연구총서 13-B-02

K O R E A N I N S T I T U T E O F C R I M I N O L O G Y

사이버범죄 관련 법령정비 방안

A Study on Revisions of Laws and Regulations of Cyber Crimes

강석구 · 이원상

KIC 한국형사정책연구원
Korean Institute of Criminology

▌강석구

한국형사정책연구원 연구위원, 법학 박사

▌이원상

조선대학교 법과대학 교수

발간사

기술의 발전과 함께 사이버범죄는 마치 살아있는 생물처럼 계속해서 진화하고 있습니다. 불과 몇 년 전만해도 우리는 많은 사람들에게 피해를 입힌 '보이스 피싱'에 주목해야 해야 했습니다. 이로 인해 정부는 보이스 피싱에 효과적으로 대응하기 위한 수많은 방안들을 모색하였습니다. 하지만 이러한 노력에도 불구하고 범죄자들은 이런 정부의 대응을 비웃기라도 하듯 최근에는 '스미싱'이라는 새로운 수법을 통해 사람들에게 범죄피해를 입히고 있습니다. 이처럼 날아가는 범죄 뒤에서 달려가는 정책들이 마련되고 있다면, 사이버범죄자들의 처벌에 근거가 되는 법령들은 걸어가고 있다고 비유할 수 있습니다. 이는 사이버범죄가 우리 기성세대들이 상대하기에는 생소하고 버거운 대상일 수 있기 때문입니다.

그런데 사이버범죄에 비해 뒤쳐져서 쫓아가고 있는 것이 법령이라지만 그마저도 충분치 못한 상황이라고 할 수 있습니다. 이는 사이버범죄에 대해 입법적으로 대응함에 있어 체계적인 대응이 요구됨에도 불구하고 사이버범죄 법령체계를 충분히 구축하지 못한 채 단순히 사안별로 마련된 개별 법률만으로 대응을 하였기 때문입니다. 이에 한국형사정책연구원은 '사이버범죄 관련 법령정비방안'이라는 연구를 기획함으로써 현재 우리나라의 사이버범죄 관련 법령의 현주소를 살펴보고, '날아가는' 사이버범죄를 제대로 조준할 수 있는 입법체계를 마련하는 데 조금이라도 도움이 되고자 하였습니다.

다만 이 연구의 내용이 워낙 방대하기 때문에 단순히 이번 연구만으로는 다소 미흡한 부분이 있을 수 있습니다. 그래서 가급적이면 연구범위를 단순화시켜 '체계'와 관련한 사항에 논의가 집중될 수 있도록 진행하였으며, 이 연구뿐만 아니라 장차 후행연구들이 계속되다 보면 사이버범죄에 적절히 대응할 수 있는 입법체계가 완성될 수 있을 것이라고 기대합니다.

돌연한 이직에도 불구하고 끝까지 책임감을 가지고 이 연구를 마무리해준 조

선대학교 이원상 교수님께 감사드리며, 이 연구가 유종의 미를 거둘 수 있도록 도와준 강석구 연구위원의 노고를 치하합니다. 또한, 우리나라에는 잘 알려지지 않은 중국의 사이버범죄 관련 법제와 정책방향을 소상하게 소개해준 중국인민대학교 법학원의 티앤 홍졔 교수님과 스 옌안 교수님께도 감사를 드립니다. 나아가 이러한 노력들이 결실을 맺은 이번 연구가 정책입안자들에게 소중한 입법자료가 되기를 기대합니다.

2014년 2월

한국형사정책연구원

원장 박상옥

CONTENTS

표 차례

그림 차례

국문요약

사이버범죄는 꾸준히 증가하고 있으며, 그 피해 역시 계속해서 증가하고 있다. 특히 사이버범죄는 기술지배적인 특징을 가지고 있기 때문에 기술이 발전함에 따라서 사이버범죄도 함께 진화하는 형국을 띠고 있다. 이로 인해서 사이버범죄에 대응하기 위한 다양한 노력들이 행해지고 있으며, 다양한 형태의 대응방안들이 도입되고 있다. 하지만 기술적인 대응방안들은 비교적 빠르게 사이버범죄에 대응하고 있는 것에 반하여 가장 늦은 발걸음을 보이고 있는 것이 법률과 관련된 부분들이다.

이처럼 법률과 관련된 부분에서 취약점이 나타나고 있는 이유는 법률이 사이버범죄의 특징에 따라 유연하게 발전할 수 있는 체계가 아니기 때문이다. 이는 사이버범죄의 경우 처음부터 체계적으로 입법화되지 않고 사안에 따라서 개별적으로 규정되었기 때문에 사안에 대해서 법률을 적용하는 것에 문제점이 나타나게 되는 것이다. 무엇보다 입법자들은 사이버범죄에 대한 특질을 제대로 이해하지 못하고, 단순히 기존의 법률 체계에 사이버범죄를 추가하는 정도로 법률을 제·개정하고 있기 때문에 사이버 스토킹과 같은 일부 범죄에 있어서는 입법적 불비가 문제가 되는 반면, 개인정보와 관련된 부분에 있어서는 법률적인 충돌이 문제가 되고 있다.

현재 사이버범죄와 관련된 우리나라의 법률체계를 살펴보면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라고 함)이 사이버범죄의 기본법적인 역할을 하고 있기 때문에 상당수 사이버범죄와 관련된 규정들이 이 법률에 규정되어 있다. 그러나 이외에도 「정보통신기반 보호법」, 「전기통신사업법」, 「위치정보의 보호 및 이용등에 관한 법률」(이하 '위치정보법'이라고 함), 「개인정보보호법」 등 다양한 법률들에 있어서 사이버범죄와 관련된

다양한 처벌규정들이 산재해 있기 때문에 사이버범죄에 대한 일반예방기능을 기대하기 어려운 실정이다. 또한, 법령 내에서도 형사처벌 규정과 과태료 규정의 구분이 명확하지 않은 점이 있으며, 벌금형이나 과태료의 부과기준도 명확하지 않기 때문에 유사한 행위에 대해서 법령에 따라 다르게 평가될 수 있는 문제점도 존재하고 있다. 이처럼 법률이 제대로 정비되지 않은 상태이기 때문에 사이버테러 대응센터에서 제공하고 있는 사이버범죄 관련 통계 역시 부정확해질 수밖에 없고, 결국 이로 인해 통계를 이용한 사이버범죄 정책의 실효성을 담보할 수 없게 된다. 이에 사이버범죄 관련 법령의 정비는 매우 시급한 문제라고 할 수 있다.

이에 이 연구는 사이버범죄 관련 법령정비를 위해 고려되어야 할 내용들을 살펴보고, 사이버범죄 관련 법령정비 방안을 위한 프레임을 제공해 주는 것을 그 목적으로 삼고 있다. 따라서 본 연구에서는 사이버범죄에 대한 이해, 사이버범죄 관련 규정을 위한 기본이념, 사이버범죄 관련 규정들, 그리고 현재 법률체계를 분석한 결과인 사이버범죄 관련 법령정비방안을 위한 제언들로 구성되어 있다. 이는 사이버범죄 관련 법령을 정비하는 것이 단순히 기존에 있는 조문들을 헤쳐모여 하는 작업이 아니라 사이버공간의 이념과 사이버범죄의 개념 하에서 일정한 원칙을 가지고 체계적이고 정합적으로 수행해야 하는 작업이기 때문이다.

이에 따라 제2장에서는 사이버공간, 사이버문화, 사이버범죄에 대해 살펴보았다. 이는 사이버범죄를 보다 제대로 이해하고, 이를 바탕으로 삼기 위함이다. 그리고 제3장에서는 사이버범죄 법령 정비를 위한 기본이념들에 대해서 살펴보았다. 이를 통해 사이버공간에서 존중해야 할 권리는 무엇이며, 원칙들은 무엇이고, 행위규제 요소는 무엇이며, 사이버범죄 관련 정비를 위한 기본법체계는 어떠한 것인지에 대한 기본 개념을 고찰해 보았다. 제4장에서는 사이버법령의 정비요청으로 사이버범죄 관련 조직, 사이버범죄 관련 법령, 최근 논의되고 있는 기본법의 논의 상황 등이 서술되었다. 이를 통해 현재 사이버범죄 관련 법령체계에 대한 내용과 새로운 법령들의 경향을 파악할 수 있었다. 그리고 제5장에서는 사이버범죄 관련 법령정비방안을 위한 제언을 하였는데, 크게 사이버범죄 처벌법 제정방안, 사이버범죄 기본법 제정방안, 정보통신망법을 통한 개정방안, 현행 법령의 개정방안 등으로 구분하여 살펴보았다.

우리나라는 이미 사이버범죄와 관련된 규정들이 여러 곳에 산재되어 있으며, 사이버범죄와 관련된 주요 행위는 주로 정보통신망법의 개정을 통해 해결하고 있다. 그러나 이렇게 원칙이 없는 상태로 계속해서 입법이 될 경우 사이버범죄를 규율하는 체계는 영원히 무질서한 채로 남아 규범력을 제대로 발휘할 수 없게 될 것이다. 따라서 지금이라도 사이버범죄 관련 법령체계를 확립하고 그 체계에 따라 사이버범죄에 보다 적절하게 대응할 수 있는 입법이 되어야 할 것이다.

제1장 서론

강석구 · 이원상

01 서론

제1절 연구 목적

사이버범죄는 꾸준히 증가하고 있으며, 그 피해 역시 계속해서 증가하고 있다. 특히 사이버범죄는 기술지배적인 특징을 가지고 있기 때문에 기술이 발전함에 따라서 사이버범죄도 함께 진화하는 형국을 띠고 있다. 이로 인해서 사이버범죄에 대응하기 위한 다양한 노력들이 행해지고 있으며, 다양한 형태의 대응방안들이 도입되고 있다. 하지만 기술적인 대응방안들은 비교적 빠르게 사이버범죄에 대응하고 있는 것에 반하여 가장 늦은 발걸음을 보이고 있는 것이 법률과 관련된 부분들이다. 이처럼 법률과 관련된 부분에서 취약점이 나타나고 있는 이유는 법률이 사이버범죄의 특징에 따라 유연하게 발전할 수 있는 체계가 아니기 때문이다.

이는 사이버범죄의 경우 처음부터 체계적으로 입법화되지 않고 사안에 따라서 개별적으로 규정되었기 때문에 사안에 대해서 법률을 적용하는 것에 문제점이 나타나게 되는 것이다. 무엇보다 입법자들은 사이버범죄에 대한 특질을 제대로 이해하지 못하고, 단순히 기존의 법률 체계에 사이버범죄를 추가하는 정도로 법률을 제·개정하고 있기 때문에 사이버 스토킹과 같은 일부 범죄에 있어서는 입법적 불비가 문제가 되는 반면, 개인정보와 관련된 부분에 있어서는 법률적인 충돌이 문제가 되고 있다.

현재 사이버범죄와 관련된 우리나라의 법률체계를 살펴보면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라고 함)이 사이버범죄의 기본법적인 역할을 하고 있기 때문에 상당수 사이버범죄와 관련된 규정들이 이 법률에 규정되어 있다. 그러나 이외에도 「정보통신기반 보호법」, 「전기통신사업법」, 「위치정보의 보호 및 이용등에 관한 법률」(이하 '위치정보법'이라고 함), 「개인정보보호법」 등 다양한 법률들에 있어서 사이버범죄와 관련된 다양한 처벌규정들이 산재해 있기 때문에 사이버범죄에 대한 일반예방기능을 기대하기 어려운 실정이다. 또한 법령 내에서도 형사처벌 규정과 과태료 규정의 구분이 명확하지 않은 점이 있으며, 벌금형이나 과태료의 부과기준도 명확하지 않기 때문에 유사한 행위에 대해서 법령에 따라 다르게 평가될 수 있는 문제점도 존재하고 있다. 이처럼 법률이 제대로 정비되지 않은 상태이기 때문에 사이버테러대응센터에서 제공하고 있는 사이버범죄 관련 통계역시 부정확해 질 수 밖에 없고, 결국 이로 인해 통계를 이용한 사이버범죄 정책의 실효성을 담보할 수 없게 된다. 이에 사이버범죄 관련 법령의 정비는 매우 시급한 문제라고 할 수 있다.

따라서 본 연구의 주요 목적은 사이버범죄 관련 법령들의 정비를 위한 개선안을 제시하여 사이버범죄에 대한 일반예방기능을 획득하고, 형사사법기관이 사이버범죄에 대해서 적절하고 합리적인 처벌을 내릴 수 있으며, 더 나아가 사이버범죄에 대한 통계가 보다 효율적일 수 있도록 사이버범죄들의 유형들을 보다 명확하게 구분하여 규정할 수 있도록 하는 것이다. 무엇보다 본 연구는 이제까지 시스템 없이 구축되어 오던 사이버범죄의 입법관행에 대해서 일정한 방향성과 체계성을 제시해 줌으로써 de lege ferenda에서는 보다 효율적으로 사이버범죄에 대처할 수 있고, 일반 국민들이 보다 쉽게 이해할 수 있는 사이버범죄 관련 법령들이 제정될 수 있도록 해 주는 것도 중요한 목적으로 삼고 있다. 이를 위해 그간 한국형사정책연구원에서 수행되어 왔던 사이버범죄와 관련된 연구들을 결집하고, 이를 바탕으로 사이버범죄에 대응하기 위한 적절한 법령정비방안을 도출해 보고자 한다.

제2절 연구 내용 · 방법 및 기대효과

본 연구는 최종 성과물인 '(가칭) 사이버범죄 기본법'을 만들기 위하여 크게 세 부분에서 연구가 수행되었다.

첫째, 사이버범죄와 관련된 기본 이념들과 사이버법령 체계와 관련된 이론들, 사이버범죄로 규정되어야 하지만 현재 법령에서 적절하게 규정되어 있지 않거나 여러 법률들에 산재되어 있는 사이버범죄에 대한 이론적인 내용들을 정리하였다. 이를 위해 현재 우리나라 사이버범죄 법령체계가 어떻게 구성되어 있는지 분석하고, 우리나라 사이버범죄 법령체계의 문제점을 도출하며, 근래에 화두로 떠오르고 있는 (가칭)인터넷 기본법, 클라우드 컴퓨팅 기본법 등과 같은 기본법적인 성격을 가진 법률들에 대해 분석하였다. 이를 바탕으로 사이버범죄 관련 법령의 정비방향 제시하고자 한다. 또한 비교법적인 분석을 위해서 해외의 사이버범죄 관련 법령을 살펴볼 것인데, 특히 UNODC에서 주도하고 있는 국제사이버범죄 방지협약과 유엔 사이버범죄 방지협약을 좀 더 상세히 살펴보고, 이를 통하여 우리 법령에 반영될 수 있는 부분을 도출하고자 하였다.

둘째, 제안될 법률에 포함될 부분들을 점검해보았다. 현재 사이버범죄에 있어서 국제적인 기준으로 볼 수 있는 유럽 사이버범죄방지협정을 보면 개념정의 부분과 실체법적 부분, 절차법적 부분과 기타 사이버범죄에 필요한 규정들이 수록되어 있다. 이는 사이버범죄가 가지고 있는 특수한 성격으로 인해 기존의 실체법이나 절차법에 반영할 필요성이 있는 내용들을 규정하고 있는 것이다. 그리고 유럽 사이버범죄방지협정에 가입한 국가들은 협정의 내용에 따라 각 국의 법령을 개정하고 있다. 이와 같이 사이버범죄의 경우 국제적인 추세를 반영할 필요가 있다. 이와 함께 사이버범죄와 관련된 법령은 서로 유기적으로 연결될 필요가 있다. 우리나라의 경우 사이버범죄와 관련된 법령들이 우후죽순처럼 제정되고 있는 것에 반해, 이를 위한 사이버범죄 법령체계는 미흡한 실정이다. 그러므로 사이버범죄 관련 법령을 정비하기 위해 우리가 어떤 법령체계를 취해야 할 것인지에 대해 살펴보고자 하였다.

셋째, 이러한 연구를 바탕으로 사이버범죄 법령 정비방안을 제시하였다. 사이버범죄와 관련된 내용들을 입법하면서 사이버범죄의 특성을 고려한 적절한 입법

체계가 없는 상황에서 사안이나 조직 개편에 따라 관련 법률을 제·개정하기 때문에 구조적인 문제뿐만 아니라 실질적인 문제들도 발생하고 있다. 이처럼 원칙 없는 입법으로 인해 수사기관은 해당 법률을 찾아 적용하기 쉽지 않은 실정이며(실체법적 측면), 법률을 적용하더라도 사이버범죄에 대해 불완전한 절차법으로 인해 제대로 처벌을 할 수 없는 실정이다(절차법적 측면). 이에 이제까지 연구된 내용을 바탕으로 사이버범죄의 법령이 담아야 하는 내용들에 대해서 고찰해보고자 하였다.

이와 함께 본 연구에서는 이제까지 서방이나 일본에 국한되어 연구가 되었던 사이버범죄 관련 법령의 비교법적 연구 범위에 중국을 포함시키고자 한다. 이미 유럽이나 미국 등의 사이버범죄 관련 법령들은 많이 소개되었음에도 유독 중국의 관련 법령들은 소개될 수 있는 기회가 거의 없었다. 이는 이제까지 중국의 사이버범죄 관련 법령에 대한 소개가 거의 없었기도 했지만, 중국의 법령을 다소 수준 낮게 보고, 거리를 두었기 때문이라고 할 수 있다. 그러나 최근 몇 년간 중국은 법이론뿐만 아니라 법제에 있어서도 괄목할 만한 성장을 하였다. 이는 사이버범죄 분야에서도 마찬가지이다. 이에 이 글 제3장 제3절에서는 중국의 사이버범죄 관련 규정에 대한 부분을 법제적인 측면과 형사정책적인 측면으로 구분하여 보다 심도 있게 소개하고자 한다.

본 연구를 위하여 법학적인 안목을 바탕으로 문헌연구, 전문가 자문 등의 방법론을 활용하였는데, 본 연구의 주제가 다소 방대하기 때문에 본 연구의 연구결과가 실무에 바로 활용되기에는 충분하지 않을 수도 있다. 그러나 본 연구를 바탕으로 지속적인 후행연구들이 나오게 되면 사이버범죄 관련 법령체계를 보다 합리적으로 구축할 수 있는 보다 좋은 대안들도 계속해서 나올 수 있을 것이라고 생각된다. 이에 본 연구가 앞으로 이어질 후속연구들의 기초자료로서 소용될 수 있기를 기대한다.

제2장

사이버범죄의 기본 개념

이원상

02

사이버범죄의 기본 개념

제1절 사이버 공간에 대한 이해

1. 사이버공간(Cyberspace)의 의미

'사이버공간(Cyberspace)'이라는 용어는 1982년 발표된 윌리엄 깁슨의 '뉴로맨서'라는 소설작품에서 처음으로 사용되었다.[1] 사이버공간의 개념에는 '사이버'라는 개념과 '공간'이라는 두 개념이 함께 작용하게 된다.

먼저 '사이버'(Cyber)라는 말은 인공두뇌를 의미하는 '사이버네틱스'(Cybernetics)라는 말에서 나왔다. 사이버네틱스라는 개념이 필요하게 된 이유는 동물이나 기계 등의 의사소통 및 통제 시스템과 관련된 인공두뇌 시스템에 적합한 개념을 담을 용어가 필요했기 때문이다.[2] 그런데 이 용어는 키잡이를 의미하는 그리스어인 'kubernetes'에서 왔는데, 이 말이 라틴어에서는 'gubernetes'라는 말로서 그 동사형인 'gubernare'는 '통제하다, 조종하다'는 뜻을 의미한다.[3] 프랑스에서 사용되고 있는 'cybernetique'라는 단어도 통제술(the art of governing)이라는 의미로 사용되는 것을 보면 통제라는 의미는 사이버의 개념에 현재에도 포함되어

1) Willian Gibson, 『Neuromancer』, An Ace Book, 1984, 3면.

2) Norber Wiener, Cybernetics or control and communication in the animal and the machine, 제2판, 1965, 11면.

3) 이원상, "'사이버'개념을 통한 사이버 모욕죄의 고찰과 대안", 형사정책 제20권 제2호, 2008, 255면.

있는 것으로 볼 수 있다.[4] 그러므로 어원적인 측면에서 살펴보면, '사이버'(Cyber)라는 개념에는 그리스어 어원에서 볼 수 있는 것과 같이 '적극적 개척'이라는 의미와 함께 라틴어 어원에서 담고 있는 통제와 조종이라는 의미가 혼재되어 있다고 할 수 있다.[5]

다음으로 '공간'이라는 개념을 살펴볼 필요가 있다. 공간의 사전적 의미 가운데 하나는 '물리적으로나 심리적으로 널리 퍼져 있는 범위. 어떤 물질이나 물체가 존재할 수 있거나 어떤 일이 일어날 수 있는 자리가 된다'라고 한다.[6] 사이버공간은 하드웨어적으로 말해 소위 컴퓨터와 컴퓨터가 통신망을 통해 연결되어 만들어진 거대한 네트워크라고 할 수 있다. 하지만 이를 단순히 '사이버 네트워크'라고 칭하지 않는 이유는 이 네트워크 속에서 물질이나 물체가 존재하고 있지는 않지만, '어떤 일이 일어날 수 있는 자리'가 되어 현실과 똑같이 문화를 누리고, 삶을 누릴 수 있기 때문이다. 그러므로 사이버공간에서 '사이버'라는 개념은 외형과 방향성을 나타낸다면, '공간'이라는 개념은 그 내용을 의미한다고 할 수 있다.

그러나 아직까지도 사이버공간은 공식적인 용어로 통용되고 있지는 않다. 이는 사이버공간이라는 개념이 여전히 모호하며, 아직까지도 구체적으로 정의되어 있지 않기 때문이다. 따라서 공식문서나 법률적 용어에서는 사이버공간이라는 개념을 사용하는 것이 회피되어 왔다. 그러나 최근 들어 유엔관련 문서나 미국 등의 공식문서 등에서 사이버공간이라는 개념이 점차 공식적으로 사용되고 있으며, 그 개념을 설정하기 위한 노력도 계속되고 있는 실정이다. 이는 우리나라의 경우에도 마찬가지이다.[7] 다만 우리나라도 아직까지는 사이버공간이라는 용어를 법률에 사용하고 있지는 않다. 다만, 우리나라에서는 사이버공간이라는 용어 대신 "정보통신망"이라는 기술적 개념을 사용하고 있는데, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라고 함)에서는 정보통신망을

4) 데이비드 월(정태진 옮김), 사이버범죄, 2013, 22면.

5) 이원상, 앞의 글, 256면.

6) http://krdic.naver.com/detail.nhn?docid=3173400.

7) 이에 2013년 서울에서 열리는 '제3회 사이버스페이스 총회'의 준비기획단에서도 사이버스페이스의 개념을 명확히 설정하기 위해 연구용역을 발주하였다.

"전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제"라고 정의하고 있다.[8)]

2. 사이버문화의 이해

사이버범죄를 이해하기 위해서는 사이버 문화를 이해할 필요가 있다. 이는 범죄가 문화의 어두운 측면으로 문화의 자양분을 먹으며 생겨날 수 있기 때문이다. 문화를 정의하기는 쉽지 않지만, 사전적 의미로 문화란 "한 사회의 개인이나 인간 집단이 자연을 변화시켜온 물질적·정신적 과정의 산물"을 의미한다.[9)] 이처럼 문화가 계속해서 형성되고, 발전될 수 있는 이유는 매체를 통해서 의사소통이 가능해지면서 사회나 인간이 가지고 있는 지식이나 지혜가 전승될 수 있기 때문이다. 특히 문자의 발명으로 인해 방대한 양의 문화적 결과물들이 전승될 수 있게 되었으며, 광범위하게 전파될 수 있게 되면서 문화도 보다 더 발달할 수 있게 되었다. 그러던 것이 매체가 발달하면서 문화적인 양상도 다르게 나타나게 되었다. 신문이나 라디오, 영화, TV 등과 같은 매스 미디어가 발달하면서 획일적이고 보편적인 대중문화가 탄생하게 되었기 때문이다.[10)] 대중문화는 발신자 위주의 문화라고 할 수 있기 때문에 수신자는 보편성과 획일성 아래 단지 문화를 소비만 하는 소비자로서의 역할만을 수행하게 되었다. 따라서 대중문화는 수신자가 영위하고 있던 미시문화(microculture)를 급속히 해체시켰으며, 점차로 전체화 되어갔다.

---

8) 이와 함께 사이버공간을 '정보통신(情報通信)공간'의 개념을 통해서 이해하려는 시도도 있다. 이어령 교수에 따르면 비록 처음의 의미는 그렇지 않았지만, 정보통신이란 정(情)을 알리고, 믿음(信)을 통하도록 하는 공간이라는 것이다. 따라서 사이버공간은 정과 믿음이 그 내용을 이루어야 하는 곳이라고 할 수 있다는 것이다; 이어령, 디지로그, 2006, 55면 이하.

9) http://terms.naver.com/entry.nhn?docId=554876&cid=1605&categoryId=1605.

10) 피에르 레비(김동윤/조준형 옮김), 사이버 문화, 2000, 164면 이하.

그러나 사이버 문화는 현대 사회의 병폐로 지적되어 오던 매스 미디어의 폐해를 벗어나고 있다고 할 수 있다. 사이버 공간 속에서는 발신자와 수신자를 나누는 것이 아무런 의미가 없게 된다. 모든 사용자가 바로 문화의 생산자이자 소비자이기 때문이다. 이로 인해 생산자(producer)와 소비자(consumer)를 합성한 프로슈머(prosumer)라는 개념이 만들어지게 되었다. 따라서 매스 미디어로 인해 해체되었던 미시문화가 다시금 살아나게 되었으며, 보편화 되어 있지만 획일적이지 않은 '획일성이 존재하지 않는 보편성'을 가진 문화가 만들어지게 된 것이다.[11] 이는 정보 생산자가 전달하고자 하는 일방적인 가치관은 사이버 문화의 거름망을 통해 다시금 걸러지게 되었으며, 사이버 공간에서는 언론기관이나 개인이 동등한 정보의 제공자로 존재하여 일방적인 가치관에 함몰되지 않게 되어 개인이나 작은 집단의 미시문화가 존치할 수 있게 되었기 때문이다. 결국 사이버 문화의 대화형(Interactive)구조 속에서 정보 생산자와 정보의 소비자는 '획일적 전체성 없는 보편'이라는 새로운 문화의 양상을 경험하게 된 것이다.[12]

이처럼 획일적 전체성이 없는 보편의 문화를 가지고 있는 사이버 문화의 특성상 사이버공간에서의 사건은 급속히 보편화 될 수 있는 반면에 그에 대한 반응은 획일적이거나 전체성이 없게 될 수 있다. 또한 전체가 개인에게 군림할 수도 있는 반면에 개인도 전체 위에 군림할 수 있는데, 이는 사이버 문화에 익숙한 개인이 사이버 문화에 익숙하지 않은 전체에게 영향을 미칠 수도 있기 때문이다. 이와 같은 사이버 문화의 특징은 사이버범죄에 대한 이해와 대응전략 수립 시에도 반드시 고려될 필요가 있다.

3. 정보화 사회

사이버범죄를 이해하기 위해 또 한 가지 유의해야 할 개념으로 정보화 사회가 있다. 이는 사이버공간이 단순히 현실공간과 독립해서 존재하고 있는 것이 아니

11) 피에르 레비(김동윤 외 1명 옮김), 앞의 책, 170면.
12) 피에르 레비(김동윤 외 1명 옮김), 앞의 책, 169면.

라 현실공간의 늘어난 팔과 같이 현실공간에 그 뿌리를 두고 있기 때문이다.

정보화 사회의 발전과정을 볼 때, 정보화 사회는 크게 3세대로 나누어 볼 수 있다.[13] 먼저 제1세대는 비록 군사적인 목적이나 인구조사라는 제한된 목적을 위해서 사용되었지만, 컴퓨터가 사용되기 시작한 시기부터라고 할 수 있다. 이 시기에는 컴퓨터와 통신이 서로 다른 발전을 하는 시기라고 할 수 있다. 따라서 컴퓨터는 전산화 작업을 통해서 과거에 수작업으로 하던 작업들을 보다 빠르고 정확하게 처리하기 위해 주로 사용되었다. 그러다가 서서히 컴퓨터시스템과 통신기술이 접목되어 전화망을 통한 네트워크가 만들어지기 시작하였으며, 기업들은 인트라넷을 통해 전자화된 업무가 가능하게 되었다. 이때부터 비로소 아날로그에서 디지털화 되었다고 할 수 있다.[14]

제2세대 정보화 사회의 시작은 광대역 통신망이 보급되기 시작한 이후라고 할 수 있다. 제2세대를 대표할 수 있는 단어는 '네트워크'라고 할 수 있는데, 제1세대에서 주로 전화망으로 연결되던 것이 제2세대에서는 속도가 빠르고, 대역폭이 넓은 광통신으로 전환되면서 급속히 네트워크화 되어 갔기 때문이다. 또한 제1세대에서는 아날로그 정보가 디지털화 되어 갔다면, 제2세대에는 디지털화된 형태의 무수히 많은 정보가 생산되기 시작한 것이다. 무엇보다 제2세대의 주연은 '포탈'(portal)이라고 할 수 있는데, 포탈은 사이버공간의 관문역할을 하면서 정보의 분배에 있어 주도적인 역할을 하였기 때문이다. 그로인해 뉴스, 블로그, 카페, 이메일 등과 같은 서비스의 이용이 주로 포탈을 통해서 이루어지게 되었다.[15]

그러다가 제3세대 정보화 사회가 시작되었는데, 가장 큰 특징은 무선통신과 단말기의 다양화를 통해 정보가 더 이상 사이버공간에 머무르는 것이 아니라 현실공간과 융합되는 육신화(Incarnation)가 나타나게 된 점이다.[16] 또한 페이스북, 트위터, 미투데이 등과 같은 SNS를 통해서 개인은 끊임없이 개인정보들을 생산해 내었으며, 사이버공간의 수많은 지식공동체들의 정보들이 데이터베이스화 되

13) 이원상, "정보화 사회와 형법", 비교형사법연구 제12권 제2호, 2010, 347면.
14) 이원상, 앞의 글, 347-348면.
15) 이원상, 앞의 글, 348-349면.
16) 이원상, 앞의 글, 349면.

는 '빅데이터'가 등장하게 되었으며, 고정되어 있던 컴퓨터의 의존에서 벗어나 스마트폰, 노트북, 아이패드 등의 다양한 단말기가 등장하며 단말기의 종류에 관계없이 자신의 데이터를 사용할 수 있게 되는 '클라우드 컴퓨팅' 기술이 나타나기도 하였다. 따라서 이제 더 이상 사이버공간과 현실공간을 구분하는 것은 무의미해졌으며, 정보는 더 이상 사이버공간에 갖혀 있는 것이 아니라 바로 개인의 삶의 환경이자 근간이 된 것이다.[17]

제2절 사이버 범죄의 이해

1. 사이버공격과 사이버범죄

전형적인 사이버범죄[18]는 사이버공격의 한 유형에 속할 수 있다. 그러므로 우선 사이버공격에 대해 살펴볼 필요가 있다. 사이버공격은 그 영역에 따라 크게 3가지로 영역으로 구분해 볼 수 있다. 첫째로, 사이버 전쟁에 속하는 영역이 있다. 사이버 전쟁에서 해킹의 목적은 국가 및 사회의 중요 정보시스템을 교란·마비시켜 정치적·군사적인 목적을 달성하는 것에 있다. 이로 인해 해킹으로 인한 피해는 국가 전체를 대상으로 하며, 매우 광범위하고 치명적으로 발생하게 된다. 이런 심각성 때문에 미국은 사이버공간에서의 해킹 침략을 막기 위해 루이지애나주 박스데일 공군기지에 사이버지휘부대를 창설하였으며, 각 군 및 국가안보국에서 사이버전쟁과 관련된 임무를 수행하고 있다고 한다.[19] 또한 중국은 중앙군사위원회산하에 설립된 컴퓨터 바이러스 부대, 반해커부대, 전자전 부대 등을 운영하고 있는 것으로 알려져 있다. 이들은 정보전을 수행하고 있으며, 해킹 기술 개발 및 전술훈련, 외국정부기관 정보의 해킹 등을 그 임무로 하고

17) 이원상, 앞의 글, 450면.

18) 일반적으로 사이버테러 대응센터는 사이버범죄를 사이버 테러형 범죄와 일반적인 사이버범죄로 구분 한다. 여기서 사이버 테러형 범죄는 사이버공간에서만 존재하기 때문에 전형적인 사이버범죄라고 할 수 있다.

19) http://www.asiae.co.kr/news/view.htm?idxno=2009120108354496329.

있다고 한다.[20] 남한과 대치하고 있는 북한의 경우에도 이미 1만 2천명 이상의 해커부대를 양성해 놓고 있으며, 미림대학에서는 매년 200명 이상의 사이버전 인력을 배출하고 있다고 한다.[21] 하지만 남한은 2010년 1월 11일에 비로소 정보본부 예하에 사이버사령부가 창설되었으며,[22] 2012년에야 영토·영해·영공 뿐 아니라 사이버공간도 군사작전의 범위에 포함시켰다. 사이버 전쟁으로 분류되지는 않았지만 이미 여러 차례에 걸쳐 국가 간 사이버 전쟁이 치러지기도 하였다. 중국의 사이버 부대가 미국방부 전산망에 침입해 일부 전산망을 1개월가량 마비시킨 것이나 독일 정부의 주요부처의 전산망을 해킹한 사건, 러시아가 그루지아를 침공할 때 사이버 공격을 통하여 그루지아의 주요 전산망을 마비시킨 사건 등이 대표적이다.[23] 이런 사이버 전쟁의 경우 국가가 국가에 대해서 해킹을 수단으로 하여 군사적인 행동을 벌이는 것이기 때문에 범죄의 영역에서 접근하는 것은 거의 불가능하므로 결국 정치적인 영역에서 해결할 수밖에 없다. 따라서 사이버 전쟁은 형사정책적인 고려에서 제외된다.

둘째로, 사이버 테러 영역이 있다. 이 영역에서는 '테러'의 개념을 어떻게 정의하는가가 매우 중요하게 된다. 테러란 "어떤 정치(또는 종교, 사상)적 목적을 달성하기 위하여 직접적인 공포 수단을 이용하는 주의나 정책"을 의미한다.[24] 그러므로 사이버 테러를 구분하는데 있어서도 그 행위의 목적이 중요한 역할을 하게 된다. 한국의 법률에서는 사이버 테러를 "해킹, 컴퓨터 바이러스, 논리폭

20) http://news.kukinews.com/article/view.asp?page=1&gCode=pol&arcid=0921287339&cp=nv.

21) http://biz.chosun.com/site/data/html_dir/2013/03/27/2013032700947.html.

22) 한국의 국방부는 사이버테러 등의 위협에 효과적으로 대응할 수 있도록 하기 위해서 국방정보부 예하에 사이버사령부를 설치할 수 있는 근거규정을 "국방정보본부령"에 규정하였다. 국방정보본부는 ① 국방정보정책 및 기획의 통합·조정 업무, ② 국제정세 판단 및 해외 군사정보의 수집·분석·생산·전파 업무, ③ 군사전략정보의 수집·분석·생산·전파 업무, ④ 군사외교 및 방위산업에 필요한 정보지원 업무, ⑤ 재외공관 주재무관의 파견 및 운영 업무, ⑥ 주한 외국무관과의 협조 및 외국과의 정보교류 업무, ⑦ 합동참모본부, 각 군 본부 및 작전사령부급 이하 부대의 특수군사정보 예산의 편성 및 조정 업무, ⑧ 사이버 보안을 포함한 군사보안에 관한 업무, ⑨ 군사정보전력의 구축에 관한 업무, ⑩ 군사기술정보에 관한 업무, ⑪ 그 밖에 군사정보와 관련된 업무 등을 수행한다.

23) http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0002756754.

24) http://100.naver.com/100.nhn?docid=155082.

탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등을 정보통신망에서 사용하는 '정보시스템 공격행위' 내지 '정보통신망 침해행위' 또는 '전자적 침해행위'에 의하여 국가적·사회적으로 공포심 내지 불안감을 조성하는 행위"라고 정의하기도 한다.[25] 하지만 이 정의에는 목적성이 나타나고 있지 않기 때문에 사이버범죄와의 차이점이 나타나고 있지 않다. 그러므로 목적성을 고려할 때, 사이버 테러는 "정치·종교·사상의 목적을 가지고 해킹을 수단으로 하여 정보통신망을 교란하거나 침해하는 행위를 통해 사회적 공포심이나 불안감을 조성하는 행위"라고 할 수 있을 것이다. 따라서 사이버 테러는 행위 주체가 국가가 아닌 개인이나 집단이라는 것에 있어서 사이버 전쟁과 구분이 되고, 개인이나 집단이 자신의 경제적 이익 등을 목적으로 행하는 사이버범죄와도 구분된다. 이런 사이버 테러는 경우에 따라 정치적 및 군사적 해결을 필요로 하기도 하지만 일정 부분은 형사사법의 범위에 속하기도 한다. 예를 들어 알카에다와 같은 테러조직의 사이버 테러의 경우가 전자에 속할 것이며, 정부기관이나 기업 등을 해킹하는 어나너머스(Anonymous)와 같은 해커 그룹은 후자에 속하게 될 것이다.[26]

셋째로, 사이버범죄로서의 해킹이 있다. 한국의 언론은 일반적인 해킹도 사이버 테러라고 보도하고 있는데, 이는 잘못된 것이다. 이미 앞에서 언급한 바와 같이 일반적인 해킹은 정치·종교·사상적인 목적이 있는 것이 아니라 개인이나 집단의 사리사욕을 위해서 행해진다. 물론 행위태양이 사이버 전쟁이나 사이버 테러와 같이 나타나는 경우도 있다. 하지만 사이버범죄로서의 해킹은 주요 상업 사이트의 서버를 공격하여 협박하고 돈을 받아 내거나[27] 보안이 허술한 서버에 침입하여 개인정보를 빼내어 제3자에게 판매하는 것을 목적으로 한다.[28] 그러므로 이런 해킹의 경우가 전형적인 형사사법의 영역에 속하게 된다. 하지만 실질적으로 사이버 전쟁과 사이버 테러, 사이버범죄로서의 해킹을 명확하게 구분하

25) 최정호, "사이버테러리즘의 변천방향과 한국의 대응", 2008 국방안보학술회의, 2008, 159면 이하.

26) Anonymous의 경우 국가기관이나 기업들을 공격하는 이외에도 아동포르노 사이트를 공격하거나 맥시코 마약상들의 사이트를 공격하기도 한다; http://www.boannews.com/media/view.asp?idx=28204&kind=1, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201111012133145&code=970100.

27) http://economy.hankooki.com/lpage/news/200710/e2007101018293670300.htm.

28) http://news.mk.co.kr/outside/view.php?year=2010&no=179086.

는 것은 쉽지 않다. 예를 들어 중국 정부가 해커부대를 운영하여 미국 정부를 공격하더라도 이를 개인이 한 행위라고 발뺌을 하게 되면 일반적인 해킹행위가 될 수 있기 때문이다.[29] 또한 어나너머스의 공격도 사이버테러의 성격을 가질 수 있음과 동시에 사이버범죄의 성격도 가지고 있다.

표 1 사이버공격의 분류

해결 방법	정차군사적 해결	정차군사적 해결 / 형사사법적 해결	형사사법적 해결
관련 영역	사이버 전쟁	사이버 테러	사이버범죄로서의 해킹
예시	미국과 중국간의 사이버 전쟁	알카에다의 사이버 공격 / 어나너머스의 공격	어나너머스의 공격 /일반적인 사이버공격

결론적으로 사이버 전쟁에서의 해킹과 사이버테러에서의 일부 해킹, 사이버 해킹이 형사사법의 영역에서 벗어나게 되면, 일부 사이버 테러의 해킹과 일반적인 해킹이 형사사법의 범위에 속하게 된다. 그러나 개념적으로는 앞에서 처럼 구분해서 설명할 수 있지만, 사실 사이버공격이 행해고 있는 상황에서는 이와 같은 구분이 행해지기 쉽지 않다. 따라서 결국 사이버공격이 행해지는 경우에는 객관적인 피해의 중대성으로 판단하여 대응할 수밖에 없다. 이런 이유로 미국에서는 자국의 정보통신망에 대규모 공격이 가해질 경우에는 이런 구분과 상관없이 해당 국가에 대해 직접적으로 물리적인 공격을 하겠다고 하였으며, 최근 나토에서는 사이버 테러 이상의 공격에서의 교전 수칙을 규정한 '탈린 매뉴얼'을 내어 놓기도 하였다. 이런 점을 고려할 때, 사이버공격이 가해지게 되면 이에 대해 군사적, 정보적, 사법적 대응을 하는 것은 이후의 과정이며, 그 이전에는 우선적 대응과 원인 파악을 위한 기관이 절대적으로 필요하게 된다. 특히 사이

29) 이 때문에 미국은 사이버공간을 육·해·공·우주에 이은 제5의 공간으로 공식 선언하고, 사이버공간에서 미국을 공격할 경우 이를 단순한 사이버범죄가 아닌 전쟁으로 간주하여 전쟁법에 따라서 물리적 타격을 하겠다고 하였다; http://news.cnbnews.com/category/read.html?bcode=157180.

버안보와 관련된 사안은 촌각을 다투는 경우가 많기 때문에 전문성을 가지고 즉각적으로 권한 있는 조치를 취하여야 한다. 그러므로 이런 역할을 수행하기 위해 전문성과 권한이 집약된 사이버안보 컨트롤타워가 필요하기도 하다. 따라서 이에 대해서는 아래에서 좀 더 자세히 살펴보고자 한다.

2. 사이버범죄의 개념이해

앞에서 언급한 바와 같이 범죄는 문화의 어두운 산물이라고 할 수 있다. 그러나 뒤르켐의 범죄정상이론에 따르면 범죄는 비록 유감스럽더라도 정상적인 현상이며, 오히려 인간사회에 필수적이고 유익할 수도 있다.[30] 따라서 우리는 범죄와 어울리어 범죄를 억제하면서 살아가는 방법을 찾아야 할 수도 있을 것이다. 사이버범죄 역시 마찬가지이다. 사이버공간이 존재하고, 사이버공간에서 사이버문화가 발달할수록 사이버범죄 역시 보다 창궐하게 될 것이다. 다만 우리가 사이버범죄를 억제하면서 사이버 문화를 누리기 위해서는 사이버범죄에 대해 보다 상세히 분석할 필요성이 있다.

가. 사이버범죄와 유사개념

이제까지 사이버범죄의 개념은 명확하지 않다. 앞에서 '사이버'라는 용어가 갖고 있는 단어적 의미를 살펴보았다. 그러나 이런 의미가 사이버범죄라는 개념으로 이어지기 위해서는 추가적인 개념정리 작업이 필요하다. 그럼에도 불구하고 아직까지 사이버범죄의 개념에 대한 명확한 기준은 존재하지 않고 있다. 따라서 사이버범죄라는 용어뿐 아니라 컴퓨터범죄나 인터넷 범죄, 정보 범죄, 하이테크 범죄 등의 용어들이 여전히 혼재되어 사용되고 있는 실정이다. 다만 최근 유럽연합(예를 들어 유럽 사이버범죄 방지협정)이나 유엔 조직 및 마약범죄 방지국(UNODC) 등 국제기구나 미국, 독일, 한국 등 정보화가 진전된 주요 국가들에서 사이버범죄라는 개념을 사용하는 빈도가 높아지면서 사이버범죄라는 용어가

30) 배종대, 『형사정책(제8판)』, 홍문사, 2011, 278면.

점차 보편화 되고 있는 추세라고 할 수 있다.

사이버범죄라는 개념보다 먼저 사용된 개념이 컴퓨터범죄라는 개념이다. 컴퓨터범죄란 컴퓨터를 대상으로 하거나 수단으로 하여 행해지는 범죄로서 1960년대 초기 이후로 사용되고 있는 개념이다. 따라서 그 개념에는 해킹과 같은 컴퓨터 부정조작, 데이터의 부정입수, 컴퓨터 스파이, 컴퓨터 파괴, 컴퓨터 업무방해, 컴퓨터 무권한 사용, 시간절도나 서비스 절도, 그리고 기타 프라이버시침해 등의 유형을 포함하고 있다.[31] 우리 형법은 1995년 법률이 개정되면서 컴퓨터범죄에 대한 규정이 도입되었다.[32] 이로 인해 컴퓨터등 정보처리장치를 이용한 사기, 업무방해, 비밀침해, 공·사전자기록의 위작·변작 및 동행사 등 컴퓨터관련 범죄 등을 신설하였으며, 재물손괴죄 등에 전자기록 등 특수매체기록을 행위의 객체로 추가하였다. 그러나 이런 컴퓨터범죄의 개념은 과거 Stand-Alone 컴퓨터 시대나 전화통신 시대에나 적합한 개념으로 현재의 정보화 사회의 모습을 온전히 담고 있지 못하다.

또한 과거에는 컴퓨터범죄와 함께 사용되던 개념으로 정보범죄라는 개념이 있었다. 관련 문헌을 보면 정보범죄란 "정보처리장치 또는 정보를 이용하는 범죄, 그리고 정보처리장치 또는 정보에 대한 범죄를 총칭하는 의미"라고 개념규정하고 있다.[33] 정보범죄는 실무적으로 컴퓨터범죄보다 광범위하게 사용될 수 있는 범죄이다. 이는 정보라는 개념이 매우 광범위하기 때문이다. 그러나 정보범죄라는 개념에는 일반적인 정보에 대한 불법 탐색, 누설 등과 같은 행위도 포함될 수 있기 때문에 그 범위가 너무 넓다. 이는 앞에서도 언급하였지만 정보라는 개념이 개념 짓기에 따라서 무한히 확장될 수 있는 개념이기 때문이다.

뿐만 아니라 주로 수사기관에서 사용하던 개념으로 하이테크범죄라는 개념도 있다.[34] 하이테크범죄란 고도의 과학기술 내지 첨단과학기술을 사용하는 범죄라

31) 백광훈, "사이버범죄의 개념과 용어의 문제", 형사정책연구소식(통권 제68호), 2001, 39면.

32) 1995년 개정 이유를 보면 "...우리사회의 산업화·정보화의 추세에 따른 컴퓨터범죄 등 신종범죄에 효율적으로 대처하여 국민생활의 안정을 도모함과 아울러 현행규정의 시행상 나타난 일부 미비점을 개선·보완하려는 것임"이라고 컴퓨터범죄를 도입한 이유를 밝히고 있다.

33) 최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책원구원, 1998, 19면.

34) 조병인, "하이테크범죄의 실태와 대책", 한국공안행정학회 국제범죄 학술세미나 발표논문, 1999, 11면.

는 의미가 포함되어 있기 때문에 이 개념은 기술적인 관념에 다소 치중된 개념이라고 할 수 있다. 그로인해 사이버 불링이나 사이버스토킹, 사이버 명예훼손 등과 같이 고도의 전문기술을 사용하지 않는 디지털화 된 범죄의 경우에는 하이테크범죄의 개념에 포함되지 못하는 불합리함이 존재하게 된다.[35]

최근에는 정보통신범죄나[36] 인터넷범죄라는 용어들도 사용되고 있다. 전자는 컴퓨터범죄와 달리 정보통신망을 매개로 벌어지는 범죄로 이를 다시금 유형화하면 정보통신망을 매개하는 일반범죄유형인 정보통신범죄(사이버 명예훼손, 사이버 스토킹 등), 정보통신망을 매개하는 기존 컴퓨터유형인 정보통신범죄(사이버사기, 사이버 업무방해 등), 새로운 유형인 정보통신범죄(해킹, 바이러스유포 등), 정보통신망을 매개하지 않은 컴퓨터범죄(컴퓨터 사용사기, 데이터 손괴 등)으로 나누어 질 수 있다고 한다.[37] 인터넷범죄는 인터넷을 범죄수단으로 이용하는 범죄로 인터넷범죄를 위해서는 컴퓨터가 사용되어야 하기 때문에 컴퓨터범죄가 인터넷범죄보다 좀 더 넓은 개념이라고 한다.[38] 이 두 개념을 보면 범죄의 수법이 정보통신망이나 인터넷을 통해 이루어지는 것을 의미하기 때문에 그 범위가 매우 협소한 개념이라고 할 수 있다. 이는 정보통신망이나 인터넷을 사용하지 않는 범죄는 컴퓨터범죄에는 속하지만 정보통신범죄나 인터넷범죄에는 속하지 않기 때문이다.

이런 점들을 고려해 보자면 사이버범죄라는 개념은 플로베르의 '일물일어설'(一物一語說)에서 설명하는 것과 같이 오직 사이버범죄라는 용어가 어울린다고 여겨진다.

나. 사이버 범죄의 개념정의

사이버범죄의 개념을 설정하기 위해서는 사이버범죄가 일반적인 범죄와 다른 것이 무엇인지를 살펴볼 필요가 있다. 따라서 사이버범죄의 뜻을 좁게 설정하면

35) 백광훈, 앞의 논문, 41면.
36) 홍승희, "정보통신범죄의 전망", 형사정책 제19권 제1호, 2007, 9면 이하.
37) 홍승희, 앞의 글, 11면.
38) 오영근, "인터넷범죄에 관한 연구", 형사정책연구 제14권 제2호, 2003 여름호, 299-300면.

사이버공간에서만 특징적으로 발생하는 행위로 제한할 필요가 있다. 그렇게 보면 사이버범죄의 특별한 유형으로는 해킹과 악성코드 유포 정도의 행위가 있을 것이다. 그러나 이런 협소한 개념설정은 현재의 사이버범죄 관련 법률체계와는 전혀 부합하지 못하게 된다. 따라서 사이버범죄의 개념에는 해킹이나 악성코드 유포 외에 사이버공간 자체를 공격하거나 사이버공간을 매개로 하여 현실공간의 보호법익을 침해하는 행위도 포함될 수 있을 것이다. 따라서 사이버범죄를 "해킹, 바이러스 유포 및 사이버 공간을 근원으로 하거나 매개 수단, 또는 대상으로 하여 현실적 공간에 영향을 미치는 범죄행위"라고 정의를 내리기도 한다.[39]

앞에서의 정의는 사이버범죄의 개념을 매우 정태적으로 설정한 개념이라고 할 수 있다. 따라서 사이버범죄의 개념정의를 세대별로 구분하여 동태적인 개념으로 설정하기도 한다. 이는 앞에서 살펴본 바와 같이 정보화 사회를 세대별로 파악한 것과 같은 방식이라고 할 수 있다. 제1세대 사이버범죄는 가장 전형적인 범죄 형태로 컴퓨터범죄의 개념이 주를 이룬다. 이 시대의 사이버공간은 Stand-Alone 컴퓨터의 공간 안이며, 따라서 컴퓨터시스템의 전산오류나 허점을 이용한 범죄로 전형적이고 평범한 사이버범죄라고 할 수 있다.[40] 제2세대 사이버범죄는 글로벌 네트워크를 통해 발생하는 범죄이다. 따라서 컴퓨터범죄와 네트워크 범죄가 혼합된 개념의 범죄가 등장하기 시작한다. 무엇보다 사이버공간이 상업화됨에 따라 아날로그 범죄가 디지털 범죄로 변화되는 모습을 보이기도 하므로 이를 혼합형 또는 적응형 범죄라고 하기도 한다.[41] 그리고 제3세대 사이버범죄는 기술에 전적으로 영향을 받는 범죄로 확산과 자동화의 특성을 갖게 된다. 따라서 봇넷이나 자동 스팸메일 등과 같이 인간의 추가적인 행위가 필요하지 않은 기술적이고 자동화된 범죄들이 사이버범죄의 개념 속에 들어오게 된다.[42] 여기에 제4세대 사이버범죄에는 무선네트워크 기술과 상황인지 인텔리전트 네트워크(ambient intelligent networks)를 기반으로 하는 사이버범죄 유형이 많아질 것으

39) 이원상, 사이버범죄에 있어서 형법의 역할과 시스템적 대처방안, 고려대학교 석사학위논문, 2003, 17면.

40) 데이비드 월(정태진 옮김), 앞의 책, 65면.

41) 데이비드 월(정태진 옮김), 앞의 책, 67면.

42) 데이비드 월(정태진 옮김), 앞의 책, 69면.

로 예상되고 있다.[43] 이처럼 사이버범죄의 개념을 세대별로 살펴 볼 경우 사이버범죄의 개념의 확장 과정을 알 수 있게 된다.

다. 사이버 범죄의 특성

사이버범죄의 가장 큰 특징으로는 익명성과 세계성을 꼽을 수 있다.[44] 이런 특징은 초기 사이버범죄 때부터 계속되어 온 것이라고 할 수 있다. 그러나 사이버범죄의 특성은 앞에서 살펴본 바와 같이 사이버공간이 변화함에 따라서 함께 변화하기도 한다. 이런 특징은 사이버범죄를 연구하는 시점에 따라서 달라지기도 한다.

2000년 초, 한국형사정책이 사이버범죄에 관한 연구를 하였을 당시에는 사이버범죄의 특징을 아래와 같이 나누고 있었다. 다만, 그 이전에 사이버공간의 특징을 다음과 같이 서술하고 있다.[45] 첫째로, 사이버공간에서는 오로지 ID와 패스워드만 필요로 하기 때문에 사이버공간 이용자에 대한 익명성이 보장된다. 둘째로, 한 게시판을 동시에 여러 명이 이용할 수 있으므로 동시 다수의 이용과 접속이 가능하다. 셋째로, 사이버공간은 열린사회이기 때문에 시간과 공간의 개념이 의미 없게 된다. 넷째로, 개인용 PC와 모뎀만 있으면 되므로 이용장소의 제한이 없다. 다섯째로, 사이버공간의 자료들은 디지털 자료이기 때문에 출입흔적이 남지 않는다. 이런 특징들은 사이버공간이 초기 확장되기 시작하면서 생기는 특징이라고 할 수 있다. 이런 특징들로 인해 사이버범죄는 첫째, 범행의 주체를 밝히기가 매우 어려우며, 둘째, 개인이나 소수의 범죄행위로 커다란 피해가 발생하고 있고, 셋째, 범죄현장이 특정되어 있지 않으며, 넷째, 범행 흔적의 확인이 쉽지 않고, 다섯째, 범행증거 확보가 용이하지 않고, 여섯째, 현실공간에서 보다 수사에 많은 장애물이 존재하며, 일곱째, 범죄혐의 입증이 어렵고, 여덟째, 범행수법이 전문성에서 기인하게 된다고 보았다.[46] 다만, 이런 분석은

43) 위와 동일.

44) 하태훈, 앞의 논문, 95면.

45) 조병인/정진수/정완/탁희성, 사이버범죄에 관한 연구, 2000년 법무부 용역과제, 한국형사정책연구원, 2000, 22-23면.

사이버범죄 그 자체의 특징보다는 사이버범죄의 형사절차적 특징을 서술하고 있는 것으로 여겨진다.

사이버범죄 연구에 있어 저명한 울리히 지버(Ulrich Sieber) 교수는 최근의 사이버범죄의 특징을 크게 고도의 위험성을 안고 있고, 형체가 없으며, 감독이 어렵고, 일시적이며, 전 지구적이라고 말하고 있다.[47] 먼저 컴퓨터시스템 및 네트워크가 우리 사회의 모든 영역에서 사용되고 있는데 반해 사이버침해에 있어 상당히 취약한 상태이기 때문에 해킹과 같은 범죄는 고도의 위험성을 창출한다.[48] 다음으로 정보와 같은 무형물이 중요한 재화가 되면서 저작권, 프라이버시, 기밀 등 무형의 재화에 대한 신종 범죄들이 많이 발생하게 된다.[49] 그리고 방대한 데이터베이스와 암호, 컴퓨터시스템의 다양성 등으로 인해 사이버공간을 감독하는 것은 어려워지고, 이로 인해 불법역시 대응하기가 매우 어렵게 된다.[50] 또한 사이버공간에 저장되는 데이터들은 일시적으로 저장되거나 시간이 지나면 삭제되는 경우가 많기 때문에 범죄의 증거를 확보하기 어려워 수사기관은 가능한 한 신속하게 증거를 확보해야 한다.[51] 그러나 무엇보다도 사이버범죄는 전 지구적(global)으로 발생한다. 따라서 범죄는 국제적·초국가적인 피해를 입히는 것에 반해 범죄지의 위치를 찾는 것이 매우 어렵고, 개별 국가법을 적용하기도 용이하지 않으며, 국제적으로 대응하기도 쉽지 않다.[52] 이와 같은 사이버범죄의 특징들이 사이버범죄에 대한 대응을 어렵게 만들고 있다.

46) 조병인/정진수/정완/탁희성, 앞의 보고서, 23면 이하.
47) 울리히 지버, 전세계적 위험사회에서 복합적 범죄성과 형법, 한국형사정책연구원, 2011, 225면 이하.
48) 울리히 지버, 앞의 책, 225면.
49) 울리히 지버, 앞의 책, 25-26면.
50) 울리히 지버, 앞의 책, 26면.
51) 위와 동일.
52) 울리히 지버, 앞의 책, 26-27면.

제3장

사이버공간의 기본이념과 법령체계

이원상 · 田宏杰 · 时延安

03

사이버공간의 기본이념과 법령체계

제1절 사이버공간의 권리와 원칙

1. 서론

컴퓨터와 컴퓨터가 통신망을 통해 연결되면서 소위 '컴퓨터 통신'이 가능하게 된 이후로 컴퓨터 기술과 통신기술은 엄청난 발전을 거듭하였다. 통신망들은 거미줄처럼 연결되어 전 세계의 컴퓨터들을 하나의 망으로 이어주는 '인터넷'을 형성하게 되었으며, 초고속 인터넷과 다양한 기기들이 서로 얽히면서 '사이버공간'으로 나아가게 되었다. 이처럼 인간의 기술에 의해 창조된 공간은 단순히 미디어로서의 기능을 하는 것이 아니라 현실공간의 연장선상에서의 '삶의 터전'이 되었다. 사이버공간에서 우리는 은행 업무를 보거나 쇼핑을 하고, 학교에 다니며, 연애도 하고, 집이나 매장과 같은 부동산을 소유하기도 한다. 하지만 사이버공간에서의 활동은 단순히 사이버공간에만 국한되지 않는다. 사이버공간에서 은행 업무를 보면, 자신의 통장 잔고에 직접적인 영향을 미치고, 쇼핑을 하게 되면 실제로 주문한 물건이 배달이 된다. 또한 사이버공간에서의 연애를 통해 실제로 결혼을 하기도 하고, 가상의 집이나 매장을 양도하면 현금을 받기도 한다. 그러

므로 사이버공간은 현실공간의 '늘어난 팔'의 역할을 한다고 할 수 있다.

이처럼 사이버공간에서의 삶과 현실공간에서의 삶의 구별이 의미가 없어지는 것과 같이 사이버공간에서의 인간의 권리도 현실공간에서의 권리와 구별을 할 수 없게 되었다. 가령 현실공간에서 표현의 자유가 중요하게 여겨지기 때문에 높은 수준의 보호를 받는 것처럼 사이버공간에서의 표현의 자유 역시 매우 중요한 권리로서 보호를 받고 있다. 하지만 현실공간에서의 권리침해와 사이버공간에서의 권리침해가 동일하게 다루어지지는 않게 되는데, 이는 사이버공간이 갖고 있는 특수성 때문이다. 예를 들어 현실공간에서 명예를 훼손하는 경우보다 사이버공간에서 명예를 훼손하는 경우 그 위험성과 불법성이 보다 크게 판단되기 때문에 사이버공간에서의 명예훼손은 보다 강하게 처벌된다. 또한 현실공간에서 권리침해가 발생하는 경우 그 피해가 확산되기 위해서는 상당한 시간이 요구된다. 따라서 사후적인 대응을 하더라도 늦지 않을 수 있다. 그러나 사이버공간에서는 권리침해가 발생하는 즉시 전 세계적으로 확산될 수 있으며, 그 흔적은 결코 사라질 수 없게 된다. 그러므로 사이버공간에서의 권리침해에 대한 대응은 촌각을 다투기 때문에 선제적일 것이 요구된다. 이와 같이 사이버공간에서의 침해대응은 현실공간과는 다른 측면이 존재하게 된다.

이런 관점에서 최근 많이 발생하고 있는 사이버공간에서의 권리침해와 이에 대한 대응원칙을 살펴보고자 한다. 즉 사이버공간에서의 권리구제방식은 현실공간과는 다를 수 있다는 것이 그 전제가 되는 것이다. 하지만 사이버공간이 현실공간과 다르고, 특수성을 가지고 있다고 해서 현실공간에서와 다른 사이버공간에서의 권리구제방식이 용인되는 것은 아니다. 사이버공간에서의 권리구제방식이 허용되기 위해서는 현실공간에서 통용되고 있는 원칙의 틀 안에서 이루어져야 하기 때문이다. 가령 사이버공간에서 문제가 되는 아이디를 삭제하는 방안은 매우 좋은 방법일 수 있지만, 비례성원칙에서 볼 때, 비례적이지 않은 대응방안이 될 수 있다. 그러므로 사이버공간에서 권리를 구제하는 방식이 사이버공간의 특수성을 고려하지 않게 되면 정당성을 잃게 될 위험성이 있다.

따라서 여기서는 우선적으로 사이버공간과 사이버권리에 대한 기본적인 이해를 통해 여기 이후에 논의될 내용에 대한 인식의 지평을 동조화시키려고 한다. 그리고 나서 사이버 법률에 있어 반드시 고려되어야 할 기본적인 원칙에 대해서

살펴보고자 한다.

2. 사이버공간에서의 권리

가. 사이버권리

1) 초기 사이버공간에서의 권리

초기 사이버공간에서의 권리는 주로 의사표현 또는 데이터베이스와 관련이 있다고 할 수 있다. 이는 초기 사이버공간이 의사소통을 위한 미디어로서의 역할과 전산화를 통한 거대한 데이터베이스로서의 역할을 주로 수행하였기 때문일 것이다. 의사표현과 관련해서는 전통적인 인권인 표현의 자유와 관련이 있다. 그러므로 미디어로서의 사이버공간에서는 기본적으로 전통적인 표현의 자유에 대한 권리 보호가 현실공간에서 논의되고 있는 논의내용의 연장선상에서 논의될 수 있다. 이에 반해 주로 국가가 운용하고 있는 데이터베이스에 대한 권리로 국민의 알 권리에 대한 문제 및 이의 공개로 발생할 수 있는 사생활의 침해, 데이터베이스의 검색과 관련해서 새롭게 부각된 Access권, 자기정보결정권 등이 주요 정보화 사회의 사이버권리로 인식되었다.[53] 이에 아래에서는 초기 사이버공간에서의 권리들에 대해서 살펴보고자 한다.

2) 표현의 자유

표현의 자유에는 비단 현실공간이나 초기 사이버공간에서의 권리만 속하는 것이 아니다. 표현의 자유는 시·공의 한계를 벗어나는 권리이기 때문에 초기 사이버공간에서 표현의 자유를 중요한 권리로 삼은 것은 아주 당연하다고 할 수 있다. 하지만 초기 사이버공간에서 표현의 자유에 대해 높은 기대치를 둔 까닭은 현실공간이 가지고 있는 표현의 자유의 제약을 극복할 수 있는 최고의 공간

53) 김철수, 헌법학신론, 제20전정신판, 2010, 293면 이하.

이라는 믿음이 있었기 때문이다. 특히 사이버공간이 처음 만들어진 미국의 경우 미국수정헌법 제1조에 따라 표현의 자유가 강력하게 보장되고 있으며, 이는 비단 현실공간에만 한정되는 것이 아니라 사이버공간에서도 강력하게 보장되어야 한다는 사고가 강하였다.[54]

3) 액세스권

현대와 같이 누구나 언론에 접근할 수 있고, 1인 미디어를 통해 개인이 바로 언론이 될 수 있는 사회가 되기 이전에는 국가가 언론을 주도하였다. 이에 대해 배런은 매스미디어의 발달로 인해 미디어 경영가라는 새로운 계급이 탄생하였고, 그로 인해 미국의 수정헌법 제1조가 보장하고 있는 언론의 자유가 새로운 계급에 의해 독점된다고 주장하였다.[55] 이처럼 언론을 주도하는 계급에 의해 국민들은 수동적인 지위에 처하게 되었으며, 이로 인해 국민들은 국가나 매스미디어에 액세스할 필요성과 요청이 대두되었다. 이에 배런은 미연방수정헌법 제1조에서 보장하는 사상의 자유 시장에 따라 전통적 언론자유이론에 대한 재평가를 요구하면서 이를 위한 권리로 '액세스권'을 주창하였다.[56] 이 액세스권은 "국민이 자신의 생각이나 의견을 발표하기 위하여 언론사에 자유로이 접근하여 그것을 이용할 수 있는 권리"로서 이는 국가를 상대로 하는 권리가 아니라 언론사를 그 상대로 하고 있는 권리이다.[57]

4) 자기정보결정권

초기 사이버공간에서 발견된 권리 가운데 가장 최근에 발견된 권리로는 개인정보자기결정권(Recht auf informationelle Selbstbestimmung)이 있다. 개인정보자기결정권이란 원칙적으로 개인이 자신의 개인정보의 제공 및 이용 등에 있어 모

54) Mike Godwin, Cyber Rights, 1998, 3면 이하.

55) 이동훈, "유비쿼터스사회에서의 액세스권과 알권리 해석론", 공법학연구 제10권 제2호, 2008, 83면.

56) J. A. Barron, "Access to the press-A New First Amendment Right", 80Harvard Law Review, 1967, 1644.

57) 문제인, "일인 미디어 시대의 액세스(access)권", 언론과 법 제9권 제2호, 2010, 166면.

든 것을 스스로 결정할 권한이 있다는 것이다. 사실 개인정보자기결정권이 처음으로 인정된 것은 독일이다. 다만, 독일의 경우 비록 독일 기본법에 개인정보자기결정권에 대한 명시적인 규정이 있지는 않으나, 1983년 인구조사결정과 관련해서 독일연방헌법재판소가 기본법 제2조의 일반적 인격권으로부터 개인정보자기결정권을 도출해 냄으로서 인정되기 시작한 권리이다. 특히 개인정보자기결정권이 인정된 이유는 개인이 자신의 개인정보를 스스로 자유롭게 결정할 수 있어야 비로소 인간의 존엄성이 보장될 수 있다고 판단되었기 때문이다.[58] 무엇보다 독일연방헌법재판소의 판결로 인해서 변화된 정보화 사회에서 반드시 필요한 개인정보보호에 관한 기본권이 만들어져서 개인정보가 기본권으로 보호될 수 있는 근간이 만들어지게 된 것이다.[59]

우리나라도 독일과 같이 헌법적으로 개인정보자기결정권을 인정하고 있다. 다만 개인정보자기결정권의 근거규정이 어디에 있는지에 대해서는 여전히 논란이 있다. 일부에서는 헌법 제17조에 있는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다"라는 규정에서 기인한다고 주장하기도 하는데, 그 이유는 우리나라는 인격권으로부터 도출할 수 밖에 없는 독일의 기본법과 달라서 제17조에서 명시적으로 사생활의 비밀과 자유로부터 개인정보보호에 관한 직접적인 근거가 존재하기 때문이라고 한다.[60] 이에 반해 일부 견해는 개인정보자기결정권이 헌법 제10조에서부터 기인한다고 보기도 한다.[61] 그러나 우리 헌법재판소는 개인정보자기결정권은 헌법에 명시되지 않은 독자적인 기본권이라는 관점을 가지고 있는 것으로 보인다. 이는 헌재의 결정에 보면 잘 나타나고 있는데, "… 개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호

58) BVefGE 65, 1.

59) 김상겸, "독일의 의료정보와 개인정보보호에 관한 연구", 한·독사회과학논총 제15권 제2호, 2005년 겨울호, 12면.

60) 김연태, "정보의 자기결정권과 경찰의 정보관리", 고려법학, 2001, 160면.

61) 김철수, 헌법학(상), 2008, 838면.

