碩士學位論文

사이버범죄에 관한 연구

濟州大學校 大學院

法 學 科

李 銀 珠

2010年 2月

사이버범죄에 관한 연구

指導敎授 김 창 군

李 銀 珠

이 論文을 法學 碩士學位 論文으로 提出함

2010年 2月

李銀珠의 法學 碩士學位 論文을 認准함

審査委員長 _____ ㊞

委 員 _____ ㊞

委 員 _____ ㊞

濟州大學校 大學院

2010年 2月

A Study on the Cyber Crimes

Eun-Ju Lee
(Supervised by professor Chang-Kuhn Kim)

A thesis submitted in partial fulfillment of the requirement for the degree of Master of Law

2010. 2 . .

This thesis has been examined and approved.

.....

.....

.....

Date 2010. 2.

Department of Law
GRADUATE SCHOOL
JEJU NATIONAL UNIVERSITY

국문요약

인터넷은 놀랄 만큼 빠른 속도로 우리의 삶에서 일상이 되었다. 우리나라는 세계최고의 정보통신 인프라를 바탕으로 정보화 사회에서 언제, 어디서나, 누구든지 편리하게 인터넷을 통한 정보 접속이 가능해지는 유비쿼터스 환경으로 변화하고 있다. 이처럼 인터넷을 이용한 생활환경의 변화로 인터넷은 이제 문화가 아닌 우리 생활영역 전반에 커다란 변화를 가져왔을 뿐만 아니라, 인터넷을 통해 연결되는 사이버공간(Cyberspace)이라는 가상공간은 현실과는 또 다른 가상공동체를 형성하고 있다. 사이버 공간은 개인의 자아발전은 물론 민주주의의 실현과 여론형성에도 커다란 역할을 하고 있지만, 인터넷 침해사고, 개인정보침해, 스팸메일, 무질서한 음란물 유통이나 불법다운로드로 인한 지적재산권 침해 등 정보사회의 역기능은 더욱 증가하고 있다.

사이버범죄는 컴퓨터범죄와 사이버테러를 포함하는 의미로 사이버공간에서 발생하는 범죄행위, 즉 사이버공간을 범행의 수단, 대상으로 삼는 모든 범죄 행위를 총칭하는 것이라고 할 수 있다. 이러한 개념적 근거와 형법의 해석과 정책에서 사이버공간의 특성을 고려해야 하는 경우를 구별하여 사이버범죄의 유형을 진정사이버범죄와 부진정사이버범죄로 분류하였다. 진정사이버범죄는 사이버공간 내에서만 가능한 범죄행위로서 해킹, 악성프로그램 및 바이러스 유포, 스팸메일 등이 이에 해당하고, 부진정사이버범죄는 사이버공간을 이용하는 범죄행위로서 전자상거래 사기, 불법복제, 사이버폭력, 사이버음란물 유포 등의 불법유해사이트, 개인정보침해, 사이버도박 등을 들 수 있다.

본 논문에서는 우리 사회에 필수적인 컴퓨터와 정보통신망을 통하여 발생하고 있는 사이버범죄에 대한 인식과 접근성을 바탕으로 그동안 발표되었던 각종 문헌과 전문서적, 인터넷 게시물 등을 활용하여 사이버범죄에 대한 이론적 고찰과 실태에 대한 분석을 하고, 이에 대한 대응방안으로서 법적규제에 초점을 맞추어 사이버범죄와 관련한 각국의 대응방안과 국내의 법령을 분석하여 사이버범죄에 효과적으로 대응할 수 있는 법률적 방안을 검토하였다.

사이버공간을 이용하는 새로운 범죄의 대부분은 기존의 형벌법규가 전혀 예상하지 못한 불법적인 유형들이기 때문에 당연히 처벌에 있어 공백이 생길 수밖에

없다. 그리하여 세계 각국에서는 사이버범죄에 대처하기 위하여 새로운 처벌법규를 신설하거나 기존의 처벌법규를 보완하는 입법을 한 바 있다. 사이버범죄에 대한 형사법적 규제는 형법뿐만 아니라 다양한 특별법에 의하여 이루어지고 있다. 그러나 특별법은 일반형법에 비해 법률제정이 덜 엄격함으로써 졸속으로 제정될 위험이 높고, 특별법의 대부분이 긴급조치의 목적으로 제정됨으로써, 과잉범죄화와 과잉형벌화, 법률제정상 남용과 졸속의 문제, 법률형식상의 법률효과의 불명확성과 법률 명칭의 비통일성, 범죄의 실효성 등 많은 문제점을 가지고 있다.

특히 해킹과 같은 범죄는 국가기반 정보통신망 자체의 안정성을 위협하고 해칠 수 있는 위험이 크므로 단순해킹이나 바이러스 제작 · 유포같은 범죄행위는 형법전에 미수범의 처벌규정을 신설 · 강력하게 대응하는 것이 바람직하고 그 피해의 규모나 중독성 · 파급효과 등 사회적 유해성이 일반 도박죄에 비해 매우 큰 인터넷을 이용한 도박은 형법이나 게임산업진흥에관한법률의 처벌을 강화시킬 필요가 있을 것이다. 또한 이미 우리 사회에서 일반적인 현상이 되어가고 있는 사이버범죄 중에 이미 형법에 그 처벌규정이 마련되어 있는 명예훼손이나 음란물 유포 같은 경우에는 형법의 개정을 통하여 형법전으로 편입시키고, 중복된 범죄에 대한 처벌성의 정도를 다른 범죄들과 비교 · 검토함으로써 체계 및 형평성을 유지하여야 하는 것이 타당하다고 본다. 이와 더불어 인터넷서비스제공자나 P2P서비스의 규제를 강화해야 하고 인터넷실명제의 확대 실시를 적극 검토해보아야 할 것이다.

미국의 경우에는 법무성 산하에 사이버범죄대책반(컴퓨터범죄 및 지적재산권 담당국:Computer Crime and Intellectual Property Section-CCIPS)을 구성, 종합보고서를 제출하고 있으며, 그 실천을 위한 입법과정에 들어가 있는가 하면, 일본의 경우에는 기존의 형법규정의 확대해석 내지는 유추해석의 가능성까지도 심각하게 고려하고 있는 실정이다. 뿐만 아니라, 유럽의 경우에는 아예 일정한 범위 내에서 정보통신서비스제공자의 편집권을 인정하면서 그에 대한 법적 책임을 추궁할 수 있는 여지를 부여하는 형태로 사이버범죄의 유통을 차단하는 장치를 실시하고 있다. 우리나라도 외국의 다양한 입법례를 고려하여 한국적 현실과 관련하여 그 적실성을 추구해야 할 것이다. 그 외에도 IT환경이 무선인터넷 중심으로 변화하고 모바일에 이러한 인터넷 기능이 확장되면서 모바일 관련 범죄가

빠르게 진행되고 있다. 이러한 의미에서 장래의 사이버범죄는 모바일범죄로 변화될 것이며, 이를 포괄적으로 수용할 수 있는 방안이 마련되어야 할 것이다.

<목 차>

<표 목 차>

I. 문제의 제기

1. 연구의 목적

우리는 지금 정보가 사회 발전의 성패를 좌우하는 시대에 살고 있다. 물질이나 에너지를 대신하여 정보의 가치가 상대적으로 높아지는 사회를 정보화 사회라 한다. 구체적으로 정보화 사회는 많은 양의 정보가 신속하게 처리되고 전달, 공급되며, 대부분의 고용이 지식과 정보의 생산 · 처리 · 유통과 관련된 정보 산업에 집중되는 사회를 의미한다. 정보사회로 발전하게 된 결정적인 계기는 컴퓨터의 보급과 정보통신 기술의 눈부신 발전 덕분이다. 컴퓨터와 정보통신의 응용 기술이 가정생활, 기업 활동, 교육 행정 등 여러 분야에 도입되어 새로운 변화를 가져오면서 인간의 삶의 질은 더욱 향상된 것이다. 정보화 사회에서 가장 중요한 것은 정보이고, 정보의 가치를 높게 한 것은 컴퓨터와 통신기술의 발달이라고 볼 수 있다. 정보화 사회에서의 컴퓨터는 지식과 기술을 처리하여 정보로 바꿔주고, 통신기술은 정보를 언제 어디서나 이용할 수 있게 해준다. 또한 사회는 정보를 활용하기 위해 사회조직, 규범, 관행, 법 등을 개선하기도 한다.

통신기술의 발달로 전세계적으로 확산된 인터넷은 놀랄 만큼 빠른 속도로 우리의 삶에서 일상이 되었다. 우리나라는 세계최고의 정보통신 인프라를 바탕으로 정보화 사회에서 언제, 어디서나, 누구든지 편리하게 인터넷을 통한 정보 접속이 가능해지는 유비쿼터스 환경으로 변화하고 있다. 그러나 이러한 기술의 발달이 낙관적인 것만은 아니다. 특히 유비쿼터스 컴퓨팅 환경에서는 모든 정보가 공유되고 누구나 쉽게 접근할 수 있다. 그 이면에는 개인의 정보가 다른 사람에게 알려지는 비밀 없는 세계가 될 수 있다. 결국 집약화된 다양한 정보로부터 국가기관 내지 가정과 직장을 포함한 전 사회의 감시와 통제가 심화될 것으로 예견되므로(디지털감시사회도래) 이로 인한 사생활 침해가 극심할 것으로 보여진다. 또한 다양한 정보의 디지털화로부터 개인정보를 포함한 중요정보에 대한 침해가 더욱 용이할 것으로 전망된다(정보범죄심화). 그리고 오늘날 심화되고 있는 사이버범죄라는 일탈현상도 많은 부분 그대로 발생할 것으로 보여지는데 유비쿼터스

환경은 오늘날 사이버범죄가 발생하게 된 네트워크 환경의 특징 부분을 그대로 가지고 있기 때문이다(사이버범죄존속).

또한, 인터넷은 이제 문화가 아닌 우리 생활영역 전반에 커다란 변화를 가져왔을 뿐만 아니라, 인터넷을 통해 연결되는 사이버공간(Cyberspace)이라는 가상공간은 현실과는 또 다른 가상공동체를 형성하고 있다. 사이버 공간은 개인의 자아발전은 물론 민주주의의 실현과 여론형성에도 커다란 역할을 하고 있지만, 인터넷 침해사고, 개인정보침해, 스팸메일, 무질서한 음란물 유통이나 불법다운로드로 인한 지적재산권 침해 등 정보사회의 역기능은 더욱 증가하고 있다. 이외에도 기계화 및 자동화로 인한 일자리 감소 및 비인간화, 익명성으로 인한 다양한 윤리적 문제, 각 부분의 네트워크화로 인한 사이버테러 및 시스템 공황상태 야기, 정보유출, 저작권 침해 등 가상공간에서의 각종 부작용들이 산재해 있다. 이에 대한 최근의 한 예로서 2009년 7월 7일부터 10일까지 3일간에 걸쳐 분산서비스거부(DDoS) 공격[1]으로 청와대와 백악관 등 한미 주요 정부기관, 민간의 홈페이지를 이용하지 못하는 사건이 발생하여 그 피해액이 최소 363억원에서 최대 544억원에 이를 것으로 추정된다는 분석이 제기됐다[2]. 이처럼 사이버공간에서의 테러로 인한 피해는 유비쿼터스 사회 등 IT 네트워크가 대규모화하는 사회로 진전될수록 더욱 대형화되는 추세이다. 이는 유비쿼터스 환경에서 피해가 단순히 개인적인 영역을 넘어 사회 · 경제적 영역으로 파급될 수 있으며, 우리의 안전을 위협하고 있다. 이처럼 정보사회가 진행될수록 기존의 전통적인 범죄에서 사이버공간을 매개로 하는 범죄행위가 증가하고 있으며, 이러한 문제점들을 해결하기 위한 방법으로 이에 대한 개념의 정립 및 법률적 대응방안의 필요성이 제기되었다. 그리고 기술적인 측면에서의 지원을 통한 직접 규제방안 등 정부, 민간기업, 일반인이 공조하여 국가 차원에서 대응책을 시급히 강구하여야 한다. 그러나 법적 · 제도장치들을 통해서 이러한 문제들을 완전히 해결하는 데는 한계가 있다.

사이버범죄에 대한 개념정의들은 다양하게 나타나고 있으나 대부분이 사이버공간 내지는 인터넷과 관련 있는 범죄를 사이버범죄로 규정한 것으로서 그 실질

1) 분산서비스거부(DDoS : Distributed Denial of Service)란 다수의 컴퓨터를 이용해 특정 서버에 대량의 트래픽을 전송해 그 서버에 과부하를 발생시켜 정상적인 서비스 이용을 방해하는 사이버 공격법이다.
2) 디지털타임즈, “DDoS공격 피해액 최대 544억원 추정”, 2009년 7월23일 보도 참조.

적인 내용에는 별다른 차이가 없다. 이러한 사이버범죄에는 해킹, 바이러스 유포, 전자상거래 사기, 스팸메일, 프로그램 불법복제, 불법· 유해사이트 운영, 개인정보 침해 등을 들 수 있다. 사이버범죄는 최근 더욱 지능화 · 고속화 · 다양화되고 있다. 디스켓을 통한 바이러스파일 유포 같은 단순한 공격패턴에서 현재는 웜 · 바이러스와 해킹기능의 결합으로 복합화 · 악성화된 공격, 자동화 · 분산화 · 은닉화하는 양상을 보이고 있다. 이에 따라 사이버범죄에 대한 효과적인 대응방안으로는 국가차원의 법적 규제, 기술적 규제 등이 이루어지고는 있지만 빠르게 변화하고 있는 사이버범죄에 대한 효과적인 대응책은 미흡한 실정이다.

우리나라에서도 산업화 · 정보화의 추세에 따른 컴퓨터범죄 등의 신종범죄에 효율적으로 대응하기 위해 1995년 12월 형법개정 및 다양한 특별법을 제정하고 있다. 그러나 사이버범죄의 처벌과 관련하여 형법의 일반원리와 당벌성 그리고 다른 범죄들과의 형평성 등의 내용들이 구체적으로 고려되기 보다는 신속한 형사법적 대응이 필요하다는 점과 발생하는 법익침해가 막대하다는 점만이 전면에 등장하였다. 이에 근거하여 사이버공간의 일탈행위에 대한 거의 전방위적 처벌과 또한 그 처벌도 엄격한 처벌을 통하여 사이버범죄를 예방하려는 시도는 도처에 중첩적인 처벌규정들과 엄격한 규정들을 생산하여, 결국 사이버범죄에 대한 형사법적 규제는 과잉범죄화와 과잉형벌화의 문제를 지니게 되었다. 또한 사이버공간의 등장과 더불어 나타난 새로운 형태의 범죄에 대하여 전통적인 범죄유형과는 전혀 다른 새로운 불법유형으로서 범죄행위의 성립여부부터 판단하여야 하는데 범죄가 성립된다는 판단은 있어도 실정법상의 규정이 없는 경우가 발생할 수 있다. 따라서 본 논문에서는 빠르게 변화하고 있는 사이버범죄에 대해 효과적으로 대응하기 위해 사이버범죄의 성격을 규명하고 형법과 특별법에 산재해 있는 처벌방안을 분석하여 처벌범위에 대한 정당성 획득과 법률적 체계 및 형평성 고찰을 목표로 사이버범죄에 대한 연구의 필요성을 제기할 수 있다.

2. 연구의 범위와 방법

본 논문에서는 우리 사회에 필수적인 컴퓨터와 정보통신망을 통하여 발생하고 있는 사이버범죄에 대한 인식과 접근성을 바탕으로 그동안 발표되었던 각종 문

헌과 전문서적, 인터넷 게시물 등을 활용하여 사이버범죄에 대한 이론적 고찰과 실태에 대한 분석을 하고, 이에 대한 대응방안으로서 법적규제에 초점을 맞추어 각국의 대응방안을 검토하고 우리나라의 사이버범죄에 대한 관계법령을 검토하여 사이버범죄에 효과적으로 대응할 수 있는 형사법적 방안을 검토해 보고자 한다.

제I장 서론에서는 연구의 목적과 연구의 범위와 방법을 서술하였고, 제II장에서는 사이버범죄를 더 자세하게 이해하기 위한 이론적 배경으로서 사이버범죄의 개념과 특징, 그리고 사이버범죄의 유형과 실태를 파악함으로써 신종화 · 첨단화되고 있는 사이버범죄에 대해 분석을 하고자 한다. 제III장에서는 국외의 사이버범죄에 대한 법적 규제 방안을 검토하고 우리나라의 형법과 정보통신망이용촉진및정보보호등에관한법률에 나타난 사이버범죄에 대한 국내의 법적 규제와 이를 유형별로 나누어 처벌규정을 검토함으로써 사이버범죄에 대한 국내외의 대응체계와 문제점을 파악하고자 하였으며, 제IV장에서는 국내외 사이버범죄에 대한 법적 규제의 문제점을 분석함으로써 사이버범죄의 대응체계에 대한 개선방안을 제시한다. 제V장 결론에서는 사이버범죄에 대한 전반적인 요약과 제IV장에서 논의되었던 사이버범죄의 문제점과 한계에 대한 보다 효과적인 대응방안을 총괄 정리하고자 한다.

II. 사이버범죄에 대한 일반적 고찰

1. 사이버범죄의 개념

(1) 사이버범죄의 개념 형성의 문제

사이버범죄라는 용어는 외국어인 'cyber[3]'와 우리말인 '범죄'가 결합된 것으로 아직 학문적으로 정립된 것은 아니며, 사이버범죄에 관한 연구는 이론적인 관점보다는 사이버공간에서 발생되는 개별적인 사회유해행위들을 종합하는 현상적인 관점에서 이루어져 왔기 때문에 사이버범죄의 개념 형성을 어렵게 하였다. 그 명칭도 학자에 따라서는 컴퓨터범죄[4], 정보통신범죄[5], 하이테크범죄[6], 사이버 테러[7] 등의 용어가 사용되기도 한다.

---

3) cyber라는 용어는 W. Gibson이라는 소설가가 1982년에 발표한 '불타는 크롬'이라는 소설에서 처음 사용했으며, 인간의 뇌와 인공지능 컴퓨터가 직접 연결되어 컴퓨터그래픽이 나타내고 있는 재현(컴퓨터 시뮬레이션,Computer Simulation) 세계를 사이버스페이스라고 하였다. 정보통신 매체에 의한 인터넷망이 형성되고 1990년대 중반 이후, 인터넷이 대중화하면서 컴퓨터상의 인터넷공간을 사이버스페이스라고 부르고 있다; 김수정, "지식정보사회에서의 사이버범죄", 「교정복지연구」 창간호, 한국교정복지학회, 2005, 174면.

4) 컴퓨터범죄란 "컴퓨터에 의한 자료처리 과정과 관련되는 위법행위"를 말하는데 이는 범죄의 수단 내지 대상이 되는 독립적인 컴퓨터 시스템에 중점을 둔 용어이다. 그런데 오늘날 우리가 흔히 사용하는 인터넷은 컴퓨터와 컴퓨터의 연결(컴퓨터 네트워크)을 넘어 네트워크와 네트워크를 연결하여 전세계의 각종 정보서비스망을 하나로 연결한 것이며, 이렇게 형성된 인터넷상의 가상공간이 사이버공간이다. 따라서 사이버범죄란 범죄가 행해지는 공간에, 인터넷범죄란 범죄공간을 형성하는 수단에 중점을 둔 용어로서 양자는 동일하다고 할 수 있다. 그런데 오늘날 정보통신기술의 발전에 의해 컴퓨터시스템을 통해서만 인터넷에 접속할 수 있는 것은 아니므로, 즉 사이버공간에의 접근이 반드시 컴퓨터통신에 의해서만 가능한 것은 아니므로, 사이버범죄가 컴퓨터범죄와 완전히 동일하다고 할 수는 없다; 강동범, 「컴퓨터범죄시론」, 경진사, 1989, 26면 이하; 이철, 「컴퓨터범죄와 소프트웨어보호」, 박영사, 1995, 23면 이하; 최영호, 「컴퓨터와 범죄현상」, 컴퓨터출판사, 1995 ; 장영민 · 조영관, 「컴퓨터범죄에 관한 연구」, 한국형사정책연구원, 1993, 27면; 강동범, "컴퓨터범죄와 개정형법", 「법조」 491호, 법조협회, 1997.8, 108면.

5) 정보통신범죄는 정보통신기술을 이용한 범죄적 행위를 의미하는 것으로, 컴퓨터범죄와 유사하게 범죄의 수단 내지 대상이 정보통신이라는 점에 착안한 용어이다. 정보통신기술의 비약적 발전이 인터넷을 가능하게 하였고 이러한 인터넷이 사이버공간을 낳았기 때문에 정보통신범죄가 사이버범죄와 유사하지만 동일하지는 않다; 김종섭, "사이버범죄의 현황과 대책", 「형사정책」 제12권 제1호, 한국형사정책학회, 2000, 238면 이하; 백광훈, "인터넷을 이용한 범죄의 유형과 처벌법규", 「2003년 한국범죄방지재단 세미나 자료집」, 2003.5.29, 한국범죄방지재단, 5~18면; 허일태, "사이버 범죄의 현황과 대책", 「동아법학」 제27호, 동아대학교 법학연구소, 2000. 9, 68면 이하.

6) 하이테크범죄는 고도의 과학기술이나 첨단기술을 이용하여 범하여지는 범죄현상을 뜻하지만 이는 사이버공간에서의 범죄만을 포섭하는 것은 아니다; 강동범, "사이버범죄 처벌규정의 문제점과 대책", 「형사정책」 제19권 제2호, 한국형사정책학회, 2007, 34~35면; 조병인, "하이테크범죄의 실태와 대책", 한국공안행정학회 국제범죄 학술세미나 발표논문, 1999.9.17, 11면 이하.

