 링크를 포함한 문자메시지를 보내는데, 휴대폰 사용자가 이를 클릭하여 접속하면 트로이목마를 주입해 인터넷으로 휴대폰을 통제하고, 이차적으로 금융사기를 유발한다.[43]

'파밍'(Pharming)은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인 네임 시스템(DNS) 또는 프락시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤에 개인정보를 훔치는 새로운 컴퓨터 범죄 수법을 말한다.[44] 최근 파밍에 대한 독일 판례[45]가 등장하여 전자정부의 운영방안에 대한 공법적

2012.1, http://academy.lawnb.com.oca.korea.ac.kr/lawinfo/link_view.asp?CID=C0E7D845FD2A48F0948841E2E0D560D4|대상판결문 최종 방문일 2017.1.30.

38) LG Düsseldorf, Urteil vom 22.3.2011 3 KLs 1/11.

39) LG Düsseldorf, Urteil vom 22.3.2011 3 KLs 1/11; Tenor "Der Angeklagte wird wegen gewerbsmäßiger Erpressung in Tateinheit mit Computersabotage in sechs Fällen, wobei es bei der Erpressung in drei Fällen beim Versuch blieb, und wegen versuchter gewerbsmäßiger Erpressung zu einer Gesamtfreiheitsstrafe von zwei Jahren und zehn Monaten verurteilt. Er hat die Kosten des Verfahrens und seine notwendigen Auslagen zu tragen.

40) 조선일보, 2013.03.21 전자정부의 정보보호를 위하여는 법적 지식과 과학적인 지식이 결합되어야 하므로 공격의 구조를 이해하기 위하여 소개한다.

41) Kugelmann, a.a.O., (Fn 16), § 5, Rn. 107.

42) 두산백과, 네이버 지식백과

43) 박대우, 서정만, 박대우, 서정만, Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해방지 연구, 한국 컴퓨터정보학회 논문집 2007.5, 174면.

접근방식을 제시해 주고 있어 논의하기로 한다. 독일연방법원은 파밍에 대하여 은행 측의 손해배상책임이 없다고 판시하였다. 참고로 아직 독일은 우리나라 보다 인터넷 뱅킹과 그 보안 시스템이 잘 발달되어 있지 못하다는 점을 전제하여 이 판결에 접근하여야 한다.[46]

그럼에도 불구하고 독일의 판례는 디지털 격차를 겪고 있는 다수의 피해 국민들이 정보통신기술의 발전에 잘 적응하지 못하고 미처 익숙하지 못하다는 점과 정보력 및 기술력의 불평등한 격차와 구조를 간과하고 있다고 생각한다. 은행과 해커는 압도적인 기술력과 정보력을 가지고 있는 반면에 피해자는 그렇지 못하므로 행정사법의 원리를 적용하여 사적 자치를 수정하고 실질적인 평등의 관점에서 판결하였어야만 한다고 생각한다. 나아가서 입법론으로 전자정부에 부합하도록 이러한 파밍이나 스미싱 등 피해자보호조항이나 은행 측의 주의의무에 대한 조항, 그리고 전자정부가 행정개입을 하여 피해방지를 위한 보안에 대한 사회안전망 구축의무 등을 입법하여야 한다고 생각한다. [47]

(2) 웹 해킹

웹 해킹은 많이 사용되고 있는 운영체제 또는 응용 프로그램을 이용하여 효과적으로 해킹하는 기법이다. 이에는 다음과 같은 다양한 방법과 기술들이 발전하고 있다.

① 파일 업로드(File Upload)는 공격자가 공격 프로그램을 해당 시스템에 업로드하여 공격하는 방법이다.[48] ② 디렉터리 탐색(Directory Traversal)은 웹브라우저에서 확인 가능한 경로의 상위로 올라가서 특정 시스템 파일을 다운로드하는 공격 방법이다.[49] ③ 디렉터리 리스팅(Directory Listing)은 웹브라우저에서 웹서버의 특정 디렉터리를 열면 그 디렉터리에 있는 모든 파일과 디렉터리 목록이 나열되는 것을 이용하여 행하는 공격 방법이다.[50] ④ 인증 우회는 관리자 페이지나 인증이 필요한 페이지의 인증을 처리하지 않고 인증을 우회하여 접속할 수 있는 취약점을 이용하는 해킹을 말한다.[51] ⑤ SQL 인젝션 공격

44) 두산백과

45) BGH, Urteil vom24.4. 2012 －XI ZR 96/11 (LG Düsseldorf), “Pharming-Opfer selbst schuld, nicht Bank Urteil” Ein Bankkunde, der im OnlineBanking Opfer eines PharmingAngriffs wird, handelt fahrlässig, wenn er beim LogInVorgang trotz ausdrücklichen Warnhinweises gleiczeitig zehn TAN eingibt.”

46) 따라서 우리나라처럼 기업과 시민사이의 법률관계(B2C)에 있어서 인터넷 뱅킹이나 공인인증시스템이 발달되어 있는 경우에는 은행의 책임이 일정 비율로 인정되도록 판결하는 것이 바람직하고 오히려 가능하다고 생각한다.

47) *See Also* 박희영, 인터넷금융사기파밍피해자의 과실에 대해서 은행은 책임 없음, 최신독일판례연구, 로앤비(www.lawnb.com), 2013. 1, 10면 이하. 다소 입장의 차이는 있지만 본 논문과 동지로 볼 수 있다.

48) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

49) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19.; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

50) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19.; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

은 웹 애플리케이션을 개발하는 과정에서 간과하는 실수를 이용하여 아이디와 비밀번호를 정상적인 문자가 아닌 특정 SQL문을 넣어 공격하는 해킹 기술이다.[52] ⑥ 크로스 사이트 스크립팅(XSS) 공격은 XSS 취약점이 존재하는 웹사이트에 악의적인 스크립트를 업로드하고, 일반 사용자의 컴퓨터에 전달하여 실행시킴으로써 사용자 쿠키를 훔쳐서 해당 사용자 권한으로 로그인하거나 브라우저를 제어한다.[53]

(3) 시스템 해킹

시스템 해킹이란 시스템에 권한이 없는 사용자가 시스템을 공격하여 시스템의 서비스를 방해하거나 정보를 빼내는 공격 기술이다. 시스템 해킹의 종류로는 패스워드 크래킹(Password Cracking), 백도어(Backdoor), NETBIOS 공격, 키로거(Keylogger), 버퍼 오버플로(Buffer overflow), 레이스 컨디션(Race Condition), SetUID 등 다양하게 발전되어 오고 있다.[54] 전술한 바와 같이 독일연방헌법재판소는 '온라인수색판결[55]'을 통하여 정보의 '시스템'에 대한 무결성과 기밀성에 대한 'IT 기본권'을 인정하는 판시를 하고 있듯이 시스템 해킹에 대한 제어가 매우 중요한 의미를 가지고 있다.

5. 해킹의 내용에 의한 유형

(1) 목적의 정당성에 의한 침해의 유형

협의의 해킹처럼 기술적으로 방어막을 뚫기 위한 것으로서 가치중립적인 침해가 있다. 크래킹에서 보듯이 정보의 탈취를 이용하여 각종 재산적 이득을 얻거나 정치적·사회적 타격을 주기 위한 침해 유형이 있다. 온라인 수색 (Online-Durchsuchung)에서처럼 국가에 의하여 적법절차를 회피하면서 각종 수사자료를 확보하려는 위법한 침해 유형도 있다. 반면에 전략적 해킹(Tactical Hacking)[56]처럼 테러로부터 시민들을 보호하거나 범죄 피해를 축소하거나 범죄의 발생을 방지하기 위한 유형도 있다. 정당한 목적을 가진 침해 유형이라도 위법성이 조각되기 위해서는 공익과 사익 사이의 엄격한 이익형량과 관련 절차의 준수가 필요하다.