하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다..."[62]라고 판단하고 있기 때문이다.

그러나 개인정보자기결정권이 비록 정보화 사회에 있어 중요한 권리라고 할 수 있지만, 무제한적으로 보호되어야 하는 것은 아니다. 이는 개인은 사회적 공동체에 속해 있는 구성원이기 때문에 지속적인 의사소통을 통해 서로 발전하며 사회를 유지시켜 갈 수 있고, 그러므로 개인의 정보가 절대적이고 무제한적으로 보호될 경우 사회시스템이 제대로 작동할 수 없게 되는 문제점이 발생할 수 있으며, 이는 최근 발효된 개인정보보호법을 통해서도 조금씩 입증되어가고 있다.[63] 특히 개인정보의 이익과 공공의 이익이 상충되는 경우도 빈번하게 발생하게 되는데, 이 때에는 서로 비교형량을 통하여 해결하여야 할 것이다.[64] 그러나 비교형량을 통해 개인정보자기결정권을 제한하더라도 반드시 명확한 법률적 근거가 필요하며, 비례성원칙의 근본이념은 동일하게 지켜져야 할 것이다.[65]

나. 사이버공간의 새로운 권리요청

현재 사이버공간에서의 권리를 보면 기본적으로 초기부터 강조되어온 권리는 그대로 존속한다. 여기에 새롭게 논의되고 있는 권리들이 추가된다고 할 수 있다. 이 가운데 가장 두드러진 권리로 독일 헌법재판소가 판결한 소위 "IT 기본권"이라고도 하는 "정보기술시스템의 기밀성과 무결성의 보장에 관한 기본권"과 최근 유럽에서 도입하려고 하는 "잊혀질 권리"가 있다. 전자는 사이버공간에서 개인이 자유롭게 활동하는 것을 보호하기 위해 요구되는 권리이며, 후자는 개인

62) 헌재 2005.5.26. 선고 99헌마513.

63) 따라서 최근 개인정보보호법의 개선을 위해 국회의원 주도의 토론회가 열리기도 하였다; http://www.etnews.com/news/computing/security/2828262_1477.html.

64) 김연태, 앞의 글, 168면.

65) 위와 동일.

이 사이버공간에서 자유롭게 퇴장하기 위해 요구되는 권리로서 초기 사이버공간에서는 크게 문제가 되지 않았던 권리들이다. 하지만 이 뿐 아니라 권리라고 할 수는 없지만, 인터넷 망을 이용하여 전달되는 인터넷 트래픽에 있어 데이터의 내용이나 유형에 상관없이 이를 생성하거나 소비하는 주체에게 차별 없이 동일하게 취급해야 한다는 '망중립성(network neutrality)'에 대한 요청도 제기되어 있다.

1) IT-기본권

최근 사이버공간에서의 권리로 가장 주목을 받고 있는 것으로 독일의 헌법재판소에 의해 도출된 소위 'IT-기본권'이라는 것이 있다. IT-기본권에 대한 논의의 도화선이 된 사인으로 테러범죄에 대응하기 위해 노르트라인-베스트팔렌주의 헌법보호법률(Gesetz über den Verfassungsschutz in Nordrhein-Westfalen)에 온라인 수색(Online-Durchsuchung)이 규정되어 2006년 12월 20일부터 효력이 발생한 것이다.[66] 물론 독일에서는 온라인 수색에 관한 규정이 존재하기 이전에도 테러범죄에 대한 대응방안으로 온라인 수색이 가능할 수 있을지에 대한 논란이 제기되었다. 특히, 형사소송법 제110a조(신분위장수사경찰; 전기통신의 검열 및 기록), 제110c조(비밀 수사), 제102조(혐의자 수색), 제161조(검사의 권한) 등에 의해서 온라인 수색의 허용성 여부가 검토되기도 하였으며,[67] 이에 대해 학계에서도 많은 논란이 있어왔다.[68] 이후 해당 내용이 연방수사청 법률에의 도입이 시도되면서 공은 연방헌법재판소로 넘어가게 되었다. 이에 대해 연방헌법재판소는 다음과 같은 이유로 헌법 불합치 결정을 내리게 되었다.[69]

「① 일반적인 인격권(Persönlichkeitsrecht: 기본법 제1조 1항과 관련한 제2조 1항)은 정보기술 시스템의 기밀성과 무결성 보장에 관한 기본권(Grundrecht auf

66) VSG-NW, Fn 10.

67) Manfred Hofmann, Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005, Heft 3, 121면 이하.

68) Werner Beulke, Strafprozessrecht, 제9판, 2006, 150쪽.

69) BVerfG 1 BvR 370/07.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)을 포괄한다.

② 비밀리에 정보기술 시스템에 침입하고, 이를 수단으로 해서 시스템의 사용을 감시하고, 그 저장장치를 검색하는 것은 매우 중요한(überragend wichtig) 법익에 대한 구체적인 위험이 있다는 실제적인 근거가 존재하는 경우에 한해서만 헌법적으로 허용될 수 있다. 매우 중요하다는 의미는 신체(Leib), 생명(Leben), 개인의 자유(Freiheit der Person) 또는 국가의 근간이나 존립, 인간의 존립근거를 위협하는 공공법익 등을 의미한다. 이런 조치는 비록 위험이 가까운 장래에 발생하리라는 충분한 개연성(Wahrscheinlichkeit)은 확인될 수 없지만, 특정 사실이 개별 사안에 있어 특정 개인에 의해 매우 중요한 법익이 위협되고 있다는 것을 가리키고 있을 경우에 한해서만 정당화 될 수 있다.

③ 비밀리에 정보기술 시스템에 침입하는 것은 원칙적으로 판사의 명령에 유보되어 있다. 그런 침입에 대한 수권 법률은 개인의 생활형태의 핵심영역(Kernbereich)을 보호하기위한 보호조치들(Vorkehrungen)을 포함하고 있어야만 한다.

④ 통신망에서 이루어지고 있는 정보통신의 내용이나 상황들을 수집하거나 그와 관련된 데이터들을 사용하는 국가의 조치들은 수권(Ermächtigung)(수권규정)에 의해서 제한될 수 있는데, 이를 위해서 기본법 제10조 제1항에 따른 침입이 고려되어야 한다.

⑤ 국가가 기술적 방법으로 인터넷 통신의 내용을 인지하는 경우 국가가 정보통신의 참여자가 아님으로 인하여 인지에 대한 권한을 획득할 수 없을 경우에만 기본법 제10조 1항에서의 침입이 존재하게 된다. 국가가 인터넷상에서 공개적으로 접근할 수 있는 정보통신내용들을 인지하거나 공개적으로 접근할 수 있는 정보통신과정에 참여하는 경우, 국가는 기본적으로 기본권을 침해하는 것은 아니다.」[70]

70) 이원상, 온라인 수색(Online-Durchsuchung)에 대한 고찰 -독일의 새로운 논의를 중심으로, 형사법연구 제20권 제4호, 2008년 겨울호, 345면 이하 재인용.

IT-기본권은 나름대로 정보화 시대에 필요한 기본권이라고 여겨지고 있던 개인정보자기결정권의 지평을 넓혀주었다고 할 수 있다. 앞에서 살펴 본 바와 같이 개인정보자기결정권은 개인정보의 제공 및 이용에 관하여 개인 스스로 결정하는 것을 보장하는 것으로 정보의 '동적인 형태'를 강조한 것이라고도 할 수 있다. 그러나 IT-기본권은 정보로서 가치를 유지할 수 있도록 해 주는 정보의 3요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보호해 줌으로 인해 정보의 '정태적인 형태' 및 정보를 실질적으로 보호해 주는 권리라고 할 수 있다. 따라서 IT-기본권과 개인정보자기결정권은 서로 보완관계에 있으며, 전자는 정보의 정적인 형태를, 후자는 정보의 동적인 형태를 보호해 줌으로 인해 개인정보를 보다 강력하게 보호해 주는 권리라고 할 수 있다. 이처럼 IT-기본권은 정보화 시대에 적합한 권리라는 인식으로 인해 독일 이외의 여러 국가들이 관심을 가지고 있기도 하다.

2) 잊혀질 권리

사람들은 하루에도 수없이 많은 정보를 인터넷에 축적하고 있다. 정보의 축적은 웹하드에 자신의 정보를 올리거나 이메일을 보내는 것, SNS에 글을 올리는 것 등과 같이 개인이 의식하면서 이루어지기도 하지만, 인터넷 웹사이트에 방문하는 경우 쿠키를 남기거나 위치정보를 이용한 서비스 이용 등과 같이 인터넷 서비스 업체들이 제공하는 서비스를 사용하면서 자신도 모르는 사이에 자신의 개인정보가 사이버공간에 축적되기도 한다.[71] 문제는 이처럼 사이버공간에 일단 기록된 내용들은 절대로 지워지지 않는다는 것이다. 따라서 이런 현상을 '디지털 판 주홍글씨'라고 표현하기도 한다.[72] 이처럼 사이버공간에 축적되는 개인정보들은 단순히 0과 1의 조합으로 남아있는 것이 아니다. 개인의 이력을 추적할 수 있게 되며, 더 나아가 범죄에 악용될 수 있는 소지도 남게 된다. 따라서 이런 문제점을 인식한 EU에서는 2014년 발효를 목표로 사이버공간에서의 잊혀질

71) 구글이나 유투브 검색, 이메일, SNS 등을 통해 2012년 현재 매 60초마다 70만건이 넘는 정보들이 생성되고 있다고 한다; http://www.boannews.com/media/view.asp?idx=32049&kind=1.

72) 다니엘 솔로브(이승훈 옮김), 인터넷 세상과 평판의 미래, 2007, 27면.

권리(right to be forgotten)의 도입을 추진하고 있다.[73]

EU가 발간한 문건에 의하면 잊혀질 권리란 "자신의 정보가 더 이상 적법한 목적들을 위해 필요치 않을 때, 그것을 지우고 더 이상 처리되지 않도록 할 개인들의 권리"로서 "정보처리가 개인의 동의에 기반하고 있을 때 그 또는 그녀가 동의를 철회하거나 저장 기간이 만료된 경우"에 그 행사를 할 수 있도록 하고 있다.[74] 특히 이처럼 잊혀질 권리가 더욱 절실히 필요하게 된 이유는 정보의 물리적인 저장 장소가 의미를 잃게 되는 클라우드 컴퓨팅 환경으로 인해 '장소'를 요건으로 하고 있던 기존의 정보보호법의 원칙들이 적용되기 힘든 영역이 생겼기 때문이다.[75] 그리고 한 번 클라우드로 들어간 정보는 개인의 의사에 의해서 전부 삭제될 수 없게 되었다. 이에 우리 정부에서도 개인정보의 보호를 강화하고, 개인의 정보에 대한 권리를 향상시키기 위해서 잊혀질 권리의 법제화를 검토하고 있는 것으로 알려져 있다.[76]

사실 우리나라는 이런 문제들에 대해서 정보통신망법이나 개인정보보호법에 관련 규정을 두고 있다. 정보통신망법 제30조에서는 이용자가 개인정보 수집·이용·제공 등의 동의를 철회할 수 있고(제1항), 오류가 있으면 정정을 요구할 수 있으며(제2항), 동의가 철회되면 수집된 개인정보를 파기하도록 되어 있다(제3항). 또한 개인정보보호법 제4조 제4호에서는 정보주체는 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리를 가지고 있다. 하지만 앞에서도 언급한 바와 같이 클라우드 컴퓨팅 환경에서는 개인이 자신의 정보를 파악하여 자신의 권리를 주장하는 것이 매우 어렵기 때문에 개인의 주장이 없는 경우에도 유효기간이 지난 정보는 자동으로 삭제될 필요가 있다.[77] 이는 본인이 사망하여 그 자신이 개인정보 삭제를 요구할 수 없는 경우에도 유효하다고 할 수 있다.[78] 또한

73) 민윤영, "인터넷 상에서 잊혀질 권리와 「개인정보보호법」에 대한 비교법적 고찰", 고려법학 제63호, 2001, 294면 이하.

74) 민윤영, 앞의 글, 299면.

75) 민윤영, 앞의 글, 302면.

76) http://www.dt.co.kr/contents.html?article_no=2012092602010831742001.

77) 민윤영, 앞의 글, 307면.

78) 이는 단순히 개인정보와 관련된 문제만을 초래하는 것은 아니다. 디지털 유산과도 연관이 되는 문제이다. 이에 대해서는 김원석, 정보통신서비스 이용자의 상호 디지털 유산 처리에 관한 연구, 서

클라우드 컴퓨팅 환경에서도 개인이 자신과 관련되어 클라우드 서비스 제공자의 서버에 남아있는 모든 자료를 지우고자 하는 경우에는 모두 지워질 수 있는 기술적 수단이 적용될 수 있도록 일관적인 제도화가 요구된다. 물론 이런 내용들은 현재 제정이 추진되고 있는 "클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안"에 반영되고 있다. 다만 이 경우에도 개인의 사망에 따른 개인정보 처리문제는 규정되어 있지 않은데, 이에 대한 규정도 도입될 필요성이 있다. 즉 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안에서 잊혀질 권리에 대한 내용들을 고려하여 클라우드 컴퓨팅 환경에 맞는 잊혀질 권리의 내용들이 보다 세밀히 규정되어야 할 것이다.

3) 망중립성

사실 망중립성은 명확히 사이버공간의 기본권이라고는 할 수 없다. 그러나 망중립성은 사이버공간에서 매우 중요한 가치임에는 틀림없다. 따라서 최근 망중립성과 관련된 논란들이 끊임없이 제기되고 있다.

망중립성이란 일반적으로 "모든 인터넷 트래픽이 동등하게 취급되어야 한다는 비차별성(non-discriminaltion) 원칙"을 의미한다.[79] 이와 같은 비차별성 원칙에는 "인터넷 접속사업자가 품질에 대한 고려 없이 도착한 순서대로 패킷을 처리하는 것"을 의미하는 절대적인 비차별성 개념과 "서비스품질 차등에 따른 추가요금수수를 인정하지 않는 범위 내에서 서비스품질 차등을 인정"하는 것과 "서비스 계약이 비배타적일 것을 전제로 서비스품질 차등에 따른 추가요금수수를 인정"하는 제한된 차별화 개념 등이 있다.[80] 그러나 망중립성을 보장하기 위한 원칙에는 이와 같은 비차별성 원칙 이외에도 전기통신사업자 상호간 서로의 요청에 의해 상호접속이 가능할 수 있도록 하는 상호접속, 모든 최종이용자가 다른 최종 이용자와 연결될 수 있어야 한다는 접근성 등 추가적인 원칙들이 있으

울과학기술대학교 석사학위논문, 2011년 참조.

79) 변재호/조은진, "망중립성 논의 최근 전개 동향", 전자통신동향분석 제25권 제4호, ETRI, 2010. 8, 122면.

80) 변재호/조은진, 앞의 책, 123면.

며, 이런 원칙 외에도 FCC는 4원칙, 6원칙 등 지속적인 원칙을 추가하고 있는 실정이다.[81]

이처럼 망중립성이 사이버공간에 중요한 이슈가 되는 것은 민간사업자의 트래픽 제어가 차별적인 정보의 유통을 유발하게 되고, 그로 인해 자유로운 사이버공간이 사익추구의 전장이 될 수 있는 위기감 때문이라고 할 수 있다.[82] 다만 망중립성에 대한 논란은 워낙 복잡한 문제들이 많이 얽혀 있기 때문에 쉽게 결론이 날 것 같지는 않다. 그러나 이처럼 복잡한 사안일수록 원칙으로 돌아갈 필요가 있다. 즉, 사이버공간이 열린 자유의 공간이라는 것이 바로 그것이다. 따라서 망중립성은 현대 사이버공간의 중요한 원칙이 될 수 있을 것이다.

제2절 사이버공간에서의 행위규제요소

사이버공간에서의 행위를 규제하는 요소에 관한 이론으로 가장 널리 사용되고 있는 것이 로렌스 레식의 소위 '행마법'이라고 하는 이론이라고 할 수 있다. 이에 따르면 사이버공간에서의 행위를 규제할 수 있는 요소로는 크게 법, 사회규범, 시장, 코드가 있다.[83] 물론 이 외에도 사이버공간에서 행위를 규제할 수 있는 요소들은 많다.

첫째로, 사이버공간에서 행위를 규제하는 가장 느슨한 형태의 요소로 사회규범을 들 수 있다. 가장 대표적인 것이 소위 네티즌들의 에티켓인 네티켓이라고 할 수 있다. 사이버공간은 대부분 문자, 사진, 동영상 등을 통해 의사소통이 이루어진다. 다만 최근 기술의 발달로 인해 이들은 이미 현실공간에서의 의사소통만큼이나 개인의 감정을 표출할 수 있게 되었다. 그런데 예를 들어 우리나라에서 아직까지도 많은 네티즌들이 사용하고 있는 카페의 경우 한 네티즌이 해당 카페의 성격과 다른 행동을 하게 되면 카페의 회원들은 그 회원에게 경고를 하거나 글 쓰는 것을 제한하는 것과 같은 제재를 가하게 된다. 따라서 해당 카페

81) 최승재, "경쟁법의 관점에서 본 망중립성에 대한 연구", 언론과 법 제10권 제2호, 2011, 372면.
82) 허진성, "헌법적 쟁점으로서의 망중립성", 언론과 법 제10권 제2호, 2011, 435면.
83) 로렌스 레식(김정오 옮김), 코드2.0, 2009, 253면 이하.

의 회원들은 공유될 수 있는 행동을 하게 되는 것이다.

둘째로, 사이버공간의 행위를 실제적으로 제한할 수 있는 것으로 시장이 있을 수 있다.[84] 가장 대표적인 예가 스마트폰의 데이터 제한 요금제라고 할 수 있다. 데이터 요금제가 정액제일 경우 사용자들은 무분별하게 데이터 트래픽을 유발할 수 있다. 그러나 한 달 동안 사용할 수 있는 데이터의 요금이 정해져 있고, 그 이상 데이터를 사용하면 추가적인 요금을 내야 할 경우 사용자는 제한된 트래픽만을 발생시키게 된다. 따라서 필요 없는 파일을 다운로드 하거나 업로드 하는 것을 하지 않을 것이며, 동영상이나 사진으로 의사소통을 하는 대신 문자를 통해 의사소통을 하게 되는 것이다. 또한 이와 관련해서 발생할 수 있는 문제가 앞에서 살펴본 망중립성과도 관련이 되어 있다. 따라서 시장이라는 요소는 사이버공간의 행위를 실질적으로 제한하는 요소이기도 하다.

셋째로, 국가권력이 작용할 수 있는 강력한 수단으로 법이 있다. 예를 들어 국가는 법을 제정하여 스팸행위를 제한하거나 포르노물의 유통을 금지하기도 한다. 특히 형법이라는 도구는 아직까지도 사람을 죽일 수도 있는 강력한 수단이므로 국가는 최후 수단으로 형법을 사용하기도 한다. 따라서 사이버공간에서 타인의 인격을 모독하는 경우 네티켓으로 해결할 수 있는 최선의 수단으로 가해자를 강제 탈퇴하는 방법이 고려될 수 있지만, 형벌이 사용될 경우 가해자의 자유를 빼앗을 수도 있다. 또한 법은 직·간접적으로 다른 요소들을 통제하는 역할도 한다.

그러나 앞의 수단들은 사이버공간의 기술지배적인 특성에는 무능력하게 된다. 따라서 사이버공간의 행동을 규제할 수 있는 가장 강력한 수단은 오히려 형벌보다도 코드라고 할 수 있다. 이는 마치 현실공간에서 과속을 막기 위해 과태료 규정을 두는 것이 아니라 과속방지턱을 설치하는 것과도 같은 것이다. 그러나 코드에 관한 문제는 아직까지 해결해야 할 과제가 많다. 이는 마치 과속방지턱을 만드는 것과 같이 국가가 코드를 제어하는 것이 적절하지 않을 수 있기 때문이다.

84) 필자는 이를 '시장' 대신 '자본'이라고 대체하였다; 이원상, Die Verhältnismäßigkeit im Cyberstrafrecht, 박사학위논문, 2010, 48면 이하.

그러나 어쨌든 사이버공간의 행위를 규제할 수 있는 요소들은 앞에서 언급한 바와 같이 네 가지 요소가 있을 수 있으며, 이들의 관계를 도식화 하면 다음과 같다.

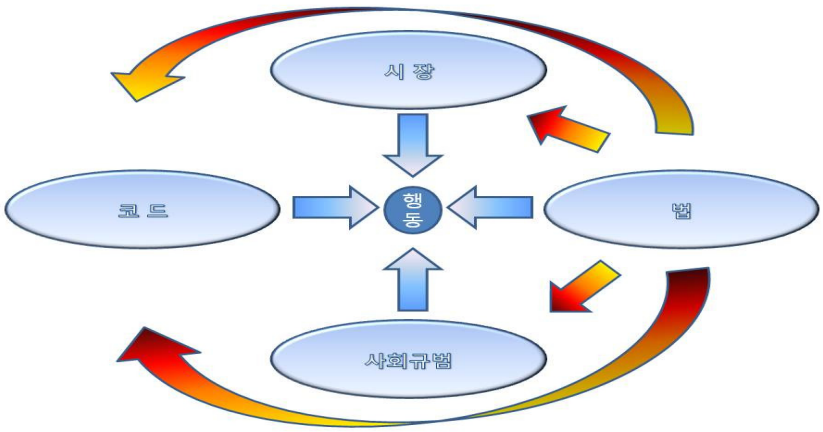


그림 1 사이버공간의 행위규제 모델

제3절 사이버범죄 관련 법률체계

1. 기본법 체계

사이버범죄는 기존의 범죄가 디지털화 된 것이라고 할 수도 있지만, 기존에는 없던 범죄가 새롭게 나타난 것이라고도 할 수 있다. 그러므로 사이버범죄를 단순히 디지털화된 범죄로 간주하여 현재와 같이 단순히 기존의 법률체계에 편입시키는 것은 문제라고 할 수 있다. 따라서 우리법 체계에서는 사이버범죄와 같이 기존의 법률체계에 편입시키기 어려운 사안들을 규정하기 위해 기본법이라는 체계를 가지고 있다. 우리나라는 일본의 기본법 법제형식을 계수하여 많은 법률에서 기본법이라는 명칭이 존재하고 있다. 우리나라 기본법의 모형이 되고 있는 일본의 경우 기본법이라는 명칭을 사용하는 경우로는 원자력기본법, 교육기본법

과 같이 의회가 형식적인 의미로 사용하는 경우, 법률의 성격상 특정 사안에 대해서 기본적인 대강이나 준칙, 원칙, 방침 등을 결정하는 경우(예로 형법을 범죄와 형벌을 규정한 법률들의 기본법이라고 함), 국가의 기본조직을 결정하는 법의 의미로 사용하는 경우 등이 있다. 마지막의 의미로 사용되고 있는 예로는 독일의 "독일연방공화국기본법"이 있으며, 이 경우의 기본법은 헌법과 동일한 의미를 가지게 된다.[85] 일본의 경우를 보면 앞의 두 의미를 혼합하는 형식으로 기본법의 개념을 사용하고 있기 때문에 형식적 의미의 기본법을 사용하며, 이 기본법에 마치 해당사항의 헌법과 같이 해당사항의 법 목적과 방침, 시책 등을 필요 최소한의 형식으로 입법하는 형식을 취하고 있다.[86]

이런 일본의 법제형태를 가지고 온 우리나라의 경우 기본법을 "정책입법, 프로그램법으로서의 기능과 성격을 가지는 독특한 입법형식, 즉 당해 정책의 이념이나 기본이 되는 사항을 정하고 그에 의거하여 시책을 추진하거나 제도의 정비를 도모하는 입법유형"[87]으로 이해하고 있다. 이런 가운데 기본법은 입법의 체계화 및 입법경제를 도모하여 특정 목적의 분야에 있어서 정책의 기본방향에 대한 정향성을 위해 기본개념, 정책추진 원칙 및 방향, 추진을 위한 조직, 추진방법 및 재원 확보방안 등을 규정하고 있다.[88]

하지만 실질적으로 우리법체계에서 기본법은 일본에서와는 사뭇 다른 지위를 갖게 된다. 기본적으로 우리나라에서 사용하는 기본법은 독일의 기본법과 같은 헌법적 규범은 아니다. 또한 일본의 경우와 같이 입법자들이 기본법이라는 형식적 개념을 사용하고, 이를 중심으로 관련 사안들에 대한 개별입법을 하고 있지도 않다. 결국 우리나라에서의 기본법은 개별법과 동일하게 취급되기 때문에 법의 일반적인 원칙, 즉 신법우선원칙, 특별법우선원칙 등이 적용되며 개별 법률과 동등한 위치를 갖고 있다.[89] 그럼에도 불구하고 기본법은 개별법률이 제정되지 않은 경우 및 규범이 흠결인 경우 이를 메워주는 법형성기능을 하기도 하며,

85) 이정훈, "입법체계상 기본법의 본질에 관한 연구", 법조 2009. 12, 276면 이하.
86) 이정훈, 앞의 글, 281면.
87) 박영도, 입법학입문, 한국법제연구원, 2008, 127면.
88) 황승흠, "기본법체제에 대한 법학적 이해", 공법학연구 제11권 제1호, 2010, 246면.
89) 이상돈, 전문법 - 이성의 지역화된 실현, 고려법학 제39호, 2002, 138면 이하.

개별법률 규정의 해석의 지침이 되는 해석적 통제기능, 개별법률들을 하나의 체계로 묶어주는 체계형성기능을 하고 있기도 하다.[90]

이런 관점에서 볼 때, 인터넷 기본법의 제정은 의미가 있다고 볼 수 있다. 다만 사이버공간과 관련된 경우 비록 기본법이라는 개념을 사용하고 있지는 않지만, 현재 "정보통신망 이용촉진 및 정보보호에 관한 법률(이하 "정보통신망법"이라고 함)"이 기본법으로서의 역할을 수행하고 있다고 볼 수 있다. 그렇기 때문에 인터넷 기본법과 정보통신망법과의 관계, 그리고 기타 관련 법률들과의 관계에서 과연 인터넷 기본법이 실질적인 기본법으로서의 역할을 수행할 수 있을지에 대한 부분을 고려할 필요가 있다.

2. 국제적인 차원에서의 사이버범죄 관련 규정 논의

가. UNODC의 사이버범죄 방지협약

1) 사이버범죄 정부간 전문가 회의

최근 유엔차원에서 사이버범죄에 대한 관심을 가지고 유럽 사이버범죄방지협정과 같은 전 세계적인 규범을 만들기 위한 노력이 계속되고 있다. 이는 초국가적인 사이버범죄의 특성상 한 국가의 형사사법체계가 이를 감당하는 것은 매우 어려운 측면이 있으며, 세계의 모든 국가들이 협력을 할 때 비로소 적절한 대응방법이 마련될 수 있다는 것을 인식하게 되었기 때문이다. 따라서 유엔 마약 및 범죄국(United Nations Office on Drugs and Crime; UNODC)은 소위 세계 사이버범죄방지협정을 만드는 작업을 시작했다. 특히 2010년 제12차 유엔 범죄방지 및 형사사법 총회(United Nations Congress on Crime Prevention and Criminal Justice)에서 사이버범죄에 대한 내용이 주요 내용으로 다루어졌으며, 그와 함께 유엔 범죄방지 및 형사사법 위원회(United Nations Crime Prevention and Criminal Justice Commission)에 사이버범죄 대응방안을 포괄적으로 연구하기 위

90) 이상돈, 앞의 글, 139면.

한 국제 사이버범죄 전문가 회의를 개최할 것을 요청하게 된다. 또한 살바도르 선언 제42조에서는 사이버범죄와 관련된 포괄적 연구가 수행되어야 할 것을 명시하였다. 따라서 2011년 1월 17일~21과 2013년 2월 23일~3월 3일에 걸쳐 국제 사이버범죄 전문가 회의가 오스트리아 비엔나에서 열리게 되었으며, 앞으로도 지속적으로 국제 사이버범죄 전문가들이 모여서 사이버범죄에 대한 여러 가지 문제점과 대안 등에 대해 논의할 예정이다.

2) 제1차 사이버범죄 정부간 전문가 회의의 주요 테마

2010년에 개최된 제1차 국제 사이버범죄 전문가 회의에서는 사이버범죄와 관련된 다양한 주제들에 대한 포괄적인 논의가 전개되었다. 제1차 국제 사이버범죄 전문가 회의에서 논의된 내용을 요약하면 다음과 같다.

① 주제 1 : 사이버범죄 현상(Phenomenon of cybercrime)
- 현행 법률 체계가 적용되는 범죄행위를 고려한 사이버범죄의 현상에 대한 분석
- 현재까지 범죄화 하지 않은 범죄행위의 조사 기록
- 피싱과 같은 복합적 범죄의 개요 및 앞으로의 동향
- 관련 사건의 조사기록
- 사이버범죄의 정의 및 유형
- 사이버범죄 예방 방법(기술적인 측면)
- 사이버범죄 정의의 중요성 연구
- 특정 사이버범죄 위법행위의 해결책으로 탈범죄화(비(非) 범죄화) 가능성과 관련한 연구

② 주제 2 : 통계정보(Statistical information)
- 사이버범죄의 확산 및 심각성에 대한 가장 최근의 통계, 조사 및 분석 수집
- 정책적 권고안을 위해 통계의 가치 평가
- 정확한 통계 수집의 방해요소 확인

- 사이버범죄 범법행위에 대한 통계를 수집한 국가 확인
- 사이버범죄에 대한 통계정보 수집의 필요성과 이점 평가
- 통계정보 수집에 이용할 수 있는 기술 평가
- 통계정보를 갖고 있는 중앙정보의 모델 논의

③ 주제 3 : 사이버범죄의 과제(Challenges of cybercrime)
- 사이버범죄 퇴치와 관련된 문제점에 대한 포괄적인 조사
- 이러한 문제를 해결함에 있어 기술과 법적 부문의 모범사례 요약

④ 주제 4 : 사이버범죄 법률에 대한 공동 접근 방식(Common approaches to legislation)
- 사이버범죄 관련법의 조화를 위한 현재 노력의 성공사례 및 제한 분석
- 국가들이 어떻게 지역기구의 법적기준을 시행하고 있는지에 관한 목록 수집 및 일관된 접근방식을 확보하는데 일조할 수 있는 기술을 결정하기 위한 분석
- 법적 표준의 차이가 국제공조에 미치는 영향의 범위에 대한 분석
- 조화를 이루는 과정에서 기본적인 법적 체계를 지켜나가는데 필요한 유연성을 보장하는 법률제정 기술 파악

⑤ 주제 5 : 사이버범죄 행위의 범죄화(Criminalization)
- 사이버범죄의 범죄화에 대한 국가적·지역적 접근 조사
- 범죄화의 모범사례 평가
- 사이버범죄 범죄화에 대한 관습법과 민사법 국가의 접근 차이 분석

⑥ 주제 6 : 수사절차(Procedural powers)
- 특정 사이버범죄 수사방법의 필요성을 잘 보여주는 사이버범죄 사건 수사의 예
- 지역적·국가적 법체계에 포함되어 있는 서로 다른 수사조항 연구
- 사이버범죄에 관한 특정 수사조항과 관련해 법집행기관의 현재 요구 개요
- 사이버범죄 관련 수사조항에 대한 관습법과 민사법 국가의 접근 차이 분석

⑦ 주제 7 : 국제협력(International cooperation)
- 사이버범죄 사건 관련 국제공조에 관한 문제점
- 사이버범죄 조사 및 기소와 관련이 있는 국제공조를 위한 조항 조사
- 양자 간 협약의 모범사례 조사
- 국제공조를 포함한 사이버범죄 사건 조사
- 정보공유와 같은 비공식 협력의 역할
- 국제공조와 관련해 관련 기관이 현재 필요로 하는 것에 대한 개요

⑧ 주제 8 : 전자증거(Electronic evidence)
- 전자증거의 취급 및 증거능력에 관한 조항 조사
- 국가 간의 전자증거와 관련한 일반 원칙의 접근 및 확인의 차이점 분석

⑨ 주제 9 : 인터넷 서비스 제공자 및 민간부문의 역할 및 책임(Roles and responsibilities of Internet service providers and the private sector)
- 서로 다른 형태의 인터넷 서비스 제공자를 구분해 인터넷 서비스 제공자의 책임을 규제하기 위한 접근방식 조사
- 인터넷 서비스 제공자의 책임 제한 개념
- 인터넷 서비스 제공자의 사법집행 지원 및 사이버범죄 예방 능력
- 민간부문의 사이버범죄 예방 및 수사 관련 모범사례 조사
- 민간부문 및 법집행기관의 요구
- 기존 접근방식의 장점 및 단점 평가

⑩ 주제 10 : 범죄방지 및 형사사법적 역량 및 사이버범죄에 대한 법률외적 대응(Crime prevention and criminal justice capabilities and other responses to cybercrime)
- 사이버범죄에 대응하기 위해 사용하는 법률 외적 접근방식 개요
- 이러한 접근의 성과를 측정할 수 있는 측정방법
- 서로 다른 법률외적 대응과 이러한 대응의 채택 가능성간의 관계 분석

⑪ 주제 11 : 국제기구(International organizations)
- 지역 및 국제기구의 모범사례 연구
- 기존 접근방식의 장점 및 단점
- 기존 국제적 법적 대응방법의 격차 분석

⑫ 주제 12 : 기술지원(Technical assistance)
- 사이버범죄 해결을 위한 기술지원의 기본 요소 및 원칙 파악
- 사이버범죄와 관련한 기술지원의 모범사례 파악

3) 제2차 사이버범죄 정부간 전문가 회의

제2차 사이버범죄 정부간 전문가 회의는 지난 제1차 회의에서 "사이버범죄의 현상 및 대응"이라는 주제 하에 논의되었던 내용들을 바탕으로 UNODC가 작성한 "사이버범죄에 관한 종합연구보고서 초안"(Comprehensive Study on Cybercrime · Draft)을 검토하고, 이를 바탕으로 보다 진전된 논의를 하기 위해 마련되었다. UNODC의 연구보고서에서는 사이버범죄에 관한 기존 국내 및 국제법 강화방안을 고찰해 보는 것과 함께 새로운 대응방안을 모색하기 위해 여러 나라의 법률을 검토하는 것, 그리고 사법제도, 기술지원 및 국제협력의 모범사례 등을 소개하고 있다.

UNODC의 연구보고서는 2011년 1월 제1차 회의에서 연구보고서의 주제 및 방법론에 대한 합의를 도출한 후 작성되기 시작하였다. 2012년 1월 UNODC가 지역그룹별 전문가들의 자문을 받아 설문지를 작성하였으며, 그에 대한 일부 수정과정을 거친 후 최종 승인되었다. 그리고 2012년 2월 6개 언어로 번역된 설문지가 회원국, 민간부문, 학술기관 및 정부기관 등으로 배포되어, 2012년 6월 69개 회원국, 40개 민간부문기관, 16개 학술기관 및 11개 정부기관이 제시된 기한 내에 자료를 제출받아 500여개의 open-source 문서에 대한 검토를 바탕으로 연구서 초안을 작성하게 되었다. 그리고 2012년 9월 연구서 초안에 대한 지역전문가들의 의견을 수렴한 후, 2013년 2월 완성된 연구보고서 초안을 제2차 전문가 회의에 앞서 회원국들에 배포하게 되었다.

이렇게 작성된 보고서는 회원국, 민간부문, 정부기관 등을 대상으로 한 설문조사 결과를 바탕으로 해서 제1차 회의에서 논의되었던 총 12개의 기본주제와 57개의 세부주제에 대해 상세하게 기술하고 있다. 다만, 특정한 결론이나 권고사항을 제시하는 대신 6개의 주요 연구 결과(key findings) 및 사이버범죄에 대한 새로운 국내·국제적 차원의 법적·법외적 대응을 강화하기 위한 4개의 옵션(possible options)을 제안하고 있는데 첫째는, 사이버범죄에 관한 국제적 모범규정(model provisions) 마련, 둘째는, 형사사건 관련 전자증거 수집 및 처리 등의 국제적 협력을 위한 다자간 협약 마련, 셋째는 사이버범죄에 관한 포괄적 다자간 협약 마련, 넷째는 개발도상국의 사이버범죄 예방 및 대응강화를 위한 기술지원 등이다.[91]

나. 유럽 사이버범죄방지협약

사이버범죄와 관련해서 국제적인 차원에서 규범력을 가지고 있는 것으로는 유럽 사이버범죄방지협약이 있다. 현재까지 사이버범죄와 관련된 협정가운데 가장 모범으로 평가되고 있는 것이 바로 유럽 사이버범죄방지협약이라고 할 수 있다. 다만, 앞에서 살펴본 UNODC 주도의 소위 세계 사이버범죄방지협약은 주로 중국과 러시아 등이 적극성을 띠고 있으며, 유럽이나 미국, 일본 등은 유럽 사이버범죄방지협약의 확장에 보다 관심을 가지고 있으므로 현재에는 서로 대립관계에 있다.

유럽 사이버범죄방지협약은 컴퓨터범죄 연구를 위해 구성된 '유럽 형사문제위원회(European Committe on Crime Problems)'가 '사이버공간에서의 범죄에 관한 전문가회의(Committee of Experts on Crime in Cyberspace)'를 설치하기로 결정하고, 이들이 1997년 4월부터 2000년 12월까지 다양한 논의를 거쳐 협정안을 구성함으로써 탄생하게 되었다. 이 후 2001년 6월 22일 최종안이 제50차 유럽 형사문제위원회의 승인을 받았고, 같은 해 11월 8일 각료위원회의 승인이후 11월 23일 헝가리의 부다페스트에서 가입절차가 개시되면서 본격적으로 가동되기

91) UNODC의 연구보고서는 현재 해당 홈페이지에서 다운을 받을 수 없는 상황이다. 추가적인 작업을 위해서 Draft를 내린 것으로 여겨진다.

시작하였다.[92]

유럽 사이버범죄방지협약은 전문과 총 4개장 48개 조문으로 구성되어 있다. 제1장에서는 주요 용어에 대한 정의를 내리고 있으며, 제2장 제1절에서는 사이버범죄에 대한 실체법적 규정들, 제2절에서는 전자증거에 대한 절차법적 규정들, 제3절에서는 관할권에 관한 규정들이 있다. 제3장에서는 국제법상 국제공조 및 범죄인 인도에 관한 규정이 있으며, 제4장은 조약의 가입, 발효, 유보 등에 대한 내용이 있다.

유럽 사이버범죄방지협약의 구조

- 전문

- 제1장 용어의 사용

  제1조 정의(컴퓨터 시스템, 컴퓨터 데이터, 서비스 제공자, 트래픽 데이터)

- 제2장 국가차원에서 취해질 수 있는 방법

제1절 형사실체법
  주제1: 컴퓨터데이터 및 시스템의 기밀성, 무결성 및 가용성에 대한 범죄
제2조 불법접속
제3조 불법감청
제4조 데이터방해
제5조 시스템방해
제6조 장치오용
  주제2: 컴퓨터 관련 범죄
제7조 컴퓨터 관련 위조
제8조 컴퓨터 관련 사기
  주제3: 콘텐츠 관련 범죄
제9조 아동포르노그래피 관련 범죄
  주제4: 저작권 및 저작인접권 침해에 관한 범죄
제10조 저작권 및 저작인접권 침해에 관한 범죄
  주제5: 종범의 책임과 처벌
제11조 미수, 방조 및 교사
제12조 법인의 책임
제13조 처벌 및 대응방안

제2절 절차법
  주제1: 일반규정
제14조 절차규정의 적용범위

92) 이영준/정완/금봉수, 사이버범죄방지조약에 관한 연구, 한국형사정책연구원, 2001, 8면 이하.

제43조 유보의 지위 및 철회
제44조 개정
제45조 논쟁의 해결
제46조 정당의 협의
제47조 폐기
제48조 통보

우리나라는 아직까지 유럽 사이버범죄 방지협약에 가입하고 있지는 않다. 다만 법무부에서는 동 협약에 가입하는 여부를 보다 적극적으로 검토하고 있다.[93] 비록 우리나라가 유럽 사이버범죄 방지협약에 가입하고 있지는 않지만, 이미 형법이나 정보통신망법 등에 상당수의 규정이 우리나라의 법률규정에 있다.[94] 또한 동 협약이 제정되던 당시인 2001년과 지금은 상당한 시간적 차이가 있어 동 협약은 현재의 상황을 온전히 반영하고 있지 못하다. 그러나 동 협약은 사이버범죄와 관련된 대표적인 협약으로 그 구조를 살펴 우리나라의 사이버범죄 관련 입법에 반영시킬 필요가 있다고 여겨진다.

우선 동 협약은 그 당시 중요한 범죄들의 실체법적인 내용을 담고 있다. 이는 주요 사이버범죄를 각 국가들이 공조하여 처벌할 수 있는 공통 처벌근거를 마련하는 작업이었다. 또한 디지털 증거와 관련된 규정 등 절차법적 규정도 담고 있다. 기존의 절차법 규정은 사이버공간을 고려하지 못하고 있기 때문에 사이버범죄에 적절한 절차규정이 담겨있지 못하다. 따라서 사이버범죄에 대한 절차규정은 새롭게 마련할 필요가 있다. 또한 사이버범죄와 관련해서 중요한 요소는 국제공조에 있다. 이는 사이버범죄가 초국가적 범죄로 국경을 넘나드는 범죄이기 때문에 한 국가의 사법이 작동하지 못하는 경우가 발생하기 때문이다. 이와 같이 동 협약은 그 당시의 사이버공간의 상황을 고려하여 다국적의 수많은 전문가들이 머리를 맞대고 만들어낸 결과이다. 그러므로 우리나라에서도 사이버범죄와 관련된 법령을 만드는 과정에 사이버범죄 전문가들이 참여할 필요가 있으며, 형사소송법 규정에 담기 어려운 사이버범죄 관련 절차규정들은 별도로 규정할 필요가 있다고 생각된다.

93) http://www.lawtimes.co.kr/LawNews/News/NewsContents.aspx?serial=61924&kind=AD 참조.
94) 이영준/정완/금봉수, 앞의 책, 169면 이하.

3. 중국에서의 사이버범죄 관련 법제 현황[95]

인터넷을 중국국민들이 이용하게 된지 불과 이십여 년의 시간밖에 되지 않았지만, 이는 사회발전의 운용방식과 사람들의 직장, 생활 및 사고방식에 큰 변화를 가져다주었다. 이는 의심할 바 없이 산업혁명 이후 인류사회 발전의 위대한 기술혁명이다. 인터넷의 광범위한 사용을 통하여 현대사회 경제의 더 빠른 발전과 인민들의 생활수준 향상, 그리고 생활방식의 편리함과 효율성에 대해 거대한 촉진작용을 발휘하고 있다는 점을 사람들은 체감하고 있고, 나아가서 그 영향이 한층 더 심화되고 광활한 영역까지 전개될 것으로 예상된다. 중국인터넷정보센터(中国互联网信息中心)가 2013년 1월에 발표한 〈제31차 중국인터넷발전현황통계보고(第31次中国互联网络发展情况统计报告)〉에 따르면, 2012년 12월 31일까지, 중국의 인터넷사용자수는 5.64억에 이르렀다고 한다. 현대사회에서도 인터넷은 수시로 어디서나 사람들의 생활에 영향을 주고 있고, 더구나 사람들의 사회생활의 각 방면에 깊이 침투되었다고 할 수 있다. 하지만 서방의 속담에서 말하듯이 매 하나의 동전은 정반대의 양면성이 있다. 인터넷의 밝은 전망의 배후에는 필연적으로 부정적인 악마가 숨어있을 것이다. 그리고 많은 부정적인 내용 중에 사람들에게 알려지고 가장 주목받는 면이 바로 사이버범죄이다.

사이버범죄라고 하면 대다수 사람들의 인상 속에는 아직도 형형색색의 사이버범죄 사건에 머물러 있다. 예를 들면, 2001년 4월 "중미해커대전(中美黑客大战)", 2007년 범람했던 "熊猫烧香案(인터넷 바이러스의 일종)", 2009년 5월의 "5·19 断网事件" 등이다. 하지만 인터넷범죄의 요지에 대해서는 항상 애매하고 한 마디로 표현하기 어려워한다. 물론, 이는 중국의 사이버환경 발전이 상대적으로 낙후한 현실과 연관이 있긴 하지만, 더 중요한 것은 중국의 사이버범죄 관련 법제가 상대적으로 낙후한 것과 관련된다. 현재 중국 학계에서도 아직 사이버범죄문제 연구의 토대가 되는 사이버범죄 개념에 대해서 여러 가지로 논의하고 있지만, 이에 대한 통일된 견해를 도출하지는 못하였다.

95) '중국에서의 사이버범죄 관련 법제 현황'과 관련한 내용은 공동연구자인 田宏杰 교수(中國人民大學校 法學院)가 책임집필한 '中国网络犯罪案例'를 가급적 원문에 가깝게 번역하여 소개하였다. 원문은 <부록 3> 참조.

가. 중국에서 사이버범죄의 의의

과학프로젝트의 연구에 있어서 첫 임무는 연구대상을 확정하는 것이다. 사이버범죄의 개념이 중국에서 사용된 이래 현재까지 20년의 시간밖에 되지 않았지만 중국내 전문학자들은 이 문제에 대해 대량적인 탐구를 거쳤고 일정한 연구성과를 기록하였음에도 불구하고, 양정명(杨正鸣), 피용(皮勇)이 말한 바와 같이 이 개념의 내연과 외연은 항상 불확실한 것이다. 그러므로 합리적으로 사이버범죄의 개념을 정하고 무엇이 사이버범죄인지를 명확히 하는 것은 이 문제를 연구함에 있어서 최우선으로 해결해야 하는 과제로 되어 있다.[96]

현재 중국 학술계에서 출판한 저작, 번역문, 논문을 보면 사이버범죄에 대한 개념사용은 모두 컴퓨터를 둘러싸고 전개된 것이다. 비교적 대표적인 관점을 살펴보면:

① 관점1: 사이버범죄의 행위주체(사람)는 컴퓨터 및 인터넷을 범죄도구로 혹은 공격대상으로 고의적으로 실시한 인터넷 안전을 위협하고, 인터넷자원을 침해하며, 타인 또는 사회를 위협하는 관련 법률규범에 저촉되는 행위이다.

② 관점2: 사이버범죄는 행위자가 사이버전문지식을 이용하여, 컴퓨터를 도구로 하여 사이버공간에 존재하는 정보를 침해하는 엄중한 사회를 위협하는 행위이다.

③ 관점3: 사이버범죄는 국가의 법률규정을 위반하고 정보기술을 이용하여 컴퓨터인터넷에서 진행되는 컴퓨터 정보교류를 방해하고 또는 사회를 엄중히 위협하며 법에 따라 형사책임을 져야하는 행위를 말한다.[97]

자세하게 살펴보면, 상술한 사이버범죄에 대한 정의는 모두 컴퓨터와 인터넷이 두개 키워드에 대한 서술에 의거하였고 컴퓨터범죄에 방점을 찍고 있다. 방

96) 皮勇, "网络犯罪比较研究", 중국인민공안대학출판사 2005년판.

97) 季境/张志超主编, "新型网络犯罪问题研究", 중국검찰출판사 2012년판.

법론에 따르면, 비슷하고 연관성 있는 개념에 대해 정의를 내리는 것에 있어서, 의사표현상 상호적으로 참고를 하는 것은 당연한 것이다. 다만 문제가 되는 것은 컴퓨터범죄의 개념에 의하여 형성된 사이버범죄의 개념은 사이버범죄의 본질적 특징을 표현할 수 없고 또한 양자 간의 관계를 분명히 하는 점에 있어서도 소홀한 점이 많다. 이로 하여금 컴퓨터범죄와 인터넷범죄에 대한 개념의 정의에 있어서 혼란이 있을 뿐더러, 국내학자들로 하여금 양자사이의 관계문제에 대하여도 장기적으로 논쟁하게 하였다.

사견으로는 컴퓨터범죄와 사이버범죄간의 관계를 정확하게 구분할 수 있는 것은 과학적으로 사이버범죄의 개념을 정할 수 있는 관건요소라고 생각한다.

1) 컴퓨터범죄(計算机犯罪)와 사이버범죄(网络犯罪)

양자 간의 관계문제에 대한 학계의 관점은 여러 가지로 나눌 수 있는데, 대체적으로 종합하면 아래와 같은 세 가지로 들 수 있다.

가) 동등설(等同說)

이 학설에 의하면, 사이버범죄는 컴퓨터범죄의 다른 표현일 뿐 사이버범죄의 본질은 여전히 컴퓨터범죄라고 한다.[98] 인터넷범죄의 실질에서 살펴보면, 이는 여전히 컴퓨터범죄의 일종으로서 사이버범죄는 필연적으로 인터넷공간에서 발생하는 것을 필요로 하지만 필연코 인터넷을 도구로 하는 것은 아니다. 인터넷 사용도구가 이미 컴퓨터에만 제한되어 있는 것이 아니라 이동통신도구(移动通信工具) 등도 인터넷에 접속할 수 있는 상황 하에서 행위자가 기타 다른 수단을 이용하여 인터넷 안전을 위협할 수 있다. 예컨대, 전자파를 발사하여 인터넷정보의 전달을 간섭하는 행위 역시 인터넷공간에서 발생하는 범죄이다.[99]

98) 刘守芬/孙晓芳, "论网络犯罪", 북경대학학보 2001년 제3기.

99) 冯卫国, "试论网络犯罪及其控制对策, 载赵秉志主编：《新千年刑法热点问题研究与适用》（上）", 중국검찰관출판사 2001년판.

나) 단계설(阶段说)

이 학설에 지지하는 학자들은, 컴퓨터인터넷과 컴퓨터시스템은 개념의 외연상(外延上) 상호적으로 교차되지만 컴퓨터정보시스템은 인터넷을 포함하지 않으므로 컴퓨터인터넷을 통해 조성된 컴퓨터정보시스템은 이의 고급형식이라고 주장하고 있다. 구체적으로 말하면 사이버범죄란 행위주체가 컴퓨터 또는 컴퓨터인터넷을 범죄도구로 혹은 공격대상으로 하는, 고의적으로 실시하는 인터넷안전을 위협하고 법률규범에 저촉되는 행위이다.[100]

다) 인터넷정보설(网络信息说)

이 학설에 의하면, 사이버범죄란 행위자가 인터넷 전문지식을 이용하여 컴퓨터를 도구로 인터넷 공간에 있는 정보를 침범하는 엄중히 사회를 해치고 있는 행위라고 인정하고 있다.[101]

사실 시간의 흐름 속에서 컴퓨터와 인터넷의 발전역사에 대해 자세히 살펴보면, 중국의 컴퓨터범죄와 인터넷범죄 간의 관계가 수면에 떠오르게 될 것이다. 즉, 1956년, 하배수(夏培劳)가 처음으로 전자컴퓨터운산기(电子计算机运算器)와 제어기(控制器)에 대한 설계를 하여 중국에서의 최초의 컴퓨터가 탄생하게 되었다. 그 후 20년의 시간동안 전자컴퓨터는 주로 계산(计算), 뉴스(新闻) 및 금융(金融) 등 각 영역에서 운용되었다.

1986년, 중국에서 첫 컴퓨터범죄사건을 해명(破获)하였다(컴퓨터를 이용하여 횡령(贪污)한 사건). 1987년, 중국에서 처음으로 이메일 노드(节点)를 건립하고 전 세계에 성공적으로 첫 메일을 보냈다. 그 후 중국은 끊임없이 컴퓨터 인터넷의 연구와 개발을 진행하였다. 1994년, 중국은 정식으로 국제인터넷(国际互联网)에 가입하였다. 1996년, 우리나라는 처음으로 사이버범죄사건을 해명하였다(컴퓨터바이러스(计算机病毒)를 제작한 사건).

중국 컴퓨터 인터넷의 발전으로부터 이와 같은 결론을 얻을 수 있다. 중국에

100) 范德繁/于宏, "针对网络犯罪之认定探讨--兼评刑法相应立法的完善", 법제여사회발전 2001년 제5기.
101) 皮勇, "网络犯罪比较研究", 중국 인민공안대학출판사 2005년판.

서는 컴퓨터가 먼저 생산되고 인터넷이 그 뒤를 이어 생산되었는데 컴퓨터범죄는 컴퓨터가 생산되고 인터넷이 생산되기 전에 이미 나타나기 시작하였고 사이버범죄는 인터넷이 생산된 후에야 나타났다.

저자는 중국의 컴퓨터범죄와 사이버범죄에 대한 개념은 중국의 컴퓨터 및 인터넷의 발전적 맥락과 관련되어 있고 중국의 특성이 내재되어 있다고 생각한다. 또한 양자 사이의 관계를 해명하기 위해서는 우선 이를 세 가지 단계로 나누어서 고찰해야 한다고 생각된다.

제1단계: 컴퓨터 시대(1950년대로부터 1980년대 초까지). 중국은 이 단계에서 인터넷이 아직 확실하게 나타나지 않았다. 당시에는 단일 컴퓨터범죄 또는 컴퓨터시스템 범죄가 주요하게 발생하였다. 저자는 이를 단순 컴퓨터범죄라 정의하되, 이는 좁은 의미상의 컴퓨터 범죄이다.

제2단계: 컴퓨터 인터넷 시대(1980년대 후반부터 1990년대 초까지). 이 단계에서 중국은 공식적으로 국제 인터넷에 가입하여 인터넷과 컴퓨터를 결합하여 컴퓨터 인터넷 시스템을 형성하였다. 이런 결합 모드에서 인터넷의 작용이 충분히 부각되지는 않았지만 컴퓨터의 기본적 지위는 공고히 자리 잡고 있었다. 이 단계는 제1단계의 인터넷이 가입되지 않은 단순 컴퓨터범죄가 존재할 뿐만 아니라 컴퓨터를 도구로 삼아 인터넷정보 및 사이버안전(网络安全)을 겨누는 범죄, 즉 실질상의 사이버 범죄도 나타났다. 그러나 이 단계에서 컴퓨터 및 인터넷의 대응관계가 사람들로 하여금 습관적으로 컴퓨터 범죄의 의미를 확장하여 모든 범죄를 컴퓨터 범죄로 일괄하였다. 이 시점의 컴퓨터 범죄는 넓은 의미로서의 컴퓨터 범죄이고 컴퓨터 범죄는 사이버 범죄를 포함하고 있다고 설명할 수 있다. 물론, 몇몇 학자들은 시대에 부응하여 발전추세를 정확히 추측하고 컴퓨터범죄 및 사이버범죄의 다른 점을 예리하게 주시하였지만 이 단계에서 주류 관점으로 형성되지 못하였다.

삼자의 관계는 아래의 그림과 같다. 큰 원은 컴퓨터인터넷시대의 모든 범죄 즉 넓은 의미에서의 컴퓨터범죄이고 작은 원은 단순 컴퓨터범죄, 작은 원 이외의 부분은 사이버 범죄이다.

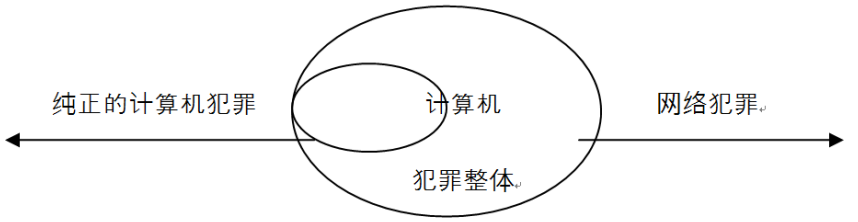


그림 2 삼자의 관계

제3단계: 인터넷 시대(1990년대 후반부터 현재까지). 이 시대에 인터넷이 정보시대의 중심이 되고 인터넷 단말기의 다양화와 컴퓨터, 스마트폰, 스마트TV 등 많은 스마트 인터넷단말기가 용솟음쳐 나왔으며 더구나 휴대폰은 컴퓨터를 대체하여 가장 큰 인터넷단말기가 되었다. 이 단계에서 인터넷은 위 단계에서 반드시 컴퓨터와 연결되어야 하는 점을 벗어나 진정으로 정보의 중심이 되었다. 컴퓨터는 단지 인터넷단말기로서의 도구 중 하나로 존재하게 되었다. 이 시기에 단순 컴퓨터 범죄의 발생은 날이 갈수록 미미해졌다. 관련 통계자료에 따르면 2000년 이후 컴퓨터인터넷 분야에서 사이버 범죄는 점차 90%를 초과하였고, 단순 컴퓨터 범죄는 10%보다도 훨씬 적었다. 학자들은 컴퓨터 범죄와 사이버 범죄의 근본적인 차이를 깊이 인식하였다. 컴퓨터 범죄는 점차적으로 사이버 범죄로 대체되고 있고 컴퓨터 범죄란 개념도 더 이상 이 단계의 모든 범죄형식을 포괄하지 못하였다.[102] 따라서 이 단계에서의 컴퓨터 범죄는 사이버 범죄와[103] 병행관계를 이루며 양자를 공동으로 컴퓨터 사이버범죄라고 지칭할 수 있었다고 저자는 생각한다.

102) 许秀中, "网络与网络犯罪", 중신출판사 2003년판.
103) 许秀中, "网络与网络犯罪", 중신출판사 2003년판.

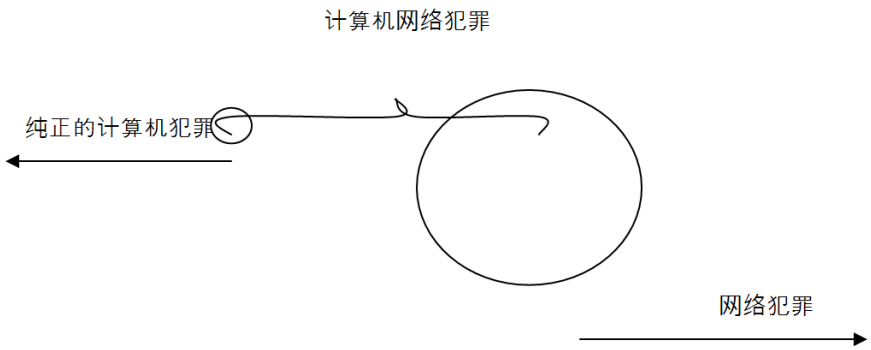


그림 3 삼자의 관계 2

이로부터 컴퓨터와 인터넷이 발전한 선후순서에 따라 다른 발전단계를 보여주고 있다는 것을 알 수 있다. 제1단계에서는 단순 컴퓨터범죄만 존재하였고 사이버범죄는 존재하지 않았다. 제2단계에서는 컴퓨터와 인터넷 사이의 밀접한 관계에 기반하여 사이버 범죄는 컴퓨터개념의 일종으로 개괄할 수 있었으며, 양자는 포함관계에 있다. 그리고 현재(제3단계)는 인터넷의 주체적 지위가 부각되었고, 컴퓨터 범죄의 개념은 더 이상 사이버범죄를 포함할 수 없게 되었다. 그리하여 현재 우리가 말하는 컴퓨터범죄는 단순 컴퓨터 범죄라는 좁은 범위로 돌아가고 사이버 범죄는 컴퓨터 범죄와 상호 포함될 수 없는 개념으로 되었다. 양자는 나타난 시간과 단계 특성 및 침해한 대상이 다름에 따라 분명한 차이를 갖고 있다.

구체적으로 말하자면 단순 컴퓨터범죄와 사이버범죄 사이의 차이는 주요하게 아래와 같다.

첫째, 발생한 시간이 다르다. 컴퓨터 범죄가 먼저 나타났고 사이버 범죄가 후에 나타났다. 위에서 상세하게 서술한 바가 있다.

둘째, 단계특성이 다르다. 컴퓨터범죄 시대에는 컴퓨터와 인터넷의 결합을 요하지만, 컴퓨터는 항상 중심적 위치에 있었다. 하지만 사이버범죄 시대에는 컴퓨터가 점차적으로 많은 인터넷 단말기의 하나로 진화되어 인터넷이 진정한 데

이터정보(数据信息)의 중심으로 되기 시작하였다.

셋째, 침해대상이 다르다. 컴퓨터 범죄의 침해대상은 컴퓨터 및 단일시스템이라는 특정성을 갖고 있다. 하지만 사이버 범죄의 침해대상은 인터넷 데이터정보로서 광범성을 띠고 있다. 발전단계로부터 볼 때 모든 인터넷에 접속한 컴퓨터가 사이버 범죄의 침해대상이 되는 것은 아니다. 인터넷 데이터정보에 간섭하지 않는 범죄는 단순 컴퓨터 범죄라고 볼 수 있다.

넷째, 위해성이 다르다. 위에서 서술한 컴퓨터 범죄의 특정성과 사이버 범죄의 광범성에서 알 수 있듯이 사이버범죄가 사회에 미치는 해가 더 심각하다.

다섯째, 범죄 비율이 다르다. 제1단계에서는 100% 컴퓨터 범죄였다면 제2단계에서는 컴퓨터 범죄의 비율이 날이 갈수록 줄어들었고, 제3단계에서의 컴퓨터 범죄의 발생량은 극히 미미했으며 사이버 범죄가 거의 모든 비율을 차지하고 있었다.

결론적으로 말하자면, 저자의 관점이 아직 많이 미숙하고 더 완벽하게 해야 할 필요가 있기는 하지만, 이렇게 단계를 나누어 해석하는 방법만이 우리로 하여금 전면적으로 컴퓨터범죄와 사이버범죄의 발전과정 및 양자 간의 관계문제를 분석할 수 있게 한다고 생각한다. 오직 이렇게 해야만 현재 사이버범죄의 과학적인 정의를 위하여 명확한 사고법과 접근방법을 제공할 수 있다고 생각한다.

나. 중국에서 사이버 범죄의 개념 및 본질적 특성

1) 사이버 범죄의 개념

현재 중국은 사이버범죄의 개념에 대해 여러 가지 학설이 존재하고 있는데, 기본적으로 6가지 유형으로 요약할 수 있다:

① 상관설(相关说)

중국 정법대학교 정보기술입법태스크포스(中国政法大学信息技术立法探讨课题组)는 사이버범죄는 컴퓨터범죄와 관련이 있는 범죄라고 주장하고 있다.

② 도구이용설(工具利用说)

컴퓨터나 컴퓨터지식을 이용하여 범죄목적을 이루는 행위이다.[104]

③ 대상데이터설(对象数据说)

컴퓨터시스템을 이용하여 비법조작 혹은 기타 수단으로 컴퓨터시스템내부의 데이터 안전완전성 혹은 시스템정상성에 위협을 가져다주는 행위이다.[105]

④ 도구대상설(工具对象说)

중국공안부컴퓨터관리감시사(中国公安部计算机管理监察司)에서 제출한 바에 의하면 사이버범죄는 컴퓨터를 도구로 하고 컴퓨터재산을 대상으로 실시하는 범죄이다.[106]

⑤ 절충설(折中说)

조병지(赵秉志)는 사이버범죄는 컴퓨터조작을 이용하여 실시하는 컴퓨터인터넷 시스템안전을 해치는 범죄라고 정의를 내리고 있다.[107]

⑥ 중국 형법에서 컴퓨터인터넷범죄에 관한 정의

개괄하여 말하면 행위자가 불법적으로 컴퓨터정보시스템에 침입하고 형법을 위반하는 범죄행위이며, 컴퓨터를 이용하여 실시하는 전통적인 범죄행위이다.

상술한 두 가지 사이버범죄의 본질에 관한 연구는 아직 컴퓨터와 사이버범죄의 관계에 얽매여 있고 심지어 정도에 따라 양자를 혼동하여 그 개념을 정의하고 있어 사이버범죄의 본질에 대한 연구를 소홀히 하였다. 이밖에 범죄학상의 사이버범죄의 개념과 규범형법 의의상의 사이버범죄의 개념을 아직 구별하지 못하고 있는 상황이다.

104) 刘江彬, “计算机法律概论”, 북경대학출판사 1992년판.

105) 孙铁成, “计算机与法律”, 법률출판사 1998년판.

106) 中华人民共和国计算机管理监察司, “计算机安全必读”, 군중출판사 1991년판.

107) 转引自许秀中, “网络与网络犯罪”, 중신출판사 2003년판.

상술한 컴퓨터범죄 및 사이버범죄관계의 해석에 따라 저자는 현 단계에서 인터넷은 현대사회의 진정한 정보중심이라고 인정한다. 개인, 조직 또는 정부에 대해서도 인터넷은 정보자원을 얻을 수 있는 제일 중요한 통로이다. 사람들은 인터넷을 통하여 정보를 공유, 전달, 수집하고 인터넷은 정보유통의 중요한 매체이다. 사이버범죄도 필연적으로 인터넷데이터정보와 인터넷안전에 대한 침해와 위협에서 주로 구현된다. 그러므로 범죄학과 사회학적 의미에서 보면, 인터넷데이터정보의 불법전달, 절취, 수정 및 기타 인터넷 안전에 위협을 줄 수 있는, 개인, 사회와 국가이익에 위협하는 행위는 모두 사이버범죄라고 정의를 내릴 수 있다.

유감스러운 것은, 우리나라 1997년 형법개정시, 학계에서 컴퓨터범죄 및 인터넷범죄에 대한 연구가 아직 깊지 못하여 양자 사이의 관계가 아직 불확실하였기 때문에 1997년 형법도 제286조, 제287조 두 개 조항에서만 이에 상응한 규정을 가하였으며, 학계에서는 이를 컴퓨터범죄라고 부르고 있다. 엄격하게 말하자면, 우리나라에는 형법상의 사이버범죄에 대한 규정은 없지만 실질적으로 사이버 범죄가 존재하고 있다. 이는 상술한 규정에 따르면 소량의 순수한 컴퓨터 범죄 외에는 다수가 모두 사이버범죄에 속한다.

2) 사이버범죄의 특징

사이버범죄와 컴퓨터범죄의 차이는 이미 상술하여 비교를 하였다. 사이버범죄는 전통범죄와 비교하여 볼 때 아래와 같은 선명한 특징이 있다 .

가) 데이터정보성(數据信息性)

인터넷은 물리설비가 일정한 방식에 따라 연결되어 형성된 하나의 정보공간이다. 이는 이해할 수 없지만 상상할 수 있는 사이버세계로서 이 세계에는 각종 신호와 데이터로 가득 차있고 사람들이 데이터를 공유, 수집, 전달하는 중요한 매체이다. 인터넷이 처리하고 있는 것은 정보이고 정보가 없으면 인터넷이 없다. 그러므로 인터넷을 침범하는 인터넷범죄는 필연적으로 인터넷데이터정보와 인터넷운행환경에 대한 침해로 표현된다. 한편으로 사이버범죄는 반드시 정보에 의

거해야 실현할 수 있고, 다른 한편으로는 인터넷이 침해하는 대상도 역시 정보이다. 예를 들면 인터넷뱅킹계좌(网上银行账户), 인터넷전자저작권(网络电子版权) 등에 침해를 가할 경우 사이버범죄가 될 수 있지만, 만약에 정보침해의 특징이 없다면 여전히 전통범죄에 속한다. 이는 사이버범죄의 제일 본질적인 특징이고 또한 사이버범죄와 컴퓨터범죄의 제일 본질적인 구별점이다.

나) 위해확산성(危害擴散性)

인터넷의 공개, 자유성으로 인해 사이버범죄가 위해영역이나, 위해대상, 위해결과 등 많은 방면에서 확산성을 소재하고 있다. 위해의 확산성은 위해성을 더 크게 유도한다.

다) 공간의 사이버성(虛擬性)

비록 인터넷은 광케이블(光缆), 위성전송(卫星传送) 등 물질방식으로 연결되어 형성되었지만, 인터넷은 이로 인해 하나의 사이버데이터공간을 형성하였다. 이 공간 내에서 세계는 몇 초의 거리로 축소되었고, 범죄행위도 순식간에 실행될 수 있어 범죄의 물리적과정재현은 아주 어렵게 되었다.

라) 방법의 지능성(智能性)

전통범죄와 달리 사이버범죄의 범죄행위자는 일반적으로 일정한 문화수준과 기술수준을 가지고 있고 범죄방법에서 일정한 지능특징을 표현하였다.