7) 사이버 테러라는 개념은 최근에 등장한 개념으로 사이버상공간의 다른 문제현상과 구분하여 국가적, 사회적 차원에서 특별히 취급하여 대응해야 한다고 주장하는 견해가 있으나, 보는 견지에 따라서 사이버테러

또한, 사이버범죄의 존재 자체에 대한 시각도 크게 두 가지로 구별된다[8]. 하나는 사이버공간에는 독특한 범죄행위가 존재하며 별도의 접근이 필요하다는 사이버범죄 존재론의 입장이고, 다른 하나는 사이버공간의 범죄행위도 기존 범죄행위의 틀에서 크게 벗어나지 않는 한 일종의 범죄 경향일 뿐이지 미래지향적 관점에서 볼 때 현실사회와 유리된 독특한 사이버공간 범죄는 존재하기 어렵다고 보는 사이버공간의 범죄행위 부인론으로 구별된다. 먼저, 사이버공간 범죄 행위 존재를 인정하는 주장은 사이버공간에는 새로운 유형의 범죄행위가 출현하고 있으며 범죄유형이 나날이 새로워질 뿐만 아니라 범죄기술 또한 고도화되고 있기 때문에 사이버범죄에 대한 별도의 대처방안이 필요하다는 의견이다. 정보화 사회의 도래와 더불어 새로운 유형의 범죄행위가 나타나고 있고 일상생활에서 전자적 방법의 의존성이 높아진다. 동시에 익명성이라는 특성으로 인하여 정보윤리의 실종현상이 발생되고 개인에 대한 프라이버시 침해로부터 국가 기간망에 대한 사이버테러에 이르는 컴퓨터 범죄는 날이 갈수록 증가하고 있다. 이러한 새로운 유형의 범죄행위는 정보통신망을 통해 자행되고 있기 때문에 종래의 범죄행위와는 다른 독특한 성향이 있으며, 사이버공간에서의 범죄행위가 존재한다는 이유도 여기에서 찾을 수 있다. 반면, 사이버공간에서의 범죄행위의 존재를 부인하는 주장은 사이버공간에서 범죄행위가 존재하지 않는다는 것이 아니라 현실사회에서와 전혀 다른 사이버공간에서의 독특한 범죄행위가 존재하지 않는다는 입장이다. 사이버공간에서의 범죄행위도 지리적 공간에서 범죄의 연장선상에서 보아야 하며 지리적 공간의 범죄와 다른 유형으로 볼 수 없다는 입장이다. 사이버공간에서 범죄행위의 존재를 인정하려 들지 않는 입장에서는 컴퓨터범죄가 무엇인가 하는 것은 아직도 명확하지 않다는 점에서 출발한다. 컴퓨터를 이용하거나 컴퓨터 시스템 자체를 대상으로 하는 범죄라고 할 수 있지만 범죄에 이용되는 도구를 중심으로 범죄행위를 규정하고 대책을 세운다면 범죄유형을 정리하고 대책을 마련

에 대해 그 대상이 개인인가 국가인가를 불문하고 사이버 공격을 이용한 모든 공격행위라고 하는 최광의의 개념을 사용하는 경우도 있다. 즉 이러한 입장에서는 인터넷 사기, 사이버 음란, 사이버 폭력, 사이버비밀침해 행위 등도 모두 사이버테러의 개념 속에 포함시키고 있으며 사이버범죄와의 구별이 모호하다; 양근원, 「사이버테러의 실태와 법적 대응에 관한 연구」, 경희대학교 국제법무대학원 석사학위 논문, 2003, 7면 이하.

8) 허만영 · 홍진표, 「사이버스페이스의 범죄현황과 경찰의 대응방안」, 치안정책연구소 연구보고서, 치안정책연구소, 2005, 46~48면; 정재봉, 「사이버 범죄의 실태와 대책에 관한 연구」, 원광대학교 행정대학원 석사학위논문, 2007, 4~7면.

하는 과정이 지나치게 복잡할 수 있다는 입장이다. 예를 들어 자동차가 흔치 않던 시절 자동차를 이용하는 범죄를 자동차이용범죄라 해서 특별 취급했으나 지금같이 자동차 사용이 일반화된 시점에서는 이를 일반범죄 취급하듯이 사회생활 과정이나 경제활동을 수행하는 과정에서 컴퓨터와 통신 이용이 계속적으로 늘어나 일반화되는 시점에서 컴퓨터를 이용하는 모든 범죄를 컴퓨터범죄라고 지칭하는 것은 문제일 수 있다는 의견을 개진한다. 워드프로세서 프로그램을 이용하여 문서를 위조하는 행위를 컴퓨터를 이용했다 해서 컴퓨터범죄라고 부르기 보다는 문서위조 범죄로 지칭되는 것과 마찬가지의 논리이다. 따라서 컴퓨터범죄는 컴퓨터 사용의 추이에 따라 일반적인 범행수법이 아니라 전문적, 기술적인 수단 및 지식 없이는 수사가 곤란한 형태의 컴퓨터 이용 및 컴퓨터 대상범죄라고 할 것이며, 이 개념은 유동적이고 사회변화에 따라 그 정의가 계속 변화할 것이라는 주장이 사이버공간에서 범죄행위의 존재를 부정하는 입장의 논리이다.

그러나 사이버공간에서 범죄행위의 존재를 부인하는 입장에서도 사이버공간의 범죄행위가 과거의 일반 범죄행위와 다르다는 점을 인정한다. 논리폭탄, 데이터 변조 등의 컴퓨터 통신이 발달하지 못한 상태에서 일어났던 유형에 비해 독특한 현상이 있을 뿐만 아니라 수사기법과 증거채집 방법이 다르기 때문에 적용되는 법률이 다를 수 있다는 점에 대해서는 인정하고 있다[9]. 따라서 과거 일반 범죄행위와 다른 이러한 범죄행위들에 대한 용어사용의 차이는 결국 동일한 대상에 대하여 그 명칭을 달리 설정한 것에 불과한 것으로 특별한 의미는 없어 보이며, 중요한 것은 그 명칭 안의 개념 즉 그 명칭에 담겨질 내용을 어떻게 규정할 것인가가 더 중요한 문제라고 생각된다.

(2) 사이버범죄의 개념

우리나라에서는 지금까지 사이버범죄에 대한 개념정의에 대한 다양한 의견들이 제기되었다. 사이버범죄라는 개념은 최근 사이버 공간이 급속도로 확장되면서 생겨난 개념으로서, 인터넷과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이를 매개로 형성되는 사이버공간을 중심으로 발생하는 범죄행위를 나타나는 용어

9) 허만영 · 홍진표, 전게보고서, 46~48면.

라는 의견(심희기 · 양근원), 사이버범죄는 사이버공간에서 이루어지는 범죄군을 칭한다라는 의견(허일태), 사이버범죄는 컴퓨터범죄를 포함하여 사이버공간에서 행하여지는 모든 범죄적 현상을 의미한다는 의견(강동범), 사이버범죄란 무수히 많은 인터넷사이트들과 그것들을 서로 연계시키는 컴퓨터연결망(인터넷)을 범행의 수단, 표적 혹은 무대로 삼는 범법사례들을 총칭하는 개념이라는 의견(정완 외 3인), 사이버범죄(및 일탈)는 인터넷사이트와 그것들을 서로 연계시키는 컴퓨터 네트워크(즉, 인터넷)를 수단으로 하여 특정 네티즌이나 사이트, 또는 네트워크 그 자체를 대상으로 하는 범죄(및 일탈)를 총칭하는 개념이라는 의견(이민식) 등을 들 수 있다. 이러한 개념정의들에 대하여 현재까지의 범죄개념 정립원칙에 반하는 것이며, 이로 인해 사이버범죄 개념을 추상화시키게 하는 주요인으로 처벌의 필요성과 가벌성을 징표하지 못하는 개념으로 법체계 전체적인 측면에서 그 통일적이고 명확한 해석을 어렵게 하는 역기능을 하고 있다는 비판의 시각도 제기되었다[10]. 최정호는 사이버범죄의 처벌과 관련된 최초의 국제조약인 '유럽 사이버범죄 방지조약(Convention on Cybercrime)'에서 사이버범죄에 대한 명확한 정의는 내려져 있지는 않지만, 그 서문에 나타난 의도들을 면밀히 검토해볼 때, 사이버범죄란 "정보처리시스템, 인터넷망 그리고 컴퓨터 자료들의 기밀성, 무결성과 유용성에 해를 끼치는 행위, 그러한 시스템, 네트워크와 자료의 악의적인 사용 또는 정보통신망과 전자정보를 이용함으로써 사이버공간에서 벌어지는 형법적 침해행위"라고 유추할 수 있을 것[11]이라고 정의를 내리고 있다. 우리나라도 1995년 12월 29일 형법 개정을 통하여 일부 컴퓨터범죄의 처벌 구성요건을 신설한 바 있다. 그러나 새로운 인터넷 환경이 나타난 1990년대 이후에는 이러한 신종범죄의 유형이 종래의 컴퓨터범죄에서 '정보통신망을 이용한 범죄'로 그 중심점이 옮겨가고 있음이 사실이다.

이상에서 나타난 바와 같이 사이버범죄에 대한 개념정의들은 모두 사이버공간 내지는 인터넷과 관련 있는 범죄를 사이버범죄로 규정한 것으로서 그 실질적인 내용에는 별다른 차이가 없는 것으로 보여진다. 그러나 비판적인 시각에서 나타

10) 이천현, "사이버범죄의 개념-일반적 개념정의에 대한 비판적 관점에서", 사이버범죄연구회 제18회 세미나, 2001. 6.16.
11) 최정호, "일반 사이버범죄 법규의 문제점", 「경찰법연구」 제6권 제2호, 한국경찰법학회, 2008, 272면.

난 바와 같이 사이버범죄의 개념을 설정하기 위해서는 개념자체가 범죄의 실질적인 내용을 제시해줄 수 있어야 하고, 사회적 유해성 · 가벌성의 필요성을 내포하고 있어야 한다. 따라서, 정보통신기술의 비약적인 발전에 따라 인터넷에 의해 형성된 '사이버공간'이라는 새로운 생활공간에서 행하여지는 범죄적 현상에 대하여 형사법적 대책을 강구함에 있어서는 이론적인 관점보다는 현상적인 맥락에서 범죄의 내용과 유해성, 가벌성을 파악할 수 있는 표현으로 사이버범죄라는 용어가 적절하다고 생각한다. 따라서 사이버범죄와 관련된 법률상의 문제점을 비교 · 고려하는 본 논문에서의 사이버범죄는 컴퓨터범죄와 사이버테러를 포함하는 의미로 "일반적으로 인터넷과 같은 정보통신망으로 연결된 컴퓨터 시스템이나 이들을 매개로 형성되는 사이버공간에서 발생하는 범죄행위, 즉 사이버공간을 범행의 수단, 대상으로 삼는 모든 범죄적 행위를 총칭하는 것"으로 정의하고자 한다.

2. 사이버범죄의 특징

흔히 범죄라 하면 현행법상 구성요건에 해당하는 행위로서 형벌이 과해질 수 있는 행위를 말한다. 그러나 사이버범죄는 입법 대응이 완결된 영역이 아니라 이제 막 대응해 나가야 할 새로운 형태의 범죄라는 특성을 가지고 있다. 사이버공간에서 일어나는 사이버범죄는 컴퓨터 네트워크로 구성된 정보사회를 배경으로 하는데, 정보통신기술의 빠른 발전으로 사이버공간에서 일어나는 사이버범죄에 대한 개념도 고정적이지 못하고 다양하게 변할 수밖에 없다. 따라서 사이버공간에서 일어날 수 있는 각종 범죄는 기존 법 이론의 단순한 확장으로는 제대로 파악할 수 없기 때문에 사이버범죄의 일반적인 특성을 밝히는 것은 어렵다[12]. 다만 여기서는 현실범죄와는 달리 사이버공간에서 일어난다는 점에 착안하여 사이버 공간의 특징으로도 볼 수 있는 사이버범죄의 특징적인 요소들을 살펴보고자 한다.

(1) 익명성과 비대면성

12) 우제태, "사이버범죄의 대응방안에 관한 연구", 「경찰연구논집」 제1호, 한국경찰이론과 실무학회, 2007, 176~177면.

사이버공간에서는 자신의 신분을 노출시키지 않고서도 거의 무제한으로 인터넷을 이용할 수 있는 특성으로 이를 익명성이라 한다. 또한 사람들이 사회생활을 영위하면서도 서로 일일이 굳이 만날 필요가 없다는 비대면적인 특성을 지니고 있다. 대부분의 경우 인터넷사이트를 이용할 때 일정한 인증절차를 통해 검증하는 경우도 있지만, 다른 사람의 인적사항을 이용한다든지 혹은 ID를 도용하면 정당한 사용자로 인정하고 이용할 수 있는 권한을 부여해 주는 곳이 대부분이다. 이러한 취약점은 행위자의 책임의식의 결여로 이어져 다른 사람에 대한 명예훼손이나 모욕, 물품판매를 가장한 사기행위, 해킹 · 바이러스의 유포, 소프트웨어나 음란물의 불법복제 및 판매 등 범죄행위 등에 쉽게 빠져들며 수사기관의 추적을 피하거나 범행을 은폐할 수 있는 환경이 마련되고 있다[13].

(2) 시간적 · 공간적 무제약성

사이버공간에서의 생활은 시간과 공간의 제약을 거의 받지 않는다. 누구든지 마음만 먹으면 인터넷을 24시간 내내 이용할 수 있으며, 별다른 어려움 없이 세계 어느 곳에 있는 인터넷사이트에도 접속할 수 있다. 사이버공간의 이러한 시간적 · 공간적 무제약성은 사이버범죄자들에게 엄청나게 많은 범죄의 기회를 제공하고 있다. 즉, 범죄자는 인터넷이 연결된 곳이면 지구 반대편에 있는 나라의 컴퓨터에도 바이러스를 유포할 수 있고 해킹도 할 수 있다. 실제로 우리나라에서 발생한 해킹사건의 대부분이 해외에서 국내로 침입한 것이며, 외국 해커들의 상당수가 우리나라를 경유지로 활용하고 있다고 한다. 사이버범죄의 이러한 특징은 사이버범죄 수사에 법률상의 많은 어려움을 안겨 주고 있을 뿐만 아니라 국제형사사법공조의 필요성을 던져주고 있다[14].

---

13) 강동범, “사이버범죄와 형사법적 대책”, 「형사정책연구」 제11권 제2호, 한국형사정책연구원, 2000, 69면; 김종세, “사이버범죄의 법적 쟁점에 관한 고찰”, 「경찰연구논집」제2호, 한국경찰이론과 실무학회, 2008, 231~232면;이수현, “인터넷범죄의 실태와 대응방안”, 「법학논고」 제25집, 경북대학교 법학연구소, 2006, 271~272면; 허일태, 전게논문, 69~70면; 정완, “사이버범죄의 실태와 동향 및 대응책”, 「홍익법학」제10권 제1호, 홍익대학교 법학연구소, 2009, 199면; 원혜욱, “인터넷범죄의 특징과 범죄유형별 처벌조항”, 「형사정책연구」제11권 제2호, 한국형사정책연구원, 2000, 96~97면;신현정, “사이버범죄에 관한 고찰”, 서강대학교 공공정책대학원 석사학위논문, 2004, 23면.

14) 강동범, 상게논문, 2000, 70면; 정완, 상게논문, 2009, 200면; 신현정, 상게논문, 23~24면; 이수현, 전게

(3) 즉흥성과 빠른 전파성

수많은 컴퓨터가 네트워크화 되고 인터넷을 통해 시공을 초월하는 사이버공간을 형성함에 따라 현실세계보다 쉽게 상대방과 접촉할 수 있으며, 단 한 번의 클릭으로도 상대방과의 의사소통이나 정보전달이 가능하게 되었다. 이러한 특성으로 사이버공간에서 반윤리적 행위나 범죄행위가 별다른 고려 없이 즉흥적으로 이루어질 수 있게 되며, 현실세계에서 보다 범죄가 더욱 쉽게 발생하고 누구나 손쉽게 해당 정보를 전파하거나 입수할 수 있는 특징을 가지게 된다. 이러한 신속하고 광범위한 전파성에 따라 범죄피해가 제한 없이 확산될 수 있으며, 특히 바이러스와 해킹에 의한 시스템 작동불능은 경우에 따라서 시스템에 연결된 모든 컴퓨터의 작동을 멈추게 함으로써 업무전반을 마비시키는 심각한 결과를 초래하여 천문학적인 재산피해를 야기하기도 한다[15].

(4) 전문성과 기술성

사이버범죄에는 사이버스토킹, 사이버성폭력, 인터넷도박과 같이 컴퓨터와 인터넷의 간단한 조작만으로도 범할 수 있는 범죄유형도 있지만, 바이러스의 제작·유포 및 해킹, 영업비밀을 몰래 절취하는 인터넷 스파이, 프로그램이나 데이터의 조작을 통한 컴퓨터 사기 그리고 지적재산권과 관련하여 컴퓨터프로그램에 부과된 기술적 보호조치를 무력화시키는 행위처럼 일정수준이상의 전문적인 기술을 갖추어야 하는 경우도 있다. 이는 사이버범죄는 전통적인 범죄와는 달리 일정한 수준이상의 컴퓨터와 인터넷에 대한 전문지식이나 기술이 있어야 함을 나타내는 것이다. 실제로 웹(Web)은 “HTTP"[16] 뿐만 아니라 다양한 프로토콜과 형식을 지원하도록 설계된 복잡한 다기능 프로그램이기 때문에 보안상의 취약점

논문; 272면; 김종세, 전게논문, 232~233면; 허일태, 전게논문, 70면.

15) 김종세, 전게논문, 223~234면; 정완, 전게논문, 2009, 200면; 강동범, 전게논문, 2000, 71~72면; 이수현, 전게논문, 273면; 정재봉, 전게논문, 13~14면.

16) HyperText Transfer Protocol의 약자이다. 이는 TCP/IP에서 문자와 함께 화상, 음성 등 다른 종류의 정보를 동시에 전달할 수 있도록 설계된 통신규약이다.

이 많아 기술적인 전문가들에 의하여 그러한 취약점들이 악용될 가능성이 크다. 사이버범죄의 이러한 기술적인 전문성을 고려한다면, 수사기관에서도 반드시 전문적 기술을 가진 수사관을 적극적으로 양성해야 할 필요성이 있다[17].

(5) 범죄성 확정 및 발각과 소추의 어려움

기존 형법은 개인의 재산에서 소유나 점유를 보호하고 있는데 견주어 보호객체인 데이터는 컴퓨터기술과 정보통신기술의 발달로 고속으로 정확하게 보존되고 처리되는 것은 물론 공간의 제약 없이 정보의 전달이 가능하므로 개인의 배타적인 소유와 점유가 가능하기도 하다. 하지만, 이동과 소유가 가능하며 쉽게 타인의 수중으로 들어갈 가능성도 많아 재산권으로서 개인의 독점적인 지배권이 인정되기 어렵다는 점이다. 또한 사이버범죄는 컴퓨터 네트워크와 연결돼 있어 범죄자가 통신망을 이용해 어느 곳에서나 범죄를 일으킬 가능성이 있다. 따라서 범죄현장이 없기 때문에 그 당시에 발각되기도 어렵고 범죄를 위해 소비되는 에너지도 적어 범행을 용이하게 하는 특성을 갖는다. 전자우편이나 전자문서가 암호화되거나 송신자의 전자주소를 은폐할 수 있는 기법이 발전되어 범죄의 적발이 매우 어려운 형편이다. 뿐만 아니라 범죄가 단시간 내에 이루어질 수 있고 광범위하기 때문에 적발이 쉽지 않고 저장된 자료의 불가시성과 익명성 등도 범행예견을 어렵게 하고 있다. 더욱이 기업 등이 피해를 입을 경우에도 신용성 때문에 은폐하려는 경향이 강해 적발이 어려울 뿐만 아니라 형사소추가 되더라도 범죄 입증이 쉽지 않다. 또 범인이 정보와 자료의 관리 소홀 등 상대방의 과실을 주장하면 이들의 고의를 입증하는 것은 거의 불가능하게 된다[18].

3. 사이버범죄의 유형

(1) 유형 분류에 대한 학설

17) 김희준, "사이버범죄의 개념과 대응방안", 「해외연수검사연구논문집」 제18집, 법무연수원, 2003, 445~446면; 정완, 전게논문, 2009, 199면; 강동범, 전게논문, 2000, 70~71면; 이수현, 전게논문, 272면.
18) 우제태, 전게논문, 178~179면; 김종세, 전게논문, 234면; 정재봉, 전게논문, 12면.

사이버범죄의 유형은 학자에 따라 다양하게 제시되고 있다. 일반적으로 언급되는 사이버범죄에 대한 유형들은 '해킹, 바이러스, 인터넷사기, 스팸메일, 사이버폭력, 불법복제, 개인정보 침해, 불법유해사이트' 등 다양하게 나타나고 있다.

1) 해킹기술의 사용유무를 기준으로 분류하는 견해

이 견해는 해킹을 기준으로 하여 해킹기술을 통해 범행이 구현되는 경우와 해킹기술과 무관한 경우로 분류하는 입장이다[19]. 이 견해에서는 해킹기술을 통해 범행이 실행되는 경우로서 사이버스파이, 사이버테러, 폰프리킹, 홈뱅킹사기, 홈페이지 훼손 등이 있다고 하고 해킹과 무관한 경우로는 인터넷을 통한 불량정보 유통, 판매사기, 저작권침해, 도박사이트 운영, 매매춘 알선, 명예훼손, 스토킹, 성희롱, 음란사이트 운영, 마약밀매, 통신방해, 서비스거부 등이 있다고 한다. 세부적으로는 사이버테러와 관련하여서도 해킹기술과 무관한 방법으로 테러목적을 달성하는 경우로서 전자우편을 통해 악성바이러스를 유포시키거나 고성능전자폭탄을 보내 컴퓨터시스템을 마비시키는 방법을 예로 들고 있다.