---

51) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19.; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

52) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

53) http://terms.naver.com/entry.nhn?docId=3432523&cid=58445&categoryId=58445 최종 방문일 2016.10.19.; 최신 웹 해킹 기법과 보안 대책, 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

54) http://terms.naver.com/entry.nhn?docId=3432462&cid=58445&categoryId=58445 최종 방문일 2016.10.1; 최신 웹 해킹 기법과 보안 대책 , 훤히 보이는 정보보호, 한국전자통신연구원(ETRI), 전자신문사, 2008. 11.

55) BVerfG, 1BvR 370/07 vom 28.2, 2008

56) Neithercutt, *Id.* (Fn. 1), at 7.

(2) 목적의 직접성에 의한 침해의 유형

정보 획득 자체가 침해의 목적인 유형이 있다. 반면에 정보의 획득을 매개로 2차적인 목적을 의도하는 간접목적의 유형이 증가하고 있다. 금융상의 사기나 테러 등을 위한 정보의 획득이 이러한 유형에 해당할 것이다.

(3) 침해의 영역에 의한 유형

침해되는 대상 정보의 분야별 유형화도 가능하다. 금융 분야에 대한 침해, 생명·신체의 안전에 대한 침해, 의료분야에 대한 침해, 기업의 영업비밀 분야에 대한 침해, 정치분야에 대한 침해, 명예 훼손이나 신용 훼손 등을 위한 침해, 사회 기간시설의 안전, 국가안전보장 등에 대한 침해 등등 다양하게 분류할 수 있다.

(4) 침해 대상이 되는 정보의 형태에 의한 유형

해킹의 대상이 되는 정보가 문서로 되어 있는 유형은 물론이고 페이스 북이나 카카오톡 등 SNS에서의 대화나 정보를 대상으로 하는 유형, 대화를 녹음한 음성파일을 대상으로 하는 유형, 각종 동영상을 대상으로 하는 유형, 컴퓨터 언어로 덮여진 코드에 대한 침해, 시스템 자체에 대한 침해 유형 등 다양하게 존재한다.

Ⅳ. 해킹에 대한 법령

1. 외국의 법령들

(1) 행정법 분야의 법률

독일 연방헌법재판소는 최근 인간의 존엄성, 인격권, 통신의 자유, 직업선택의 자유 등으로부터 국민들에게 정보기술시스템상의 보안이 유지되어야 한다는 '기밀성'(機密性; Vertraulichkeit, Confidentiality)과 정보의 내용이 변경되지 않아야 한다는 '무결성'(無缺性; Integrität, Integrity) 등이 기본권[57]으로서 보장된다고 선언하였다.[58]

개정된 독일 행정절차법 제3조 a 제2항에서는 전자문서의 등가성을 위해서는 전자서명법에 의해 인정되는 전자서명이 수반되어야 한다고 보안성(保安性; Security)에 대한 규정을 입법하고 있다.[59] 전자서명에 의하여 권한 없이 전자문서에 접근하고 훼손하게 될 위험을 방지할 수 있게 되기 때문이다.

57) Kugelmann, a.a.O., (Fn 16), § 7, Rn. 190.
58) BVerfGE 120, 274 (315 f.)
59) Skrobotz, Das elektronische Verwaltungsverfahren, Duncker & Humblot, Berlin, Band 14, 2005. S. 66.

일반법으로서 독일 「IT 안보법」(IT-Sicherheitsgesetz, IT Security Law)[60]이 최근 입법되어 시스템의 안보기준을 상향시키고 각종 시스템 안보 조치에 대한 입법이 이루어지게 되었다. 이로 인하여 '시스템에 대한 해킹'으로부터 방어할 수 있게 되었다. 최근 독일연방헌법재판소는 '온라인수색판결[61]'에서 정보의 '시스템'에 대한 'IT 기본권'을 인정하는 판시를 한 것이 배경으로 구체적인 입법이 이루어진 것이다.

개별법으로서 독일 연방 「전기통신법」(Telekommunikationsgesetz)[62]도 사이버 안보에 대한 관련 규정을 추가하고 있다. 독일 연방 「텔레미디어법」(Telemediengesetz, TMG)은 서비스 제공자들과 국가 등의 책임(Verantwortlichkeit)을 강조하여 규정하고 있다.[63] 해킹이 가능하도록 한 악성코드 등을 탑재한 인터넷상의 콘텐츠는 콘텐츠를 작성하여 올리는 사람인 콘텐츠 프로바이더(Content Provider)가 우선적으로 위험제거에 대한 행위책임이 있다. 그러나 인터넷접속서비스업자(Internet Access Service Provider)는 원칙적으로 책임을 부담하지 않지만, 예외적으로 서비스 제공법자가 해킹과 관련된 위법내용을 알 수 있고, 이를 차단하는 것이 기술적으로 가능하다면, 서비스 제공업자도 해킹과 관련된 상태책임자가 될 수도 있다.[64] 행정청이나 사인이 해킹과 관련된 위법한 내용을 지적하였을 때에는 서비스제공업자라도 웹사이트를 자발적으로 차단하는 자율규제를 하여야 한다.[65]

독일 연방 「정보보호법」(BDSG, Bundesdatenschutzgesetz)[66]은 개인정보를 보호하기 위하여 요건을 엄격하게 규정하고 있다. 동법은 정보자기결정권(Informationelle Selbstbestimmungsrechts)을 보장하기 위한 중심이 되는 대표적인 규범으로 평가된다.[67] 해킹 방지라는 공익이 크다고 하더라도 함부로 정보자기결정권을 침해할 수 없으며, 예외적인 침해의 경우에도 엄격한 이익형량이 요구된다는 점을 유념하도록 하는 입법이라고 할 것이다.

프랑스의 라리유(Larrieu)에 의하면 정보접근과 관련하여 '옵트인'(opt-in) 방식과 '옵트아웃'(opt-out) 방식 등 두 가지가 강구된다.[68] 해킹의 방지, 정보통신기술의 발전, 개인의 자기정보결정권 등에 대한 조화로운 접근을 위해서는 원칙적으로는 옵트인 방식을 취하되, 엄격한 이익형량하에 예외적으로 옵트아웃 방식을 허용하여야 할 것이다.

독일의 「에너지 산업법」(Energiewirtschaftsgesetz)[69]은 최근 에너지발전시설의 네트워

60) https://dejure.org/BGBl/2015/BGBl._I_S._1324 최종 방문일 2016.11.26.
61) BVerfG, 1BvR 370/07 vom 28.2, 2008
62) https://dejure.org/gesetze/TKG/111.html 최종 방문일 2016.11.27.
63) https://dejure.org/gesetze/TMG 최종 방문일 2016.11.27.
64) 서정범・박병욱, 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015년, 295면.
65) 성봉근, 앞의 논문 (주 3), 239면.
66) https://dejure.org/cgi-bin/suche?Suchenach=bdsg+sicher#Treffer 최종 방문일 2016.11.27.
67) Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011, S. 415.
68) Larrieu, Droit de I'nternet, ellipses, 2e édition, 2010, 189 p.
69) https://dejure.org/gesetze/EnWG/11.html 최종 방문일 2016.11.27.

킹 안보에 대한 입법을 하여 해킹 등에 의한 산업시설망에 대한 공격에 대비하고 있다. 동 법의 특징은 보장국가의 보장책임에 입각하여 국가와 민간의 책임을 분할 및 분담하여[70] 에너지 망을 운영하는 자들에 대한 책임과 과제도 함께 규정하고 있다.