마) 다국적 지역성(地域跨國性)

인터넷은 시간과 공간을 압축하는 특징이 있어 각양각색의 정보가 인터넷을 통해 발송되었을 경우, 국계와 지리적 거리는 잠시 없어진다고 할 수 있다. 이는 범죄자에게 다지역과 다국적범죄의 실시에 가능성을 제공하였다. 범죄자들은 단 한대의 단말기만 있으면 인터넷을 통하여 여느 지역에 대한 범죄의 실행이 가능하게 되었다. 그러므로 사이버 범죄는 강한 섭외특징을 보여준다.

위에서 서술한 두 차례 비교를 통해, 사이버범죄, 컴퓨터범죄와 전통범죄에 대한 구별점을 명확히 하였고, 각자의 특징, 성격과 내용에 대해 이해를 가할 수 있었다고 생각한다.

다. 중국에서 사이버범죄의 현황

이 문제에 대해 서술하기 전에 꼭 지적해야 하는 것은 바로 학계와 실무계의 컴퓨터범죄와 사이버범죄에 대한 연구가 혼란상태에 처해있기에, 이의 상황을 연구하는데 정확한 사이버범죄의 데이터를 찾는 것이 매우 어렵다는 것이다. 현재 중국의 조사통계의 대부분수치는 인터넷 불법범죄의 총체적수치 혹은 컴퓨터범죄와 사이버범죄의 총체적 수치이다. 그러므로 저자는 오로지 위의 수치에 대한 기초분석을 통하여 우리나라 사이버범죄의 현재 상황을 알아 낼 수 있다. 이론 및 실무계에서 전문적인 사이버범죄의 수치를 빠른 속도로 수집하고 정리하는 것이 연구를 진행함에 있어서 우선적으로 해야 할 일이라고 생각된다.

1) 수량(數量)과 증폭(漲幅)

《제31차중국인터넷발전상황통계리포트》(第31次中国互联网络发展情况统计报告)에 의하면 중국의 컴퓨터수량 및 인터넷사용인구수의 증폭이 세계의 앞자리를 차지하고 있다는 것을 알 수 있다. 중국에서의 인터넷의 쾌속한 발전으로 인하여 그와 관련된 범죄도 급속히 늘어나고 나날이 심각해지고 있다.

중국공안기관(中国警察机关)의 통계에 의하면, 1999년 공안기관에 인터넷불법범죄사건수사가 진행되게 된 안건은 단지 400여건, 2000년은 2700여건으로 증가하였고, 2001년에는 4500여건에 달하였는데 그중 90%이상이 인터넷에 관한 인터넷 불법범죄사건이다.[108]

공안부 인터넷안전보위국의 유관 책임자의 소개에 의하면 2008년부터 시작하여 중국 사이버범죄의 수량은 매년 30%의 빠른 속도로 증가하고 있으며 이후 장시간 내에도 사이버범죄가 계속 증가하는 추세일 것이라고 판단하였다.[109]

108) 赵秉志, "中国网络犯罪现状", 중국형사법치망, 2007년 2월 2일.

중국공안인민대학경무개혁과 발전연구중심(中国公安人民大学警务改革与发展研究中心)에서 발표한《2012년 중국인터넷위법범죄문제 연간리포트》(2012年中国互联网违法犯罪问题年度报告)에서 보듯이 2012년 우리나라 사이버범죄는 발생확률이 크고 피해자의 규모 및 관련금액도 매우 거대하다고 할 수 있다. 2011년 7월 초부터 2012년 7월 중순까지만 하여도 중국에서는 약 2.57억 명의 사이버범죄피해자와 2,890억 위안의 경제손실을 입었다. 같은 시기에 사이버범죄의 침해를 받은 온라인 성인 인터넷 사용자만 하여도 72%나 되었고, 즉 매일 70만 명을 넘는 중국 인터넷 사용자가 사이버범죄의 침해를 받고 있으며, 평균적으로 매분 489명의 피해자가 있고, 피해자별 평균손실액이 위안으로 1,126위안에 달한다.[110]

통계기준의 차이에 따라 위의 수치와 중국 사이버범죄의 진실한 상황 사이에는 약간의 차이가 있지만 위의 자료에 따르면 중국의 사이버범죄의 범죄수량이나 증가폭은 아직도 증가하는 추세를 나타내고 있으며 위협적이라는 것을 알 수 있다.

2) 분포현황(分布状况)

이론분석과 사법데이터(司法数据)에 근거하여 우리나라 현재의 사이버범죄의 집중분포 영역은 아래와 같다고 본다.

가) 컴퓨터바이러스범죄(计算机病毒犯罪)

컴퓨터바이러스범죄는 컴퓨터프로그램 속에 침입하여 컴퓨터기능 또는 데이터를 파괴함으로써 컴퓨터사용의 지령(指令) 혹은 프로그램코드(程序代码)에 영향을 준다. 우리나라 컴퓨터 바이러스범죄는 신속히 성장하는 추세를 보이고 있다.

나) 컴퓨터시스템불법침입범죄(非法侵入计算机系统犯罪)

컴퓨터시스템불법침입범죄란 통속적으로 말하면 해킹범죄(黑客犯罪)라고도 말

109) http://www.sina.com.cn 참조.

110) 《2012년 중국 호련망 위법범죄문제 연도보고》.

할 수 있다. 이런 범죄는 우리나라에서 가끔 발생하는데 피해자가 많다.

다) 인터넷사기·도난·횡령 등 범죄(网络詐騙、盗窃、貪污賄賂等犯罪)

이런 유형의 범죄는 위의 자료에서 표시한 바 있고, 이를 전통범죄와 구별하였기에 여기에서는 설명을 더 하지 않기로 한다.

라) 온라인 지적재산권 침해범죄(网上侵犯知識産權犯罪)

반세기에 달하여 빛, 전기 및 컴퓨터 등의 새로운 기술의 발전은 지적재산권의 침해범죄에 유리한 조건을 제공하였으며 근본적으로 지적재산권법의 많은 개념에 변화를 가져다주었다.

마) 인터넷도박(网絡賭博), 음란범죄(色情犯罪)의 범람(泛濫)

음란과 도박도 인터넷 등의 과학기술의 발전을 통하여 정보범죄의 이름을 걸고 날이 갈수록 범람하고 있다.

위에서 예로 열거한 것은 사이버범죄의 전부가 아니라 그중에서 빈번하게 발생하고 있는 일부분에 불과하다. 컴퓨터 및 인터넷의 광범위한 분포에 따라 사이버범죄도 날이 갈수록 새로운 분포상태를 나타낼 것이다.

라. 중국 사이버범죄의 발전추세

많은 전문학자들은 중국 사이버범죄의 현재 상황을 기초로 자세한 관찰과 사고를 통하여 중국 사이버범죄의 미래발전 추세에 대해 예측하고 있다. 앞에서 소명한 《2012년중국인터넷위법범죄문제년간리포트》(2012年中国互联网违法犯罪问题年度报告)에 의해 저자는, 미래중국의 사이버범죄는 다음과 같은 발전추세를 보일 것이라고 생각한다.

1) 범죄주체의 저연령화(低齡化) 심화(更加)

최근의 사이버범죄를 보면, 저연령화의 추세가 아주 선명해지고 있다. 2012년을 예로 든다면 호북성(湖北省)에서의 사이버범죄 사건에서는 30세 이하의 범죄자가 90%를 차지하였다고 한다. 서주(徐州)에서의 사이버범죄 사건에서도 90년생의 범죄자수가 절반 이상을 차지하였다고 한다. 의심할 바가 없이 청소년들이 인터넷을 접촉하는 시기가 너무 빠르고 또한 학교에서의 컴퓨터 및 인터넷지식 교육이 보편화됨에 따라 인터넷기술에 숙달한 미성년자들이 늘어나고 있기에 사이버범죄의 주체의 저연령화 추세도 피하기 어렵다고 본다.

2) 범죄주체의 대중화 심화

중국 교육방식의 개혁을 통하여 인터넷교육, 원격교육 등 여러 가지 지식획득의 경로가 부단히 발전되어 왔지만, 컴퓨터 교육의 조기화와 보편화로 인하여 많은 대중들이 인터넷과 컴퓨터를 접촉하고 날로 익숙해져 가고 있기에 컴퓨터, 인터넷 기술은 더 이상 사람들이 바라만 보는 첨단기술이 아니라 점차적으로 사람들이 생존하고 생활함에 있어서 필요한 기능 중의 하나가 되어버렸다. 그러므로 미래의 사이버범죄는 초기의 사이버범죄의 주체의 영재화(精英化)와 다르기에 더욱 더 사회화되고 대중화될 것이다.

3) 범죄의 산업화와 집단화

최근에 발전을 통하여 인터넷분자(网络分子们)는 점점 더 완벽한 산업을 형성하였을 뿐만 아니라 범죄사슬의 매개 고리에서 분업(分工)이 명확하고 서로 배합(配合)하며 기능의 부단한 세밀화로 인하여 구조가 엄밀하고 거대한 범죄조직을 형성하였다. 최종적으로 사이버범죄는 더욱 더 산업화와 집단화로 나아갈 것이며 사회에 대한 위협은 더욱 엄중해질 것이다.

4) 새로운 형식의 사이버범죄 출현

시만텍(赛门铁克)이 24개 나라와 지구의 13,000명의 성인에 대해 조사를 한 결

과 새로운 형식의 사이버범죄는 점차적으로 여러 가지 모바일네트워크기술로 전이하고 있다는 것을 발견하였다. 이것 또한 사이버범죄중에서 컴퓨터가 전반을 통제할 수 없으며, 과학기술의 진보와 발전에 따라 여라 가지 새로운 형식의 사이버범죄시스템이 계속 나타날 것임을 의미한다.

5) 전통범죄의 점차적인 인터넷화(网络化)

사이버범죄의 발생 초기에는 일부 새로운 형식의 범죄와 소수의 특정된 영역에만 보편적으로 집중되었고, 전통범죄 영역에는 상대적으로 적게 집중되었다. 사회와 기술이 발전함에 따라 이런 현상은 사라졌고 전통범죄도 점점 인터넷화로 나아가고 있으며, 즉 사이버범죄가 점점 전통영역으로 침투해 들어가고 있다는 것을 알 수 있다.

6) 다국적 범죄현상(犯罪跨國化)의 가속화

국제교류협력이 날로 빈번하고 국민의 생존과 발전영역이 부단히 확장되면서 현실세계의 변화는 어느 정도의 사이버세계를 반영할 수 있다. 더욱이 국경을 넘어선 인터넷은 물리공간의 제한이 없어 사이버범죄는 필연적으로 다국적 방향으로 발전할 것이며, 국경을 넘어선 범죄가 부단히 많아질 것이다.

7) 인터넷 자체가 범죄를 제지하는 유리한 요소로 되고 있음

인터넷이 생기면서 사이버범죄는 시작되었다. 인터넷의 발전이 사이버범죄의 발생을 촉진하였다 하지만 인터넷 주요 문화의 형성으로 인터넷 안전방어 체계도 날로 개선되고 있기에 인터넷 자체도 사이버범죄를 억제하는 중요한 힘이 될 것이다.[111]

사이버범죄가 미래에도 날로 늘어날 수 있다. 새로운 기술과 새로운 상품들이 많이 나오고 인터넷서비스도 보편적으로 편리하게 될 것이며 인터넷 주요 문화

111) 孙景仙/安永勇, "网络犯罪研究", 지식산권출판사 2006년판.

의 형성도 법률규범을 통해 개선하고 있지만, 많은 요소들로 하여 사이버범죄의 새로운 추세가 나타날 수도 있다. 오직 사이버범죄 실제상황을 파악하는 기초에서 미래의 사이버범죄에 대해 열심히 사고하고 사이버범죄의 미래의 발전추세를 인식하여야만 미래의 사이버범죄가 법에 의해 처리될 수 있을 것이다.

바. 중국에서 사이버범죄의 원인

사이버범죄를 연구함에 있어서 중점은 사이버범죄의 예방에 있다. 위의 사이버범죄의 개념에 대한 정의나 현재 상황 및 발전추세의 탐구는 모두 범죄의 원인을 찾기 위해서이며, 예방대책을 탐색하기 위해서는 그 원인을 정확하게 알아내야 한다.

알다시피 사이버범죄의 원인은 아주 복잡하고 거대한 시스템인 바, 범죄결과의 발생은 시스템 내부의 수많은 범죄요소들로 하여금 서로 작용하고 서로 영향을 주는 복잡한 과정의 산물이다. 비록 구체적 범죄 중에서 다른 원인이 발생하는 작용도 다르겠지만 우리가 사이버범죄를 하나의 총체로 생각하고 종합연구를 진행하였을 때 매개의 원인들은 모두 없어서는 안 되는 각자의 의미와 가치를 가지고 있다.

1) 경제원인(經濟原因)

경제원인면에서 중요한 3가지 방면:

첫째, 최근에 세계경제정세가 처참한 배경 하에서 중국경제의 쾌속적인 성장은 사람들을 주목하게 만들었다. 경제발전은 국민의 생활수준과 생활의 질을 개선하였다. 생계를 위해 바삐 보내던 사람들도 이제는 정신적 만족을 수요하고 있다. 이런 추세는 사람들로 하여금 컴퓨터를 구매하고 인터넷을 설치하며 인터넷활동을 시작하게 하였다. 인터넷사용자들과 인터넷기수의 확장은 객관적으로 사이버범죄의 증장에 객관적 기초를 마련해 주었다.

둘째, 중국의 경제 전환은 사람들의 생활수준과 생활의 질을 개선한 동시에 많은 사람들의 경제적 수요를 팽창시켰다. 이런 팽창의 수요를 만족시키지 못하였을 때 범죄의 원천은 무형으로 열린다.

셋째, 이와 동시에 컴퓨터와 인터넷기술이 편리하고 능률적일 수 있는 중요한 원인의 하나가 바로 정보수치의 집중성과 그것의 거대한 가치이다. 재산이 과도하게 집중되면 필연적으로 범죄수익이 증가되며, 이로 인하여 범죄자들의 범죄에 대한 유혹이 더욱 더 증가되고, 경제전환시기에 사람들의 경제이익수요의 거대한 팽창으로 인하여 범죄억제능력이 낮아지고 이로 인하여 범죄를 저지르게 된다.

2) 기술원인(技術原因)

과학기술진보와 과학기술혁명이 파생(衍生)한 사이버범죄의 발생과 존재는 과학기술과 필연적으로 연관되어 있다. 왜냐하면 과학기술은 양날의 칼(双刃剑)로서 인류사회 발전의 길에서 긍정적 역할을 할 수도 있지만 인류 자체에 피해를 줄 수도 있기 때문이다. 컴퓨터와 인터넷기술의 발명과 응용은 인류문명을 산업문명으로부터 정보문명으로 추진하는데 있어서 중요한 공헌을 하였다. 하지만 인터넷의 개방성, 연약성과 복잡성 등의 기술특징은 사이버범죄로 하여금 정보화시대로 나아가는데 유리한 조건을 마련해 주게 되었다. 특히 인터넷 전자상품 자체의 디자인상에서의 결점과 안전상에서의 약점이 사이버범죄에 유리한 조건을 마련해 주었다.

3) 문화원인(文化原因)

범죄는 일종의 사회법률 현상으로서 일정한 물질생활 방식에 의해 결정되고 사회물질 생산방식 모순의 반응이다. 하지만 범죄는 유의식적으로는 인류행위로서 일정한 사상의식과 가치관념에 의해 지배된다. 사상의식과 가치관념 자체는 특정된 문화개념이 포함되어 있기 때문에 어떤 의미에서 말하면 범죄 자체는 하나의 문화 현상이기도 하고 특정사회의 소극적 문화작용의 산물이기도 하다.[112]

현대 중국에서 전통문화가 무너지고 시장경제발전의 개방, 자유, 발전의 요구에 적응하는 현대문화가 아직 형성되지 못하였고, 서방 외래문화가 끊임없이 유

112) 孙景仙/安永勇, "网络犯罪研究", 지식산권출판사 2006년판.

입하여 중국 전통문화와 격렬한 충돌이 생겨 현실사회 예절문화가 거대한 전환을 겪게 되었으며, 사이버세계의 인터넷 주요 문화가 아직 형성되지 못하였으며 폭력, 음란 등 불량문화가 범람하여 인터넷과학기술이 정보의 문을 여는 동시에 범죄를 향하여서도 문을 열게 되었다.

4) 교육원인(教育原因)

중국이 정보화 시대의 요구에 순응하여 인터넷기술교육을 가속화하였지만, 인터넷사용자들의 자아관리, 자아자제, 자아책임 등 방면의 심리와 도덕교육을 소홀히 하였고 이로 인하여 기술을 숭상하고 도덕을 홀시하는 분위기가 형성되었다. 중국 인터넷교육 하에서 대량의 기술향상만 중시하고 규칙준수를 홀시하는 네티즌들이 배양되었고, 이런 네티즌들이 규범의 인도가 부족하기에 사이버범죄자의 후보자로 될 수 있었다.

5) 제도원인(制度原因)

제도원인에서의 중요한 2가지 방면:

① 관리제도(管理制度)

다른 국가와 비교하였을 때 중국이 세계에 남긴 외적 인상은 의무가 자유보다 많고 관리가 자치보다 많은 형상이었다. 하지만 사실은 그게 아니라 한 방면으로는 중국 인터넷이 완벽한 관리제도가 부족하였고 다른 한 방면으로는 인터넷 관리제도는 형식에만 그쳤다("装点门面", "束之高阁", "一纸空文").

② 법률제도(法律制度)

법률 자체는 지연성을 가지고 있고 지연성의 특점은 사이버범죄를 통제하는 방면에서 특별히 선명하였다. 양적으로 말할 때 중국이 인터넷안전규범 및 운영에 관한 법률문서가 아주 많지만 법률문서들이 대부분 행정규정이고 행정법규가 적은 편이며 나아가 행정법률과 형사규범은 더 말할 나위가 없다. 다른 대량의 법률문서에는 내용이 서로 중복, 저촉되어 이는 범죄를 타격하는데 실제효과를 발휘하지 못하는 중요한 요소이다.

이외에도 사이버범죄를 유발하는 원인은 많고 또 서로 다른 각도에서 관찰하면 다른 결론을 얻을 수 있다. 하지만 사이버범죄에 영향을 주는 주요 요소를 말하자면 이뿐만이 아닐 수도 있다.

사. 중국에서 사이버범죄 관련 입법 현황(中国网络犯罪之立法现状)

사이버범죄에 영향을 주는 요소는 비록 많지만 일부분은 사람의 힘으로는 실행하기 힘들며 어떤 요소는 사람의 힘으로 개선시킬 수 있지만 직업적인 제한으로 깊게 파고 들 수가 없다. 사이버범죄 기본문제에 대해 인식이 있는 기초 상에서 이 문장은 오로지 중국 사이버범죄의 법률규정 문제에 대해 깊이 탐구할 예정이다.

인터넷이 발전함에 따라 우리나라 사이버범죄 입법은 점차 발전하였고 비교적 완벽한 법률체계를 형성하였다. 인터넷안전을 보장하고 사이버범죄를 억제함에 있어서 적극적인 작용을 발휘하였다.

1) 근본법(根本法)

중화인민공화국 헌법은 중국의 근본법이지만 헌법에서는 인터넷 및 사이버범죄에 대한 구체적 규정을 하지 않았다. 하지만 중국 헌법 제40조: “중화인민공화국공민의 통신자유와 통신비밀은 법률의 보호를 받는다. 국가안전 혹은 범죄조사의 필요가 없는 이상 공안기관 및 검찰기관은 법률규정에 의한 프로그램을 통해 통신에 대해 검사를 하는 외에 기타 조직 및 개인은 어떠한 이유로 공민의 통신자유와 통신비밀을 침범할 수 없다”라는 규정을 두고 있다.

이 규정 및 그 정신에 의하면 이메일은 통신자유와 통신비밀의 보호범위 내에 속하기에 불법채취(截取)하거나 타인의 메일을 훼손(毁弃)하거나 비밀리에 타인의 이메일을 훔쳐보는 행위는 모두 불법행위에 속한다.

2) 기본법(基本法)

우리나라에서 기본법이란 전국인민대표대회에서 반드시 통과해야 되는 법이

며, 이에는 형법·행정법·형사소송법·민사소송법·행정소송법 등을 포함한다. 현재 우리나라에는 사이버범죄와 연관된 기본법이 있다.

가) 형법(刑法)

① 형법전(刑法典)

1997년 수정한 형법 제285조·제286조·제287조는 컴퓨터 사이버범죄에 대해 구체적으로 규정하였다.

> 제285조: 국가규정을 위반하고 국가사무·국방건설·최첨단 과학기술영역을 침입하는 컴퓨터정보시스템은 3년 이하의 징역 또는 형사 구류에 처한다.
> 국가 규정을 위반하고 전항에 규정된 것 보다 컴퓨터정보시스템 또는 다른 기술수단으로 침입하여 컴퓨터 정보시스템에 저장되었거나 처리 혹은 전수한 데이터를 절취하거나 혹은 컴퓨터정보시스템에 대해 불법사용을 실시하여 상황이 엄중할 경우 3년 이하의 징역 혹은 구류에 처하고 동시에 벌금을 줄 수 있고 상황이 특별히 엄중할 경우 3년 이상 7년 이하의 징역 및 벌금에 처한다.
> 불법적으로 컴퓨터정보시스템프로그램에 침입하기 위해 도구를 제공하는 것과 타인이 불법적으로 컴퓨터정보시스템에 침입하는 범죄행위인 것을 알면서도 도구를 제공하는 경우에는 엄중할 경우 전항에 따라 처벌한다.
> 제286조: 국가규정을 위반하고 컴퓨터정보시스템의 기능에 대해 삭제·수정·증가·간섭함으로 인하여 컴퓨터 정보시스템이 정상적으로 운행하지 않을 경우 엄중하면 5년 이상의 징역을 받을 수 있다.
> 국가규정을 위반하고 컴퓨터정보시스템에 저장·처리 또는 전송하려는 응용프로그램을 삭제·수정·증가 등의 작업을 하였을 경우 엄중하면 전항에 의해 처벌한다.
> 의도적으로 컴퓨터가 정상적으로 작동할 수 없게 파괴성적인 바이러스를 제작·전파할경우 엄중하면 첫 항에 의해 처벌한다.
> 제287조: 컴퓨터를 통해 금융사기·절도·탐몰·횡령·국가의 비밀 혹은 기타 범죄를 절취할 경우 법에 의해 유죄판결을 받게 된다.

② 형법사법해석(刑法司法解释)

2000년 4월 28일 최고인민법원의《최고인민법원이 통신시장질서를 방해하는 사건에 관한 구체적 법률응용문제의 약간의 해석》(最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释) 전문 10조는 주요하게 형법전 제287조에 대한 해석이다.

나) 형사소송법(刑事诉讼法)

2013년 1월 1일에 실행한 본«중화인민공화국형사소송법»의 임무는 적절하고 정확하게 범죄사실을 조사해내고 법률을 정확하게 응용하여 범죄자들을 처벌하

며 무죄자들이 형사책임을 받지 않도록 보장해야 한다고 규정을 두고 있다. 사이버범죄도 일종의 범죄로서, 형사소송법은 사이버범죄사실을 조사하고 사이버범죄주체의 프로그램성을 보장하는 법률이기도 하다. 그 외에 수정한 새로운 《중화인민공화국형사소송법》 제48조에서는 증거종류에 전자수치도 포함된다고 규정하였다. 이는 사이버범죄를 조사하고 사이버범죄자들을 타격하는 유리한 보장이다.

3) 일반법(一般法)

근본법과 기본법 외에 우리나라에는 전국인민대표대회상무위원회의에서 규정한 2부와 사이버범죄에 관련한 일반법이 있다.

가) 《중국인민대표대회상무위원회가 인터넷안전을 수호하는 것에 관한 결정》 (全國人民代表大會常務委員會關于維護互聯网安全的決定)

이는 2000년 12월 28일 제9기 전국인민대표대회상무위원회 제19차 회의심의를 통과하여 결정된 것이고 이 결정은 명확하게 형사책임을 추구하는 5가지 유형의 사이버범죄행위를 규정하였다.

① 인터넷안전을 침범하는 사이버범죄행위(侵犯网络安全的网络犯罪行为);
② 국가안전과 사회안전을 침범하는 사이버범죄행위(侵犯国家安全与社会稳定的网络犯罪行为);
③ 사회주의시장경제질서를 침범하는 사이버범죄행위(侵犯社会主义市场经济秩序的网络犯罪行为);
④ 인신·재산 등 합법적 권익을 침범하는 사이버범죄행위(侵犯人身、财产等合法权益的网络犯罪行为);
⑤ 기타.

나) 《중화인민공화국전자서명법》 (中華人民共和國電子簽名法)

이 법은 2004년 8월 28일 제10기 전국인민대표대회상무위원회 제11차 회의심

의를 통해 결정되었다. 이 법은 총 36조이고 그 중 제32조·제33조는 법에 의해 범죄가 구성될 때 법에 의해 형사책임을 추궁해야 한다는 것을 규정하였다.

4) 행정법규와 행정규정(行政法规和行政规章)

국무원·공안부 등 각 부문에서는 각기 대량의 행정법규 및 행정규장을 발표하였고 그 중 행정법규와 행정규정에는 모두 "해당 상황에 부합될 경우 법에 의해 행사책임을 추궁한다" 는 규정이 있다.

아. 중국 사이버범죄 법률규정의 곤경(中国网络犯罪法律规制之困境)

중국 사이버범죄입법은 비록 일정한 성과를 거두었지만 아직도 문제가 존재하고 있고 인터넷기술의 발전에 따라 새로운 문제와 새로운 모순이 부단히 나타나고 입법의 지연성이 유난히 돋보였다. 개괄하면 아래 몇 가지 방면이 중요하다:

1) 법률규제의 지연성이 유난히 돋보임(法律规制滞后性尤为突出)

변화하는 사회현실과 비교할 때, 법률자체는 지연성을 가지고 있다. 법률의 지연성은 법률의 안정성과 예측성의 불가피한 부가속성이다. 하지만 컴퓨터·인터넷영역, 정보시대지식의 대폭발과 인터넷과학기술의 쾌속한 발전은 법률의 지연성을 유난히 돋보였다. 외국의 입법경험을 부단히 참고하였지만 우리나라 사이버범죄방면의 입법은 아직도 많은 보수성을 가지고 있고 상황성 법률이 불규칙적이고 전망성 법률이 아주 희소하다.

2) 법률규제에 의거하고 비법률적인 수단의 응용 소홀(倚重法律规制, 忽视非法律手段运用)

분석해보면 중국 사이버범죄를 다스리는 과정에서 비록 기본법과 일반법의 수는 많지 않지만 대량의 행정법규와 부문규장을 반포하였다. 거대한 체계를 과소평가할 수 없다. 하지만 사이버범죄를 통제하는 과정에서 기술안전의 결점이 많

고 인터넷관리가 지연성을 띠고 있으며 형식과 표면에만 얽매여 있고 사회의 인도와 교육이 부족하며 응당 발휘해야할 작용을 발휘하지 못했다.

위의 사실들은 모두 중국 사이버범죄의 다스림이 너무 법률규정에 중시를 돌리고 기타 불법수단의 투자와 사용을 소홀히 했다는 것을 설명할 수 있다.

3) 이미 형성된 법률규정체계 자체가 불합리(業已形成的法律規制体系本身不合理)

중국 사이버범죄의 입법상황에 근거해 보면 법률체계는 방대하고 체계구조는 합리성이 결핍하며 법률이 대량의 공백을 보이고 있다. 수많은 행정법규와 부문 사이에는 내용이 복잡하고 교차가 중복되며 상호충돌, 집행곤란 등 문제도 존재한다.

또한 과도하게 형법의 규제작용을 강조했고 구체적인 사회현실과 결합해볼 때 사이버범죄에 관하여 전문적으로 입법하기에는 아직 시기가 성숙되지 못했다고 생각하고 있다. 형법에 대한 수정은 응당 충분한 조사연구를 거친 기초 위에 기인하여 완성해야 한다.

인정해야 할 것은 사이버범죄는 확실히 전통형법이론에 대해 많은 도전을 제기했고 예를 들면 범죄주체의 문제, 범죄형태의 문제, 공동범죄의 문제, 형벌과 사회보안처분의 문제 등이다. 저자는 이론과 사법실무계 연구의 성숙한 기초 위에 형법의 조문에 대해 조정을 하는 것은 반대하지 않지만 형법의 안정성과 협조성을 무시하는 것은 반대한다.

4) 사이버범죄에 관한 개념의 과학계정이 부족(网絡犯罪相關概念缺少科學界定)

이 점은 저자가 위에서 간단하게 제기하였었고 특히 사이버범죄의 개념을 예로 들어 학계와 실무계에 모두 상응한 과학정의가 없고 컴퓨터범죄와 사이버범죄에서 오히려 범죄학정의와 형법학 정의 등 문제가 서로 얽혀있다고 하였다.

5) 지역간·국제간의 교류합작의 진일보 확대(區域間國際間的交流合作需進一步拓展)

위에서 강조했다시피 인터넷에는 국경이 없고 물리속성상의 시간과 공간제약

이 존재하지 않으며 인터넷의 개방성과 유동성은 사이버범죄 돌파지역과 국경의 한계를 받지 않고 지역과 국가를 넘어서는 특징을 가지고 있음으로 인하여 공안 검찰기관이 범죄를 조사하고 증거를 수집하는데 어려움을 가하였다.

이미 입증되었듯이 인터넷은 점차적으로 테러범죄와 같게 되어 어느 국가가 스스로 다스릴 수 있는 문제가 아니다. 지금 현재 국내형세로 보면 지역간, 국가간의 사이버범죄사법협조가 부족한데 이는 사법기관의 사건에 관한 수사가능성과 수사속도를 방해하고 더욱 범죄자들의 기세를 북돋아 주었다.

자. 중국 사이버범죄 관련 법제의 발전과 개선방향

위에서의 세 방면을 결합하여 저자는 사이버범죄를 더욱 완벽하게 다스리기 위해 아래 다섯 방향으로 집중적으로 진행해야 한다고 본다.

1) 법률과 비법률수단의 이원통치모델(法律与非法律手段的二元治理模式)

범죄를 다스림에 있어서 가장 효과적인 방법이 법률수단밖에 없는 것이 아니다. 법률수단은 오래 사용하기엔 부적절하다. 의학자가 말하듯이 약을 많이 먹으면 효과는 빠르지만 몸도 상한다. 그러므로 사회발전과 진보의 발전이라는 관점에서 출발하여 문제를 고려할 경우, 범죄를 다스리는 데는 절대로 법률수단만 사용해서는 아니 되고 법률과 비법률적 수단을 결합하여 이원화 통치를 실현해야 한다.

가) 비법률 수단통치의 주요표현:

① 네티즌(网民)에 대한 인터넷사전교육(网络入门教育)과 인도(引导) 실시

앞에서 밝힌 바와 같이 중국은 인터넷기술교육을 중시하였지만 인터넷사용자의 사전교육과 인도를 홀시하였다. 네티즌들이 인터넷을 처음으로 접촉하였을 때 마땅히 규범화된 지도를 받아야 하고 인터넷자원과 인터넷자유를 향수하는 동시에 다른 사람의 합법적 권리의 침해 여부에 대한 자아통제와 자아 관리를 진행하여야 한다.

② 인터넷 윤리도덕 건설 강화 및 인터넷문화 홍보

현실세계와 사이버세계는 명확한 차이가 있기 때문에 현실세계에 적응되는 행위규칙이 가상사회에도 완전히 적응된다고 말할 수 없고 현실세계에 적응되는 도덕문화가 사이버세계에도 적응될 수 있다고 말할 수 없다.

그러므로 현실세계와는 다른 활동공간으로서의 사이버세계는 응당 자신만의 인터넷이론건설과 인터넷문화건설을 진행함으로서 네티즌이 자발적으로 폭력, 색정 등 불건전한 인터넷문화를 거절하고 각종 사이버범죄를 멀리하도록 해야 한다.

개별학자들이 말하듯이, 범죄는 본질적으로 볼 때 "사람"의 문제이다. 법률, 기술, 관리, 대책 등은 모두 인간에 대한 내화 통제를 실현할 수 없고 인터넷활동 자체도 현실적인 감독이 결핍하며 내화성 감독은 사이버범죄자에 대해 더욱 중요하게 되었다. 그러므로 "사람"을 잘 다스려 사이버범죄자에 대해 내화 통제하고 이들로 하여금 사이버범죄를 면역할 수 있는 도덕병풍을 건립하는 것이 매우 중요하다.

그럼 인터넷문화란 무엇일까? 중국사회과학원연구소의 심걸(沈杰) 선생이 정의를 내리기를 "사람들이 인터넷이란 특수한 세계에서 진행한 작업, 교섭, 학습, 교류, 오락 등으로 형성한 활동방식 및 그가 반영한 가치관과 사회심태 등 각 방면의 총합"이라고 했다. 건전하고 건강한 인터넷문화는 사이버범죄를 억제할 수 있고 소극적인 인터넷문화는 사이버범죄를 유발할 수 있다.[113] 그러므로, 하루속히 적극적이고 건전한 인터넷문화를 주류로 숙성해야 네티즌들이 많은 유혹 앞에서도 냉정하게 극복할 수 있고 사이버범죄를 거절할 수 있다.

나) 산업자치조직(行業自治組織)과 자치규정(自治規章)

방대한 사회조직은 법치의 촉수가 미치지 못하는 사회 각 곳을 관리하고 있다. 설사 관리와 법치가 이러한 강대한 효능이 있다 하더라도 그의 작용은 부단히 낮아지는 면면에서 감소되고 있다. 중국 전통사회에서는 사회 중간역량의 힘

113) 转引自许秀中, "网络与网络犯罪", 중신출판사 2003년판.

을 중시하고 특히 산업내부의 자리와 자치를 강조하는데 이를 또한 중국전통사회의 예의치국의 요인일 수도 있다.

가상적인 세계에서 법률의 촉수는 쉽게 가상적인 공간에 의해 해소될 수 있다. 그러므로 더욱 네티즌의 내부자치와 정보기술 산업내부의 자아조직과 자아관리를 중시해야 한다.

다) 인터넷안전관리(网络安全管理)의 강화(加强)

각국의 인터넷발전경험 교훈을 종합해 보면 인터넷안전 실수가 빈번히 발생하고 있고 인터넷안전 관리효율의 저하는 사이버범죄를 유발하는 원인 중의 하나이다. 그러므로 인터넷 안전관리를 강화하고 전자제품의 설계를 엄격화하고 생산과 제조, 근원으로부터 안전실수를 막아야 하며 전문적인 인터넷안전권리보호기구와 관리검찰체제를 건립하여 인터넷서비스업체와 종업자의 책임을 규범화하는 것이 사이버범죄를 처리하는 유효적인 방법이다.

라) 인터넷기술지지(网络技術支持)의 강화

선진적인 과학기술로서의 인터넷은 기술형의 사이버범죄를 유발시켰다. 그러므로 사이버범죄로 놓고 볼 때, 전통적인 치유방법은 효과를 보지 못한다. 사이버범죄를 억제하는 결정적 역량은 과학기술 자체에 있을 수도 있다. 새로운 인터넷 안전방어상품을 연구개발하고 전업적인 인터넷 순찰대오를 배양하고 고기술함량이 들어있는 인터넷 안전관리대오를 건설하여 사이버범죄 처리작업에 기술적인 지지를 주어야 한다.

만약 법률을 "타치(他治)"라고 한다면 이상의 5가지 측면은 "자치(自治)"를 강조했고, 타치와 자치를 결합해야만 법률은 보다 효과를 발휘할 수 있다.

2) 사이버범죄형사정책의 선택(選擇)

중국에서 인터넷형사정책에 대해 연구하는 학자가 많지 않기에 이 방면은 아직도 대량의 발전공간이 있다. 허수중(许秀中)의 관점에 의하면 사이버범죄형사

정책의 주체(완전한 의미상과 불완전한 의미상의 형사정책의 주체)는 사이버범죄예방, 사이버범죄통제에 기초한 것으로서 자유, 질서유지, 정의를 수호하는 것을 목적으로 제정, 실시한 준칙, 책략, 방침, 계획 및 그 구체적 조치의 총칭이다. 그중 중국의 사이버범죄의 형사정책은 아래와 같은 4가지 방면이 포함된다.

① 정보화 및 정보화안전조직에 관해 활동을 전개하여 전반 인터넷작업을 지도
② 인터넷정보안전에 관한 규범성 문서를 제정하고 점차 법률화를 실행
③ 영도들이 발표한 구체적 연설로 인터넷안전작업을 지도
④ 사법방면의 형사정책[114]

허수중(许秀中)이 제공한 것은 사이버범죄를 대처하는 구체적인 대책인데, 사이버범죄처리를 놓고 볼 때 진정으로 필요한 것은 구체적인 대책 외에 기본적이고 일반적인 형사정책지도이다.

비록 이 방면을 연구하는 학자가 적지만 허수중(许秀中) 외에도 적지 않은 학자들이 사이버범죄형사정책에 대해 많은 관심을 가지고 있다. 예를 들면 왕작부(王作富), 유동항(刘同舫), 레고봉(靳高峰) 교수 등이 사이버범죄 처리의 일반정책에 대해 자신의 의견을 제출했다. 여러 학자들의 관점을 결합한 저자의 생각은 우리나라 사이버범죄형사정책에 대해 3가지의 차원으로 나누어 설명하자는 것이다.

가) 기본형사정책(基本刑事政策)

형사범죄와 사이버범죄는 일반과 특수, 보통과 개별의 관계이다. 그런데 사이버범죄가 아무리 다르다 해도 결국엔 모두 형사범죄의 한 부분에 속하고 형사범죄의 기본속성과 기본특징을 갖고 있다. 그러므로 형사입법과 형사사법의 기본형사정책을 지도함에 있어서 사이버범죄에도 똑같이 적용된다.

최고인민법원이 2010년에 발표한 "엄격함과 관용을 병행하는 형사정책을 관철하는 여러 의견"(关于贯彻宽严相济刑事政策的若干意见)에 근거하면 아래와 같은 5

114) 许秀中, "网络与网络犯罪", 중신출판사 2003년판.

가지 내용이 포함된다:

첫째, 엄격함과 관용을 병행하는 형사정책을 관철하여 범죄의 구체적 상황에 근거하여 차별적으로 대함.

둘째, 엄격함과 관용을 병행하는 형사정책을 관철하여 엄격함과 느슨함을 절실히 병행.

셋째, 관용과 엄격함의 관계를 정확히 파악하고 반드시 엄격히 법에 의해 사건을 심리하고 실죄법정원칙의 실행, 죄형에 상응한 원칙과 법률 앞에서 사람마다 평등하다는 원칙을 철저히 관철하며 법에 의해 정확한 양형을 규정.

넷째, 경제사회의 발전과 치안형세의 변화에 근거하여 특히는 범죄정황의 변화에 근거하여 법률이 규정한 범위 내에서 적당히 관대히 대하고 엄격히 처리하는 모식의 대상, 범위와 강도를 조절. 전면적 객관적으로 부동한 시기에 부동한 각국의 경제 사회상황과 사회치안 형세를 파악하고 인민군중의 안전감과 범죄를 징벌하는 실제적 수요를 충분히 고려하며 국가안전, 사회치안, 인민이익을 엄중히 해치는 범죄를 타격하는데 중점.

다섯째, 엄격함과 관용을 병행하는 형사정책을 관철하고 엄격히 법에 의해 진행하며 법률의 통일과 위엄을 수호함으로서 법률의 양호한 효과를 담보.

사실 실제로 2004년에 왕작부(王作富) 교수가 논문을 발표하여 해커 등 사이버범죄에 대해서는 응당 양극화의 형사정책을 견지하여 위험성적인 해커에 대해선 엄하게 징벌하고 완화형적인 해커에 대해선 경하게 징벌해야 한다고 지적했다. 이는 훗날의 엄격함과 관용을 병행하는 형사정책이 제창한 바와 극히 비슷한 바, 엄격함과 관용을 병행하는 형사정책의 사이버범죄에 대한 지도의의도 바로 이곳에 있다.[115] 이러한 법률의식이 상대적으로 결핍하고 주관적으로 인신위험성이 크지 않고 사회위험성이 엄중하지 않는 사이버범죄자들에 대해서는 되도록이면 관용원칙을 견지하여 범죄자를 징벌하는 동시에 자아반성을 적극 추진하고 하루속히 사회에 귀환하도록 해야 한다. 또한 사회위험성이 엄중한 집단사이버범죄, 공동사이버범죄 등 범죄자들에 대해선 되도록이면 엄격히 하는 원칙을 견지하여 형사책임을 추궁해야 한다.

115) 王作富/庄劲, "黑客行为与两极化刑事政策", 호남사회과학 2004년 제1기.

사이버범죄 처리과정에서 엄격함과 느슨함을 병행하는 형사정책을 파악하는 것은 기로에 들어선 범죄자들에 대한 교육과 개조에 유리할 뿐만 아니라 죄행이 극히 엄중하고 사회위험성이 거대한 범죄자들에 대해 엄격한 처리와 징벌에도 유리하다.

나) 구체적 형사정책(具体刑事政策)

그 자체가 독특한 속성과 본질을 가지고 있는 사이버범죄로서 이에 대해 법률 규제를 행하는 과정에 응당 전문적인 형사정책을 제정해야 한다.

① 종합처리형사정책(综合治理刑事政策)

현재 중국사회는 경제이익, 가치추구 및 의식형태가 다원화된 사회이므로 이러한 사회조건 하에서 산생된 사이버범죄의 처리방법도 응당 종합처리형사정책을 견지하고 적극적으로 종합적인 다원화 처리방식을 모색해야 한다. 이러한 형사정책의 지도하에서 사이버범죄의 처리는 응당 경제, 정치, 기술, 관리, 법률, 문화, 도덕 등 각 방면에서 공동으로 관리하고 종합적으로 처리해야 한다.

② 협력처리형사정책(作治理刑事政策)

위의 문장에서 제기했던 바와 같이, 인터넷이 인터넷신호를 기초로 한 가상공간으로서 인터넷신호가 있는 곳은 모두 네티즌이 자유로이 진입할 수 있는 사이버세계이다. 그러므로 인터넷의 존재는 지역과 지역, 국가와 국가 간의 계선을 타파하여 세계로 하여금 진정한 일체화를 실현하게 하였고 다국적 범죄도 쉽게 조성했다. 곧바로 사이버범죄가 다지역적, 다국가적인 특점은 사이버범죄의 피해자가 단지 협애한 모 영역에 국한된 것이 아니라 각 지역 심지어는 각 국가에 전파되게 하였다. 사이버범죄의 현황이 부단히 증명한 바와 같이, 그리고 테러범죄의 경우에서 보듯이 어느 나라도 독립적으로 인터넷 범죄를 대응할 수 있는 거대한 능력을 갖고 있지 않다. 그러므로 반드시 세계 여러 나라와 적극 교류하여 부단히 국제입법의 통일, 국제사법의 합작, 국제관할 등 여러 문제의 전면적인 처리합작방식을 탐색해야 한다.

③ 예방을 주로, 타격을 보조적으로 하는 형사정책(预防为主打击为辅的刑事政策)

인류사회는 날로 더욱 위험한 시대로 매진하고 있다. 위험은 한 방면으로는 인류위험의식의 제고에서 오고, 다른 한 방면은 선진과학기술이 인류에게 가져다준 부작용에서 온다. 과학 낙관주의자는 혹시 반박할지 모르지만 과학진보는 모두 일정한 위험을 가져온다. 이미 입증된 바와 같이 시대의 과학진보는 모두 현대과학 기술혁명처럼 이토록 거대하고 예측할 수 없고 통제할 수 없고 심지어 되돌릴 수 없는 거대한 재난이지는 않았다.

인터넷이 현대과학기술의 한 가지로 쓰이면서 사이버범죄의 사회위험성은 일정한 정도에서 거대하고 예측할 수 없고 통제할 수 없으며 되돌릴 수 없는 등과 같은 현저한 특징을 가졌다. 그러므로 사이버범죄의 처리는 사전예방이 징벌보다 효과적이다. 또한 반드시 예방전제의 정황 하에서 형사정책을 견지해야 한다.

④ 자유와 안전을 모두 중히 여기는 형사정책(自由与安全并重刑事政策)

자유와 공유의 기초에서 건립된 인터넷은 자유의 건립의 취지로, 또한 부단히 추구하는 것을 목표로 하고 있다. 그러나 세상에는 절대적인 자유가 없고 절대적인 자유는 모두 타인의 자유에 방해와 침범을 구성한다. 인터넷안전보장이 결핍한 인터넷자유는 진정한 자유가 아니다. 그러므로 사이버범죄의 처리는 반드시 자유와 안전의 관계를 조화시켜야 하며, 자유를 희생하는 것을 대가로 아무런 의미 없는 안전을 바꿔온다든가 안전을 희생하는 것을 대가로 신기루같은 절대적인 자유를 추구해서는 아니 된다.

3) 법부문사이의 연동관리(律部門之間的联动治理)

가) 연동입법(联动立法)

연동입법이란 즉 각 부문이 입법시 응당 전체적, 전반적인 관념이 있어야 하고, 기타부문과 서로 요해하고 상호 조화하고 상호 배합해야지 각자 입법을 하지 못하고 각자 자신만의 정책을 고집하여 나중의 법률이 서로 중합되거나 서로 저촉되어 실행될 수 없게 해서는 아니 된다는 것이다.

나) 연동사법(聯動同法)

연동사법이란 즉 각 부문이 사법시 서로 배합하고 공동으로 노력하는 것이다. 이는 범죄기초수가 크지만 사법기술이원이 상대적으로 결핍한 현황에 의해 결정한 것이다.

4) 행정, 민사가 앞서고 형사가 보장(行政, 民事在先, 刑事保障)

법학의 기초이론에 근거하여 형법은 사회통제의 수단으로서 보충성의 특징을 갖고 있음으로 기타 일체 법률을 뒷받침하는 최후의 보장법이다. 전반 법질서의 각도에서 사고할 때, 기타 법률부문의 개입이 충분히 문제를 해결할 수 있을 때 형법은 개입하지 말아야 한다. 형법은 국가, 사회 혹은 개인이 오직 형벌이라는 도경을 통해서만 효과적인 보호를 진행할 때에만 사용된다. 이는 형법의 겸허함과 억압함의 원칙에 부합될 뿐만 아니라 법률경제원칙에도 부합된다. 일반적으로 말할 때 사람들이 정상적으로 권리를 행사하고 의무를 이행할 때, 즉 정상적인 사회관계가 산생할 때이다. 일단 사람들이 불법적으로 권리를 행사하거나 법에 의한 의무를 이행하지 않았을 때, 즉 정상적인 사회관계가 파괴될 때 법률을 이용하여 시정과 회복을 진행할 수 있다. 이때의 사회관계는 정상적인 사회관계 영역을 타파하고 처음으로 행정법, 민법조정의 범위에 진입하게 되었고 사건접수 후 행정법, 민법의 조정을 접수하여 제1보호성 법률관계를 형성한다. 이때의 불법행위는 행정위법성 혹은 민사위법성을 가지고 있어 행정위법행위 혹은 민사위법행위를 구성한다. 그런데 만약 행정위법행위 혹은 민사위법행위가 계속 진행될 시 정도가 계속 가중화되어 행정법, 민법 등 전치법이 손해당한 사회관계를 보호하지 못할 경우 행정법, 민법의 영역을 돌파하여 형사조정의 범주에 귀속시켜 형법의 조정을 거쳐 제2보호성 사회관계를 형성한다.[116]

그림에서와 같이:

116) 田宏杰, "行政优于刑事：行刑衔接机制构建", 인민사법 2010년 제1기.

如图所示：

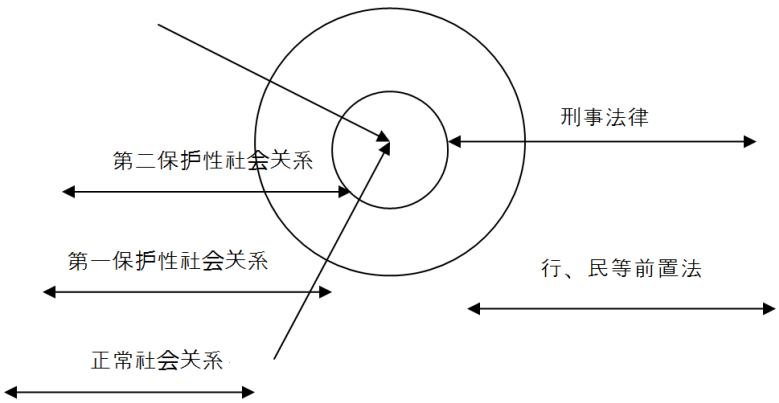


그림 4 국가와 사회의 관리

그림에서와 같이 국가와 사회의 관리는 먼저 행정법, 민법 등 전치법에 의뢰하는 면에서부터 법률조정하여 파괴된 사회관계로부터 정상적인 상황으로 돌아오게끔 해야 된다. 단지 범죄행위가 행정법, 민법 등 전치법의 범위를 돌파하여 형법의 영역에 진입하여 전치법이 그 행위를 규제할 수 없고 파괴된 사회관계로 하여금 정상상태로 회복시키지 못할 때 형법이 그 보장적인 뒷받침 역할을 한다.

이렇게 볼 때, 형법자체의 특수속성은 사이버범죄의 관리과정을 결정했지만 과분하게 형법의 작용에 의뢰할 것이 아니라 행정법, 민법 등 전치법률의 작용을 더욱 중시해야 한다. 그러므로 인터넷위법행위가 전치법에서의 공백을 신속히 미봉하기 위해서는 행정법, 민법 등 전치법률을 신속히 개선해야 이로 하여금 인터넷위법범죄행위를 타격하고 사이버범죄를 감소하는 유력한 도구로 되게 할 수 있다.

5) 형법자체의 조정과 완선(刑法的自身調整与完善)

행정법, 민법 등 전치법률이 인터넷위법범죄를 관리하는데 있어서의 작용을 중시한다 하여 형법의 규제수단을 버린다는 것이 아니다.

사회는 진보, 변천하고 있고 범죄도 발전·변화하고 있기에 형법은 응당 전치법을 결합하는 동시에 자체의 조정과 완선을 고려해야 한다. 학자들의 광범한 토론에 의하면 형법 자체의 완벽화는 응당 아래와 같은 몇 개 방면에서 진행해야 한다.

가) 범죄확정(犯罪確定)

앞에서 저자가 제기한 바와 같이 중국의 형사입법은 진정으로 컴퓨터범죄와 사이버범죄 양자 간의 관계를 구분하지 못했다. 이러한 입법규정은 필연코 양자의 구체적 특징 및 그 위해정도에 의한 적절한 형벌을 저해하여 범죄타격의 불리한 효과를 초래할 것이다.

또한 형법이 사이버범죄 관리과정에서 행정법, 민법 등 전치법의 뒤에 놓이게 함으로서 보장성 작용을 발휘하게 해야 한다. 그런데 행정법률, 민법률이 부단히 완벽화함에 따라 인터넷위법행위가 부단히 나타나 형법의 영역도 이에 따라 상응한 범죄권을 조정함으로써 사이버범죄를 타격하는 현실적 수요에 적응시켜야 한다.

나) 범죄주체(犯罪主体)

우리나라 형법 제17조의 규정에 의하면 만 16세의 사람이 범죄시 응당 형사책임을 져야 한다. 또한 만 14세 이상, 16세 미만인 사람이 의도적으로 사람을 죽이거나 중상을 입히거나 강간, 강도, 독품판매, 불을 지르거나 폭발, 독을 파는 등 죄를 범했을 때 응당 형사책임을 져야 한다.

그러나 인터넷범죄의 현실적상황과 미래의 발전추세에 근거하면, 인터넷범죄의 주체는 날로 젊어지고, 저연령화의 추세로 나아가고 있으며 전통적인 형사책임 연령규정도 부단히 도전받고 있다. 또한 중국형법 제30조의 규정에 의하면 단위당 사회에 위해를 실시하는 행위는 법률이 규정한 단위당 범죄일 때만 형사책임을 진다. 중국형법 제285조, 제286조, 제287조에서는 명확히 인터넷범죄 중의 단위범죄를 규정했다. 예를 들면 단위에서 결정하고 조직, 실시한 컴퓨터바이러스를 조작, 전파한 행위, 그리고 사법현실 중에서도 확실히 두 단위의 사이

버범죄 진실 사건이 있었다. 그러므로 형사입법을 완벽화하여 입법상에서 단위가 사이버범죄의 주체로 되게 하는 것이 최상의 선택경로이다.

다) 공동범죄(共同犯罪)

위의 서술에 의하면 사이버범죄는 미래의 발전 중에서 점차 산업화, 집단화의 추세를 보이고 있다. 이런 추세 하에서 사이버범죄 상당수는 공동범죄의 형식으로 표현될 수 있다. 이를 사이버범죄현황과 어떻게 결합할 것인가 하는 문제로부터 공동범죄자의 지위와 작용, 공동범죄자 사이의 합리한 형사책임분배 나아가서 공동범죄의 목적을 일치화하는데 이르기까지 모두 공동범죄 상관이론에대한 거대한 도전으로 볼 수 있다.

라) 형벌완벽화(刑罰完善)

중국 제285조, 제286조에서는 사이버범죄에 대하여 자유형과 자격형을 규정했다. 그런데 컴퓨터사이버 범죄주체의 특점을 고려하여 각국의 형벌규정을 볼 때 일반적으로는 일정한 자격형을 규정하고 범죄분자가 일정한 시간 내에 종사한 상관사업과 상관활동을 진행할 자유를 박탈한다.

6) 국제간의 통일입법과 사법협조(國際間統一立法及司法協作)

인터넷기술의 발전과 더불어 사이버범죄 문제는 날로 전사회, 전지구적인 문제로 되고 있다. 많은 전문가가 부단히 의식하고 지적한데 의하면 단지 일국의 유한한 힘으로는 전지구적인 사이버범죄의 수요를 만족시킬 수 없기에 각국과 전지구적인 다변합작기제를 건립하는 쪽으로 발전하고 있다.

가) 관할권문제(管轄權問題)

전통적인 범죄와 비교하여 볼 때, 사이버범죄는 전지구성과 방사성의 특징을 나타내고 있기에 영향범위가 매우 광범하다. 이는 불가피하게 사이버범죄 관할권 측면에서의 충돌이 생기게 될 것이고 이로부터 인도, 사법협조와 영역외 판

결승인 등 다방면의 문제를 가져오게 될 것이다.

전통국계와는 달리 인터넷공간은 변경을 구분하기 매우 어렵다. 전통적인 관할제도 중에 행위지와 결과지를 중심으로 하는 것은 엄중한 도전을 받게 될 것이고 일부 학자는 사이버범죄 관할문제에서 민법영역 중의 협력 관리제도를 채택할 것을 건의한다.

나) 국제통일입법(國際統一立法)

유럽형사법일체화를 배경으로 사이버범죄는 테러범죄(恐怖犯罪)마냥 적극적으로 전 지구적인 관리를 추구하고 있기에 불가피하게 법률표준이 있어야 한다. 비록 국가의 주권을 무시하고 국가화와 완전히 일치한 법률표척을 주도 한다는 것은 과도하게 이상화된 일이지만 세계 범위 내에서 제일 기본으로 또 각국이 보편적으로 받아들일 수 있는 사이버범죄입법을 건설하는 것은 실행가능성이 있다.

그러기에 지역일체화의 기초상에서 사이버범죄전지구성의 인터넷 기본입법을 적극적으로 추진하여 국제성사이버범죄공약을 제출시키는 것도 현명한 선택일 수 있다.

다) 국제사법협조(國際司法協助)

지금 세상은 하나의 개방적인 세상이 되어 각국 간의 교류와 합작이 경제, 정치, 문화 등 여러 영역으로 광범위하게 늘어나고 있다. 국가를 넘어선 사이버범죄가 날로 빈번하고 사회위협이 날로 엄중해지는 상황 하에서 각국은 적극적으로 사이버범죄를 타격하는 지역을 넘어서고 국가를 넘어서서 합작하여야 하며 각국의 인터넷안전과 사회안전을 지키는데 유리할뿐만 아니라 각국 사법경험의 교류와 발전에도 유리하다.

이외에 사이버범죄 국제검찰조직과 조합조직을 수립한다는 것은 각국이 제시간에 나라를 넘어선 사이버범죄를 발견하는데 유리하기 위해서이고 각국 사이버범죄 연합통치와 다면협력의 편리를 제공하기 위해서 이다.

결론적으로 말하면 학계는 아직도 사이버범죄 연구에 대한 탐험단계에 처해있고 근본적으로 사이버범죄의 정성문제를 해결하지 않고 컴퓨터범죄와 사이버범

죄 간의 관계문제를 순리롭게 해결하지 못한다면 인터넷범죄에 대한 연구에 있어서 든든한 기초가 될 수 없다. 이는 학술자원의 거대한 낭비이고 중국법치건설과 발전에 대한 극도로 책임성이 없는 태도이다. 사이버범죄 중의 근본문제를 홀시하고 세부적인면만 본다면 결국엔 근본적인 문제를 해결할 수 없다.

4. 중국에서 사이버범죄 관련 형사정책[117]

인터넷은 사람들의 생활에 혁신적인 변화를 가져왔다. 이는 현재 우리가 상상할 수 없는 방식으로 사회이익 최대화를 추구하며 비교할 바 없는 기회를 가져다주었다. 예를 들면 교육, 연구, 비즈니스, 엔터테인먼트, 공공사무 등이다. 다른 한편으로, 이는 네트워크를 이용하여 범죄활동을 진행하려는 자들에게 아주 저렴한 원가 및 잠재적인 익명방식으로 범죄활동을 진행할 수 있게 하였다. 예를 들면, 사기, 음란소설의 판매와 유통, 총기, 마약 또는 기타 불법 물품의 판매, 컴퓨터소프트웨어의 불법유통, 지적재산권 보호를 받는 성과물에 대한 침범 등이다.[118] 인터넷기술은 교류가 편리하고 신속하며 날마다 다른 특성을 가지고 있어 사회교류의 가능성을 증가시키는 동시에 불법범죄행위의 가능성도 증가시켰다. 중국 인터넷 데이터센터의 통계에 따르면, 2012년 6월 말을 기준으로, 중국네티즌의 수량은 5.38억에 달하였고 인터넷 보급률은 39.9%에 달하였다고 한다.[119] 현재 전 세계적으로 규모가 제일 큰 개인 사용자에 대한 인터넷 안전연구 리포트—사이먼테이크노둔(賽門鐵克諾頓) 인터넷 안전리포트—에 따르면 2012년 사이버범죄로 인한 전 세계적인 직접적 손실은 1,100억 달러에 이르렀다고 한다. 중국에서는 2.57억에 달하는 사람이 사이버범죄의 피해자로 되었고, 피해를 끼친 직접적인 경제손실은 2890억 위안에 달하였다. 또한 84%에 달하는 네

117) '중국에서의 사이버범죄 관련 형사정책'과 관련한 내용은 공동연구자인 时延安 교수(中國人民大學校 法學院)가 책임집필한 '网络犯罪刑事政策论纲'를 가급적 원문에 가깝게 번역하여 소개하였다. 원문은 <부록 4> 참조.

118) 參見葉海濤摘譯, "美國關於控制互聯網犯罪的報告", 상해대외무역학원학보 2000년 제7기.

119) 中國互聯網資訊中心 : 《제30차 중국 호련망로 발전상황 통계보고》.

티즌들이 예전의 생활에서 사이버범죄의 침해를 받았었고, 2012년만 해도 사이버범죄의 침해를 본 네티즌이 72%에 달하였다(즉 매일 70만 명을 초과하는 중국 네티즌이 사이버범죄의 침해를 받고 있는데 이는 매 분당 489명의 피해자가 나타난 셈이다). 2012년 한해만 해도 사이버범죄 피해자들이 본 직접적인 경제손실은 1,126억 위안에 달하였다.[120] 데이터는 거짓말을 하지 않는다. 인터넷은 사람들을 현실로부터 사이버세계로 이끌었고 여기는 또한 범죄자들이 제일 좋아하는 세계로 되었다. 그러므로 사이버범죄를 타격하고 사이버사용자들의 안전을 수호하는 것은 형사정책의 중요한 부분으로 되어야 한다. 이성적인 정책구조를 통하여, 사이버범죄를 효과적으로 예방 및 징벌하고, 과도한 사용공제로 인한 사이버세계에도 동일하게 존재하는 기본권리 및 기술발전의 잠재적 가능성을 침범하지 않게 하는 것이 연구자들의 중점적인 과제가 아닌가?

가. 사이버범죄의 유형분석

1) 학술계에서 정한 사이버범죄에 대한 정의

중국 학술계에서는 사이버범죄에 대하여 광의설과 협의설로 나누어서 설명을 하고 있다. 협의설상의 사이버범죄의 개념은 컴퓨터조작으로 실시한 인터넷정보시스템(램데이터(內存數據)와 프로그램 포함)안전을 위협하는 범죄행위로 정의되고 있다.[121] 이 설에 의하면 컴퓨터와 인터넷은 필요한 범죄도구인 동시에 범죄대상이기도 하다. 사이버범죄는 형법 제285조의 컴퓨터 정보시스템 불법침입죄(非法侵入計算機信息系統罪), 컴퓨터정보시스템의 데이터 불법획득, 컴퓨터정보시스템의 불법공작죄(非法獲取計算機信息系統數據, 非法控制計算機信息系統罪), 불법적으로 침입, 공작할 수 있는 컴퓨터정보시스템의 프로그램 및 도구를 제공한 죄, (提供侵入, 非法控制計算機信息系統的程序, 工具罪), 제286조의 컴퓨터정보시스템 파괴죄(破壞計算機信息系統罪) 등을 포함할 수 있다. 광의상의 사이버범죄의

120) 參見新華網, "諾頓網路安全報告 : 망로범죄 중국 연손실2890억원"; http://news.xinhuanet.com/legal/2012-09/12/c_113056800.htm.

121) 參見趙秉志/於志遠, "論電腦犯罪的定義", 현대법학 1998년 제5기.

개념은 사이버공간에서 컴퓨터전문지식을 이용하여 실시하는 범죄행위를 말하는데 이는 컴퓨터네트워크를 공격대상으로 또는 컴퓨터네트워크를 수단, 도구로 사용하는 범죄행위를 말한다.[122]

연구측면에서 볼 때도 우리는 협의설에서 정의한 사이버범죄의 범위가 너무 좁다고 인정한다. 컴퓨터 네트워크를 공격대상으로 하거나 컴퓨터네트워크를 수단 또는 도구로 하는 모든 범죄행위는 컴퓨터 네트워크 전문지식을 이용하여야만 실시가 가능한 것이다. 컴퓨터 네트워크를 수단 또는 도구로 하는 범죄행위, 예를 들면 형법 제287조에서 규정한 컴퓨터를 이용하여 실시한 금융사기, 절도, 탐오, 횡령, 국가비밀 절취 또는 기타 범죄는 전통범죄의 범주에 속하지만, 범죄수단의 과학특정에 비추어 볼 때 이러한 범죄행위는 행위성질, 위해정도, 수사과정, 관할지 등 방면에서 전통적인 범죄와 아주 큰 차이가 있으므로, 연구를 함에 있어서는 사이버범죄의 한 부류에 귀납하는 것이 적당하고 전통범죄와 달리 규범을 적용하여야 할 것이다.

입법자들도 같은 태도를 취하고 있다. 2000년 12월 28일 제9기 전국인민대표대회 상무위원회 제19차 회의에서 통과한 〈전국인민대표대회 상무위원회 인터넷 안전수호에 관한 결정(全國人民代表大會常務委員會關于維護互聯網安全的決定)〉에서는 실제 사례를 드는 방식으로 국가사무, 국방건설 첨단과학기술 영역의 컴퓨터 정보시스템을 침입; 고의적으로 컴퓨터 바이러스 등 파괴성프로그램을 제작하거나 전파; 마음대로 컴퓨터네트워크 또는 통신서비스를 중단하는 등 방식으로 인터넷 운영안전을 위협하거나 인터넷을 통하여 국가비밀 정보 또는 군사비밀을 절취하거나 누설; 인터넷을 이용하여 민족보복과 민족차별을 유발; 인터넷조직 사교조직을 이용하여 국가안전과 사회온정을 위협; 인터넷을 이용하여 가짜제품을 판매 혹은 상품 서비스에 대해 허위광고를 진행; 인터넷을 이용하여 타인의 상업신용과 상품명예를 훼손; 인터넷을 이용하여 타인의 지적재산권을 침범; 인터넷을 이용하여 증권, 펀드의 허위정보를 전파; 인터넷에서 음란사이트를 설립하여 사회주의 시장경제질서와 사회 관리질서를 파괴; 인터넷을 이용하여 타인을 모욕 혹은 타인을 비방; 불법적으로 타인의 이메일 혹은 기타 데이터자료를

122) 參見劉守芬/孫曉芳, "論網路犯罪", 북경대학학보(철학사회과학판) 2001년 제3기.

절취 왜곡 혹은 삭제; 인터넷을 이용하여 절도, 사기, 협박 등으로 개인, 법인과 기타조직의 인신 재산 등 합법적 권리를 침범하는 등을 명확하게 사이버범죄라고 정의를 내리고 중점적으로 전문적으로 예방 및 타격한다고 규정하고 있다.

2) 실천에 있어서 사이버범죄의 다발유형

전반적으로 볼 때, 우리나라 사이버범죄는 다발추세를 나타내고 있고 범죄유형도 비교적 집중 되어있다. 중국인민 공안대학교 경찰개혁과 발전연구중심에서 발표한 〈2012년 중국인터넷 위법범죄문제 연간 리포트(2012年中國互聯網違法犯罪問題年度報告)〉(이하 '리포트'라고 약칭〉에 의하면, 2012년 중국공안기관에서 해명한 사이버범죄사건은 11.8만 건에 달하고 체포한 범죄혐의자는 21.6만여 명에 달하였다. 총기, 마약, 음란 등에 관한 불법정보를 572만여 건 처리하였고 법에 의거하여 폐기한 사이트(채널)는 8만여 개에 달하였으며 2.6만여 개의 인터넷서비스단체를 처리하였고 1.1만여 개의 불법아이디를 정지시켰다.[123] 리포트에 의하면, 중국의 주요 사이버범죄유형은 인터넷사기(網絡詐騙), 인터넷 다단계 판매(網絡傳銷), 인터넷음란(網絡色情), 인터넷피싱(網絡釣魚), 인터넷도박(網絡賭博), 인터넷 마약밀수(網絡販毒), 인터넷 총기매매(網絡販槍), 인터넷 인체장기판매(網絡販賣人體器官), 인터넷불법융자(網絡非法集資), 인터넷해킹(網絡黑客攻擊), 인터넷가짜약품판매(網絡販賣假藥), 인터넷 공민정보매매(網絡販賣公民個人信息), 인터넷협박절취(網絡敲詐勒索), 인터넷 범죄방법전수(網絡傳授犯罪方法), 인터넷 폭발약품판매(網絡販賣爆炸物品), 인터넷 유독화학제품판매(網絡販賣劇毒化學品), 인터넷인신매매(網絡拐賣人口), 인터넷을 이용한 소문전파(利用網絡制造傳播謠言), 테러정보전파(散布虛假恐怖信息), 인터넷을 이용한 국가비밀절취 및 누설(利用網絡竊取, 泄漏國家秘密) 등이 있다. 리포트는 범죄피해자의 수량, 금액, 위해정도, 영향정도에 따라 2012년 사이버범죄의 10대 유형을 귀납하였는데 이는 인터넷사기(網絡詐騙), 인터넷음란(網絡色情), 인터넷 다단계판매(網絡傳銷), 인터넷 공민정보매매(網絡販賣公民個人信息), 인터넷피싱(網絡釣魚), 인터넷도박(網絡賭博), 인터넷

123) 參見中國人民公安大學警務改革與發展研究中心 : 《2012년 중국 호련망 위법범죄문제 연도보고》.