그러나 해킹기술의 개입여부에 따라 사이버범죄를 양분하는 견해는 해킹기술이 중요한 수단이기는 하지만 이것이 곧바로 범죄유형을 구분하는 기준이 되느냐에 대한 규범적 근거를 제시하기는 어렵다. 이 견해에서 나타났듯이 해킹기술과 무관한 바이러스나 전자폭탄으로도 테러목적을 달성할 수도 있고, 저작권 침해나 명예훼손 등은 해킹에 의하여 발생할 수도 있기 때문이다.

2) 사이버스페이스의 범죄와 실정법상의 범죄로 구별하는 범죄

이 견해는 정보통신 범죄[20]라는 용어를 사용하여 사이버스페이스의 범죄와 실

19) 조병인·정진수·정완·탁희성, 「사이버범죄에 관한 연구」, 한국형사정책연구원 연구보고서, 30면이하, 2000.

20) 정보통신범죄라는 용어를 사용하면서, 정보통신보호범죄와 정보통신내용범죄로 구분하는 입장(백광훈, 전게논문, 16면)과 정보통신망을 매개하는 일반범죄유형인 정보통신범죄(사이버명예훼손, 사이버음란정보유포, 사이버성폭력, 사이버스토킹, 사이버저작권침해, 사이버도박), 정보통신망을 매개하는 기존 컴퓨터범죄유형인 정보통신범죄(사이버사기, 사이버데이터손괴, 사이버업무방해), 정보통신망을 매개하는 새로운 범죄유형으로서의 정보통신범죄(해킹, 바이러스유포, 스팸메일), 정보통신망을 매개하지 않은 컴퓨터범죄(컴퓨터사용사기, 컴퓨터업무방해, 데이터손괴, 컴퓨터무권한사용, 프라이버시침해)로 구분하는 입장(홍승희, "정보통신범죄의 전망", 「형사정책」 제19권 제1호, 한국형사정책학회, 2007, 10~11면)도 있다.

정법상의 범죄로 구별하는 입장이다[21]. 전자의 유형에는 사이버스페이스에서 존재하는 독특한 범죄행위라는 관점에서 컴퓨터범죄, 네트워크범죄, 사이버범죄가 있다고 하며, 후자는 형법상의 범죄와 특별법상의 범죄로 구분한다. 실정법상의 범죄행위로 보는 관점에서는 사이버스페이스에서 인권이나 재산권 침해행위, 혹은 반사회적 행위가 발생할 경우 실정법을 근거로 하여 형벌을 가할 수 있으며, 실정법에 규정되어 있지 않은 인권이나 재산권 침해행위, 혹은 반사회적행위는 처벌할 수 없다는 입장이다. 그러나 이 견해 또한 정보통신범죄에 대한 실질적 분류기준이 모호하다는 점에서 인정하기 어렵다는 비판이 있다[22].

3) 사이버공간을 이용한 전통적 범죄와 신종범죄로 나누는 견해

이 견해는 사이버범죄를 사이버공간을 이용한 전통적인 범죄와 사이버공간의 등장으로 새롭게 발생하는 범죄로 나누는 입장이다[23]. 이 견해는 범죄의 불법내용이 사이버공간 자체의 등장에 의존하고 있는가의 여부를 기준으로 한 입장이라고 할 수 있다. 또한 사이버화된 일반범죄와 사이버공간 고유의 범죄로 양분하여 전자의 예로는 사이버스토킹, 사이버명예훼손, 통신사기, 음란 · 불법물배포 등이고 후자의 예로는 해킹, 바이러스 유포, 음란사이트 운영 등이 있다고 양분하여 설명하는 견해[24]도 같은 입장에 속한다. 일반 범죄의 수단으로 인터넷을 사용하는 범죄로서 인터넷도박, 인터넷몰에서의 사기판매 행위, 인터넷을 통한 명예훼손, 저작권침해 및 사이버스토킹, 음란물의 판매 · 전시행위, 각종 위조 · 변조행위, 사이버테러가 있으며, 인터넷의 특성으로 비로소 출현하는 범죄로서 아이디 · 패스워드의 공개행위, 무차별적인 광고메일의 송신, 다른 사이트나 홈페이지의 무단복사행위 등을 들고 있는 입장도 역시 같은 견해[25]에 속한다고 볼 수 있다. 그리고 다수설의 입장에 속한다고 볼 수 있는 견해로서 사이버공간의 등장과 더불어 나타난 범죄에 대하여 형사정책적 대책을 마련하기 위해서, 특히 구성요건의 신설 또는 정비를 위한 목적론적 관점에서 사이버공간에서의 전통적

21) 허만영 · 홍진표, 전게보고서, 53~54면.
22) 백광훈, "정보통신범죄의 개념과 유형 및 분류", 사이버범죄연구회 제23회 세미나 자료, 2001.10.13.
23) 김종섭, 전게논문, 239면.
24) 양근원, "사이버범죄 현황과 대책", 「21세기 도전과 사이버스페이스」, 사이버커뮤니케이션학회 '99추계 학술대회 자료집, 1999.11, 6면이하.
25) 원혜욱, 전게논문, 98면.

범죄유형, 사이버공간에서의 새로운 범죄유형 그리고 사이버공간에 특유한 불법유형으로 구분하는 것이 적절하다는 견해도 있다[26]. 이에 의하면, 사이버공간에서의 전통적 범죄유형이란 전통적인 범죄행위가 사이버공간이라는 새로운 생활공간에서 행하여지는 경우로서 사이버도박, 사이버명예훼손, 사이버성추행, 사이버테러 또는 인터넷 협박, 인터넷 사기, 사이버포주, 인터넷음란물 유포 등이 이에 해당하고, 사이버공간에서의 새로운 범죄유형이란 사이버공간이라는 새로운 생활공간이 등장하면서 비로소 나타나게 된 새로운 불법유형으로서 바이러스 제작과 유포, 해킹 등이 이에 해당하고, 사이버공간에서만 특유한 불법유형이란 도메인 주소를 훔치는 행위, 사이버상의 아이템을 훔치는 행위, 사이버캐릭터에 대한 침해행위 등을 의미한다. 위 견해에서는 첫 번째와 두 번째 유형의 사이버범죄는 현실세계와 관련된 것이지만 세 번째의 경우는 사이버세계에서만 관련된 것이라고 설명한다.

이 견해가 다른 학설들보다 보다 정밀하지만 다음과 같은 비판이 있다[27].

첫째, 현실세계에 영향을 전혀 주지 않는 정보통신범죄의 개념을 생각하기는 어렵고 도메인 주소를 훔치는 행위의 경우 현실세계의 영업상 · 재산상 이익과 관련되는 경우처럼 사이버공간에서의 특유한 유형도 현실세계와 무관한 유형이라고 볼 수는 없다는 것이다.

둘째, 입법정책적 관점에서 볼 때 사이버공간을 이용한 전통적인 범죄유형과 사이버공간으로 인한 신종범죄유형을 구별하는 것은 기능적인 분류방법으로 생각되기 어려우며, 그 이유로 사이버공간을 이용한 전통적 범죄유형에 대한 입법적 필요가 사이버공간을 통하여 새로이 출현한 범죄유형들에 비하여 감소되는 것은 아니라는 점을 든다.

셋째, 인터넷공간을 이용한 전통적 범죄유형과 인터넷공간의 새로운 범죄유형을 구별하는 것에는 논리필연적 근거가 미약하다는 것이다. 예를 들어 인터넷도박, 인터넷사기, 또는 사이버성폭력이라는 것이 보통 인터넷공간을 이용한 전통범죄 내지 일반범죄의 유형으로 일컬어지나 이것은 도박, 사기, 성폭력이라는 행위들이 전통적으로 범죄행위로 취급되어 왔다는 것을 환기시키는 기능만을 담당

26) 강동범, 전게논문, 2007, 35~36면.
27) 백광훈, 전게 발표자료, 제23회 2001.10.13.

할 뿐이라는 것이다. 왜냐하면 인터넷도박 행위라는 것이 인터넷공간을 매개로 새로이 나타난 범죄유형으로 볼 수 있다고 주장한다.

넷째, 사이버공간의 전통범죄와 사이버공간에 관련한 신종범죄의 구별기준은 첨단과학기술이 급속히 발전하는 현 시대를 반영하는 실질적 효과도 가지고 있지 못하다는 것이다. 즉 오늘날 사이버공간 때문에 나타난 새로운 범죄유형이라고 부르는 것들이 불과 얼마 후에는 전통범죄가 되어버린다는 점에서 위와 같은 다수설의 입장은 사이버범죄가 출현한 초기시점에서는 유용한 입장일지 모르지만 사이버문화가 확립되어버린 현재와 같은 정보사회에서는 이미 설득력을 상실했다는 것이다.

4) 정보통신보호범죄와 정보통신내용범죄로 구분하는 견해

백광훈은 다수설인 사이버공간에서의 전통적 범죄유형, 사이버공간에서의 새로운 범죄유형 그리고 사이버공간에 특유한 불법유형으로 구분하는 견해에 대한 비판을 하고 정보통신범죄를 '정보통신망의 안정성 그 자체 내지 정보통신상의 타인의 정보 등을 불법적으로 위협 내지 침해하는 범죄(정보통신보호범죄)'와 '정보통신상에 제공하거나 기고하는 정보의 내용이 그 사회의 법질서를 위협하는 범죄(정보통신내용범죄)'로 구분하였다[28]. 즉, 정보통신보호범죄는 정보통신사회의 사회구조적 근간이 정보통신망 자체의 안정성을 위협하고 나아가 타인의 인격적 · 재산적 법익의 구현이라 볼 수 있는 그의 정보를 침해한다는 점에서 그 범죄유형에 가벌성을 인정하는 것이 당연하므로 형법적으로 대응하여야 하며, 정보통신내용범죄는 해당 정보의 내용이 최고규범인 헌법이 기본권으로 보호하는 행복추구권 및 표현의 자유와 같은 인격적 권리나 재산권의 표현과 관련되는 경우가 있으므로 그 가벌성을 인정하는데 있어 신중을 기해야 할 경우가 있다는 점을 들어 분류기준을 제시하고 있다. 이 기준에 의하여 정보통신범죄의 유형들을 분류하여 본다면, 정보통신보호범죄에는 해킹이나 바이러스 유포 또는 ID도용 등을 위시한 사이버테러리즘, 프로그램 불법복제나 타인저작물 무단전송 · 사용행위 등의 인터넷상의 저작권침해, 고객들의 개인정보 유출 · 침해나 기업의 영업비밀 유출 · 침해와 같은 사이버정보침해 등이 포함되고, 정보통신내용범죄에

28) 백광훈, 전게 발표자료, 제23회 2001.10.13.

는 인터넷공간에서 음란물을 유포하는 등의 사이버포르노그래피, 사이버명예훼손, 사이버성폭력, 사이버스토킹, 인터넷도박, 인터넷사기, 사이버윤락, 자살사이트, 폭탄제조사이트, 무허가약품거래사이트 등을 포함한다.

5) 사이버테러형범죄와 일반사이버범죄로 구분하는 견해

경찰청 사이버테러 대응센터에서는 사이버범죄를 크게 사이버테러형범죄와 일반사이버범죄로 구분하고 있다. 해킹, 바이러스 유포와 같이 고도의 기술적인 요소가 포함되어 정보통신망 자체에 대한 공격행위를 통해 이루어지는 것은 사이버테러형범죄로, 전자상거래 사기 · 프로그램 불법복제 · 불법사이트 운영 · 개인정보침해 등과 같이 사이버공간이 범죄의 수단으로 사용된 유형은 일반사이버범죄로 구분한다[29]. 그 이유는 사이버테러형 범죄가 여러 가지 특성을 가지고 있기 때문인데 첫째 그 수단의 특징으로 인하여 기술적 · 인적인 대응방법이 일반사이버범죄와 다르고, 둘째 정보보안과 밀접한 관련이 있어 이를 담당하는 정부관계기관, 정보보안회사 등 민간기업, 학계 등의 상호 밀접한 공조가 필요하기 때문이며, 셋째 사이버테러형범죄는 사이버테러의 수단으로 이용될 우려가 있기 때문에 철저한 대비가 필요하기 때문이라고 한다[30].

(2) 진정사이버범죄와 부진정사이버범죄

이상에서 살펴본 바와 같이 사이버범죄의 유형을 분류한다는 것은 간단한 문제가 아니다. 사이버범죄에 대한 개념정립이 확실히 되어 있지 않은 상태에서 유형을 분류하기 위한 기준설정 자체가 어렵고, 사이버범죄의 특성상 종래의 전통적 범죄와 달리 여러 가지 형태가 결합되어 나타나는 경우가 있어 일정한 유형에 해당한다고 결정짓기가 어려우며, 새로운 기술의 발달에 따라 새로운 유형의 범죄가 출현할 수도 있으므로 기존의 분류에 해당되지 않는 범죄가 발생할 가능성과 새로운 범죄유형이라 할지라도 불과 얼마 후에는 전통범죄가 되어버리기 때문이다. 따라서 본 논문에서는 사이버공간에서 발생하는 범죄행위, 즉 사이버

29) 경찰청 사이버테러대응센터 http://www.ctrc.go.kr
30) 양근원 · 임종인, "사이버범죄분석과 법률적 대응방안", 「과학사상」 통권49호, 범양사, 2004, 86~87면.

공간을 범행의 수단, 대상으로 삼는 모든 범죄적 행위를 총칭하는 개념적 근거와 사이버공간의 등장으로 인해 나타나는 새로운 형태의 범죄에 대한 법률적 고찰을 목적으로 하는 본 논문의 기준으로 진정사이버범죄와 부진정사이버범죄로 분류하고자 한다. 이와 같은 견해로 종전의 형법의 해석과 정책이 대체로 현실공간의 범죄에 초점이 맞추어져 있기 때문에 사이버범죄의 유형화는 형법의 해석과 정책이 새롭게 문제되는 영역이 어디인지에 초점을 맞추어 형법의 해석과 정책에서 사이버공간의 특성을 반드시 고려해야 하는 경우와 그렇지 않은 경우로 구별하여 진정사이버범죄와 부진정사이버범죄로 구별하는 견해[31]가 본 논문에서의 유형화에 대한 견해와 같은 맥락이라고 할 수 있다. 진정사이버범죄는 사이버공간내에서만 가능한 범죄행위로서 해킹, 악성프로그램 및 바이러스 유포, 스팸메일 등이 이에 해당하고, 부진정사이버범죄는 사이버공간을 이용하는 범죄행위로서 전자상거래 사기, 불법복제, 사이버폭력, 사이버음란물 유포 등의 불법유해사이트, 개인정보침해, 사이버도박 등을 들 수 있다.

1) 진정사이버범죄

진정사이버범죄는 사이버공간의 등장으로 인하여 나타나게 된 사이버공간내에서만 가능한 범죄행위로서 해킹, 악성프로그램 및 바이러스 유포, 스팸메일 등을 들 수 있다.

① 해킹(Hacking)

해킹은 일반적으로 다른 사람의 컴퓨터 시스템에 무단 침입하여 정보를 빼내거나 프로그램을 파괴하는 전자적 침해행위를 의미한다. 해킹은 사용하는 기술과 방법 및 침해의 정보에 따라 다양하게 구분된다. 경찰청에서는 해킹에 사용된 기술과 방법 침해의 정도에 따라서 단순침입[32], 사용자 도용[33], 파일 등 삭제변

31) 윤동호, "사이버공간에서 관세법의 금지품수출입죄의 해석과 정책", 「법조」통권639호, 법조협회, 2009.12, 219~220면.

32) 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 인증절차를 거치지 않거나 비정상적인 방법을 사용해 해당 정보통신망의 접근권한을 획득하는 것.

33) 정보통신망에 침입하기 위해서 타인에게 부여된 사용자계정과 비밀번호를 권한자의 동의 없이 사용하는 것으로 개념상으로만 보면 단순침입의 한 가지 유형에 해당하지만 사용자 도용이 차지하는 부분이 많아 별도로 구분한다.

경[34], 자료유출, 폭탄스팸메일[35], 서비스거부공격으로 구분하고 있다. 그러나 대부분의 해킹범죄는 단순침입에 그치지 않고 통상 다른 행위를 위한 수단으로, 예컨대 시스템에 수록되어 있는 자료나 비밀을 알아내거나 변경하기 위하여, 또는 자료를 삭제하거나 재산상의 이득을 취득하기 위하여 행하여진다.

② 악성프로그램(Malicious Program)

정보시스템의 정상적인 작동을 방해하기 위하여 고의로 제작 · 유포되는 모든 실행 가능한 컴퓨터 프로그램을 악성프로그램이라 한다. 악성프로그램은 리소스의 감염여부, 전파력 및 기능적 특징에 따라 크게 바이러스, 웜[36], 트로이 목마[37], 스파이웨어[38] 등으로 구분할 수 있다. 악성프로그램에 감염된 컴퓨터는 처리속도가 현저하게 감소하거나 평소에 나타나지 않았던 오류메시지 등이 표시되면서 비정상적으로 작동하기도 하고 지정된 일시에 특정한 작동을 하기도 한다[39].

③ 스팸메일

스팸메일(spam mail)이란 수신자가 원하지 않는 정보를 영리목적으로 반복하여 전송하는 메일을 말하며, 정크메일(junk mail) · 벌크메일(bulk mail)이라고도 한다. 반복성이 있다는 점에서 사이버스토킹과 유사하지만, 영리목적을 갖고 불특정 또는 다수인을 대상으로 하는 점에서 다르다. 하루에도 수많은 재화와 용역이 창출되는 오늘날의 시장경제상황에서 소비자에게 정보를 제공하는 점에서 스팸메일의 긍정적 기능을 인정할 수도 있지만, 원하지 않는 수많은 정보를 반복적 · 지속적으로 받아야 하는 점에서 업무방해까지 가져올 정도로 그 폐해는 적지

34) 정보통신망에 침입한 자가 행한 2차적 행위의 결과로, 일반적으로 정보통신망에 대한 침입행위가 이루어진 뒤에 가능함.
35) 메일서버가 감당할 수 있는 한계를 넘는 많은 양의 메일을 일시에 보내 장애가 발생하게 하거나 메일내부에 메일 수신자의 컴퓨터에 과부하를 일으킬 수 있는 실행코드 등을 넣어 보내는 것으로 서비스거부공격의 한 유형으로 볼 수 있다.
36) 시스템 과부하를 목적으로 이메일의 첨부파일 등 인터넷을 이용하여 확산되며, 확산 시 정상적인 파일이 이메일에 첨부되기도 하기 때문에 개인정보 유출의 위험을 내포하고 있다.
37) 프로그램에 미리 입력된 기능을 능동적으로 수행하여 시스템 외부의 해커에게 정보를 유출하거나 원격제어 기능 수행. 트로이목마처럼 유용한 유틸리티로 위장하여 확산되기 때문에 감염사실 알아채기 어려움.
38) 공개프로그램, 쉐어웨어, 평가판 등의 무료 프로그램에 탑재되어 정보를 유출시키는 기능이 있는 모든 종류의 프로그램.
39) 경찰청 사이버테러대응센터 http://www.ctrc.go.kr.

않다. 따라서 스팸메일을 규제[40]할 필요가 있는 것이다.

2) 부진정사이버범죄

부진정사이버범죄는 사이버공간을 이용하는 범죄행위로서 현실공간에서도 이루어지는 범죄행위들이 그 범죄의 수단으로 사이버공간을 이용하는 것으로 전자상거래 사기, 불법복제, 사이버폭력, 불법 · 유해사이트, 사이버음란물 유포, 개인정보침해, 사이버도박 등을 들 수 있다. 정보통신망이 실생활에 미치는 영향이 증대되고 사이버공간을 통해서 다양한 형태의 생활을 영위할 수 있게 됨에 따라 이를 악용한 범죄행위가 빈번하게 발생하고 있는 실정이다.

① 전자상거래 사기

인터넷을 통하여 물건을 사고파는 과정에서 발생하는 것으로 인터넷의 보급이 확대됨에 따라 그 규모는 날로 팽창하고 있다. 인터넷 화면을 보며 마우스 클릭만으로 주문에서 결제 · 배송까지 확인 할 수 있다는 편리성 때문에 온라인쇼핑몰 이용자들이 급증하는 추세지만, 통상 '先결제'라는 인터넷 거래의 특성을 악용하여 인터넷 쇼핑 사이트를 그럴듯하게 만들어 놓고 유명한 상품을 시중 가격에 비해 싸게 판매하는 것처럼 광고 한 후 고객으로부터 선불금을 받은 뒤 잠적해 버리거나, 상대방이 확인하기가 힘들다는 점을 악용하여 물건을 가지고 있지 않거나 팔 생각이 없으면서도 거래를 하기로 한 후 돈만 받고 연락을 끊어버리는 등의 수법을 이용한 사기 사건이 급증하고 있다. 게임사기는 인터넷 게임인구가 늘어나고 게임시장이 점점 확대됨에 따라 게임사이트에서 실제 돈으로 게임머니를 충전해 주거나 사이버 상에서 통용되는 게임머니나 게임아이템 등이 게임매니아 사이에서 실물처럼 거래되고 있는 실정으로, 게임머니나 아이템을 거래하기로 하는 과정에서 사기피해가 발생하고 있다[41].

2004년부터 전세계에 확산된 인터넷 사기방식인 '피싱(Phishing)'은 일반인이 거래하는 은행이나 인터넷사이트 등의 이름을 도용해 개인정보를 갱신하라는 메

40) 스팸메일의 규제방식에는 옵트인(opt-in)방식(사전동의를 요함)과 옵트아웃(opt-out)방식(거부의사 표시 전까지는 허용)이 있다.
41) 경찰청 사이버테러대응센터 http://www.ctrc.go.kr.