(2) 해킹 방지를 위한 인접 분야의 법령

독일의 경우는 최근 '정보 해킹죄'를 구성요건으로 연방『형법』에서 ①제202조 a의 '데이터 감시죄'(Ausspähen von Daten, Spying out data)와 ② 제202조 b의 '데이터 가로채기죄'(§ Abfangen von Daten, Interception of data), ③ 제202조 c의 '데이터 감시 및 가로채기 예비죄'(§ 202c Vorbereiten des Ausspähens und Abfangens von Daten)[71]를 신설하여[72] 사이버 안보를 해치는 경우에 대비하고 있다.

「형법」 제149조에서 '컴퓨터 사기죄'(Vorbereitung der Fälschung von Geld und Wertzeichen)를 두어 보이스 피싱 등을 처벌하고[73], 제303조 b에서 '컴퓨터 업무방해죄'(Computersabotage, 컴퓨터 작동마비죄)[74]를 입법하여 타인에게 중요한 의미를 가지는 정보처리업무를 방해하는 자에 대한 처벌하는 규정을 두고 있다.

그러나 형사처벌로는 효과가 미미하며, 해외에 서버를 두고 있는 경우 형사처벌이 어렵다는 한계를 여전히 가지고 있다. 따라서 사이버 안보에 대한 행정법적 정비를 해 나가는 것이 가장 효과적인 입법 방식이라고 생각한다.

개정된 독일 연방 민법전(BGB) 제126조 a에서도 등가성을 인정받기 위한 요건으로서 전자서명법에 따라 인증된 전자서명과 표의자의 명의가 제공되어야 한다고 요구하고 있다. 사이버 안보의 기본적인 전제는 전자서명을 통한 보안성의 확보에 있다는 것을 인식하여 민사거래의 일반법인 민법전에 이를 규정하고 있다.[75]

2. 우리의 법령

(1) 기존에 활용하던 법률

「형법」의 업무방해죄, 비밀침해죄, 컴퓨터사기죄 등이 있고 이를 활용하는 방식이다. 또한 「전기통신사업법」도 마찬가지이다. 그러나 이러한 전통적인 법률들로 무리하게 구성요건에 적용하려고만 든다면 전자정부에서 등장하는 변형되고 우회적인 해킹들에 대하여 죄

70) 성봉근, 앞의 논문 (주 3), 235면.
71) https://dejure.org/gesetze/StGB/202c.html 최종 방문일 2016.11.27.
72) https://dejure.org/gesetze/StGB/202b.html 최종 방문일 2016.11.27.
73) https://dejure.org/gesetze/StGB/149.html 최종 방문일 2016.12.4.
74) https://dejure.org/gesetze/StGB/303b.html 최종 방문일 2016.11.27.
75) 우리의 경우 기본법인 민법에서 등가성에 대한 규정이 흠결된 채, 개별법에서 등가성에 대한 규정을 두는 경우들이 있어 입법체계상 문제가 있다. 성봉근, 앞의 논문 (주 22) 45면.

형법정주의에 어긋나는 무리한 적용이 될 위험이 있다. 특히 정보통신망으로 볼 수 없는 블루투스에 대한 침해 등을 처벌할 수 없다면 이는 입법의 공백에 해당한다.

또한 해킹의 경우 서버를 해외에 두면서 자주 이동을 시키며, 해킹에 대한 교묘한 조직 운영 등으로 인하여 형사제재의 실효성이 매우 떨어지게 된다.

따라서 새로운 입법수단과 해킹 제어 수단들을 연구하여야 한다. 이행강제금, 과징금, 몰수, 과태료, 각종 허가 취소·철회, 신용제한, 금융거래 제한, 명단공표 등 다양한 수단들을 강구하여야 한다.

(2) 전자정부에서 구축된 법률들

「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 등 새로운 입법을 통하여 규율하려는 것이다. 동법은 개인정보의 수집과 이용에 대하여는 사전동의를 받아야 한다고 옵트인 (opt-in) 방식의 입법을 취하고 있다. 동법에서는 정보통신서비스 제공자는 해당 서비스를 이용하기 위하여 이용자(User)의 이동통신 단말장치 내에 저장되어 있는 정보 및 동 장치에 의하여 설치된 기능에 대하여 접근권한이 필요한 경우에는 명확하게 설명하고, 사전동의를 받도록 의무를 신설하고 있다. 특히 동법에서 이용자가 이에 동의하지 않는다고 하여 이용자에게 해당 서비스의 제공을 거부할 수 없도록 하여 실질적인 이용강제를 방지하는 규정을 신설하고 있어 의미가 있다. 또한 정보통신서비스 제공자에게 이용자의 사상, 신념, 가족 및 친인척 관계, 학력, 병력, 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집할 수 없도록 금지의무를 설정하고 있다.

특히 유럽이나 미국에는 없는 '주민등록번호제도'를 실시하는 우리나라에서는 개인정보에 대한 해킹에 따른 침해의 위험과 피해 정도가 매우 크다.

다만, 동법에서 정보통신서비스 제공자에게 인구조사판결에서 확인된 목적구속성의 원칙을 규정하고 있다는 점에서 큰 의미가 있다. 또한 정보통신서비스 제공자에게 옵트인(opt-in)원칙을 취하고 있다.

그러나 전통적인 정부에서 구축되고 활용되는 법률들과 차이점에 대하여는 명확하지가 않아서 이에 대한 연구가 보다 필요하다. 입법의 공백은 역시 마찬가지의 고민이다.

그밖에도 전자거래에서 전자서명[76]을 필수요건으로 하게 하여 해킹을 방지하고 방어하려는 규율을 시도하고 있다. 「전자서명법」에서도 해킹을 방지하기 위하여 다양한 제어업무와 위임에 대한 규정을 두고 있다.[77] 인증업무에 대하여 제어기구의 설치 및 위임 등에 대하여도 규정하고 있다.

해킹과 관련된 보안성을 극복하고 장점을 살려서 정보화 사회와 전자정부에서 소통의

76) Hinkel, Practical Real Estate Law, Delmar, 2011, at 179.
77) 현대호, 전자거래입법의 문제점과 개선방안, 한국법제연구원, 2002, 39면.

수단으로 안정적으로 인정받기 위해서는 전자서명의 요건을 강화하여야 한다. 다만, 전자서명에 대하여 기술적인 의존성이 심화되어 가는 문제는 좀 더 입법적으로 고민하여야 보아야 한다.

전자 안전거래 시스템을 지속적으로 개발하고 보안해 나가야 한다.[78] 전자인증과 전자서명의 수준과 기술을 담보하도록 전자거래시장의 특성을 고려한 제어행정이 이루어져야 한다.[79] 대법원도 해킹 등에 의한 재산권 침해의 위험과 부실등기의 방지를 위한 제어행정을 수행하기 위한 서비스를 수행하려고 노력하고 있다.[80]

Ⅴ. 제어국가에서 해킹 제어와 방식

1. 제어국가의 의의

국가와 민간이 공동으로 국민에 대한 급부를 책임지는 '보장국가'(保障國家; Gewährleistungsstaat, Garantie Staat; Guarantee State, Ensuring State)가 최근 행정개혁의 국가관으로 확대 등장하고 있다. 동시에 이를 배경으로 시장과의 거리에 따라 제어하는 형태로 구현하는 '제어국가'(Steuerungsstaat; Steering State)가 새로운 규제 패러다임의 배경이 되고 있다.[81]