해킹(網絡黑客攻擊), 인터넷 가짜제품판매(網絡販賣假冒僞劣産品), 인터넷마약밀수(網絡販毒), 인터넷불법융자(網絡非法集資)를 포함한다. 소주시(蘇州市) 인민검찰원 과제팀(課題組)에서 소주시의 2007-2010년 사이의 사이버범죄를 조사분석한 결과에 의하면, 소주시 사이버범죄는 인터넷사기, 인터넷도박, 인터넷음란물품전파, 인터넷매춘, 인터넷불법판매 등 유형으로 집중되어 있다고 한다.[124]

가) 인터넷사기(網絡詐騙)

인터넷의 보급에 따라 전통적인 사기수단이 부단히 변화 및 업데이트 되면서 인터넷의 비 직접적인 접촉식 정보전파와 정보교류방식이 직접 접촉사기에서 사기범죄자들이 쉽게 긴장하는 결점을 해결해 주어 더욱 쉽게 사기에 성공할 수 있게 되었다.[125] 이로 인하여 사이버세계는 사기범죄의 중(重) 재해구로 되었다. 인터넷사기방식은 주로 인터넷응모사기, QQ인터넷채팅사기, 인터넷피싱사이트 혹은 허위사이트사기, 인터넷쇼핑사기, 인터넷로또사기, 인터넷주식사기, 인터넷취직사기, 인터넷 수능시험사기 등이 있다. 동시에 신형의 웨이신사기(微信詐騙), 인터넷 다단계판매사기, 비즈니스 협력파트너를 사칭한 인터넷사기도 부단히 나타나고 있다. 그중 피싱 사이트와 사기 사이트가 특히 창궐하고 있다. 중국 전자 비즈니스협회 커이신 전자 비즈니스 추진센타(中國電子商務協會可信電子商務推進中心), 중국 커이신 사이트 응용추진연맹(中國可信網站應用推進聯盟)과 커이신 사이트 검증관리기구(可信網站驗證管理機構)가 연합하여 발표한 〈2012년 중국 사이트 커이신 검증산업 발전리포트(2012年中國網站可信驗證行業發展報告)〉에서 발표한바와 같이, 2012년 6월말까지 31.8%의 인터넷쇼핑경험이 있는 네티즌들이 인터넷 쇼핑 중 직접적으로 인터넷 피싱 사이트 또는 사기 사이트에 접속하였다는 연구결과가 있다. 인터넷 쇼핑 피해 네티즌 수는 보수적으로 예상컨대 6,169만 명에 달하고 39.7%에 달하는 네티즌의 손실금액이 500위안을 초과할 것으로 예상된다. 보수적으로 예측컨대, 매년 피싱 사이트 또는 사기 사이트로 인한 네티즌에 대한 경제손실이 308억 위안에 달할 것이다.[126]

124) 參見李贊等, "蘇州市2007-2010年網路犯罪調查分析", 중국형사법잡지 2011년 제10기.

125) 参见《报告》.

나) 인터넷음란(網絡色情)

인터넷전파의 신속성, 은밀성, 공유성에 의하여 인터넷을 이용하여 음란물품과 매춘을 전파하는 사건이 빈번히 발생하고 있는데 이의 피해 주체는 광범위한 동시에 미성년자에 대한 위해성도 유난히 크다고 할 수 있다. 인터넷 음란전파 방식은 아주 다양한데 전통적인 칼럼형 음란 사이트(論壇型色情網站), 예를 들면 칼럼, 블로그, 미니블로그, 사교형(社交型) 사이트, 검색사이트, 뮤직비디오사이트 외에도 채팅사이트 즉 인터넷 실시간채팅도구 예를 들면 QQ그룹 및 개인QQ 도구, 핸드폰사이트, 인터넷 게임사이트 등이 있고 모바일 응용프로그램 플랫, 온라인 비디오 소프트웨어, 인터넷 공유사이트(서버), 인터넷 자원다운로드 등 새로운 인터넷 응용 기술전파방식 등이 있다고 할 수 있다.

다) 인터넷도박(網絡賭博)

전통도박은 물리적공간의 제한을 받으나 인터넷 사이버공간은 짧은 시간 내에 다량의 군체(群体)가 집중되게 할 수 있어 도박업의 환영을 받은 장소로 꼽히고 있다. 인터넷도박은 주로 두 가지 방식이 있는데, 하나는 전통도박을 인터넷으로 전이한 것이다. 이는 인터넷의 상호작용성이 강하고 은밀성이 강하며 지불방식이 편리하며 증거보류가 어려운 점 등을 이용하여 도박활동을 진행하는 것인데 인터넷의 실시간성과 다지역성으로 인해 도박참여범위를 크게 확대하여 인터넷도박금액이 부단히 증가하게 되었다. 다른 하나는 인터넷 게임 중에 생성되는 일부 도박행위인데 즉 “변상적인 도박형 인터넷게임(變相的賭博類網絡遊戲)”이라고 하는데 이는 인터넷 게임서비스, 가상화폐, 제3방 교역 플랫 등 여러 절차로 법률을 스쳐지나가는 형식으로 도박금액이 직접적으로 인민폐와 연결되지 않게 하는 방식이다. 이는 전에 언급한 도박유형에 비추어 볼 때, 그 정의에 있어서 어려움이 있을 수 있다. 다만 이런 사이버도박형식이 발전하기 시작하면 상당한 은밀성과 방대한 인터넷게임사용자들의 존재로 인해 전파범위가 더 넓고 발전변

126) 參見中國電子商務協會可信電子商務推進中心, 中國可信網站應用推進聯盟和可信網站驗證管理機構中網 : 《2012년 중국 망참가신험증행업 발전보고》.

화도 더 빠를 것으로 예상된다.

라) 인터넷요언(網絡謠言)

최근에 들어서서, 인터넷을 이용하여 요언을 제작, 복제, 전파하는 등 유해정보사건이 가끔 일어나 사회의 광범위한 관심을 불러일으키고 있다. 인터넷 요언의 전파는 돌발적이고 전파속도가 급속하게 빠르므로 쉽게 정상적인 질서에 불량한 영향을 일으킬 수 있다. "여성 고위급 간부가 거액공금을 들고 캐나다로 도주"로부터 "에이즈 환자가 피로 에이즈를 전파", "여대생이 구직 중 신장을 도난당함" 등 요언들이 났었는데 사후에는 모두 거짓으로 증명되었다. 2008년 광원 "구더기 귤사건(蛆橘事件)"으로 인해 전국 감귤판매가 엄중하게 부진되었고 충해요언(蟲害謠言)이 인터넷을 통하여 신속하게 전국에 퍼짐으로 하여 호북성 한개성만 해도 경제적 손실이 15억위안에 달하게 되었다.[127] 2013년 8월 "요언으로 중국을 뒤엎었다"고 하는 유명한 네티즌 "진회 진화화(江淮 秦火火)"는 고의적으로 트집 잡아 분쟁을 일으킨 혐의로 불법 경영죄로 형사구류에 처하였다. 진모는 웨이버(微博)에 선후하여 10개의 다른 인터넷아이디를 설치하고 다른 사람과 연합하여 인터넷 추진그룹을 설립하고 소위 "의견리더"로 인터넷 "수군"을 조직하여 장기적으로 인터넷에서 허위뉴스를 만들고 고의적으로 사실을 왜곡하며, 사건분쟁을 제작하고 타인의 평론을 삭제하며 IP주소를 연락 및 찾는 등 방식으로 불법적인 이익을 챙겼으며 인터넷질서를 엄중하게 파괴하였다.[128] 이로 인하여 2013년 9월, 양고(两高)에서는 이런 유형의 형사사건에 적용하는 법률인 〈정보네트워크를 이용하여 비방 등을 하는 형사사건 적용법률에 관한 약간의 문제해석(關于辦理利用信息網絡實施誹謗等刑事案件適用法律若幹問題的解釋)〉은 어떤 인터넷 풍설이 범죄를 구성하는지를 명확하게 규정하여 인터넷 요언비설을 엄격하게 타격하는 목적 하에 반포한 것이다.

127) 黃慶暢/張揚, "網路謠言害人害己, 社會公眾勿傳勿信", 인민일보 2012년 4월 16일.

128) 李恩樹, "網路造謠者"如此興風作浪, 法制日報 2013년 8월 21일.

마) 인터넷시스템안전파괴(破壞網絡系統安全)

전세계 인터넷을 공제하고 인터넷 독점권을 실행하기 위하여 일부 나라들에서는 인터넷에 “공성약지(攻城略地)”를 하였다. 필요한 정보를 획득하기 위하여 인터넷 간첩들은 불법적으로 적방 또는 해외컴퓨터네트워크에 침입하여 상대방의 인터넷상의 정보를 수집 정리하였다. 정보화 사회의 주의를 불러일으키기 위해, “해킹행동주의자”들은 사이트의 홈페이지에 선명한 메모를 남겨 인터넷이 막히게 하거나 사이트에 일부 격렬한 반대관념을 침투시키기도 하였다. 심지어 사이트에 “서비스공격을 거절”한다는 내용을 추가하여 사이트의 마비를 조성하기도 하였다. 불법적으로 이윤을 획득하기 위하여 해커는 사용자의 인터넷 은행계좌, 게임장비 등을 절취하였고; 해킹수단으로 협박 혹은 악성경쟁을 진행하였으며; 정부, 금융, 교통, 전력, 교육, 과학연구 등 각 영역의 공공 서비스 정보시스템을 공격하였다. 해킹도구를 제작 판매 및 해킹기술전수도 이미 지하 산업 체인을 형성하였다.

바) 인터넷마약밀수(網絡販毒)

인터넷공간의 사이버성, 인터넷활동의 익명성, 지령(指令)의 은밀성은 마약밀수가 온라인상으로 발전하게 하였고 날로 창궐하게 되었다. 행위자는 일반적으로 전문쇼핑사이트를 통하여 위장을 걸친 마약을 매매하는데 전반 매매과정은 몇개의 간단한 조작만 거치면 되므로 본금이 적게 들고 이에 대한 수사는 어려울 수밖에 없다. 2012년 3월, 길림경찰은 전국 18개성을 거친 400여명의 혐의자가 있는 특대형 인터넷 마약밀수사건을 해명하였는데 이 사건 중에서 QQ등 인터넷채팅도구와 토보우(淘寶) 등 인터넷쇼핑사이트가 마약을 판매, 흡식하는 비밀통로가 되었다.

사) 인터넷 가짜제품 제작 및 판매(網絡制假售假)

인터넷 전자비즈니스의 발전은 이미 사람들의 소비습관을 개변시켜 인터넷쇼핑은 현재 젊은 세대들의 첫 선택이 되었다. 아이루이컨설팅(艾瑞咨询)의 데이터

에 근거하면, 2012년 전 3분기 중국 인터넷 쇼핑시장교역규모는 7807.7억 위안에 달하였고 이는 2011년과 비교할 때 7665.8억을 초과하여, 중국 전 3분기 사회소비품 소매총액의 5.2%를 차지하였다. 이와 동시에 인터넷상의 가짜제품 제작 및 판매가 창궐하였다. 인터넷가짜제품 제작 및 판매는 주로 가짜증서, 가짜인장, 가짜 술담배, 가짜약, 가짜생활용품 등을 포함한다. 심천〈경보(晶报)〉조사에 따르면, 현재 토보우 사이트에서 가짜제품의 비율은 3분의 1을 초과하고 품종은 토보우 상의 거의 모든 온라인 상품을 포함하며 그중 화장품, 핸드폰, 패션, 신발과 액세서리가 제일 많다고 한다. 이로부터 보다시피 인터넷상의 가짜제품제작 및 판매는 종류가 다양하고 수량이 큰 특징이 있으며 인터넷점포를 통해 공개적으로 가짜판매행위를 진행하므로 판매범위가 넓다.

아) 인터넷총기매매(網絡買賣槍支)

〈총기관리법(槍支管理法)〉에는 명확하게 복제총기의 제작 판매를 금지하였으나 불법상인들은 관리를 회피하여 각종 은밀한 수단으로 복제총기를 판매하고 있다. 특히 최근에 들어서서 인터넷쇼핑이 신속하게 발전하면서 인터넷 총기매매가 총기구매자의 제일 중요한 구매도경으로 되었다. 다수의 총기동호인들은 각종 사이트를 통하여 복제총기를 구매하여 자신의 흥취애호를 만족시키면서 복제총기수요에 거대한 구매시장을 형성하였으며 이로 하여 또한 지하산업체인을 형성하고 인터넷총기매매문제를 유발하게 되었다.

자) 인터넷테러활동(網絡恐怖活動)

전통적인 테러활동과 비교하면 인터넷정보전파는 더 편리하고 신속하다. 인터넷은 아주 강한 시효성을 가지고 있어 공간이 테러활동에 대한 제한을 타파하여 테러분자들이 제일 빠른 시간 내에 테러활동을 조작할 수 있게 할 수 있다. 또한 인터넷을 이용하여 테러활동을 진행하면 소요되는 원가가 저렴하고 조작난도가 낮으며 영향이 미칠 수 있는 범위가 넓을 수 있어 테러분자들이 인터넷플랫을 이용하여 테러활동을 진행하고 허위테러정보를 전파하는 것을 선호하고 있다. 최근에 발생한 종말요언, 신강테러분자들이 인터넷을 이용하여 진행한 테러

활동, 농구협회 사이트가 해킹당한 사건, 야후서버가 해킹당한 사건 등 모두가 테러활동 사건들이었다.

3) 사이버범죄의 특징분석

인터넷세계에서는 왜 범죄가 많이 발생하는가? 인터넷 시스템안전의 전형적인 의의상 사이버범죄뿐만 아니라 전통범죄(사기, 도박, 음란 등)도 잇달아 인터넷으로 전이하는 추세이다. 그 원인은 인터넷의 고기술, 낮은 원가, 낮은 리스크, 가상성 등 특점 때문이라고 할 수 있다. 이는 사이버범죄를 전통범죄와 비교하여 볼 때 다른 특징을 찾아볼 수 있다.

가) 사이버범죄의 지능화 기술성 특징

컴퓨터와 인터넷자체는 고기술의 증명이다. 컴퓨터와 인터넷을 이용하여 진행하는 범죄도 마찬가지로 지능화 기술성의 특징을 가지고 있다. 불법적으로 컴퓨터정보시스템에 침입하여 컴퓨터정보시스템기능 혹은 컴퓨터정보시스템에 저장, 처리 혹은 전달중인 데이터와 응용프로그램을 파괴하거나 혹은 고의적으로 컴퓨터바이러스를 제작 전파하는 파괴성 행위 등은 모두 행위자에게 상당한 컴퓨터와 인터넷전문지식이 있어야 하고 인터넷언어에 정통하고 계산기 프로그램과 정보네트워크운행규칙을 잘 알고 있어야 하며 그중에서도 많은 기타방면의 지식배경(예를 들면 금융제도, 비밀번호기술)을 장악하고 있어야 한다. 컴퓨터 인터넷을 이용하여 전통 범죄를 실시한다 해도 일정한 기술함량이 있어야 한다. 간략히 말하면 컴퓨터 사이버범죄는 하나의 “기술일”이다.

나) 사이버범죄자들의 문화소질이 높고 연령구조가 젊은 특징

사이버범죄는 전문지식과 기능이 필요하다. 이로 인하여 사이버범죄의 행위자는 일정한 문화수준을 구비하고 있어야 하고 자주 인터넷을 이용하는 젊은 세대여야 한다. 소주시 검찰원 연구팀이 작성한 소주시 2007-2010년 사이버 범죄통계 분석에서 볼 수 있다시피, 사이버범죄의 피고인 중 중학교 이하의 문화정도

가 7.22%를 차지하고 중학교 이상의 문화정도가 92.78%를 차지하며, 고등학교 이상의 문화정도가 57.72%를 차지한다. 또한 단과대학 이상의 문화정도가 36.59%를 차지하여 사이버범죄피고인의 문화수준은 비교적 높다고 말할 수 있다. 연령구조를 놓고 보면, 사이버범죄의 연령은 청년을 위주로 하는데 158명이 18~35세에 속하는데 이는 통계 총 샘플수의 81.03%를 차지한다. 이는 이 연령층의 인원들이 기본적으로 현대기술발전의 영향을 받고 있음을 반영한다. 컴퓨터와 인터넷 사용상의 우세와 사이버범죄주체의 젊음화는 네티즌이 젊은 세대의 비율이 큰 것 및 젊은이들이 인터넷을 즐겨하는 특유의 심리상태등과도 큰 관계가 있다.[129]

다) 사이버범죄의 저렴한 원가, 넓은 전파, 광범위한 영향

사이버범죄는 많은 인력과 재력을 소비할 필요가 없고 단지 한대의 컴퓨터, 하나의 전화선, 하나의 모뎀만 있으면 전 세계적인 컴퓨터인터넷에 연결할 수 있고 대형서버가 사건발생지와 떨어져 있으므로 이런 범죄활동을 조작하려면 아주 편리하다.[130] 사이버세계는 가상공간이고 물리적인 장애가 없고 전 세계가 동시에 인터넷상의 정보를 공유할 수 있다. 이로 인하여 사이버범죄의 전파는 더 광범위하고 피해민중은 더 많으며, 조성된 후과는 더 엄중하다. 2012년 장사경찰은 "중국 자원부"라는 정보매매집단을 타격하였다. 범죄혐의자들의 컴퓨터에서 저장된 공민개인정보는 중국에서의 거의 모든 성(省)에 미치고 총량은 1.5억 건 이상에 달하였는데, 이에는 성명, 전화, 주소, 부동산정보, 차량정보, 통화기록, 비행기록 등이 있었다. 정보내용은 종류가 다양하고 자세하기로 사람들을 경악하게 하였다.[131]

라) 사이버범죄는 강한 은밀성, 증거확보가 어렵고 수사가 어려운 점이 있다. 인터넷사이버공간의 특성은 사이버범죄의 은밀성을 결정하였다. 시간상으로

129) 參見李贊等, "蘇州市2007-2010年網路犯罪調查分析", 중국형사법잡지 2011년 제10기.

130) 參見卓翔, "網路犯罪綜合治理刑事政策芻議", 복건정법관리간부학원학보 2002년 제4기.

131) 新華網, "網路資訊保護路在何方?"; http://news.xinhuanet.com/politics/2012-12/22/c_114120113.htm.

볼 때 24시간 내내 사건을 조작할 수 있고 공간상으로 볼 때 인터넷상으로 범죄 혐의자는 임의의 인터넷이 연결되어 있는 컴퓨터가 있는 장소에서 범죄를 실시할 수 있으며 처음부터 마지막까지 피해자를 접촉하지 않을 수 있다. 정보데이터는 원래 보이지 않고 만질 수 없다. 대다수 사이버범죄자들은 프로그램과 데이터를 통하여 이런 무형의 조작으로 범죄를 실현하여 직접대상도 바로 무형의 전자데이터와 정보가 된다. 동시에 사이버범죄의 증거가 소프트웨어에 있으므로 범죄분자들이 쉽게 전이 혹은 소멸할 수 있어, 특히는 원격컴퓨터 통신네트워크를 이용하여 실시한 범죄는 추측하기 아주 어렵다. 설사 증거를 찾아냈다 하여도 범죄분자는 이미 도주한지 오래라서 이는 또한 사건해명의 난도를 높였다.[132] 미국 연방조사국 전국 사이버범죄 특파팀의 추측에 의하면 약 1%가 발견되고 발견된 사건 중 약 4%만 수사기관에 넘겨진다고 한다. 때문에 인터넷세계의 범죄는 85%~97%의 암수범죄(犯罪黑數)가 존재한다.[133]

마) 사이버범죄는 다지역성, 다국계성을 가지고 있다. 정보네트워크세계는 사통발달한 공간이고 지역과 국가의 제한을 받지 않는다. 이는 사이버공간의 쌍방성, 다방성 교류를 가능하게 하였다. 사이버범죄가 사이버공간에서 발생하게 되어 전통적인 형법상의 "범죄현장"성이 없어 전통범죄행위상에 공간상의 도전을 초래하였다. 또 각 국가, 각 지구간의 사이버범죄관할지의 인정이 극히 불통일적이라고 할 수 있다. 이런 범죄객관상의 은밀성은 행위인의 주관상의 요행(僥幸)심리와 사후 죄책감을 경감하게 하였을 뿐만 아니라 범죄분자가 연속적으로 범죄를 실시할 수 있는 거대한 가능성을 제공하였다.[134]

132) 參見卓翔, "網路犯罪綜合治理刑事政策芻議", 복건정법관리간부학원학보 2002년 제4기.

133) 參見楊堅爭/時啟亮, "電腦與網路法講座", 우전기업관리 2001년 18기.

134) 魏紅/劉學文, "網路犯罪的形勢及其對國際刑法的影響", 정치여법률 2007년 제1기.

나. 사이버범죄를 다스림에 있어서의 문제와 도전

1) 예방이 어렵다: 발견이 발생보다 늦다.

인터넷기술과 응용서비스 창신주기는 짧지만 전파확산속도는 빠르다. 많은 사람들이 새로운 인터넷서비스를 접촉시도 혹은 사용하고 있을 때 불법범죄동기가 있는 자들은 이미 들어도 못 본 새로운 형식과 수단으로 불법행위를 실시하고 있다. 공중의 예방의식이나 사회공제기구의 주시 정도나 기술대응과 타격조치는 선명하게 "지연성"을 가지고 있다. 사이버범죄는 늘 "먼저 발생하고, 사후에 처리"하는 국면을 형성하므로 예방난도가 엄청 크다.[135]

2) 증거확보가 어렵다: 전자증거라서 고정하기 어렵다.

사이버범죄는 인터넷하드웨어와 소프트웨어를 물리적 기술기초로 하는 사이버공간에서 발생하므로 행위자의 진실한 신분과 실제주소를 추적하기 어렵게 하였다. 관련 위법범죄행위의 흔적도 많게 혹은 적게 전자정보의 형식으로 표현되어 증거가 쉽게 지워질 수 있고 증거의 확보도 높은 정보와 인터넷 기술상의 지지를 필요로 한다. 또한 전자데이터증거의 진실성과 관련성도 실천 중에서 아주 쉽게 쟁론을 일으킬 수 있다. 이는 모두 법에 따라 사이버범죄를 타격함에 있어서의 난도를 높였다.[136]

3) 수사가 어렵다: 고기술성과 무경계선성은 수사에 어려움을 주고 있다.

사이버범죄는 일정한 기술함량을 가지고 있고 많은 해커들이 가지고 있는 기술수단은 인터넷경찰이 장악하고 있는 인터넷기술을 초과하여 전자증거가 쉽게 소멸되고 고정이 어려우며 이 모든 것은 사이버범죄의 수사에 적지 않은 기술도전을 가져왔다. 사이버범죄의 무경계선성은 국제형사수사에 큰 영향을 주었다. "중국음란사이트제일사건"이라고 불리는 "구구음란칼럼안(九九情色论坛案)"은 바

135) 參見《報告》.

136) 參見《報告》.

로 http://www.99bbs.com 도메인 네임을 통하여 국내에서 음란영리행위를 전개하는 사이트인데 서버를 미국에 설치하였고 등록한 회원이 30만 명을 초과하였으며 2004년 11월까지 초보적인 통계에 따르면 조회수가 4억여 회에 달하며 온라인접속자수가 매 10분에 15,000명에 달했다고 한다. 조성한 사회위해성은 국내범죄자가 국외와 결탁하여 국경외 서버를 이용한 다국적 인터넷 음란위법범죄의 전형적인 사건이 되었다. 마지막으로 2004년 12월, 공안부의 지도 협조하에 안휘성(安徽省) 공안청에서 국경내의 사이트 관리수호체계를 소멸하고 사건유관 범죄혐의자 12명을 체포하였다. 하지만 미국에서는 음란서비스가 범죄라고 인정하지 않고 중미 양국 간에도 통일된 사이버 범죄형사 수사협조체제가 없고, 쌍방인도조약도 체결하지 않은 상황이라서 국외의 범죄분자들에 대해 근본적으로 타격을 진행할 수 없다는 것이 실정이다.[137]

4) 관할이 어렵다: 무경계선성은 관할에 어려움을 주고 있다.

사이버범죄의 개방성, 허위성, 국제성 특징으로 인해 사이버범죄의 징벌이 가져온 제일 큰 도전은 바로 전통국제형사 관할권 문제이다. 사이버 범죄행위는 충분하게 인터넷이 국경이 없는 특점을 이용하여 대량으로 다국적 범죄행위형식으로 행해지고 있다. 많은 상황하에 상이한 국가가 범죄에 대한 법률정의가 다름으로 하여 사이버다국적범죄를 타격할 때 반드시 유관행위가 동시에 양국의 법률에 저촉될 때만이 합작의 기초로 간주될 수 있다. 동시에 타격원가와 협조체제에도 적지 않은 어려움이 있다. 2000년에 백여억 달러의 경제손실을 조성한 "애충(愛虫)" 바이러스를 조작한 필리핀대학생 구츠만은 여러 나라에서 인도할 요구를 제기하였으나 짧게 감옥살이를 하다가 무죄 석방되었다. 그 이유는 단지 필리핀에서 당시 이런 유형의 사이버범죄를 타격하는 유관 법률이 없었기 때문이었다. [138]

137) 参见魏彦/刘学文, "网络犯罪的形势及其对国际刑法的影响", 정치여법률 2007년 제1기.

138) 参见高富平主编, "电子商务法律指南", 법률출판사 2003년판 제717-718면.

다. 사이버범죄형사정책 : "기술로 기술을 대응"

사이버범죄는 일종 기술범죄이므로 충족한 기술수단이 있어야만 예방 및 제지할 수 있다. 정보안전기술은 사이버정보안전을 실현하는 중요한 보장이고 인터넷정보안전수준을 제고하려면 반드시 좋은 안전기술로서 이를 지지하여야 한다. 이는 인터넷안전기술과 안전설비의 연구개발을 하루빨리 추진하여야 하며 이로 인해 국가는 반드시 이방면의 투자를 고려하여야 한다. 중요한 부서정보망에 대하여는 기술안전방비를 강화하고 인터넷안전기술을 개발하여 비밀번호추가, 인터넷침입예비경보처리 및 방비, 불법정보 저장기술 방지, 해커의 발원지 추적시스템, 바이러스 테스트와 소멸기술 및 데이터 비밀번호기술, 인터넷감시 및 안전성분석 등 인터넷안전보호시스템을 완벽화하여야 한다. 기업에서 자아보호를 강화하는 것을 격려하고 사이버범죄의 침해를 방비하여야 한다. 공격을 회피하기 위해 다수의 각 나라 정부는 실천중 기업에서 자아보호를 강화하는 것을 격려하는 방식을 취하고 있다. 예를 들면 모든 시스템과 서버에 패치프로그램을 추가하고 복잡한 비밀번호와 방화벽설치를 요구하며 인터넷에 대하여 자주 스캔하고 또 기타 인터넷 안전조치를 취하여 종합성적인 보호체계를 수립하는 것이다.[139]

첫째, 공안부문에 전문적으로 사이버범죄를 다스리는 인터넷기술과 교육센터를 건설한다. 비록 우리나라 공안부문에 인터넷 감시부서가 있기는 하지만 이는 전문성이 부족하고 사회참여도도 높지 않다. 그리고 수사에 치우쳐 예방성과 기술성조치의 지도와 교육이 부족하다. 미국의 NCFTA(미국국가인터넷 형사감시 및 훈련연맹)을 모델로 하여 중국버전의 NCFTA를 창립하여 사이버범죄에 대응할 수 있다. NCFTA는 미국연방조사국(FBI), 정보안전대회사 사이먼태크(赛门铁克), 카내지 메롱(卡内基·梅隆)대학 등 산관학(产官学) 세 개의 구성원으로 형성된 단체인데 이는 1997년에 설립된 것이다. 정부와 민간은 같이 일종 사이버범죄수단, 사이버 바이러스정보 등 방면의 방대한 데이터를 건립하였고 대학연구자들로부터 분석을 진행하여 수사인원을 훈련하고 사이버범죄에 대응하였다. 일

139) 參見卓翔, "網路犯罪綜合治理刑事政策芻議", 복건정법관리간부학원학보 2002년 제4기.

본경찰청도 사이버범죄정보를 분석하고 인터넷 수사원의 기능을 제고하는 새로운 조직(일본판 NCFTA)을 건립하려고 한다. 둘째로, 중점적으로 사이버 신기술의 개발, 모니터링을 통해 사이버범죄를 예방 및 타격해야 한다. 셋째, 부단히 기술수단을 업데이트하여 인터넷수사와 증거확보를 진행하여 인터넷기술의 국제협력을 전개하여야 한다. 마지막으로 부단히 사이버범죄의 국내입법과 국제입법을 완비하고 사이버범죄의 국제간의 협력을 강화하여야 한다.

라. 사이버범죄를 다스림에 있어서 가치충돌 : 경계는 질서의 이름을 빌어 자유를 희생할 수 있다

법의 여러 가치—정의, 자유, 질서, 안전, 효율 중 질서는 제일 기초적인 가치이다. 질서는 본질상 조직화의 활동방식이고 임의의 가치추구가 모두 조직이 있으며 목적성과 방향성이 있는 활동은 모두 일정한 질서에 의거하여 진행되어 가며 질서가치는 기타 가치실현의 기초라고 할 수 있다.[140] 제일 기본적인 질서를 떠나서는 자유, 정의 등 기타 가치는 실현하기 어렵다. 이로 인하여 질서는 입법자들이 특별히 편애하는 가치이고 또 입법 시 우선적으로 고려하는 가치이기도 하다. 입법자들의 입장에서 보면, 질서는 사회존재의 최소공약수이고 최저한도의 사회공동의식에 도달하게 하는 기초이다. 자유는 질서추구의 최종목표이고 질서는 자유실현의 기본전제이다. 단 양자는 절대적인 통일이 아니다. 자유가 강조하는 것은 주체개성의 발휘이고 질서가 강조하는 것은 서열이 있는 상태의 건립과 유지이다. 자유는 질서의 고유한 형평을 파괴하고 질서는 일정한 정도에서 자유를 제약하며 평형의 규정성을 유지한다. 이로 하여 양자간의 충돌은 회피할 수 없다.[141] 인터넷 관할과정 중에서, 특별히 언론에 대하여 여과하고 혹은 실명제 방식으로 사이버범죄를 예방할 때 질서와 자유가치의 평형에 주의를 기울여서 질서를 유지하는데 신경을 써야 한다.

인터넷실명제를 예로 들면, 2010년부터 웨이버가 전 중국 네티즌의 생활에서 아주 중요한 역할을 하게 되었다. 2011년 12월, 북경시 공안국 등 4개 단위에서

140) 參見龍文燮, "'自由與秩序的法律價值衝突'辨析", 북경대학학보(철학사회과학판) 2000년 제4기.

141) 參見卓澤淵著, "法的價值論", 북경대학출판사 1999년판 제635-636면.

연합 발표한〈북경시 웨이버 발전관리에 관한 약간의 규정(北京市微博客發展管理若幹規定)〉, 제9조에서 규정하기를 "임의의 조직 혹은 개인이 웨이버를 등록, 조작, 복제, 발표, 정보내용전파는 진실한 신상정보를 사용하여 진행해야 하고 허위 혹은 도용한 주민등록증 정보, 기업등록 정보, 조직기구 번호정보로 등록하면 아니된다"고 하였다. 이 규정은 〈웨이버실명제〉로 약칭되어 신속히 전 국민의 최대관심사가 되었다. 2012년 3월 16일, 신랑, 소후, 왕이와 텅쉰(新浪, 搜狐, 网易和腾讯)은 정식 및 공동으로 웨이버 실명제를 실행하였다. 2012년 12월 28일, 제11기전국인민대표대회 상무위원회 제30차 회의에서 심의통과된 〈인터넷정보보호를 강화에 관한 결정초안(關于加強網絡信息保護的決定草案)〉에서는 "인터넷 서비스제공자가 사용자에게 사이트접속서비스를 제공하고 전화와 핸드폰 등의 인터넷 가입을 제공하거나 사용자에게 정보발표서비스를 제공하여 사용자와 협정을 체결할 때는 진실한 신분정보를 요구해야 한다"고 규정하였다. 2013년 3월 29일, 국무원반공청(办公厅)이 반포한 〈국무원 기구개혁과 직책 전이방안을 실시하는데 관한 임무분공통지(關于實施《國務院機構改革和職能轉變方案》任務分工的通知〉에서 "2014년 완성 해야할 임무" 제13조가 바로 "정보 네트워크 실명 등록제도를 발표 및 실행하는 것"[공업과 정보화부(工业和信息化部), 국가인터넷 정보판공실(国家互联网信息办公室) 공안부(公安部)와 책임진다. 2014년 6월말 전에 완성]이다. 2013년 6월 28일, 공신부(工信部)에서 발표한 〈전화사용자진실신분정보등록규정(電話用戶真實身份信息登記規定)〉에서는 "핸드폰사용자, 전화사용자, 네티즌 심지어 무선 네트워크 카드사용자 모두가 실명등록을 진행해야 한다"고 규정을 두고 있다. "먼저 등록하고 후에 서비스"하는 새로운 규정은 2013년 9월 1일부터 정식으로 실행되었다. 인터넷실명제는 이미 중국에서 보급되었고 이미 필연적인 발전추세로 되었다.

웨이버 실명제가 실행되기 전야, 모 사이트에서는 웨이버 사용자에 대하여 조사를 진행하였는데 데이터가 보여주기를 〈웨이버가 실명제를 실행하면 사용을 포기하겠다〉는 비율이 89%를 차지했다.[142] 사용자가 실명제 실행 후 계속 웨이버를 사용한다고 하여도, 실명제로 인한 언론공제와 우려는 웨이버의 매력을 떨

142) 劉建 : "微博即將實名制, 方便了誰? 傷害了誰?" http://soft.zol.com.cn/272/2726275.html.

어지게 할 것이고 또는 웨이버를 사용하는 흥취가 무쟁론한 오락 및 사회화제에 집중되게 할 것이며 또는 부분적인 웨이버 사용자들이 다른 익명성적인 공공블로그에 전이 할 것이다. 실명제는 "불법언론"의 오물을 퍼부음과 동시에 그릇까지 버릴 가능성이 아주 높다. 이로 인하여 인터넷실명제의 적용은 다른 영역을 통하여 진행하여야 한다. 인터넷언론 영역에서 인터넷질서와 익명자유표현의 가치충돌에서 응당 이익고려를 진행해야 한다. 실명제의 실시는 모두 〈이득이 손해보다 적은〉결과를 초래하게 되어 반드시 연기실행 하여야 한다. 기타 영역을 예로 들면 인터넷 비즈니스, 인터넷사교(혼인사이트), 인터넷게임 등 안전, 질서, 건강(미성년자가 게임에 빠져있는 것)등 가치는 자유가치에 비해 압도성적인 승리를 가져왔으므로 실명제의 정당성이 추진되고 있다.

제4절 사이버범죄 관련 규정

1. 사이버전쟁 영역에서의 규정

전쟁과 같이 국가 간의 문제는 주로 국제법적인 문제로 다루어지기 때문에 주로 조약이나 협정 등의 형태를 띠게 된다. 그러므로 사이버전쟁 영역에서의 규정들은 조약에서 그 근거를 찾아볼 수 있을 것이다. 그러나 사이버전쟁과 관련된 규정은 아직까지 마련되어 있지 않다. 그런 가운데 최근 사이버전쟁과 관련된 지침 형태의 탈린 매뉴얼이 만들어져 주목을 받고 있다. 따라서 사이버전쟁 영역과 관련된 내용을 담고 있는 탈린 매뉴얼을 살펴볼 필요가 있다.

가. 탈린 매뉴얼의 배경

일반적으로 전쟁과 범죄는 명확하게 구분이 된다. 그러므로 현실공간에서 범죄에 대해서는 각 국의 형법이 적용될 수 있지만, 전쟁에 있어서는 국제공법인 전쟁법이 적용될 수 있다. 그런데 사이버 공격에 있어서는 사이버공간에서의 행위의 성격상 현실공간과 달리 명확하게 구분되지 않는 측면이 있다. 따라서 미

국방부가 마련한 사이버 전쟁 전력을 보면 미국의 주요시설이 사이버공격을 당할 경우 미사일을 사용하여 물리적으로 타격을 하겠다고 공공연하게 밝히기도 하였다.[143] 그런 문제들로 인해 현실공간에서의 전쟁법과 같이 사이버공간에서도 적용될 수 있는 규정이 필요하다는 주장이 제기되었으며, 그런 개념의 선상에서 사이버전에 적용될 수 있는 국제법 매뉴얼이 북대서양조약기구(NATO) 합동 사이버방위센터(CCDCOE)의 주도하에 마련되기에 이르렀다. 그 결과물로 나온 것이 비록 강제적인 효력은 없지만 사이버전에 대한 지침 역할을 하게 될 '탈린 매뉴얼(Tallinn Manual)'이라고 할 수 있다.

탈린 매뉴얼이 탄생하게 된 배경에는 2007년 러시아가 DDoS 공격을 가하여 에스토니아의 정부와 국회, 언론사, 은행 등 인터넷 망을 2주 동안 마비시킨 사건이 있다. 사실 사이버 공격이 탈린에 있던 소련군의 동상을 외각으로 옮긴 이후에 시작되었기 때문에 러시아가 사이버공격의 주체로 지목되었으나, 러시아가 그를 부인하였기 때문에 러시아의 소행이라고 단정 지을 수는 없다.[144] 이처럼 에스토니아의 수도인 탈린에서 발생한 사이버 공격이 발단이 되어 사이버전에 있어서의 교전 수칙의 필요성이 제기되었다. 이에 사이버전에 대한 연구와 토론회가 진행되면서 영국과 미국, 독일, 호주 등의 국제법, 정보기술, 군사 전문가 23명이 지난 3월에 나토의 사이버방위센터의 위탁을 받아서 약 3년에 걸쳐 사이버전과 관련된 세계 최초의 문서인 탈린 매뉴얼을 작성하였다.[145] 탈린 매뉴얼은 총 95개 조항의 교전수칙을 규정하고 있으며, 국제적으로 구속력이 있는 문서는 아니므로 사이버전 지침에 해당한다고 할 수 있다. 우리나라의 경우에도 일전에 있었던 북한의 GPS 신호교란 행위에 대한 즉각적인 무력대응은 유엔헌장 51조에 따른 자위권 발동 기준으로 인해 제약될 수 있으며(특히 비례적인 대응), 현재의 국제법 법리에 따라 사이버공격에 대해서는 사이버공격과 동일 수준의 전자전으로 대응할 수밖에 없는 어려움이 존재하기 때문에 사이버전에 적합한 규정이 필요하다는 주장이 제기되고 있다.[146]

143) http://www.naeil.com/News/economy/ViewNews.asp?nnum=706123&sid=E&tid=3.

144) http://news.donga.com/3/all/20130411/54378689/1.

145) http://blog.naver.com/PostList.nhn?blogId=cspark14; 박춘식의 월요 보안정보(250) 참조.

146) http://kookbang.dema.mil.kr/kookbangWeb/view.do?bbs_id=BBSMSTR_000000000251&ntt

나. 탈린 매뉴얼의 내용

탈린 매뉴얼은 크게 국제 사이버 보안법(International cyber security law) 부분과 사이버 무력충돌에 관한 법(The law of cyber armed conflict)으로 나누어져 있으며, 다시 전자는 국가와 사이버공간(States and cyberspace)과 무력사용(The use of force)으로 구성되어 총 19개의 규정이 있으며, 후자는 무력충돌에 관한 법일반(The law of armed conflict generally), 적대행위들(Conduct of hostilities), 특정 사람들, 사물들, 활동들(Certain persons, objects, and activities), 주둔(Occupation), 중립(Neutrality)으로 나누어져 총 76개 규정이 마련되어 있다.[147]

탈린 매뉴얼과 관련해서 크게 세 가지 미신이 지적되기도 했는데, 하나는 탈린 매뉴얼이 나토의 지령에 의한 것이라는 것인데, 탈린 매뉴얼은 순수하게 참여자들의 개인적 역량의 결과물이라는 것이다. 또 하나로 탈린 매뉴얼에 따르면 스턱스넷(Stexnet)이 미국에 의한 전쟁행위라는 것인데 그것도 사실과 다르다고 한다. 그리고 탈린 매뉴얼을 통해 각 정부들이 해커를 죽일 수 있는 것을 허용한다고 하는 것도 잘못된 인식이라는 것을 밝히고 있다.[148]

특히 탈린 매뉴얼에서는 사이버전과 관련된 다양한 정의를 규정하고 있다. 이런 정의들은 일반적인 사이버범죄와는 다소 다르다고 할 수 있는데, 예를 들어, 탈린 매뉴얼에서 사이버 공격이란 공격적이든 방어적이든 간에 사람에게 상처를 입히거나 사망에 이르게 하는 것, 또는 사물을 손상시키거나 파괴하는 것이 합리적으로 예견되는 사이버 작전을 의미하게 된다.[149] 이와 함께 탈린 매뉴얼에는 사이버전과 관련된 다양한 내용들이 규정되어 있는데, 탈린 매뉴얼의 전체적인 규정 내용들은 다음과 같다.

_writ_date=20130419&parent_no=1.

147) 이에 대한 논지는 Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambrige University Press, 2013 참조.

148) http://www.acus.org/files/tallinn_fact_sheet_20130322.pdf.

149) Michael N. Schmitt, 앞의 책, 106면.

표 2 규정내용

규정 내용	
Part I: International cyber security law	
1. States and cyberspace	
Section 1: Sovereignty, jurisdiction, and control	Rule 1 – Sovereignty
	Rule 2 – Jurisdiction
	Rule 3 – Jurisdiction of flag States and States of registration
	Rule 4 – Sovereign immunity and inviolability
	Rule 5 – Control of cyber infrastructure
Section 2: State responsibility	Rule 6 – Legal responsibility of States
	Rule 7 – Cyber operations launched from governmental cyber infrastructure
	Rule 8 – Cyber operations routed through a State
	Rule 9 – Countermeasures
2. The use of force	
Section 1: Prohibition of the use of force	Rule 10 – Prohibition of threat or use of force
	Rule 11 – Definition of use of force
	Rule 12 – Defnition of threat of force
Section 2: Self-defence	Rule 13 – Self-defence against armed attack
	Rule 14 – Necessity and proportionality
	Rule 15 – Imminence and immediacy
	Rule 16 – Collective self-defence
	Rule 17 – Reporting measures of self-defence
Section 3: Actions of international governmental organizations	Rule 18 – United Nations Security Council
	Rule 19 – Regional organizations
Part II: The law of cyber armed conflict	
3. The law of armed conflict generally	
	Rule 20 – Applicability of the law of armed conflict
	Rule 21 – Geographical Limitations
	Rule 22 – Characterization as international armed conflict
	Rule 23 – Characterization as non-international armed conflict
	Rule 24 – Criminal responsibility of commanders and superiors
4. Conduct of hostilities	

Section 1: Participation in armed conflict	Rule 25 – Participation generally
	Rule 26 – Members of the armed forces
	Rule 27 – Levèe en masse
	Rule 28 – Mercenaries
	Rule 29 – Civilians
Section 2: Attacks generally	Rule 30 – Definition of cyber attack
	Rule 31 – Distinction
Section 3: Attacks against persons	Rule 32 – Prohibition on attacking civilians
	Rule 33 – Doubt as to status of persons
	Rule 34 – Persons as lawful objects of attack
	Rule 35 – Civilian direct participants in hostilities
	Rule 36 – Terror attacks
Section 4: Attacks against objects	Rule 37 – Prohibition on attacking civilian objects
	Rule 38 – Civilian objects and military objectives
	Rule 39 – Objects used for civilian and military purposes
	Rule 40 – Doubt as to status of objects
Section 5: Means and methods of warfare	Rule 41 – Definitions of means and methods of warfare
	Rule 42 – Superfluous injury on unnecessary suffering
	Rule 43 – Indiscriminate means or methods
	Rule 44 – Cyber body traps
	Rule 45 – Starvation
	Rule 46 – Belligerent reprisals
	Rule 47 – Reprisals under Additional Protocol I
	Rule 48 – Weapons review
Section 6: Conduct of attacks	Rule 49 – Indiscriminate attacks
	Rule 50 – Clearly separated and distinct military objectives
	Rule 51 – Proportionality
Section 7: Precautions	Rule 52 – Constant care
	Rule 53 – Verification of targets
	Rule 54 – Choice of means or methods
	Rule 55 – Precautions as to proportionality
	Rule 56 – Choice of targets
	Rule 57 – Cancellation or suspension of attack
	Rule 58 – Warnings
	Rule 59 – Precautions against the effects of cyber attacks

Section 8: Perfidy, improper use, and espionage	Rule 60 – Perfidy
	Rule 61 – Ruses
	Rule 62 – Improper use of the protective indicators
	Rule 63 – Improper use of United Nations emblem
	Rule 64 – Improper use of enemy indicators
	Rule 65 – Improper use of neutral indicators
	Rule 66 – Cyber espionage
Section 9: Blockade and zones	Rule 67 – Maintenance and enforcement of blockade
	Rule 68 – Effect of blockade on neutral activities
	Rule 69 – Zones
	5. Certain persons, objects, and activities
Section 1: Medical and religious personnel and medical units, transports, and material	Rule 70 – Medical and religious personnel, medical units and transports
	Rule 71 – Medical computers, computer networks, and data
	Rule 72 – Identification
	Rule 73 – Loss of protection and warnings
Section 2: United Nations Personnel, installations, materiel, units, and vehicles	Rule 74 – United Nations personnel, installations, materiel, units, and vehicles
Section 3: Detained persons	Rule 75 – Protection of detained persons
	Rule 76 – Correspondence of detained persons
	Rule 77 – Compelled participation in military activities
Section 4: Children	Rule 78 – Protection of children
Section 5: Journalists	Rule 79 – Protection of journalists
Section 6: Installations containing dangerous forces	Rule 80 – Duty of care during attacks on dams, dykes, and nuclear electrical generating stations
Section 7: Objects indispensable to the survival of the civilian population	Rule 81 – Protections of objects indispensable to survival

Section 8: Cultural property	Rule 82 – Respect and protection of cultural property
Section 9: The natural environment	Rule 83 – Protection of the natural environment
Section 10: Diplomatic archives and communications	Rule 84 – Protection of diplomatic archives and communications
Section 11: Collective punishment	Rule 85 – Collective punishment
Section 12: Humanitarian assistance	Rule 86 – Humanitarian assistance
6. Occupation	
	Rule 87 – Respect for protected persons in occupied territory
	Rule 88 – Public order and safety in occupied terriory
	Rule 89 – Security of the Occupying Power
	Rule 90 – Confiscation and requisition of property
	Rule 91 – Protection of neutral cyber infrastructure
	Rule 92 – Cyber operations in neutral territory
	Rule 93 – Neutral obligations
	Rule 94 – Response by parties to the conflict to violations
	Rule 95 – Neutrality and Security Council actions

2. 사이버테러 영역에서의 규정

테러와 관련된 특수한 영역의 법률들이 만들어지기 시작한 것은 9·11테러 이후라고 할 수 있을 것이다. 미국의 경우 9·11테러 이후 테러와 관련된 여러 규정들이 도입되었으며, 거기에는 시민의 자유를 상당한 수준까지 제한하는 내용을 담고 있다. 이는 사이버테러 영역에서도 마찬가지라고 할 수 있다. 특히 미국의 경우 9·11 테러 이후 국토안보법(HSA: Homeland Security Act)과 애국법(Patriot Act)이 마련되었고, 독일의 경우 연방수사청법(BKA: Bundes Kriminal

Amt)에 온라인수색(Onlinedurchsuchung)을 비롯하여 테러에 대응할 수 있는 여러 수단들이 규정되기에 이르렀다. 이에 비해 우리나라는 사이버테러 영역이 특별하게 다루어지고 있는 규정은 현재 존재하고 있지 않다. 다만 현재 서상기 의원이 대표발의한 "국가 사이버테러 방지에 관한 법률안(이하 '사이버테러 방지법안'이라고 함)"이 국회에 계류 중에 있다.

사이버테러방지법안의 제안배경은 1·21 인터넷 대란과 같이 최근 우리나라에서 발생하였던 사이버테러에 기인한다. 이미 여러 차례에 걸쳐 우리나라는 사이버테러 공격을 받았지만, 여전히 그 대응은 미진하며, 사이버위기가 국가안보와 국가의 이익에 미치는 영향이 큼에도 불구하고 아직까지도 적절한 대응법률이 미흡한 실정이다. 그러므로 사이버테러와 관련해서 사이버테러를 사전에 탐지하여 예방하고, 사이버테러가 발생하였을 경우 조속히 문제를 해결하는 것이 동 법안의 목적이라고 할 수 있다.[150]

동 법안의 가장 큰 특징을 들자면, 현재 실질적으로는 사이버테러에 대해 국가정보원이 컨트롤타워의 역할을 수행하고 있지만, 법률에 명확히 근거하고 있지 않은 실정이다. 따라서 동 법안에서는 국가정보원에게 사이버테러에 대한 권한을 주는 것을 명확하게 하고 있다는 것이다. 그러나 해당 법률에 따르면 현재에도 많은 권한을 가지고 있는 정보기관인 국가정보원에게 과도한 권한이 집중되는 결과를 가져올 수 있으며, 따라서 야당에서는 민간인 사찰에 대한 수단으로 이용될 수 있다는 이유로 법안의 처리에 난색을 표하고 있다.[151] 따라서 일각에서는 법률에 사이버테러 전담기구를 명시함과 동시에 제도적인 견제장치가 필요하다고 하기도 한다. 그러므로 사이버테러 기관에 집중되는 권력을 견제하기 위해 의회에 대한 보고 및 감사 의무 등을 함께 명시할 필요가 있다고 한다.[152]

사이버테러 방지법안은 "국가 사이버테러 방지에 관한 기본적인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버위기 발생 시 국가 역

150) 국가 사이버테러방지에 관한 법률(의안번호 1904459)의 제안이유 참조.

151) http://news1.kr/articles/1097442.

152) 심우민, "최근 전산망 마비사태와 사이버 테러 대응체계 개선방안", 국회입법조사처 이슈와 논점 제160호, 2013.4.18.

량을 결집하여 신속하게 대처함으로써 국가의 안전보장과 이익보호에 이바지함”을 그 목적으로 삼고 있다(제1조). 그리고 동 법안에서는 사이버테러에 대한 정의를 “해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡전파 하는 등 모든 공격행위”라고 하고 있다(제2조 제1호).

3. 사이버범죄 영역에서의 규정

가. 사이버범죄 관련 규정

현재 우리나라의 사이버범죄와 관련된 규정은 여러 법률에 분산되어 규정되어 있다. 형법뿐 아니라 사이버범죄 기본법이라고 여겨질 수 있는 정보통신망법, 전기통신기본법, 성폭력범죄의 처벌 등에 관한 특례법, 신용정보의 이용 및 보호에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률, 정보통신기반 보호법 등 수 많은 법률들에 사이버범죄와 관련된 행위들이 조각조각 규정되어 있다. 그러나 개별법에서 규정하고 있는 사이버범죄의 유형을 보면 일정한 유형들은 공통되는 것이 발견되기도 한다. 특히 개인정보나 비밀침해 등의 규정을 보면 그러하다. 또한 특별법 규정들을 보면 형사벌로 처벌되어야 하는 행위와 그 외에 행정벌 등으로 처벌되어야 하는 행위의 구분이 명확하지 않은 것이 발견된다. 그러므로 사이버범죄를 규정해 놓은 주요 규정들 가운데 공통되는 행위유형을 도출해 보고, 공통되는 행위유형은 보다 일반화 시켜 형법에 규정하는 것이 적절할 것으로 여겨진다. 또한 낮은 형량의 형벌로 규정되어 있는 행위와 행정벌 등으로 규정되어 있는 행위를 살펴볼 필요가 있다. 이는 비범죄화 또는 범죄화의 논의와 관련이 될 수 있는데, 행정벌로 법률의 목적 달성이 가능한 경우에는 구태여 형벌을 부과할 필요가 없게 된다. 다만, 여기에서는 주요 사이버범죄에 규정되어 있는 행위 유형들을 살펴보고, 공통되는 행위 유형을 도출해 보는 작업을 수행해 보고자 한다.

나. 주요 법률 규정

1) 정보통신망법

정보통신망법은 본래 "전산망의 개발보급과 이용 등을 촉진하여 정보화사회의 기반을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지함"을 목적으로 해서 제정되었던 '전산망 보급확장과 이용촉진에 관한 법률'(이하 "전산망법"이라고 함)이 그 전신이다. 이후 1999년 2월 8일 미비점과 장래의 발전방향을 수정하여 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"로 전면 개정되었다. 따라서 현행 법률에 따르면 정보통신망법은 "정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함"을 목적으로 삼고 있다.

그러나 사실 정보통신망법은 정보통신망의 이용촉진 보다는 정보보호적인 측면에 좀 더 영향력이 있는 것으로 보인다. 그러므로 현재 정보통신망법은 소위 사이버범죄의 기본법적인 역할을 수행하여 사이버범죄와 관련된 내용이 도입될 경우 주로 동 법률에 규정되고 있다. 이는 동 법률의 개정 횟수를 보면 잘 알 수 있는데, 동 법률의 전신인 전산망법이 제정된 1986년 이래로 이제까지 총 38차례에 걸쳐서 개정되었으며, 이를 보면 정보통신망법이 우리나라의 사이버사회를 보호하는 선두에 서서 총체적인 역할을 수행하고 있다는 것을 나타내는 것이라고 할 수 있다.[153] 이는 아래에서 좀 더 심도 깊게 논의되겠지만, 우리나라의 경우 형법 각론에 새로운 처벌이 규정되는 것이 입법실무적으로 매우 어려운 구조를 가지게 되어 결국 특별법인 정보통신망법을 통해 사이버범죄와 관련된 내용들을 규정하기 때문이다. 그러나 개별법의 난립으로 인해 정보통신망법은 전기통신사업법이나 청소년보호법 등 다른 관련 법률들과 혼선을 빚곤 하며,[154] 동법 제70조에 규정되어 있는 사이버 명예훼손죄의 경우와 같이 형법에 규정될

153) 양재모, 정보통신망법의 발전적 분화와 새로운 통합, 정보통신연구진흥원 학술정보 - 인터넷이슈리포트 2007권 10호, 2007, 10면.

154) 양재모, 앞의 글, 12면.

필요가 있는 일반적인 처벌 내용들도 담고 있는 문제점이 발생하고 있다.[155] 그럼에도 불구하고 정보통신망법은 여전히 사이버범죄에 대한 기본법 역할을 수행하고 있다. 정보통신망법은 제1장 총칙, 제2장 정보통신망의 이용촉진, 제3장 전자문서중계자를 통한 전자문서의 활용, 제4장 개인정보의 보호, 제5장 정보통신망에서의 이용자 보호, 제6장 정보통신망의 안정성 확보, 제7장 통신과금서비스, 제8장 국제협력 등 총 8장 60개 조문으로 규정되어 있다.[156]

2) 정보통신기반보호법

정보통신기반보호법은 1999년 2월 "사이버테러 방지 관계 장관회의"에서 제정을 추진하기로 결정하고, 2000년 5월 (구)정보통신부에서 관계부처 및 학계, 연구계, 산업계 등 전문가와 제정위원회를 구성하여 동년 7월 법률안을 마련하여 공청회를 개최한 후 정식으로 제정되었다.[157] 따라서 2001년 1월 26일 컴퓨터 해킹이나 바이러스 등으로 인해 국가의 주요 정보통신기반시설을 보호하기 위해 제정되었으며, 현재까지 총 7회에 걸쳐 개정작업이 수행되었다. 따라서 동 법률은 "전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것"을 목적으로 삼고 있다(제1조). 정보통신기반보호법은 제1장 총칙, 제2장 주요정보통신기반시설의 보호체계, 제3장 주요정보통신기반시설의 지정 및 취약점 분석, 제4장 주요정보통신기반시설의 보호 및 침해사고의 대응, 제6장 기술지원 및 민간협력, 제7장 벌칙 등 총 6개장 23개 조문으로 구성되어 있다.[158]

155) 이에 대해서는 주승희, "현행 사이버 명예훼손죄 법리의 문제점 및 개선방안 관련 최근 논의 검토", 형사정책연구 제77호, 2009 참조.

156) 특히 개인정보보호법이 제정됨에 따라 개인정보분쟁조정위원회와 관련된 규정이 삭제되었다.

157) 한국정보통신산업협회, 정보통신기반보호법(안), 한국정보통신산업협회, 정보화사회 142, 2000년, 60-61면.

158) 제5장 정보보호컨설팅전문업체의 지정 등에 관한 장과 제17조~제23조의 규정들은 삭제되었다. 이는 2009년 5월 22일 개정에 의해 "정보통신산업 진흥법" 제33조 규정에 따라 삭제된 것이다.

3) 개인정보보호법

과거 사이버범죄는 통신망에 침입하여 주요 기밀을 알아내는 것에 주요 목적이 있었다면, 최근의 사이버범죄는 개인정보가 주요 표적이 되고 있다. 또한 개인정보는 여러 분야에서 사용되기 때문에 개인정보와 관련된 개별법들이 많이 존재하고 있다(우리나라의 법령 가운데 개인정보보호를 규정해 놓은 법령들은 아래와 같다). 그러나 최근 개인정보보호법이 제정되면서 개인정보에 대한 일반 규정이 마련되었다. 다만, 개인정보보호법이 다른 법률들과 상충되는 부분이 있기도 하고, 전자상거래법 등과 같은 다른 개별 법률과 상충되는 부분도 있기 때문에 기업들이나 기관 등이 어려움을 호소하기도 한다.[159] 이와 같은 문제점이 발생한 이유는 개인정보보호법이 보다 체계적이고, 다른 개별 법률과의 관계 등을 고려해서 만들어져야 함에도 불구하고 그런 부분이 미흡했기 때문이다.

개인정보보호법은 제1장 총칙, 제2장 개인정보 보호정책의 수립, 제3장 개인정보의 처리, 제4장 개인정보의 안전한 관리, 제5장 정보주체의 권리 보장, 제6장 개인정보 분쟁조정위원회, 제7장 개인정보 단체소송, 제8장 보칙, 제9장 벌칙 등 총 9개장 75개 조문으로 구성되어 있다.

159) http://www.itdaily.kr/atl/view.asp?a_id=37489.

표 3 관계부처 및 개인정보 관련 법률 현황(18개부처 39개 법률)

부처	법령	대상 및 내용
행정안전부	개인정보보호법	– 관련 법조: 제59조, 제60조 등 – 대상: 공공기관 및 기업, 사인 – 내용: 개인정보 보호를 위한 제반규정들(형사처벌규정 포함) – 처벌규정: 제70조, 제71조, 제72조, 제73조, 제74조(양벌규정), 제75조(과태료 규정)
	공공기관의 정보공개에 관한 법률	– 관련 법조: 제9조 – 대상: 공공기관 – 내용: 공공기관이 보유•관리하는 정보 가운데 개인정보는 원칙적으로 비공개 대상임 – 처벌규정: 없음
	민원사무처리에 관한 법률	– 관련 법조: 제26조 – 대상: 행정기관 및 행정업무 위탁기관•개인 – 내용: 행정기관의 장은 민원인의 신상정보 침해 방지노력 – 처벌규정: 없음
	주민등록법	– 관련 법조: 제30조, 제31조 등 – 대상: 중앙행정기관, 지방자치단체 – 내용: 주민등록정보 관련 보호 의무 – 처벌규정: 제37조, 제38조, 제39조(양벌규정), 제40조(과태료 규정)
	전자정부법	– 관련 법조: 제4조 등 – 대상: 행정기관, 공공기관 – 내용: 개인정보 및 사생활 보호 원칙 – 처벌규정: 제76조, 제77조(양벌규정), 제78조(과태료 규정)
	전자서명법	– 관련 법조: 제24조 등 – 대상: 공인인증기관 – 내용: 인증업무와 관련된 개인정보 보호 – 처벌규정: 제31조, 제32조, 제33조(양벌규정), 제34조(과태료 규정)
	공직자윤리법	– 관련 법조: 제14조, 제28조 등 – 대상: 공직자 재산등록기관 – 내용: 재산등록 사안에 대한 보호 – 처벌규정: 제22조(징계 규정), 제27조, 제28조, 제28조의2
방송통신위원회	정보통신망 이용촉진 및 정보보호에 관한 법률	– 관련 법조: 제22조~제29조, 제71조 등 – 대상: 정보통신서비스 제공자 – 내용: 개인정보의 수집이용 및 제공 등 – 처벌규정: 제71조, 제73조, 제75조(양벌규정), 제76조(과태료 규정)

부처	법령	대상 및 내용
	위치정보의 보호 및 이용 등에 관한 법률	– 관련 법조: 제18조 이하 – 대상: 일반인, 위치정보사업자 – 내용: 개인위치정보 보호 및 제한적 이용 – 처벌규정: 제39조, 제40조, 제42조(양벌규정), 제43조(양벌규정)
	인터넷주소자원에 관한 법률	– 관련 법조: 제15조 – 대상: 인터넷주소관리기관 등 – 내용: 인터넷주소 사용자의 개인정보 보호 – 처벌규정: 없음
금융위원회	**신용정보의 이용 및 보호에 관한 법률**	– 관련 법조: 제16조, 제31조 이하 등 – 대상: 신용정보집중기관, 신용정보회사 등 – 내용: 신용정보주체의 보호 – 처벌규정: 제50조, 제51조(양벌규정), 제52조(과태료 규정)
	보험업법	– 관련 법조: 제177조 – 대상: 보험사업자 – 내용: 개인정보의 누설·제공 금지 – 처벌규정: 제202조, 제208조(양벌규정)
	은행법	– 관련 법조: 제21조의2 – 대상: 금융기관 임직원 – 내용: 공개되지 않은 정보 누설·이용 금지 – 처벌규정: 제66조, 제68조의2(양벌규정)
	금융실명거래 및 비밀보장에 관한 법률	– 관련 법조: 제4조 – 대상: 금융회사 등의 종사자 – 내용: 거래정보의 제공·누설 금지 – 처벌규정: 제6조, 제8조(양벌규정)
보건복지부	**의료법**	– 관련 법조: 제21조 – 대상: 의료인·의료기관 종사자 – 내용: 환자 기록의 열람·사본제공 등 금지 – 처벌규정: 제88조, 제90조, 제91조(양벌규정)
	건강검진기본법	– 관련 법조: 제18조, 제23조 – 대상: 국가건강검진 업무 종사자(또는 종사하였던 자) – 내용: 개인정보 및 사생활 보호 대책 마련 및 비밀누설금지 – 처벌규정: 제28조
	장기등 이식에 관한 법률	– 관련 법조: 제31조 – 대상: 장기이식 관련 기관 종사자 가운데 대통령령으로 정하는 사람 – 내용: 장기등기증자·이식자 등에 대한 비밀유지의무 – 처벌규정: 제49조, 제52조(양벌규정)

부처	법령	대상 및 내용
	생명윤리 및 안전에 관한 법률	– 관련 법조: 제35조 – 대상: 유전자은행의 장 또는 그 종사자 – 내용: 유전정보 제공·부당한 사용 금지 – 처벌규정: 제52조, 제54조(양벌규정), 제55조(과태료 규정)
	인체조직안전 및 관리 등에 관한 법률	– 관련 법조: 제22조 – 대상: 조직은행·조직이식의료기관 또는 관련 업무의 종사자 – 내용: 조직기증자·이식자 관련 정보 보호 – 처벌규정: 제34조, 제36조(양벌규정)
교육과학 기술부	**교육기본법**	– 관련 법조: 제23조의3 – 대상: 교육관련 기관 등 – 내용: 학생정보의 보호의무 – 처벌규정: 없음
	초중등교육법	– 관련 법조: 제30조의6 – 대상: 초중등 교육기관 – 내용: 학생관련 자료 제공의 제한 – 처벌규정: 제67조
법무부	**통신비밀보호법**	– 관련 법조: 제3조, 제11조 등 – 대상: 일반인, 전기통신사업자, 정부기관 등 – 내용: 통신 및 대화비밀의 보호 – 처벌규정: 제16조, 제17조, 제18조(미수범 규정)
	출입국관리법	– 관련 법조: 제73조의2 등 – 대상: 출입국관리공무원 – 내용: 예약정보시스템의 자료를 누설·권한없는 처리·타인에 제공 금지 – 처벌규정: 없음
공정거래 위원회	**소비자기본법**	– 관련 법조: 제15조 – 대상: 국가 및 지방자치단체 – 내용: 소비자의 개인정보 보호 시책 강구 – 처벌규정: 없음
	전자상거래등에서의 소비자 보호에 관한 법률	– 관련 법조: 제11조 – 대상: 사업자 – 내용: 소비자에 관한 정보 수집·이용·침해에 따른 대처 – 처벌규정: 제32조(시정조치)
	방문판매 등에 관한 법률	– 관련 법조: 제48조 – 대상: 특수판매업자 – 내용: 소비자에 관한 정보 수집·이용·침해에 따른 대처 – 처벌규정: 제42조(시정조치)

부처	법령	대상 및 내용
기획재정부	관세법	– 관련 법조: 제116조 – 대상: 세관공무원 – 내용: 비밀유지의무 – 처벌규정: 없음
	관세사법	– 관련 법조: 제14조 – 대상: 관세사 및 그 직무보조자 – 내용: 비밀엄수의무 – 처벌규정: 제29조, 제30조(양벌규정)
지식경제부	전자거래기본법	– 관련 법조: 제12조 – 대상: 정부 – 내용: 개인정보보호 시책 수립·시행 – 처벌규정: 없음
외교통상부	여권법	– 관련 법조: 제8조 – 대상: 외교통상부 – 내용: 여권업무 수행에 필요한 정보의 수집·보관·관리 의무 – 처벌규정: 없음
국토해양부	공인중개사의 업무 및 부동산 거래신고에 관한 법률	– 관련 법조: 제29조 – 대상: 중개업자등 – 내용: 비밀누설금지 – 처벌규정: 제49조(제2항에 의해서 반의사불벌죄임), 제50조(양벌규정)
	자동차관리법	– 관련 법조: 제7조, 제69조 – 대상: 국토해양부 – 내용: 자동차관리업무의 전산 처리 시 개인정보 보호의무 – 처벌규정: 없음
노동부	노동위원회법	– 관련 법조: 제28조 – 대상: 노동위원회의 위원 및 직원 – 내용: 비밀엄수의무 – 처벌규정: 제29조(공무원 의제 규정), 제30조, 제32조(양벌규정)
국세청	국세기본법	– 관련 법조: 제81조의13 – 대상: 세무공무원 – 내용: 비밀유지의무 – 처벌규정: 없음
통계청	통계법	– 관련 법조: 제31조, 제33조, 제34조 – 대상: 통계작성기관 및 통계종사자 – 내용: 비밀보호의무 – 처벌규정: 제39조, 제40조(양벌규정), 제41조(과태료 규정)

부처	법령	대상 및 내용
경찰청	경찰관직무집행법	– 관련 법조: 제2조 – 대상: 경찰관 – 내용: 치안정보의 수집작성배포 – 처벌규정: 제12조
병무청	병역법	– 관련 법조: 제11조의2, 제20조의3 – 대상: 병역담당기관 및 공무원 등 – 내용: 징병검사 대상자에 대한 정보자료 공개누설제공 금지 – 처벌규정: 없음
감사원	감사원법	– 관련 법조: 제27조 – 대상: 감사원 – 내용: 금융거래 내용의 제공누설다른 목적 이용 금지 – 처벌규정: 제51조
선거관리위원회	공직선거법	관련 법조: 제272조의3 대상: 정보통신서비스제공자 내용: 통신관련 선거범죄의 조사를 위한 개인자료 열람 및 제출 요구에 대한 불응 처벌규정: 제261조(과태료 규정)

앞서 언급한 바와 같이 개인정보보호법이 제정되면서 개인정보와 관련해서는 개인정보보호법이 일반법 또는 기본법적인 역할을 수행하게 되었다. 그러므로 다른 법령에 규정되어 있는 개인정보보호와 관련된 규정들은 개인정보보호법과 상충되지 않도록 개정될 필요성이 발생하게 된 것이다. 그러므로 개인정보 침해행위를 살펴보기 위해 우선 개인정보보호법에서 규정해 놓고 있는 개인정보침해행위를 살펴볼 필요가 있다.