일을 보내고 위장된 사이트로 접속을 유도해 은행 계좌번호, 금융거래용 비밀번호, 기타 개인정보 등을 입력하게 한 후 이를 이용해 불법으로 타인의 예금을 이체하거나 물품구매 사기 등에 악용한다. 또한 최근에는 '파밍(Pharming)'이 신종 인터넷 사기 수법으로 부상하고 있다. 파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS)[42] 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도, 개인정보를 훔치는 새로운 수법으로 기존의 피싱 공격방식보다 사용자들을 쉽게 속일 수 있어 이에 대한 대책 마련이 필요하다. 기존의 피싱 공격이 사회공학적 기법을 가미해 금융기관 등의 웹사이트에서 보낸 이메일로 위장, 링크를 유도해 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내는 반면, 파밍은 아예 해당사이트가 공식적으로 운영하고 있던 도메인 자체를 중간에서 탈취한다. 사용자들은 늘 이용하는 사이트로 알고 의심 없이 탈취된 해당사이트를 이용해 개인ID, 패스워드, 계좌정보 등을 쉽게 노출시키는 것이 특징[43]이라고 한다.

또한 최근에는 인터넷을 이용한 전자상거래가 활발해지면서 카드결제, 휴대폰 인증 및 가정용 전화 인증을 통한 요금결제, 인터넷계좌이체 등의 결제수단이 널리 사용되고 있으며, 이 점을 이용하여 타인의 전화번호를 도용하여 물품 구입대금을 결제하거나, 게임 아이템 · 사이버머니 등을 구입하여 다른 사람에게 요금이 부과되게 하는 범죄가 많이 발생하고 있다. 보통 전화요금 결제사기는 게임을 할 때, 게임상의 대화창을 통해 운영자인 척 하면서 아이템을 공짜로 주겠다고 하거나, 공짜로 얻는 방법을 알려주겠다, 또는 이벤트에 당첨되었다며 접근하여, 집 전화번호나 주민등록번호 등의 개인정보(청소년들의 경우에는 부모님의 개인정보)를 물어보아 이렇게 알게 된 타인의 개인정보를 이용하여 게임 아이템이나 물건 구입 결제를 하고 피해자에게 요금이 부과되게 하는 방식으로 이루어지고 있다.

---

42) TCP/IP 애플리케이션에서, 'chollian.dacom.co.kr'와 같은 주 컴퓨터의 도메인 네임을 '164.124.101.2'와 같은 IP 주소로 변환하고 라우팅 정보를 제공하는 분산 데이터베이스 시스템으로 통신하려는 상대 호스트의 IP 주소를 모를 때 도메인 네임 시스템(DNS)에 조회하면 DNS는 그 호스트의 도메인 네임을 IP 주소로 바꾸어 알려주는 역할을 한다.

43) 정완, "사이버범죄의 주요동향과 형사정책적 과제", 「형사정책연구」제18권 제3호, 한국형사정책연구원, 2007, 1512~1513면.

② 불법복제

불법복제는 저작권법의 창작물에 대한 저작권을 침해하는 행위이다. 인터넷의 발달로 불법복제가 쉬워지면서 과거 불법복제되어 오프라인에서 거래되던 컴퓨터프로그램·영화·음반CD들이 최근에는 인터넷을 통해 파일 형태로 유포되거나 인터넷을 매개로 판매되는 등, 불법복제물의 유포 및 판매가 사이버범죄의 한 형태로 나타나고 있다. 특히 최근에는 자신의 컴퓨터에 관련 프로그램만 설치하면 동일한 프로그램을 사용하는 다른 사람의 컴퓨터에 보관되어 있는 자료를 공유할 수 있는 P2P(peer to peer)[44] 방식의 인터넷 자료공유 서비스가 확산되면서 자료공유를 원하는 네티즌들 사이에 범죄의식 없이 불법복제된 컴퓨터 프로그램이나 영화 및 음반들이 유포되고 있다. 음악, 사진, 영화, 글 등은 그것을 만든 사람에게 사용할 모든 권리가 주어져 있으며 그 권리를 '저작권'이라고 한다. 노래나 영화뿐만 아니라, 다른 사람이 찍은 사진이나 창작한 글 · 그림, 또 신문기사 등도 저작권이 인정되는 것으로, 이런 저작물을 P2P프로그램을 이용하여 전송하거나 받는 것, 다른 사람의 홈페이지에서 무단으로 사진이나 글 등을 복사하여 쓰는 것 등은 모두 저작권을 침해하는 행위로서 최근에는 저작권자들이 적극적으로 자신의 권리 찾기에 노력하고 있고 그에 관한 신고가 증가하고 있다.

③ 사이버 폭력

최근 탤런트 최진실씨의 자살사건에서 피해자에 대한 악성 루머가 주요 원인이 되었음이 밝혀진 후 사이버공간상의 모욕 및 명예훼손 행위의 심각성이 크게 사회문제화 되고 있다. 사이버모욕이나 사이버명예훼손 · 사이버스토킹 등 타인의 정신적 공황을 가져오는 범죄를 이른바 '사이버폭력' 범죄로 부른다. '사이버폭력'이란 아직 확정된 개념은 아니며 다의적이고 논쟁적인 개념이다. 대체로 사이버공간에서 행해지는 온갖 형태의 폭력적 표현행위를 포함하는 개념이라 하겠다. 사이버폭력의 일반적 사례로는 특정인에 대하여 모욕적인 언사나 욕설 등을 게시판에 올리거나 메모 또는 채팅 상에서 행하는 '사이버 모욕', 특정인에 대한

44) PC 대 PC, 개인 대 개인처럼 서버의 도움 없이 1:1 통신을 하는 관계. 공급자와 소비자, 서버와 클라이언트 등의 주종 관계나 상하 관계를 벗어나 참여자 모두가 참여하는 동등한 관계를 말한다. 인터넷에서는 주로 개인들 간의 파일 공유 수단으로서 PC와 PC를 상호 공유하도록 연결해 주는 것을 의미하는데, 콘텐츠의 저작권 문제와 성능과 안정성 문제가 제기되고 있다.

허위의 글이나 명예에 관한 사실을 인터넷게시판 등에 올려 불특정 다수인에게 공개하는 '사이버명예훼손', 인터넷상에서 음란한 대화를 강요하거나 성적 수치심을 주는 대화로 상대방에게 정신적 피해를 주는 '사이버성희롱', 인터넷 또는 PC통신상의 대화방, E-mail 등 정보통신망을 이용하여 특정인에게 원하지 않는 접근을 지속적으로 시도하거나 성적 괴롭힘을 행사하는 '사이버 스토킹', 인터넷이나 PC통신망의 대화방을 이용하여 원조교제를 유도하거나 알선 · 중개하여 10대 매매춘을 확산시키는 '사이버성매매' 등을 들 수 있다. 특히 사이버 명예훼손 · 모욕은 기존 명예훼손 · 모욕과 달리 매우 다양한 매체를 통하여 행해진다. 즉, 단순한 텍스트에 의한 경우는 물론 컴퓨터로 변조한 화상을 이용하거나, 음란 사진 또는 동영상을 이용하는 경우, 타인이 작성한 명예훼손성 글을 퍼뜨리는 2차적 명예훼손 등 다양한 방법을 통하여 행하여진다. 특히 퍼나르기에 의한 명예훼손의 확산은 일반 현실공간의 범죄에서는 찾아볼 수 없는 특수한 피해라고 할 수 있다. 이에 따라 명예훼손 피해자의 의사에 따라 가해자의 범죄에 대한 처벌 여부를 고려해야 하는 현실범죄로서의 명예훼손 · 모욕죄와는 그 처벌의 요건과 방법을 달리할 필요성이 발생하는 것이다. 사이버공간은 빠른 전파력이 특징인데다 익명성이 상당 부분 보장돼 정치인이나 연예인 등 유명인뿐 아니라 누구라도 명예훼손의 피해자가 될 수 있다는 점에서 사이버명예훼손 문제의 심각성은 크다고 하겠다. 현재 정보통신망이용촉진및정보보호등에관한법률[45]에서는 이러한 사이버범죄의 특수성을 고려하여 '사람을 비방할 목적으로'라는 요건을 추가하여 형법의 일반명예훼손죄[46] 보다는 무겁게, 출판물에 의한 명예훼손죄[47]와 유사한

---

45) 제70조 (벌칙)
① 사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실을 적시하여 타인의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처한다.
② 사람을 비방할 목적으로 정보통신망을 통하여 공연히 허위의 사실을 적시하여 타인의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

46) 제307조 (명예훼손)
① 공연히 사실을 적시하여 타인의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
② 공연히 허위의 사실을 적시하여 타인의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처한다.

47) 제309조 (출판물등에 의한 명예훼손)
① 사람을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 제307조 제1항의 죄를 범한 자는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에 처한다.
② 제1항의 방법으로 제307조 제2항의 죄를 범한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 1천500만원 이하의 벌금에 처한다.

처벌 규정을 두고 있다.

사이버 스토킹 또한 우리나라에서는 현재까지 사이버스토킹을 구체적으로 범죄로 규정하지 않고 사이버 성폭력의 한 사례로 분류하고 있으나 외국에서는 사이버 스토킹을 독립된 하나의 범죄로 중요하게 취급하고 있으며 우리나라도 스토킹에 대한 입법이 요구되고 있는 실정이다.

④ 불법 · 유해사이트

공공의 안녕 · 질서 또는 미풍양속을 해하는 등 반사회적 내용을 담고 있는 사이트로 개설목적 자체가 법률에 위반되거나 범죄수단으로 사용되는 위법사이트를 포함한다. 접근의 제한이나 이용의 제약이 없는 인터넷을 이용하여 각종 불법행위에 대한 정보교환 등이 이루어지고 있으며 특히 자살사이트나 마약거래를 위한 사이트는 물론이고 최근에는 청부살인이나 폭력을 의뢰하는 심부름센터 사이트까지 생겨나 인터넷으로 정보를 주고받음으로써 오프라인 범죄의 모태가 되기도 한다. 누구나 접근할 수 있는 사이버공간에 이러한 유해정보를 제공하는 것은 청소년이나 기타 일반 네티즌 등에게 범죄의 유혹을 제공함으로써 사회적으로도 큰 물의를 빚게 된다. 불법사이트에서 유통되는 정보 중 가장 심각한 것은 음란물과 관련된 정보로써 가장 광범위한 피해를 발생시키고 있으며, 이들 피해는 심리적 불쾌감에서 그치지 않고, 금전적 · 사회적 피해에까지 이르기도 한다. 또한 사이버상에서 유통되는 음란물은 매우 빠르고 은밀하게 전파되는 특성을 갖고 있어 그 영향력은 매우 크다. 그러므로 성별이나 연령에 관계없이 많은 사람들이 이러한 음란물에 쉽게 접할 뿐 아니라 이러한 정보가 쉽게 복제되거나 엄청난 속도로 전파된다는 것은 간과할 수 없는 매우 심각한 문제이다

⑤ 개인정보침해

쇼핑, 오락, 교육, 행정, 금융업무 등 생활 전반이 온라인을 통해 이루어짐에 따라 온라인에서 개인의 성명, 주민등록번호, 주소 및 전화번호 등과 같은 개인정보의 중요성은 점점 커지고 있다. 개인정보침해 범죄의 심각성은 단순히 개인정보가 유출된 것으로 끝나는 것이 아니라 유출된 개인정보가 다른 범죄에 사용될 수 있다는 것에 있으며 이러한 개인정보는 범죄의 표적이 되고 있다. 또한 각

종 포털사이트들이나 전자상거래 사이트에서 회사의 신뢰성과 사업규모를 증명하기 위한 수단으로 가입자의 수를 선전하고 이 가입자수를 늘리기 위해 경쟁적으로 경품을 제공하고 있으며, 경품제공을 조건으로 해당사이트에 가입할 것을 제시하고 있다. 해당 사이트에 가입하기 위해서는 개인의 모든 신상정보를 기재해야 하는 것이 필수적인 과정으로 되어 있기 때문에 이러한 사이트들에는 가입자 수만큼의 개인정보가 메인 서버에 입력되어 있다고 볼 수 있다. 그러나 이러한 메인서버의 보안장치가 완벽하지 못한 경우가 많아 해킹으로 인해 쉽게 개인정보가 유출되고 아울러 일부 악의적인 사이트의 경우 경품을 미끼로 가입자를 모은 후 수집된 개인정보를 인터넷상 거래 업체 등에 돈을 받고 넘기는 경우까지 있다. 또한 국가기관이 효율적으로 업무를 수행하기 위하여서는 개인의 정보가 필요한데 이러한 국가기관에 의한 개인정보 침해도 사이버범죄와 무관하지 않다고 본다[48]. 개인정보는 재화로서의 가치를 갖고 유통되기도 하기 때문에 법에서는 정보통신서비스제공자가 이용자의 동의 없이 개인정보를 수집하는 경우나 개인정보를 취급하거나 취급하였던 자가 개인정보를 타인에게 누설하거나 제공하는 경우 등과 같은 조직적인 개인정보침해행위도 규제하고 있다.

4. 사이버범죄의 실태

국내 사이버범죄의 통계자료는 경찰청 사이버테러대응센터와 대검찰청 첨단수사과 인터넷범죄사센터에서 공개하는 통계자료를 통하여 확인할 수가 있다. 아래에서는 경찰청과 대검찰청의 사이버범죄의 발생현황을 살펴보고 최근의 언론보도 사례를 통하여 그 실태를 파악하고자 한다.

(1) 경찰청 사이버테러대응센터 통계자료

경찰청 사이버테러대응센터의 자료에 따르면 사이버범죄의 발생건수는 2003년 6만8천여건, 2004년 7만7천여건, 2005년 8만8천여건, 2006년 8만2천여건, 2007년 8만8천여건이고 지난 2008년도에는 13만6천여 건으로 꾸준한 증가추세

48) 김종세, 전게논문, 237~238면.

를 보이고 있다[49]. 표 2-1에서 보이듯이 이중 사이버테러형 범죄보다 일반사이버 범죄의 발생건수가 월등히 많은 것을 볼 수 있다.

<표 2-1> 사이버범죄의 발생과 검거 현황

구분 / 연도	총계			사이버테러형 범죄		일반사이버 범죄	
	발생	검거	검거율	발생	검거	발생	검거
2003	68,445	51,722	75.6%	14,241	8,891	54,204	42,831
2004	77,099	63,384	82.2%	15,390	10,339	61,709	52,391
2005	88,731	72,421	81.6%	21,389	15,874	67,342	56,547
2006	82,186	70,545	85.8%	20,186	15,979	62,000	54,566
2007	88,847	78,890	88.7%	17,671	14,037	71,176	64,853
2008	136,819	122,227	89.3%	20,077	16,953	116,742	105,274

출처 : 경찰청 사이버테러대응센터

사이버범죄는 2008년에 총 136,819건 발생 중에서 122,227건을 검거하였다. 사이버범죄를 유형별로 살펴보면 표 2-2에서 나타나듯이 불법복제 및 판매가 32,084건으로 가장 많고, 인터넷사기가 29,290건, 해킹 · 바이러스 16,953건이 그 뒤를 이었다. 범죄 유형별 주요 범죄 양상을 살펴보면 저작권법 위반행위가 불법복제 및 판매의 다수를 이루었고, 인터넷 사기에서는 허위쇼핑몰 개설, 대포폰 · 대포통장을 이용한 1:1 직거래사기, 온라인 게임 아이템 사기 등이 주류를 이루었으며, 해킹은 시스템 해킹과 전자우편 및 게임 계정 해킹이 대부분을 차지하였다. 사이버범죄는 2000년 이후 2005년까지 지속적으로 증가하다가 2006년에 소폭 감소 후 다시 증가세를 보이고 있다. 특히 2008년도에는 사이버범죄 발생건수가 전년대비 약 54% 증가하였는데 이는 불법복제 판매에 대한 유관기관의 집중 단속의 결과로 분석하고 있다[50]. 경찰은 매년 인터넷 사기 · 도박, 불법 음란 · 스팸메일, 사이버폭력 등 시의성 있는 주제를 선정하여 전국 또는 지방청 단위 집중수사로 강력한 단속활동을 전개하고 있다. 특히 2008년에는 경기침체에 따른 「민생침해 사이버사범 집중단속」을 실시('08.3.1~4.30)하여 총 6,469건 8,198명을 검거(구속 130명, 불구속 8,068명)하였고, 허위 사실 유포에 의해 연예인이 자살하는 등 사회적으로 큰 문제가 됨에 따라 「허위사실

49) 경찰청 사이버테러대응센터 http://www.ctrc.go.kr
50) 경찰청, 2009 경찰백서, 116면.

유포 및 악성댓글 집중단속」을 실시('08.10.6~11.5)하여 총 1,842건 2,030명을 검거(구속 11, 불구속 2,019)하는 등 사이버치안 확보를 위해 노력하고 있다[51]. 그러나 2007년 이후부터 2008년까지 사이버범죄가 다시 급격히 증가하고 특히 사이버폭력이나 불법사이트 운영, 불법복제판매 범죄의 경우 오히려 2006년 이후 급격히 증가하였다. 또한 사이버범죄의 현황이나 발생건수에 대한 검거율을 살펴보면 사이버범죄에 대한 경찰 대책에 대한 실효성은 크게 효과를 보이고 있지 않은 것으로 판단된다.

<표 2-2> 유형별 사이버범죄 발생 · 검거 현황

유형 / 년도		총계	사이버테러형 범죄		일반사이버범죄					
			해킹	바이러스	통신사기 게임사기	명예훼손 성폭력 등	개인정보 침해	불법사이트 운영	불법 복제 판매	기타
발생	'08	136,819	19,950	127	36,591	9,543	5,769	7,723	33,537	23,579
	'07	88,847	17,593	78	31,685	10,028	4,214	5,229	8,866	11,154
	'06	82,186	20,119	67	33,041	7,881	2,839	6,798	2,313	9,128
	'05	88,731	21,336	53	42,675	6,642	3,759	1,836	1,257	11,173
	'04	77,099	15,348	42	40,283	3,667	3,137	2,308	1,064	11,250
검거	'08	122,227	16,854	99	29,290	8,690	5,129	8,056	32,084	22,025
	'07	78,890	13,988	49	28,081	9,164	3,741	5,505	8,167	10,195
	'06	70,545	15,934	45	26,711	7,109	2,327	7,322	2,284	8,813
	'05	72,421	15,831	43	33,112	6,338	2,889	1,850	1,233	11,125
	'04	63,384	10,955	38	30,288	3,751	2,065	2,410	1,244	12,633

출처: 2009 경찰백서

(2) 대검찰청 첨단범죄수사과 인터넷범죄수사센터

경찰청과는 별도로 검찰청에서 처리하고 있는 사이버범죄의 단속실태는 인터넷범죄수사센터에서 1997년부터 2008년까지의 자료를 공개한 컴퓨터범죄의 유형별 처리현황에 제시되어 있다[52]. 인터넷범죄수사센터는 컴퓨터범죄의 유형을

51) 정재봉, 전게논문, 37면.
52) 대검찰청 첨단수사과 인터넷범죄수사센터 http://www.spo.go.kr

공용전자기록손상 등 전자문서관련죄, 전산업무방해, 전자기록비밀침해, 컴퓨터사용사기, 전자기록손괴, 정보통신망법, 개인정보보호법, 기타 특별법 등으로 분류하여 발생건수, 인원, 구속인원에 대한 통계를 공개하고 있다.

2003년도에 12,501건 15,575(1,745)명, 2004년도에 11,523건 15,683(1,104)명, 2005년도에 12,672건 19,234(1,766)명, 2006년도에 15,652건 23,951(986)명, 2007년도에 20,886건 32,449(944)명, 2008년도에 25,509건 36,330(661)명 등으로 꾸준한 증가추세를 보이고 있으며, 1997년부터 12년간 총 108,273건에 155,723명 입건, 8,866명 구속으로 나타나고 있다. 특히, 사이버범죄의 중심법이라고 할 수 있는 정보통신망 이용촉진 및 정보보호에 관한 법률위반사범의 숫자는 크게 높아 12년간 총 58,159건에 73,210명 입건, 1,659명 구속으로 나타났다.

<표 2-3> 대검찰청 컴퓨터범죄의 유형별 처리현황

연도 / 범죄유형	2003		2004		2005		2006		2007		2008	
	건	인원수 (구속)	건	인원수 (구속)	건	인원수 (구속)	건	인원수 (구속)	건	인원수 (구속)	건	인원수 (구속)
공용전자기록 손상등	2	4(0)	1	2(0)	2	4(1)	1	1(1)	2	2(0)	0	0(0)
전자문서 관련죄	535	694 (117)	890	1442 (282)	2406	5752 (1133)	3016	7051 (555)	4029	10580 (521)	4336	11058 (255)
전산업무방해	26	43(2)	33	39(8)	27	35(0)	84	103 (4)	54	100 (4)	38	47(2)
전자기록 비밀침해	10	16(0)	7	10(0)	3	3(1)	12	19(0)	13	20(0)	6	13(0)
컴퓨터 사용사기	2403	2777 (846)	1634	2040 (323)	1208	1465 (203)	1127	1314 (154)	1478	1650 (175)	1324	1524 (166)
전자기록손괴	8	9(0)	12	18(0)	12	12(1)	17	18(1)	18	26(0)	13	21(1)
정보통신망법 (명예훼손)	837	1091 (25)	1040	1420 (37)	1569	2257 (43)	1911	3379 (29)	2100	3850 (14)	2113	3159 (10)
정보통신망법 (개인정보 누설 등)	53	123 (12)	51	92 (13)	69	143 (19)	94	204 (15)	136	261 (16)	100	246 (1)
정보통신망법 (정보통신망 침해 등)	1248	1459 (95)	1204	1409 (61)	1188	1450 (80)	1465	1775 (52)	1487	1760 (36)	1993	2396 (47)
정보통신망법 (음란물유통)	1145	1568 (93)	2164	2663 (143)	2807	3435 (147)	4729	5435 (113)	6684	7796 (98)	6056	6595 (25)
정보통신망법 (기타)	2248	2789 (12)	1763	2191 (56)	1920	2424 (45)	1746	2323 (27)	3023	3499 (53)	5216	6018 (134)
개인정보 보호법	72	114 (2)	75	131 (5)	112	215 (10)	127	218 (10)	160	236 (5)	188	312 (3)
사기 (컴퓨터범죄)	2992	3477 (255)	1741	1988 (110)	668	773 (46)	450	525 (9)	235	275 (5)	226	254 (10)
기타특별법	922	1411 (118)	908	2238 (66)	681	1266 (37)	873	1586 (16)	1467	2394 (17)	3900	4687 (7)
총계	12501	15575 (1745)	11523	15683 (1104)	12672	19234 (1766)	15652	23951 (986)	20886	32449 (944)	25509	36330 (661)

출처 : 대검찰청 첨단수사과 인터넷범죄수사센터

5. 사이버범죄의 최근 동향

사회 전반적으로 인터넷 의존도가 심화됨에 따라 해킹, 분산 서비스거부 공격, 악성코드 감염 등 침해사고로 인하여 국가기관 · 첨단기업 중요자료 절취, 개인정보 유출, 프라이버시 침해, 금전적 갈취 등의 정보화 역기능이 지속적으로 발생하고 있다. 따라서 최근의(2007~2009) 사이버범죄에 대한 동향과 사례를 분석하여 새롭게 대두되고 있는 사이버범죄의 유형과 그 피해의 위험성에 대해 살펴보고자 한다.