과연 보이스피싱, 스팸과 악성 코드 및 각종 해킹 등으로부터 보호받기 위해서 시민들은 정부의 개입과 행정 통제를 필요로 하는가? 사이버 안전을 효과적으로 달성하기 위하여 정부가 규제를 통하여 개입하는 것을 원칙으로 하여야 한다는 논리가 있다. 피구(Pigou)는 정부에 의하여 부과되는 정책규제에 크게 의지하여야 한다고 본다.[82]

반대로 사이버 안전 역시도 시장의 자율성을 존중하여 정부가 비개입하는 것이 타당하다는 논리가 있다. 경제학자인 코즈(Coase)는 사이버 안전을 강화하기 위한 정부의 개입과 행정통제에 대하여 회의적이며, 시장의 보이지 않는 손(Invisible Hand)에 맡기는 것이 오히려 효과적이라고 한다.[83]

서로 상충되는 논리 중 어떠한 것이 사이버 안보를 향상시키면서 프라이버시를 잘 보호할 수 있는 길인가 고민하지 않을 수 없다. 사이버 상에서 정부의 규제는 오프라인상에서의 행정규제와 달리 충분한 효과를 발휘할 수 없으며, 국경을 초월하거나 단속이 사실상

78) 조춘만・정문섭, 공간정보기반 부동산거래선진화시스템 구축방안, 한국공간정보학회지, 제21권 제6호, 2013 74면.
79) 정영화, 전자상거래법, 제2판, 다산출판사, 2001, 173면, 175면.
80) 김상철/양은상, 부동산 등기제도의 개선 방안에 관한 연구, 대법원 사법정책연구원, 2015, 61면.
81) 제어국가의 구체적인 논의에 대하여는 성봉근, 앞의 논문 (주 3), 234-234면.
82) Spinello, Cyberethics - Morality and Law in Cyberspace, 5th Edition, Jones & Barlett Learning, LLC, an Ascend Learning Company, 2014, at 45.
83) Spinello, *Id.* (Fn. 82), at 44.

불가능한 경우도 많다. 84)사이버 세계의 특성상 정부의 힘이 미치는 범위와 효과는 매우 축소될 수밖에 없다.

그렇다고 하여 철저하게 방치하게 되면 사이버 안전을 담당하는 기업들의 권력은 비대하여 지게 될 것이고, 사이버 안전을 담보로 시민들에게 지나치게 높은 비용을 요구하게 될 것이다.

따라서 해킹에 대한 규제도 시장의 자율성을 존중하여 시장과의 '거리'(Distanz; Distance)를 멀리 두는 것을 원칙으로 하되, 시장이 자율적으로 사이버 안전을 도저히 달성할 수 없게 될 현저한 위험이 있는 경우에만 예외적으로 시장과의 거리를 좁혀서 개입을 하는 구조를 설정하는 것이 타당하다. 국가의 패러다임을 '제어국가'(Steuerungstaat; Steering State)라고 한다.85)

이러한 제어국가의 새로운 패러다임에서는 해킹과 같은 시대적인 난제에 대하여 다음과 같이 제어하고 규제하는 대안을 제시할 수 있게 된다.

2. 헌법 · 일반법 · 개별법의 체계적 입법을 통한 해킹 제어

개별적이고 수없이 산만하게 흩어져 있는 해킹 관련 법령으로는 규정의 중복과 저촉 및 모순 등으로 인하여 법을 집행하는 공무원들조차 제대로 규범을 파악하기가 어렵고 곤란하게 된다. 특히 과학기술법은 기술발전의 속도가 매우 빠르므로 개별법에서 제 각각 규정하고 있는 규범들이 현실을 충분히 따라가기가 어렵다.

미국 연방정부는 총론적인 역할을 하는 「전자정부법」(the E-Government Act of 2002을 제정하면서 비로소 개별법들과 체계적인 조화를 잘 이루게 되었다.86) 독일은 많은 어려움을 겪다가 독일 「기본법」 제91c조를 신설함으로써 헌법차원의 입법을 이루어내면서 체계적인 입법이 진행되기 시작하였다.87)

전자정부가 실패와 성공 사례들을 비교법적 관점에서 종합하면 총론주의 입법을 취하여 '체계적으로 규범구조'를 구축하는 것이 타당하다. 우리나라도 일반법인 전자정부법을 입법한 것으로 만족할 것이 아니라, 개별법과 정서하는 작업을 지속적으로 수행해 나가야 하며, 헌법을 개정할 때 전자정부에 대한 조항을 삽입할 필요가 크다.88)

---

84) Spinello, *Id.* (Fn. 82), at 45.
85) 성봉근, 앞의 논문 (주 3). 233면.
86) 한국전산원, 앞의 논문, 4면; 김도승, 앞의 논문, 44면.
87) 서보국, '독일 전자정부법 제정의 현황과 전망', 2010년도 세계법제 연구보고서, 법제처, 2010, 2면.; 성봉근, 앞의 논문 (주 20), 49면
88) 성봉근, 앞의 논문 (주 20), 48면

3. 해킹 제어에 대한 대화형 입법과 행정을 통한 해킹 제어

해킹에 대한 효과적인 제어를 위해서는 임시방편적이고 비전문적으로 개별법으로 입법을 할 것이 아니라, IT 전문가들과 행정학자 및 법학자들과 공무원들, 민간전문가들 및 사용자(User)인 일반국민들이 끊임없이 대화하면서 입법을 해 나가는 '대화형 입법 방식과 체계'가 필요하다. 의원입법이나 정부입법의 실질적 내용이 상당부분 비전문적인 경우들이 상당히 많다. 이러한 대화형 행정법을 형성해 감에 있어서 시행착오를 감안하여 지속적인 대화를 해 나가면서 법률을 보완해 나갈 수 있도록 함이 바람직하다.

정부가 일일이 사이버 안전을 담당하고 책임진다는 것은 국경을 초월하며 기술적으로 정부에 비하여 때때로 우위를 점할 정도로 발전하여 하는 사이버 세계의 특성을 간과한 비현실적인 사고이다. 따라서 '공사협동'(PPP ; Public Private Partnership)을 다양하게 활용하는 방향이 바람직하고 타당하다.[89]

해킹 제어에 있어서 사이버 안전과 관련된 보호가치들의 충돌문제를 해결하는 적법절차의 연구도 매우 중요하다. 정보주체의 참여, 기업의 참여, 일반시민의 참여 등을 어떻게 효과적으로 진행시켜 나갈 것인지에 대해 고민해 보아야 한다. 전자청문, 전자 공청회, 홈페이지나 모바일상의 토론, SNS 상의 토의, 전자투표 등등을 실질적인 사이버상의 토의수단으로 발전시킬 수 있어야 한다.

해킹을 효과적으로 처리하고 보장국가의 의무를 다하기 위하여 전자정부를 활용하는 과정에서 거치게 될 시행착오들을 고려하면서 수정해 나갈 수 있도록 '실험규정'[90](Experimentierklausel)의 입법기술을 활용할 필요가 있다.