4) 위치정보보호법

위치정보의 보호 및 이용 등에 관한 법률은 개인정보보호법의 특별 영역을 규정하는 법률이라고 할 수 있다. 이는 위치정보가 개인정보 가운데 최근 가장 민감하게 사용되는 정보이기 때문이다.[160] 물론 동 법률이 제정되기 이전에도 관련 규정은 전기통신사업법이나 정보통신망법에서 부분적으로 규정되어 있기는

160) 이에 대해 이원상, "형사사법에 있어 개인위치정보에 대한 고찰: 긴급구조 및 수사를 중심으로", 형사정책연구 제23권 제2호, 2012 여름호, 113면 이하 참조.

하였다. 그러나 위치정보의 보다 효율적인 활용 및 보호를 위해 체계적인 법률의 필요성이 제기되었으며, 그로 인해 위치정보보호법이 제정되기에 이르렀다.[161] 따라서 2005년 위치정보보호법은 "위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함"을 목적으로 제정되었다. 위치정보보호법은 제1장 총칙, 제2장 위치정보사업의 허가 등, 제3장 위치정보의 보호, 제4장 긴급구조를 위한 개인위치정보 이용, 제5장 위치정보의 이용기반 조성 등, 제6장 벌칙 등 총 43개 조문으로 구성되어 있다.

근래에 위치정보보호법과 관련해서 문제가 된 사안으로는 긴급구조를 위해 수사기관이 위치정보를 사용할 수 있는지에 대한 것과 애플이나 구글 등과 같은 기업이 개인의 동의 없이 위치정보를 수집한 것 등이 있다.[162] 전자의 경우에는 위치정보보호법을 통해 어느 정도 해결을 보았지만,[163] 후자의 경우는 방송통신위원회가 위치정보보호법 제15조 및 제16조의 규정에 위반을 이유로 애플에 대해 단지 300만원의 과태료와 위치정보의 암호화를 명령하는 선에서 마무리를 지었다.[164] 이에 대해 너무 솜방망이 처벌이라는 견해와[165] 옹호하는 견해가 대립하기도 하였으며,[166] 위치정보보호법이 현재의 트렌드를 제대로 반영하고 있지 못하다는 비판도 제기되었다.[167] 어쨌든 위치정보의 사용이 증대되고 있는 상황

161) 김도경, "위치정보보호법의 제정에 따른 LBS산업의 규제정책 방향", 정보통신정책 제15권 19호, 2003, 4면 이하.

162) 애플은 2010년 6월 22일부터 2011년 5월 4일까지 약 10개월에 걸쳐 이용자가 설정메뉴에서 위치서비스를 사용하지 않는 것으로 하였음에도 그와 상관없이 아이폰의 특정 영역에 암호화와 같은 기술적 조치 없이 저장될 수 있도록 프로그래밍 하였다. 따라서 이는 이용자의 동의 없이 개인정보인 개인의 위치정보를 수집한 것으로 많은 사회 문제가 되었다.

163) 이원상, 각주 112번 논문, 123면 이하.

164) "방통위, 애플·구글 위치정보보호법 위반 첫 결정", http://www.edaily.co.kr/news/NewsRead.edy?SCD=DC13&newsid=02433766596343712&DCD=A01404&OutLnkChk=Y.

165) "방통위, 애플·구글 위치정보보호법 '위반' 결론", http://www.asiae.co.kr/news/view.htm?idxno=2011080316485654797.

166) "위치정보보호법 애플적용, 문제 있다", http://biz.heraldm.com/common/Detail.jsp?newsMLId=20110823000137.

이기 때문에 앞으로도 위치정보와 관련된 다양한 유형의 문제들이 제기될 것으로 예상되어 위치정보보호법이 그에 어떻게 대응할 수 있을지에 대한 면밀한 검토가 있어야 할 것이다.

5) 전기통신기본법

전기통신기본법은 1982년에 한국전기통신공사가 발족되어 전기통신정책과 사업주체가 분리되면서 전기통신법령을 보다 체계화시키기 위해 1983년 12월 30일 제정되었다. 이에 따라 전기통신법으로만 존재하던 기존의 법률을 전기통신기본법과 공중전기통신사업법으로 분리하여 각각 제정하였다.[168] 그 이후 총 39차례의 개정을 거듭하며 현재에 이르고 있다.

최근 전기통신기본법이 문제가 된 것은 소위 '미네르바사건'과 관련해서 적용된 법률규정으로 인해서이다. 해당 사안에 대해 동 법률 제47조 제1항에 규정되어 있던 "공익을 해할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다"라는 그동안 적용되지 않던 규정을 수사기관이 적용하면서 문제가 불거지게 되었다. 결국 이에 대해 헌법재판소는 단순위헌 결정을 내리게 되어 현재 제47조 제1항은 적용되지 못하고 있다.[169]

전기통신기본법이 제정된 이후 전파법이나 전기통신사업법, 방송통신발전 기본법, 정보통신산업 진흥법 등이 뒤를 이어 제정되어 전기통신기본법에 존재하던 여러 관련 규정들이 해당 법률로 이관되거나 삭제되었다. 따라서 현재에는 제1장 총칙의 6개 조문과 제6장 보칙의 1개 조문, 제7장 벌칙의 1개 조문만이 남아있는 실정이다. 또한 제47조 제1항도 위헌결정이 내려진 상태이기 때문에 사실상 적용될 수 있는 처벌조항도 거의 남아있지 않다. 따라서 생각건대 실질적으로 거의 의미가 없는 동 법률은 폐지되고, 남아있는 규정들도 큰 의미가 없

167) "펄펄 뛰는 모바일 산업…설설 기는 IT 법령", http://www.hankyung.com/news/app/newsview.php?aid=2011101775201.

168) 김혜경, "전기통신기본법상 형사처벌규정의 검토", 연세대학교 법학연구, 2008, 228면.

169) 2008헌바157, 2010.12.28.

기 때문에 모두 삭제하거나 다른 법률로 이전하는 것이 적절할 것이다.

6) 통신비밀보호법

1993년 12월 27일 제정된 통신비밀보호법의 제정 동기는 "국민의 통신 및 대화의 비밀과 자유를 보장하기 위하여 전기통신의 감청과 우편물의 검열 등은 그 대상을 한정하고 엄격한 법적 절차를 거치게 함으로써 우리 사회를 사생활의 비밀과 통신의 자유가 구현되는 자유로운 민주사회로 진전시키려는 것"이라고 밝히고 있다. 특히 법률제정의 기폭제가 된 사건으로 1992년에 있었던 소위 '초원복국집 사건'이며, 해당 사건 이후 도청에 대한 내용을 보다 체계화할 필요성이 적극적으로 제기되었다.[170] 제정 이후 총 19차례에 걸쳐 개정작업이 이루어졌으며, 현재 동 법률은 벌칙을 비롯해서 총 18개 조문으로 구성되어 있다.

최근 들어 국가기관의 감청에 대한 문제가 사회문제시 되는 경우가 많아지면서 통신비밀보호법에 대한 관심도 높아지고 있다. 이에 통신비밀보호법의 문제점에 대한 지적도 많아지고 있는 추세이다. 그 가운데 하나로 통신제한조치에 대한 법원의 통제가 매우 느슨하다는 점이 지적되고 있다. 법률을 보면 긴급통신제한조치의 경우 조치 후 "지체 없이" 법원에 허가청구를 하도록 규정되어 있는데, 이는 36시간 이내에 승인을 받아야 한다는 규정과 결합하게 될 경우 36시간까지는 무방비로 긴급통신제한조치가 가능하게 된다고 지적되고 있다.[171] 이와 함께 통신제한조치기간의 연장이 2월 범위내에서 가능하다고 되어 있어 결과적으로 통신제한조치는 횟수에 제한을 받지 않는다는 문제점도 제기되었다. 이에 대해서는 헌법재판소의 헌법불합치 결정이 있었기 때문에 2011년 12월 31일을 시한으로 입법자가 개정할 때까지 적용하도록 하였지만, 여전히 법률이 개정되지 않고 있는 상황이다. 다만 현법재판소 결정의 취지와 통신비밀보호법의 실효성을 고려해 보면 단순한 총연장 제한보다는 동 법률 제5조 제1항을 고려하여 중대범죄의 경우 연장의 상한을 두지 않는 방안도 모색할 필요가 있다.[172]

170) 조국, "개정 통신비밀보호법의 의의, 한계 및 쟁점", 형사정책연구 제15권 제4호, 2004 겨울호, 103면 이하.

171) 오길영, "통신비밀보호법, 통신국가보안법?", 진보평론 제33호, 2007년 가을호, 176면 이하.

다. 침해 행위의 중복규정

사이버범죄와 관련해서 주로 개별법 위주로 법령이 만들어지기 때문에 앞에서 본 바와 같이 개인정보와 관련된 법률 규정은 여러 법률들에 산재되어 있다. 비단 개인정보 뿐 아니라 다른 행위들의 경우에도 여러 법률들에서 중복적으로 규정되고 있는 것을 보게 된다. 따라서 아래에서는 가장 대표적인 예로 개인정보 침해 행위와 허위정보 유포행위를 살펴보고자 한다.

1) 개인정보 침해행위

가) 개인정보보호법상 개인정보 침해행위

개인정보보호법에서 개인정보침해를 통해 형사처벌 될 수 있는 경우는 크게 세 부분으로 나누어 볼 수 있다. 다만, 침해주체는 개인정보처리자로 한정된다. 그러나 개인정보보호법상에서 개인정보처리자의 범위를 개인에까지 확대하고 있기 때문에 개인정보의 범위에 따라 개인정보처리자의 범위는 매우 광범위하게 확대될 수 있다.[173] 개인정보처리자가 처벌될 수 있는 사유 가운데 하나는 개인정보를 무단으로 제공하고, 제공받고, 처리하는 행위이다. 이는 개인정보가 개인의 동의 없이 유통됨으로 인해서 개인의 정보자결권을 침해하는 행위라고 할 수 있다. 이런 행위에는 첫째로 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 등에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공

172) 형사입법연구회, 2011년도 형법·형사소송법 및 형사특별법 제·개정안 분석과 입법정책 개선방안, 한국형사정책연구원, 2011, 381면.

173) 개인정보보호법에서는 개인정보처리자를 "업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등"이라고 정의하고 있다.

할 수 없음에도 정보주체의 동의를 받지 않은 채 개인정보를 제3자에게 제공하거나 그 사실을 알고도 개인정보를 제공받는 행위가 있다. 둘째로, 개인정보처리자가 동 법률 제18조 제2항에 정하고 있는 특별한 규정에 의하지 않고 개인정보를 그 취득 목적범위를 초과하거나 목적이외의 용도로 이용하는 행위를 하거나 제3자에게 제공한 때, 업무위탁에 따른 수탁자가 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공한 때, 영업양도 등에 따른 영업양수자 등이 이전 받은 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 행위이다. 그리고 셋째로 개인정보처리자가 특별한 경우[174]에 해당하지 않음에도 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보인 소위 "민감정보"를 처리하여서는 안됨에도 이를 처리한 경우이다. 넷째로, 개인정보처리자가 특별한 경우를 제외하고 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보인 소위 "고유식별정보"를 처리한 경우이다. 다섯째로, 개인정보를 처리하거나 처리하였던 자가 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위와 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위가 있다. 그리고 여섯째로, 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위가 있다. 이런 행위를 한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해진다(제71조).

다음으로는 개인정보침해의 유형이 앞선 유형들보다는 다소 완화된 형태로 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 행위는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해진다(제72조). 그런데 여기에서 말하고 있는 행위 유형이 과연 앞선 행위들보다 완화해서 처벌할 필요가 있는지는 의문이다. 개인정보를 부정한 방법

174) 여기서 특별한 경우란 정보주체에게 제15조 제2항 각 호 또는 제17조 제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우, 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 등을 말한다(동법 제23조 1호, 2호).

으로 취득하거나 동의를 받고, 이를 제공하거나 제공받는 행위의 불법 정도도 앞선 행위들보다 결코 작다고 할 수 없기 때문이다.

그리고 마지막으로 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 경우, 정보주체의 개인정보 정정·삭제 요구에도 불구하고 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 경우, 정보주체의 요구에도 불구하고 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 경우에는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처해진다(제73조).

그런데 개인정보보호법상의 처벌규정을 보면 일관된 원칙이 발견되지 않는다. 예를 들어 정보주체의 요구에도 불구하고 계속해서 개인정보처리자가 개인정보를 이용하거나 제3자에게 제공하는 것은 정당한 권한 없이 다른 사람의 개인정보를 유출하는 행위라고도 할 수 있다. 따라서 그런 경우 제71조 제6호가 적용될 수 있을지, 아니면 그보다 완화된 제73조 제2호나 제3호가 적용될지 불분명하게 된다. 그러므로 개인정보보호법상의 처벌 규정에 관해서는 반드시 다시금 재고할 필요가 있다고 사료된다.

나) 정보통신망법상 개인정보 침해행위

정보통신망법에는 제71조 내지 제74조에서 개인정보 침해와 관련된 행위를 처벌하고 있다. 다만, 이에 대해 새로 제정된 개인정보보호법과 혼란을 초래할 수 있을 여지가 있기 때문에 해당 침해내용을 정보통신망보다는 개인정보보호법에서 다룰 필요가 있다고 주장되기도 한다.[175] 그러나 아직까지 정보통신망법에 해당 처벌규정이 있는 이상 개인정보보호법과 중복으로 적용될 여지가 남아있다. 다만 정보통신망법에서 개인정보를 침해하는 주체는 주로 정보통신서비스 제공가가 된다.

제71조에서는 정보통신서비스 제공자가 이용자의 동의를 받지 않고 개인정보를 수집하거나(제1호) 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가

175) 심우민, "개인정보 보호법 시행과 당면과제", 이슈와 논점 제308호, 국회입법조사처, 2011 참조

있는 개인정보를 수집하는 경우(제2호), 개인정보의 이용제한 등을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 경우(제3호), 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 경우(제4호), 오류정정에 대한 요청에도 불구하고 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 경우(제7호), 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우(제8호)에는 5년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌된다. 또한 이용자의 개인정보를 취급하고 있거나 취급하였던 자가 직무상 알게 된 개인정보를 훼손·침해 또는 누설하는 경우(제5호), 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 경우(제6호)에도 동일하게 처벌된다.

제72조에서는 속이는 행위에 의해 다른 사람의 개인정보를 수집하는 경우(제2호) 3년 이하의 징역이나 3천만원 이하의 벌금에 처해진다. 또한 제73조에서는 정보통신서비스 제공자 등이 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우(제1호)와 속이는 행위로 개인정보 제공을 유인한 경우(제7호)에 2년 이하의 징역 또는 1천만원 이하의 벌금형에 처해진다.

다) 위치정보보호법상 개인정보 침해행위

위치정보보호법에서는 주로 개인위치정보를 침해한 행위를 처벌하고 있다. 여기에서는 주로 위치정보사업자 등이 그 침해의 주체로 나타나고 있다. 제39조를 보면 위치정보사업자 등이 개인위치정보를 누설·변조·훼손 또는 공개한 경우(제2호), 개인위치정보주체의 동의를 얻지 아니하거나 동의의 범위를 넘어 개인위치정보를 수집·이용 또는 제공한 자 및 그 정을 알고 영리 또는 부정한 목적으로 개인위치정보를 제공받은 경우(제3호), 이용약관에 명시하거나 고지한 범위를 넘어 개인위치정보를 이용하거나 제3자에게 제공한 경우(제4호)에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해진다. 긴급구조기관 및 경찰관서와 긴급구조업무에 종사하거나 종사하였던 사람이 긴급구조 목적으로 제공받은

개인위치정보를 긴급구조 외의 목적에 사용한 경우에도 동일하게 처벌된다(제5호).

제40조에서는 누구든지 개인의 동의를 얻지 아니하고 당해 개인의 위치정보를 수집·이용 또는 제공한 경우(제4호)와 타인의 정보통신기기를 복제하거나 정보를 도용하는 등의 방법으로 위치정보 사업자 등을 속여 타인의 개인위치정보를 제공받은 경우(제5호) 3년 이하의 징역 또는 3천만원 이하의 벌금에 처해진다. 그리고 제41조에서는 위치정보사업자가 개인정보를 파기해야 함에도 개인위치정보를 파기하지 아니한 경우(제1호)에는 1년 이하의 징역 또는 2천만원 이하의 벌금에 처해진다.

라) 소결

이 외에도 개인정보와 관련된 규정들은 여러 개별 법률에 존재하고 있다. 예를 들어 개인신용과 관련된 정보의 경우에는 신용정보의 이용 및 보호에 관한 법률에 관련 처벌내용이 규정되어 있으며(제50조), 전자서명과 관련된 개인정보는 전자서명법(제31조)에 존재하고 있다. 그런데 이처럼 여러 개별조문에 규정되어 있는 처벌 내용들이 서로 동기화 될 필요가 있다. 즉 개인정보보호법을 기반으로 유사한 침해행위는 그 형량 등을 서로 동일하게 할 필요가 있다.[176] 특히 동 보고서에는 자세히 언급해 놓고 있지 않지만, 과태료에 대한 규정과 형벌규정을 비교해 볼 때에도 어떤 행위는 왜 과태료 규정에 있고, 어떤 행위는 왜 형벌 규정에 있는지 이해되지 않는 경우도 있다. 따라서 어떤 행위는 형사처벌 하고, 어떤 행위는 행정처벌을 해야 할 지에 대해 보다 면밀한 검토가 요구된다.[177]

176) 이런 문제점에 대해서는 이원상/안정민, 방송통신융합에 따른 처벌법규 정비방안 연구, 한국형사정책연구원, 2011, 196면 이하 참조.

177) 이에 대해서는 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 108면 이하 참조.

2) 사이버공간에서의 진실·허위 사실의 유포행위

가) 형법상 진실·허위 사실의 유포행위

개별법에서 진실·허위 사실을 유포하는 경우 해당 구성요건을 충족시키지 못하는 경우에는 형법상 명예훼손죄 또는 모욕죄로 처벌될 수 있다. 예를 들어 정보통신망법상 사이버 명예훼손죄에 속하지 않는 경우에는 형법 제307조 규정에 의해 처벌될 수 있는 것이다. 따라서 진실·허위 사실유포에 대한 처벌은 형법상 제307조가 가장 일반적으로 적용될 수 있으며, 허위사실일 경우에는 제307조 제2항이 적용되어 가중처벌되고, 그 매체가 출판물 등일 경우에는 형법 제309조가 적용되며(이 경우에도 허위는 가중처벌 됨), 사이버공간일 경우에는 정보통신망법 제70조가 적용되는 것이다.[178] 그리고 적시한 사실이 모욕적인 행위일 경우에는 형법 제310조가 적용된다.

이뿐 아니라 적시한 사실이 선거와 관련될 경우에는 공직선거법 제250조(허위사실공표죄)와 제251조(후보자비방) 등으로 처벌될 수 있으며, 지금은 위헌이 되었지만, 공익을 해하는 것을 목적으로 허위통신을 하는 경우에는 전기통신기본법 제48조 제1항에 의해 처벌될 수 있었다.

나) 정보통신망법상 진실·허위 사실의 유포행위

정보통신망법 제70조 제1항에서는 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처하도록 규정하고 있으며, 제2항에서는 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처하도록 하고 있다. 형법 제307조는 형법의 출판물 등에 의한 명예훼손에서처럼 '비방의 목적'과 '정보통신망을 통하여'라는 추가 구성요건 표지를 요구하고 있으며, 단지 형법 제309조와 차이점은 벌금에

178) 이에 대해 이원상, "허위사실에 의한 명예훼손죄의 딜레마", 2013년 형사판례연구 발제문 12면 이하 참조.

있다.[179] 따라서 출판물 등에 의한 명예훼손죄와 징역형은 같지만 벌금형은 월등히 높게 규정되어 있다. 동법 동조 제3항에서는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없도록 하여 반의사불벌죄로 규정하고 있다.

다) 전기통신기본법상 진실·허위 사실의 유포행위

전기통신기본법 제47조 제1항에는 공익을 해할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정해 놓고 있다. 동 규정은 단순위헌 결정으로 인해 더 이상 적용되지는 않지만,[180] 개정이 되지 않아 여전히 존재하고 있는 실정이다. 아직까지 존치하고 있는 동조 제2항, 제3항, 제4항도 허위통신을 처벌하고 있다. 따라서 제47조는 허위통신과 관련된 범죄를 처벌하는 규정이며, 제1항은 사회적 법익에 속하는 공공의 이익을 그 법익으로 삼고 있으며, 제2항과 제3항은 개인적 법익을 보호하고 있다.[181]

동법 제48조 제1항은 '공익을 해할 목적'을 구성요건으로 하고 있기 때문에 목적범을 염두에 두고 있으며, 그 수단은 '전기통신설비'이고, 그 내용은 '허위의 통신'이다. 동 법률에 따르면 전기통신설비란 "전기통신을 하기 위한 기계·기구·선로 기타 전기통신에 필요한 설비(제2조 제2호)"이고, 전기통신은 "유선·무선·광선 및 기타의 전자적 방식에 의하여 부호·문언·음향 또는 영상을 송신하거나 수신하는 것(제2조 제1호)"이다. 특히 '공연히'라는 의미의 모호성이 지적되고 있는데, 사실 공연성 요건이 여기에서만 규정되어 있는 것은 아

179) 이원상, "'사이버'개념을 통한 사이버 모욕죄의 고찰과 대안", 형사정책 20권 2호, 2008, 261면.

180) 2010. 12. 28. 2008헌바157, 2009헌바88(병합); 헌재의 주요결정요지를 살펴보면 헌재는 "....나아가 현재의 다원적이고 가치상대적인 사회구조 하에서 구체적으로 어떤 행위상황이 문제되었을 때에 문제되는 공익은 하나로 수렴되지 않는 경우가 대부분인바, 공익을 해할 목적이 있는지 여부를 판단하기 위한 공익간 형량의 결과가 언제나 객관적으로 명백한 것도 아니다. 결국, 이 사건 법률조항은 수범자인 국민에 대하여 일반적으로 허용되는 '허위의 통신' 가운데 어떤 목적의 통신이 금지되는 것인지 고지하여 주지 못하고 있으므로 표현의 자유에서 요구하는 명확성의 요청 및 죄형법정주의의 명확성원칙에 위배하여 헌법에 위반된다."라고하여 본 규정이 특히 명확성원칙에 위배된다고 밝히고 있다.

181) 김혜경, 앞의 논문, 232면.

니다. 형법을 보면 명예훼손죄나 공연음란죄 등에서도 동일한 개념을 사용하고 있으며, 따라서 형법상 공연성이란 "불특정 또는 다수인이 인식할 수 있는 상태"를 의미하고 있다.[182] 이 때 불특정인에는 가족 및 애인관계처럼 특수한 관계에 속하지 않되,[183] 상대방이 한정되어 있지는 않는 것이며, 다수인이란 상당한 다수의 사람을 의미한다.[184] 물론 이는 이론적인 개념이며, 판례는 한 사람에게 유포하더라도 이를 통해서 불특정 다수에게 전파될 가능성이 있으면 공연성이 있고,[185] 특정한 한 사람에게 유포하더라도 비밀이 보장되거나 전파될 가능성이 없는 경우에는 공연성이 없다고 하는[186] '전파성이론'을 펴고 있다.

헌법재판소의 다수 견해를 보면 해당 규정에서 '공익을 해할 목적'과 '허위의 통신'이 명확성 원칙에 위반된다고 한다. 따라서 전자의 경우 법률뿐 아니라 헌법재판소, 대법원 등도 명확한 개념 정의를 내리지 못한다는 주장이 있다.[187] 헌법재판소의 다수견해는 "…여기서의 '공익'은 형벌조항의 구성요건으로서 구체적인 표지를 정하고 있는 것이 아니라, 헌법상 기본권 제한에 필요한 최소한의 요건 또는 헌법상 언론·출판의 자유의 한계를 그대로 법률에 옮겨 놓은 것에 불과할 정도로 그 의미가 불명확하고 추상적이다. 따라서 어떠한 표현행위가 '공익'을 해하는 것인지, 아닌지에 관한 판단은 사람마다의 가치관, 윤리관에 따라 크게 달라질 수밖에 없으며, 이는 판단주체가 법전문가라 하여도 마찬가지이고, 법집행자의 통상적 해석을 통하여 그 의미내용이 객관적으로 확정될 수 있다고 보기 어렵다. 나아가 현재의 다원적이고 가치상대적인 사회구조 하에서 구체적으로 어떤 행위상황이 문제되었을 때에 문제되는 공익은 하나로 수렴되지 않는 경우가 대부분인바, 공익을 해할 목적이 있는지 여부를 판단하기 위한 공익간 형량의 결과가 언제나 객관적으로 명백한 것도 아니다."라고 밝히며 이는 명확성원칙에 위배된다고 하였다.[188]

182) 김일수/서보학, 형법각론, 새로쓴 7판, 2007, 190면; 배종대, 형법각론, 제7전정판, 2011, 51/3; 이재상, 형법각론, 제9판, 2012, 12/13; 박상기, 형법각론, 제7판, 2008, 180면.

183) 김일수/서보학, 앞의 책, 190면.

184) 배종대, 앞의 책, 51/3; 이재상, 앞의 책, 12/13.

185) 대법원 1968.12.24. 선고 68도1569 판결; 대법원 1996.7.12. 선고 96도1007 등.

186) 대법원 1984.4.10. 선고 83도49 판결; 대법원 1989.7.11. 선고 89도886 판결 등.

187) 김혜경, 앞의 논문, 231면 이하.

이와 함께 헌법재판소의 다수견해는 '허위의 통신'도 명확성 원칙에 어긋나는 것으로 본다. 이 때 형법상 일반적으로 사용되는 허위의 개념은 "내용이 진실(또는 사실)에 합치되지 않는 것"을 말한다.[189] 다시 말해 형법상 허위라는 개념은 '진실'에 대응되는 개념이고, "진술내용이 객관적 진실에 반하거나 불합치하게 되는 객관적 허위와 진술자의 기억이나 확신에 반하는 주관적 허위"로 나누어지게 된다.[190] 다만 장래의 사실에 대한 적시는 단지 의견진술일 뿐이므로 현재의 사실에 대한 주장을 포함할 경우에만 사실여부가 문제시 된다.[191] 그리고 가치판단도 그 정당성 여부가 주관적 확신에 근거하므로 사실여부와는 구별되는 개념이라고 할 수 있다.[192] 이에 대해 다수견해는 "…'허위'란 일반적으로 '바르지 못한 것', 또는 '참이 아닌 것'을 말하고, 그 안에는 내용의 거짓이나 형식의 오류가 모두 포함될 수 있기 때문에, 법률 용어, 특히 형벌조항의 구성요건으로 사용하기 위하여는 보다 구체적인 부연 내지 체계적 배치가 필요한 개념이라고 할 수 있다. 예컨대 명예훼손죄의 행위태양으로 '허위로' 명예를 훼손하는 행위를 규정하지 않고 '허위사실을 적시'하여 명예를 훼손하는 행위로 규정한 것, 문서에 관한 죄에서 형식, 명의의 거짓을 말하는 '위조'나 '모용'과 대비하여 내용상의 거짓을 의미하는 '허위' 개념을 사용하는 것은 그와 같은 명확성의 요청에 따른 것이다. 그런데 이 사건 법률조항은 법조문 자체의 문언이나 관련조항의 체계상 그와 같은 구체화의 취지를 명백하게 드러내지 아니한 결과, 앞서 살핀 당초 입법취지와는 달리, 확대된 법률의 해석, 적용이 가능하게 된 것이다…"라며 명확성 원칙에 반한다고 판단한 반면, 소수견해는 "… "허위의 통신" 부분에

188) 이에 반해 소수견해는 "이 사건 법률조항은 "공익을 해할 목적"이라는 초과주관적 구성요건을 추가하여 '허위의 통신' 가운데 구성요건해당성이 인정되는 행위의 범위를 대폭 축소시키고 있는바, 초과주관적 구성요건 부분에 대하여 객관적 구성요건 행위와 같은 정도의 명확성을 요구할 것은 아니다. 한편 법률상 '공익' 개념은 '대한민국에서 공동으로 사회생활을 영위하는 국민 전체 내지 대다수 국민과 그들의 구성체인 국가사회의 이익'을 의미하고, 공익을 '해할 목적'은 행위의 주요 목적이 공익을 해하는 것인 때를 의미하는바, 그 의미가 불명확하다고 보기 어렵다."라고 하며 다수의 견해에 반대하고 있다.

189) 배종대, 앞의 책, 117/15.

190) 김일수/서보학, 앞의 책, 930면.

191) 이재상, 앞의 책, 12/16.

192) 위와 동일.

관하여 살펴보면, 일반적인 '허위'의 관념은 내용의 거짓과 명의의 거짓을 모두 포괄하는 점 및 다른 형사처벌 규정에서의 '허위' 개념의 용례에 비추어 볼 때, 이 사건 법률조항의 "허위의 통신"에서 '내용이 거짓인 통신'이 배제된다는 해석은 불가능하다. 한편 '내용의 허위'란 내용이 진실에 부합하지 않는 것으로서, 전체적으로 보아 '의견 표명'이나 '제안'이라고 볼 수 있는 경우는 이에 해당하지 아니한다. 결국 이 사건 법률조항의 "허위의 통신"은 그 의미가 명확하고, 죄형법정주의의 명확성원칙에 위배되지 않는다..."라고 판단하였다.

라) 소결

사이버공간에서 진실·허위 사실의 유포와 관련해서 동 보고서에서 예를 든 까닭은 이와 같은 행위는 일반적인 행위이기 때문에 여러 개별 법률에 규정하기보다는 하나의 법률에 통합적으로 규정할 필요가 있기 때문에다. 따라서 정보통신망법에 있는 사이버 명예훼손규정은 형법으로 옮겨갈 필요성이 있으며, 전기통신기본법의 제48조 제1항 규정은 서둘러 삭제될 필요가 있다. 예와 같이 사이버범죄와 관련해서 개별법에 산재하여 규정되어 있는 유사규정들은 하나의 규정에 통합하여 규정함으로써 일반예방기능을 높일 수 있으며, 법률의 적용에 있어서 발생할 수 있는 충돌 등의 문제점도 해결할 수 있을 것으로 사료된다.

제4장

사이버범죄 법령정비 요청

이원상

04

사이버범죄 법령정비 요청

제1절 사이버범죄 관련 유관 조직의 변화

1. 새로운 정부의 조직변화

이번 정부는 기존의 정부와 다른 조직체계를 가지고 있다. 그러므로 이번 정부 들어 개편된 조직에 대해서 살펴볼 필요가 있다. 중앙행정기관은 미래창조과학부·해양수산부 등이 신설되었다. 따라서 중앙행정기관은 종전 47개에서 50개로 3개 늘어나 지난 정부가 15부2처18청 2원3실7위원회 구조로 꾸려진 것보다 다소 늘어난 17부3처17청 2원5실6위원회로 구성되어 있다. 식품의약품안전청은 식품의약품안전처로 격상됐고, 국가안보실, 대통령경호실, 국무총리비서실 등이 새로 생긴 반면, 특임장관실과 국가과학기술위원회도 폐지됐다.

특히 사이버범죄와 관련된 부서로 신설되는 미래창조과학부는 4실 21국(관) 64과로 구성되며 과학기술과 ICT 융합 촉진 및 창조경제 선도를 위해 장관 직속 '창조경제기획관'을 신설하였다. 그리고 안전행정부는 재난안전 기능 보강을 위해 '재난안전실'을 '안전관리본부'로 개편하고 교육부는 교육분야 핵심 대선 공약사항인 공교육 정상화를 위해 '공교육진흥과'를 신설하였다.[193]

193) http://www.korea.kr/policy/societyView.do?newsId=148757690.

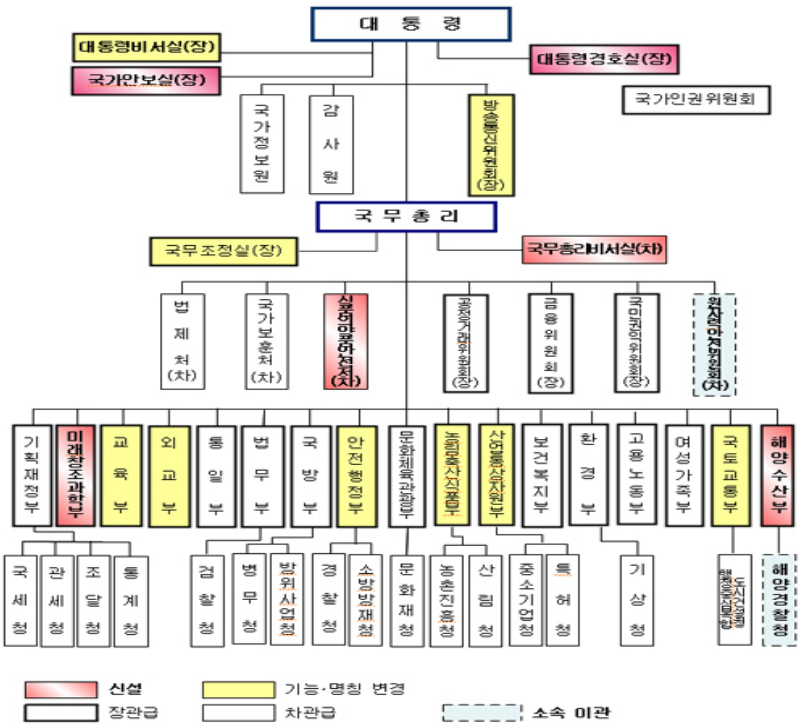


그림 5 개편된 정부조직체계

특히 새 정부의 4대 국정기조 가운데 "II. 국민행복", 14대 추진전략 가운데 "6. 국민안전", 140개 국정과제 가운데 9개 과제가 범죄로부터 안전을 주요 테마로 삼고 있다. 이것은 새 정부의 안전에 대한 강력한 의지를 표명하는 것이라고 할 수 있다. 다만 다소 우려스러운 것은 사이버범죄(사이버공격 등도 포함)에 대한 대응과제가 국민안전과 관련된 국정과제에서 고려되고 있는 것이 아니라 경제부흥과 관련된 국정과제 가운데 창조경제(19. 세계 최고의 인터넷 생태계 조성)에서 부수적으로 등장하고 있는 것이다. 새 정권에서도 사이버공간에서의 안전이 여전히 주요 국정과제에는 포함되지 않는 것을 보면 정치권에서는 여전히 사이버공간이나 사이버안보, 사이버범죄 등에 대한 이해가 부족한 것으로 여겨진다. 따라서 사이버범죄, 사이버안보와 관련된 문제는 미래창조과학부의 업무로 다소 축소되는 모양새를 가지게 되었다.

2. 사이버범죄 관련 조직의 변화

가. 미래창조과학부의 관련 업무

새 정부 들어 사이버범죄와 관련해서 생긴 조직적 변화 가운데 가장 큰 것으로 매머드급 조직인 미래창조과학부가 창설되면서 기존에 분산되어 있던 ICT와 관련된 부분들을 대부분 흡수한 것이다. 이에 따라 방송통신위원회의 소관으로 있었던 사이버범죄와 관련된 상당수의 업무들이 미래창조과학부로 이관되었다.

사실 그동안 관련 학계나 기업 등에서는 과거 정보통신부와 같이 ICT를 전담으로 담당해 줄 부처가 만들어지기를 바라왔었다. 이는 지난 정부가 정보통신부를 해체하면서 ICT산업 육성 진흥 정책을 지식경제부로 통합하고, 그와 함께 새롭게 설립된 방송통신위원회와 문화관광체육부, 행정안전부 등으로 정보통신부가 가지고 있던 기능들을 이관하였기 때문이다.[194] 하지만 이관 되는 업무들이 확실하게 구분되는 것이 아니었기 때문에 ICT 컨트롤타워가 필요하다는 지적이 나오면서 관련 부처들 사이에 주도권을 놓고 다툼이 일어나기도 하였다.[195] 그런데 이처럼 지난 정부에서 ICT관련 업무를 분할함으로 인해 우리나라의 ICT관련 경쟁력이 많이 떨어지게 되었다는 주장이 꾸준하게 제기되었고, 그런 현상들은 각종 국제적인 지표에서도 나타나게 되었다. 그러므로 이번 정권에서는 ICT에 관련된 업무들을 다시금 한 곳으로 집중하였으며, 그 업무를 미래창조과학부가 담당하게 된 것이다. 이는 단순히 ICT에만 국한되는 것이 아니다. 그동안 사이버안보를 위한 구조에도 변화가 생기게 되어 방송통신위원회와 구 행정안전부에 속해 있던 부분들이 다수 이관되어 미래창조과학부의 역할이 보다 증대되는 결과를 가져왔다.

미래창조과학부의 업무보고를 보면 제2차관실이 방송통신 융합・진흥 및 전파관리(과거 방통위 소관), ICT 연구개발 및 산업진흥(과거 지경부 소관), SW 산업・융합(과거 지경부 소관), 국가정보화기획・정보보안・정보문화(과거 행안부 소관), 디지털 콘텐츠(과거 문체부 소관) 등을 담당하도록 하고 있다.[196]

194) 차성민, "ICT정부조직 비교연구", 한국비교정부학보 제16권 제3호, 2012. 12, 189면 이하.
195) 차성민, 앞의 글, 192면.

미래창조과학부는 비전을 “과학기술과 ICT를 통한 창조경제와 국민행복 실현”으로 삼고 있으며, 그를 위한 전략으로는 창조경제 생태계 조성,[197] 국가 연구개발 및 혁신역량 강화,[198] SW와 콘텐츠를 핵심 산업화,[199] 국제협력과 글로벌화,[200] 국민을 위한 과학기술과 ICT 구현[201] 등이 있다. 이 가운데 사이버범죄와 관련해서 주목할 만한 중점과제로는 ‘국민을 위한 과학기술과 ICT 구현’의 전략에 대한 중점 과제로 ‘3. 사이버 보안 강화’가 있다.[202]

미래창조과학부는 사이버 보안 강화로 사이버테러와 해킹으로부터 안전한 사이버 환경조성을 구상하고 있다. 이를 위해 기업 정보보호 안전망 구축과 국가 사이버 예방·대응체계 구축을 계획하고 있다. 전자를 위해서는 방송, 금융, 정수, 교통, 의료 등 기반시설 보안 강화와 기업 정보보호 투자 촉진을 모색하고 있으며, 후자를 위해서는 해킹의 조기 탐지 및 신속 대응, 첨단 방어기술 확보,

196) 제2차관실이 관할하는 법률들로는 소프트웨어산업진흥법, 전기통신기본법, 전기통신사업법, 정보통신공사업법, 정보통신산업진흥법, 전파법, 통신비밀보호법, 국가정보화 기본법, 인터넷 주소자원에 관한 법률, 전자문서 및 전자거래 기본법, 전자서명법, 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 방송법, 방송통신발전 기본법, 인터넷멀티미디어 방송사업법, 지상파 텔레비전방송의 디지털 전환과 디지털방송의 활성화에 관한 특별법 등이다.

197) 이를 위한 중점과제로는 ① 창의적 아이디어와 인재가 넘치는 대한민국 실현, ② 창의적 아이디어의 기술사업화 및 창업 활성화, ③ 과학기술과 ICT 기반 신산업·신수요 창출 및 기존산업 강화, ④ 인터넷 신한업 육성, ⑤ 국가 정보화를 통한 ICT 신수요 창출, ⑥ 산학연 연구공동체 활성화로 지역산업 육성, ⑦ 지식재산의 창출-보호-활용체계 선진화 등이 있다.

198) 이를 위한 중점과제로는 ① 창조경제 실현을 위한 과학기술정책 패러다임 전환, ② 현장 친화형 R&D 기획·관리·평가시스템 구축, ③ 미래 성장기반 확충을 위한 R&D 투자전략 고도화, ④ 우주기술 자립으로 우주강국 실현, ⑤ 세계 선도형 원자력 기술개발을 통한 신산업 창출, ⑥ 출연연을 세계 일류 연구기관으로 육성, ⑦ 과학기술인이 마음껏 연구하는 사회 실현 등이 있다.

199) 이를 위한 중점과제로는 ① 21세기 언어인 SW를 핵심산업으로 육성, ② 누구나 SW를 개발·활용할 수 있는 교육기반 조성, ③ ‘한국스타일’콘텐츠로 세계 진출, ④ 방송산업 및 스마트미디어산업 육성, ⑤ 세계 최고의 네트워크 인프라 구축 등이 있다.

200) 이를 위한 중점과제로는 ① 범부처 합동 전략적 과학기술·ICT 국제협력 추진, ② 국제과학비즈니스벨트를 글로벌 기초과학 연구거점으로 조성, ③ 중소벤처기업의 해외진출 지원 강화, ④ 국내 ICT 인재의 해외진출 지원 등이 있다.

201) 이를 위한 중점과제로는 ① 사회이슈 해결형 기술 개발, ② 가계 통신비 부담 낮추기, ③ 사이버 보안 강화, ④ 글로벌 웹 표준 이용환경 조성, ⑤ 건전한 사이버문화 정착 및 정보격차 해소, ⑥ 창조경제·국민행복을 위한 우체국 네트워크 활용 등이 있다.

202) http://www.msip.go.kr/upload/work/msip_report.pdf.

사이버 예비군 육성을 모색하고 있다.

나. 안전행정부의 관련 업무

새 정부 들어 과거 행정안전부에서 안전행정부로 변경한 것은 단순한 명칭변경에 그치는 것이 아니라 행정보다는 국민의 안전을 우선적으로 생각하겠다는 새 정부의 의지가 표명된 것이라고 할 수 있다. 안전행정부는 "국민 모두가 안전하고 행복한 대한민국"을 비전으로 삼고, 이를 위한 정책목표를 "안전한 사회, 유능한 정부, 성숙한 자치"로 정하였고, 국정과제를 국민안전분야, 정부운영분야, 지방자치 분야로 구분하였다. 이 가운데 사회안전과 관련된 분야인 국민안전분야의 국정과제는 ① 안전관리 패러다임 근본적 전환, ② 국가 안전관리체계 획기적 개혁, ③ 4대악 근원적 척결, ④ 위기상황으로부터 국민보호 등이다.[203]

이 가운데 사이버범죄와 관련해서는 '④ 위기상황으로부터 국민보호'에 마련되어 있다. '④-② 사이버 공격 대응·개인정보보호를 통한 안심사회 구현'을 보면 사이버 공격에 대한 선제적 대응체계를 구축하여 중단 없는 대국민 서비스를 제공하고, 개인정보 침해사고 사전 예방 및 개인정보보호에 대한 사회 전반의 실태를 개선하는 것을 주요 목적으로 삼고 있다. 사이버 공격 대응을 통한 안정적 행정 서비스 제공을 위해서는 행정기관 정보시스템에 대한 사이버공격 방어체계 강화, 주요정보통신기반시설 정보보호 강화(지하철 등 소관 기반시설(63개) 취약점 점검, 백신설치 등 보안조치), 사이버테러에 대응하기 위해 '국가통합 콘트롤타워' 구축 지원을 모색하고 있다. 또한 개인정보 침해·유출 사고에 대한 선제적 대응 및 제도 개선을 위해서는 「범정부 합동점검단」을 통한 개인정보 불법매매·유출행위 조사·단속(주민번호 유·노출 모니터링 및 삭제조치 등 사전 예방활동 강화), 주민번호 무단 수집·오남용 금지 및 유출기업의 책임성 강화(주민번호 수집 법정주의, 주민번호 유출시 과징금 및 CEO 징계권고제 도입) 등을 모색하고 있다. 이와 함께 민·관 협업으로 개인정보보호 수준 향상을 도모하고 있는데, 이를 위해서는 행정·민원서식, 통신·금융·쇼핑 등 주요 업종의 계약

203) http://www.mospa.go.kr/gpms/resource/popup/new2013/mospa2013_sub3_03.html.

서·서식 일괄 정비, 지역 소상공인, 영세사업자 대상 컨설팅·기술지원 및 교육 실시(「지역 거점지원센터(대학, 주민자치센터)」 운영 및 현장 방문 지원), 전국 순회교육 및 생활밀착형 업종(주택관리, 위생) 의무교육 실시 등이 모색되고 있다.

3. 사이버공격 대응 컨트롤 타워 필요성

최근 몇 년 동안 한국은 사이버공격으로 인해 많은 피해를 입었다. 가장 대표적인 사건으로는 2009년 7월 7일에 발생하였던 '7.7 디도스 공격'이 있다. 악성코드에 감염된 5만 여대의 개인PC가 국가기관 및 금융권 웹사이트를 공격하여 서비스 이용을 중단시킨 사건으로 그 피해액이 최대 544억에 이르렀다. 이 사건으로 인해 사이버공격의 위험성을 직접 체험하게 된 한국정부는 사이버공격에 대응하기 위해 나름대로 여러 가지 대응방안을 마련하였다. 그럼에도 불구하고 사이버공격은 계속되고 있으며, 가장 최근에는 2013년 3월 20일 한국의 방송사와 금융권에 '지능형지속위협공격'(APT)이 가해져 또 한 번 대규모의 피해가 발생하게 되었다. 이처럼 사이버공격에 대한 위협은 계속되고 있는데 반해 그에 대응하는 조직체계는 아직까지 다소 미흡한 실정이다. 더욱이 사이버공격은 대부분 해외 서버를 경유하기 때문에 외국과의 공조는 필수불가결하다. 이는 사이버공격이 더 이상 한 국가에만 국한되는 문제가 아니라는 것을 의미한다. 하지만 법규적인 문제와 실무적인 문제들로 인해 국제공조수사를 하는 것도 쉽지 않은 상황이다. 그런데 이런 상황은 비단 한국에만 국한되는 것은 아니다. 아시아의 많은 국가들이 사이버공격에 대한 위험에 처해있음에도 아직까지 적절한 조직체계나 공조체계를 수립하지 못하고 있는 실정이다. 즉, 사이버공격은 보다 지능화되고 있으며, 강력해지고 있는 반면에 그에 대한 효과적인 대응이 어려운 상황에 처해 있는 것이다. 이런 상황에 대한 해결책으로 여러 가지가 제시될 수 있겠지만 가장 절실하게 요구되고 있는 것이 사이버공격에 대한 적절한 대응을 수행할 수 있는 사이버안보 컨트롤타워의 확립이다. 여기서 말하는 컨트롤 타워는 단순히 형식적인 것을 의미하는 것이 아니라 실질적인 컨트롤 타워를 의미하

는 것이다.

가. 현 사이버안전 대응체계의 한계

한국의 국가사이버안전관리체계를 보면 국가정보원장을 의장으로 하는 "국가사이버안전전략회의"를 설치하고,[204] 그 산하에 국가정보원 차장을 의장으로 하는 "국가사이버안전대책회의"를 두고 있다.[205] 그리고 그를 사실적으로 지원해 주기 위해 각 유관기관의 과장급 공무원이 위원이 되는 "국가사이버안전실무회의"를 두고 있다.[206] 이에 따라 국가정보원이 국가사이버안전과 관련된 정책 및 관리에 있어 적어도 형식상으로 컨트롤타워의 역할을 수행하도록 되어 있는 것이다. 그리고 국방부는 사이버사령부(국방사이버지휘통제센터)를 통해 국방 분야의 사이버안전 업무를 수행하고, 미래창조과학부는 산하 한국 인터넷진흥원에 설치된 인터넷침해대응센터를 통하여 민간분야의 사이버안전 업무를 수행하며, 국가정보원은 국가사이버안전센터를 통해 국가 및 공공분야의 사이버안전 업무를 수행함과 동시에 국가차원의 종합적이고 체계적인 대응 업무를 수행하도록 체계화 되어 있다.

204) 국가사이버안전전략회의는 국가정보원장을 의장으로 하고, 각 유관기관의 차관급 공무원을 그 위원으로 하고 있다. 주요 심의 사항으로는 국가사이버안전체계의 수립 및 개선에 관한 사항, 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, 그 밖에 전략회의 의장이 부의하는 사항 등이다.

205) 국가사이버안전대책회의는 국가정보원의 사이버안전업무를 담당하는 차장이 의장이 되며, 각 유관기관의 실·국장급 공무원이 위원이 된다. 주요 심의 사항으로는 국가사이버안전 관리 및 대책방안, 전략회의의 결정사항에 대한 시행방안, 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항, 그 밖에 대책회의의 의장이 부의하는 사항 등이다.

206) 국가사이버안전실무회의는 국가사이버안전전략회의 및 대책회의에 부의된 안건과 각 회의로부터 위임 또는 지시 받은 사항의 전달 및 처리방안 협의, 사이버공격으로 인한 침해사고 발생 및 사이버위기시 대응방안 실무협의, 각 회의의 연락창구 등의 역할을 수행한다.

그림 6 국가 사이버 안전관리체계(출처: 한국인터넷진흥원)

그러나 이처럼 형식상으로는 국가정보원이 컨트롤타워 역할을 하는 것처럼 보이지만 사실 아직까지 실질적인 컨트롤타워는 존재하지 않고 있다. 그로 인해 사이버공격이 발생할 경우 여전히 대응에 많은 애를 먹고 있다. 그런 모습은 3.20 사이버공격에서도 나타나게 되었다. 우선 형식적 컨트롤타워의 전문성에 대한 의구심이 제기되기도 하였다. 사이버공격초기 민·관·군 합동조사단은 사이버공격 초기 공격에 사용된 IP가 중국 것이고, 이에 따라 북한군의 소행일 것이라고 발표했다가, 다시금 공격에 사용된 IP가 한국 것이라고 해서 조사에 신뢰성을 의심하게 하는 모습을 보였다. 결국 이후 합동조사단은 다시금 해당 사이버공격이 북한 정책총국의 소행이라는 발표를 하였다.[207] 그러나 사이버공격 초기 허둥대는 모습으로 인해 국민들의 위기감이 고조됨과 함께 정부에 대한 신뢰도가 낮아지는 문제점이 나타나게 되었다.

또한 컨트롤타워가 운영한 합동조사단의 구성 및 운영에 있어서도 문제점이 지적되었다. 이번 3.20 디도스 공격의 경우처럼 사건이 발생하면 국가 사이버안전 매뉴얼에 따라 주로 국가정보원 주도로 대응팀이 꾸려지게 되었다.[208] 하지

207) http://www.theverge.com/2013/4/10/4207980/south-korea-says-north-is-responsible-for-march-hack?utm _source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+google%2FDTsn+(ICT).

만 이번 3.20 사이버공격은 민간부문의 공격이었기 때문에 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에 따라 '민·관 합동조사팀'이 구성되어 조사가 이루어져야 했다.[209] 그러나 이번에는 해당 법률에 의하지 않고 '민관군 합동조사단'이라는 별도의 조직을 구성하여 운영한 것이다. 즉 민관군 합동조사단의 운영은 실정법의 범위를 벗어난 것이 된다. 더구나 그 운영에 있어서도 사이버공격이 발생하는 경우 그 원인 분석과 예방책, 대응방법에 중심을 두기보다는 책임소재를 규명하는데 급급하였다는 비판도 제기되었다.[210]

그러나 특히 문제가 되는 것은 비록 형식적으로 사이버안전을 위한 담당조직과 형식적인 컨트롤타워로 국가정보원을 지정해 놓고 있지만, 실질적으로는 유관기관들과 민간, 군 등이 협력하기 어렵다는 것이다. 각 조직들은 자신들만의 특징과 개성이 있고, 조직의 생리가 다르기 때문에 이들 조직들이 한 문제의 해결을 위해 서로 협력하기가 쉽지 않다. 특히 그런 조직들의 협력을 이끌어내는 컨트롤타워 기능을 주로 정보제공보다는 정보수집에 초점이 맞추어져 있는 정보기관인 국가정보원이 수행하는 것은 적절하지 않으며, 자칫하면 사이버안보 컨트롤타워가 국민을 감시하는 역할을 할 수 있다는 비판도 제기되고 있다.[211] 이런 가운데 2013년 4월 11일 정부는 국가사이버안전전략회의에서 청와대 국가안보실이 국가 사이버컨트롤타워 역할을 직접 수행하기로 결정한 것은 매우 의미가 있다. 이에 대해 청와대가 컨트롤 타워 역할을 맡아 국정원, 경찰청, 미래창조과학부, 국방부 등의 업무를 조율하고 협력체계를 구축하게 되면 부처 간 다툼이나 경쟁이 줄어들어 효과적인 협력과 조율이 가능해질 것이라고 평가되기도 했다. 다만 이는 아직까지는 원론적인 합의에 불과한 실정이다.

208) 국가사이버안전센터의 '국가 사이버안전 매뉴얼' 참조.

209) 민·관 합동조사단은 해당 법률 제48조의4에 그 근거를 두고 있으며, 평소에는 민·관 합동조사단 인력풀이 구성되어 있다가 민간부문에 사이버공격이 발생할 경우 인력풀 가운데서 선정된 전문가들로 민·관 합동조사단이 구성되어 운영된다.

210) http://www.boannews.com/media/view.asp?idx=36241&kind=1.

211) http://www.etnews.com/news/computing/security/2742801_1477.html.

나. 실질적 사이버안보 컨트롤타워 설립필요

컨트롤타워에 있어서 가장 중요한 것은 전문성이다. 사이버공간은 현실공간과 연결이 되어 있지만, 인류가 이제까지 경험해 보지 못한 특수한 공간이다. 그러므로 특히 대부분의 기성세대에게는 매우 낯선 공간이기도 하다. 이에 사이버안보에 있어서도 현실공간의 안보개념을 그대로 답습하려는 경향을 보인다. 그러나 사이버안보는 현실공간에서의 안보개념과 구분된다. 결국 사이버안보 컨트롤타워는 사이버공간에 대한 전문성을 지닌 전문가들이 주가 되어야 한다는 것이다.[212] 따라서 기존의 조직에 사이버안보 컨트롤타워의 기능을 부가적으로 맡기는 것보다는 전문성을 지닌 전문가들을 중심으로 새롭게 조직할 필요가 있다.

또한 컨트롤타워는 대내적으로 관련 유관기관들의 원활한 공조가 가능하도록 할 필요가 있으며, 대외적으로는 다른 나라들과의 공조가 가능할 수 있도록 하는 기능을 수행해야 한다. 먼저 컨트롤타워는 유관기관들의 실질적인 협력을 가능하게 할 수 있을 뿐 아니라 민·관·군에 이르기까지 광범위한 협조를 이끌어 내어야 한다. 또한 사이버안보는 매우 치명적이고 촌각을 다투는 사안이기 때문에 최고 통수권자의 빠른 판단을 요구할 수 있다. 그러므로 이를 위해서는 기존의 한 부처에서 컨트롤타워를 하는 것보다는 청와대에서 직접적으로 관여할 필요가 있다. 이런 점을 볼 때, 최근 한국의 국가사이버안전전략회의에서 청와대 사이버안보 수석이 컨트롤타워를 맡도록 결정한 것은 매우 바람직한 것이라고 생각된다. 이와 함께 컨트롤타워는 국제적인 공조를 위한 거점이 되어야 한다. 국제공조가 어려운 것은 국제적으로 통일된 법령이 없다는 것에도 있지만, 각 국가마다 서로 다른 조직체계를 가지고 있기 때문에 공조가 어려운 측면도 있다. 예를 들어 한국은 경찰뿐만 아니라 검찰도 수사권이 있다. 따라서 검찰이 수사를 하는 경우 다른 나라의 경찰에게 공조를 요구해야 한다. 이처럼 사이버공격을 담당하는 조직이 국가마다 다른 경우 공조에 어려움이 있을 수 있다. 그러므로 사이버공격에 있어 각 국가마다 컨트롤타워가 확립된다면 공조의 창구를 일원화 시킬 수 있을 것이다. 우리는 한 국가를 공격하는 사이버공격자는 그 국

212) http://www.itdaily.kr/news/articleView.html?idxno=40513#.

가만의 적이 아니라 전 세계의 적이라는 사실을 잊으면 안 된다. 다만, 컨트롤타워는 초동대처와 조사에 그 주안점을 두어야 한다. 따라서 초동대처와 조사 이후 관련 사안이 사이버전으로 판단되었을 경우에는 국방부 사이버사령부로, 사이버테러의 경우에는 국가정보원으로, 그리고 사이버범죄의 경우에는 경찰청으로 조사내용을 이관하도록 한다. 가장 이상적인 조직은 컨트롤타워가 사이버공격에 대한 전체를 관장하는 것인데, 그것은 사이버공간의 새로운 거대 권력을 창설할 수 있기 때문이다. 따라서 사이버공간에서도 권력은 분립될 필요가 있기 때문에 초기 이후의 대처는 유관기관에게 이양하며, 추후 대처를 지원해주는 역할을 하는 것이 바람직할 것이다.

4. 민 · 관 합동조사단 운영문제

가. 현행 민·관 합동조사단 운영의 문제점

민・관 합동조사단(이하 '조사단'이라고 함)의 설치 목적은 정보통신망 침해사고가 발생할 시 피해확산 방지, 사고대응, 복구 및 재발방지를 위하여 정보보호의 전문가들이 그 원인을 조사하는 것이다. 다만, 이번 3.20사이버테러의 사안에서 살펴볼 때, 조사단의 운영과 관련하여 몇 가지 문제점이 나타나고 있다. 이를 크게 조사단의 활동과 전문가 풀의 활용 면에서 살펴볼 수 있다.

「국가사이버안전관리규정」 제11조 제1항에 따르면 민간분야에 대해서 방송통신위원회 위원장은 국가정보원장과 사전에 관련정보를 공유한 후 경보를 발령하도록 하고 있으며(사이버위기경보는 정상, 관심, 주의, 경계, 심각으로 구분됨), 경계 단계에 이르렀을 경우 조사단이 조사업무를 수행하도록 되어 있다. 조사단의 근거규정은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 "정보통신망법"이라고 함) 제48조의4에 규정되어 있다. 그에 따르면 조사단은 정보통신망에 '중대한' 침해사고가 발생 시 침해사고의 원인 분석을 위해 구성될 수 있다(제2항). 이 때 조사단은 원인 분석을 위해 필요한 경우 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수

있으며, 관련 사업장에서 조사를 할 수 있다(제3항). 조사단 구성에 대한 부분은 「정보통신망법 시행령」 제59조에 규정되어 있는데, 그에 따르면 조사단은 침해사고를 담당하는 공무원, 침해사고에 관한 전문지식과 경험이 있는 자, 인터넷진흥원의 직원, 그 밖에 침해사고의 원인 분석에 필요하다고 인정되는 자 등으로 구성되며(제1항), 그 구성은 침해사고의 규모 및 유형에 따라 조정할 수 있도록 하고 있다. 그 외 조사단의 운영에 대해서는 「민·관합동조사단 운영지침」(이하 '지침'이라고 함)에 규정이 되어 있다.

나. 관계 법령의 문제점

현 법령에 따르면 조사단의 설치목적은 '경계' 단계에 이르는(중대한) 정보통신망 침해사고가 발생 시 그 원인을 분석하는 것이다. 국가사이버안전센터에 따르면 경계 단계는 복수 정보통신서비스 제공자망-기간망의 장애 또는 마비가 발생하고, 침해사고가 다수기관에서 발생했거나 대규모 피해로 발전될 가능성이 증가하여 다수 기관의 공조 대응이 필요한 단계이다. 이에 따르면 이번 3.20사이버테러와 같이 '주의' 단계이지만 그 정도가 심각한 경우에도 조사단은 활동할 수 없게 된다. 따라서 이번 사태에서 정부는 '민·관·군 합동대응팀'이라는 새로운 조직을 구성하여 조사를 수행하였다. 이는 조사단을 법률에 규정한 입법의 의미를 퇴색시킬 수 있는 것이다. 그러므로 조사단의 활동 시기를 정해주고 있는 '중대한'의 개념을 '경계' 단계에서 '주의'단계로 낮출 필요가 있다.

특히 이번 3.20사이버테러에서 눈에 띄는 것은 법률적 근거가 있는 조사단이 있음에도 법률적 근거도 없는 '민·관·군 합동대응팀'과 같이 임의적인 조직이 꾸려져서 해당 사안에 대한 조사를 벌였다는 것이다. 그러나 이번 사안과 같이 조사단이 활동해야 하는 사안임에도 불구하고 단지 중대하지 않다는 이유로 인해 임의적인 조직이 꾸려져 조사를 수행한 것은 입법취지에 어긋나는 것으로 여겨진다. 그러므로 3.20사이버테러 정도의 사안(주의)에 대해서는 조사단이 활동할 수 있도록 체계를 정비하는 것이 적절하다고 할 것이다.

조사단 구성을 위해 해당 분야의 전문가들을 필터링 하여 전문가 풀을 구성하고 있다. 현 시스템과 같이 조사단이 구성되기 이전의 전문가 풀은 법률 규정에

의해 운영되는 것이 아니라 지침에 의해 운영되고 있다. 그러므로 조사단은 법률적 근거를 두고 있는 것에 반해 조사단 풀은 단지 지침에 따라 운영되고 있는 실정이다. 조사단의 임무는 침해사건의 원인을 조사하는 것에 있기 때문에 조사를 수행하지 않을 경우 어렵게 선정해 놓은 전문가 풀을 그대로 방치하게 되는 비효율성이 존재하게 된다. 따라서 조사단의 침해사건 조사 목적이 피해 확산 방지, 사고대응, 복구 및 재발 방지에 있는 것을 고려해 볼 때, 조사단 구성 이전의 전문가 풀에서 목적을 위한 다양한 전문적인 활동을 수행할 수 있도록 조사단 전문가 풀을 활용할 수 있는 방안을 모색할 필요가 있다.

또한 지침 제6조에 따르면 전문가 풀에 속한 전문가들에게는 기술세미나 및 워크숍 참여, 모의훈련에 참여, 기타 침해사고 예방 및 대응 관련 활동에 참여하도록 하고 있으나 실제로 참여할 수 있는 기회는 이제까지 그리 많지 않았던 것으로 알려져 있다. 그러므로 조사단 구성을 위한 전문가 풀이 실제 상황 발생 시 제대로 된 조사활동을 수행할 수 있도록 상시 준비체계가 보다 정비될 필요가 있다. 따라서 예를 들어 현재 전문가 풀의 80여명의 전문가들을 미리 7~8개 정도의 조직으로(예를 들어 제1팀, 제2팀...) 구분해 놓고, 조사단이 활동할 상황이 발생 시 바로 해당 팀이 투입될 수 있도록 하는 방안도 고려해 볼 필요가 있다.

그리고 가장 큰 문제점은 실제 조사단이 구성될 경우 전문가 풀의 전문가가 조사단에서 활동을 하도록 강제하는 규정이 없다는 것이다. 따라서 최악의 경우 모든 전문가가 조사단 구성에 거부할 경우 강제할 방안이 없게 된다.

제2절 사이버범죄 절차의 개선 요청

1. 디지털 포렌식 분야의 요구

사이버범죄 법령에 반드시 포함될 필요가 있는 것으로 디지털 포렌식과 관련된 절차규정이 있다. 앞서 언급한 사이버범죄 관련 법령의 모범이 될 수 있는 유럽 사이버범죄방지협약을 보면 디지털 포렌식에 대한 규정이 비록 자세하지는

않지만 포함되어 있다. 이는 현재 우리나라에서 디지털 포렌식에 대한 법률규정이 제도로 구비되어 있지 않기 때문에 반드시 그것을 법제화 할 필요가 있다.

최근 사이버수사와 관련해서는 다음과 같은 기회요인과 위협요인이 있을 수 있다.

- 기회요인

- 정보화 사회의 고도화
- 형사소송절차의 변화
- 사이버범죄 수사의 신뢰도 증대
- 디지털 포렌식 사용영역의 확대
- 디지털 포렌식 전문인력 및 전문기술의 필요성 증대
- 국가 산업 발전 수단이라는 인식의 확대

- 위협요인

- 새로운 정부의 검찰에 대한 개혁안
- 정부기관 상호 공조체제의 어려움
- 국제공조 필요성 증대
- 형사소송법적인 문제점
- 기술발전에 따른 어려움 증대
- 전담인력 양성 인프라의 부족
- 민간기업과의 경쟁

사이버범죄수사에 있어 이런 요소를 분석해 볼 때, 한 마디로 다음과 같이 표현할 수 있다. “사이버범죄수사에 대한 외부의 요청 및 필요성은 강화되고 있는 것에 반해 사이버범죄수사의 현실은 크게 개선되지 않고 있다”라는 것이다. 이런 가운데 디지털 포렌식과 관련해서 최근 개정된 형사소송법은 사이버 범죄수사를 더욱 어렵게 하고 있다. 이와 함께 그동안 수사기관의 전유물로 생각하고 디지털 포렌식에 관심이 없던 민간부문에서도 디지털 포렌식에 관심을 갖고 많은 노력을 기울이면서 사이버범죄수사관들은 그들과의 경쟁을 이겨내야 하는 처

지가 되었다.

그럼에도 문제는 일선 수사기관에서 디지털 포렌식에 대한 현실은 여전히 많은 어려움이 있으며,[213] 법규정은 보다 엄격해 지고 있다. 그러나 더욱 불분명한 것은 관련 규정이 미비하기 때문에 그런 어려움이 배가되고 있다. 따라서 적어도 디지털 포렌식과 관련된 명확한 규정이 사이버범죄 관련 법률에 규정될 필요가 있다. 이는 형사소송법에 관련 규정이 도입되는 것이 매우 어렵기 때문이다. 현재 법무부에서 형사소송법 개정에 대한 작업이 진행중에 있는데, 여전히 디지털 포렌식에 대한 규정은 도입될 여지가 보이지 않고 있다.

2. 디지털증거 압수 · 수색에 있어서의 요구

디지털 포렌식과 함께 디지털증거 압수·수색 등에 관한 규정도 사이버범죄 관련 법률정비과정에서 마련될 필요가 있다. 그 이유는 형사소송법은 아날로그 세상을 기본으로 하고 있기 때문에 디지털증거에 대한 규정은 여러 다른 규정들과 충돌할 위험이 있기 때문이다. 따라서 사이버범죄 관련 법령이 새롭게 만들어 지는 경우에는 반드시 디지털증거에 관한 규정도 함께 도입되어야 할 필요성이 있다. 다만, 실무에서는 디지털증거에 대한 합리적인 규정의 도입을 요구하고 있지만, 현재 법무부에서 논의되고 있는 내용을 보면 아직까지도 제대로 된 디지털증거 압수·수색 규정이 마련되고 있지 않다.

디지털 포렌식과 디지털증거 압수·수색에 대한 자세한 논의는 이미 2012년 한국형사정책연구원에서 발간된 “클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구”에서 충분히 논의되었기 때문에 본 보고서에서는 생략하고자 한다.

213) 이에 대해 이원상/탁희성/송봉규, 디지털 포렌식 역량강화방안, 2012년 경찰청 연구용역보고서, 27면 이하 참조.

제3절 사이버범죄법령 관련 논의

1. 민간주도의 기본법 제정 논의

사이버범죄 관련 법령정비와 관련해서 민간차원에서 '(가칭)인터넷기본법'을 제정해야 한다는 주장이 나오기도 하였다. 2012년 10월 23일 클린넷법입법추진위원회, 클린사이버네트워크, CCN포럼, 정감넷위원회의 공동 주최로 클린넷법안 제·개정(안)을 위한 공청회·포럼이 개최되었다.[214] 해당 공청회에서는 인터넷 윤리와 기본적인 규범, ISP관리 책임, 인터넷 모욕죄 등이 담긴 (가칭)인터넷 정책기본법이 제시되었으며, 이와 함께 정보통신망법 개정을 촉구하기도 하였다. 물론 이런 논의는 진보적인 진영의 목소리보다는 다소 보수적인 측면의 견해가 주로 반영되었다고 할 수 있다.[215]

214) http://m.dt.co.kr/contents.html?article_no=2012102202012169661002.