(1) 단순 웜 · 바이러스는 감소, 금전적 목적의 악성코드 유포와 해킹으로 개인정보 유출 피해의 지속적 증가

2007년도에 정부에 접수된 웜 · 바이러스 신고건수는 5,996건으로 2006년 7,789건에 비하여 23.0% 감소하였다. 감소한 원인은 최근 들어 지적호기심, 컴퓨터 사용능력 과시를 목적으로 네트워크를 통해 대량 전파되는 단순 웜 · 바이러스 제작 및 유포가 감소했기 때문이다[53]. 반면 2008년도에 국가사이버안전센터에 접수된 웜 · 바이러스 감염은 5,655건이며, 방송통신위원회에 접수된 웜 · 바이러스 신고건수는 8,469건으로 2007년(총 5,996건)에 비하여 41.2% 증가하였다. 단순한 지적호기심, 능력과시 목적의 웜 · 바이러스 제작 · 유포는 점차 감소하는 추세이나, 온라인 게임의 계정정보 탈취 및 허위광고나 경고메시지 등을 통해 사용자의 클릭 및 결제 유도 등 금전적 이익을 목적으로 하는 악성코드 유포는 지속적으로 증가하는 추세에 있다.

경찰청 사이버테러대응센터는 2006년 8월 21일 국내 유명 포털사이트 로그인 화면을 모방하여 약 36만개의 ID와 비밀번호를 불법 수집한 피의자를 검거(불구속)하였고, 2006년 8월에는 국내 ○○은행 사이트 로그인 화면을 모방하여 같은 방법으로 개인정보 1만2천건을 가로챈 피의자 2명을 검거(구속)하였다[54]. 이외에도 2008년 1,100만명이라는 사상 최대 규모의 개인정보유출사고였던 GS칼텍

53) 국가정보원, 2008 국가정보보호백서, 11면.
54) 경찰청, 2009 경찰백서, 118면.

스 사고를 비롯하여, 엔씨소프트의 아이디 유출사고, 옥션 해킹사고, 하나로 텔레콤 사고, Daum 사고, 대한상공회의소 등과 공공기관의 개인정보노출사고[55]가 이어져 왔고, 수시로 일어나는 중국 해커들에 의한 해킹 피해사례[56] 등 무수히 많은 개인정보 유출 피해가 잇따르고 있다. 특히 중국발 악성코드 전파 및 해킹이 증가하고 있는데, 중국은 1990년대 중반부터 시스템 및 네트워크에 대한 연구를 통하여 중국 특유의 언더그라운드 해커 문화를 형성하였다. 1990년대 후반 중국 해커들의 기술은 외국에서 개발된 프로그램을 이용하는 수준이었지만 점차 해커들 스스로 트로이목마 및 해킹 프로그램을 제작하기 시작하였고, 최근에는 국내 국가·공공기관의 시스템을 해킹하여 주요 자료를 빼내가거나 웹서버 해킹을 통하여 우리나라 국민의 개인정보를 유출하는 수준에 이르고 있다. 중국발 해킹은 우리나라뿐만 아니라 미국 등도 목표가 되고 있어 미 육군에서는 PC를 매킨토시로 교체하는 작업까지 수행하고 있는 상황이다. 그만큼 중국발 해킹은 전 세계적으로 큰 위협으로 자리 잡고 있다. 중국발 해킹에서 개인정보를 빼내가는 절차를 보면, 우선 접속자가 많은 유명사이트의 웹서버를 해킹하고, 악성코드를 은닉한 뒤, 보안이 취약한 PC를 이용하여 해당 웹사이트에 접속하는 인터넷 이용자의 PC를 악성코드에 감염시킨다. 감염된 접속자 PC에 상주하며 주민등록번호, 각종 사이트 아이디 및 비밀번호를 추출하여 개인정보를 해커 컴퓨터로 이동시키는 방법을 이용하고 있다. 심지어 중국 내에서 한국의 웹서버를 해킹하는 방법이나 한국인의 개인정보를 취득하는 해킹기법에 대한 자세한 설명과 도구가 담겨져 있는 잡지가 시중에 유통되고 있는 상황이다. 하지만 국가차원에서 중국발 해킹에 대한 근원지를 조사하는 과정에서 중국 내 IP가 근원지로 확인된 경우에도 중국과의 사법공조협정이 체결되지 않아 공격자 조사에 어려움을 겪고 있다. 향후에도 이러한 중국발 해킹 및 악성코드의 전파는 계속적으로 증가할 것으로 예상된다[57]. 더욱이 취약한 웹서버를 사전에 해킹한 후 초기화면에 악성코드를 은닉하여 해당 사이트 방문자 PC를 악성코드에 감염시키는 침해사례는 이미 2006년도에 발생하였으나 2007년도에는 대상 웹서버를 실제 해킹하지 않고

55) 2006년 국정감사에서 심재엽의원 제출자료에 의하면 81개 공공기관의 개인정보유출이 있었다고 한다.
56) 2007년 2월 메이플스토리와 한게임 등의 국내 1천여개사의 아이디와 비밀번호 해킹사건을 들 수 있다.
57) 국가정보원, 2008 국가정보보호백서, 13~14면.

도 정상적인 인터넷 사용자가 특정 웹사이트로 접속하는 트래픽을 가로채어 변조함으로써 인터넷 이용자의 PC를 악성코드에 감염시키는 이른바 ARP(Address Resolution Protocol)스푸핑[58]을 이용한 악성코드 유포사례가 새롭게 출현하였다. 또한 자동화 도구에 의한 손쉬운 변종 제작 및 마이크로소프트 오피스, 어도비 아크로뱃 등 복합적 전파경로의 확대로 공격 성공 가능성을 높이고, 자기 은폐기술의 진화 등 생존력을 높이기 위한 기술이 적용되어 악성코드 기술이 갈수록 대응 및 치료가 어렵게 진화 · 발전하고 있다[59]. 2007년 한국정보보호진흥원의 발표에 따르면 2007년 한해 개인정보유출피해는 주민번호 도용이 7,111건(78%), 아이디도용 886건(10%), 타인정보침해 659건(7%), 전화번호도용 269건(3%), 게임아이템도용 161건(2%)의 순으로 밝혀져 개인정보 중에서 '주민등록번호'의 유출피해가 가장 심각한 것으로 드러났다.

(2) 조직적 사이버범죄 심화

소규모 음성적 사이트를 대상으로 시작된 금품요구 목적의 협박성 분산서비스거부(DDoS)공격은 게임, 쇼핑몰, 증권사 등 사회 전반의 모든 분야를 대상으로 확대되어 지속적으로 발생하였다. 더욱이 이러한 협박성 분산서비스거부 공격은 분산서비스거부 공격용 악성코드 제작자, 유포자, 금품요구 및 협박자, 분산서비스거부 공격자 등 각기 고유한 역할을 가진 조직화된 사이버범죄로 발전하였으며, 일회성으로 끝나지 않고 특정시즌을 겨냥하거나 해당 업체의 경제적 파급효과와 고객과의 관계까지 감안하여 공격대상을 선정하는 등 날로 지능화된 수법을 보이고 있다. 여기에 '넷봇(Netbot)'과 같은 자동화된 분산서비스거부 공격도구를 통해 한 번의 공격으로도 일반적인 회선 대역폭을 초과하는 수십Gbps까지 트래픽을 유발시킴으로써 보안장비를 통한 방어도 한계에 이르고 있다[60].

(3) 사회적 갈등의 온라인 표출 심화

58) 네트워크 어댑터의 물리적인 주소(MAC 어드레스) 정보를 위조하여 정상 사용자의 네트워크 트래픽을 공격자가 의도한 특정 시스템으로 전달되도록 하는 해킹수법의 일종.
59) 국가정보원, 2009 국가정보보호백서, 52면.
60) 국가정보원, 2009 국가정보보호백서, 53면.

2007년 에스토니아 정부 사이트에 분산서비스거부 공격에 이어 2008년도에도 러시아 · 그루지야 간 '현실세계의 전쟁'과 함께 '사이버 전쟁'으로 그루지야 정부기관 및 기간산업 전산망이 마비되었다. 국내에서도 2008년 초 한 · 미 쇠고기 및 FTA협상, 한반도 대운하 등의 사회적 찬반 논쟁이 오프라인을 넘어 일부 정부기관 웹사이트를 대상으로 변조, 분산서비스거부 공격 등 온라인의 사이버 시위로 이어졌으며, 일본 중학교 사회 학습지도 요령 해설서의 독도 표기 등 독도에 대한 한 · 일 네티즌간의 사이버공격은 이제 연례 행사화 되어가고 있다. 이외에도 국내 포털사이트의 한 카페에서 강제 탈퇴당한 10대 청소년이 이에 앙심을 품고 분산서비스거부 공격을 하여 불구속 입건된 사례도 있었다. 이처럼 사회적 갈등으로 인한 의사표현이 이제는 사람들이 모여 벌이는 집회 등에서 사이버상의 온라인 시위로 표출되고 있으며 이는 점차 심화될 것으로 보인다[61].

(4) 사회공학적 기법의 지능화

보이스 피싱과 같이 사람의 심리를 이용하는 사회공학적 기법의 위협이 어제오늘의 얘기는 아니다. 그럼에도 연초 사법기관을 대상으로 벌금이 부과되었다는 피싱메일 발송을 통해 주민번호 등 개인정보를 입력하도록 유인한 사례를 시작으로, MSN 메신저 이용자의 친구 목록으로 URL이 전송되어 해당 이용자가 별의심없이 클릭하면 '누가 당신을 MSN으로부터 차단했는지 확인해보라'거나, 네이트온 메신저로 친구인척 대화를 걸고 급히 돈이 필요하다며 특정계좌로 송금을 받는 사기사고가 발생하기도 하였다. 또한 일부 도박사이트에서 게임 프로그램 설치 시 악성코드가 동시에 설치되거나 'CNN속보', '베이징 올림픽', '세계 3차 대전 시작' 등과 같이 메일 수신자들을 현혹하는 문구를 포함하는 메일을 발송하여 허위 백신을 설치하게 한 후 PC에 악성코드가 설치되어 있는 것처럼 속여 악성코드 치료를 위한 결제를 요구하는 사례 등, 사이버범죄의 큰 흐름이 조직화 · 고도화 될 뿐만 아니라 금전적 이익을 목적으로 하는 공격성향과 맞물려 사회공학적 기법까지 갈수록 지능화 되어가고 있다. 이와 같은 사고들은 사회공

61) 국가정보원, 2009 국가정보보호백서, 53~54면.

학적인 방법이 활용되어 개인 이용자들을 속이므로, 생활의 일부로 이용되고 있는 인터넷에 대한 신뢰를 무너뜨릴 수 있으며 피해 예방을 위해서는 사용자들의 주의를 더욱 필요로 한다[62].

(5) 웹 2.0 보안 고려 필요성 대두 및 UCC의 역기능

웹 2.0환경에서는 정보 소비의 주체로만 여겨졌던 사용자가 정보 생성의 참여자로, 의견을 제시하고 타인과 연계해 전문가 수준의 영향력을 갖게 되었다. 이는 사용자의 정보 접근성과 편의성이 높아지고, 사용자가 정보를 능동적으로 이용하게 되었음을 의미한다. 또한 정보자체 측면에서 볼 때 다양성과 품질이 향상되는 특성도 보이고 있다. 결국 인터넷 업계에서는 웹 2.0이 하나의 추세이자 새로운 비즈니스 모델로 자리 잡아 가고 있다고 볼 수 있다. 하지만 웹 2.0기술을 도입하고자 할 때 보안을 고려해야 하는데, 사용자의 참여가 높은 개방성의 특징을 갖는 환경이므로 기존 웹이 가지고 있는 취약점보다 더 많은 보안 취약점이 존재하게 된다. 또한 웹 2.0에서는 검증되지 않은 정보의 공개로 인하여 개인 프라이버시 침해의 문제가 발생할 수 있다. 웹 2.0환경의 미국의 MySpace에서 동영상 재상을 위해 사용하고 있는 애플사의 Quick Time 동영상 파일에 악성 자바 스크립트를 삽입해 동영상을 재생하면 피싱사이트로 연결되어 사용자의 계정정보를 유출하려는 시도가 있었다. 따라서 웹 2.0환경에서는 보안을 더욱 중요시해야 하며 발생 가능한 보안 위협에 대하여 철저한 대응이 필요하다[63].

또한 최근에는 UCC[64]가 유행하면서 그 피해 또한 증가하고 있다. 2006년 6월 호주의 한 여대생은 UCC사이트인 유튜브에 '에멀리나(Emmalina)' 라는 필명으로 애완동물 · 운동 · 취미 등 자신의 일상을 공개하는 동영상을 연재했고, 이 동영상은 조회수가 30만을 기록하는 폭발적인 인기를 끌며 인터넷 백과사전 위키피디아에 등재되기도 했다. 그러나 이 여대생은 이어지는 개인정보 해킹 및 악용, 음해성 동영상 · 악플 등에 시달리다 2개월만에 자신의 프로필과 동영상 콘

62) 국가정보원, 2009 국가정보보호백서, 54~55면.
63) 국가정보원, 2008 국가정보보호백서, 12면.
64) UCC(User Created Contents) 즉, 사용자 제작 컨텐츠를 뜻하는 신조어로서 개인적으로 직접 만든 저작물들을 일컫는다.

텐츠를 모두 삭제했고, 유명해지는 것이 꼭 좋은 것만은 아니라는 취지의 글을 남기고 떠났다. UCC는 선거결과에도 영향을 미친다. 2006년 미국 중간선거에서 공화당 조지 앨런 상원의원이 인도계 청년을 향해 '원숭이'라고 말하는 동영상이 퍼지자, 승리가 예상됐던 그는 낙선했다. 이처럼 UCC를 통하여 누구나 새로운 경제적 부를 창출하는 것은 물론 한순간에 스타가 되거나 몰락하기도 한다. UCC가 가져다주는 역기능은 프라이버시 침해, 유해정보, 저작권 · 초상권 침해, 명예훼손 등이다. 개인정보화 도구를 갖춘 영상세대는 소위 '뜨기 위해' 어지간한 개인정보 노출은 가볍게 여긴다. 흥미를 위해 타인의 사생활 등을 쉽게 노출하고 드러내거나 무작위로 사이버 '폄질'도 마다하지 않는다. UCC사이트를 이용하는 네티즌들은 내 개인정보와 마찬가지로 타인의 개인정보를 보호해야 한다. 그렇지 않을 경우 발생하는 인격모독이나 마녀 사냥 등으로 인한 피해는 확산될 것이다. 개인들에게 팽배한 개인정보보호 무의식증과 노출증의 확산은 결국 UCC세상을 위협하게 될 것이다. UCC사이트 운영 기업들의 보안에 대한 시급한 대책도 필요하다. 현재 보안 시장에서 가장 큰 테마는 분산서비스거부(DDoS : Distribute Denial of Service) 공격이 부각되고 있으며 그 공격유형의 하나로서 UCC를 통한 악성코드 확산, 재생을 가장한 스파이웨어 배포, 트로이목마 등을 들고 있으며, 이러한 보안 취약점에 대한 법적 제도적정비가 이루어져야 한다고 강조하고 있다[65].

(6) 인터넷도박의 증가

2009년 상반기 인터넷 불법 도박을 한 회사원과 무직자 등 400여명이 입건되는 사건과 인터넷 도박장을 개설, 네티즌에게서 판돈을 끌어 모아 4억원의 부당이득을 챙긴 운영자가 구속되는 등 최근 불법 인터넷 도박이 성행하고 있다. 사행성 인터넷 도박을 벌인 혐의로 적발된 이들은 주부, 대학생, 교수, 의사, 세무사, 교사 등 누구나 인터넷을 쉽게 접속할 수 있는 만큼 직업군도 다양했다. 실제 오프라인에서 벌어지는 도박에 비해 인터넷도박은 남의 시선이나 장소에 구애받지 않고 집에서 편하게 할 수 있고 소액으로 시작해 잘 만하면 뭉칫돈도 쥘

65) 보안뉴스, 2009.10.17.

수 있다는 유혹 때문에 이용하는 네티즌이 적지 않다는게 경찰의 지적이다. 인터넷 사이트 순위를 매기는 랭킹닷컴에 따르면 이 같은 유료 게임사이트가 전국에 40여개나 되고 이용자도 수백만명에 달할 것으로 추정되고 있다. 이들 사이트 운영자들은 단속을 피해 필리핀이나 캄보디아 등지의 해외서버를 이용하고 게임머니를 현금으로 환전해주면 불법인 것을 알면서도 '진짜 돈이 오가는' 돈 버는 장사를 포기하지 않고 편법으로 운영했던 것으로 드러났다. 이들은 도박을 위해 게임머니를 구입할 때는 부가세 명목, 환전수수료 명목으로 거래되는 현금의 20~30%까지 챙기는 등 수입이 적지 않아 앞으로도 경찰 단속망을 피하면서 계속 운영할 것으로 경찰은 보고 있다. 최근에는 해외에 인터넷도박 사이트를 개설, 도박장을 운영한 운영자에게 도박개장죄를 적용하고, 그 심각성에 비추어 실형이 선고되기도 하였다[66]. 또한, 지난 1999년 미국의 국립도박중독연구소의 조사에 따르면 온라인 도박은 즉각적인 욕구 충족과 프라이버시 보장 때문에 도박의 폐해를 증대시키며, 영국 정부가 지원한 연구 결과에서도 합법적인 오프라인 카지노 방문객은 20%만이 문제를 일으키거나 중독되는 것으로 나타났지만 온라인 도박의 경우 이 비율이 75%까지 높아졌다는 보고가 온라인 도박 피해의 심각성을 보여주고 있다[67].

(7) 인터넷 사기의 증가

인터넷 쇼핑몰 · 오픈마켓 등의 성장으로 전자상거래 규모는 지속적으로 증가함에 따라 허위의 물품거래 사이트를 개설한 사기범죄 또한 증가하고 있으며 전자상거래의 선지급 · 후배송을 이용한 인터넷 사기범이 주로 발생하고 있다[68]. 게임사기 역시 빈번하게 이루어지는데 인터넷 이용자 중 특히 청소년의 경우 게

66) 청주지법 형사2단독 김정곤 판사는 해외에 인터넷 도박 사이트를 개설한 뒤 도박장을 운영한 최모씨(34)에 대해 도박개장죄를 적용, 징역 1년에 추징금 1400여만원을 선고했다. 김 판사는 "인터넷 도박은 서민들로 하여금 게임에 빠져들게 해 가정파탄에 이르게 하고 게임중독자 및 신용불량자를 양산하는 등 심각한 사회적 폐해를 유발하고 있어 이를 엄히 처벌할 필요가 있다"고 덧붙였다; 뉴시스, 2009.11.15.

67) 서울경제, 2009.11.10.

68) 인터넷 사기 쇼핑몰이 여전히 기승을 부리고 있습니다. 가전제품에서 가짜 명품까지 사기 사이트 종류도 다양해지고 수법도 지능화되고 있는 것으로 나타났습니다. 시중가격보다 훨씬 싸게 판다며 현금 결제를 유도한 뒤, 돈만 받고 물건은 보내지 않았습니다.(중략) 지난 2005년부터 서울시 전자상거래센터가 적발한 사기 사이트는 197곳. 신고된 피해자 수만 4,000명이 넘고 피해금액도 26억 8,000만 원에 이릅니다. 사기 피해 품목 가운데는 가전제품과 컴퓨터, 상품권 등이 가장 많았습니다; YTN 2009.6.25.

임을 하기 위해 인터넷을 이용하는 경우가 많다. 게임에 중독된 청소년을 현혹하여 게임에 필요한 아이템 등을 불법거래하거나 대금을 받고 잠적하는 등의 사례들이 많이 일어나고 있다[69].