전략적 해킹을 예외적으로 허용할 수 있게 하기 위해서는 남용되지 않도록 과학기술적인 기법에 대하여 국회에서 허용 여부와 허용 범위[91]에 대한 규정을 두어야 한다. 니더커트(Neithercutt)에 의하면 국가에 의한 전략적 해킹은 6단계로 이루어진다. 1단계로서 사전지식 수집과 SNS에 접근하는 '정보수집'(Intelligence Gathering), 2단계로서 어떻게 정보를 수집할 것인가에 대한 '모델 설정 단계'(Threat Modeling), 3단계로서 해킹의 대상의 취약점을 분석하는 단계('Vulnerability Analysis), 4단계로서 취약점을 이용하여 구체적인 방법을 개발하는 단계 (Exploitation), 5단계 전략적 해킹 등 이용 사후조치(Post Exploitation), 6단계 행정 및 사법상의 각종 보고(Reporting) 등으로 절차가 진행되게 된다. 이때 허용단계와 단계별 범위 등은 기본권의 본질적이고 중대한 침해를 수반할 수 있으므로 법률유보의 원칙상 규정을 두는 것이 필요하다. 이로써 법률유보의 원칙에 부합하고[92], 헌법에

89) 성봉근, 앞의 논문 (주 3). 248-249면.
90) 서보국, 앞의 논문, (주 88), 7면.; 성봉근, 앞의 논문 (주 20), 51면
91) Neithercutt, *Id.* (Fn. 1), at 12. 이러한 단계별 규정을 입법하는 것이 법치주의에 부합하는 방향이 될 것이다.
92) Neithercutt, *Id.* (Fn. 1), at 9.

합치하는 행정이 되도록 하여야 할 것이다.

4. 책임지는 담당기관의 구축을 통한 해킹 제어

해킹에 대하여 법적으로 책임지고 전담할 수 있는 컨트롤 타워를 실질적으로 구축하여야 한다. 컨트롤 타워는 실질적으로 해킹과 관련된 문제들을 해결하고 지시할 권한이 부여되어야 한다. 또한 해킹을 제어할 수 있는 전문성을 구비하여야 하며, 민주주의적이고 법치주의적인 절차와 과정을 수행할 수 있는 능력을 갖추어야 한다. 사전에 상시적인 시뮬레이션을 실시하고 평가하며, 이에 따라 책임을 묻고 인센티브를 줄 수 있도록 하여야 한다.

5. 해킹 방지의무의 강화를 통한 해킹 제어

해킹 같은 정보 분야의 위험의 경우에는 행정기관들이나 공무수탁사인, 담당 민간기업들에게 개인이나 중요한 기간시설, 사회안전시스템 등에 대한 정보보호의무를 강화하여야 한다. 이를 위한 입법이 이루어져 나가야 하고, 이러한 의무를 잘 준수할 수 있도록 담당 공무원들이나 담당 직원들에 대한 재교육 시스템의 구축이 필요하다.

미국의 경우 종이행정시대에서 전자행정시대로 넘어가면서 전자행정을 담당할 수 있는 공무원들을 신규로 채용하거나 재교육을 시키는 방안을 실시하였고 이에 적응하지 못하는 수많은 공무원들이 해임되었다. 행정 기관들이 정보 기술을 도입하고 사용하는 근본자세가 전통적인 정부에서 전자정부로 이전되고 있음에도 불구하고 잘 적응하지 못하는 문제가 있었다.[93]

해킹을 방지할 수 있는 최초의 단계에서 행정개입을 하는 방법으로서 사전적인 정보보호의무를 법적으로 인정하고, 이를 위한 여러 가지 정보보호방안을 강구하여야 한다. 사전에 정보보호를 위하여 국가와 지자체에게 보안체계 수립 및 유지 의무를 인정하여야 한다. 금융사기나 보이스 피싱, 전자정부가 보유하는 국민들의 개인정보유출 등을 방지하기 위한 해킹과의 전쟁 및 보안기술의 개발 및 보완의무 등이 법적으로 부과되어야 한다.

개인이나 기업체는 정보보안과 관련하여 해킹을 하는 제3자에 의한 개인정보침해의 위험이 현저한 경우 행정기관에게 사전에 행정개입으로서 보안설정과 관리[94] 및 유출방지 등을 미리 요구할 수 있게 하는 법리가 가능하다.[95]

---

93) 平野　美惠子,「米國の電子政府法」, 調査と情報 第423号, 2頁.

94) 공무원들의 증언에 의하면 삼성과 같은 기업체들도 이러한 경우에는 국정원 같은 전문적인 국가기관에게 보안유지와 관리를 위탁하고 있다고 한다. 국가와 지자체의 민간 보안체계에 대한 감시와 통제는 기본권의 대사인적 효력과 관련하여 국민의 생명, 신체, 재산 등에 대한 급박하고 중대한 위험이 발생하는 경우 행정개입을 요구할 수 있다.

95) 이러한 행정개입신청권에 의하여 사후적인 권리구제로서 의무이행심판, 부작위위법확인소송, 거부처분취소소송이나 거부처분취소심판 등이 가능하다고 생각한다.

6. 지속적인 모니터링과 보고

제어국가는 철저하게 위험에 대한 제어가 가능하여야 한다. 이를 위하여 수시로 해킹이 발생할 위험과 관련된 행위나 상황들에 대한 모니터링[96]이 이루어져야 한다. 특히 사전 보고 뿐만이 아니라 사후 보고가 제대로 이루어져서 이 보고서가 최종적으로는 법원에까지 제출될 수 있도록 하여야 한다. 예를 들면, 언제 국가에 의한 전략적 해킹이 이루어졌는지. 어떠한 방법과 경로로 이루어졌는지, 전략적 해킹을 통하여 무엇을 획득하였는지, 어떠한 행동들을 하였는지, 절차에 대한 준수가 어떻게 이루어졌는지 등에 대한 기재[97]가 이루어짐으로써 법치주의에 부합하는 행정이 되도록 하여야 한다.

7. 과학기술의 발전을 반영하는 법제도를 통한 제어

과학기술의 발전과 격차가 벌어지지 않도록 이를 법제도에 반영하는 과정들이 지속적으로 이루어져야 한다. 대표적인 예로서 해킹을 방지하는 키가 되는 전자서명을 강화하는 것을 들 수 있다. 해킹 사례들과 판결들에서 보듯이 공인인증서도 위조 및 변조가 이루어지고 보안이 해킹당하여 전자문서와 전자서명까지 위조 및 변조가 대량으로 이루어질 수 있는 위험도 동시에 존재한다. 전자서명에 대한 법제도가 잘 정비되도록 함으로써 전자상거래의 활성화, 전자투표 및 전자공청회, 전자재판, 개인정보보호 등의 진실성을 담보할 수 있게 된다.

8. 해킹에 적합한 실효성 확보수단의 정비와 강구

해킹을 발생시킨 해커들에게는 물론 기업이나 사인 및 공무원들에 대하여 적합한 실효성 확보수단들이 제대로 마련되어 있지 못하다. 해킹에 대한 위험을 야기하였더라도 처벌을 할 수 없는 법의 사각지대 안에 안전하게 도피하게 하거나, 효과 없는 제재를 가하는 경우들이 많이 발생하고 있어 근절이나 재발방지와 거리가 멀다.

특히 해킹 등 현대형 위험에 대하여 전통적인 정부(C-Gov.)에서의 민사 및 상사판결은 판결이 확정될 때까지 기간이 지나치게 장기간이고, 승소할 때에는 현대형 위험을 유발한 책임 기업이나 단체가 소멸되고 숨어버리거나 법인을 새로 설립함으로써 존재하지 않게 되는 경우들도 많으며, 행정형벌을 비롯한 형사재판은 형 집행 후의 경제적 이익이 보장되는 경우에는 효과가 거의 없다고 보아야 한다. 또한 서버폐쇄를 시킨다고 하더라도 서버를 계속 바꾸어가거나 해외에 서버를 두고 있어서 이에 대한 집행은 효과가 없다고 할 것이다.[98]

96) 성봉근, 앞의 논문 (주 15), 1062면.
97) Neithercutt, *Id.* (Fn. 1), at 12.