215) 이는 공청회가 주최된 취지의 글에서 잘 나타나고 있다. 공청회 자료집의 처음을 보면, 공청회가 개최된 이유로 "1. 인터넷상에서 야기되고 있는 개인의 기본권에 대한 침해는 일반적으로 사이버 공간에서의 익명성을 매개로 하기 때문에 그 증거를 확보하기가 용이하지 않고 직접적으로 생명이나 신체에 결부되는 것은 아니므로 피해가 경미하다는 인식 때문인지 형사사법기관의 인지도가 낮고 법적 처벌이 제대로 이루어지지 않고 있는 실정이다. 그러나 인터넷간에 게시된 정보 등은 빠른 시간 내에 광범위하게 확산되는 특징을 갖고 있기 때문에 그 피해정도는 결코 경미하다고 치부해 버릴 수 없음은 주지의 사실이다. 인터넷의 대중화와 함께 발생한 이러한 폐단들에 대해서, 인터넷 이용자들에 의한 자율적 규제와 통제는 사실상 그 기능을 다하지 못하고 있으며, 기능을 하고자 하는 의지가 있는지 마저 의심케 하는 실정이라고 할 수 있다. 무엇보다 우려스러운 것은 인터넷에서의 명예훼손과 모욕 등은 별달리 죄가 되지 않는다고 느끼는 도덕적 불감증이 사회 전반에 아직까지도 만연해 있다는 사실이다. 익명성과 비대면성의 그림자가 우리의 자아를 흉폭한 하이드의 모습으로 변화시키는 촉매제의 역할을 너무도 쉽게 수행하고 있다고 할 수 있다.

2. 이른 바 '사이버 폭력'에 대응하는 법률적인 장치가 없는 것은 아니지만 실효성 있게 운용되지는 못하고 있는 실정이다. 물론 규제를 강화하는 것만이 능사는 아니며 근본적으로 국민의 알권리 및 표현의 자유와 개인의 인격권은 적절한 형량의 관계를 유지해야 할 것이다. 그러나 국민에게 알 권리가 있다고 해서, 표현의 자유가 있다고 해서, 그 권리와 자유에는 한계가 있는 것이다. 인터넷 관련법은 피해자가 규제받을 수 있을 뿐 아니라 잊혀질 권리를 보장받아야 하고, 가해자는 피해자에게 발생한 피해를 배상하여야 하며, 인터넷포털사(ISP)는 시간적 공간적으로 무한대에 가까운 인터넷의 특성과 청소년에 미치는 영향력이 지대하다는 점을 감안하여 그 책임을 강화하는 등 인터넷 이용의 윤리와 철학과 법적 규율 및 표현의 자유와의 한계선을 그을 필요가 있다. 이러한 인식하에 클린인터넷을 위한 제개정법안은 다음 두 가지로 구성된다. 그 하나는 정보통신망법의 개정안이고 다른 하나는 인터넷 기본법의 제정이다." 등을 언급하고 있다.

해당 공청회에서 논의된 내용을 보면 정보통신망법에서의 논의 주제로 사이버 모욕죄를 신설하되 친고죄로 규정하는 것, ISP의 책임 강화, 사이버 명예훼손죄를 반의사불벌죄에서 배제 여부, 인터넷실명제 유지 여부에 관한 것들이었다. 더 나아가 인터넷 이용자의 윤리 및 책임의식을 고취시키고, 정보통신망법을 포함하여 보다 실질적인 기본법이 필요하다는 인식하에 (가칭)인터넷기본법(안)을 제시하였다. 해당 안의 내용은 다음과 같다.

(가칭) 인터넷 기본법(시안)

제1장 총칙

제1조(목적) 이 법은 건전한 인터넷 환경 조성을 위한 국민의 권리·책무와 국가 책무를 명확히 하고 인터넷 정책의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정하여 인간의 존엄을 바탕으로 한 사회적, 윤리적 가치와 창의 및 혁신을 유지함으로써 국민의 삶의 질을 높이는 것을 목적으로 한다.

제2조(기본이념) 이 법은 인간의 존엄을 바탕으로 한 사회적, 윤리적 가치와 창의 및 혁신이 조화를 이루는 인터넷 환경을 실현하고 이를 지속적으로 발전시키는 것을 기본이념으로 한다.

제3조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “인터넷”이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비와 컴퓨터를 연결하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제의 집단을 서로 연결한 정보통신망을 말한다.
2. "인터넷서비스"란 제1호의 인터넷을 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
3. "인터넷서비스 제공자"란 제2호의 인터넷서비스를 제공하는 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. "이용자"란 인터넷서비스 제공자가 제공하는 인터넷서비스를 이용하는 자를 말한다.
5. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
6. "인터넷 관련 산업"이란 제1호의 인터넷과 관련된 제품을 개발·생산 또는 유통하는 사업이나 인터넷에 관한 컨설팅 등과 관련된 산업을 말한다.

제4조(다른 법률과의 관계) ① 인터넷 정책의 추진에 관한 다른 법률을 제정하거나 개정할 때에는 이 법의 목적과 기본이념에 맞도록 노력하여야 한다.
② 인터넷 정책의 추진에 관하여 이 법률의 규정과 「정보통신망 이용촉진 및 정보보호에 관한 법률」, 「개인정보보호법」, 「국가정보화기본법」 등의 적용이 경합하는 때에는 이 법을 우선 적용한다.

제5조(정부의 책무) ① 정부는 인간의 존엄을 바탕으로 한 사회적, 윤리적 가치와 창의 및 혁신이 조화를 이루는 인터넷 환경을 실현하고 이를 지속적으로 발전시키기 위하여 인터넷기본계획을 수립하여 시행할 책무를 진다.
② 정부는 인터넷서비스의 특성이나 기술 또는 이용자의 서비스 수용행태 등을 종합적으로 고려하여

동일한 서비스로 볼 수 있는 경우에는 동일한 규제가 적용되도록 노력하여야 한다.
③ 정부는 인터넷서비스 제공자단체 또는 이용자단체가 건전한 인터넷 환경을 조성하기 위한 활동을 지원할 수 있다.
④ 정부는 인터넷 정책을 추진하기 위하여 대통령령으로 정하는 바에 따라 민간기관 등과 협의체를 구성·운영할 수 있다.

제6조(인터넷서비스 제공자의 책무) ① 인터넷서비스 제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 인터넷서비스를 제공하여 이용자의 권익을 보호하고, 자신이 운영·관리하는 인터넷서비스에 타인의 권리를 침해하는 정보가 유통되지 아니하도록 노력하여야 한다.
② 인터넷서비스 제공자는 인터넷서비스 제공과 관련하여 정당한 사유 없이 이용자를 차별하여서는 아니 된다.
③ 인터넷서비스 제공자단체는 이용자를 보호하고 안전하며 신뢰할 수 있는 인터넷서비스를 제공하기 위하여 인터넷서비스 제공자 행동강령을 정하여 시행하는 등 자율규제를 할 수 있다.

제7조(이용자의 권리와 책무) ① 이용자는 합법적인 콘텐츠, 애플리케이션, 서비스 및 인터넷에 위해가 되지 않는 기기 또는 장치를 자유롭게 이용할 권리가 있다.
② 이용자는 인터넷에서 다른 이용자의 권리를 침해하지 않고, 인간의 존엄을 바탕으로 한 한 사회적, 윤리적 가치가 유지되도록 노력하여야 한다.
③ 이용자는 정부의 인터넷 정책에 협력하여야 한다.

제8조(보고) ① 정부는 매년 주요 인터넷 정책의 추진상황에 관한 보고서를 국회에 제출하여야 한다.
② 제1항의 보고서에는 다음 각 호의 사항이 포함되어야 한다.
1. 국내외 인터넷 현황
2. 인터넷 정책의 추진상황
3. 그 밖에 인터넷에 관한 주요 사항
③ 방송통신위원회는 제1항의 보고서 작성에 필요한 자료의 제출을 관계 중앙행정기관의 장에게 요청할 수 있으며, 관계 중앙행정기관의 장은 특별한 사유가 없으면 이에 따라야 한다.

제2장 인터넷 정책의 계획 및 추진체계

제9조(인터넷 정책의 계획) ① 인간의 존엄을 바탕으로 한 사회적, 윤리적 가치와 창의 및 혁신이 조화를 이루는 인터넷 환경을 실현하고 이를 지속적으로 발전시키기 위하여 방송통신위원회는 관계 중앙행정기관의 장과 협의 하에 작성하여 3년마다 인터넷 정책의 계획을 작성하여 제10조의 인터넷정책위원회에 제출하고, 위원회의 심의·의결을 거쳐 시행하여야 한다.
② 제1항에 따른 정책에는 다음 각 호의 사항이 포함되어야 한다.
1. 인터넷에서 사생활 및 인터넷을 통하여 수집·처리·보관·이용되는 개인정보의 보호 및 그와 관련된 기술의 개발·보급
2. 인터넷의 안전성 및 신뢰성 제고
3. 인터넷에서 정보격차의 해소
4. 인터넷에서 지적재산의 보호와 이용의 조화
5. 인터넷에서 이용자의 명예 보호
6. 인터넷에서 청소년의 보호
③ 방송통신위원회는 제1항에 따른 정책 중 「국가정보화 기본법」에 따른 국가정보화 기본계획과 관련되는 사항은 같은 법에 따른 국가정보화전략위원회에 통보하여야 한다.

제10조(인터넷정책위원회) ① 인터넷 정책에 관한 사항을 심의·의결하기 위하여 OOO 소속으로 인터넷정책위원회(이하 "위원회"라 한다)를 둔다. 위원회는 그 권한에 속하는 업무를 독립하여 수행한다.
② 위원장은 OOO가 하고, 위원은 다음 각 호의 사람이 된다.
1. 국회사무총장, 법원행정처장, 헌법재판소사무처장과 중앙선거관리위원회사무총장
2. 중앙행정기관의 장과 지방자치단체의 장 중 대통령령으로 정하는 사람
3. 인터넷에 관한 전문지식과 경험이 풍부한 사람 중에서 OOO가 위촉하는 사람
③ 제2항제3호에 따른 위원의 임기는 2년으로 하고, 1차에 한하여 연임할 수 있다.

④ 위원회의 효율적 운영 및 지원을 위하여 간사 1명을 두되, 간사는 방송통신위원장이 된다.
⑤ 제1항부터 제4항까지에서 규정한 사항 외에 위원회의 조직과 운영에 필요한 사항은 대통령령으로 정한다.

제11조(위원회의 기능 등) ① 위원회는 다음 각 호의 사항을 심의·의결한다.
1. 제8조에 따른 계획
2. 인터넷과 관련된 정책, 제도 및 법령의 개선에 관한 사항
3. 인터넷에 관한 법령의 해석·운용에 관한 사항
4. 제8조에 따른 보고서의 작성·제출에 관한 사항
5. 인터넷과 관련하여 대통령, 위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
6. 그 밖에 이 법 또는 다른 법령에 따라 위원회가 심의·의결하는 사항
② 위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요하면 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터 의견을 들을 수 있고, 관계 기관 등에 대하여 자료 등의 제출을 요구할 수 있다.

제3장 인터넷의 기본 방향 및 관련 정책

제12조(인터넷에서 사생활 및 개인정보의 보호) ① 이용자는 인터넷에서 타인의 사생활과 개인정보를 침해하는 정보를 유통시켜서는 아니 된다.
② 인터넷서비스 제공자는 자신이 운영·관리하는 인터넷에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
③ 방송통신위원회는 인터넷에 유통되는 정보로 인한 타인의 사생활과 개인정보를 침해하는 행위를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을 마련하고 이를 인터넷서비스 제공자에게 권고할 수 있다.

제13조(인터넷에서 안전성 및 신뢰성 제고) ① 이용자는 인터넷의 안전성 및 신뢰성을 저해하는 행위를 하여서는 아니 된다.
② 인터넷서비스 제공자는 자신이 운영·관리하는 인터넷에서 제1항에 따른 행위가 발생하지 아니하도록 노력하여야 한다.
③ 방송통신위원회는 인터넷의 안전성 및 신뢰성을 저해하는 행위를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을 마련하고 이를 인터넷서비스 제공자에게 권고할 수 있다.

제14조(인터넷에서 정보격차의 해소) 방송통신위원회는 이용자가 인터넷서비스에 원활하게 접근하고 정보를 유익하게 활용할 권리를 실질적으로 누릴 수 있도록 필요한 정책을 마련하여야 한다.

제15조(인터넷에서 지적재산의 보호와 이용의 조화) ① 이용자는 인터넷에서 타인의 지적재산을 침해하는 정보를 유통시켜서는 아니 된다.
② 인터넷서비스 제공자는 자신이 운영·관리하는 인터넷에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
③ 방송통신위원회는 지적재산권자의 권리와 이용자의 공정한 이용을 조화하여 문화 및 인터넷 관련 산업이 향상발전 할 수 있도록 노력하여야 한다.

제16조(인터넷에서 명예 보호) ① 이용자는 인터넷에서 타인의 명예를 훼손하는 정보를 유통시켜서는 아니 된다.
② 인터넷서비스 제공자는 자신이 운영·관리하는 인터넷에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
③ 방송통신위원회는 인터넷에 유통되는 정보로 인한 타인의 명예훼손 행위를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을 마련하고 이를 인터넷서비스 제공자에게 권고할 수 있다.

제17조(인터넷에서 청소년의 보호) ① 이용자는 인터넷에서 청소년에게 유해한 정보를 유통시켜서는 아니 된다.
② 인터넷서비스 제공자는 자신이 운영·관리하는 인터넷에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
③ 방송통신위원회와 여성가족부장관은 인터넷을 통하여 유통되는 음란·폭력정보 등 청소년에게 해로운 정보로부터 청소년을 보호하기 위한 시책을 마련하여 이를 인터넷서비스 제공자에게 권고할 수 있다.

제18조(인터넷서비스의 품질 개선) ① 방송통신위원회는 인터넷 서비스 이용자의 권익을 보호하고 인터넷 서비스의 품질 향상 및 안정적 제공을 보장하기 위한 시책을 마련하여야 한다.
② 방송통신위원회는 제1항에 따른 시책을 추진하기 위하여 필요하면 인터넷서비스 제공자단체 및 이용자단체 등의 의견을 들어 인터넷서비스 품질의 측정·평가에 관한 기준을 정하여 고시할 수 있다.
③ 인터넷서비스 제공자는 제2항에 따른 기준에 따라 자율적으로 인터넷 서비스의 품질 현황을 평가하여 그 결과를 이용자에게 알려줄 수 있다.

제19조(인터넷 관련 산업의 기반 조성) 정부는 인터넷 관련 산업의 기반조성을 위하여 필요한 시책을 마련하여야 한다.

제20조(국제협력) 정부는 인터넷 정책에 관한 국제적 동향을 파악하고 국제협력을 추진하여야 한다.

제21조(투명한 인터넷 트래픽 관리) 「전기통신사업법」에 따라 인터넷접속서비스를 제공하는 자(이하 "인터넷접속서비스제공사업자"라 함)는 인터넷 트래픽 관리의 목적, 범위, 조건, 절차 및 방법 등을 명시한 트래픽 관리기준을 공개하고, 트래픽 관리에 필요한 조치를 하는 경우 그 사실과 영향 등을 이용자에게 고지하여야 한다. 다만, 이용자에게 고지하기 어려운 부득이한 사유가 있는 경우에는 공지로 갈음할 수 있다. 방송통신위원회는 필요한 경우 공개 및 고지 또는 공지 대상 정보의 범위 및 방식 등을 별도로 정할 수 있다.

제22조(차단 금지) 인터넷접속서비스제공사업자는 합법적인 콘텐츠, 애플리케이션, 서비스 또는 망에 위해가 되지 않는 기기 또는 장치를 차단해서는 안된다. 다만, 합리적인 트래픽 관리의 필요성이 인정되는 경우에는 그러하지 아니하다.

제23조(불합리한 차별 금지) 인터넷접속서비스제공사업자는 콘텐츠·애플리케이션·서비스의 유형 또는 제공자 등에 따라 합법적인 트래픽을 불합리하게 차별해서는 안된다. 다만, 합리적인 트래픽 관리의 필요성이 인정되는 경우에는 그러하지 아니하다.

제24조(합리적인 트래픽 관리) ① 인터넷접속서비스제공사업자는 다음 각 호의 하나에 해당하는 경우 트래픽 관리를 할 수 있다.
1. 망의 보안성 및 안정성 확보를 위해 필요한 경우
2. 일시적 과부하 등에 따른 망 혼잡으로부터 다수 이용자의 이익을 보호하기 위해 필요한 경우
3. 국가기관의 법령에 따른 요청이 있거나 다른 법령의 집행을 위해 필요한 경우
4. 그 밖에 합리적인 트래픽 관리의 필요성이 있다고 방송통신위원회가 인정한 경우
② 그 밖에 합리적인 트래픽 관리의 범위, 조건, 절차, 방법 및 트래픽 관리의 합리성 여부에 대한 판단 기준 등은 방송통신위원회가 별도로 정한다. 이 경우 유무선 등 해당 망의 유형과 기술 특성에 따라 다르게 정할 수 있다.

부칙

이 법은 2013년 1월 1일부터 시행한다.

2. 해당 법률안에 대한 검토

민간차원에서 기본법에 대한 논의가 나오고 있다는 것은 매우 바람직하다고 여겨진다. 대부분의 법률안들은 국회나 정부, 기업 등에 의해 제시되는 경우가 많기 때문에 민간의 목소리가 담기기 쉽지 않기 때문이다. 그러나 해당 주제가 민간차원에서 제기된 만큼 정책적으로 반영되기 어려운 측면도 존재한다.

가. 정보통신망법 개정안에 대한 고찰

1) 사이버모욕죄 신설

본 법률안 제44조의7 제2의2호에서는 소위 사이버모욕죄의 내용을 기술해 놓고 있으며, 벌칙규정인 제70조 제4항에서는 이에 대한 처벌로서 1년 이하의 징역이나 금고 또는 1천만원 이하의 벌금에 처하도록 규정해 놓고 있다. 또한 동조 제4항에서는 이를 친고죄로 규정하고 있다. 본 법률안을 보면 기본적으로 사이버명예훼손죄와 유사한 구조를 띠고 있다. 따라서 사이버모욕죄의 경우 자유형은 같지만 벌금형은 1천만원으로 형법상 모욕죄의 200만원보다 높게 규정되어 있다.

현재 사이버공간에서의 모욕은 형법 제311조에 의해서 처벌될 수 있다. 과거 사이버모욕죄의 신설을 주장하면서 입법의 불비를 근거로 제시한 경우도 있지만, 입법의 불비는 아니다. 다만, 소위 사이버명예훼손죄와 같이 별도의 규정으로 특정되어 있지 않기 때문에 일반인들이 쉽게 알 수 없는 점은 있다.

과거 사이버모욕죄와 관련한 법률안들을 보면 그 형량이 매우 높다는 점과 친고죄를 반의사불벌죄로 고치는 것을 골자로 하고 있었다. 이에 대해 형법학계에서는 많은 우려를 나타내며 대체적으로 반대하는 견해가 우세하였다. 이에 반해 본 법률안에는 과거 지적되었던 문제점들은 나타나지 않고 있다. 이는 법리적으로 볼 때, 설사 사이버모욕죄를 인정하더라도 그 범위가 명예훼손죄 보다는 낮아야 한다는 것에 부합하는 것이라고 할 수 있다. 다만 벌금형이 1천만원으로 규정되어 형법 제307조 제1항의 명예훼손죄보다는 높다. 또한 친고죄도 유지하고 있기 때문에 반의사불벌죄로 대체되어 수사기관에 의한 수사가 언제라도 개시될 수 있다는 우려도 존재하지 않고 있다.

그럼 이처럼 사이버모욕죄에 대해서 과거에 제기되었던 문제점들이 나타나지 않으며, 현행 법률에 의해서도 이미 처벌되고 있는 수준에서 규정되고 있는 사이버모욕죄가 과연 필요한지로 문제의 초점이 이동될 수 있다. 즉, 앞에서도 언급한 바와 같이 이미 사이버공간에서의 모욕행위는 형법에 의해서 처벌이 가능하기 때문에 구태여 형량에서 큰 차이가 없는 사이버모욕죄를 신설할 필요성이 있는지가 문제가 될 것이다. 물론 개정안은 사람을 비방할 목적과 정보통신망을

명예훼손죄에서 그대로 차용하고 있기 때문에 형법상 모욕죄보다는 구성요건이 엄격해졌으며, 형량에서도 벌금형이 1천만원으로 높아졌다. 사실 본 개정안이 의미를 갖기 위해서는 강화된 구성요건을 통해 형량이 높아진다거나 친고죄가 반의사불벌죄로 바뀌는 것이다. 따라서 '사람을 비방할 목적으로 정보통신망을 통하여'라는 요건을 통해 벌금형만을 높이는 것이 현행 모욕죄로 처벌하는 것과 비교하여 큰 의미를 가질 수 있을지 의문이 든다.

다만, 사이버모욕죄가 일반적인 모욕죄에 비해 불법성이 클 수 있는 것은 사이버공간의 특성상 그 피해가 광범위할 뿐 아니라 그 내용이 삭제되기 쉽지 않아 검색을 통해 누구라도 언제나 그 내용을 알 수 있게 되기 때문이다. 그러므로 이런 점에 의해서 일반적인 모욕죄보다는 엄하게 처벌해야 한다는 요청이 있을 수 있다.

하지만 이런 요청에 의하더라도 본 법률안에는 다소 문제가 있을 수 있다. 사이버명예훼손죄가 사람을 비방할 목적을 통해서 목적범으로 구성하고 있는 것은 일반적인 명예훼손죄에 비해 형량이 높은 대신 그 구성요건을 제한하고 있는 장치를 마련한 것이라고 할 수 있다. 그런데 모욕죄는 판례에 따르면 '도둑놈', '죽일놈', '저 망할 년 저기 오네'와 같이 그 성격상 추상적인 경멸을 표현하였을 경우를 의미한다. 따라서 이미 비방의 목적이 있다고 볼 수 있다. 또한 정보통신망을 통할 경우 이미 공공연한 것이 되기 때문에 구태여 '공공연하게'라는 표현을 할 필요도 없게 된다.

2) 정보통신서비스 제공자 의무강화

본 법률안에는 정보삭제 및 임시조치 등과 같은 요청을 받고 정보통신서비스 제공자가 지체 없이 삭제 및 임시조치를 취하지 않을 경우 3천만원 이하의 과태료를 부과하도록 하고 있다. 이는 현행 법률이 방송통신위원회의 명령을 이행하지 않은 경우 과태료를 부과하고 있는 것에 비해 그 적용범위를 매우 넓혀 놓은 것이다. 여기에서 우려가 되는 것은 현재에도 정보통신서비스 제공자가 자의적이고 임의적, 형식적으로 게시물에 대해 임시조치를 취하여 표현의 자유를 침해하고 있다는 비판이 가해지고 있는 가운데 방통위의 명령이 없이도 삭제 및 임

의조치를 강요하도록 규정하는 것이 적절한지에 대한 반론이 제기될 수 있다는 것이다. 이는 한 편으로는 정보통신서비스 제공자에게 검열의 가능성을 높여줄 수 있으며, 다른 한 편으로는 표현의 자유를 과도하게 제한할 수 있는 것이기 때문에 실제로는 과태료 규정 이상의 의미를 가질 수 있다. 따라서 이에 대해서는 다시 한 번 생각해 볼 필요성이 있다.

나. 인터넷 정책 기본법에 대한 고찰

먼저 제목에 대한 부분에 있어서 본 법률안은 “인터넷”이라는 용어를 사용하고 있다. 이 법은 사이버공간 전체를 규율하는 것을 목적으로 하고 있다고 여겨지는데 제목을 “인터넷”이라고 할 경우 그 범위가 매우 좁아지게 된다. 일례로 이 개념을 그대로 사용하게 되면 인트라넷망이나 전화망은 개념에서 제외되게 된다. 더 나아가 기존에 있는 정보통신망법과의 차별성도 나타나지 않을 수 있으며, 오히려 기본법임에도 불구하고 정보통신망법보다도 그 개념범위가 줄어들게 되는 불합리함도 나타나게 된다. 따라서 제목에 대한 고려를 다시금 할 필요가 있다고 사료된다.

그리고 제1조의 목적 및 제2조 기본이념, 기타 여러 조문들에 있어서 사회적, 윤리적 가치를 규정해 놓고 있는데 현대의 다원화된 사회에서 사회적, 윤리적 가치도 매우 다원화 되어 있다고 할 수 있어 과연 어떤 사회적, 윤리적 가치를 의미하는지가 불명확하다. 이는 자칫하면 사이버공간을 사회적, 윤리적 가치의 전쟁터로 내몰 수 있는 위험이 있다. 이에 대해서 다시금 고려해 볼 필요가 있다.

○ 제4조(다른 법률과의 관계) ② 인터넷 정책의 추진에 관한 다른 법률을 제정하거나 개정할 때에는 이 법에 부합되도록 하여야 한다.

앞에서 언급한 바와 같이 우리나라의 법체계의 경우 기본법이 다른 법률에 비해 우위에 있을 어떤 이유도 없다. 따라서 이후에 제정되는 법률이 이 기본법에 부합하지 않는다고 하더라도 문제가 되지 않는다. 즉, 본 조문은 큰 의미가 없게 되는 것이다.

○ **제7조(이용자의 권리와 책무) ③ 이용자는 정부의 인터넷 정책에 협력하여야 한다.**

우려가 되는 조문이다. 이용자가 정부의 인터넷 정책에 협력해야 하는 의무를 규정하고 있는데 특정 사업자나 대상자가 아닌 전체 이용자(국민)에게 정부의 정책에 협력하라는 의무를 규정하는 것은 매우 위험하다고 할 수 있다. 혹시라도 이것이 가능하기 위해서는 정부의 인터넷 정책이 언제나 옳고 정당하다는 전제가 있어야 하는데 이는 불가능하다. 매우 많은 논란이 예상되는 규정이다. 따라서 이 규정은 삭제되어야 할 것이다.

제10조에서는 인터넷 정책에 관한 사항을 심의·의결하기 위하여 인터넷정책위원회를 설치하도록 되어 있는데, 이 위원회와 방송통신위원회와의 차이점이 무엇인지가 분명하지 않다. 제11조를 참조해 볼 때, 인터넷정책위원회에서 하는 업무는 이미 방송통신위원회에서 하고 있는 업무이다. 그렇다면 본 법률안의 성격과 내용을 고려해 볼 때, 방송통신위원회의 업무 가운데 일부가 인터넷정책위원회로 이관되는 것으로 이해해야 할 듯하다. 하지만 제18조에서는 방송통신위원회가 인터넷서비스 품질개선을 위한 노력을 하도록 규정되어 있다. 그렇다면 방송통신위원회도 관련 업무를 수행한다는 것을 의미하게 되는데, 두 기관의 업무가 어떻게 구분될 수 있을지가 의문이다. 더구나 구태여 이미 기능을 하고 있는 위원회가 있음에도 다시금 인터넷정책위원회를 만들어야 하는지도 의문이 든다.

○ **제13조(인터넷에서 안전성 및 신뢰성 제고) ① 이용자는 인터넷의 안전성 및 신뢰성을 저해하는 행위를 하여서는 아니 된다.**

제13조에서는 "안정성 및 신뢰성을 저해하는 행위"를 하지 말도록 하고 있는데, 그 개념이 매우 모호하다. 자신의 컴퓨터에 있는 바이러스를 체크하지 않는 경우 인터넷의 안정성을 저해하는 행위이며, 실명을 사용하지 않는 경우는 신뢰성을 저해하는 행위가 된다. 이런 부분들까지도 염두에 두고 있는 규정인지 의문이 든다.

제14조(인터넷에서 정보격차의 해소)는 인터넷이 보급되기 시작할 초기에나 규정될만한 규정이다. 이미 국가정보화사업 등으로 인해서 우리나라에서는 사라진 개념이라고 할 수 있다.

제15조는 이미 지식재산권 기본법 등에서, 제16조는 정보통신망법에서, 제17조도 청소년보호법 등에 규정되어 있는 등 이미 개별법 등에 보다 상세하게 규정되어 있다.

다. 소결

정보통신망 개정안의 경우 세 가지 부분의 논점이 있다. 먼저 헌재의 위헌결정에 따른 실명제 관련 부분의 삭제가 있다. 이는 헌재의 위헌결정에 따른 필연적인 것이라고 할 수 있다. 다음으로 사이버모욕죄에 대한 부분은 과거의 법률안보다는 합리적이라고 생각되지만, 양형이나 조문 자체의 문제점들이 눈에 띈다. 그리고 정보통신서비스 제공자에 대한 과태료 규정은 재고할 필요가 있다고 여겨진다.

기본법과 관련해서는 개인적으로 가장 좋은 입법형식은 먼저 인터넷 기본법이 제정되고 이를 바탕으로 입법자들이 다른 법률들이 이 법률을 프레임으로 하여 작동할 수 있도록 법률을 제정하는 것이다. 하지만 이미 개별법률들이 존재하는 상황에서, 더구나 본 법률안이 고려하고 있는 내용들이 이미 개별법률들에 규정이 되어 있는 상황에서 과연 본 법률안이 (제정되면) 실제적으로 기본법으로서의 역할을 수행할 수 있을지 우려된다. 또한 본 법률을 보면 상당수의 내용이 이미 정보통신망법에 규정되어 있으며, 이를 주관하는 인터넷정책위원회의 업무는 방송통신위원회의 업무와 중복된다. 결국 하나의 업무를 하는 두 위원회가 존재하게 되는 것으로 결국 또 하나의 위원회만 만들어지게 되는 것이다. 또한 다른 관련 규정들은 이미 관련 내용들이 개별법률들에 규정되어 있기 때문에 큰 의미가 없다고 여겨진다. 그렇다면 결국 본 기본법에서 의미를 찾을 수 있는 것은 제20조~제23조의 규정들이라고 할 수 있다.

본 법률안이 의미를 갖기 위해서는 기본법의 성격을 최대한 활용하여 현재 입

법이 미치지 않는 범위를 고려하여 제정되는 것이다. 물론 본 기본법이 제정되고, 기타 개별법률들이 기본법에 맞게 다시금 정비되는 것이 가장 바람직한 경우일 것이다. 하지만 이것을 기대하는 것은 쉽지 않다. 이것이 가능하기 위해서는 대대적인 법률정비작업이 요구되기 때문이다. 그러므로 본 입법안이 기본법으로서의 기능을 하기 위해서는 현재 개별입법들이 다루고 있지 않은 IT기본법 관련 내용들, 망중립성 등의 내용이 추가되어야 될 것 같다.

3. 기술 환경 변화에 따른 기본법 논의

가. 입법론의 배경

기술 환경이 변화함에 따라 그에 대응하기 위한 기본법이 제정되어야 한다는 논의도 제기되고 있다. 입법이유서에 따르면 클라우드컴퓨팅 환경에 따른 기본법이 필요한 이유로서 클라우드컴퓨팅 환경이 전 세계적으로 점차 보편화되어 감에 따라 글로벌 시장에서는 클라우드컴퓨팅 환경에 맞추어 법과 제도적인 장치들이 마련되고 있다는 점을 들고 있다. 그런데 우리나라는 클라우드컴퓨팅의 서비스 경쟁력이나 기술역량, 인적 자원 등이 경쟁국들에 비해 상대적으로 뒤쳐져 있을 뿐 아니라 클라우드 컴퓨팅 환경과 관련된 법과 제도적 장치도 미흡한 상황에 처해 있다. 따라서 그와 같은 세계적인 추세에 맞추어 가기 위해서는 “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(이하 ‘클라우드컴퓨팅법’이라고 함)”을 제정하여 클라우드 환경에 대한 서비스, 기술 등에 대한 여러 문제들과 클라우드컴퓨팅을 사용하는 사용자들을 보호하기 위한 근거들이 마련될 필요가 있다.

본 법률안이 중요할 수 있는 이유는 이제까지는 정보통신망법이 해당 사안의 기본법적인 역할을 수행하였지만, 클라우드컴퓨팅 환경이 조성되면서 클라우드컴퓨팅법이 바통터치를 할 수 있다는 것이다. 물론 현재의 법률안을 보면 아직까지는 제한적인 부분이 많지만, 일단 법률안이 발효되고, 클라우드컴퓨팅 환경이 보다 보편화 된다면 정보통신망법의 역할을 상당부분 흡수할 것이라고 생각

된다. 그러므로 본 법률안의 내용을 주의 깊게 살펴볼 필요가 있다.

나. 주요내용

클라우드컴퓨팅법의 기본 내용은 크게 총칙(안 제1조~제5조), 클라우드컴퓨팅 시책의 마련 및 발전기반 조성(안 제6조~제13조), 클라우드컴퓨팅서비스의 이용촉진 등(안 제14조~제20조), 클라우드컴퓨팅서비스의 신뢰성 제고(안 제21조~제32조), 기타 필요사항 규정(안 제33조~제38조) 등으로 나누어질 수 있다.

먼저 제1장 총칙에서는 법의 목적, 정의, 국가 및 지방자치단체의 책무, 클라우드컴퓨팅서비스 제공자 및 이용자의 책무, 다른 법률과의 관계 등이 규정되어 있다. 여기에서 눈에 띄는 것은 국가와 지방자치단체에게는 클라우드컴퓨팅의 발전과 이용촉진, 안전, 재원 확보에 대한 책무를, 클라우드컴퓨팅서비스 제공자에게는 이용자의 정보보호 및 서비스의 신뢰에 대한 책무를, 이용자에게는 안전한 사용의 책무를 부과하고 있다는 것이다.

제2장 클라우드컴퓨팅 시책의 마련 및 발전기반 조성 등에 대한 규정에서는 클라우드컴퓨팅 발전 및 이용자 보호에 관한 시책의 마련·시행 요청, 실태조사 실시, 연구개발 촉진, 시범사업 추진, 세재지원 방안, 중소기업 등의 지원 방안, 전문인력 양성 방안, 국제협력 및 해외진출의 촉진 방안 등이 규정되어 있다.

제3장 클라우드컴퓨팅 서비스의 이용촉진 등에서는 클라우드컴퓨팅 서비스업의 신고 등의 절차에 관한 사항, 클라우드컴퓨팅 서비스업의 양수 및 법인의 합병 등 사업에 관한 사항, 공공기관등의 클라우드컴퓨팅 도입 및 이용 등에 관한 사항, 전산시설·장비·설비 등의 구비와 관련된 사항, 서비스 제공자간 상호운영성의 확보 방안, 클라우드컴퓨팅 서비스의 인증 및 인증기관 취소 등에 관한 내용이 규정되어 있다.

제4장 클라우드컴퓨팅 서비스의 신뢰성 제고에서는 클라우드컴퓨팅의 품질·성능의 신뢰성 향상, 해당 표준약관, 침해 사고의 통지, 서비스 안전지침, 정보의 제3자 제공 금지, 클라우드컴퓨팅서비스 이용사실의 공개, 정보의 국외저장에 대한 공개, 정보의 보존 및 복구를 위한 조치, 이용자 정보의 임치, 정보의 반환·파기, 클라우드컴퓨팅 서비스의 중단에 대한 대책 마련, 손해배상 책임

등 클라우드컴퓨팅 서비스 제공자와 관련된 제반 사항들이 규정되어 있다. 이는 최근 서비스제공자에 대한 높은 욕구를 반영한 것이라고 할 수 있다.

그리고 제5장 보칙에서는 클라우드컴퓨팅 서비스 제공자의 협회설립, 방송통신위원회의 시정명령 등의 조치, 권한 또는 업무의 위임·위탁 등에 관한 내용이 규정되어 있으며, 제6장 벌칙에서는 일정한 행위에 대한 형벌 규정과 과태료 규정을 명시해 놓고 있다.

다. 해당 법률안의 검토

클라우드 컴퓨팅법에 대한 논의는 여전히 진행 중에 있다. 아직까지 확실한 법률안은 도출되지 않은 실정이다. 다만, 그 기본적인 줄기는 어느 정도 만들어졌다고 여겨진다. 이제까지 논의된 결과를 보면 클라우드컴퓨팅법은 초기 정보통신망법이 제정될 당시의 모습과 흡사하다는 생각이 든다. 다만, 클라우드컴퓨팅법이 "...클라우드컴퓨팅의 발전 및 이용을 촉진하고 클라우드컴퓨팅서비스를 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 국민경제의 지속가능한 발전에 이바지함..."을 그 목적으로 하고 있는 것에 반해 규정된 내용들은 주로 클라우드컴퓨팅 서비스제공자에 초점이 맞추어져 있기 때문에 그 규정범위가 생각보다 협소하다는 생각이 든다. 물론 아직까지 완결된 법률이 아니기 때문에 최종안을 살펴볼 필요는 있다.

제5장

사이버범죄 관련 법령정비방안 제언

이원상 · 강석구

05

사이버범죄 관련 법령정비방안 제언

제1절 사이버범죄 처벌법의 제정안

사이버범죄 관련 법령을 정비하기 위해 크게 세 가지의 관점에서 제언을 하고자 한다. 먼저 가장 이상적인 방법은 이른바 '사이버범죄 처벌법'이라는 특별법을 제정하고 그에 따라 여러 법률에 산재되어 있는 사이버범죄 관련 규정들을 한 곳에 집중시키는 것이다. 독일의 경우 처벌과 관련되는 규정들은 대부분 형법에 규정되어 있기 때문에 일반인이 어떤 행위가 처벌되는지를 찾으려면 형법전을 보면 된다. 사이버범죄와 관련해서 새로운 처벌규정이 필요한 경우 형법전을 개정하면 되는데, 예컨대 독일의 경우 제41차 형법 개정안을 통해 정보의 기밀성, 무결성, 사용가능성의 정보보호원칙을 고려하여 데이터의 탐지, 데이터 가로채기, 컴퓨터 사보타주 그리고 데이터 탐지와 가로채기의 예비죄 규정을 형법에 도입하였다.[216] 반면 우리나라의 경우 그와 유사한 규정들이 정보통신망법 등 특별법과 형법에 산재하여 규정되어 있다.

216) 이에 대해서 상세히는 이원상, "해킹의 전단계 범죄화와 일상영역화", 안암법학 제28호, 2009, 295면 이하; Eric Hilgendorf/Brian Valerius, Computer- und Internetstrafrecht, 2. Aufl., 2012, 169면 이하.

이와 같이 사이버범죄 관련 처벌규정을 '사이버범죄 처벌법'으로 단일화시킬 경우 일반인들이 사이버범죄에 해당하는 행위가 어떤 행위인지를 쉽게 찾아볼 수 있기 때문에 사이버범죄에 대한 일반예방적 기능을 향상시킬 수 있을 뿐 아니라 새롭게 범죄화시킬 필요성이 생긴 사이버범죄를 입법화하는데 있어서도 지금과 같이 여러 법률들을 손댈 필요 없이 오직 사이버범죄 처벌법만 개정하면 될 것이다.

다만, 이는 형법 개정이 헌법 개정만큼이나 쉽지 않은 우리나라의 입법실무에 대한 궁여지책의 성격을 가지고 있다. 앞에서 언급한 바와 같이 지금과 같이 사이버공간과 현실공간이 융합되어 있는 정보화 사회에서는 형법이 더 이상 현실공간에만 안주할 필요가 없고, 사이버공간에 대한 보다 많은 규정을 둘 필요가 있다. 그럼에도 불구하고 우리 형법에는 여전히 1995년 개정 때 도입된 일부 컴퓨터범죄와 관련된 규정들만이 존재하고 있다. 그러므로 형법 개정이 좀 더 유연화될 수 있다면 사이버범죄 처벌에 대한 규정도 '사이버범죄 처벌법'이라는 특별법을 따로 제정하는 것보다는 형법에 모아두는 편이 보다 바람직할 것이다. 그러나 지금과 같이 형법의 개정이 용이하지 않은 현실이 계속된다면 '사이버범죄 처벌법'이라는 특별법 제정을 통해서라도 사이버범죄 관련 처벌규정들 한 곳에 모을 필요가 있다.

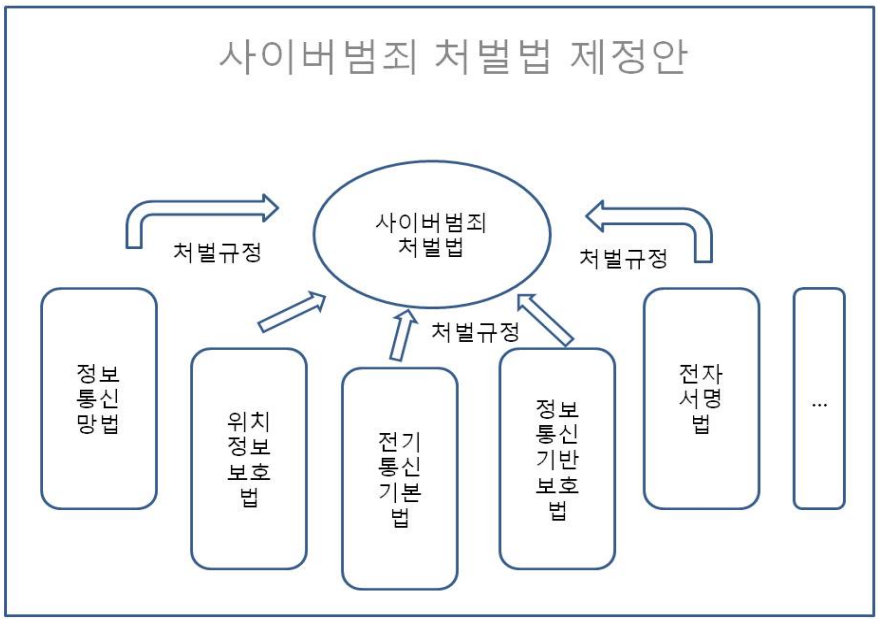


그림 7 사이버범죄 처벌법 제정안

제2절 사이버범죄 관련 기본법의 제정안

1. 기본법체계의 확립

사이버범죄 관련 법령정비의 방안으로 고려해 볼 수 있는 또 다른 대안은 사이버범죄 기본법체계를 확립하는 것이다. 여기서는 사이버범죄 기본법체계를 확립하는 것이라고 했지만, 사실 이는 허울뿐인 기본법체계 전체를 확립하는 것과도 관련이 있다. 인터넷을 검색해 보면 우리나라는 시행령과 시행규칙을 제외하고 '기본법'이라는 명칭을 달고 있는 57개의 기본법이 발견된다.[217] 그런데 앞에서 살펴본 바와 같이 우리나라의 기본법은 법률 이상의 어떠한 기능도 없다. 법

217) http://www.law.go.kr/lsSc.do?menuId=0&p1=&subMenu=1&nwYn=1&query=%EA%B8%B0%EB%B3%B8%EB%B2%95&x=0&y=0#AJAX.

률체계상 기본법이 헌법과 일반적인 법률의 중간에 위치할 수 있는 그 어떤 규정도 존재하지 않고 있기 때문이다. 그러므로 기본법이 실질적으로 일반법의 기본법으로서의 역할을 수행할 수 있으려면 일본과 같이 입법부가 기본법에 실질적인 효력을 부여하는 방법 밖에는 없을 것이다. 그렇지 않으면 기본법 이후에 제정되는 일반적인 법률의 효력이 기본법에 우선할 수 있기 때문에 기본법은 단지 이름만 기본법인 명칭사기의 대상이 될 수 있기 때문이다. 그러므로 기본법이 기본법으로서 자리매김하기 위해서는 입법과정에서 입법자의 배려가 필요할 것이다.

2. 사이버범죄 기본법 제정

사이버범죄 기본법의 모델은 '유럽 사이버범죄 방지협정'이라고 할 수 있다. 유럽 사이버범죄 방지협정을 보면 협정에 규정되어 있는 내용들을 가입국들이 이행입법을 하도록 되어 있다. 그러므로 가입국들은 협정의 내용을 참조하여 자국내 관련 법률을 개정하게 된다. 따라서 협정에는 사이버범죄와 관련한 실체법 규정뿐만 아니라 절차법 규정, 형사사법공조 등과 같이 사이버범죄와 관련된 주요 내용들이 규정되어 있다. 그러므로 우리나라도 이런 메커니즘을 도입하여 다양한 사이버범죄 관련 규정이 정합적으로 운용될 수 있도록 해야 할 것이다.

사이버범죄와 관련해서 우리 입법의 가장 큰 문제점은 문제가 생길 때마다 단순히 정보통신망법이나 개인정보보호법 등과 같은 해당 법률만을 개정하는데 그치기 때문에 다른 유관 법령과의 관계에서 문제점이 발생하게 되는 것이다. 그에 대한 가장 대표적인 예가 바로 개인정보보호법이라고 할 수 있다. 개인정보보호법이 제정되면서 개인정보보호법이 다른 법령들에 존재하고 있는 개인정보보호 관련 규정의 일반법적인 역할을 수행하게 되었다. 따라서 적어도 다른 법령의 개인정보보호 규정들은 개인정보보호법과 보조를 맞추어야 한다. 그런데 일부 규정에는 개인정보보호에 관한 주의적 규정만 있고 처벌규정이 존재하지 않으며, 일부 규정에서는 개인정보침해에 대해 단순히 시정조치만을 규정하고 있다. 그리고 다른 규정에서는 개인정보침해를 반의사불벌죄로 규정하고 있으

며, 다른 일부 규정에서는 개인정보의 특수성을 반영하지 않은 채 개인정보를 전체적인 비밀보호의무와 함께 보호되도록 규정되어 있다.[218] 이처럼 개인정보보호법에서는 강력하게 보호되고 있는 개인정보가 다른 법률에서는 그 보호정도가 다르게 규정되어 있는 것이다. 또한 개인정보침해에 따른 책임에 있어서도 규정들은 여전히 천차만별이다. 여러 법률 규정에서는 개인정보침해가 있는 경우 형벌이나 과태료를 부과하도록 하고 있는데, 그 내용이 천차만별이다. 물론 처벌 규정이 없다고 하더라도 개인정보보호법이 마련되어 있기 때문에 처벌의 흠결은 어느 정도 해소될 수 있지만, 개인정보침해라는 동일한 행위가 법에 따라 다른 책임이 부과되는 것은 문제라고 할 수 있다.[219] 따라서 처벌 규정을 도입함에 있어서는 반드시 형법 전문가가 참여할 필요가 있다고 여겨진다.

그러나 가장 눈에 띄는 것은 개인정보보호법이 제정되어 정보통신망법에서 개인정보보호와 관련된 여러 규정들이 삭제되었음에도 불구하고 일부 규정에서는 개인정보관련 규정을 참조하고 있다. 즉, 개인정보보호법 제정으로 인해 정보통신망법의 제33조~제40조가 삭제되었음에도 동법 제44조의10 제3항에서는 여전히 제33조의2 제2항, 제35조~제39조까지를 준용한다는 규정이 존치하고 있다.[220] 이는 명백한 입법오류라고 할 수 있다.

표 4 정보통신망법 VS 개인정보보호법[221]

정보통신망법		개인정보보호법	
금지행위 유형	처벌 내용	금지행위 유형	처벌 내용
▸이용자의 동의를 받지 아니하고 개인정보를 수집한 자	▹5년 이하의 징역 또는 5천만원 이하의 벌금	▸정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자	▹5년 이하의 징역 또는 5천만원 이하의 벌금

218) 이원상/이성식, 앞의 책, 168면.

219) 위와 동일.

220) 이원상/안정민, 방송통신융합에 따른 처벌법규 정비방안 연구, 한국형사정책연구원, 2011, 110면 각주 54.

221) 이원상/안정민, 방송통신융합에 따른 처벌법규 정비방안 연구, 한국형사정책연구원, 2011, 112면.

<table>
<tr><th colspan="2">정보통신망법</th><th colspan="2">개인정보보호법</th></tr>
<tr><th>금지행위 유형</th><th>처벌 내용</th><th>금지행위 유형</th><th>처벌 내용</th></tr>
<tr><td>▸이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자</td><td rowspan="8"></td><td>▸개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자</td><td rowspan="8"></td></tr>
<tr><td>▸개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자</td><td>▸민감정보를 처리한 자</td></tr>
<tr><td>▸이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 자</td><td>▸고유식별정보를 처리한 자</td></tr>
<tr><td>▸이용자의 개인정보를 훼손·침해 또는 누설한 자</td><td>▸업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자</td></tr>
<tr><td>▸그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자</td><td rowspan="4">▸다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자</td></tr>
<tr><td>▸필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자</td></tr>
<tr><td>▸법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자</td></tr>
<tr><td>▸속이는 행위로 다른 사람의 개인정보를 수집한 자</td><td>▹3년 이하의 징역 또는 3천만원 이하의 벌금</td><td>▸거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자</td><td>▹3년 이하의 징역 또는 3천만원 이하의 벌금</td></tr>
<tr><td rowspan="3">▸기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자</td><td rowspan="3">▹2년 이하의 징역 또는 1천만원 이하의 벌금</td><td>▸안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자</td><td rowspan="3">▹2년 이하의 징역 또는 1천만원 이하의 벌금</td></tr>
<tr><td>▸정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자</td></tr>
<tr><td>▸개인정보의 처리를 정지하지 아니하고 계속 이용하거</td></tr>
</table>

정보통신망법		개인정보보호법	
금지행위 유형	처벌 내용	금지행위 유형	처벌 내용
		나 제3자에게 제공한 자	

개인정보보호법의 예에서 볼 수 있는 것과 같이 사이버범죄 관련 법령의 제·개정으로 인해 다른 유관 법령들은 영향을 받게 된다. 그런데 앞에서 언급한 바와 같이 우리의 입법 실무는 그런 부분들을 충분히 고려하고 있지 못하다. 예를 들어, 독일의 경우에는 'Artikelgesetz'가 존재한다. 이는 관련된 여러 법률들을 동시에 개정하는 입법방식이다.[222] 따라서 앞에서 예를 든 바와 같이 일부 법령은 개정되지만, 일부는 개정되지 않아 문제가 발생하게 될 가능성이 거의 없다. 따라서 우리나라에서는 독일의 Artikelgesetz와 같은 입법방식이 존재하지 않으므로 ―비록 형식적으로 존재하고 있지만― 기본법체계를 통해 문제를 해결할 수 있다고 생각된다.

이른바 '사이버범죄 기본법'은 유럽 사이버범죄 방지협정과 같이 사이버범죄와 관련된 중요 내용들인 법원칙, 주요 정의, 일반적인 범죄유형, 전자증거, 디지털 포렌식, 국제사법공조 등의 내용들을 담을 필요가 있다. 그리고 사이버범죄를 규정하고 있는 다른 규정들은 사이버범죄 기본법의 내용을 참조하도록 하는 것이다. 예를 들어 사이버공간에서의 비밀침해에 대해 사이버범죄 기본법이 정의를 규정하면, 관련 법률들이 해당 규정을 참조하는 것이다. 또한 이후에 제정되는 유사 법령들은 사이버범죄와 관련된 내용을 규정할 때 사이버범죄 기본법의 내용을 반영하도록 하는 것이다. 이로 인해 사이버범죄의 역동성과 발전성으로 인해 추후 해당 내용에 변화가 필요하여 개정되는 경우에도 다른 법률의 제·개정 없이 사이버범죄 기본법의 개정만으로 바로 다른 법률에서 적용이 가능하게 되는 것이다. 사이버범죄와 같이 기술적으로나 방법적으로 매우 빠르게 진화하는 범죄의 경우 매우 요긴한 입법방식이라고 할 수 있을 것이다.

222) http://www.bundestag.de/service/glossar/A/artikelgesetz.html.

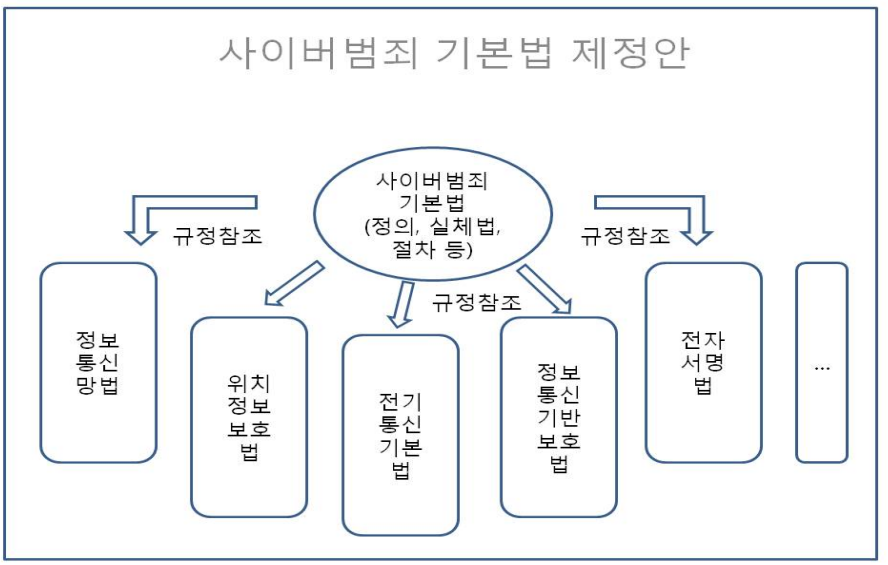


그림 8 사이버범죄 기본법 제정안

이와 유사한 방법으로 현재 정보통신망법이 사이버범죄의 기본법적 역할을 하는 것을 그대로 이용하는 방법이 있다. 다만 그 경우에도 정보통신망법은 다소 개정될 필요가 있는데, 이는 정보통신망법이 제정될 당시부터 그 목적에 다소 제한이 있기 때문이다. 정보통신망법에 따르면 동 법률의 목적은 "이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함"이라고 하고 있다. 따라서 법률의 목적범위를 사이버범죄를 수용할 수 있도록 다소 넓히고, 명실공히 사이버범죄의 기본법이 될 수 있도록 다소 광범위한 개정을 할 필요성이 있다.

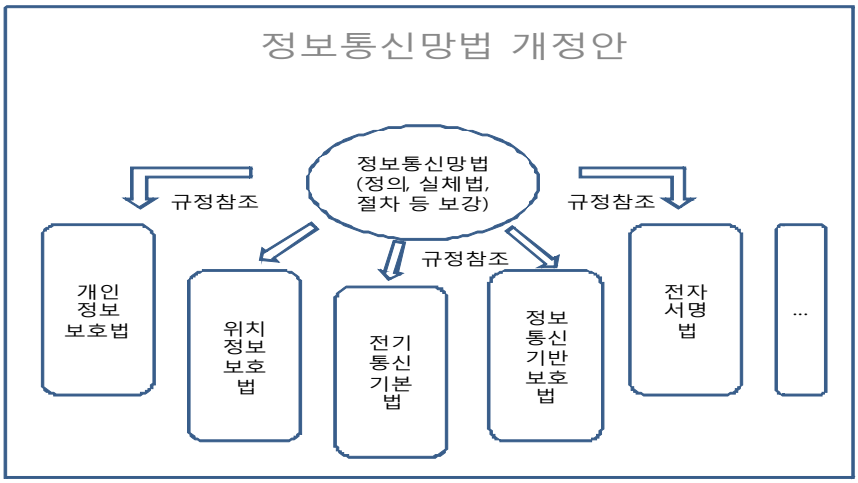


그림 9 정보통신망법 개정안

제3절 현행 관련 법령의 재정비

마지막으로 사이버범죄 관련 법령정비에 있어서 고려할 수 있는 방법으로 현행 체계를 유지하되 주요 문제점들을 도출하여 그에 따라 관련 법령들을 모두 개정하는 것이다. 이에 대해서는 이미 2011년 한국형사정책연구원의 연구보고서인 "방송통신융합에 따른 처벌법규 정비방안 연구" 일부분에 자세히 소개되어 있다. 그에 따르면 일단 현행 관련 법령을 정비하기 위해 크게 용어 통일, 일반조항 문제 해결, 공무원의제 규정의 개선, 자유형과 벌금형 규정들의 균형성 확보, 형벌과 행정벌의 구분, 일반적인 형벌규정은 형법으로 이전 등이 해결되어야 할 것으로 보고 있다.[223]

첫째로, 법률용어의 통일이 중요하다. 가장 대표적인 예가 '허위'라는 용어라고 할 수 있다. 형법적으로 '진실에 합치되지 않는 것'을 의미하는 허위라는 개념은 법률에 따라서 '거짓'이나 '속임수'라는 용어로 사용되고 있다. 그러나 법제처가 내놓은 "알기 쉬운 법령정비기준"에서는 '거짓'이라는 용어로 대체될 필요

223) 이원상/안정민, 앞의 책, 181면 이하.

성이 있다고 한다. 따라서 '허위'라는 용어를 '거짓'이라는 용어로 통일할 필요가 있다.[224]

둘째로, 가능한 한 일반조항으로의 회피하는 것을 줄여야 할 것이다. 일반조항은 주로 행정법에서 많이 사용되고 있는데, 이는 모든 상황이나 위험을 규정하는 것은 불가능한 일이기 때문에 입법의 공백을 메우기 위한 포괄적인 행정작용의 근거로 사용하고 있는 입법형식이라고 할 수 있다.[225] 그러나 형법에서는 명확성원칙에 반할 수 있기 때문에 일반조항이 금지되고 있다. 물론 사이버범죄의 경우 행위의 변화가 심하고, 기술의 발전도 매우 빠르기 때문에 행정법과 같이 일반조항으로 회피하고자 하는 유혹이 있을 수 있다. 그러나 가능한한 일반조항을 도입하는 것은 최소화 하여야 할 것이며, 부득이하게 일반조항을 도입하는 경우에도 그 내용이나 목적, 범위 등을 제한할 필요성이 있다.[226]

셋째로, 공무원 의제규정을 개선할 필요가 있다. 사이버범죄와 관련해서 많은 처벌규정이 정보통신 등의 업무를 제공하는 서비스제공자들을 처벌함에 있어 공무원으로 의제하고 있다. 그러나 이익에 있어서는 공무원으로서의 이익을 누리지 못하는데도 불구하고 업무의 특성에 의해 일반인을 공무원으로 의제하여 처벌하는 것은 불합리하다고 여겨진다. 따라서 비록 공무원으로 의제하더라도 그 형량에 있어서는 공무원보다 낮게 규정하여 공무원과 공공업무를 수행하는 사인과의 차이를 반영할 필요가 있다.[227]

넷째로, 가장 큰 문제점으로 유사한 행위 유형들에 대해서 자유형이나 벌금형의 형량이 천차만별인 것이다. 특히 특별법 규정들은 형법의 규정보다 대부분 형량이 높다.[228] 따라서 여기서는 크게 두 가지 문제점이 제기될 수 있다. 하나는 행위자는 자신의 행위에 어느 법률이 적용되는지에 따라 다른 형량이 부과될 수 있기 때문에 매우 불안한 지위에 서게 된다. 그리고 다른 하나는 형벌규정에서 체계화되어 있는 양형기준은 특별법에는 무용지물이 되어 특별법범이 형법범

224) 이원상/안정민, 방송통신융합에 따른 처벌법규 정비방안 연구, 한국형사정책연구원, 2011, 182-183면.

225) 이원상/안정민, 앞의 책, 184면.

226) 이원상/안정민, 앞의 책, 185면.

227) 이원상/안정민, 앞의 책, 189면.

228) 이원상/안정민, 앞의 책, 190면 이하 비교표 참조.

보다 많은 상황에서 형법의 양형체계는 반쪽자리로 될 수밖에 없게 된다. 그러므로 이런 불합리함이 해소되기 위해서는 특별법에서 형량을 정함에 있어 형법학자가 반드시 참여해야 할 필요성이 있다.

다섯째로, 형벌과 행정벌의 기준을 보다 명확히 할 필요성이 있다. 행정벌의 목적은 행정의 실효성을 확보하기 위한 것인데 반하여 형벌은 생명이나 신체, 명예 등 보호법익을 침해하는 범죄행위에 대해 국가가 사용할 수 있는 가장 강력한 수단을 사용하는 것이다.[229] 그런데 사이버범죄 관련 규정, 예를 들어 정보통신망법을 보게 되면 행정벌과 형벌의 구분기준이 모호하다. 동법 제74조 제1항 제7호에서는 등록사항의 변경등록 또는 사업이 양도·양수 또는 합병·상속의 신고를 하지 않은 경우 1년 이하의 징역이나 1천만 원 이하의 벌금에 처하도록 규정하고 있다. 그런데 제76조 제1항 제3호에서는 개인정보 보호를 위한 기술적·관리적 조치를 취하지 않은 경우에는 오히려 3천만원 이하의 과태료만이 부과 될 뿐이다. 전자는 오히려 과태료 대상이 될 수 있으며, 후자에게 형벌이 부과될 수도 있다. 따라서 가능한 한 행정적인 문제는 행정벌인 과태료 등으로 해결하고, 형법이론에 따라 보호법익을 침해하는 행위를 구분하여 형사처벌 해야 할 것이다. 이를 위해서도 형벌관련 규정을 입법함에 있어서는 형법전문가가 참여할 필요성이 있다.

여섯째로, 일반적인 처벌규정으로 규율해야 할 행위들은 과감히 형법으로 이전할 필요가 있다. 가장 대표적인 규정이 정보통신망법 제70조의 사이버 명예훼손죄와 아동·청소년의 성보호에 관한 법률 제11조에 규정되어 있는 아동·청소년이용 음란물의 제작·배포 등에 관한 규정이다. 비교법적으로 볼 때에도 많은 나라들이 해당 규정과 유사한 규정을 형법에 두고 있다. 예를 들어, 독일의 경우 해당 규정들이 모두 형법에 규정되어 있다. 해당 규정들은 특별법에 규정되어 일부 사람들에게 적용되는 것이 아니라 일반인들 모두에게 적용될 수 있기 때문에 형법에 규정되는 것이 적절할 것이다. 그로 인해 일반예방기능도 보다 향상될 것이다. 따라서 일반적인 행위에 속하는 사이버범죄 관련 규정들은 가능한 한 형법에 규정할 필요가 있다.

229) 이원상/안정민, 앞의 책, 196면.

참고문헌

[국내문헌]

김도경, “위치정보보호법의 제정에 따른 LBS산업의 규제정책 방향”, 정보통신정책 제15권 19호, 2003.

김상겸, “독일의 의료정보와 개인정보보호에 관한 연구”, 한·독사회과학논총 제15권 제2호, 2005년 겨울호.

김연태, “정보의 자기결정권과 경찰의 정보관리”, 고려법학, 2001.

김일수·서보학, 형법각론, 새로쓴 7판, 2007.

김철수, 헌법학(상), 2008.

_____, 헌법학신론, 제20전정신판, 2010.

김혜경, “전기통신기본법상 형사처벌규정의 검토”, 연세대학교 법학연구, 2008.

다니엘 솔로브(이승훈 옮김), 인터넷 세상과 평판의 미래, 2007.

데이비드 월(정태진 옮김), 사이버범죄, 2013.

로렌스 레식(김정오 옮김), 코드2.0, 2009.

문제인, “일인 미디어 시대의 액세스(access)권”, 언론과 법 제9권 제2호, 2010.

민윤영, “인터넷 상에서 잊혀질 권리와 「개인정보보호법」에 대한 비교법적 고찰”, 고려법학 제63호, 2001.

박상기, 형법각론, 제7판, 2008.

박영도, 입법학입문, 한국법제연구원, 2008.

변재호·조은진, “망중립성 논의 최근 전개 동향”, 전자통신동향분석 제25권 제4호, ETRI, 2010. 8.

배종대, 형사정책(제8판), 홍문사, 2011.

_____, 형법각론, 제7전정판, 2011.

백광훈, “사이버범죄의 개념과 용어의 문제”, 형사정책연구소식(통권 제68호), 2001.

심우민, “최근 전산망 마비사태와 사이버 테러 대응체계 개선방안”, 국회입법조사처 이슈와 논점 제160호, 2013.

_____, “개인정보 보호법 시행과 당면과제”, 이슈와 논점 제308호, 국회입법조사처, 2011.

양재모, 정보통신망법의 발전적 분화와 새로운 통합, 정보통신연구진흥원 학술정보 - 인터넷이슈리포트 2007권 10호, 2007.

울리히 지버, 전세계적 위험사회에서 복합적 범죄성과 형법, 한국형사정책연구원, 2011.

이동훈, “유비쿼터스사회에서의 액세스권과 알권리 해석론”, 공법학연구 제10권 제2호, 2008.

이상돈, 전문법 - 이성의 지역화된 실현, 고려법학 제39호, 2002.

이어령, 디지로그, 2006.

이영준・정완・금봉수, 사이버범죄방지조약에 관한 연구, 한국형사정책연구원, 2001.

이원상・이성식, 클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구, 한국형사정책연구원, 2012.

이원상・안정민, 방송통신융합에 따른 처벌법규 정비방안 연구, 한국형사정책연구원, 2011.

이원상・탁희성・송봉규, 디지털 포렌식 역량강화방안, 2012년 경찰청 연구용역 보고서.

이원상, “‘사이버’개념을 통한 사이버 모욕죄의 고찰과 대안”, 형사정책 제20권 제2호, 2008.

_____, “정보화 사회와 형법”, 비교형사법연구 제12권 제2호, 2010.

_____, “해킹의 전단계 범죄화와 일상영역화”, 안암법학 제28호, 2009.

_____, 온라인 수색(Online-Durchsuchung)에 대한 고찰 -독일의 새로운 논의를 중심으로, 형사법연구 제20권 제4호, 2008년 겨울호.

_____, “허위사실에 의한 명예훼손죄의 딜레마”, 2013년 형사판례연구 발제문.

_____, 형사사법에 있어 개인위치정보에 대한 고찰: 긴급구조 및 수사를 중심으로, 형사정책연구 제23권 제2호, 2012 여름호.

_____, 사이버범죄에 있어서 형법의 역할과 시스템적 대처방안, 고려대학교 석사학위논문, 2003.

_____, Die Verhältnismäßigkeit im Cyberstrafrecht, 박사학위논문, 2010.

이재상, 형법각론, 제9판, 2012.

이정훈, "입법체계상 기본법의 본질에 관한 연구", 법조 2009. 12.

전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010.

조병인·정진수·정완·탁희성, 사이버범죄에 관한 연구, 2000년 법무부 용역과제, 한국형사정책연구원, 2000.

조병인, "하이테크범죄의 실태와 대책", 한국공안행정학회 국제범죄 학술세미나 발표논문, 1999.

주승희, "현행 사이버 명예훼손죄 법리의 문제점 및 개선방안 관련 최근 논의 검토", 형사정책연구 제77호, 2009.

차성민, "ICT정부조직 비교연구", 한국비교정부학보 제16권 제3호, 2012.

최승재, "경쟁법의 관점에서 본 망중립성에 대한 연구", 언론과 법 제10권 제2호, 2011.

최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책원구원, 1998.

최정호, "사이버테러리즘의 변천방향과 한국의 대응", 2008 국방안보학술회의, 2008.

피에르 레비(김동윤/조준형 옮김), 사이버 문화, 2000.

한국정보통신산업협회, 정보통신기반보호법(안), 한국정보통신산업협회, 정보화사회 142, 2000.

허진성, "헌법적 쟁점으로서의 망중립성", 언론과 법 제10권 제2호, 2011.

형사입법연구회, 2011년도 형법·형사소송법 및 형사특별법 제·개정안 분석과 입법정책 개선방안, 한국형사정책연구원, 2011.

홍승희, "정보통신범죄의 전망", 형사정책 제19권 제1호, 2007.

황승흠, "기본법체제에 대한 법학적 이해", 공법학연구 제11권 제1호, 2010.

[외국문헌]

Eric Hilgendorf/Brian Valerius, Computer- und Internetstrafrecht, 2. Aufl., 2012.

Hofmann, Die Online-Durchsuchung - staatliches "Hacken" oder zulässige Ermittlungsmaβnahme?, NStZ 2005, Heft 3.

J. A. Barron, "Access to the press-A New First Amendment Right", 80Harvard Law Review, 1967.

Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambrige University Press, 2013.

Mike Godwin, Cyber Rights, 1998.

Norber Wiener, Cybernetics or control and communication in the animal and the machine, 제2판, 1965.

Willian Gibson, 『Neuromancer』, An Ace Book, 1984.

Werner Beulke, Strafprozessrecht, 제9판, 2006.