(8) 불법사이트의 다양화

불법사이트에는 음란, 도박, 마약 및 의약품 판매, 자살조장 사이트, 대포차 · 장기매매 · 신분증 위조 · 성매매 · 폭발물 제조 및 판매 등의 사이트가 있다. 최근의 언론에 보도된 내용은 자살 관련 정보의 유통이 광범위하게 이루어지고 있다고 주장하고 있다. 2005년 8월 22일 '한국일보'의 보도에 따르면, 최근 들어 자살카페가 급증하고 있다고 한다. 한때 경찰의 단속으로 잠시 주춤했던 자살카페가 급격히 퍼지면서 자살풍조가 확산되고 있다는 것이다. 포털사이트의 '자살', 'suicide' 등을 금칙어로 설정, 자살카페의 생성을 막고 있다. 그러나 금칙어를 교묘하게 바꿔 자살카페를 만들거나 안티 자살 사이트로 가장한 유사 자살카페를 만드는 사례가 많이 발생하고 있다. 이들 자살카페에서는 독극물까지 거래되고 있는 등 피해가 심각하다. 실제로 이 사이트들에는 독극물을 사고 판다는 글, 자살을 도와주는 자살 도우미, 고통을 덜 받으면서 자살에 이를 수 있다는 구체적인 방법까지 묘사되어 있다. 대다수의 자살 사이트들은 '자살'과 같은 금기어는 포함시키지 않은 채 자살 사이트임을 유추할 수 있는 카페명을 통해 회원을 모집한다. 웬만한 변칙어로 검색되지 않을 경우 자살과 연관있는 단어를 통해 검색되도록 하는 등 사이트는 우후죽순격으로 늘어나는 실정이다[70]. 최근 강원지방경찰청에 따르면 상반기 도내에서는 모두 9건의 동반자살이 시도돼 모두 18명이 숨지고 11명이 구조됐다. 올 들어 첫 동반자살은 지난 4월 8일 정선의 한 민박에서 발생했는데 남자 2명과 여자 2명이 방안에 연탄불을 피우는 방식으로 자살을 기도, 모두 숨졌고 곧바로 동반 자살이 잇따랐다. 경찰은 대부분 인터넷 자살사이트나 카페 등을 통해 만남을 갖고 동반 자살을 선택한 것으로 보고 있다[71].

---

69) 2001년 5월부터 2003년 6월까지 진해 거제지역의 PC방에서 인터넷 리니지게임의 사이버머니인 아데나를 판매한다고 속여 40명으로부터 1,500만원을 교부받아 편취한 10대 상습피의자 검거;경찰청 사이버테러대응센터,http://www.ctrc.go.kr/example/index.jsp

70) 정재봉, 전게논문, 43~44면.

이외에도 주변에서 쉽게 구할 수 있는 재료들을 사용하여 폭탄을 제조할 수 있는 방법을 소개하는 한편 적극적으로 폭탄제조를 선동하는 글이 게시된 이른바 '폭탄사이트'들이 경찰에 적발되는 사례가 많이 발생한다. 신문사 기사에 따르면 경찰에 적발된 폭탄사이트의 운영자가 주로 청소년, 대학생 등 나이어린 학생들로 드러났다[72]. 실제 폭탄이 사용되어 인명 및 재산피해도 발생[73]했다[74].

2005년 7월 21일 '문화일보' 기사는 해외에 서버를 두고 국내에서 인터넷 성매매를 알선하는 사이트들이 운영되고 있는 실태를 소개하고 있다. 기사에 따르면 이들 사이트는 포털사이트의 뉴스 댓글이나 대형 커뮤니티 게시판을 통해 사이트를 광고하는 방법을 사용하여 회원을 모집하고 있다고 하는데 이들 사이트는 '해외에 서버를 두고 있어 국내법에 저촉되지 않는다'거나 '미국에서 합법적으로 운영 중인 사이트'임을 내세워 이용자들을 안심시킨다고 한다. 또한 지난 2004년 발표된 청소년보호위원회의 모니터링 보고서에 따르면 다음카페, 세이클럽, 프리챌, 네이버, 네이트닷컴 등 거의 모든 포털 사이트의 주요 커뮤니티 및 게시판에 직접적인 성매매가 이루어지고 있는 것으로 드러났다. 다음카페의 '영계클럽'에는 남자 청소년이 용돈을 벌 목적으로 주부에게 원조교제를 요청하는 글이 수없이 올라와 있는가 하면 '10대들의 원나잇' 게시판도 역시 성매매 대상을 구하는 글로 도배된 것으로 조사된 것이다. 청소년보호위원회가 같은 기간 모니터링 한 버디버디, 한게임, 넷마블, 토마토넷, 세이클럽 등에서는 채팅 접속시 성매매를 제의하는 메시지가 실시간으로 뜨거나 이를 통해 무수한 성매매 만남이 성사되는 것으로 나타났다[75]. 2008년 11월 2일 YTN 기사에는 '여성단체 등의 조사결과 온라인 성매매를 알선하는 것으로 의심되는 사이트만 줄잡아 90여 곳이며, 이들 성매매 카페의 경우 카페 내에서 은어를 사용함으로써 규제를 피해

71) 강원일보 2009.9.10.
72) 폭탄제조방법을 알려주는 인터넷 카페를 운영해 온 운영자가 중학교 3학년 학생이었습니다. 인터넷 검색창에 폭탄이나 무기 제조 등의 키워드를 넣자 수십개의 인터넷 카페가 뜹니다. 폭탄을 만드는 방법을 알려주는 이른 바 폭탄사이트입니다.(중략) 전문가들은 학생들이 호기심에 폭탄을 만들다 큰 사고를 당할 수도 있다며 이런 위험성에 대한 교육이 필요하다고 강조했습니다; YTN 2005.7.13.
73) 경찰에 따르면 임군은 지난 3일 오후 1시 40분께 대구시 북구 고성동 대구시민 운동장 축구장 9번 출입구 부근에 시한폭탄이 든 노트북용 가방을 설치해 이를 주운 윤석인(26.대구시 중구 달성동)씨 등 2명에게 화상을 입게 한 혐의다. 경찰 조사결과 임군은 지난해 2월부터 인터넷 폭발물 사이트를 접속해 폭발물 제조법을 학습하고 다양한 소규모 실험을 한 뒤 범행을 저지른 것으로 드러났으며 지난해 9월에는 학교 운동장에서 폭발물 실험중 파편을 맞아 1주간 치료를 받은 것으로 드러났다; 한겨레 2001.2.20.
74) 정재봉, 전게논문, 45면.
75) 정재봉, 상게논문, 47~48면.

나가고 있고 메일이나 메신저를 이용함으로써 증거를 남기지 않고 또한 잠깐 동안 성매매를 알선하고 금세 다른 사이트를 여는 등 교묘한 방법 때문에 적발이 어렵다'고 전하고 있다. 2009년 9월 11일자 '뉴시스' 기사를 보면 광주 · 전남지역에서 이뤄지는 인터넷 성매매의 95% 가량이 채팅사이트를 매개로 한 것으로 드러났다. 이러한 성매매 알선 사이트는 성매매를 전혀 원하지 않는 불특정 다수에게까지 피해를 끼쳐 심각한 사회적 문제를 야기하고 있다. 부산 사하경찰서는 2008년 9월 인터넷 파일공유사이트를 개설한 후, 회원 40만명을 대상으로 음란물을 유포하여 다운받게 하는 방법으로 30억 상당의 부당이득을 취한 운영자 40명을 검거하는 등 인터넷상 각종 불법 사이트에 대한 지속적인 단속을 실시하고 있다[76].

음란 사이트는 가장 대표적인 유해사이트라고 할 수 있다. 음란 사이트에서 유통되는 음란 정보들은 가장 광범위한 피해를 발생시키고 있으며, 이들 피해는 심리적 불쾌감에서 그치지 않고, 금전적 · 사회적 피해에까지 이르기도 한다. 또한 사이버상에서 유통되는 음란물은 매우 빠르고 은밀하게 전파되는 특성을 갖고 있어 그 영향력은 매우 크다. 그러므로 많은 사람들이 이러한 음란물에 쉽게 접할 뿐 아니라 이러한 정보가 쉽게 복제되거나 엄청난 속도로 전파된다는 것은 간과할 수 없는 매우 심각한 문제이다[77].

(9) 응용프로그램을 겨냥한 보안 취약점 출현 증가 지속

마이크로소프트사(이하 MS)는 2008년도 보안업데이트를 MS08-001부터 MS08-078까지 78종을 발표했으며, 관련된 보안 취약점은 총 155건을 발표하였다. 이것은 2007년도 보안업데이트 69종(MS07-001~MS07-069)과 관련 보안 취약점 130건을 발표한 것과 비교할 때 보안업데이트는 약 13%, 보안취약점은 약 19.2% 증가된 결과이다. 이중 2008년 Office 관련 보안 취약점은 69건으로 2007년 22건과 비교할 때 약 3배 정도 증가하였는데, 이는 Office 제품의 취약점을 이용한 첨부파일을 열어보는 것을 통해 악성코드 감염을 유도하는 형태

76) 경찰청, 2009 경찰백서, 118면.
77) 정재봉, 전게논문, 49~50면.

의 취약점 비중이 높아진 것으로 보인다. 특히 Office 제품군의 경우 MS Word, Excel, Power Point 등 각 제품에 대한 보안취약점이 2006년 이후 전체 보안업데이트 중 차지하는 비율이 꾸준히 증가하고 있다. 여기에 대중적인 응용프로그램인 어도비사의 Flash Player 및 PDF Reader등 운영체제 자체보다는 응용프로그램 취약점의 증가가 지속되었다[78].

(10) 메모리 해킹수법의 사회 이슈화

메모리 해킹이란 램(RAM : Random Access Memory)이라고 불리는 주기억장치에 저장되는 데이터를 절취하거나 이를 조작하는 해킹기법이다. 기존의 피싱과 파밍 등의 해킹 수법들이 메일이나 전화 등 외부수단을 이용해 사용자의 계좌와 비밀번호 등의 금융정보를 빼내는 것이라면 메모리 해킹은 PC해킹을 통해 백도어 프로그램[79]을 설취한 뒤 전용도구를 통해 메모리상의 데이터를 절취하고 변조한다는 점에서 차이가 있다. 이러한 메모리 해킹을 통한 인터넷뱅킹의 실질적인 피해는 아직 보고된바 없지만 메모리 해킹 방식이 범죄에 악용될 경우 인터넷 뱅킹 자체의 신뢰성과 안전성에 큰 위협이 된다는 점에서 최근 금융권과 정보보호 업계에서 이슈로 떠오르고 있다[80].

(11) 무선 보안 취약점 악용 증대

무선네트워크가 보안상 취약하다는 지적이 오래 전부터 있어온 가운데 실제 국내 은행 전산망을 대상으로 지향성 안테나를 통해 관리자 정보를 빼낸 일당이 검거되었다. 다행히 해당 정보는 암호화가 되어 있어 추가적인 피해는 발생하지 않았으나, 최근 크게 증가하고 있는 무선네트워크 보급 및 무선네트워크 기능이 기본 탑재된 노트북의 보급률이 높아짐에 따라 개인 사용자들도 크게 증가하고 있는 상황에서, 관련 인증 · 보안 시스템을 통한 외부 침투 시도에 적극적 대응

78) 국가정보원, 2009 국가정보보호백서, 55면.
79) 백도어는 말 그대로 '뒷문'이라는 뜻으로, 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용 프로그램 또는 시스템에 접근할 수 있도록 하는 프로그램이다.
80) 국가정보원, 2008 국가정보보호백서, 14면.

이 필요하다는 시사점을 안겨준 사례이다. 더욱이 최근 위피(WIPI)[81] 의무 탑재 고시 해제(2008년 12월 10일, 방송통신위원회)에 따라 외산 스마트폰의 국내 도입 및 활성화가 예상되어 개인정보 유출, 불법 스팸발송 및 문자메시지 전송으로 인한 피해가 발생할 위험성이 증가하고 있다[82].

81) WIPI(Wireless Internet Platform for Interoperability)는 대한민국의 표준 모바일 플랫폼의 이름이다. 통신사간의 모바일 플랫폼을 표준화함으로써, 하나의 콘텐츠를 여러 통신사에서 서비스할 수 있도록 하기 위해 제정되었다.

82) 국가정보원, 「2008 국가정보보호백서」, 14면.

III. 사이버범죄에 대한 법적 규제

1. 사이버범죄에 대한 국외의 법적 규제

(1) 미국

미국[83]은 컴퓨터와 인터넷의 개발과 보급에 선두적인 역할을 해왔던 만큼 정보화에 대한 역기능의 빠른 제도적 대응을 마련하고 있다. 1984년 연방형법으로 '위장접근장치, 컴퓨터사기 및 부정이용에 관한 법률(The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984)'을 제정하였고 1986년 10월 16일 개정을 통해 인터넷 범죄의 유형을 체계화 하였다[84]. 연방형법에서는 인터넷사기, 온라인아동포르노, 아동유인, 불법적성관계매개, 인터넷처방약판매, 인터넷규제물질판매, 인터넷증권사기, 사이버스파이, 소프트웨어절도, 지적재산권 침해, 사이버도박, 인터넷화기판매 및 주류판매 등에 관한 규정을 두고 있다. 그리고 연방정보와 정보시스템 보안에 관한 법률로서 1986년 '컴퓨터사기 및 부정이용에 관한 법(Computer Fraud and Abuse Act)', 1987년의 '컴퓨터보안법(Computer Security Act)'을 제정하였고, 1996년에는 사이버 테러리즘으로부터 자국 내의 정보통신시스템을 보호하고 범정부적 차원의 정보보호체계를 정비하기 위하여 '국가정보기반보호법(National Infrastructure Protection Act)'을 제정하고 이에 의거하여 1998년 2월 26일 '국가기반구조보호센터(NIPC:National Infrastructure Protection Center)'를 발족시켰다.

'국가정보기반보호법'은 사이버테러리즘으로부터 자국의 정보통신시스템을 보호하기 위하여 범정부적 차원의 정보보호체계를 정비하기 위한 법률로서, 미 연방법전 제18장 제1030조의 컴퓨터사용 사기 및 관련범죄에 대한 특별법으로서 기능하고 있다. 국가기반구조보호센터는 국가주요기반구조에 대한 물리적 또는 가상적 공격이나 위협에 대하여 방어 · 탐지 · 위협평가 · 경고 · 조사 · 법집행 · 대응 등을 수행하기 위한 핵심기관으로서 기능을 수행하고 있다. 1999년 8월에

83) 이하 법조항에 대하여는 http://www.cybercrime.gov/
84) 정상훈, "사이버범죄에 관한 연구", 공주대학교 대학원 석사학위논문, 2007, 70면.

는 클린턴 대통령에 의하여 인터넷불법행위대책반(Working Group on Unlawful Conduct on the Internet)이 창설되어 법무장관의 지휘 하에 인터넷 사용과 관련되어 일어나는 사기, 아동포르노 등 불법적 행위들에 대한 효과적 수사·기소를 위한 충분한 근거를 현행 연방법률이 제공하고 있는가의 여부 및 인터넷상의 불법행위에 대한 수사·기소를 위하여 요구할 수 있는 기술적 수단, 능력 또는 법률적 조치 등이 무엇인가를 다루고, 그에 관한 보고서를 준비하는 것을 임무로 삼고 있다[85].

사이버 음란물에 대하여는 온라인아동보호법(COPA:Child Online Protection Act), 아동인터넷보호법(CIPA:Children's Internet Protection Act), 아동온라인 프라이버시보호법(Children's Online Privacy Protection Act of 2003), 아동포르노그래피방지법(Child Obscenity and Pornography Prevention Act of 2003), 아동도메인 보충과 효력법(Dot Kids Implementation and Efficiency Act of 2002), 아동P2P보호법(Protection Children from Peer-to-Peer Pornography), 아동포르노에 대해 천명된 불관용주의(Zero-Tolerance Policy), 그리고 전기통신법 제5장의 통신품위법(Communication Decency Act) 등이 주된 대응법안 및 정책이다[86]. 1990년에 캘리포니아에서 최초로 스토킹 규제법률을 시행한 이래 1993년에 이르러 모든 50개주와 컬럼비아 특별구까지 스토킹규제법을 두고 있다. 또한 연방형법 제18장 제2319조와 동법 제17장 506(a)조에 의하여 저작권침해를 규제하여 오던 중, 1997년에 인터넷프로그램의 불법복제 및 배포를 금지하는 내용의 전자절도방지법(NET Act:No Electronic Theft Act of 1997)을 제정하여 저작권보호를 강화하고 있다. 사이버정보 침해 중 영업비밀에 관하여 미국은 1996년 제정된 경제스파이법(Economic Espionage Act)에 의하여 규제하고 있는데, 그에 의하면 영업비밀에 대한 절도 내지 배임행위에 대하여 처벌하고 있다. 영업비밀의 개념에 대하여는 연방법과 통일영업비밀법(Uniform Trade Secret Act)에 정의되어 있다.

'국토안보법(Homeland Security Act of 2002)'은 각 연방기관이 담당하고 있던 국토안전보장업무를 국토안보부(DHS : Department of Homeland Security)

85) 박성택, "사이버범죄의 현황과 대응방안", 영남대학교 행정대학원 석사학위논문, 2004.8, 62~64면.
86) 신현정, 전게논문, 55~56면.

가 총괄하도록 동 부서를 창설하고, 정보기술을 유효하게 활용하여 사이버공격이나 물리적 공격으로부터 미국 국토를 방위하는 것을 목적으로 한다. '국토안보법'은 총 17장으로 구성되는데 특히 사이버보안과 관련된 규정은 제2장(정보분석 및 기반시설 보호)과 10장(정보보호)등이 대표적이다. 제2장에서는 국토안보부의 임무, 국토안보부 장관과 관련 공무원 임명 등 신설되는 국토안보부의 조직구조에 관해 규정하고 있다. 이에 국토안보부가 테러 관련 정보를 수사기관과 법집행기관으로부터 제공받을 수 있도록 연방수사국의 국가 기반보호센터(NIPC), 국방부의 국가 통신 시스템(NCS : National Communication System), 상무부의 주요기반 보장국(CIAO : Critical Infrastructure Assuarance Office), 에너지부의 국가 기반 시뮬레이션 및 분석 센터와 에너지부의 에너지 안보 및 보장프로그램, 총무청의 연방 컴퓨터 사고 대응센터(FedCIRC) 등의 기관에 속한 직무, 인적자원, 권한 및 책임이 국토안보부로 이관되었다.

'사이버보안강화법(CESA : Cyber Security Enhancement Act of 2002)'은 '국토안보법' 제2장에 규정되어 있다. 동 법에는 양형위원회(Sentencing Commission) 관련 내용, 긴급 공개 예외(Emergency Disclosure Exception), 선의의 예외규정(Good Faith Exception), 불법 인터넷 광고 금지 및 처벌강화, 프라이버시 보호 등이 규정되어 있다.

9/11테러 직후 계속되는 테러위협에 대응하기 위한 수사력 강화와 국가적 안보 확립을 목적으로 미국은 'H. R. 3162 USA PATRIOT Act'를 제정하였다. 동 법은 정보의 수집이나 정부기관에 의한 정보공유, 테러협력자의 취조, 테러조직과 관련된 은행구좌나 자산의 동결 등에 관한 법집행기관이나 첩보기관의 권한을 확대했다. 그러나 이 법은 컴퓨터 범죄 및 전자 증거 관련하여 상당한 신규 권한을 부여하였으나, 이들 대부분은 2005년 12월 31일 만료되는 한시법조항이었다. 이에 2006년 3월 한시법 조항의 기한을 연장하거나 만료시킨 내용을 정한 '미국 PATRIOT 개선 및 재승인법(USA PATRIOT Improvement And Reauthorization Act of 2005)'을 승인함으로써 사실상 대부분의 한시법 조항이 연장되거나 영구화되었다.

'컴퓨터사기 및 부정이용에 관한 법(CFAA : Computer Fraud and Abuse Act)'은 고의로 보호되고 있는 컴퓨터에 권한 없이 손해를 야기한 행위를 불법으

로 처벌하고 있다. 9/11테러 이전에는 이러한 범죄를 야기한 자에 대해 초범의 경우에는 5년 이하의 징역, 재범의 경우에는 10년 이하의 징역을 선고하였다. 그러나 9/11테러 이후 'USA PATRIOT Act'제정으로 해커에 대한 최고 형량을 초범에게 10년, 재범인 경우 최고 20년형으로 상향 조정하였다. CFAA는 기밀성(confidentiality), 무결성(integrity), 가용성(availability)을 보장하기 위해 아래의 행위를 불법행위로 규정 · 금지하고 있다.

- 고의로 승인받지 않거나 승인의 범위를 벗어난 정보에 접근하여 스파이 활동을 수행한 경우
- 승인되지 않거나 승인의 범위를 벗어난 정보에 접근하는 행위
- 공개되지 않은 정부 컴퓨터에 접근하는 행위
- 사기를 칠 목적으로 컴퓨터에 접근하는 행위
- 고의적으로 컴퓨터에 손해를 입히는 행위
- 고의적으로 패스워드를 거래하는 행위
- 금전적이거나 기타 가치를 지닌 것을 탈취하기 위한 목적으로 컴퓨터에 손해를 야기하거나 이를 협박하는 행위

CFAA에 따라 불법적으로 정보에 접근하는 것을 중범죄(felony)로 정의한다. 또한 금융기관 및 관련 기관이 보유하고 있는 금융기록에서 고객의 개인정보에 불법적으로 접근하는 것 또한 중범죄로 규정한다[87].

(2) 유럽연합

유럽연합은 전자통신 네트워크 및 서비스의 규제 틀을 정의하기 위해 '프레임워크 지침(Directive 2002/21/EC, 2002년 3월 7일)'을 제정하고, 각국 정부의 규제기관과 유럽집행위원회가 일관적인 규제를 시행하도록 하였다. 동 지침은 개인정보나 프라이버시를 안전하게 보호하고 통신네트워크의 안전성을 확보하는 것을 목적으로 한다.

'데이터보호 지침(EU Directive on Privacy Protection, 1995/46/EC, 1995

87) 국가정보원,「2007 국가정보보호백서」, 2007, 295~320면.

년 10월 24일)'은 개인정보의 처리 및 자유로운 이동에 관한 지침이다. 이 지침을 통하여 회원국에게 개인의 기본 권리로서 개인정보보호 책임을 부과하고 궁극적으로 개인에게 개인정보보호 권리를 보장하고자 하는 목적으로 제정되었다. 동 지침은 EU회원국과 업무를 하는 비회원국들에도 적용된다.

'프라이버시와 전기통신에 관한 지침(Directive 2002/58/EC, 2002년 7월 12일)'은 개인정보의 처리 및 전기통신 분야에서의 프라이버시 보호를 목적으로 하는 지침으로 유럽 내 스팸메일의 발송을 방지하기 위한 대책을 포함하고 있다.