따라서 과징금을 활용하여 현대형 위험을 일으킨 대가로 벌어들인 불법적인 수익을 박탈하고 이를 사회안전망을 복구하는 분야로 재배분하는 방안을 적극적으로 활용할 필요가 있다고 생각한다. 또한 이러한 위험을 야기한 기업이나 사람 또는 행정기관의 이름을 대외적으로 널리 공표함으로써 이에 대한 사회적이고 국가적인 차원에서의 책임을 지도록 하는 것이 피해의 확산방지와 재발방지를 위하여 필요하다고 생각한다.

해킹 등 현대형 위험에 대한 책임이 있는 기업체에 대하여는 현대형 위험관리를 업으로 할 수 있도록 발급한 허가나 특허를 취소·철회하는 것도 한 방법이 될 수 있다.[99] 예컨대, 미래창조과학부 장관은 「전자서명법」에 의하여 공인인증기관이 지정 후 결격사유가 생기거나 인증업무기준을 위반하거나 가입자나 이용자를 불합리하게 차별하거나 신고의무를 이행하지 않거나 자료제출명령에 불응하거나 인증업무와 관련된 보안업무상의 보호조치를 하지 않거나 보험에 가입하지 않는 등의 사유가 있을 때에는 시정명령을 발급할 수 있고(제11조), 나아가 그 실효성확보수단으로서 수익적 행정행위인 공인인증업무에 대한 허가나 특허를 6월 이내에 정지하거나 전부나 일부 업무의 취소·철회를 할 수 있도록 규정하고 있다(제12조).[100]

9. 해킹 제어과정에서 발생하는 기본권 제한의 한계 설정

해킹을 사전에 인지하고 적발하기 위하여 정보를 수집하거나 정보의 공개를 제한할 때에도 독일과 우리 대법원이 판시하듯이 정보공개의 공익과 비공개의 사익 간의 이익형량에 의하여 판단하여야 한다. 즉, 공익과 사익의 충돌에 대하여는 이익형량을 조화롭게 하는 것이 필요하다.[101] 그러나 그 한계를 지나치게 강조하다 보면 전자정부에서 SNS를 통한 시민들의 표현의 자유가 과도하게 제한되고 민주주의적이고 법치주의적인 기반이 위험해 질 수 있으므로 한계설정은 최소한도로만 되어야 한다.

해킹 제어과정에서 법철학적인 대립이 숨어 있다. 해킹을 방지하고 사이버 안전을 강화하고자 하는 실용주의적인 법철학[102]에 의하여 정보의 접근을 용이하게 하고자 하게 된다. 그러나, 칸트(Kant)는 제2정언명제를 통하여 '인간을 수단이 아닌 목적으로 대하라'고 하고 있다.[103] 이러한 칸트와 자연법주의에 의하면 사이버 안전을 규율하는 법도 규범적으로 '정당한 법'(richtiges Recht)[104]이어야 한다.

98) 성봉근, 앞의 논문 (주 20), 127면
99) 다만 이 역시 법인을 수시로 설립하고 폐쇄하는 경우에도 효과가 한계에 부딪히게 된다.
100) 성봉근, 앞의 논문 (주 20), 127면
101) *See Also* 유일상, 유계환, 표현과 소통으로서의 인터넷 댓글과 그 책임에 관한 일 고찰, 언론과 법 제10권 제2호, 20011, 323면, 331면 이하;*See Also* Harmut Maurer, a.a.O., S.484 Rn.20.
102) Spinello, *Id.* (Fn. 82), at 11.
103) Spinello, *Id.* (Fn. 82), at 166.
104) 성봉근. 앞의 논문 (주 20), 36면.

특히 프라이버시가 보장될 때에 비로소 자유로운 사상의 자유, 표현의 자유, 행동의 자유, 기업의 자유 등과 평등이 실질적으로 보호될 수 있으므로,[105] 해킹을 방지하기 위한 기본권의 제한은 비례의 원칙에 부합하여야 하고 최소한도로 그쳐야 한다.

해킹 제어를 위한 각종 조치들이 민주주의의 적이 될 수 있는 또 다른 사이버 공격과 침해의 토양을 제공하지 않도록 하여야 한다. 사이버 상으로 서로 다른 관점을 교환하고 소통하는 것이 오프라인 상에서 모여서 하는 것보다 훨씬 용이하다는 점을 고려하여, 보다 적극적인 소통과 토의 마당을 열어야 할 것이다. 따라서 사이버 안전을 둘러싼 보호가치의 충돌을 해결하는 방법론으로서 하버마스 등의 대화이론을 수용하고 이를 입법과 행정 및 사법에 반영하여야 할 필요가 있다.[106]

10. 해킹에 대한 철저한 권리구제제도의 마련

국가나 국가의 위임을 받은 민간기관등은 물론 일반 민간기업 등에서 이러한 사전적인 해킹방지의무를 위반하여 국민에게 손해를 발생시킨 경우에는 사후적으로 적극적으로 국가배상이나 손실보상 등이 인정되어야 한다. 이를 용이하게 하기 위한 입법과 판례 형성이 필요하다.

기업이 해킹으로부터 고객정보의 보안을 지키기 위하여 주의의무를 충실하게 이행하지 않는 행위들이 만연해 가고 있다. 이에 대하여 국가의 행정은 관대하며 심지어 법원은 경제발전과 산업의 활성화를 고려하여 해킹 방지의무에 대한 위반에 대하여 위법성을 잘 인정하려 들지 않거나, 해킹 방지의무의 수준을 '높은 주의의무'가 아니라 '해킹 당시의 사회통념상 기대 가능한 수준'으로 완화하려 들기도 한다. 이에 따라 보안관리를 철저하게 하지 않은 기업들에게 면죄부를 줌으로써 기업들의 보안비용에 대한 투자를 소홀하게 만들기도 한다. 최근의 '옥션판결'은 이러한 면을 단적으로 보여준다. [107]

---

105) Spinello, *Id.* (Fn. 82), at 166.

106) 성봉근, 앞의 논문 (주 22), 39면.

107) 정보통신서비스제공자가 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제28조 제1항이나 정보통신서비스 이용계약에 따른 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였는지 여부를 판단함에 있어서는 '해킹 등 침해사고 당시 보편적으로 알려져 있는 정보보안의 기술 수준', 정보통신서비스제공자의 업종·영업규모와 정보통신서비스제공자가 취하고 있던 전체적인 보안조치의 내용, 정보보안에 필요한 경제적 비용 및 효용의 정도, 해킹기술의 수준과 정보보안기술의 발전 정도에 따른 피해발생의 회피 가능성, 정보통신서비스제공자가 수집한 개인정보의 내용과 개인정보의 누출로 인하여 이용자가 입게 되는 피해의 정도 등의 사정을 종합적으로 고려하여 정보통신서비스제공자가 해킹 등 침해사고 당시 사회통념상 합리적으로 기대 가능한 정도의 보호조치를 다하였는지 여부를 기준으로 판단하여야 한다. 특히 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙 제3조의3 제2항은 "정보통신부장관은 제1항 각 호의 규정에 의한 보호조치의 구체적인 기준을 정하여 고시하여야 한다."라고 규정하고 있고, 이에 따라 정보통신부장관이 마련한 「개인정보의 기술적·관리적 보호조치 기준」은 해킹 등 침해사고 당시의 기술수준 등을 고려하여 정보통신서비스제공자가 구 정보통신망법 제28조 제1항에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있으므로, 정보통신서비스제공자가 고시에서 정하고 있는 기술적·관

이러한 의무를 위반한 경우에 대비한 사후적인 권리구제로서 고의·과실이 있는 경우에는 국가배상법 제2조의 직무상의 책임을 강구하고, 고의·과실이 없는 경우라 하더라도 국가배상법 제5조의 공물의 설치·관리상의 하자에 대한 안전의무 위반 등을 재판의 법리로 삼아서 국가배상을 통한 권리구제를 강화하여야 한다. 물론 상당인관관계의 입증에 있어서는 입증책임의 전환이나 완화를 고려하여야만 한다. 해킹과 같은 경우 인과관계에 대한 입증이 무척 어렵다는 특징이 있어 이러한 배려를 하는 것이 보장국가에서 요구되는 재판의 기준이 된다. 이들을 통하여 해킹에 대한 사전적인 주의의무를 지키기 위한 투자와 노력이 원활하게 담보될 수 있다.