Abstract

A Study on Revisions of Laws and Regulations of Cyber Crimes

LEE, Won-Sang · KANG, Seok Ku

The purpose of the study was to effectively regulate regulations out of prevention effects and equity of many laws of cyber crime. The study investigated understanding upon cyber crime, principles of legislation of regulations of the crime, regulations of the crime and revisions of laws and regulations of the crime that investigated current legal system. The revision of cyber crime did not gather existing legal provisions but enacted laws and regulations systematically in matching way in accordance with principle of cyber space as well as concept of cyber crime.

Chapter 1 investigated cyber space, culture and crime to understand the crime and have base. Chapter 2 investigated principles of revision of laws and regulations of the crime to find out rights to respect at cyber space, principles, behavior regulating factors and principles of legal systems for revision of the crime. Chapter 3 described organizations and laws and regulations of the crime and recent discussions of the fundamental law to find out contents of legal system of the crime and trend of new laws and regulations. Chapter 4 suggested revision of laws and regulations of the crime to legislate and to revise current laws and regulations, that is to say, the law on punishment of cyber crime, fundamental law on cyber crime, and the law

on promotion of use of information and communication network.

In the nation, cyber crime regulations were adopted at many areas here and there, and revision of "the Act on Promotion of Use of Information and Communication Network and Protection of Information" regulated behaviors of cyber crimes. Disorder of regulating system of the cyber crime having no principle could not exercise legal force. So, legal system of the crime should be made to take actions against the crime.

부록

〈부록 1〉 국가 사이버테러 방지에 관한 법률안

제1장 총칙

제1조(목적) 이 법은 국가 사이버테러 방지에 관한 기본적인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버 위기 발생 시 국가 역량을 결집하여 신속하게 대처함으로써 국가의 안전보장과 이익보호에 이바지함을 목적으로 한다.

제2조(정의) ① 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "사이버테러"란 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신시설을 침입·교란·마비·파괴하거나 정보를 절취·훼손·왜곡전파 하는 등 모든 공격행위를 말한다.
2. "사이버안전"이란 사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함한다.
3. "사이버위기"란 사이버테러로 인하여 국가·사회기능에 심각한 지장을 초래하거나 피해가 전국적으로 확산될 가능성이 있는 경우를 말한다.
4. "사이버테러정보"란 정보시스템 및 정보보호시스템(소프트웨어를 포함한다) 등에 의해 사이버테러 행위로 판단되는 정보로서 사이버테러 근원지를 파악하기 위한 인터넷프로토콜주소(IP)와 네트워크카드주소(MAC)를 포함한다.
5. "사이버위기경보"란 사이버테러 징후를 식별하거나 사이버위기 발생이 예상되는 경우 그 위험 또는 위협수준에 부합되는 조치를 할 수 있도록 미리 정보를 제공하고 경고하는 것을 말한다.

6. “사이버위기관리”란 사이버위기를 예방하고 사이버위기가 발생하였을 경우 신속하고 체계적으로 대응하기 위한 사이버테러 탐지·대응, 사고의 조사·복구, 모의훈련, 경보발령 및 관계기관 간의 협조 등 국가차원의 모든 활동을 말한다.
7. “사이버테러 방지 및 위기관리 책임기관(이하 “책임기관”이라 한다)”이란 사이버테러 방지 및 위기관리에 관한 업무를 수행하고 있는 다음 각 목의 기관을 말한다.
   가. 「대한민국헌법」, 「정부조직법」, 그 밖의 법령에 따라 설치된 국가기관과 지방자치단체 및 「국가정보화 기본법」 제3조제10호에 따른 공공기관
   나. 「정보통신기반 보호법」 제5조제1항에 따른 주요정보통신기반시설을 관리하는 기관
   다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설사업자 및 같은 법 제47조의4제2항에 따른 주요정보통신서비스 제공자
   라. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관
   마. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 법 제3조제10호에 따른 전문연구기관
8. “사이버테러 방지 및 위기관리 지원기관(이하 “지원기관”이라 한다)”이란 사이버테러에 대한 신속한 탐지·대응 및 사고조사·복구 등을 지원하는 다음 각 목의 기관 또는 업체를 말한다.
   가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원 부설연구소
   나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원
   다. 「소프트웨어산업 진흥법」 제24조에 따라 소프트웨어사업자로 신고한 자 중 컴퓨터바이러스 백신소프트웨어를 제작 또는 판매하는 자
   라. 「국가정보화 기본법」 제3조제6호의 정보보호시스템을 제작하거나 수입하는자

마. 「정보통신기반 보호법」 제9조에 따라 지정된 지식정보보안 컨설팅전문업체

바. 관계 행정기관의 장이 지정한 보안관제전문업체

② 이 법에서 사용하는 용어의 정의는 제1항에서 정하는 것을 제외하고는 「정보통신기반 보호법」·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」·「국가정보화 기본법」·「전기통신사업법」에서 정하는 바에 따른다.

제3조(다른 법률과의 관계) 사이버테러 방지 및 위기관리에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. 다만, 사이버위기가 발생할 경우에는 다른 법률에 우선하여 적용한다.

제4조(책임기관의 책무) 책임기관의 장은 사이버테러를 사전 예방하기 위하여 소관 정보통신시설의 안전을 유지할 책임이 있으며, 이를 위하여 사이버테러 방지 및 위기관리 업무를 전담하는 전문인력 및 예산 확보 등의 필요한 조치를 강구하여야 한다.

제5조(민·관 협력) ① 정부는 사이버테러 방지 및 대응에 협력하고 사이버위기를 효율적으로 관리하기 위하여 대통령령으로 정하는 바에 따라 민간기관 등과 협의체를 구성·운영할 수 있다.

② 제1항에 관하여 필요한 사항 등은 대통령령으로 정한다.

제2장 국가 사이버테러 방지 및 위기관리 추진체계

제6조(국가사이버안전전략회의) ① 국가사이버테러 방지 및 위기관리에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다.

② 전략회의의 의장은 국가정보원장이 된다.

③ 전략회의의 위원은 중앙행정기관의 차관급 공무원과 전략회의 의장이 위촉하는 자로 한다.

④ 전략회의는 다음 각 호의 사항을 심의한다.

1. 사이버테러 방지 및 위기관리 관련 전략·정책·제도 수립 및 개선

2. 사이버테러 방지 및 위기관리 관련 기관간 역할조정에 관한 사항
3. 제12조제2항에 따른 사이버위협정보 공유 및 보호에 관한 사항
4. 사이버테러 방지 및 위기관리 관련 대통령 지시사항에 대한 조치방안
5. 그 밖에 전략회의 의장이 부의하거나 위원이 제출한 사항

⑤ 전략회의의 효율적 운영을 위하여 전략회의에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 둘 수 있다.

⑥ 전략회의 및 대책회의의 구성·운영 등에 관하여 필요한 구체적인 사항은 대통령령으로 정한다.

제7조(국가사이버테러 방지 및 위기관리 기본계획 수립 등) ① 정부는 사이버테러 방지 및 위기관리 대책의 효율적·체계적 추진을 위하여 국가사이버테러 방지 및 위기관리 기본계획(이하 "기본계획"이라한다)을 수립·시행하여야 한다.

② 기본계획은 대통령령으로 정하는 바에 따라 국가정보원장이 관계 중앙행정기관의 장과 협의하여 전략회의 심의를 거쳐 마련한다.

③ 중앙행정기관의 장은 제1항의 기본계획에 따라 소관 책임기관의 장이 활용할 수 있도록 국가사이버테러 방지 및 위기관리 시행계획(이하 "시행계획"이라고 한다)을 작성하여 소관 책임기관의 장에게 배포하여야 한다.

제8조(시행계획의 이행여부 확인 및 국회 보고) ① 중앙행정기관의 장은 소관 책임기관에 대하여 매년 시행계획의 이행여부를 확인하여야 한다.

② 국가정보원장은 제1항의 확인결과를 종합하여 국가사이버테러 방지 및 위기관리 실태를 점검·평가하고 그 결과를 국회에 보고하여야 한다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회에 대한 점검·평가는 국회 사무총장, 법원행정처장, 헌법재판소 사무처장 및 중앙선거관리위원회 사무총장이 요청한 경우에 한한다.

③ 제1항 및 제2항의 절차와 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제9조(국가사이버안전센터의 설치) ① 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터(이하 "안전센터"라 한다)를 둔다.

② 안전센터는 다음 각 호의 업무를 수행한다.

1. 국가사이버테러 방지 및 위기관리 정책의 수립
2. 전략회의 및 대책회의 운영에 대한 지원
3. 사이버테러 관련 정보의 수집·분석·전파
4. 국가정보통신망의 안전성 확보
5. 국가 사이버테러 방지 및 위기관리 매뉴얼 작성·배포
6. 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원
7. 외국과의 사이버 공격 관련 정보의 협력

③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 민·관·군 합동대응팀(이하 "합동대응팀"이라 한다)을 설치·운영할 수 있다.

④ 국가정보원장은 합동대응팀을 설치·운영하기 위하여 필요한 경우에는 중앙행정기관 및 지원기관의 장에게 인력의 파견과 장비의 지원을 요청할 수 있다.

제3장 사이버테러 방지 및 위기관리 활동

제10조(사이버테러 방지대책의 수립·시행) ① 책임기관의 장은 소관 정보통신망과 정보 등의 안전성 및 신뢰성 확보를 위한 사이버테러 방지대책을 강구하여야 한다.

② 국가정보원장은 제1항에 따른 사이버테러 방지대책의 수립에 필요한 지침을 작성 배포할 수 있다. 이 경우, 국가정보원장은 미리 관계 중앙행정기관의 장과 협의하여야 한다.

③ 제2항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다.

제11조(악성프로그램의 확산 차단) ① 정부는 악성프로그램 등이 포함된 웹사이트 또는 소프트웨어 등을 발견한 경우에 그 운영자에게 악성프로그램의 감염 확산방지 등에 필요한 보안조치를 할 수 있도록 관련 정보를 제공하여야 한다.

② 정부는 제1항의 조치에도 불구하고 사이버테러에 악용되거나 위험성이 높

다고 판단되는 경우에 백신프로그램의 유포 등을 통해 악성프로그램 등을 삭제 또는 차단하게 할 수 있다.

③ 제1항 및 제2항에 따라 필요한 조치의 구체적인 사항은 대통령령으로 정한다.

제12조(보안관제센터 등의 설치) ① 책임기관의 장은 사이버테러 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 구축·운영하거나 다음 각 호의 기관이 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 한다. 다만, 「정보통신기반 보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.

1. 관계 중앙행정기관
2. 국가정보원
3. 제2조제1항제8호바목의 보안관제전문업체

② 책임기관의 장은 제1항에 따른 사이버테러 정보와 정보통신망·소프트웨어의 취약점 등의 정보(이하 "사이버위협정보"라 한다)를 관계 중앙행정기관의 장 및 국가정보원장과 공유하여야 한다.

③ 국가정보원장은 제2항의 사이버위협정보의 효율적인 관리 및 활용을 위하여 관계기관의 장과 공동으로 사이버위협정보통합공유체계를 구축·운영할 수 있다.

④ 누구든지 제2항에 따라 공유하는 정보에 대하여는 사이버위기관리를 위하여 필요한 업무범위에 한하여 정당하게 사용·관리하여야 한다.

⑤ 제1항에 따른 보안관제센터와 제3항에 따른 사이버위협정보통합공유체계 구축·운영 및 정보 관리에 관한 사항과 제2항에 따른 사이버테러 정보의 공유에 관한 범위·절차·방법 등에 관한 사항은 대통령령으로 정한다.

제13조(사고조사) ① 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하고, 피해가 중대하거나 확산될 우려가 있는 경우 즉시 관계 중앙행정기관의 장 및 국가정보원장에게 그 결과를 통보하여야 한다.

② 국가정보원장은 제1항에도 불구하고 국가안보 및 이익에 중대한 영향이 미친다고 판단되는 경우 관계 중앙행정기관의 장과 협의하여 직접 그 사고조사를 실시할 수 있다.

③ 국가정보원장은 제1항에 따라 사고조사 결과를 통보받거나 제2항에 따라 사고조사를 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

제14조(대응훈련) ① 정부는 사이버테러를 방지하고 사이버위기에 체계적이고 효율적으로 대응하기 위하여 훈련을 실시하여야 한다.

② 제1항의 훈련은 매년 정기 또는 수시로 구분하여 실시할 수 있으며, 정기훈련은 「비상대비자원 관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

③ 제1항의 훈련 실시방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제15조(사이버위기경보의 발령) ① 국가정보원장은 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 제12조제2항에 따라 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있다.

② 국가정보원장은 사이버테러가 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 국가안보실의 국가위기상황 업무를 담당하는 수석비서관과 협의하여 심각 수준의 경보를 발령할 수 있으며, 심각단계의 사이버위기경보를 발령한 경우에는 그 사유를 국회에 통보하여야 한다.

③ 국가정보원장은 사이버위기경보를 발령할 경우 관계기관의 장과 경보 수준을 사전 협의하여야 한다.

④ 책임기관의 장은 제1항에 따른 사이버위기경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.

⑤ 사이버위기경보 발령의 절차·기준 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다.

제16조(사이버위기대책본부의 구성) ① 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를

취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기 대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다.

② 대책본부의 장(이하 "대책본부장"이라 한다)은 국가정보원장으로 하며, 대책본부의 구성·운영 등에 관하여 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.

③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다. 이 경우 책임기관 및 지원기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 대책본부장은 제3항에 따라 인력의 파견 및 장비의 제공을 한 기관의 장에게 그 소요경비를 지원할 수 있다.

제17조(기술지원) ① 책임기관의 장이 제12조제1항 및 제15조제4항의 업무를 수행함에 있어 필요한 경우 관계 중앙행정기관의 장 및 국가정보원장에게 지원을 요청할 수 있다.

② 관계 중앙행정기관의 장 및 국가정보원장은 제1항에 따른 지원을 요청받았을 때 신속한 대응이 이루어질 수 있도록 기술지원 등 필요한 조치를 하여야 한다.

③ 제2항에 따른 조치를 위하여 관계 중앙행정기관의 장 및 국가정보원장은 해당 지원기관의 장에게 필요한 지원을 요청할 수 있으며, 이 경우, 지원기관의 장에게 지원할 내용과 기간을 미리 통보하여야 한다.

④ 관계 중앙행정기관의 장 및 국가정보원장은 제3항에 따라 지원을 한 기관의 장에게 그 소요경비를 지원할 수 있다.

제4장 연구개발 및 지원 등

제18조(책임기관에 대한 지원) 정부는 책임기관에 대하여 정보통신망을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 및 그 밖의 필요한 지원을 할 수 있다.

제19조(연구개발) ① 정부는 사이버테러 방지 및 위기관리에 필요한 기술개발과

기술수준의 향상을 위하여 다음 각 호의 시책을 추진할 수 있다.

1. 사이버테러 방지 및 위기관리에 관한 국가 연구개발 계획의 수립·시행
2. 사이버테러 방지 및 위기관리기술 수요조사 및 동향분석 등에 관한 사업
3. 사이버테러 방지 및 위기관리에 관한 기술의 개발·보급·확산 사업
4. 그 밖에 사이버테러 방지 및 위기관리 관련 기술개발 및 기술향상 등에 관하여 필요한 사항

② 국가정보원장은 제1항에 따라 연구소를 설립하거나, 다른 법령에 의하여 설립된 기관을 전문기관으로 지정할 수 있다.

③ 국가 사이버테러 방지 및 위기관리 기술의 연구개발에 관한 절차·방법 등 세부사항은 국가정보원장이 따로 정한다.

제20조(산업육성) ① 정부는 사이버테러 방지 및 위기관리에 필요한 산업의 육성을 지원하기 위하여 다음 각 호의 시책을 수립·시행하고 이에 필요한 재원 확보 방안 등을 마련하여야 한다.

1. 사이버테러 방지 및 위기관리 산업 정책수립 지원
2. 사이버테러 방지 및 위기관리 산업 발전을 위한 유통시장 활성화 지원
3. 사이버테러 방지 및 위기관리 산업 육성을 위한 산·학·연 협력체계 구축
4. 사이버테러 방지 및 위기관리 산업 관련 국제교류·협력 및 해외진출의 지원

② 정부는 제19조제2항의 연구소 및 전문기관으로 하여금 제1항의 산업육성에 필요한 업무를 수행하게 할 수 있다.

제21조(인력양성 및 교육홍보) 정부는 사이버테러 방지 및 위기관리의 기반을 조성하고 사이버위기에 대한 국민의 인식을 제고하기 위하여 다음 각 호의 시책을 강구하여야 한다.

1. 사이버테러 방지 및 위기관리 관련 전문인력의 양성
2. 사이버테러 방지 및 위기관리에 관한 대국민 홍보활동 및 교육
3. 그 밖에 사이버테러 방지 및 위기관리 관련 전문인력 양성 및 교육홍보 등에 관하여 필요한 사항

제22조(국제협력) 정부는 사이버테러 방지 및 위기관리에 관하여 국제기구·단체 및 외국과의 협력을 증진하기 위하여 다음 각 호의 업무를 수행할 수 있다.

1. 사이버테러 방지 및 위기관리를 위한 상호간 협력체계 구축

2. 사이버테러 방지 및 위기관리 기술에 관한 정보의 교류와 공동대응
3. 사이버테러 방지 및 위기관리 전담인력의 상호간 파견교육

제23조(비밀 엄수의 의무) 이 법에 따라 사이버테러 방지 및 위기관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제24조(포상 등) ① 국가정보원장은 사이버테러 방지 및 위기관리와 관련하여 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.

1. 사이버테러 기도에 관한 정보를 제공한 자
2. 사이버테러를 가한 자를 신고한 자
3. 사이버테러의 탐지 및 대응·복구에 공이 많은 자

② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 구체적인 지급액 등 필요한 사항은 국가정보원장이 정한다.

제5장 벌칙

제25조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제12조제2항 및 제12조제4항을 위반한 자
2. 제13조제4항을 위반한 자
3. 제23조를 위반한 자

② 업무상 과실로 인하여 제1항의 죄를 범한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

제26조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자는 2천만원 이하의 과태료에 처한다.

1. 제13조제1항을 위반한 자
2. 제16조제3항을 위반한 자

② 제13조제3항을 위반한 자는 1천만원 이하의 과태료에 처한다.

③ 제1항 및 제3항에 따른 과태료는 대통령령이 정하는 바에 따라 관계 중앙행정기관이 부과·징수한다.

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(보안관제전문업체에 대한 경과조치) 이 법 시행 당시 책임기관에 제12조 제1항의 보안관제센터 업무를 제공하고 있는 업체는 이 법 시행일부터 6개월 내에 행정기관의 장에게 보안관제전문업체로 지정 받아야 한다.

〈부록 2〉 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안

제1장 총칙

제1조(목적) 이 법은 클라우드컴퓨팅의 발전 및 이용을 촉진하고 클라우드컴퓨팅서비스를 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 국민경제의 지속가능한 발전에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “클라우드컴퓨팅”이란 논리적인 분할 또는 결합을 통해 집적·공유된 정보통신기기·설비, 소프트웨어 등 정보통신자원을 필요에 따라 정보통신망을 통해 신축적으로 제공함으로써 정보통신자원의 이용효율을 극대화하는 컴퓨팅을 말한다.
2. “클라우드컴퓨팅기술”이란 클라우드컴퓨팅의 구축 및 이용에 관한 기술로서 방송통신위원회가 고시로 정하는 것을 말한다.
3. “클라우드컴퓨팅서비스”란 클라우드컴퓨팅을 이용하여 타인의 요청에 따라 정보통신자원을 이용하게 하는 서비스로서, 다음 각 목의 어느 하나에 해당하는 서비스를 말한다.
   가. 서버, 스토리지, 네트워크 등을 이용하게 하는 서비스
   나. 응용프로그램 등 소프트웨어의 개발·운영 등을 위한 도구환경을 이용하게 하는 서비스
   다. 응용프로그램 등 소프트웨어를 이용하게 하는 서비스
   라. 그 밖에 이에 준하는 서비스로서 방송통신위원회가 고시로 정하는 서비스
4. “클라우드컴퓨팅서비스 제공자”란 클라우드컴퓨팅서비스를 제공하는 자를 말한다.
5. “이용자”란 클라우드컴퓨팅서비스를 이용하는 자를 말한다.

제3조(국가 및 지방자치단체의 책무) 국가와 지방자치단체는 클라우드컴퓨팅의 발전 및 이용촉진, 클라우드컴퓨팅서비스를 안전하게 이용할 수 있는 환경의

조성과 이에 필요한 재원확보를 위해 노력하여야 한다.

제4조(클라우드컴퓨팅서비스 제공자 및 이용자의 책무) ① 클라우드컴퓨팅서비스 제공자는 이용자의 정보를 보호하고 신뢰할 수 있는 클라우드컴퓨팅서비스를 제공하여 이용자의 권익보호에 이바지하여야 한다.

② 이용자는 안전한 클라우드컴퓨팅서비스 이용 환경이 정착되도록 노력하여야 한다.

제5조(다른 법률과의 관계) 클라우드컴퓨팅의 발전 및 이용촉진, 이용자 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

제2장 클라우드컴퓨팅 관련 시책의 마련 및 발전기반 조성 등

제6조(클라우드컴퓨팅 발전 및 이용자 보호에 관한 시책의 마련·시행) ① 정부는 클라우드컴퓨팅기술 및 서비스의 발전과 안전한 이용환경 조성을 위한 시책을 마련하고 이를 시행하여야 한다.

② 제1항의 시책에는 다음 각 호의 사항이 포함되어야 한다.

1. 클라우드컴퓨팅 도입과 이용 활성화에 관한 사항
2. 클라우드컴퓨팅기술 및 서비스의 연구개발 촉진에 관한 사항
3. 클라우드컴퓨팅 인력양성 및 전문성 강화에 관한 사항
4. 클라우드컴퓨팅 국제협력과 해외진출 촉진에 관한 사항
5. 클라우드컴퓨팅서비스의 인증에 관한 사항
6. 클라우드컴퓨팅서비스의 정보보호에 관한 사항
7. 그 밖에 클라우드컴퓨팅기술 및 서비스의 발전과 안전한 이용환경 조성을 위하여 필요한 사항

제7조(실태조사) ① 정부는 클라우드컴퓨팅에 관한 정책의 효과적인 수립·시행에 필요한 산업 현황 및 통계를 확보하기 위하여 실태조사를 실시할 수 있다.

② 정부는 제1항에 따른 실태조사를 위하여 필요한 경우 클라우드컴퓨팅서비스 제공자 또는 그 밖의 관련 기관 및 단체에 대하여 자료의 제출이나 의견의

진술 등을 요청할 수 있다.

③ 제2항에 따라 자료의 제출이나 의견의 진술 등을 요청받은 자는 정당한 사유가 없는 한 이에 응하여야 한다.

제8조(연구개발) ① 정부는 클라우드컴퓨팅기술 및 서비스의 연구개발을 촉진하기 위하여 다음 각 호의 사업을 추진할 수 있다.

1. 클라우드컴퓨팅기술 및 서비스 관련 정부연구개발 투자
2. 클라우드컴퓨팅기술 및 서비스 사업화 등에 대한 금융지원
3. 클라우드컴퓨팅기술 및 서비스 관련 전문인력의 양성 및 국제협력
4. 클라우드컴퓨팅기술 및 서비스 동향, 우수사례 등 정보의 수집·분석 및 제공

② 정부는 제1항 각 호의 사업을 실시하는 자에 대하여 그 소요되는 비용의 전부 또는 일부를 지원할 수 있다.

제9조(시범사업) ① 정부는 클라우드컴퓨팅기술 및 서비스의 사업화 또는 이용촉진을 위하여 시범사업을 추진할 수 있다. 이 경우 정부는 지방자치단체에 협력을 요청할 수 있다.

② 정부는 제1항의 시범사업을 실시하는 자에 대하여 필요한 경우 재정적 지원을 할 수 있다.

제10조(세제지원) 국가나 지방자치단체는 클라우드컴퓨팅기술 및 서비스의 발전과 이용촉진을 위하여 「조세특례제한법」, 「지방세특례제한법」, 기타 관련 법률이 정하는 바에 따라 클라우드컴퓨팅서비스 제공자 또는 이용자에 대해 소득세·법인세·취득세·재산세 등을 감면할 수 있다.

제11조(중소기업 등의 지원) ① 정부는 클라우드컴퓨팅기술 및 서비스의 발전과 이용촉진을 위하여 클라우드컴퓨팅 관련 중소기업(「중소기업기본법」 제2조에 따른 중소기업을 말한다)에 대해 행정적·재정적·기술적 지원을 할 수 있다.

② 정부는 클라우드컴퓨팅서비스를 이용하는 1인 창조기업(「1인 창조기업 육성에 관한 법률」 제2조에 따른 1인 창조기업을 말한다)에 대해 그 비용의 전부 또는 일부를 지원할 수 있다.

제1항 및 제2항에 따른 지원의 대상 및 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제12조(전문인력의 양성) ① 정부는 클라우드컴퓨팅에 관한 전문인력을 양성하기 위하여 필요한 정책을 수립하고 추진할 수 있다.

② 정부는 클라우드컴퓨팅 관련 교육훈련을 실시하는 교육기관 중 전문인력, 시설 등 대통령령으로 정하는 요건을 갖춘 기관을 지정하여 필요한 경비의 전부 또는 일부를 지원할 수 있다.

③ 제1항 및 제2항에 따른 전문인력 양성 정책의 수립, 교육기관의 지정절차 및 지원내용 등에 관한 사항은 대통령령으로 정한다.

제13조(국제협력 및 해외진출의 촉진) 정부는 클라우드컴퓨팅 관련 국제협력과 클라우드컴퓨팅기술 및 서비스의 해외진출을 촉진하기 위하여 다음 각 호의 사업을 추진할 수 있다.

1. 클라우드컴퓨팅 관련 기술 및 인력 교류
2. 전시회 등 홍보 및 해외 마케팅
3. 해외진출에 관한 정보의 수집·분석 및 제공
4. 그 밖에 국제협력 및 해외진출 촉진을 위하여 필요한 사항

제3장 클라우드컴퓨팅서비스의 이용촉진 등

제14조(클라우드컴퓨팅서비스업의 신고 등) ① 클라우드컴퓨팅서비스를 제공하는 사업을 하려는 자는 대통령령으로 정하는 바에 따라 방송통신위원회에 신고하여야 한다. 이 경우 「전기통신사업법」 제22조에 따른 부가통신사업의 신고(변경신고를 포함한다)를 한 것으로 본다.

② 제1항에 따라 신고한 자는 신고한 날부터 1년 이내에 사업을 시작하여야 한다.

③ 제1항에 따라 신고한 자는 그 신고한 사항 중 대통령령으로 정하는 중요한 사항을 변경하려면 방송통신위원회에 변경신고를 하여야 한다.

④ 제1항에 따라 신고한 자가 그 사업의 전부 또는 일부를 휴지 또는 폐지하고자 하는 때에는 휴지 또는 폐지하고자 하는 날의 30일 전까지 이를 방송통신위원회에 신고하여야 한다. 이 경우 1년 이상 계속하여 사업을 휴지하여서

는 아니 된다.

⑤ 방송통신위원회는 제1항에 따라 신고한 자가 다음 각 호의 어느 하나에 해당하면 사업의 전부 또는 일부의 폐지를 명하거나 1년 이내의 기간을 정하여 사업의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호에 해당하는 경우에는 사업의 전부 또는 일부의 폐지를 명하여야 한다.

1. 속임수나 그 밖의 부정한 방법으로 신고를 한 경우
2. 제2항을 위반하여 신고한 날부터 1년 이내에 사업을 시작하지 아니하거나 제4항을 위반하여 1년 이상 계속하여 사업을 휴지한 경우
3. 제34조에 따른 시정명령을 이행하지 않은 경우

⑥ 제1항, 제2항, 제3항 및 제4항에 따른 신고, 변경신고 및 휴지·폐지신고의 요건, 방법 및 절차, 제5항에 따른 처분의 기준, 방법 및 절차 그 밖에 필요한 사항은 대통령령으로 정한다.

제15조(클라우드컴퓨팅서비스업의 양수 및 법인의 합병 등) ① 제14조제1항에 따라 신고한 자는 사업의 전부 또는 일부의 양수, 상속 또는 법인의 합병·분할이 있는 경우에는 그 사업의 양수인, 상속인 또는 합병·분할에 의하여 설립되거나 합병·분할 후 존속하는 법인은 대통령령이 정하는 바에 따라 방송통신위원회에 신고하여야 한다.

② 제1항에 따른 양수인, 상속인 또는 합병·분할에 의하여 설립되거나 합병·분할 후 존속하는 법인은 양도인, 피상속인 또는 합병·분할 전의 법인의 지위를 각각 승계한다.

제16조(공공기관등의 클라우드컴퓨팅 도입·이용) ① 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관(이하 "공공기관등"이라 한다)은 업무의 효율화·자동화·고도화를 위해 클라우드컴퓨팅의 도입·이용에 노력하여야 한다.

② 지방자치단체와 공공기관은 클라우드컴퓨팅을 도입·이용하고자 하는 경우에는 정부에 기술 등의 지원을 요청할 수 있다.

③ 공공기관등이 업무를 위하여 클라우드컴퓨팅서비스(공공기관등에서 제공하는 서비스는 제외한다)를 이용하려는 경우에는 해당 클라우드컴퓨팅서비스 제공자로 하여금 사전에 정부가 수행하는 정보보호인증을 받도록 할 수 있다.

제3항에 따른 정보보호인증의 내용, 방법 및 절차에 관하여는 대통령령으로 정하는 바에 따른다.

제17조(전산시설등의 구비) 법령에 따라 인·허가 등의 요건으로 다음 각 호의 전산시설·장비·설비 등(이하 "전산시설등"이라 한다)을 갖추어야 하는 자가 해당 법령에서 요구하는 전산시설등에 관한 요건을 충족한 클라우드컴퓨팅서비스를 이용하는 때에는 해당 전산시설등을 갖춘 것으로 본다.

1. 「관세법」 제233조의2제2항에 따라 수출입물품의 원산지정보 수집·분석 업무를 위탁받으려는 법인 또는 단체가 전산설비를 갖추어야 하는 경우
2. 「농림수산식품투자조합결성 및 운용에 관한 법률」 제6조에 따라 투자전문기관으로 지정받으려는 자가 전산장비를 갖추어야 하는 경우
3. 「농업협동조합법」 제115조제2항제3호에 따라 중앙회의 회원으로 가입하고자 하는 자가 전산설비를 갖추어야 하는 경우
4. 「발명진흥법」 제21조에 따라 특허기술정보센터로 등록하려는 자가 시설, 전산설비, 데이터베이스를 갖추어야 하는 경우
5. 「발명진흥법」 제23조제3항에 따라 지역지식재산센터를 등록하려는 자가 전산장비를 갖추어야 하는 경우
6. 「사이버대학 설립·운영규정」 제5조제3항에 따라 각종 서버, 통신장비 및 콘텐츠개발 설비 등 원격교육에 필요한 설비를 갖추어야 하는 경우
7. 「소비자기본법」 제29조제1항제3호에 따라 소비자단체로 등록하려는 자가 전산장비를 갖추어야 하는 경우
8. 「위치정보의 보호 및 이용 등에 관한 법률」 제5조제1항에 따라 위치정보사업을 하고자 하는 자가 위치정보시스템을 포함한 사업용 주요 설비를 갖추어야 하는 경우
9. 「전자상거래 등에서의 소비자보호에 관한 법률」 제24조의2제4항에 따라 광고수신거부의사 등록시스템의 운용을 위하여 전산설비를 갖추어야 하는 경우
10. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제53조에 따라 통신과금서비스제공자로 등록하려는 자가 전산설비와 각종 컴퓨터프로그램을 갖추어야 하는 경우

11. 「콘텐츠산업진흥법」 제21조제2항에 따라 콘텐츠 거래사실 인증기관으로 지정 받으려는 자가 네트워크 및 조회설비를 갖추어야 하는 경우
12. 「콘텐츠산업진흥법」 제22조제2항에 따라 콘텐츠 제공서비스의 품질 인증기관으로 지정 받으려는 자가 네트워크 설비를 갖추어야 하는 경우
13. 「평생교육법」 제33조제3항에 따라 원격대학형태의 평생교육시설을 설치하고자 하는 자가 각종 서버, 통신장비 및 매체제작장비 등 설비를 갖추어야 하는 경우

제18조(상호 운용성의 확보) 방송통신위원회는 클라우드컴퓨팅서비스의 상호 운용성을 확보하기 위하여 필요한 경우에는 클라우드컴퓨팅서비스 제공자에게 상호간 협력 체계를 구축하도록 권장할 수 있다.

제19조(클라우드컴퓨팅서비스의 인증) ① 방송통신위원회는 클라우드컴퓨팅서비스의 품질 및 신뢰성을 높이기 위하여 클라우드컴퓨팅서비스를 대상으로 인증을 실시할 수 있다.

② 방송통신위원회는 제1항에 따른 인증을 위하여 심사기준(이하 “인증기준”이라 한다) 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

③ 방송통신위원회는 제1항에 따른 인증업무의 효율적 수행을 위하여 방송통신위원회가 지정한 기관(이하 “인증기관”이라 한다)으로 하여금 그 업무를 수행하게 할 수 있다.

④ 인증기관은 제1항에 따라 인증을 신청한 클라우드컴퓨팅서비스가 인증기준에 적합한 경우에는 인증서를 교부하여야 한다.

⑤ 방송통신위원회는 제1항에 따른 인증이 다음 각 호의 하나에 해당하는 경우 그 인증을 취소하여야 한다.

1. 속임수나 그 밖의 부정한 방법으로 인증을 받은 경우
2. 제2항에 따른 인증 기준에 미달하게 된 경우

⑥ 제1항에 따라 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다. 인증을 받지 않은 자는 인증 표시 또는 이와 유사한 표시를 하여서는 아니 된다.

⑦ 제1항에 따른 인증의 방법·절차·범위·수수료, 제3항에 따른 인증기관의 지정기준, 방법·절차, 제5항에 따른 인증취소의 절차, 그 밖에 필요한 사항

은 대통령령으로 정한다.

⑧ 방송통신위원회는 제1항에 따른 인증을 받은 자에 대하여 이 법에 따른 지원을 우선적으로 할 수 있다.

제20조(인증기관의 지정취소 등) ① 방송통신위원회는 제18조제3항에 따라 인증기관으로 지정받은 자가 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 6개월 이내의 기간을 정하여 업무의 정지를 명할 수 있다. 다만, 제1호에 해당하는 경우에는 그 지정을 취소하여야 한다.

1. 속임수나 그 밖의 부정한 방법으로 지정을 받은 경우
2. 정당한 사유 없이 1년 이상 계속하여 인증업무를 하지 아니한 경우
3. 제19조 제7항에 따른 지정기준에 미달한 경우

② 제1항에 따른 인증기관의 지정취소·업무정지의 기준 등에 관하여 필요한 사항은 대통령령으로 정한다.

제4장 클라우드컴퓨팅서비스의 신뢰성 제고

제21조(품질·성능의 신뢰성 향상) ① 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질 및 성능을 향상시키기 위해 노력하여야 한다.

② 방송통신위원회는 클라우드컴퓨팅서비스의 품질 및 성능, 그 적정한 수준 등에 관한 세부 기준을 정하여 이를 클라우드컴퓨팅서비스 제공자에게 권고할 수 있다.

제22조(표준약관) ① 클라우드컴퓨팅서비스 제공자 단체는 이용자를 보호하고 분쟁 발생을 예방하기 위하여 표준이 될 약관(이하 "표준약관"이라 한다)을 정하여 방송통신위원회에 그 심사를 청구할 수 있다.

② 방송통신위원회는 필요한 경우 클라우드컴퓨팅서비스 제공자 단체에 표준약관의 마련 또는 방송통신위원회가 마련한 표준약관을 사용할 것을 권장할 수 있다.

③ 클라우드컴퓨팅서비스 제공자는 그가 사용하는 약관이 표준약관의 내용보다 이용자에게 불리한 경우 표준약관과 다르게 정한 약관의 내용을 이용자가

알기 쉽게 표시하거나 고지하여야 한다.

제23조(사고의 통지 등) ① 클라우드컴퓨팅서비스 제공자는 침해사고(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조에 따른 침해사고를 말한다), 심각한 서비스 장애 및 정보유출 등의 사고가 발생하면 이용자에게 그 사실을 지체 없이 알려야 한다.

② 클라우드컴퓨팅서비스 제공자는 제1항에 따른 침해사고 또는 대통령령이 정하는 일정 규모 이상의 정보유출이 발생하면 그 사실을 즉시 방송통신위원회에 신고하여야 한다.

③ 방송통신위원회는 제2항에 따른 신고를 받거나 해당 사실을 알게 되면 피해 확산 방지, 복구 및 재발 방지 등을 위하여 대통령령이 정하는 바에 따라 필요한 조치를 할 수 있다.

제24조(서비스 안전지침) 방송통신위원회는 안전한 클라우드컴퓨팅서비스의 제공 및 이용을 위하여 대통령령으로 정하는 관리적·물리적·기술적 보호조치를 포함한 구체적인 서비스 안전지침을 정하여 고시하고, 이를 클라우드컴퓨팅서비스 제공자 또는 이용자에게 권고할 수 있다.

제25조(정보의 제3자 제공 금지 등) ① 클라우드컴퓨팅서비스 제공자는 다른 법률에 특별한 규정이 있는 경우 외에는 이용자의 정보를 동의 없이 제3자에게 제공하거나 서비스 제공 목적 외로 이용할 수 없다.

② 클라우드컴퓨팅서비스 제공자는 이용자와 계약이 종료된 때에는 계약의 내용에 따라 지체 없이 이용자의 정보를 반환하거나 파기하는 등 필요한 조치를 하여야 한다.

③ 제2항의 경우 계약에서 특별히 정함이 없는 때에는 클라우드컴퓨팅서비스 제공자는 지체 없이 이용자의 정보를 반환하여야 하며, 이용자의 요청이 있거나 성질상 반환이 불가능한 경우에는 해당 정보를 파기하여야 한다. 다만, 다른 법률에 따라 해당 정보를 보존해야 하는 경우에는 그러하지 아니하다.

제26조(클라우드컴퓨팅서비스 이용사실의 공개) ① 업무상 클라우드컴퓨팅서비스를 이용하여 타인의 정보를 취급하는 자(이하 “클라우드컴퓨팅서비스이용정보취급자”라 한다)는 대통령령으로 정하는 바에 따라 클라우드컴퓨팅서비스 이용사실을 공개하여야 한다.

② 제1항에 따른 이용사실의 공개내용, 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제27조(정보의 국외저장에 대한 공개 등) ① 클라우드컴퓨팅서비스 제공자는 이용자의 정보를 국외에 저장하는 경우에는 해당 국가의 명칭, 정보보호수준 및 구제절차 등(이하 "국외저장현황정보"라 한다)을 대통령령이 정하는 방법·절차 등에 따라 이용자에게 공개하여야 한다.

② 클라우드컴퓨팅서비스 제공자는 이용자의 정보를 국외에 저장하는 경우에는 대통령령이 정하는 바에 따라 정보보호에 필요한 관리적·물리적·기술적 조치 등을 취하여야 한다.

제28조(정보의 보존 및 복구를 위한 조치) ① 클라우드컴퓨팅서비스 제공자는 재난, 침해사고 등에 대비하기 위하여 정보의 보존 및 복구를 위한 시스템을 구축하도록 노력하여야 한다.

② 제1항의 클라우드컴퓨팅서비스 제공자 중 이용자 수, 매출액 등을 감안하여 대통령령으로 정한 일정 규모 이상의 클라우드컴퓨팅서비스 제공자는 정보의 보존 및 복구를 위한 시스템을 구축하여야 한다.

③ 제2항의 정보의 보존 및 복구를 위한 시스템의 기준은 방송통신위원회가 고시로 정한다.

제29조(이용자 정보의 임치) ① 클라우드컴퓨팅서비스 제공자와 이용자는 전문인력과 설비 등을 갖춘 기관으로서 대통령령으로 정하는 자(이하 "수치인"이라 한다)와 서로 합의하여 이용자의 정보, 소프트웨어 등을 수치인에게 임치할 수 있다.

② 클라우드컴퓨팅서비스 제공자 또는 이용자는 제1항에 따른 합의에서 정한 사유가 발생한 때에 수치인에게 정보의 제공을 요구할 수 있다.

제30조(정보의 반환·파기 등) ① 클라우드컴퓨팅서비스 제공자가 서비스를 종료하려면 서비스 종료 예정일 30일 전까지 대통령령으로 정하는 방법·절차에 따라 이용자에게 그 사실을 통지하여야 한다.

② 이용자는 제1항에 따른 통지를 받거나 서비스 종료 사실을 알게 된 때에는 클라우드컴퓨팅서비스 제공자에 대하여 본인이 제공한 정보의 반환 또는 파기를 요구할 수 있다.

③ 클라우드컴퓨팅서비스이용정보취급자의 서비스가 종료하게 되는 때에는 해당 서비스를 이용하는 자는 클라우드컴퓨팅서비스이용정보취급자에게 자신의 정보를 반환 또는 파기하도록 하는 것이 현저히 곤란하거나 불가능한 경우 클라우드컴퓨팅서비스 제공자에 대하여 일정 기간 내에 자신의 정보를 파기할 것을 요구할 수 있다.

④ 클라우드컴퓨팅서비스 제공자는 제2항과 제3항에 따라 정보의 반환 또는 파기를 요구받으면 지체 없이 이에 필요한 조치를 취하여야 한다.

제31조(클라우드컴퓨팅서비스의 중단에 대한 대책 마련 등) ① 클라우드컴퓨팅서비스 제공자는 파산·폐업 등으로 서비스가 예견치 못하게 중단되는 경우에 대비하여 이용자 정보의 반환·파기에 필요한 대책을 마련하여야 한다.

② 클라우드컴퓨팅서비스 제공자는 제1항의 사유에 따른 중단에 대비하여 대통령령으로 정하는 일정 기간 동안 이용자 정보의 반환·파기가 가능하도록 서비스를 유지하기 위하여 보증보험에 가입하여야 한다. 이 경우 보증보험금은 「채무자회생 및 파산에 관한 법률」 규정에도 불구하고 우선적으로 이용자 정보의 반환·파기를 위한 서비스 유지에 사용되어야 한다.

③ 제2항에 따라 보증보험에 가입한 클라우드컴퓨팅서비스 제공자는 보증보험 증권을 방송통신위원회에 제출하여야 한다.

④ 방송통신위원회는 제2항에 따라 보증보험에 가입한 클라우드컴퓨팅서비스 제공자의 서비스가 중단된 경우에는 대통령령으로 정하는 바에 따라 이용자 정보의 반환·파기에 관한 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 임시관리인으로 지정할 수 있다.

제4항에 따른 임시관리인의 지정에 관한 기준·방법·절차 및 지정 취소 등에 관한 사항은 대통령령으로 정한다.

제32조(손해배상책임 등) ① 이용자는 클라우드컴퓨팅서비스 제공자가 이 법의 규정을 위반한 행위로 손해를 입으면 그 클라우드컴퓨팅서비스 제공자에게 손해배상을 청구할 수 있다. 이 경우 해당 클라우드컴퓨팅 서비스 제공자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

클라우드컴퓨팅서비스 제공자 또는 이용자는 제1항에 따른 손해배상에 관하여 당사자 간 협의가 이루어지지 아니하거나 협의를 할 수 없는 경우에는 방송통

신위원회에 재정(裁定)을 신청할 수 있다.

제5장 보 칙

제33조(협회의 설립 등) ① 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅기술 및 서비스의 발전과 안전한 이용환경을 조성하기 위하여 방송통신위원회의 인가를 받아 협회를 설립할 수 있다.

② 제1항에 따른 협회는 법인으로 한다.

③ 제1항에 따른 협회는 다음 각 호의 업무를 수행할 수 있다.

1. 클라우드컴퓨팅기술 및 서비스 현황 등에 관한 통계 및 실태 조사
2. 클라우드컴퓨팅기술 및 서비스에 관한 인식 제고
3. 클라우드컴퓨팅 관련 응용 서비스의 개발 등 컨설팅
4. 클라우드컴퓨팅서비스 표준약관 등의 개발 및 보급
5. 클라우드컴퓨팅서비스 이용 관련 각종 상담·피해접수 및 분쟁조정
6. 클라우드컴퓨팅기술 및 서비스에 관한 국제협력 등

④ 방송통신위원회는 제3항 각 호의 업무수행을 위해 필요한 경우에는 예산의 범위 내에서 협회에 재정 및 기술을 지원할 수 있다.

⑤ 이 법에서 정한 것 외에 협회의 설립·운영 등에 관하여 필요한 사항은 민법 중 사단법인에 관한 규정을 준용한다.

제34조(시정명령 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 클라우드컴퓨팅서비스 제공자에게 관계 물품·서류 등을 제출하게 할 수 있다.

1. 이 법에 위반되는 사항을 발견한 경우
2. 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 방송통신위원회는 클라우드컴퓨팅서비스 제공자가 제1항에 따른 물품·서류 등을 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 클라우드컴퓨팅서비스 제공자의 사업장에 출입하여 업무상황, 장

부 또는 서류 등을 검사하도록 할 수 있다.

③ 방송통신위원회는 이 법을 위반한 클라우드컴퓨팅서비스 제공자에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있다.

④ 제1항과 제2항에 따른 자료의 제출 요구 및 출입검사 등의 방법 및 절차에 관하여는 "행정조사기본법"에서 정하는 바에 따른다.

제35조(권한 또는 업무의 위임·위탁) ① 이 법에 따른 정부의 권한 또는 업무는 그 일부를 대통령령으로 정하는 바에 따라 그 소속 기관의 장에 위임하거나 전문기관에게 위탁할 수 있다.

② 정부는 제1항 따라 업무의 일부를 위탁하는 경우 해당 전문기관의 업무수행을 위하여 필요한 경비를 출연할 수 있다.

제36조(벌칙적용에서의 공무원 의제) 정부가 제35조제1항에 따라 위탁한 업무에 종사하는 전문기관의 임직원은 「형법」 제129조부터 제132조까지의 규정에 따른 벌칙을 적용할 때에는 공무원으로 본다.

제6장 벌칙

제37조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

1. 제14조제1항을 위반하여 신고를 하지 않은 자
2. 제14조제5항에 따른 사업폐지명령에 위반한 자

② 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제14조제3항를 위반하여 변경신고를 하지 않은 자
2. 제14조제5항에 따른 사업정지명령에 위반한 자
3. 제15조제1항을 위반하여 신고를 하지 않은 자

제38조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료에 처한다.

1. 제19조제6항에 위반하여 인증 표시 또는 이와 유사한 표시를 한 자

2. 제30조에 따라 이용자의 정보를 반환·파기하기 위한 조치를 하지 않은 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료에 처한다.

1. 제31조제2항을 위반하여 보증보험에 가입하지 아니한 자
2. 제34조에 따른 시정명령을 이행하지 아니한 자

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날로부터 시행한다.

제2조(부가통신사업 신고자에 대한 경과조치) 이 법 시행 당시 「전기통신사업법」 제22조제1항에 따라 부가통신사업의 신고를 하고 클라우드컴퓨팅서비스를 제공하는 사업을 하고 있는 자는 이 법 시행일로부터 6월 이내에 제14조제1항에 따른 신고를 하여야 한다.

〈부록 3〉 '중국에서의 사이버범죄 관련 법제 현황' 원문

中国网络犯罪探究

田宏杰* · 刘红霞**

摘要：网络这一现代技术，极大便利社会生活的同时，也带来了形形色色的犯罪问题。中国学界对网络犯罪的研究始于20世纪90年代，至今已形成极为丰富的学术著作和科研成果。但遗憾的是，学界对网络犯罪的认识一直深陷计算机犯罪与网络犯罪之间的泥泞深渊，使网络犯罪的相关研究呈现出一定程度的混乱局面。有鉴于此，笔者结合中国计算机、网络发展的实际情况，分三阶段分析了计算机犯罪与网络犯罪之间的关系，并指出当下阶段，网络犯罪绝不等同于计算机犯罪，而是具有独特本质和鲜明特征的新事物，从而为本文进一步研究网络犯罪的现状、发展趋势以及法律规制等问题提供了新视野和新途径。

关键词：网络犯罪 犯罪现状 发展趋势 法律规制

网络进入国人视野短短不过廿年时间，但却极大地改变了社会发展的运转模式和人们的工作、生活、思维方式。这无疑是继工业革命之后，人类社会发展史上又一次伟大的科技革命。网络的广泛使用，在现代社会经济快速进步、人民生活质量迅速提高、生活方式便利高效等诸多方面所发挥的巨大功用，早已为人们有目共睹，且即将向着更深入、更广阔的领域展开。据中国互联网信息中心2013年1月发布的《第31次中国互联网络发展情况统计报告》显示，截止2012年12月31日，中国网民数量已达到5.64亿之众。放眼当今社会，网络无时不有，无处不在，早已深深融入社会生活的方方面面。但也正如西方古谚所讲，每一枚硬币都有正反两面。网络光明前景的背后，必然也隐藏着消极的梦魇。而众多消极内容之中，最早为人所知也最为人瞩目的方面之一，非网络犯罪莫属。

谈及网络犯罪，大多数国人的印象仍旧停留于形形色色的网络犯罪案件之上。比如2001年4月的"中美黑客大战"，2007年初肆虐的"熊猫烧香案"，2009年5月的"5·19断网事件"等等，而对于网络犯罪的要旨却始终懵懵懂懂，无法一语道尽。当然，这与我国网络发展相对落后的客观现实有关，但显然更为重要的是与我国网络犯罪法制发展相对滞后密切相关。即使在中国目前学术界，对于网络犯罪问题的研究基石——网络犯罪概念，该如何界定也是众

说纷纭，莫衷一是，尚未形成统一一致的见解。

一、中国网络犯罪之概念厘定

任何科学项目的研究，首要任务便是确定研究对象。网络犯罪这一概念在中国提出至今不过二十年时间，国内专家学者虽然也就此问题进行了大量探索，取得了一定研究成果，但正如杨正鸣、皮勇所言，这一概念的内涵、外延始终不甚明确，因此，合理界定网络犯罪之概念，明晰何谓网络犯罪，理应成为研究该问题首当其冲必须解决的难题。[1][2]

就目前我国学界出版的专著、译著、论文来看，网络犯罪概念的界定，均围绕着计算机与互联网展开。比较有代表性的观点有：

观点1：网络犯罪是行为主体（人）以计算机及网络为犯罪工具或攻击对象，故意实施的危害网络安全，侵害网络资源，危害他人或者社会的触犯有关法律规范的行为。

观点2：网络犯罪是指行为人利用网络专门知识，以计算机为工具，对存在于网络空间里的信息进行侵犯的严重危害社会的行为。

观点3：网络犯罪是违反国家法律规定，利用信息技术，在计算机网络上进行的妨害计算机信息交流或者严重危害社会，依法应负刑事责任的行为。[3]

仔细观察，便不难发现，上述几种关于网络犯罪的概念界定，无不围绕计算机和网络这两个关键词表述而成，且明显烙印着计算机犯罪概念的影子。就方法论而言，相似、相关概念的界定在表达上相互参考，本也无可厚非，但问题在于，参照计算机犯罪概念而形成的网络犯罪的概念，缺乏对网络犯罪本质特征的凸显，也疏于二者之间关系的澄清，这就导致了计算机犯罪与网络犯罪在概念上的混淆不清，也致使国内学者就二者关系问题长期争论不休。

正因如此，笔者认为，厘清计算机犯罪与网络犯罪二者之间的关系，理应成为科学界定网络犯罪之概念的关键所在。

---

* 田宏杰，法学博士、金融学博士后，中国人民大学法学院教授、博士生导师，中国人民大学教师教学发展中心主任，北京市东城区人民检察院副检察长。

** 刘江霞，中国人民大学刑法学博士生。

1) 杨正鸣：《网络犯罪概念论》，载《犯罪研究》2002年第2期。

2) 皮勇：《网络犯罪比较研究》，中国人民公安大学出版社2005年版。

3) 季境、张志超主编：《新型网络犯罪问题研究》，中国检察出版社2012年版。

(一) 计算机犯罪与网络犯罪

在二者的关系问题上，学界的观点众多，但归纳起来主要有以下三种：

1. 等同说。该说认为网络犯罪就是计算机犯罪的另一种称谓，网络犯罪在本质上仍然是计算机犯罪。[4] 网络犯罪就其实质而言，仍属于计算机犯罪的一种，网络犯罪必然发生于网络空间，但并不必然以网络为犯罪工具。在上网工具已不限于计算机，利用移动通信工具等也可以进入互联网的情况下，行为人也可能利用其他手段危害网络安全，如通过发射电磁波干扰网络信息的传输，这同样是发生在网络空间的犯罪。[5]

2. 阶段说。持该说的学者认为，计算机网络与计算机系统在概念外延上是相互交叉的，计算机信息系统并非包含着网络，通过计算机网络组建的计算机信息系统是其高级形式。具体而言，网络犯罪就是行为主体以计算机或者计算机网络为犯罪工具或者攻击对象，故意实施的危害网络安全的，触犯有关法律规范的行为。[6]

3. 网络信息说。该说认为，网络犯罪是指行为人利用网络专门知识，以计算机为工具，对存在于网络空间中的信息进行侵犯的严重危害社会的行为。[7]

其实，随着时间脉络认真考察计算机及网络发展的历史，中国计算机犯罪与网络犯罪的关系便会逐渐浮出水面。

1956年，夏培苏完成了第一台电子计算机运算器和控制器的设计工作，中国第一台计算机诞生。之后的二十年间电子计算机主要应用于计算、新闻及金融等各个领域。

1986年，中国破获第一例计算机犯罪案件（利用计算机贪污案）。

1987年，中国首次建成电子邮件节点，向世界成功发送了第一封电子邮件。之后我国不断不断致力于计算机网络的研究与开发。

1994年，我国正式加入国际互联网。

---

4) 刘守芬、孙晓芳：《论网络犯罪》，载《北京大学学报》2001年第3期。

5) 冯卫国：《试论网络犯罪及其控制对策》，载赵秉志主编：《新千年刑法热点问题研究与适用》（上），中国检察官出版社2001年版。

6) 范德繁、于宏：《针对网络犯罪之认定探讨——兼评刑法相应立法的完善》，载《法制与社会发展》2001年第5期。

7) 皮勇：《网络犯罪比较研究》，中国人民公安大学出版社2005年版。

1996年，中国破获第一例网络犯罪案件（制造计算机病毒案）。

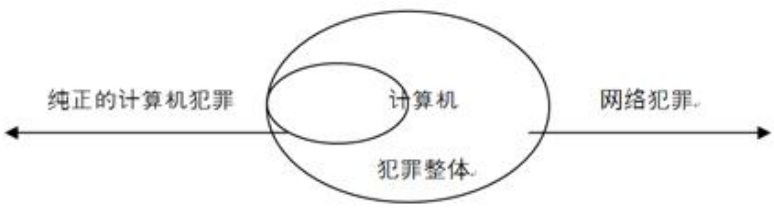
从中国计算机网络发展大事件基本可以得出这样的结论，在中国，计算机产生在前，网络产生在后；计算机产生之后网络产生之前，计算机犯罪就已经开始出现；网络犯罪出现在网络产生之后。

在笔者看来，中国的计算机犯罪概念和网络犯罪概念与中国计算机、网络发展的历史脉络密切相关，表现出了一些中国自身的特点。在理顺二者关系的问题上，笔者认为应当分为三个阶段分别进行考察。

第一阶段：计算机时代（50年代至80年代初）。于此阶段的中国，网络尚未真正出现，因此当时存在的大多是计算机单机犯罪或者计算机系统犯罪，笔者将其称之为纯正计算机犯罪，是狭义的计算机犯罪概念。

第二阶段：计算机网络时代（80年代末至90年代初）。于此阶段，中国正式加入国际互联网，网络和计算机相互结合，形成计算机网络系统。在这种结合模式之下，网络的作用并未十分凸显，计算机的基础地位仍然巩固。此阶段，既存在上阶段中与网络无涉的纯正计算机犯罪，又出现了以计算机为工具针对网络信息与网络安全的犯罪，即实质上的网络犯罪。但由于此阶段计算机与网络之间的对应关系，人们习惯的将计算机犯罪的内涵扩大化，试图将所有犯罪以计算机犯罪一词概之。此时的计算机犯罪为广义的计算机犯罪，计算机犯罪和网络犯罪之间可谓是包含关系。当然，也有部分学者审时度势，敏锐的注意到了计算机犯罪与网络犯罪的不同，但于该阶段中并未形成主流观点。

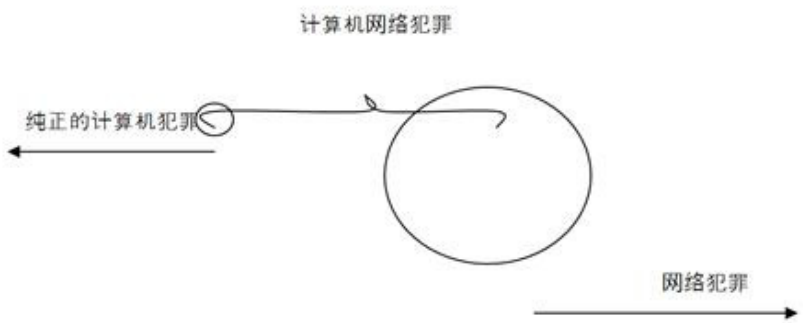
三者关系如下图所示：大圆即计算机网络时代的犯罪整体——广义的计算机犯罪，小圆为纯正计算机犯罪，小圆之外为网络犯罪。



第三阶段：网络时代（90年代末至现在）。在这个时代，网络成为信息时代的中心，网

络终端多元化，计算机、智能手机、智能电视等众多智能网络终端不断涌现，手机更是取代电脑成为最大的网络终端。于此阶段，网络打破上阶段中与计算机牢不可破的必然联系，真正成为了信息中心，计算机只是作为网络终端的工具之一而存在。此时，纯正的计算机犯罪变得益发微乎其微，据相关资料统计，自2000年后，计算机网络领域中的犯罪，网络犯罪逐步超过90%，而纯正计算机犯罪远远不足10%，学者们更是深深意识到计算机犯罪与网络犯罪的本质差异。[8] 至此，计算机犯罪逐步为网络犯罪所取代，计算机犯罪这一概念也再无法用以概括该阶段下所有的犯罪形式。因此，笔者认为此阶段计算机犯罪与网络犯罪应为并列关系，二者可以统称为计算机网络犯罪。

三者关系如图所示：



由此可见，中国计算机与网络的发展先后有别，呈现出不同的发展阶段。第一阶段只存在纯正计算机犯罪，而无网络犯罪；第二阶段，基于计算机与网络的密切关系，网络犯罪尚可以计算机概念蔽之，二者间为包含关系；然就当下而言（第三阶段）而言，网络的主体地位凸显，计算机犯罪的概念再无法涵盖网络犯罪，因此，当下我们所称的计算机犯罪回归纯正计算机犯罪的狭义范畴，而网络犯罪与计算机犯罪绝非可以相互包含的概念，二者在产生时间，阶段特征和侵犯对象上均存在明显差别。

具体而言，纯正计算机犯罪与网络犯罪之间的区别主要体现在：

第一，二者产生时间不同。计算机犯罪出现在前，网络犯罪出现在后。上文中已有详述，

8) 许秀中：《网络与网络犯罪》，中信出版社2003年版。

此处不再赘述。

第二，二者的阶段特征不同。显然在计算机犯罪时代，即使后来计算机也与网络相结合，但计算机始终处于中心位置；而网络犯罪时代，计算机逐步演变为众多的网络终端之一，网络开始真正成为数据信息的中心。

第三，二者侵害对象不同。计算机犯罪侵害的是计算机及其单机系统，具有特定性；而网络犯罪侵害的对象是网络数据信息，具有广泛性。从发展阶段上来看，并不是所有的联网计算机都可以成为网络犯罪的侵害对象，与网络数据信息无涉的犯罪，只能是纯正计算机犯罪。

第四，二者危害性不同。从上述三点可以看出，计算机犯罪的特定性和网络犯罪的广泛性决定了网络犯罪的社会危害性必然要严重的多。

第五，犯罪的比例不同。如果说第一阶段中100%为计算机犯罪；第二阶段中，计算机犯罪比例已日趋减少；而第三阶段中，计算机犯罪已微乎其微，网络犯罪占据了几乎"全部江山"。

总而言之，或者笔者的观点仍稚嫩十足，有待完善，但是笔者始终认为只有通过这种分阶段的认识方法，我们才可以全面解读计算机犯罪与网络犯罪的发展过程及二者之间的关系问题，也唯有如此，才能为当下网络犯罪的科学界定提供清晰的思路和途径。

㈡ 网络犯罪概念及其本质特征

1. 网络犯罪的概念

目前我国关于网络犯罪概念的界定存在多种学说，概括起来为六大基本类别：

⑴相关说。中国政法大学信息技术立法探讨课题组认为，网络犯罪就是与计算机相关的犯罪。

⑵工具利用说。即利用计算机或计算机知识达到犯罪目的的行为。[9]

⑶对象数据说。是指针对和利用计算机系统，通过非法操作或者以其他手段对计算机系统内部数据的安全完整性或系统正常性造成危害后果的行为。[10]

⑷工具对象说。中国公安部计算机管理监察司指出：网络犯罪是以计算机为工具或者以计算机资产为对象实施的犯罪。[11]

9) 刘江彬：《计算机法律概论》，北京大学出版社1992年版。

10) 孙铁成：《计算机与法律》，法律出版社1998年版。

(5)折中说。赵秉志认为网络犯罪是利用计算机操作所实施的危害计算机网络系统安全的犯罪。[12]

(6)我国刑法关于计算计网络犯罪的定义。概括起来为行为人非法侵入或者破坏计算机网络信息系统，违反刑法的犯罪行为，以及利用计算机实施的传统犯罪行为。

显然上述关于网络犯罪的定义仍纠缠于计算机与网络犯罪的关系，甚至不同程度将二者混淆，忽视了对网络犯罪本质的研究；另外将犯罪学上的网络犯罪概念与规范刑法学意义上的网络犯罪概念混为一谈。

根据上述对计算机犯罪与网络犯罪关系的剖析，笔者认为现阶段，网络是现代社会真正的信息中心。无论是个人、组织或是政府，网络都将成为其获取信息资源的最为重要的途径。人们通过网络分享、传输、搜集信息，网络是信息流动的载体。网络犯罪也必然主要体现为对网络数据信息及其网络安全的侵害与威胁。因此，就犯罪学与社会学意义而言，凡是涉及网络数据信息的非法传输、截取、篡改以及其它破坏网络安全，危害个人、社会和国家利益的行为，都是网络犯罪。

遗憾的是，我国1997年刑法修改时，学界对计算机犯罪与网络犯罪的研究尚未深入，二者间的关系也尚未明朗，因此1997年刑法只在286、286、287条对其进行了相关规定，学界贯以计算机犯罪称之。严格说来，我国并无严格刑法意义上的网络犯罪之名，但确有网络犯罪之实，因为上述规定中除了少量的纯正计算机犯罪之外，大多数均属于网络犯罪。

2. 网络犯罪的特征

网络犯罪与计算机犯罪的差异，上文已经进行了比较。网络犯罪与传统犯罪相比，具有以下鲜明特点：

(1)数据信息性。

网络是由物理设备按照某种方式连接而成的一个信息空间，这是一个难以理解但却可以想象的虚拟世界，这个世界充满了各种信号数据，是人们数据分享、搜集、传输的重要载体。网络传递处理的是信息，没有信息就没有网络。因此，由网络的信息本质所决定，侵犯网络的网络犯罪，必然表现为对网络数据信息及网络运行环境的侵害。一方面，网络犯罪必须依赖信息才能实现；另一方面，网络犯罪侵害的对象也是信息。传统犯罪只有对信息进行侵

11) 中华人民共和国计算机管理监察司：《计算机安全必读》，群众出版社1991年版。

12) 转引自许秀中：《网络与网络犯罪》，中信出版社2003年版。

害，如网上银行账户，网络电子版权等，才能构成网络犯罪，若不具有信息侵害的特点，便依旧为传统犯罪。这是网络犯罪最本质的特征，也是网络犯罪与传统犯罪最本质的区别。

⑵危害扩散性。基于网络的公开、自由性，使得网络犯罪无论是在危害领域、危害对象、危害结果等诸多方面都表现有扩散性。而危害的扩散性必然导致危害巨大。

⑶空间的虚拟性。虽然网络由光缆、卫星传送等物质方式连接而成，但是网络却是由此而形成一个虚拟数字空间。在这个空间内世界缩小成几秒或者几毫毛的距离，因此，犯罪可能瞬时完成，很难再现犯罪的物理过程。

⑷方法的智能性。与传统犯罪不同，网络犯罪的犯罪主体一般都具有一定的文化水平和技术水平，犯罪方法表现出一定的智能特征。

⑸地域跨国性。网络具有时空压缩的特性，各种各样的信息通过网络传送时，国界和地理距离暂时消失。这也就为犯罪分子跨地域和跨国界实施犯罪提供了可能。犯罪分子只需一台联网的终端机，就可以通过网络到任何站点实施犯罪活动。因此网络犯罪也往往表现出极强的涉外性质。

正是基于上述两次比较，才将网络犯罪与计算机犯罪与传统犯罪相互区别，厘定了自身特定的本质及内涵。

二、中国网络犯罪现状分析

在阐述这一问题之前，必须指出，由于学界和实务界研究计算机犯罪与网络犯罪的混沌状态，很难找到极为准确的网络犯罪数据。目前中国调查统计的大部分数据，要么是网络违法犯罪的整体数据，要么是计算机犯罪与网络犯罪的总体数据。因此笔者只能通过对上述数据进行基本分析后，得出我国网络犯罪的现状。理论及实务界尽快搜集整理专门的网络犯罪数据是做好研究的当务之急。

㈠ 数量和涨幅

《第31次中国互联网络发展情况统计报告》显示，中国上网计算机数量、上网用户人数的增幅均位居世界前列。计算机网络在中国的迅猛发展，也使得相关的犯罪迅速滋生蔓延，愈演愈烈。

据中国警察机关的统计，1999年公安机关；立案侦查的计算机违法犯罪案件仅为400余起，2000年剧增为2700余起，2001年达到4500余起，其中90%以上的计算机违法犯罪案件牵涉网络。[13]

据公安部网络安全保卫局有关负责人介绍，从2008年开始，中国的网络犯罪数量便开始以年均30%的速度快速增长，在今后较长一段时间内，网络犯罪都将呈现持续增长趋势。[14]

中国公安人民大学警务改革与发展研究中心发布的《2012年中国互联网违法犯罪问题年度报告》显示，2012年我国网络犯罪依然保持高发态势，受害人规模及涉案金额均十分巨大。仅2011年7月至2012年7月间，中国估计有2.57亿人成为网络犯罪的受害者，经济损失高达人民币2890亿元。同一时期，被网络犯罪侵害的在线成人网民达72%，即每天有超过70万名中国网民遭受网络犯罪的侵害，平均每分钟有489名受害者，每位受害者的平均损失达人民币1126元。[15]

尽管由于统计标准的差异，上述统计数字与中国网络犯罪的真实情况会发生多多少少的不同，但是根据上述资料，我们不难看出，中国的网络犯罪无论在犯罪数量还是增长幅度上均保持着高压态势，不容乐观。