유럽 전역의 주요한 국제적인 법적 수단 중 하나가 유럽이사회에 의한 '사이버범죄 조약(Convention on Cybercrime)[88]'이다. 이 조약은 사이버범죄에 관한 가장 포괄적인 문서이자 최초의 국제조약으로, 날로 기승을 부리는 각종 인터넷 범죄를 퇴치하기 위해 각 국가가 공조할 것을 명기하고 있다. 동 조약은 인터넷을 이용한 모든 범죄행위에 대해 상세히 규정 및 처벌할 수 있는 근거를 마련하고 참여 국가들은 네트워크에 대한 불법 침입, 사기, 웜 · 바이러스 유포, 아동 포르노 보유 · 유포, 저작권 침해 등 다양한 활동에 대하여 조사 및 처벌할 수 있도록 규정하고 있다. 동 조약은 기초단계부터 미국, 일본, 캐나다 등이 참관자(Observer)로 참여하였고 2001년 11월 서명식에는 유럽연합의 30개국과 G7국가들을 포함하여 총 38개국이 서명하였으며, 이후에 5개국이 추가로 가입하여 43개국이 가입했다. 본 조약은 2004년 7월 1일 발효되었으나 국가별 관련 국내법 제정이나 개정의 문제점 등으로 인해 자국내 의회의 비준을 받은 국가는 18개국에 그치고 있다.

'유럽이사회의 정보시스템 공격에 관한 프레임워크 결의(2005년 2월 24일)'는 정보시스템 공격에 대한 회원국의 형법상 제규정을 보완하여 사법당국 및 관련 부처 간의 협력을 보다 효과적으로 하는 것을 목적으로 한다[89].

(3) 영국

영국은 인터넷 내용에 대한 자율성을 최대한 존중하는 시스템을 가지고 있다.

---

88)Convention on Cybercrime, http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm
89) 국가정보원,「2007 국가정보보호백서」, 2007, 321~322면.

이는 미국과 다른 국가들에 비하여 자유주의적 법제도를 가지고 있는 것으로 유럽의 대부분의 특성인 인터넷상의 불법정보에 대한 시민들의 자율적인 참여를 보장한다. 영국은 인터넷상의 불법자료 유포금지, 사용자 및 아동의 유해정보로부터의 보호장치 고안 등의 2가지 목적으로 발기된 1996년 9월 기업차원의 인터넷감시재단 IWF(Internet Watch Foundation)가 설립되었으며, 이들 단체는 '핫라인(Hotline)'을 통해 유럽의 다른 국가들의 NGO와 상호 협력관계 체제를 구성하고 있다[90].

컴퓨터범죄에 대하여는 1971년 '형사손해구제법(Criminal Damage Act 1971)' 으로 하여 컴퓨터 바이러스, 해킹 등 신종범죄를 처벌하기 위한 1990년 '컴퓨터오용법(Computer Misuse Act 1990)'과 사이버스토킹을 처벌하기 위한 법률인 '부당통신법(Malicious Communications Act 1988)'을 모체로 한 1997년 '희롱방지법(Protection from Harassment Act 1997)' 제7조 제2항, 개인비밀정보에 대하여는 '개인자료의 처리 및 자유로운 이전에 관한 개인정보 지침', '정보통신부문에 있어서 개인 정보의 처리 및 프라이버시 보호에 관한 지침'을 기반으로 하는 '데이터보호법(Data Protection Act 1998)'의 입법추진이 있었다. '조사권한규제법(RIPA : Regulation of Investigatory Powers Act 2000)'은 통신감청에 관한 법률로서 인터넷이나 컴퓨터 암호화기술의 발전으로 인해 도입된 법으로, 일반인을 모니터하기 위한 기술을 기반으로 하고 있다.

'대테러 범죄 및 안전보장법(Anti-terrorism, Crime and Security Act 2001)'은 미국의 'USA PATRIOT Act of 2001'이나 다른 여러 가지 테러대책의 내용을 포함하고 있다. 동 법 제11편 102~108에는 통신데이터 보전을 위한 권한 관계를 규정하고 있다[91].

영국을 비롯한 유럽에서는 미국과 달리 데이터베이스에 대한 보호를 강화하고 있는 것이 특징이다. 영국은 1996년에 마련된 유럽연합의 데이터베이스보호지침의 규정을 국내법상 실행시키기 위하여 1997년 '데이터베이스에 대한 저작권 및 권리에 대한 규정(The Copyright and Right in Database Regulations)'을 제정하여 데이터베이스의 침해행위에 대하여 규제하고 있다. 그 외에 사이버범죄에

90) 정상훈, 전게논문, 71~72면.
91) 국가정보원,「2007 국가정보보호백서」, 2007, 328~329면.

대한 대응법규로서 통신방해법, 저작권, 도안 및 특허법, 상품표시법, 상표법 등이 있다[92].

(4) 독일

'화이트칼라 범죄 대응을 위한 2차법(Second Law on Combating White-Collar Crime)'은 IT관련 범죄에 대처하기 위해서 1986년 독일 형법에 도입된 법규이다. 컴퓨터 데이터 절도 및 시스템 파괴 등 형사상 범죄, 컴퓨터 및 통신시스템을 사용하는 컴퓨터 범죄에 대한 대처를 목적으로 하고 있다[93].

독일은 컴퓨터와 관련된 경제범죄에 대처하기 위해서 1986년 5월 15일 형법 개정이 이루어졌다(경제범죄 대처를 위한 제2차 법률:2WiKG). 주요 내용은 컴퓨터사기(독일형법 제263조의 a), 증명에 중요한 데이터의 위조(형법 제303조의 a) 및 컴퓨터업무방해(형법 제303조의 b) 등이 신설되었다. 사이버음란정보에 대해서는 데이터저장장치의 표현물도 문서와 동일하게 보고 음란문서 등 반포죄의 행위객체를 새롭게 규정하였고(형법 제1조 제3항, 제184조), 특히 아동포르노에 대해서는 형량을 강화시켰다(형법 제184조 제4항)[94]. 이러한 입법적인 대책을 통하여 컴퓨터에 대한 부정조작 행위와 컴퓨터에 저장된 정보에 대한 변조, 위조 또는 파괴 등에 대한 행위에 대하여 처벌하도록 규정하고 있다. 또한 1993년에 개정된 저작권법에 의하여 컴퓨터 프로그램의 저작권보호를 강화하였고, 반도체 보호법을 제정하여 마이크로칩의 회로에 대한 특별한 보호조치를 신설하였으며, 개인정보 침해나 영업비밀 침해와 같은 범죄행위를 규제하기 위하여 연방정보보호법을 마련하고 있다[95]. 또한 정보통신서비스의 활용을 위한 제반 여건을 개선하고 인터넷에서의 불법 및 유해정보의 유통을 방지하고자, 1997년 8월부터 정보통신서비스법(IuKDG)을 시행하고 있다[96].

'사이버 범죄에 대한 형법 수정 제안서'는 EU의 '사이버범죄조약'을 기초로 독

92) 박성택, 전게논문, 61면.
93) 국가정보원,「2007 국가정보보호백서」, 2007, 334면.
94) 신현정, 전게논문, 59~60면.
95) 박성택, 상게논문, 62면.
96) 정상훈, 전게논문, 70면.

일의 처벌 및 그 원칙을 제안하고 있다. 1장은 형사법 변경과 관련한 설명이며 2장은 위반에 대한 법률 변경, 3장은 효력발생을 설명하고 있다. 설명은 일반사항과 특별사항으로 구성되는데 일반사항에서는 개요, 징계법률 원칙, 형법의 확장, 남녀공통 적용에 대해서 설명하고 있고 특별사항은 형법 변경사항, 위반법률사항, 효력발생에 대해서 구체적으로 설명을 추가하고 있다[97].

(5) 프랑스

프랑스는 가장 빨리 정보사회에 진입하고자 노력한 국가 중의 하나에 속하며, 따라서 프랑스인들은 새로운 정보통신기술이 개인의 자유 및 프라이버시에 미칠 수 있는 위험을 인식하였다. 이러한 인식에 따라 프랑스 정부는 1972년 법무성을 통해 이에 대한 구체적인 조사검토를 시작하였고, 국가정보처리자유위원회(The National Commission on Informatics and Freedom : CNIL)의 보고를 통해 1977년 12월 국민의회에서 '정보처리축적및자유에관한법률'을 제정하였다. 이 법률은 프라이버시를 중시하는 국민들의 특성상 그 적용범위가 대단히 넓고 법률내용이 혁신적이라는 데 그 특징이 있다. 특히 이는 영미법계 국가들의 시각에서 본다면 개인의 사생활 보호나 감시통제를 넘어서는 대단히 광범위한 사회문제들을 다루는 법이다. 또한 그 규제대상으로 공공부문과 민간부문을 모두 포함하고 있으며, 반드시 전산 처리된 정보에 대해서만 법적용을 한정하고 있지는 않고 있다[98].

'ICT부정행위법(Law No. 1988-19 of 5 January 1998 regarding ICT Fraud)'은 프랑스에 있어서 최초의 컴퓨터범죄 처벌에 관한 법률이다.

'사이버범죄 진화에 대한 사법조직의 적응법(Law No. 2004-204 of 3 March 2004 adapting the organization of justice to evolutions in crime)'은 지적재산 침해에 대해 형사처벌 규정을 강화한 법이다. 구체적으로 지적재산권 중 상표권 침해를 대상으로 하고 있다[99].

97) 국가정보원,「2007 국가정보보호백서」, 2007, 334면.
98) 박성택, 전게논문, 61면; 「2003 국가정보보호백서」, 국가정보원, 2003, 223~224면.
99) 국가정보원,「2007 국가정보보호백서」, 2007, 340면.

(6) 일본

사이버범죄에 대응하기 위한 일본의 입법은 1987년 발효된 일본형법의 일부 개정으로 이루어졌는데, 이 개정에 의하면 전통적 구성요건이라고 할 수 있는 문서위조죄(형법 제157조 이하), 사기죄(제246조), 업무방해죄(제234조), 문서손괴죄(제258조) 등의 확장과 보안이 이루어졌다. 또한 행위객체로서 '전자적기록'과 '전자계산기'라는 개념을 도입하였으며, 특히 컴퓨터업무방해죄의 신설에 의하여 컴퓨터 또는 컴퓨터내의 정보의 파괴, 허위의 정보나 명령의 권한 없는 입력, 기타 방법에 의한 장애를 구성요건화 하였다[100]. 그리고 풍속영업 등의 규제 및 업무적정화 등에 관한 법률(1999)은 어린이를 소재로 한 음란물을 포함하는 음란물의 유통을 막기 위하여 성인정보 제공자의 정화노력을 의무화하는 것을 목적으로 하고 있다. 이 법에서는 '무점포형 성풍속 특수영업'(통신판매 등) 및 '영상송신형 성풍속 특수영업'(인터넷이용영업)에 대한 규제를 신설하고, 무점포형 성풍속 특수영업이나 영상송신형 성풍속 특수영업을 하는 자는 18세 미만의 미성년자를 대상으로 영업을 할 수 없도록 명시하고 있다[101]. 1999년 5월 26일에는 '아동매춘, 아동포르노에 관련된 행위 등의 처벌 및 아동의 보호 등에 관한 법률'을 제정하여 아동매춘과 아동포르노를 규제하고 있다. 2003년 제정된 '인터넷 이성소개 사업을 이용해 아동을 유인하는 행위의 규제 등에 관한 법률'은 아동포르노의 인터넷 중개 사이트인 '만남사이트'와 휴대전화의 서비스를 규제하고 있다. 일본의 경우 아동포르노 유통의 세계적 비중이 가장 높기 때문에 아동포르노의 유통에 심혈을 기울이고 있다. 또 ISP와 민관협력체제간의 협력도구를 모델로 채택하고 있는데 이러한 협력을 통해 위법 · 유해정보의 감시는 물론 필터링 서버를 통해 유해정보를 ISP에게 근거로 제공하여 차단하고 '인터넷핫라인연락협의회'를 구성하여 정보공유 및 국내기관의 공조체제를 강화하고 있다[102].

---

100) 박성택, 전게논문, 66면.

101) '영상송신형 성풍속 특수영업'이란 오로지 성적 호기심을 불러일으키기 위해 성적인 행위를 나타내는 장면 또는 의복을 벗은 사람의 모습을 영상으로 보여주는 영업으로 전기통신설비를 이용하여 그 손님에게 해당 영상을 전달하는 것(방송 또는 유선방송에 해당하는 것을 제외)에 의해 운영하는 것을 말한다; 정완, 전게보고서, 2004.12, 66면.

102) 정상훈, 전게논문, 72~73면.

또한 고도 정보사회로의 발전에 따라 사회경제활동 전반에 걸쳐 정보시스템에 대한 의존이 커지면서 해킹, 컴퓨터바이러스 유포, 프라이버시 침해 등 정보시스템과 관련한 범죄도 크게 증가함으로 인하여, 정보시스템의 취약성을 악용하는 부정 액세스 행위를 기초로 이루어지는 범죄에 대한 금지 및 처벌 규정을 마련하여 정보시스템관련범죄 방지를 목적으로 입법 추진하여 '부정한액세스행위[103] 의금지등에관한법률'이 1999년 8월에 제정, 2000년 2월 13일부터 시행하고 있다. 동법은 컴퓨터관련 범죄나 전자통신방법에 의한 범죄를 방지하고 접근통제를 이용하여 설치되어 있는 전자통신에 관한 질서를 유지하는데 목적이 있다. 동법은 크게 4개의 구성요건을 규정하고 있는데(제3조 제1항, 제2항 제1호, 제3호, 제8호 이하), 접근통제장치가 되어 있는 컴퓨터에 타인의 ID를 무단 입력하는 행위, 당해 컴퓨터에 접근제한을 회피하는 정보는 명령(ID제외)을 입력하는 행위, 다른 인증서버에 의하여 접근이 통제되는 컴퓨터에 정보나 명령을 입력하는 행위 등을 규정하고 있다[104]. 200년 5월 18일에는 '스토커행위등의규제에관한법률'을 제정하여 사이버스토커에 대하여 규제를 하고 있다. 일본이 추구하고 있는 고도정보통신네트워크 사회의 형성에 관한 정책 책정에 있어, 기본이념 및 기본방침을 정하는 동시에 국가와 지방공공단체의 역할을 명확히 하기 위하여 'IT기본법'이 2001년 1월부터 시행되고 있고, 이 중 정보보호 관련 부분으로 네트워크의 안전성 · 신뢰성 확보와 개인정보보호에 관해서도 규정하고 있다[105]. 또한 2001년 EU의 '사이버범죄조약'에 가입하여 2004년 국회비준을 거치고 국내법에 반영하기 위해 '범죄의 국제화 및 조직화 그리고 정보처리의 고도화에 대처하기 위한 형법 등의 일부를 개정하는 법률안' 등을 정비하기 위해 노력하고 있다[106].

(7) 중국

---

103) 액세스 제어기능을 가진 특정 정보시스템 등에 전기통신회선을 통하여 타인의 식별부호 등을 입력하여 작동시키거나, 해당 액세스 제어기능에 의하여 제한되어 있는 특정기능은 이용할 수 있는 상태로 만드는 행위 ; 「2005 국가정보보호백서」, 국가정보원, 2005, 186~187면.

104) 신현정, 전게논문, 63~64면.

105) 박성택, 전게논문, 65~66면; 국가정보원,「2003 국가정보보호백서」, 227면 ; 국가정보원「2005 국가정보보호백서」, 186~187면.

106) 국가정보원,「2007 국가정보보호백서」, 345면.

1986년 중국에서 최초로 컴퓨터 이용 공금횡령사건이 발생한 이후, 컴퓨터 · 인터넷 범죄는 그 종류 또는 발생 건수를 불문하고 매년 대폭의 증가세를 보이고 있다. 최근 중국에서 가장 심각한 사이버범죄는 역시 재산범죄이다. 그 다음으로 사회질서를 위협하는 사이버범죄로 사이버도박, 사이버음란물 등이 해당한다. 마지막으로 인터넷망의 안전을 위협하는 범죄활동이 많이 발생하고 있다[107].

중국은 1997년 컴퓨터바이러스부대 창설에 이어 2000년 미래 하이테크전 수행방안을 결정하고, 컴퓨터전문가로 구성된 전자전 특수부대인 Net Force를 창설하여 사이버공격 및 정보교란 모의훈련을 수시로 실시하는 등 사이버공격에 치중해 왔었다. 그러나 2000년부터 인터넷 인구가 급증하여 미국에 이어 세계 2위의 인터넷 시장으로 성장하면서 최근 금융 · 전자상거래 사이트가 잇달아 해킹당하는 등 사이버테러가 빈발함에 따라 사이버테러 대응을 위한 대응책 마련에 부심하고 있는 실정이다. 2001년 해킹, 바이러스 전파, 유해정보 전파 등 컴퓨터 관련 범죄활동 방지를 위한 컴퓨터정보시스템 안전보호등급 구분을 제정 · 시행 등 제도를 정비하는가 하면, 컴퓨터 제품의 안전성을 평가하는 국가정보 안전 측정센터를 설립하는 등 제도를 정비하여 왔다. 최근 중국은 유명 웹사이트들이 해커들의 공격에 쉽게 마비되고 특히, 반체제 세력의 해킹사례로 피해가 나타나고 있어 불법 인터넷사이트 색출강화와 함께 보안기술 개발에 주력해 나갈 것으로 보인다[108].

(8) 유형별 법적 규제

1) 해킹

독일은 해킹행위에 대하여 형법 제202조a의 데이터탐색죄(Ausspähen von Daten, §202a StGB)를 적용하여 트로이목마 등의 해킹툴과 악성코드 프로그램을 침투시키거나 쿠키(cookie)[109]를 이용한 개인정보 습득 등을 처벌하고 단순 해킹의 경우 처벌에 대한 논란이 있지만 다수설로서는 형법 제202조a의 적용이

107) 남재도, "중국내 사이버범죄 실태 및 한중간 효과적인 공조방안 연구", 행정안전부 교육훈련정보센터 국외훈련보고서, 2009, 9~11면.
108) 국가정보원, 「2003 국가정보보호백서」, 228~229면.
109) 인터넷 웹사이트의 방문기록을 남겨 사용자와 웹사이트 사이를 매개해 주는 정보.

배제된다고 한다. 그러나 모니터에 타인의 데이터를 불러오는 경우는 해당된다고 보는 입장이며, 그러나 이 경우 보안장치의 해제를 충족요건으로 한다. 또 해킹 등으로 컴퓨터의 데이터를 권한 없이 삭제, 은닉, 사용불능케 하거나 또는 이를 변경하는 경우 형법 제303조a의 데이터손괴죄를 적용하여 2년 이하의 징역이나 벌금형으로 처벌하고 있다. 해킹의 결과로 초래되는 업무방해에는 컴퓨터방해죄를 적용하고 있으며 인터넷상의 바이러스 유포행위, 웜, 트로이목마 등의 유해행위로 업무방해를 가져오는 경우에 대하여는 가중 처벌하고 있다[110].