11. 해킹에 대한 사회보험의 강구

국가배상이나 손실보상 등에 대한 요건이 충족되지 못하는 경우에는 해킹에 대한 구제가 어렵다. 그러나 보장국가에서는 해킹에 대한 책임을 끝까지 이행하여야 한다. 따라서 사회보험의 창설 및 운영을 통해 보이스 피싱 등을 비롯한 각종 해킹으로부터 보호할 책임을 수행하는 것이 필요하다. 해킹으로 인한 피해에 대하여 피해 국민과 국가 및 사회가 손실을 분할하고 분담하는 것이 필요하다. 이를 위한 공적 부조 내지 공공보험제도의 구축이 필요하다. 해킹을 당하여 전 재산을 상실하게 될 잠재적 피해자들에 대한 사회안전망의 설치라는 의미도 가진다.

Ⅵ. 결 론

첫째, 해킹의 의의와 성격, 위험의 범위 등 해킹에 대한 '이론적인 규명'을 하여 보았다.

둘째, 제어하여야 할 해킹의 범위와 관련하여 과학기술규범의 규범력과 실효성을 유지하기 위해서는 '새로운 분류체계'의 구상이 필요하다. 이에 새로운 분류체계를 최초로 시도해 보았다.

주체별로 해커에 의한 침해뿐만 아니라 국가에 의한 침해 등으로 확장하여 검토하여야 한다. 해커에 의한 침해도 외부적인 침해와 내부적인 침해. 통상적인 침해, 웹 해킹, 시스템 해킹 등으로 다양하게 이제는 제어하여야 한다. 국가에 의한 침해도 위법한 온라인 수색 등과 적법한 전략적 해킹 등으로 분류하여 연구할 필요가 있다.

셋째. 해킹을 제어하는 '제어' 변화가 필요하다.

리적 보호조치를 다하였다면, 특별한 사정이 없는 한, 정보통신서비스제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다. 대법원 2015.2.12. 선고 2013다43994,44003 판결; 오길영, 소위 '옥션판결(대판 2013다43994, 44003)에 대한 비판과 TOM, 공법학회 정보인권연구포럼 발표문, 2016.5, 11면.

해킹을 정보화사회에서 효과적으로 제어하기 위해서는 국가기관이 일방적으로 전담하는 패러다임에서 보장국가와 제정국가의 패러다임으로 이전하여야 한다.

일방적으로 국가가 해킹을 전담하고 일방적으로 제어하려다 보면, 규범구조적인 면에서 민주주의와 헌법적 가치를 훼손하게 되는 무리한 경우들이 발생하게 된다. 실효성면에서도 온라인과 오프라인이 연결되어 있고, 국경이 의미가 없으며, 기술의 발전이 국가수준을 종종 초월하는 사이버 세계에서 국가에게 큰 부담이 될 뿐만 아니라 성과를 확보할 수 없다,

최근의 세계적인 흐름에 따라 국가는 사인들과 협력하여 공동으로 해킹 제어에 대한 책임을 분담하여야 한다. 시장의 자율규제를 활용하기도 하고, 규제된 자기규제를 활용하는 등의 약한 규제 방식을 취하기도 하고, 때로는 국가가 직접 개입하여 강하게 규제하는 방식을 취하는 등의 다양한 제어방식으로 접근하여야 한다.

넷째, 해킹을 규제하는 법령들을 검토하여 보았다.

독일을 위주로 유럽에서의 해킹을 제어하기 위한 법령들을 살펴보았다. 헌법적 차원의 독일기본법, 일반법인 개정 독일 「행정절차법」, 독일 「IT 안보법」을 분석하였다. 개별법으로서 독일 연방 「전기통신법」, 독일 연방 「텔레미디어법」, 독일 연방 「정보보호법」, 독일의 「에너지 산업법」 등도 검토하였다. 인접 분야의 법령으로서 독일 「형법」과 독일 연방 「민법전(BGB)」 등도 살펴보았다.

우리의 법령으로서 「형법」, 「전기통신사업법」, 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 등을 검토하였다.

다섯째. 다양한 제어국가에서의 해킹 제어를 위한 방안들을 살펴 보았다.

구체적으로는 헌법·일반법·개별법의 체계적 입법을 하여 해킹에 대한 입법적 제어가 필요하다. 입법은 물론 행정에 있어서도 일방적으로 해킹을 처벌하고 규제하는 패러다임보다는 대화형 입법과 행정을 통한 해킹 제어가 바람직하다. 해킹에 대하여 책임지는 담당기관의 구축을 하여야 한다. 해킹 방지의무를 국가기관과 사회 및 기업체, 시민들에 대하여 전반적으로 강화하는 것이 필요하다. 제어국가에서 시장과의 자율성을 존중하면서도 해킹의 위험을 감소시키기 위해서는 지속적인 모니터링을 하고 보고체계를 갖추는 것이 필요하다. 과학기술규범의 특성상 과학기술의 발전을 반영하는 법제도를 정비해 나가야 한다. 해킹에 적합한 실효성 확보수단을 정비하고 강구하여야 한다. 그러나, 해킹 제어과정에서 발생할 수 있는 기본권 제한의 한계를 설정하고 조화되도록 하여야 한다. 해킹 피해를 개인의 문제로만 보지 아니하고, 권리구제를 철저히 함과 동시에 해킹에 대한 사회보험을 강구하는 것이 필요하다.

(투고일 : 2017. 1. 31 / 심사일 : 2017. 2. 8 / 확정일 : 2017. 2. 10)

참 고 문 헌

<국내문헌>

[단행본]

김남진, 행정법의 기본문제, 제4판, 법문사, 1996.
김남진・김연태, 행정법 Ⅰ, 법문사, 제20판, 2016.
김상철/양은상, 부동산 등기제도의 개선 방안에 관한 연구, 대법원 사법정책연구원, 2015.
김재광, 디지털경제법제의 제문제(Ⅰ) - 전자정부법제를 중심으로-, 한국법제연구원, 2001.
김중권, 행정법기본연구 Ⅳ, 제1판, 2014.
박균성, 행정법강의, 제13판, 박영사, 2016.
서정범・박병욱, 쿠겔만의 독일경찰법, 세창출판사, 제1판, 2015년.
정영화, 전자상거래법, 제2판, 다산출판사, 2001.
주지홍/류지태/송동수/오태원, 지식정보사회에서의 정보화법제 재정립을 위한 법제도 연구, 정보통신정책연구원, 2002.
안전행정부, 국가정보화 백서, 2011.
오병철, 전자거래법, 법원사, 1999.
윤광운/박정기/김철호/고형석/손성문/김제양, 전자상거래법, 삼영사, 2002.
윤주희, 전자거래의 적정화에 관한 법제연구, 한국법제연구원, 2001.
정남철, 행정구제의 기본원리, 제1판, 법문사, 2013.
정하중, 행정법개론, 제10판, 법문사, 2016.
_____, 행정법의 이론과 실제, 제1판, 법문사, 2012.
현대호, 전자거래입법의 문제점과 개선방안, 한국법제연구원, 2002.
홍정선, 민간위탁의 법리와 행정실무, 박영사, 제1판, 2015.
_____, 행정법특강, 제15판, 박영사, 2016.