㈡ 分布状况

根据理论分析和司法数据，我国目前网络犯罪集中分布于以下领域：

1. 计算机病毒犯罪

计算机病毒犯罪是指编制或者在计算机程序中插入破坏计算机功能或者数据，影响计算机使用的计算机指令或者程序代码。我国计算机病毒犯罪呈持续快速上涨趋势。

2. 非法侵入计算机系统犯罪

非法侵入计算机系统犯罪，俗称黑客犯罪。该种犯罪在我国时有发生，受害者众多。

3. 网络诈骗、盗窃、贪污贿赂等犯罪

关于此类犯罪，笔者之前已经对其以信息为依据，与传统犯罪进行了区分，此处不再赘述。

13) 赵秉志：《中国网络犯罪现状》，中国刑事法治网，2007年2月2日。

14) http://www.sina.com.cn 2012年07月27日 09:49 中国广播网

15) 《2012年中国互联网违法犯罪问题年度报告》

4. 网上侵犯知识产权犯罪

近半个世纪，光电以及计算机等新技术的发展，使侵犯知识产权的犯罪变得更加便捷，而且从根本上改变着知识产权法上的许多概念。

5. 网络赌博、色情犯罪泛滥

色情和赌博也借着网络等高科技的东风，换上信息犯罪的外衣，日益成泛滥之势。

当然，上述所列绝不是网络犯罪的全部，而是其中多发常见的部分。或许随着计算机及网络的日益普及，网络犯罪还会呈现出新的分布状态。

三、中国网络犯罪之发展趋势

众多专家学者在认真观察思考我国网络犯罪现状的基础上，对中国网络犯罪的未来发展趋势进行了预测。结合上述《2012年中国互联网违法犯罪问题年度报告》，笔者认为，未来一个阶段，中国网络犯罪将逐步呈现出以下发展趋势：

1. 犯罪主体更加低龄化

纵观近年来的网络犯罪，主体低龄化的趋势已经相对明显。以2012年为例，湖北省破获的网络犯罪案件，30岁以下的犯罪人占到了90%。在徐州警方破获的网络犯罪案件中，仅90后边几乎占据了犯罪总人数的"半壁江山"。毫无疑问，随着青少年触网的时间日益早期化以及学校计算机、网络知识教育的逐步普及，精通计算机网络技术的未成年人将迅速增长，网络犯罪主体更加低龄化的趋势不可避免。

2. 犯罪主体更加大众化

伴随着中国教育方式的变革，网络教育、远程教育、自学自考等多种知识获取途径不断发展，加之计算机教育的早期化和普及化，愈来愈多的公众接触并日益熟悉网络、计算机，计算机、网络技术也再不是人们可望而不可及的高科技，而将逐步演变为人们生存与生活所需的必备技能之一。因此，与早期的计算机网络犯罪主体精英化不同，未来的网络犯罪必然更加社会化和大众化。

3. 犯罪日趋产业化和集团化

历经了近些年的发展，网络分子们日益形成了完整的产业链条，不仅在犯罪链条的每一个环节，分工明确、相互配合，功能不断细化，同时促进了结构严密庞大的犯罪组织的形成。最终的结果是网络犯罪将愈趋产业化和集团化，社会危害将更加严重。

4. 新型网络犯罪终端不断涌现

赛门铁克对来自24个国家和地区的13000名成年人进行了走访调查，调查结果显示，新型网络犯罪正逐步转向各种移动网络设备。这也就意味着网络犯罪中计算机不再一统天下，随着科学技术的不断进步和发展，各种新型网络犯罪终端设备将持续涌现。

5. 传统犯罪逐步网络化

网络犯罪产生初期普遍集中在一些新型犯罪和少数特定领域，而对传统犯罪领域少为光顾。随着社会和技术的发展，这种现象早已被打破，传统犯罪正在逐渐网络化，或者说网络犯罪正在逐步向传统领域渗透。

6. 犯罪跨国化将更加明显

国际交流合作日益频繁，民众的生存与发展领域不断扩大，际遇障碍逐步消除，现实世界的上述变化也必将一定程度上折射于虚拟世界。加之网络本无国界，缺乏物理时空的限制，网络犯罪必然会朝着跨国化和国际化方向发展，跨境网络犯罪将不断攀升。

7. 网络本身将成为阻止犯罪的有利因素

网络自产生以来，网络犯罪便如影随行。网络的发展促进了网络犯罪的发生已是不争的事实。但是，随着网络主流文化日益形成，网络安全防护体系日益完善，网络自身也将逐步成为抑制网络犯罪的重要力量。16)

无论如何，网络犯罪的发展远未触底，其未来仍有可能持续保持高位增长态势。新技术新产品层出不穷，网络服务将更为广泛便捷，而网络主流文化尚有待形成，法律规范仍待继续完善，众多因素将促使网络犯罪不断呈现出新趋势。只有在省察网络犯罪现状的基础之上，认真思考认识网络犯罪的未来发展趋势，才能高瞻远瞩，高屋建瓴，为未来网络犯罪的依法治理之路夯实基础，寻找进路。

四、中国网络犯罪之原因省察

研究网络犯罪，旨在网络犯罪的预防，上述网络犯罪概念之厘定也好，现状与趋势的探究也罢，无疑都在为寻求犯罪原因，探索预防对策，搭桥铺路，而原因与对策二者间的关系，犹如病因与治病，只有病因诊断清楚，才能对症下药。

16) 孙景仙、安永勇：《网络犯罪研究》，知识产权出版社2006年版。

显然，网络犯罪的原因是一个十分复杂的庞大系统，犯罪结果的发生是系统内部众多致罪因素相互作用相互影响之复杂过程的产物。虽然在具体犯罪中，不同原因所发挥的作用不尽相同，但是当我们将网络犯罪视为一个整体进行综合研究时，每一个个因都必不可少，具有各自的意义和价值。

1. 经济原因

说到经济原因，不得不提到以下三个方面：

第一，近年来，在世界经济局势一片惨淡的大背景下，中国经济的快速持续增长确实令人瞩目。经济的发展迅速提高了国人的生活水平和生活质量。不必忙于生计的人们开始将目光转向精神需求的满足。这一趋势使得人们愿意，也有能力购买电脑，安装网络，并进行网络活动。网民和网络基数的扩大，客观上为网络犯罪的增长提供了客观基础。

中国的经济转型，提高人们生活水平和生活质量的同时，膨胀了很多人的经济

需求。一旦这种膨胀的需求得不到满足，便无形中打开了犯罪的源头。

第三，与此同时，计算机和网络技术之所以便捷高效的重要原因之一，就在于信息数据的集中性和其所代表的巨大价值。财富过于集中必然导致犯罪成本降低，犯罪收益增大，从而导致犯罪对犯罪分子的诱惑力明显增强，加上经济转型时期，人们经济利益需求巨大膨胀而导致的犯罪抑制力的降低，最终使得犯罪常常一促即发。

2. 技术原因

作为科技进步和科技革命衍生物的网络犯罪，其产生与存在势必与科技相关，因为任何科学技术都是一柄双刃剑，在人类社会发展路上披荆斩棘的同时，也必定会伤害人类自己。计算机与网络技术的发明和应用，将人类文明从工业文明推进入信息文明，完成了里程碑式的一步。然而，网络的开放性、脆弱性和复杂性等技术特征，也使得网络犯罪行为顺风顺水，搭上了信息化时代的快车。尤其是电子网络产品本身设计上的漏洞和安全上的缺陷更为网络犯罪大开方便之门，使网络犯罪一路长驱直入。

3. 文化原因

诚然，犯罪作为一种社会法律现象，首先是由一定的物质生活方式决定着，是社会物质生产方式矛盾的反应。但是犯罪作为有意识的人类行为，又总是为一定的思想意识和价值观念所支配。而思想意识和价值观念本身始终具有着特定的文化内涵。因此，从某种意义上说，犯罪本身亦是一种文化现象，是特定社会消极文化作用的产物。[17]

当代中国，传统文化土崩瓦解，适应市场经济发展要求的开放、自由、发展的现代文化尚

未完全成形；西方外来文化不断涌入，与中国传统文化激烈冲突；现实社会礼制文化经历巨大转型，虚拟世界网络主流正文化远未形成，暴力、色情等不良文化泛滥开花，使得网络科技为我们大开信息之门的同时，也为犯罪打开了汹涌的大门。

4. 教育原因

中国顺应信息化时代要求，加速计算机网络技术教育的同时，却忽视了网民自我管理、自我约束、自我负责等方面的心理和道德教育，形成了技术崇拜而道德漠视的风气。中国网络教育下，培养出大批只重技术提高，忽视规则遵守的网络公民，这些公民在规范引导缺失的情况下，势必成为网络犯罪人的后备军。

5. 制度原因

谈及制度原因，十分重要的两个方面是：

⑴管理制度。与世界其他国家相比，中国给世界留下的外在印象，似乎是义务多于自由，管理多于自治。实则不然。一方面中国网络缺乏整套完善的管理制度，另一面既存的网络管理制度又往往是"装点门面"、"束之高阁"、"一纸空文"。

⑵法律制度。法律本身就具有滞后性，但其滞后性的特点在控制网络犯罪方面表现得尤为明显。就数量而言，中国规范网络安全及运行的法律文件，确实不在少数，但是法律文件大多为行政规章，行政法规尚不多见，更遑论行政法律和刑法规范。另外大量的法律文件，内容相互重复、抵触，难以落实也是制约犯罪打击实际效果的重要因素。

当然，除此之外，诱发网络犯罪的原因可能还有很多，从不同的角度观察也往往会得出不同的结论。但是若论及影响网络犯罪的主要因素，或许不外如此。

五、中国网络犯罪之立法现状

影响网络犯罪的因素固然很多，但是部分因素人力难违，有些因素虽人力可改，但是由于专业所限，本文也无法深入论及。在对网络犯罪基本问题有所认识的基础之上，本文只想着力就中国网络犯罪的法律规制问题进行深入探讨。

随着互联网络的发展，我国网络犯罪立法从无到有，基本形成了相对完整的法律体系。对于保障网络安全，遏制网络犯罪发挥了积极作用。

17) 孙景仙、安永勇：《网络犯罪研究》，知识产权出版社2006年版。

㈠ 根本法

中华人民共和国宪法是我国的根本大法，在宪法中并未涉及网络及网络犯罪的具体规定。但是我国宪法第40条规定：中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

根据该条规定及其精神，电子邮件应属于通讯自由和通讯秘密的保护范围，任何非法截取、毁弃他人电子邮件或者私自查看他人电子邮件的行为均属于违法犯罪行为。

㈡ 基本法

在我国，基本法是指必须由全国人民代表大会通过的重要法律，包括刑法、民法、行政法、刑事诉讼法、民事诉讼法、行政诉讼法等。目前我国涉及网络犯罪的基本法有：

1. 刑法。

⑴刑法典

1997年修订后的刑法典285、286、287条对计算机网络犯罪进行了具体规定：

①285条：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违法国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

②286条：违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修

改、增加的操作，后果严重的，依照前款的规定处罚。

故意制造、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

③287条：利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

⑵刑法司法解释

2000年4月28日最高人民法院发布了《最高人民法院关于审理扰乱电信市场管理秩序案件具体应用法律若干问题的解释》。《解释》全文十条，主要是关于刑法典第287条的相关解释。

2. 刑事诉讼法

2013年1月1日生效的《中华人民共和国刑事诉讼法》的任务，是保证准确、及时地查明犯罪事实，正确应用法律，惩罚犯罪分子，保障无罪的人不受刑事追究。网络犯罪作为一种犯罪，刑事诉讼法也是查明网络犯罪事实，惩罚网络犯罪主体的程序性保障法律。另外，修改后新颁布的《中华人民共和国刑事诉讼法》第48条明确规定证据的种类中包括电子数据。这无疑是查明网络犯罪，打击网络犯罪分子的有力保障。

㈢ 一般法

在根本法和基本法之外，我国还有全国人民代表大会常会委员制定的2部与网络犯罪相关的一般法。

1. 《全国人民代表大会常务委员会关于维护互联网安全的决定》

该决定于2000年12月28日由第九届全国人民代表大会常务委员会第十九次会议审议通过，该决定明确规定了应追究刑事责任的5类网络犯罪行为：

⑴侵犯网络安全的网络犯罪行为；

⑵侵犯国家安全与社会稳定的网络犯罪行为；

⑶侵犯社会主义市场经济秩序的网络犯罪行为；

⑷侵犯人身、财产等合法权益的网络犯罪行为；

⑸其他。

2. 《中华人民共和国电子签名法》

该法于2004年8月28日由第十届全国人民代表大会常务委员会第十一次会议审议通过。该法共36条，其中第32、33条分别规定了依法构成犯罪的，应当依法追究刑事责任。

㈣ 行政法规和行政规章

国务院、公安部等各部门相继颁布了大量的行政法规及行政规章。其中多数行政法规和行政规章中都有"符合相关情况，依法追究刑事责任"的规定。

六、中国网络犯罪法律规制之困境

我国网络犯罪立法虽已取得了一定成就，但是问题依然存在，并随着网络技术的飞速发展，新问题与新矛盾不断涌现，立法的滞后性尤为突出和明显。概括起来，主要包括以下几个方面：

㈠ 法律规制滞后性尤为突出

与变动不居的社会现实相比，法律本身就具有滞后性。法律的滞后性是法律稳定性与可预测性无法避免的附带属性。然而，在计算机、网络领域，信息时代知识的大爆炸以及网络科学技术的飞速发展，使得法律的滞后性变得尤为突出和明显。即使不断借鉴国外立法经验，我国网络犯罪方面的立法仍表现出十足的保守性，应景性法律层出不穷，前瞻性法律鲜为少见。

㈡ 倚重法律规制，忽视非法律手段运用

如前所析，中国网络犯罪治理过程之中，虽颁布的基本法和一般法为数不多，但是却颁布了极其大量的行政法规和部门规章。体系之庞大，不容小觑。但是，在网络犯罪控制过程中，技术安全漏洞层出不穷，网络管理相对滞后，浮于形式和表面，社会引导和教育更是差强人意，完全没有发挥应当具有的作用。

上述事实均可说明，中国网络犯罪的治理，太过倚重法律规制，而忽视了其他非法律手段的投入和使用。

㈢ 业已形成的法律规制体系本身不合理

根据上述我国网络犯罪的立法现状来看，法律体系庞大有余，但是体系结构有欠合理，不同效力级别的法律之间各自为战，衔接不足，留有大量法律空白。众多的行政法规和部门之间也存在内容混杂，交叉重复，或相互冲突，难以执行等问题。

另外，过于强调刑法的规制作用。动辄要求重新立法，或者重新修改解释刑法。笔者认为，借鉴世界各国相关立法，结合我国具体的社会发展现实，进行网络犯罪专项立法的时机还远未成熟。而且对于刑法的修改也不宜过于频繁，应当在充足调研的基础之上，进行成熟的刑法完善。

不得不承认，网络犯罪确实对传统刑法理论提出了诸多挑战，学者们也进行了诸多讨论，一如犯罪主体问题，犯罪形态问题，共同犯罪问题，刑罚与社会保安处分等等。笔者并不反对在理论与司法实务界研究成熟的基础之上，对刑法条文做出审慎的调整，但是笔者反对那种头痛医头，脚痛医脚，无视刑法稳定性与协调行，缺乏前瞻性盲目的修葺乱造。

㈣ 网络犯罪相关概念缺少科学界定

这一点笔者上文已经简单提到，尤其以网络犯罪的概念为例，至今学界和实务界都没有形成对其的科学定义，反而在计算机犯罪与网络犯罪，犯罪学定义与刑法学定义等问题之间纠缠不清。

㈤ 区域间国际间的交流合作需进一步拓展

上文有过强调，网络没有国界，不存在物理属性上的时空制约，网络的开放性和流动性也很容易使网络犯罪突破区域和国界的限制，具有跨区域和跨国家的特征，从而导致受害人遍及各个地区和各个国家。同时，网络犯罪的跨区域和跨国家的特征，也必然使得公检法机关对犯罪调查取证等工作更加困难。

而且事实已经证明，网络将逐步与恐怖犯罪一样，很难成为某个国家单枪匹马就可以良好治理的问题。而就目前的国内形势来看，区域间、国家间的网络犯罪司法协作相当匮乏，这不仅阻碍了司法机关对案件的侦破可能和侦破速度，更助长了犯罪分子的嚣张气焰。

七、中国网络犯罪法律规制的发展与完善

结合上述三个方面，笔者认为，为了更好地治理网络犯罪，应该从以下五个方向着力进行：

(一) 法律与非法律手段的二元治理模式

治理犯罪最立竿见影的手段非法律手段莫属，但是法律手段却并非最为长远有效之计。一如医者所言，猛药起效快却亦伤身。因此，从社会发展与进步的长远角度来看，犯罪治理绝不能仅靠法律手段一蹴而就，而理应法律与非法律手段齐抓共举，实现二元化治理。

非法律手段的治理主要体现在：

1. 进行网民网络入门教育和引导

上文曾简单提到过，我国计算机网络技术教育的同时，恰恰忽略了网民的网络入门教育和引导。网民在接触网络之初，便应接受入网规范的指导，学会如何在享受网络资源和网络自由的同时，不侵犯他人的合法权利，进行自我控制和自我管理。

2. 加强网络伦理道德建设，弘扬主流网络文化

现实世界与虚拟世界存在着明显差别，正因如此，适用于现实世界的行为规则不一定完全适合虚拟世界，适合于现实世界的道德文化，也不一定适应虚拟世界。所以，作为有别于现实世界的活动空间，虚拟世界应当进行自己的网络伦理建设和网络文化建设，从而使网民自觉抵制暴力、色情等网络亚文化，远离各种网络犯罪。

正如个别学者所说，犯罪，归根到底是"人"的问题。法律、技术、管理对策，都不能实现对人的内化控制，网络活动本身就缺乏现实监督，内化性监督对网络犯罪人而言更为重要。因此，做好"人"的工作，对网络犯罪人进行内化控制，使之建立起免疫于网络犯罪的道德屏障尤为重要。

那么何谓网络文化呢？中国社会科学院社会学研究所的沈杰先生将其定义为"人们在互联网这个特殊世界中，进行工作、交往、学习、沟通、休闲、娱乐等所形成的活动方式及其所反映的价值观念和社会心态等各方面总和"。[18] 积极健康的网络文化抑制网络犯罪，消极堕

18) 转引自许秀中：《网络与网络犯罪》，中信出版社2003年版。

落的网络文化催生网络犯罪，因此，只有尽快塑成并积极弘扬健康主流的网络文化，网民才有可能在诸多的诱惑面前，保有足够的冷静和克制，坚决对网络犯罪说不。

3. 行业自治组织和自治规章

庞大的社会组织，管理和法制的触角很难延伸到社会的角角落落。即使管理和法制有如此强大的功效，但其作用也会在不断下放的层次中递减。俗话说"县官不如现管"，说的就是此理。传统中国社会极为重视社会的中间力量，极为强调行业内部的自理和自治，这或许是中国传统社会主要以礼治天下的要义所在。

虚拟世界中，法律的触角更容易为虚拟的空间所消解。因此，更应当重视网民的内部自治以及信息技术行业内部本身自我组织和自我管理。

4. 加强网络安全管理

总结各国网络发展的经验教训，网络安全漏洞频发，网络安全管理效率低下，是刺激网络犯罪的诱因之一。因此，加强网络安全管理，严格电子产品的设计、生产和制造，从源头上堵塞安全漏洞，建立专门的网络安全权利保护机构和管理监察体制，规范网络服务商和从业者的责任，是进行网络犯罪法律治理的有效方式。

5. 加强网络技术支持

网络做为一种先进的科学技术，催生了技术型的网络犯罪。因此就网络犯罪而言，传统的治理方式疗效并不显著。俗语说"解铃还须系铃人"。抑制网络犯罪的决定性力量或许仍旧在科技本身。研发新的网络安全防护产品，培养专业的网络巡查人员，组建高技术含量的网络安全治理队伍，都将为网络犯罪治理工作提供技术支持。

如果说法律是"他治"的话，上述五个小方面均在强调"自治"，只有将"他治"和"自治"完美的结合起来，法律才能更好得发挥效用。

㈡ 网络犯罪刑事政策的选择

我国目前关于网络犯罪刑事政策进行研究的学者并不多见，在这方面存在着大量尚待开发的空间。按照我国学者许秀中的观点，网络犯罪刑事政策是刑事政策主体（包括完全意义上的和不完全意义上的刑事政策主体）基于预防网络犯罪、控制网络犯罪以保障自由、维持秩序、实现正义的目的而制定、实施的准则、策略、方针、计划以及具体措施的总称。其认为我国关于网络犯罪的刑事政策包括以下四个方面：

1. 有关信息化及信息安全组织开展有效活动，指导整个网络工作

2. 制定有关网络信息安全的规范性文件，并逐步法律化

3. 领导们多次发表具体讲话指导网络安全工作

4. 司法方面的刑事政策[19]

显然许秀中学者所提供的是治理网络犯罪的极其具细的对策，而网络犯罪治理需要的，除了具体网络对策之外，似乎还需要基本性一般性的刑事政策指导。

尽管研究此方面的学者数量较少，但许秀中学者之外，还是有不少学者给予了网络犯罪刑事政策相当的关注，比如王作富教授、刘同航教授、靳高峰教授等等，并在治理网络犯罪的一般政策方面提出了自己的意见。结合诸位学者的观点，笔者认为，我国网络犯罪刑事政策的选择应当划分为三大基本层次：

1. 基本刑事政策

刑事犯罪与网络犯罪之间是一般与特殊、普通与个别的关系。但是无论网络犯罪如何不同，其归根结底属于刑事犯罪的一部分，具有刑事犯罪的基本属性和基本特征。因此，作为指导我国刑事立法和刑事司法的基本刑事政策，对于网络犯罪而言同样适用。

根据最高人民法院2010年发布的《关于贯彻宽严相济刑事政策的若干意见》，宽严相济刑事政策包含以下五个方面的内涵：

第一，贯彻宽严相济刑事政策，要根据犯罪的具体情况，实行区别对待，做到该宽则宽，当严则严，宽严相济，罚当其罪。

第二、要正确把握宽与严的关系，切实做到宽严并用。

第三、贯彻宽严相济刑事政策，必须坚持严格依法办案，切实贯彻落实罪刑法定原则、罪刑相适应原则和法律面前人人平等原则，依照法律规定准确定罪量刑。

第四、要根据经济社会的发展和治安形势的变化，尤其要根据犯罪情况的变化，在法律规定的范围内，适时调整从宽和从严的对象、范围和力度。要全面、客观把握不同时期不同地区的经济社会状况和社会治安形势，充分考虑人民群众的安全感以及惩治犯罪的实际需要，注重从严打击严重危害国家安全、社会治安和人民群众利益的犯罪。

第五、贯彻宽严相济刑事政策，必须严格依法进行，维护法律的统一和权威，确保良好的法律效果。

19) 许秀中：《网络与网络犯罪》，中信出版社2003年版。

其实早在2004年王作富教授就曾发文指出对待黑客等网络犯罪应当坚持两极化的刑事政策，对危险性黑客从重处罚，对温和型化黑客从轻处罚。[20] 这与后来宽严相济刑事政策所提倡的要义极其类似，宽严相济刑事政策对网络犯罪治理的指导意义恰恰也在于此。对那些由于缺乏法律认识、主观人身危险性不大，社会危害性不重的网络犯罪人，应坚持当宽则宽的原则，惩罚犯罪分子的同时，积极促进其悔过自新，尽早回归社会。对于社会危害性极其严重的集团网络犯罪、共同网络犯罪等犯罪分子，理应坚持当严则严的原则，应当严格依法追究其刑事责任。

在网络犯罪治理中，把握宽严相济刑事政策，既有利于对误入歧途的犯罪分子进行教育和改造，又有利于对罪行极其严重，社会危害性巨大的犯罪分子进行严厉的惩治和惩罚。

2. 具体刑事政策

作为具有自身独特属性和本质的网络犯罪，对其进行法律规制的过程中，理应为其制定专门刑事政策。

⑴综合治理刑事政策。

当今中国社会是一个经济利益、价值追求以及意识形态不断多元化的社会，因此生成于此种社会条件下的网络犯罪的治理方式，也应当坚持综合治理刑事政策，积极探索综合多元化的治理模式。在这种刑事政策的指引下，网络犯罪的治理应当从经济、政治、技术、管理、法律、文化、道德等多方面齐抓共管，综合治理。

⑵合作治理刑事政策。

上文已然提到，由于网络是一个建立在网络信号基础之上的虚拟空间，凡是网络信号能够覆盖的地方，都是网民能够自由进入的虚拟世界，因此，网络的存在打破了地区与地区、国家与国家之间的界限，使世界真正的实现了一体化，也使得跨国犯罪简单易行。而正是网络犯罪跨地区、跨国家的特点，往往导致网络犯罪的受害人不会仅仅局限于某一个狭小的领域，而是会遍及各个地区，甚至各个国家。网络犯罪的现状也不断证明，其与恐怖犯罪一样，任何国家都不能独善其身，也不具有独自应对网络犯罪的巨大能力。因此，必须与世界其他地区和其他国家积极交流，不断寻求在统一国际立法、国际司法协作以及国际管辖等诸多问的全面治理合作方式。

⑶预防为主打击为辅的刑事政策

20) 王作富、庄劲：《黑客行为与两极化刑事政策》，载《湖南社会科学》2004年第期。

无论人们是否承认，人类社会都日益迈入了一个更加危险的时代。危险一方面来自于人类危险意识的提高，而另外一方面则来自先进科学技术给人类发展带来的负面作用。科技乐观主义者或许会反驳，任何一项科技进步都会带来一定的风险，但事实却在不断证明，以往时代的任何科技进步都不曾像现代科技革命一样，带来如此巨大、无法预测、无法控制、甚至无法逆转的巨型灾难。

网络做为现代科技的一种，网络犯罪的社会危害在某种程度上也具有极其巨大、无法预测、无法控制和无法逆转等显著特征。因此，对网络犯罪的治理，事前的预防远优越于时候的惩罚。当然预防提前的情况下，必须同时坚持下一项刑事政策。

⑷自由与安全并重刑事政策

建立在自由、共享基础之上的互联网络，自由是其建立的宗旨，也是其不懈追求的目标。但是世界中没有绝对的自由，任何绝对的自由，都将构成对他人自由的妨碍和侵犯。缺乏网络安全保障下的网络自由才是真正的不自由。

因此，网络犯罪的治理必须平衡好自由和安全之间的关系，既不能以牺牲自由为代价换来毫无意义的安全，也不能以牺牲安全为代价追求海市蜃楼的绝对自由。

㈢ 律部门之间的联动治理

解决中国目前网络犯罪的法律规制困境，就要实现各法律部门之间的联动治理。这是由我国计算机网络管理的多元局面造成的。只有在各部门之间实现联动治理，才不至使各部间的努力相互抵消，从而实现加功的效果。

1．联动立法

所谓联动立法，即各部门立法时都应有整体全局观念，与其他部门之间相互了解，相互协调，相互配合，而不能各自立法，各自为政，以致最后的法律或者相互重合，或者相互冲突，最终无法落实和执行。

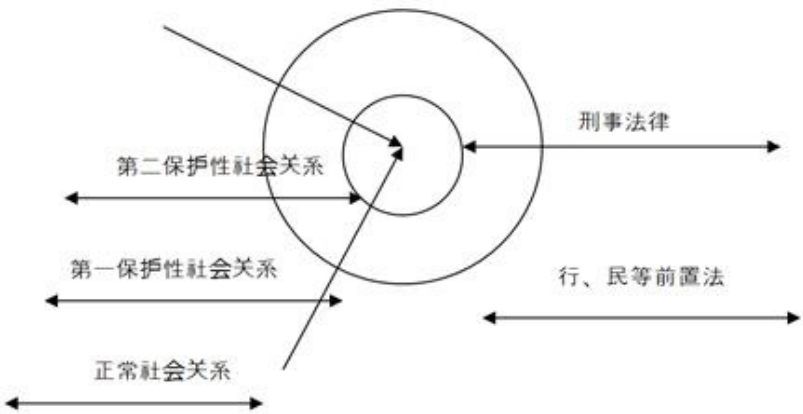
2．联动司法

所谓联动司法，即各部门在司法时要相互配合，共同努力。这是由我国犯罪基数大，而司法技术人员相对匮乏的现实情况决定的。

㈣ 行政、民事在先，刑事保障

根据法学基础理论，刑法作为社会统制手段，具有补充性的特征，是其他一切法律的后盾，是最后的保障法。从整个法秩序的角度思考，当其他法律部门的介入足以解决有关问题时，刑法便不应介入，也就是说，刑法只有在国家、社会或者个人以其他手段无法有效保护其合法利益而只能通过刑罚才能有效进行保护的情况下才能使用。这既符合刑法谦抑原则，也符合法律经济原则。一般来说，只要人们正常行使权利，履行义务，即产生正常社会关系。一旦人们非法行使权利或者不依法履行义务时，正常的社会关系就遭到破坏，需要利用法律来进行纠正和恢复。此时的社会关系就突破正常社会关系领域，首先进入行政法、民法调整的范围，接受行、民调整后形成第一保护性法律关系，此时的不法行为便具有了行政违法性或者民事违法性，构成行政违法行为或者民事违法行为。而如果行政违法行为或者民事违法行为继续进行，程度继续加重，行、民等前置法已不足以保护受到损害的社会关系时，向内延伸，其就会突破行、民领域，进入刑法调整的范畴，并在经过刑法调整后形成第二保护性社会关系。[21]

如图所示：



21) 田宏杰：《行政优于刑事：行刑衔接机制构建》，载《人民司法》2010年第1期。

如图所示，国家和社会的治理首先应依赖行、民等前置法进行法律调整，以使被破坏的社会关系恢复到正常情况；只有犯罪行为突破行、民等前置法，进入刑法领域，前置法已无法规制该行为，使被破坏的社会关系恢复到正常状态时，刑法才发挥其保障性后盾的作用。

由此看来，刑法自身的特殊属性，就决定了网络犯罪的治理过程中，不应过分倚重刑法的作用，而应更加注重行、民等前置法律的作用。因此，迅速弥补网络不法行为在前置法上的空白，迅速完善我国行政法、民法等前置法律，才能使其成为打击网络违法犯罪行为，减少网络犯罪的有利工具。

㈤ 刑法的自身调整与完善

当然，注重行、民等前置法律在治理网络违法犯罪中的作用，并不意味着可以将刑法这一规制手段弃之不理。

社会在进步变迁，犯罪也在发展变化，刑法也应结合前置法，考虑自身的调整与完善。根据学者们的广泛讨论，刑法的自身完善应从以下几个方面进行：

1. 犯罪圈定

如前文笔者所指出，我国刑事立法并未能认真区分计算机犯罪与网络犯罪二者之间的关系。这种不加区分的立法规定，必将导致不能根据二者的具体特征及危害情况规定适当的刑罚，从而也致使犯罪打击的不利效果。

另外，虽然刑法在治理网络犯罪过程中，应在、行、民等前置法之后，发挥其保障行作用。但随着行、民法律的完善，网络违法行为的不断呈现，刑法领域也应跟随其进行相应犯罪圈的调整，以适应打击网络犯罪的现实需要。

2. 犯罪主体

我国刑法第17条规定：已满十六周岁的人犯罪，应当负刑事责任。

已满十四周岁不满十六周岁的人，犯故意杀人、故意伤害致人重伤或者死亡、强奸、抢劫、贩卖毒品、放火、爆炸、投毒罪的，应当负刑事责任。

然而，根据网络犯罪的现实情况和未来发展趋势，网络犯罪的主体将日趋年轻和低龄化，传统的刑事责任年龄规定正在不断受到挑战。

且根据我国刑法30条的规定，单位实施危害社会的行为，只有法律规定为单位犯罪时，才应当负刑事责任。显然我国刑法285、286、287条并未明确将网络犯罪中规定单位犯罪。

然而根据法律条文内涵所指以及网络犯罪的现实情况，单位确实可以成为网络犯罪的主体。例如单位决定并组织实施的制作、传播计算机病毒的行为。而且司法现实中确也出现了单位网络犯罪的真实案例。因而完善刑事立法，从立法上明确规定单位可以成为网络犯罪的主体无疑是最佳的路径选择。

3. 共同犯罪

根据前文所述，网络犯罪在未来发展中将愈发呈现产业化和集团化的趋势。这种趋势下，网络犯罪将更多的表现为共同犯罪。如何结合我国网络犯罪的实际情况，确定共同犯罪人的地位与作用，并在共同犯罪人之间合理分配刑事责任，从而达到一直共同网络犯罪的目的，似乎对共同犯罪相关理论提出了巨大的挑战。

4. 刑罚完善

根据我国刑法的规定，285、286条中对网络犯罪规定了自由刑和资格刑。但考虑到计算机网络犯罪主体的特点，从各国刑法规定来看，一般应对其规定一定的资格刑，剥夺犯罪分子在一定时间内从事相关职业，进行相关活动的自由。

㈥ 国际间统一立法及司法协作

随着网络技术的发展，网络犯罪问题日益成为全社会、全球性问题。大量专家不断意识到并指出，仅仅依靠一国的有限力量，已远远无法满足遏制全球性网络犯罪的需要，建立各国和全球性的国际多边合作机制已成为大势所趋。

1. 管辖权问题

与传统犯罪相比，网络犯罪呈现出全球性和辐射性特征，其影响范围十分广泛。这将无可避免的导致网络犯罪管辖权上的冲突，以及由此带来的引渡、司法协作和域外判决承认等多方面的问题。

与传统国界不同，网络空间很难准确的划分边界。传统管辖制度中以行为地和结果地为主属地中心主义将受到严峻挑战，部分学者建议网络犯罪管辖问题上可以采用民法领域中的协议管辖制度，或许是可以尝试之举。

2. 国际统一立法

以欧洲刑事法一体化为背景，笔者认为，网络犯罪正如恐怖犯罪一样，应积极地寻求全球治理，那么不可避免的就需要统一的法律标准。当然无视国家主权，倡导去国家化完全一致

的法律标尺，似乎过于理想，但是在世界范围内建立最为基本的，且能为各国普遍接受的网络犯罪最低立法，或许还有可行之机。

因此在区域一体化的基础上，积极推进网络犯罪全球性的网络基本立法，出台国际性网络犯罪公约，不失为明智之举。

3. 国际司法协助

当今世界是一个开放的世界，各国之间的交流与合作广泛延伸至经济、政治、文化等诸多领域。在跨国网络犯罪日益频繁，社会危害日益严重的情况下，各国积极开展打击网络犯罪的跨区域和跨国合作，不仅有利于维护各国的网络安全与社会稳定，也有利于各国司法经验的交流与发展。

此外，建立网络犯罪国际监察组织和协调组织，更有利于各国及时发现跨国网络犯罪，便于各国网络犯罪的联合治理和多方协作。

总而言之，学界对网络犯罪的研究仍然处于探索阶段，不从根本上解决网络犯罪的定性问题，不彻底理顺计算机犯罪与网络犯罪之间的关系问题，网络犯罪的研究即使呈现出繁荣之势，也只是空中楼阁，终将推到重来。这将是学术资源的巨大浪费，也是对中国法治建设与发展极其不负责任的态度。忽略网络犯罪中的根本问题，在细枝末节上的辛勤耕耘，只能为陋室添花，是治标不治本的暂时之选。

文章已到尾声，笔者对于网络犯罪的界定仍有许多困惑不解之处，尚需进一步思考整理。但愿笔者在此问题上的努力，可以抛砖引玉，为网络犯罪基础理论的研究吸引更多学界探索的目光。

至于文章中关于网络犯罪现状、未来发展趋势，法律立法现状，法律规制的困境及完善等各个方面的探讨，均是建立在前辈学者的研究基础之上，笔者也未形成太多独到的见解。只就刑事政策一部分，笔者偶得一些简单的想法，希望不至于贻笑大方之余，可以使更多学人进入网络犯罪刑事政策这块荒蛮之地，开垦并收获累累硕果。

参考文献

著作类

1.李双其：《网络犯罪防控对策》，群众出版社2001年版。

2.刚主编：《极端及犯罪疑难问题司法对策》，吉林人民出版社2001年版。

3.志刚主编：《网络犯罪定性争议与学理分析》，吉林人民出版社2001年版。

4.【法】达尼埃尔·马丁、弗雷德里克-保罗·马丁合著，陆建平译：《网络犯罪 威胁、风险与反击》，中国大百科全书出版社2002年版。

5.许秀中：《网络与网络犯罪》，中信出版社2003年版。

6.杨正鸣主编：《网络犯罪研究》，上海交通大学出版社2004年版。

7.皮勇：《网络犯罪比较研究》，中国人民公安大学出版社2005年版。

8.孙景仙、安永勇：《网络犯罪研究》，知识产权出版社2006年版。

9.孙春雨编著：《计算机与网络犯罪专题整理》，中国人民公安大学出版社2007年版。

10.于同志：《网络犯罪》，法律出版社2008年版。

11.于志刚：《传统犯罪的网络异化研究》，中国检察出版社2010年版。

12.于志刚主编：《共同犯罪的网络异化研究》，中国方正出版社2010年版。

13.季境、张志超主编：《新型网络犯罪问题研究》，中国检察出版社2012年版。

论文类

1.杨正鸣：《网络犯罪概念论》，载《犯罪研究》2002年第2期。

2.刘守芬、孙晓芳：《论网络犯罪》，载《北京大学学报》2001年第3期。

3.冯卫国：《试论网络犯罪及其控制对策》，载赵秉志主编：《新千年刑法热点问题研究与适用》（上），中国检察官出版社2001年版。

4.范德繁、于宏：《针对网络犯罪之认定探讨——兼评刑法相应立法的完善》，载《法制与社会发展》2001年第5期。

5.中华人民共和国计算机管理监察司：《计算机安全必读》，群众出版社1991年版。

6.王作富、庄劲：《黑客行为与两极化刑事政策》，载《湖南社会科学》2004年第期。

7.田宏杰：《行政优于刑事：行刑衔接机制构建》，载《人民司法》2010年第1期。

8.赵秉志：《中国网络犯罪现状》，中国刑事法治网，2007年2月2日。

新闻类

1. 互联网信息中心发布《第31次中国互联网发展情况统计报告》，网址：http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201301/t20130115_38508.htm。

2. 中国人民公安大学警务改革与发展中心发布《2012年中国互联网违法犯罪问题年度报告》，网址：http://special.cpd.com.cn/n15549540/index.html。

〈부록 4〉 '중국에서 사이버범죄 관련 형사정책' 원문

网络犯罪刑事政策论纲

时延安* · 陈磊

摘要：网络将犯罪从线下聚焦到网上。打击网络犯罪、维护互联网用户安全，成为刑事政策的重中之重。通过理性的政策架构，以预控技术对抗犯罪技术，平衡潜在的价值冲突，既能有效预防和惩治网络犯罪，又能避免过度使用控制网络危险的技术手段而侵犯虚拟世界同样存在的基本权利以及技术发展的潜在可能。

关键词：网络犯罪；刑事政策；技术对抗技术；价值平衡

一、导言

网络给人们的生活带来了革命性的变化。它以我们现在甚至可能不能想象的方式为谋求社会利益的努力提供了空前机遇，如教育、科研、商务、娱乐和谈论公共事务。另一方面，它也会给那些希望将互联网作为工具来便利其犯罪活动的个人提供了巨大的、低成本的、潜在的匿名方式来进行犯罪活动，如欺诈、色情文学的销售或分销、枪支或毒品或其他不受法规保护的违禁物品的销售、电脑软件的非法分销或其他受知识产权保护的创造性成果侵权。[1] 互联网技术沟通迅捷、信息共享和日新月异的特性，在增加社会交往可能性的同时，也增加了违法犯罪行为的可能性。据中国互联网数据中心的统计，截至2012年6月底，中国网民数量已经达到5.38亿，互联网普及率为39.9%。[2] 而据目前全球规模最大的针对个人用户的网络安全研究报告——赛门铁克诺顿网络安全报告显示，2012年网络犯罪致使全球个人用户蒙受的直接损失高达1100亿美元。在中国，2012年估计有超过2.57亿人成为网络犯罪受害者，所蒙受的直接经济损失达人民币2890亿元。84%的中国在线成人在以往的生活中曾遭受过网络犯罪侵害，而仅在2012年一年，被网络犯罪侵害的在线成人就达72%（即每天有超过70万名中国网民遭受网络犯罪的侵害，每分钟有489名受害者），在2012年一年平均每位

* 时延安，中国人民大学刑事法律科学研究中心教授；陈磊，最高人民检察院助理研究员。

1) 参见叶海涛摘译：《美国关于控制互联网犯罪的报告》，载《上海对外贸易学院学报》2000年第7期。

2) 中国互联网信息中心：《第30次中国互联网络发展状况统计报告》。

网络犯罪受害者蒙受的直接经济损失达到人民币1126元。[3] 数据不会说谎，互联网将人们的生活从现实世界聚焦到虚拟空间，但也已成为犯罪者最喜爱的温床。由此，打击网络犯罪、维护互联网用户的安全，理应成为刑事政策的重中之重。如何通过理性的政策架构，既能有效预防和惩治网络犯罪，又能避免过度使用控制网络危险的技术手段而侵犯虚拟世界同样存在的基本权利以及技术发展的潜在可能，应当成为研究者重点关注的课题。

二、网络犯罪的类型分析

(一) 学理上网络犯罪的范畴界定

我国学界对网络犯罪的界定有广义说和狭义说两种。狭义的网络犯罪概念是指利用计算机操作所实施的危害网络信息系统（包括内存数据及程序）安全的犯罪行为。[4] 依据狭义说，计算机和网络本身既是必需的犯罪工具，同时也是犯罪对象。网络犯罪仅包括刑法第285条的非法侵入计算机信息系统罪，非法获取计算机信息系统数据、非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统的程序、工具罪，第286条的破坏计算机信息系统罪。广义的网络犯罪概念是指在互联网上运用计算机专业知识实施的犯罪行为，包括以计算机网络为攻击对象或者以计算机网络为手段或工具的犯罪行为。[5]

我们认为，从研究的角度来看，狭义说界定的网络犯罪范围过窄。无论是以计算机网络为攻击对象或者以计算机网络为手段或工具的犯罪行为，都需要运用计算机网络专业知识。尽管以计算机网络为手段或工具的犯罪行为，比如刑法第287条规定的利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪，属于传统犯罪的范畴，但是因犯罪手段所具有的科技特征，这些犯罪在行为性质、危害程度、侦查取证、管辖地等方面已经与传统犯罪具有很大的差异，因此在研究时应当归入到网络犯罪一类，与传统犯罪有所区别。

立法者也持相同的态度。2000年12月28日第九届全国人大常委会第十九次会议通过《全国人民代表大会常务委员会关于维护互联网安全的决定》，以列举的方式将侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统，故意制作、传播计算机病毒等破坏性程

3) 参见新华网，“诺顿网络安全报告：网络犯罪致中国年损失2890亿元”，http://news.xinhuanet.com/legal/2012-09/12/c_113056800.htm，访问日期：2013年9月25日。

4) 参见赵秉志、于志远：《论计算机犯罪的定义》，载《现代法学》1998年第5期。

5) 参见刘守芬、孙晓芳：《论网络犯罪》，载《北京大学学报（哲学社会科学版）》2001年第3期。

序，擅自中断计算机网络或者通信服务等危害互联网的运行安全以及通过互联网窃取、泄漏国家秘密、情报或军事秘密，利用互联网煽动民族仇恨、民族歧视，利用互联网组织邪教组织等危害国家安全和社会稳定；利用互联网销售伪劣产品或者对商品、服务作虚假宣传，利用互联网损害他人商业信誉和商品声誉，利用互联网侵犯他人知识产权，利用互联网编造并传播证券、期货交易等虚假信息，在互联网上建立淫秽网站、网页等破坏社会主义市场经济秩序和社会管理秩序；利用互联网侮辱他人或捏造事实诽谤他人，非法截获、篡改、删除他人电子邮件或者其他数据资料，利用互联网进行盗窃、诈骗、敲诈勒索等侵犯个人、法人和其他组织的人身、财产等合法权利等犯罪行为明确界定为网络犯罪，予以重点、专项地预防和打击。

(二) 实践中网络犯罪的多发类型

整体而言，我国网络犯罪呈多发态势，但是犯罪类型比较集中。根据中国人民公安大学警务改革与发展研究中心发布的《2012年中国互联网违法犯罪问题年度报告》（以下简称《报告》），2012年全国公安机关累计破获涉网违法犯罪案件11.8万起，抓获犯罪嫌疑人21.6万余人。清理涉枪、涉毒、淫秽色情等违法信息572万余条，依法关闭网站（栏目）8万余个，整治互联网服务单位2.6万余家，关停违法网络帐号和通信码号1.1万余个。[6] 根据《报告》显示，我国网络犯罪的主要类型有网络诈骗、网络传销、网络色情、网络钓鱼、网络赌博、网络贩毒、网络贩枪、网络贩卖人体器官、网络非法集资、网络黑客攻击、网络贩卖假药、网络贩卖公民个人信息、网络敲诈勒索、网络传授犯罪方法、网络贩卖爆炸物品、网络贩卖剧毒化学品、网络拐卖人口、利用网络制造传播谣言、散布虚假恐怖信息以及利用网络窃取、泄漏国家秘密等。《报告》根据犯罪的受害者数量、涉案金额、危害度、影响度进行测算，归纳出了2012年度网络犯罪十大类型，分别是：网络诈骗、网络色情、网络传销、网络贩卖公民个人信息、网络钓鱼、网络赌博、网络黑客攻击、网络贩卖假冒伪劣产品、网络贩毒、网络非法集资。根据苏州市人民检察院课题组对苏州市2007-2010年网络犯罪调查分析，苏州市的网络犯罪也集中在网络诈骗、网络赌博、网络传播淫秽物品、网络卖淫、网络非法营销等类型。[7]

6) 参见中国人民公安大学警务改革与发展研究中心：《2012年中国互联网违法犯罪问题年度报告》。

7) 参见李赞等：《苏州市2007-2010年网络犯罪调查分析》，载《中国刑事法杂志》2011年第10期。

1．网络诈骗。随着网络的普及，一些传统的诈骗手段开始在网络上出现并不断演变、升级，网络的非直接接触式的信息传播和信息交流方式，正好弥补了面对面诈骗时，诈骗分子容易出现的心虚、紧张、面貌容易被识别等缺点，更容易诈骗成功。[8] 因此网络世界成为了诈骗犯罪的重灾区。网络诈骗方式主要包括网络中奖诈骗、QQ网络聊天诈骗、网络钓鱼网站或虚假网站诈骗、网络购物诈骗、网络彩票诈骗、网络股票诈骗、网络招聘诈骗、网络高考诈骗等。同时，新型的微信诈骗、网络传销诈骗以及冒充商业合作伙伴的网络诈骗也不断出现。其中钓鱼网站与诈骗网站尤其猖獗。根据中国电子商务协会可信电子商务推进中心、中国可信网站应用推进联盟和可信网站验证管理机构中网联合发布的《2012年中国网站可信验证行业发展报告》显示，截止2012年6月底，31.8%有网络购物经历的网民本人曾在网购过程中直接碰到钓鱼网站或诈骗网站，网购遇骗网民的规模保守估算为6169万。超过39.7%的网民损失额度超过500元。保守估算，每年因钓鱼网站或诈骗网站给网民造成的损失不低于308亿。[9]

2．网络色情。因网络传播的迅捷性、私密性、共享性，利用互联网传播淫秽物品和读淫的网络色情案件多发频发，涉及的受众广，危害性特别是对未成年人危害比较大。网络色情传播方式多样化，除传统的论坛型色情网站如论坛、贴吧、博客、微博客，社交型（交友型）色情网站，搜索引擎网站，音频视频网站外，还包括即时通信群组即网上即时通讯工具如qq群组及个人qq工具，手机网站，网络游戏网站等，以及利用移动智能终端应用程序平台、在线视频播放软件、网络共享网站（服务器）、网络资源下载工具等网络新应用技术传播网络色情等方式。

3．网络赌博。传统的赌博有物理空间的限制，而互联网的虚拟性使其能在短时间内聚集大量的群体，从而成为赌博业所青睐的场所。网络赌博主要涉及两种方式：一是传统的赌博转移到网络上，利用网络互动性强、隐蔽性强、支付方便、证据保全难等特点开展赌博活动，由于网络的即时性和跨区域性更有可能大大增加参赌的范围，从而使网络赌博的数额不断升级。另一种是网络游戏中衍生的一些赌博活动，即“变相的赌博类网络游戏”，涉及网络游戏服务、虚拟货币、第三方交易平台等多个环节，采取一些打法律“擦边球”的形式，赌资

8) 参见《报告》。

9) 参见中国电子商务协会可信电子商务推进中心、中国可信网站应用推进联盟和可信网站验证管理机构中网：《2012年中国网站可信验证行业发展报告》。

往往不直接与人民币挂钩。与前一类赌博方式相比，在界定上存在一定的困难。而这种网络赌博形式一旦发展起来，由于其相当的隐蔽性和我国目前庞大的网络游戏用户的存在，其传播范围可能更广、发展变化更快。

4. 网络谣言。近年来，利用互联网制作、复制、传播谣言、谎言等有害信息的事件时有发生，引起社会广泛关注。网络谣言传播具有突发性且流传速度极快，因此极易对正常的社会秩序易造成不良影响。从“女干部携巨款潜逃加拿大”，到“艾滋病患者滴血传播艾滋病”，再到“女大学生求职被割肾”，谣言最终都证实为谎言。2008年广元“蛆橘事件”让全国柑橘严重滞销，虫害谣言通过网络迅速传遍全国，仅在湖北一省造成的经济损失就达15亿元。[10] 2013年8月号称“谣翻中国”的知名网民“江淮秦火火”以涉嫌寻衅滋事罪、非法经营罪被刑事拘留，秦某在微博上先后注册了10个不同的网名，并与他人组成网络推手团队，伙同少数所谓的“意见领袖”、组织网络“水军”长期在网上炮制虚假新闻、故意歪曲事实，制造事端，并以删除帖文替人消灾、联系查询IP地址等方式非法攫取利益，严重扰乱了网络秩序。[11] 为此，2013年9月，两高就此类刑事案件的法律适用出台了专门的《关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》，明确何种网络造谣传谣情形构成犯罪，严厉打击网络造谣传谣。

5. 破坏网络系统安全。为了控制全球互联网，推行网络霸权，某些国家在互联网上“攻城略地”。为了获取所需情报，网络间谍非法入侵敌方或国外计算机网络，收集整理对方网络上的信息。为引起政府和社会的注意，“黑客行动主义者”会在网站的主页上留下醒目的留言，引起网络拥塞，或者在网页中嵌入某些激烈的反对观点。甚至可能在网站上加载“拒绝服务攻击”来造成站点瘫痪。为了获取非法利益，黑客会攻击盗窃用户网络银行帐号、游戏装备；利用黑客手段敲诈勒索或恶性竞争；攻击政府、金融、交通、电力、教育、科研等各个领域的公共服务信息系统。制作、出售黑客工具及教授黑客攻击技术已经形成地下产业链。

6. 网络贩毒。网络空间的虚拟性、网络活动的匿名性、指令的隐蔽性，使得贩毒活动从线下发展到网上，愈加猖獗。行为人一般都是通过专业的购物网站对伪装过的毒品进行交易，整个交易过程只需几个简单的操作就能完成，成本低、侦破难。2012年3月，吉林警方

10) 黄厚畅、张扬：《网络谣言害人害己，社会公众勿传勿信》，载《人民日报》2012年4月16日。

11) 李恩树：《“网络造谣者”如此兴风作浪》，载《法制日报》2013年8月21日。

查获一起横跨全国18个省市、涉案人员达400多人的特大网络贩卖毒品案，在这起案件中，QQ等网络聊天工具、淘宝等网络交易平台成了贩毒、吸毒的“秘密通道”。

7. 网络制假售假。网络电子商务的发展已经改变了人们的消费习惯，网购代替了实体店成为时下年轻人购物的首选。根据艾瑞咨询数据显示，2012年前三季度中国网络购物市场交易规模为7807.7亿元，超过2011年7665.8亿元的全年交易额，占中国前三季度社会消费品零售总额的5.2%。与此同时，网络上制假贩假横行。网络制假贩假主要包括假证、假印章、假烟假酒、假药、假生活用品等。根据深圳《晶报》调查，目前淘宝网上的假货比例超过三分之一，品种几乎涵盖了淘宝所有线上在售的商品，其中尤以化妆品、手机、服装、鞋子和珠宝首饰类为多。从中可以看出网络售假呈现品种多、数量大特点，且依托网店进行公开的售假行为，销售范围广。

8. 网络买卖枪支。《枪支管理法》明确规定禁止制造、销售仿真枪，大量不法商贩为了规避管制通过各种隐蔽手段贩售仿真枪，尤其是近几年随着网络购物的快速发展，网络贩枪成为了贩枪者最主要的贩枪途径。大批枪迷通过各种网络途径购买仿真枪来满足自己的兴趣爱好，对仿真枪的需求形成了一个巨大的买方市场，由此涌现出了一批暗藏在地下的黑色产业链，网络贩枪问题随之产生。

9. 网络恐怖活动。与传统的恐怖活动相比，网络信息传播更便捷迅速。网络具有极强的时效性，打破了时空对恐怖活动的限制，恐怖分子可以在第一时间内组织、策划、控制恐怖活动，而且利用网络实施的恐怖活动消耗的成本小，操作难度小，受众广，使得恐怖分子描上了网络的平台，利用网络组织恐怖活动、散布虚假恐怖信息。近年来接连发生了末日谣言、新疆恐怖分子利用网络进行恐怖犯罪活动、篮协网站被黑、雅虎服务器被黑等恐怖活动事件。

(三) 网络犯罪的特征分析

网络世界缘何犯罪多发？不仅是针对网络系统安全的典型意义上的网络犯罪，还包括传统犯罪（如诈骗、赌博、色情等）相继“转战”网上。原因就在于网络具有高科技、低成本、低风险、虚拟性等特点，这些也构成了网络犯罪区别于传统犯罪的特征。

1. 网络犯罪具有智能化、技术性的特征。计算机和互联网本身就是高科技的证明。利用计算机和互联网实施的犯罪同样具有智能化、技术性的特征。非法侵入计算机信息系统，对计算机信息系统功能或计算机信息系统中存储、处理或者传输的数据和应用程序进行破坏，

或者故意制作、传播计算机病毒等破坏性程序，行为人都需要掌握相当专业的计算机和网络知识，需要精通计算机的汇编语言，深谙计算机程序及信息网络运行规则，其中许多还要具有其他方面的知识背景（如懂得金融制度、密码技术）。即使是利用计算机网络实施的传统犯罪，也需要一定的技术含量。概言之，计算机网络犯罪是一项"技术活"。

2. 网络犯罪人具有文化层次高、年龄结构轻的特征。网络犯罪需要专业的知识和技能，因此实施网络犯罪的行为人多具有一定的文化水平，且属于经常上网的年轻人。据苏州市检察院课题组对该市2007-2010年网络犯罪的统计分析表明，在网络犯罪被告人中，初中以下文化程度的，占7.22%。初中以上文化程度的，占92.78%。高中以上文化程度的，占57.72%。大专及以上文化程度的占36.59%。网络犯罪被告人整体文化水平较高。就年龄结构而言，网络犯罪被告人年龄上以青年人为主，有158人属于18-35岁，占统计样本总数的81.03%。反映出这个年龄层次的人员，基本都受到现代信息技术发展的影响，在计算机及网络运用上有所优势，且网络犯罪主体的年轻化与上网者年轻人占较大的比例及年轻人对网络的情有独钟和特有的心态有很大的关系。[12]

3. 网络犯罪成本低、传播广、影响大。网络犯罪不需要耗费很多的人力物力。黑客只需要一台计算机、一条电话线、一个调制解调器就可以接入全球性计算机网络中的大型主机远距离作案，而且这些犯罪活动操作起来极为方便。[13] 网络世界是个虚拟的空间，不存在物理介质的阻碍，全世界都可以同时共享网络上的信息，因此网络犯罪传播广泛、受害者众多、造成的后果可能也会更为严重。2012年长沙警方打掉了一个名为"中国资源部"的信息倒卖团伙。在犯罪嫌疑人的作案电脑中，存储的公民个人信息数据涉及全国几乎所有省份，总量在1.5亿条以上，从姓名、电话、住址、房产、车辆到通话详单、航班记录，信息内容门类众多，详细程度令人瞠目。[14]

4. 网络犯罪具有很强的隐蔽性、取证难、侦破难。网络虚拟空间的特性，决定网络犯罪的隐蔽性和较高的犯罪黑数。从时间上看，24小时均能作案；从空间上看，网上犯罪嫌疑人可以在任何有联网计算机的地方实施犯罪，而且可以从头至尾不接触被害人。信息数据本身是看不见、摸不着的，大多数网络犯罪是通过程序和数据等这些无形的操作来实现，作案的

12) 参见李赞等：《苏州市2007-2010年网络犯罪调查分析》，载《中国刑事法杂志》2011年第10期。

13) 参见卓翔：《网络犯罪综合治理刑事政策刍议》，载《福建政法管理干部学院学报》2002年第4期。

14) 新华网，"网络信息保护路在何方？"，http://news.xinhuanet.com/politics/2012-12/22/c_114120113.htm，访问日期：2013年9月29日。

直接对象也通常是那些无形的电子数据和信息。同时，由于网络犯罪的证据主要存在于软件之中，这也使得犯罪分子很容易转移或毁灭罪证，尤其是利用远程计算机通信网络实施的犯罪，罪犯往往难以追寻，即使查出某些蛛丝马迹，犯罪分了也早已逃之夭夭，从而增加了破案难度。[15] 根据美国联邦调查局全国计算机犯罪特勤组的估计，计算机犯罪只有大约1%被发现，而在这些被发现的案件中，也只有大约4%会送到侦查机关。网络世界的犯罪存在85%-97%的犯罪黑数。[16]

5. 网络犯罪具有跨地域性、跨国界性。信息网络世界是个四通八达的空间，不受地域、国别的限制。这使得网络空间的双向性、多向性交流成为了可能。正因为网络犯罪的实施发生在互联网的虚拟空间，因此无传统刑法上的"犯罪现场"之说，它对传统的犯罪行为的实施形成了空间上的挑战，这造成各个国家、各个地区对网络犯罪的管辖权的认定极不统一。这种犯罪客观上的隐蔽性也导致了行为人在主观上的心存侥幸及事后的罪恶感不强，甚而导致犯罪分子连续作案的巨大可能。[17]

三、网络犯罪治理面临的问题和挑战

(一) 预防难：发现迟于发生

互联网的技术和应用服务创新周期短，传播扩散速度快。当多数人还在尝试接触和使用新网络应用时，具有违法犯罪动机的人就已经开始使用闻所未闻的新形式或手段实施违法犯罪行为。不管是公众的防范意识，还是社会控制机构的重视程度、技术应对和打击措施都存在明显的"滞后性"。网络违法犯罪常常呈现"先爆发、后治理"的局面，预先防范的难度极大。[18]

(二) 取证难：电子证据难以固定

由于网络违法犯罪发生在以网络硬件和软件为物理和技术基础的虚拟空间，难以追查行为人的真实身份和实际处所。相关违法犯罪行为的痕迹或多或少表现为电子信息的形式，违法犯罪证据容易销毁，证据的提取要求有较高的信息和网络技术支持，电子数据证据的真实性

15) 参见卓翔：《网络犯罪综合治理刑事政策刍议》，载《福建政法管理干部学院学报》2002年第4期。

16) 参见杨坚争、时启亮：《计算机与网络法讲座》，载《邮电企业管理》2001年18期。

17) 魏红、刘学文：《网络犯罪的形势及其对国际刑法的影响》，载《政治与法律》2007年第1期。

18) 参见《报告》。

和关联性在实践中很容易引发争议。这些都为依法打击网络违法犯罪增加了难度。[19]

(三) 侦查难：高科技性和无边界性带来侦查难题

网络犯罪都有一定的技术含量，许多黑客高手使用的技术手段甚至超过了网络警察掌握的网络技术，而且电子证据易被销毁、难以固定，这些都给网络犯罪的侦查带来不小的技术挑战。网络犯罪的无边界性还给国际刑事侦查带来很大的影响。被称为"中国淫秽色情网站第一大案"的"九九情色论坛案"就是利用 http://www.99bbs.com 的域名在国内开展色情营利行为的网站，其主服务器设在美国，该网站的注册用户超过30万人，至2004年11月份，初步统计其点击率高达4亿次之多，在线人数每10分钟竟达15000人。其造成的社会危害非常之大，是国内犯罪分子与国外相勾结，利用境外网站服务器从事跨国网络淫秽色情违法犯罪活动的典型案例。最后于2004年 12月，在公安部的指导协调下，由安徽省公安厅摧毁其境内的网站管理维护体系，抓获涉案犯罪嫌疑人12人，由于美国并不认为色情服务属于犯罪，且中美两国也无统一的关于网络犯罪的刑事侦查协助机制，也无签订双边引渡条约，故对于国外的犯罪分子不能从根本上予以打击。[20]

(四) 管辖难：无边界性带来管辖难题

由于网络犯罪的开放性、虚拟性、国际性的特点，对网络犯罪行为的惩治带来的最大挑战就在于传统的国际刑事管辖权问题。网络违法犯罪行为充分利用了互联网络"无国界"这一特点，大量采用跨国犯罪的形式来实施犯罪行为。由于很多情况下不同国家对于犯罪的法律定义不同，打击网络跨国犯罪时只有相关行为同时触犯两国法律，才有合作的基础。同时，在打击成本和协调机制上都存在不小的难度。2000 年制作了造成高达上百亿美元经济损失的"爱虫"病毒的菲律宾大学生古兹曼，多个国家都曾对其提出引渡要求，但他在短暂入狱后被无罪释放，只因菲律宾当时还没有打击此类网络犯罪的相关法律。[21]

19) 参见《报告》。

20) 参见魏彪、刘学文：《网络犯罪的形势及其对国际刑法的影响》，载《政治与法律》2007年第1期。

21) 参见高富平主编：《电子商务法律指南》，法律出版社2003年版，第717-718页。

四、网络犯罪刑事政策："以技术对抗技术"

网络犯罪是一种技术犯罪，要有足够的技术手段才能防范、制止。信息安全技术是实现网络信息安全的重要保障，要提高网络信息安全水平，必须有较好的安全技术为支撑。这就需要加快网络安全技术和安全设备的研究开发，为此，国家应考虑增加在这方面的投入。针对重要部门信息网应考虑加强技术安全防范，开发网络安全技术，包括加密、网络入侵预警、处理与防范、防止非法存取技术、查明黑客来路的跟踪系统、病毒检测与消除技术及数据密码技术、网络监测及安全性分析等，完善网络安全保护体系。鼓励企业加强自我保护，防范网络犯罪侵害。为避免遭受攻击，各国政府在实践中大多是积极鼓励企业加强自我保护，如采取给所有操作系统和服务器加装补丁程序，要求设立复杂密码和防火墙，经常对网络进行扫描，及其它网络安全措施，以建立一个综合性的保护体系。[22]

首先，可以考虑在公安部门建立一个专门治理网络犯罪的网络技术和培训中心。虽然我国当前公安部门也存在网络监察部门，但是专业性不够强，社会参与度不够高，而且主要着眼于侦查，缺少预防性和技术性措施的指导和培训。可以考虑以美国的NCFTA(美国国家网络刑事监视与训练联盟)为模型，创立中国版的NCFTA，以应对网络犯罪。NCFTA是美国联邦调查局(FBI)、情报安全大公司赛门铁克、卡内基·梅隆大学等产官学三方面成员构成的团体，成立于1997年。官民一起组建了一个有关网络犯罪手段、网络病毒情报等方面的庞大数据库，主要由大学研究者进行分析，训练搜查人员能够去对应这些网络犯罪。日本警察厅正在考虑创设一个分析网络犯罪信息、提高网络搜查员技能的新组织(日本版NCFTA)。其次，要重点通过网络新技术的开发监测、预防和打击网络犯罪。再次，要不断更新技术手段进行网络侦查和取证，开展网络技术的国际合作。最后，要不断完善网络犯罪的国内立法和国际立法，加强打击网络犯罪国际间的合作。

五、网络犯罪治理的价值冲突：警惕以秩序为名牺牲自由

在法的诸价值－正义、自由、秩序、安全、效率中，秩序是最基础的价值。因为秩序在本质上是组织化的活动方式，而任何价值追求都是有组织的、具有目的性和方向性的活动，即都必须依赖一定的秩序进行，所以秩序价值是其他价值实现的基础。[23] 离开了最基本的秩

22) 参见卓翔：《网络犯罪综合治理刑事政策刍议》，载《福建政法管理干部学院学报》2002年第4期。

23) 参见龙文燮：《"自由与秩序的法律价值冲突"辨析》，载《北京大学学报（哲学社会科学版）》）2000年

序，自由、正义等其他价值也无从实现。因此，秩序是立法者特别偏爱的价值，也是立法时优先考虑的价值。在立法者眼中，秩序是社会存续的最小公约数，是达致最低限度社会共识的基础。自由是秩序追求的终极目标，秩序是实现自由的基本前提。然而，两者并非绝对统一的。自由强调的是主体个性的发挥，而秩序强调的是有序状态的建立与维持；自由难免有打破既有平衡——秩序的趋势，秩序有在一定程度上制约自由、维持平衡的规定性。因此，二者之间的冲突就在所难免。[24] 在网络管控的过程中，特别是对言论进行过滤或者以实名制方式防控网络犯罪时，要注意实现秩序和自由价值的平衡。

以网络实名制为例，自2010年起，微博开始在全中国网民生活中扮演至关重要的角色。2011年12月，北京市公安局等4家单位联合颁布《北京市微博客发展管理若干规定》，其中第9条规定"任何组织或个人注册微博客帐号，制作、复制、发布、传播信息内容的，应当使用真实身份信息，不得以虚假、冒用的居民身份信息、企业注册信息、组织机构代码信息进行注册"，该条规定被冠以"微博实名制"简称，迅速成为全民关注热点。2012年3月16日，新浪、搜狐、网易和腾讯微博共同正式实行微博实名制。2012年12月28日，第十一届全国人大常委会第三十次会议审议并通过《关于加强网络信息保护的决定草案》，其中规定了"网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入互联网手续，或者为用户提供信息发布服务，应当在与用户签订协议时，要求用户提供真实身份信息。"2013年3月29日，国务院办公厅"关于实施《国务院机构改革和职能转变方案》任务分工的通知"，其中"2014年完成的任务"第13条为"出台并实施信息网络实名登记制度。（工业和信息化部、国家互联网信息办公室会同公安部负责。2014年6月底前完成）"。2013年6月28日，工信部发布《电话用户真实身份信息登记规定》，要求手机用户、固定电话用户、宽带用户甚至无线上网卡用户，都应当实名登记，"先登记，后服务"，这一新规于2013年9月1日正式施行。网络实名制在中国已经普及，并且成为必然的发展趋势。

在微博实名制即将推出的前夕，有网站对微博用户进行过调查，数据显示"微博实名制后决定放弃使用微博"的占据了89%。[25] 即使用户选择实名制后继续使用微博，相信因为实名制引发的言论管制的担忧也会使微博的吸引力下降，或者将使用微博的兴趣点集中在无争议

第4期。

24) 参见卓泽渊著：《法的价值论》，北京大学出版社1999年版，第635-636页。

25) 刘建："微博即将实名制，方便了谁？伤害了谁？"http://soft.zol.com.cn/272/2726275.html，访问日期：2013年9月3日。

的娱乐和社会话题，或者使部分微博使用者转投其他具有匿名性的公共论坛软件。实名制在泼“不法言论”脏水的同时，很可能会将盆子一起给扔了。因此，网络实名制的适用应区分不同领域而为。在网络言论领域，面对网络秩序和匿名表达自由的价值冲突，应当进行利益衡量，无论是实行前台还是后台的实名制，都会导致“得不偿失”，应当缓行。在其他领域，如网络电子商务，网络交友（婚恋网站），网络游戏等，安全、秩序、健康（防止未成年人沉溺网游）等价值，对位自由价值时取得了压倒性的胜利，实名制的推行才具有正当性。

연구총서 13-B-02

사이버범죄 관련 법령정비 방안연구

발 행 / 2014년 2월
발행인 / 박상옥
발행처 / 한국형사정책연구원
서울특별시 서초구 태봉로 114
(02)575-5282/5283
등 록 / 1990. 3. 20. 제21-143호
인 쇄 / (사)한국신체장애인복지회인쇄사업장
(02)6401-8891

정가 10,000원
ISBN 978-89-7366-018-6 93360