[논문]

길준규, 통합개인정보보호법과 효과적인 개인정보의 보호, 토지공법연구, 제57집, 2012.5.2, 218면.
김남진, 공사협력과 행정법상 주요문제, 학술원통신, 제269호, 2015.12.1. 22면.
_____, 자본주의 4.0과 보장국가・보장책임론, 학술원통신, 제221호, 2011. 12. 6-7면.
_____, 제어학(制御學)으로서의 행정법학론(行政法學論), 법연, 제39권, 2013. 27면.

박재윤, 사이버안보의 복합적 특성과 국가사이버안보기본법(안)에 관한 토론문, in 국가사이버안보법제의 제정필요성과 법적 쟁점, 한국행정법학회 등 공동학술대회, 2016.10, 71면.

박희영, 단순해킹의 가벌성에 관한 비교법적 연구 - 독일 형법 및 사이버범죄 방지조약을 중심으로-, 인터넷법률 통권 제34조, 2006.3, 23-24면.

_____, 인터넷금융사기파밍피해자의 과실에 대해서 은행은 책임 없음, 최신독일판례연구, 로앤비(www.lawnb.com), 2013. 1, 10면.

서보국, '독일 전자정부법 제정의 현황과 전망', 2010년도 세계법제 연구보고서, 법제처, 2010, 2면, 7면.

성봉근, 보장국가에서의 위험에 대한 대응 - 전자정부를 통한 보장국가의 관점에서 본 위험-, 법과 정책연구, 제15권 제3호, 2015.9, 1050면, 1062면.

_____, 제어국가에서의 규제, 공법연구, 제44집 제4호, 2016.6, 234-235면, 239면.

_____, 종이문서에서 전자문서로의 이전에 따른 법정책적 연구, 법과 정책연구, 제16집 제2호, 2016.6, 60면.

손형섭, 개인정보의 보호와 그 이용에 관한 법적 연구, 법학연구, 법학연구 제5집, 2014.6, 11면.

오길영, 소위 '옥션판결(대판 2013다43994, 44003)에 대한 비판과 TOM, 공법학회 정보인권연구포럼 발표문, 2016.5, 11면.

유일상, 유계환, 표현과 소통으로서의 인터넷 댓글과 그 책임에 관한 일 고찰, 언론과 법 제10권 제2호, 20011, 323면, 331면.

조춘만・정문섭, 공간정보기반 부동산거래선진화시스템 구축방안, 한국공간정보학회지, 제21권 제6호, 2013, 74면.

현대호, 전자거래입법의 문제점과 개선방안, 한국법제연구원, 2002. 39면.

<독일문헌>

Bremer, Gewährleistungsverantwortung als Infrastrukturverantwortung am Beispiel der Eisenbahnreform in Deutschland, in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2005.

Franzius, Gewährleistung im Recht, Mohr Siebeck Tübingen, 2009.

Hermes, Gewährleistungsverantwortung als Infrastrukturverantwortung, in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2005.

Hinkel, Practical Real Estate Law, Delmar, 2011, at 179.

Hoffmann-Riem, Das Recht des Gewährleistungsstaates, in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2005.

_____, Modernisierung von Recht und Justiz - Eine Herausforderung des Gewährleistungsstaates, 1 Aufl., Shurkamp, 2001.

_____, Ermöglichung von Flexibilität und Innovationsoffenheit im Verwaltungsrecht - Einleitende Problemskizze-, in Hoffmann-Riem/Schmidt-Aßmann, Innovation und Flexibilität des Verwaltungshandelns, 1. Aufl., Nomosverlagsgesellschaft, Baden-Baden, 1994.

_____, Verwaltungsrecht in der Informationsgesellschaft - Einleitende Problemskizze, in Hoffmann-Riem/Schmidt-Aßmann(Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Nomos Verlagsgesellschaft, Baden-Baden, 1.Auflage, 2000.

Maurer, Allgemeines Verwaltungsrecht, 18. Aufl., Verlag C.H. Beck, 2011.

Kloepfer, Neutralität in der Informationsgesellschaft, Duncker & Humblot · Berlin, 2011.

Kugelmann, Polizei- und Ordnungsrecht, 2. Aufl., Springer-Verlag Berlin Heidelberg, 2012.

Schmidt-Aßmann, Das allgemeine Verwaltungsrecht als Ordnungsidee, Springer-Verlag Berlin Heidelberg, 2004.

_____, Regulierte Selbstregulierung als Element verwaltungsrechtlicher Systembildung, Schmidt-Aßmann, Regulierte Selbstregulierung als Element verwaltungsrechtlicher Systembildung, in Die Verwaltung - Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Duncker&Humblot, Berlin, Beiheft 4., 2001.

_____, Verwaltungsrechtliche Dogmatik - Eine Zwischenbilanz zu entwicklung, Reform und Künftigen Aufgaben, Mohl Siebeck, 2013.

Schmitt Glaeser, Partiztipation an Verwaltungsentscheidungen, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Heft 31, Wallter de Gruyter & Co., 1973.

Schulz, Regulierte Selbstregulierung im Telekommunikationsrecht, in Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaat, Die Verwaltung, Beiheft 4., Duncker & Humblot, Berlin, 2001

Schuppert, Der Gewährleistungsstaat -modisches Label oder Leitbild sich wandelnder

Staatlichkeit? in Schuppert (Hrsg.), Der Gewährleistungsstaat - Einleitbild auf dem Prüfstand, 1.Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2005.

Skrobotz, Das elektronische Verwaltungsverfahren, Duncker & Humblot, Berlin, Band 14, 2005.

Simitis(Hrs.), Bundesdatenschutzgesetz, 7. Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2011.

Suchanek, Grundsatzüberlegungen zur Verwaltungskontrolle aus ökonomischer Sicht, in Hoffmann-Riem/ Schmidt-Aßmann(Hrsg.), Verwlatungskontrolle, 1 Aufl., Nomos Verlagsgesellschaft, 2001.

Thoma, Regulierte Selbstregulierung im Ordnungsverwaltungsrecht, Duncker&Humblot Gmbh, Berlin, 2008.

Voßkuhle, Neue Verwaltungsrechtswissenschaft, in: Hoffmann-Riem/ Schmidt-Aßmann/ Voßkuhle(Hrsg.), Grundlagen des Verwaltungsrechts, 2Aufl., Verlag C.H. Beck, 2012.

<프랑스문헌>

Jacques Larrieu Droit de I'nternet, ellipses, 2e édition, 2010.

<영미문헌>

Coglianese · Mendelson,, Meta-Regulation and Self-Regulation, in Baldwin · Cave · Lodge (Edited by.), The Oxford Handbook of Regulation, Oxfor University Press, Reprinted, 2013.

Croley, Regulation and Public Interest - The Possibility of Good Regulatory Government, Princeton University Press, Princeton and Oxford, 2008, p. 305.

Barberis, The New Public Management and a New Accountability, Blackwell Publishers Ltd., 1998

Gellhorn, Administrative Law and Process in a Nutschell, West Publishing Co., 1972

Neithercutt, Introduction to Tactical Hacking : A Guide for Law Enforcement, Police Technical, 2015.

Spinello, Cyberethics - Morality and Law in Cyberspace, 5th Edition, Jones & Barlett Learning, LLC, an Ascend Learning Company, 2014.

<일본문헌>

板垣 勝彦, ドイツ公法學における「距離」概念について, 日本公法學會 公募報告セッション, 2012.
平野　美恵子,「米國の電子政府法」, 調査と情報 第423号