미국은 연방법전 제18권의 제1030조[111]에 규정된 '국가정보기반구조보호법'에서 사이버테러행위에 대해 규정하고 있다. 이 법률은 위법행위의 대상이 되는 컴퓨터를 정부기관에서 독점적으로 사용하는 컴퓨터에 한정시키지 않고 그 범위를 폭넓게 인정하고 있으며, 그 행위의 태양도 '권한 없이 접근(access)하거나 권한을 초과하여 접근한 경우'와 같이 규정함으로 '접근권한' 자체를 위법행위를 결정하는 중요한 기준으로 삼고 있다. 이러한 미국의 국가정보기반구조보호법인 컴퓨터사기 및 남용방지법은 인터넷을 통한 국가적 비밀침해(간첩죄), 금융기관 등에서 보관하는 개인 비밀침해(개인정보보호), 해킹범죄(컴퓨터의 무결성 확보), 인터넷 사기, 컴퓨터에 손해를 가한 경우(컴퓨터의 비밀성과 무결성 확보), 통신 중인 비밀번호나 이와 유사한 정보 보호, 갈취 목적으로 컴퓨터 손상을 입히겠다는 협박행위 등에 대처하기 위한 규정을 마련하고 있다. 컴퓨터사기 및 부정이용에 관한 법의 제1030(a) (1)항[112]은 권한 없이 또는 권한을 초과하여 고의적으로 정부기관의 컴퓨터에 접근하고 비밀정보를 취득하여 이를 미국에 해가 되거나 이익이 될 것을 의도하고 타인에게 전송하는 등의 행위를 처벌하고 있다. 본 규정은 컴퓨터를 이용한 비밀정보에 대한 첩보행위를 규제하기 위한 것이다. 본 규정은 연방법 제793조 (e)항과 서로 중복되는 부분이 상당히 있지만 두 법률이

110) 정상훈, 전게논문, 81면.
111) http://www.cybercrime.gov/1030NEW.htm
112) (a)누구든지
(1) 고의로 권한 없이 또는 권한을 초과하여 컴퓨터에 접근하여 미국 정부가 법령에 근거하여 국가방위 또는 외교관계를 위하여 그 정보가 누설되는 것을 방지하기 위한 차원에서 보호가 필요하다고 판단한 정보나 원자력법 제11조 y항에서 규정하는 비밀 데이터 등을 침해하고, 이렇게 입수한 정보를 미국의 이익을 해치거나 외국을 유리하게 할 목적으로 의도적으로 권한 없는 자에게 통신, 전달, 전송(이하 통신 등이라고 한다)하거나 통신 등이 이루어지도록 원인을 제공하거나 통신 등을 하려고 시도하거나 위 정보를 미국관리에게 전달하여야 할 자가 고의로 이를 전달하지 않은 경우

같은 행위를 규율하는 것은 아니라고 한다. 즉 미국의 현행 '첩보활동에 관한 법률'이 정부의 기밀을 외국 정부에 '넘기려는 행위'를 처벌하기 위한 규정인 반면, 본 규정은 비밀로 분류되거나 제한된 정보를 취득하기 위해 '고의로 컴퓨터에 침입'하거나 '침입을 시도'하는 자를 '그 행위만으로도 처벌'할 수 있는 근거를 마련하고 있다. 제1030(a) (2)항[113]은 권한 없이 또는 권한을 초과하여 고의적으로 컴퓨터에 접근하고 금융기관의 금융기록이나 고객에 대한 정보기록을 취득하거나 정부기관의 정보를 취득하는 행위 등을 처벌하고 있다. 1996년 개인정보의 중요성을 인식하고 이를 포함한 국가정보인프라보호를 위하여 개정된 조항으로서 프라이버시 보호를 염두에 두고 컴퓨터 데이터를 보호하는 조항이다. 본 규정은 단순한 정보의 습득을 처벌하는 것이 아니라 의도적으로 권한 없이 또는 권한을 초과하여 컴퓨터에 접근하여 그러한 정보를 취득하는 것을 금지한다는 것이다. 그리고 '정보의 취득'에는 단순히 그것을 읽는 것도 포함되고 정보가 복사되거나 전송되어야 할 필요는 없다고 한다. 제1030(a) (3)항[114]은 권한 없이 고의적으로 정부기관의 비공개 컴퓨터에 접속하거나 정부기관의 비공개 컴퓨터가 아닌 경우에도 정부기관이 사용하는 컴퓨터에 권한 없이 접근하여 정부기관의 사용에 영향을 미치는 행위를 처벌하고 있다. 이 규정은 해커가 정보를 취득하지 않은 경우에도 정부의 컴퓨터를 보호하는 것으로 정부장비의 무결성을 침해하면 그 책임을 묻는 조항이다. 또한 본 규정은 미국정부가 배타적으로 사용하는 컴퓨터뿐만 아니라 미국정부를 위해서 사용되는 컴퓨터도 보호하고 있다. 제1030(a) (4)항[115]은 권한 없이 또는 권한을 초월하여 사기의 고의로 보호되는 컴퓨터에

113) (2) 고의로 권한 없이 또는 허용된 권한을 초과하여 컴퓨터에 접속한 후
(A) 금융기관이나 법령15U.S.C의 1602(n)조에서 정의하고 있는 카드발급사가 관리하는 금융관계자료에 포함된 정보를 취득하거나 Fair Credit Reporting Act(15U.S.C 1681)가 규정하는 소비자에 관한 정보를 취급하는 회사가 보유하는 소비자에 관한 정보를 취득하는 경우
(B) 미국의 행정각부나 정보기관으로부터 정보를 획득한 경우
(C) 이 법률에 의해 보호의 대상이 되는 특정한 컴퓨터에서 정보를 취득하여 그 행위가 주간의 통신이나 외국과의 통신에 영향을 미친 경우

114) (3) 고의로 권한 없이 미국정부의 부서 혹은 기관의 비공개 컴퓨터에 접속하기 위해 미국정부가 배타적으로 사용하는 미국정부의 부서 혹은 기관의 컴퓨터에 접속하거나 미국정부에서 독점적으로 사용하고 있지는 않으나 미국정부에 의해서 혹은 미국정부를 위해서 사용되는 컴퓨터에 권한 없이 접속하고 이로 인하여 미국정부에 의한 컴퓨터의 이용 혹은 미국정부를 위한 컴퓨터의 이용에 영향을 미친 경우

115) (4) 고의로 사기의 의도로 권한 없이 또는 월권하여 '이 법률에 의하여 보호의 대상이 되는 특정한 컴퓨터'에 접속하고 나아가 의도한 사기행위를 실행함으로써 타인으로부터 재산상 이익을 사취한 경우, 단 그 재산상의 이익이 그 컴퓨터를 사용하는 것 자체에 그치거나 그 가액이 1년간 5천불을 넘지 않는 경우에는 예외로 한다.

접근하고 연간 5천불을 초과하는 재산적 가치를 편취하는 행위를 처벌하고 있다. 중범죄 수준의 컴퓨터 무단사용을 제재하는 규정이다[116]. 월권하여 보호가 필요한 컴퓨터에 접속하는 행위, 접속을 통해 계획적으로 사기를 조장하여 경제적 가치가 있는 이익을 획득하는 일체의 행위 또한 처벌된다. 다만 사기를 범하고자 하는 의도가 없거나 또는 획득한 경제적 가치가 1년에 5,000달러 이하인 경우에는 처벌하지 아니한다. 제1030(a) (5)항[117]은 보호되는 컴퓨터에 프로그램, 정보, 부호 또는 명령을 전송하여 의도적으로 권한 없이 손상시키는 행위, 보호되는 컴퓨터에 고의적으로 권한 없이 접근하여 과실로 손상을 유발하는 행위, 보호되는 컴퓨터에 권한없이 고의로 접근하여 손상을 야기한 행위를 처벌하고 있다. 1996년에 개정된 규정으로 '보호되는 컴퓨터'라는 용어를 사용하여 연방정부를 위한 컴퓨터를 망라함으로써 적용범위를 넓히고, 현대사회에서 컴퓨터 네트워크의 중요성이 부각됨에 따라 컴퓨터 정보의 기밀성과 무결성을 확보하기 위하여 고의뿐만 아니라 과실의 경우에도 손해를 야기하면 처벌하도록 개정하였다. 본 규정은 보호되는 컴퓨터를 바이러스 유포나 서비스거부 공격과 같은 행위와 해킹행위로부터 보호하기 위해 마련된 규정이다. 제1030(a) (6)[118]항은 권한 없이 컴퓨터 접근암호나 정보장치에 대한 사기행위의 고의로 이를 통하여 주간 또는 외국과의 거래에 영향을 미치거나 정부기관의 컴퓨터에 접근하는 행위를 처벌하고 있다. 제1030(a) (7)[119]항은 공갈(extort)의 고의로 보호되는 컴퓨터에 피해를 가한다는 협박내용을 전송하는 행위를 처벌하고 있다. 국가정보기반의 근간인 컴퓨터를 보호하기 위한 규정이다. 본 규정은 이러한 공갈에 대한 기존의 법 규정들이 재산의 개념에 손상을 주지 않는 범위 내에서 컴퓨터를 작동하거나

116) 미의회는 모든 무단침입행위를 사기의 중범죄로 취급하는 것을 우려하여 5천불을 기준으로 하여 이를 상회하는 경우에만 본 규정을 적용하기로 하였다고 한다.

117) (5) (A)(i) 고의로(knowingly) 프로그램, 정보, 부호 또는 명령의 전송을 야기하고 그 행위의 결과로서 보호되는 컴퓨터에 권한 없이 고의로 손상을 야기한 경우, (ii) 고의로 권한 없이 보호되는 컴퓨터에 접근하고 그러한 행위의 결과로 과실로 손상을 야기한 경우, (iii) 고의로 권한없이 보호되는 컴퓨터에 접근하고 그 행위의 결과로서 손상을 야기한 경우

118) (6) 고의로 권한 없이 컴퓨터에 접속하기 위해 접속에 필요한 비밀번호나 이와 유사한 정보를 통신상에서 몰래 취득하는 행위(defraud traffics, 연방법 제1029조에 규정)를 하되 (A) 그러한 행위(trafficking)가 주간 또는 외국과의 상거래에 영향을 미치거나, (B) 그러한 컴퓨터가 미국정부에 의하여 또는 미국정부를 위하여 사용되는 경우

119) (7) 개인, 기업, 단체, 교육기관, 금융기관, 정부 또는 법인으로부터 재산상의 이익을 갈취할 목적으로 주간 또는 외국과의 상거래에 있어서 '이 법률에 의하여 보호의 대상이 되는 특정한 컴퓨터'에 피해를 야기하겠다는 협박에 해당하는 통신내용을 전송한 경우

컴퓨터와 그 주변기기에 들어 있는 데이터 또는 프로그램에 무제한적으로 접근하는 것을 포함하는지가 불분명한 점을 개선하기 위해 마련되었다[120].

일본은 해킹과 같은 사이버테러에 대하여 1999년 4월에 동경경시청에 하이테크범죄 대응을 위한 하이테크범죄 종합대책 센터를 설치, 경찰청에 기술대책과를 신설, 2001년 사이버포스(Cyber Force)를 신설하고 사이버테러에 대한 신고처리 및 수사 기술지원 업무를 종합적으로 처리하도록 하고 있다. 관련 법률을 보면 '형법'과 2000년 2월 13일부터 시행중인 '부정액세스행위의금지등에관한법률'로 나뉘어 대응하고 있으며 후자는 부정접속행위의 금지 및 처벌에 관한 내용을 담고 있다. '부정액세스행위의금지등에관한법률'은 위반규정으로 제3조, 제8조 제1호에 1년 이하 징역 또는 50만엔 이하의 벌금에 처하도록 하고 있으며 부정접속행위를 조장하는 행위에 대하여도 금지하고 있다. 홈페이지의 게시판을 통하나 ID · 패스워드를 판매하는 행위 등 타인의 식별부호를 공표하거나, 식별부호가 어느 특정 컴퓨터에 관계되는가를 공개하거나 또는 이를 알고 있는 자의 요구에 따라 접속관리자 및 정당 이용권자 이외의 자에게 무단으로 제공하는 행위를 말하는 것으로써 제4조와 제9조에 의하여 30만엔 이하의 벌금에 처하고 있다. 또 이법 제5조는 접속관리자의 방어조치, 보안조치 등의 강구에 노력해야 한다고 규정하고 제7조는 접속관리자의 적절한 보호조치가 이루어질 수 있도록 접속관리자의 요청이 있으면 필요한 원조를 하여야 한다고 하여 각급공안위원회에 의한 원조 등의 역할을 규정하고 있다[121].

1990년에 제정된 영국의 컴퓨터오용법[122]은 컴퓨터프로그램이나 데이터에 대한 권한 없는 접근행위, 다른 범죄를 목적으로 하는 해킹범죄행위, 그리고 컴퓨터 관련 자료의 권한 없는 변경행위 등을 규율하고 있다. 컴퓨터오용법 제2조에서는 다른 범죄를 목적으로 하는 해킹행위를 5년 이하의 자유형으로 처벌하고 있고 미수범 처벌규정을 두고 있다. 그리고 바이러스유포행위와 관련하여 영국의 컴퓨터오용법에서는 피해자의 실질적 손해와 그에 대한 가해자의 고의를 요구하지 않고 바이러스의 유포 및 제조를 처벌하는 새로운 규정을 신설하였다는 점도

120) 유석준, "사이버범죄에 대한 외국의 입법례", 「영산법률논집」 제15권 제1호, 영산대학교 법률연구원, 2008.9, 8~12면; 정상훈, 전게논문, 81~82면; http://www.cybercrime.gov/1030NEW.htm.
121) 정상훈, 상게논문, 81~82면.
122) http://www.iwar.org.uk/law/resources/cma/computer-misuse-act.htm

주목된다[123].

2) 사이버 비밀침해

미국은 사이버 스파이라고도 불리우는 영업비밀 침해에 대하여 연방법과 통합 영업비밀보호법(Uniform Trade Secrets Act)에서 정의하고 있으며 미 연방법 제101장(Section 101. Protection of Trade Secrets) 제1831조, 제1839조 규정의 경제스파이 방지법(Economic Espionage Act of 1996, EEA), 연방법 제1832조(Theft of trade secrets) 영업비밀절도 등을 적용하여 처벌하고 있다.

독일은 개인의 비밀침해와 업무상 비밀침해로써 형법 제203조의 규정이 적용되고 1977년 1월 27일 연방정보보호법에 개인관련 데이터 보호를 위한 형벌규정이 수용되었다(1977년 연방정보보호법 제41조, 제42조). 1990년 12월 20일에는 연방헌법재판소의 '정보의 자기결정권'에 대한 권리의 인정을 받아들이는 개정이 이루어졌는데, 이는 연방정보보호법의 데이터보호권의 규정으로 나타났다(1990년 연방정보보호법 제43조, 제44조). 또한 기업의 주요 영업비밀 등을 보호하기 위하여 업무상 기업비밀에 관하여 부정경쟁방지법(Gesetz gegen den unlauteren Wettbewerb, UWG) 제17조가 적용되어 가중 처벌된다. 부정경쟁방지법의 행위객체는 업무상 기밀유지 의무가 있는 사무원(Angestellter), 업무자(Arbeiter)가 포함되며 수습사원(Lehrling eines Geschaeftsbetriebs)까지도 포함된다. 사이버 비밀침해의 경우에도 동법이 적용되고 있다[124].

3) 사이버 음란물

미국의 음란성(Obscenity) 판단은 판례를 통하여 정의되어 왔으며 온라인아동보호법(Child Online Protection Act)을 통하여 음란물 사이트로부터 아동을 보호하기 위하여 웹사이트의 상업적 음란물이나 미성년자에게 유해한 자료의 제작 및 유포행위를 금지하고 있다. 아동포르노그래피에 대한 연방법은 보다 강력하며 연방법 제18장 제2251조 (18 U.S.C § 2251. 아동성착취(Sexual exploitation of children))를 규정하여 성행위 장면의 시각적 표현물을 제작, 운반, 취득, 분

123) 양근원, 전게논문, 2003.8, 23~34면; 유석준, 전게논문, 14면.
124) 정상훈, 전게논문, 79면.

해하는 행위를 금하고 있으며, 위반규정으로 10년 이상 20년 이하의 징역에 처한다고 규정하고 있다. 또 아동포르노에 대한 불관용주의(Zero Tolerance Policy)와 통신법(Telecommunication Act, 1996), 통신품위법(Communication Decency Act)등이 있으며 인터넷과 컴퓨터를 이용한 음란성 대화 및 화면전파 금지, 음란통신, 유선방송에 의한 음란프로그램 규제 등을 다루고 있다. 또한 미국은 사이버음란물에 대해 ISP의 자율규제를 유도하고 있다. ISP 약관에 법률로 금지된 성표현물을 이용자들이 자신의 서버에 저장하지 못하도록 하는 규정을 두도록 하였다. ISP들은 실제로 청소년 보호를 위한 필터링 소프트웨어를 무료로 제공하거나, 아동용 웹브라우저를 제공하고, 필터링 된 인터넷 접속 서비스와 필터링 된 검색엔진 서비스를 제공하고 있다.

독일은 인터넷을 통한 음란물의 게시, 유포 등의 행위는 형법 제184조의 적용을 하고, 18세미만 청소년에게는 접근을 용이하게 하는 행위조차 형법 제184조(§184 Nr.1 StGB), (§184 Nr.2 StGB)에서 규율하고 있는데 '접근가능성'(Zuänglichmachen)을 '전자기록으로 저장된 정보를 모니터에서 볼 수 있게 하는 상태에 두는 것으로 간주되며'로 해석하여 인터넷상의 게시판에 음란문서를 올려놓는 것도 당연히 해당된다고 독일판례는 명시하고 있다. 또 독일은 인터넷상의 전자도화(digitalisierte Avvildungen)의 개념을 사이버 음란물에 포함된다고 보아 형법 제184조의 적용을 받도록 통설과 판례의 입장을 취하고 있다. 미국과 마찬가지로 아동포르노그래피의 경우 접근을 용이하게 하는 경우 3년 이하의 징역이나 벌금형으로 가중처벌하고(§184 III StGB) 청소년보호법(Jugendschutzesetz)을 제정하여 다양한 매체로부터 14세 이상 18세 미만의 청소년을 포괄적으로 보호하고 있다.

영국은 2004년 5월에 발효된 '성범죄법(Sexual Offences Act 2003)'을 적용하고 있는데 그 모체인 1978년의 아동보호법과 달리 성범죄법에서는 제45조에 아동을 16~18세로 상향조정하였다. 따라서 다른 형사법에서도 이와 같은 연령이 적용되며 예외규정으로 아동이 촬영시 16세이상이거나 촬영에 이해된 동의를 한 경우(Section 1A(1))와 촬영된 자와 사진 소유자가 혼인이나 동거 등의 가족 또는 준가족관계에 있는 경우를 예외로 인정하고 있으나 촬영에 동의한 아동 이외의 아동이 함께 표현된 경우는 제외된다[125].

스코틀랜드 의회는 2005년 소위 그루밍 법안(grooming law)으로 불리는 아동보호법안(Protection of Children Bill)을 통과시켰는데, 그 내용은 인터넷 채팅방을 통해 16세 미만의 아이들과의 만남을 꾀하는 행위에 대한 중형 선고, 17세 미만의 음란성 아동사진 제공 행위에 대한 처벌 등의 아동과 관련한 음란물 및 음란행위에 관한 것이다.

일본의회는 1998년 '풍속영업정화법' 개정안을 상정하여 불건전정보 유통을 방지하고 있으며, 1999년에 '아동매춘 및 포르노처벌법'을 시행하여 18세 미만의 아동에 대하여 아동매춘 및 포르노에 관계되는 행위자를 강력하게 처벌할 수 있는 법적 근거를 마련하였다. 또한 인터넷을 통한 포르노 산업의 활개로 인해 통산성을 인터넷관련 산업계에서 창설한 전자네트워크협의회의 활동을 지원하여 '인터넷사업자 윤리실천강령'과 '이용자윤리강령'등을 제정토록 하여 자율적으로 규제하는 정책을 펴고 있다[126].

4) 사이버 도박

상업적 도박이 경제의 일부분이 된 미국은 최근 인터넷을 이용한 사이버도박(Virtual gambling)의 성행을 집중적으로 단속하여 도박시장이 인터넷 중심으로 전환되는 것에 대한 강력한 대응을 하고 있으며 다른 한편으로는 합법적으로 도박을 허용하는 나라에 서버를 둔 도박사이트들로 인해 도박자금이 해외로 유출되는 것을 우려하고 있는 추세이다.

미국도 도박을 금지하는 연방법인 유선망법(The Wire Act)이 존재하고 주간 또는 외국의 도박 및 스포츠, 경연 등에 돈을 거는 정보를 전송하거나, 도박의 결과로 도박하는 자가 돈이나 기타 예금을 받는 행위, 돈을 거는 행위를 돕는 정보를 전송하는 도박업 종사자에게 1만달러 이하의 벌금 또는 2년 이하의 징역 또는 병과하도록 규정하고 있다. 그러나 이법의 '유선통신망'이 유선(Wire)으로만 국한되어 있기 때문에 무선으로 이루어지는 모바일 도박은 적용할 수 없다는 한계가 존재 한다. 미국은 이와 같은 문제점을 감안하여 1998년 연방 상원의원회

125) 정상훈, 전게논문, 75~76면; 유석준, 전게논문, 15면.
126) 조성택, "사이버 범죄의 규제에 관한 연구:사이버 음란물을 중심으로", 「한국지역정보화학회지」 제9권 제2호, 한국지역정보화학회, 2006.12, 136~138면.

는 인터넷 도박금지를 명문화한 '인터넷도박금지법(Internet Gambling Prohibition Act)'을 통과시켰다. 이 법안에 따르면 도박업자뿐 아니라 이 도박을 즐기는 개인도 처벌할 수 있게 되어 있다. 또 정부는 ISP들에게 도박사이트의 접속을 금지하도록 명령할 수 있다[127].

5) 사이버스토킹

1989년 캘리포니아 주의 여배우 셰퍼(Revecca Schaeffer)사건으로 처음 제정된 미국의 스토킹 금지법은 1992년 27개의 주로 확대되어 스토킹 관련 유사법률의 제정을 도모하였으며 1996년 연방법으로 제정되어 모든 주에서 처벌할 수 있도록 '스토킹방지 및 피해자보호법(Stalking Prevention and Victim Protection Act of 1999)'이 수정 공포되었다. 연방법 제18장 제2261A조는 스토킹이란 '어떤 사람의 2회 이상 특정개인에 대한 죽음이나 신체상해 또는 그 개인의 가까운 가족구성원에 대한 죽음이나 신체상의 상당한 공포감(reasonable fear of the death or serious bodily injury)을 주거나 또 그러한 행위가 공포감을 준다고 믿을 만한 상당한 이유가 있거나, 있음을 알고 있는 경우'라고 규정하고 있다. 미국의 스토킹금지법은 피해자보호에 중심을 두고 있으며 양형에서도 중형을 명문화하여 초범인 경우에도 1년 이하의 징역까지 처할 수 있도록 하고 있다. 그러나 급속히 변해가는 사이버공간의 다양성으로 스토킹의 수법이 날로 변화하고 있어 적절한 대응을 위해 사이버스토킹에 대한 별도의 법안을 만들자는 입법추진이 제기되어 2000년 7월27일에 상원 사법위원회에 제출되어 심의중이다[128].

독일에서는 사이버스토킹에 대한 처벌이 사실상 규정되어 있지 않아서 형법에서 규정하고 있는 강요죄(§240 StGB, Nötigung) 및 협박죄(§241 StGB, Bedrohung), 상해죄(§223ff StGB) 등을 확대 해석하여 적용하고 있었으며, 2001년 12월 11일 '폭력보호법(Gewaltschutzgesetz, GesSchG vom)'의 제정으로 피해자의 의지에 반하여 반복해서 따라다니는 행위, 통신수단을 이용한 추적행위는 1년 이하의 징역이나 벌금형에 처하고 있다.

---

127) 정상훈, 전게논문, 74~75면; 신현정, 전게논문, 58면.
128) 2000년 사이버 스토커 처벌법(Just Punishment for Cyberstalkers Act of 2000).

영국의 경우 스토킹 행위를 규제하기 위하여 1988년 '부당통신법(Malicious Communications Act 1988)'이 제정되었으며 타인에게 고통 또는 근심을 야기할 의도로 음란하거나 심히 모욕적인 메시지 또는 위협 등의 정보를 전달하는 편지 또는 글을 보낼 경우도 처벌하고 있다. '희롱방지법(Protection from Harassment Act 1977)' 제7조 제2항을 통하여 누구든지 고의 또는 과실로 타인을 괴롭히는 일련의 행위를 한 경우 징역 또는 벌금형에 처할 수 있도록 하고 있고, 2회 이상의 폭력의 공포에 빠뜨리는 행위에는 징역 또는 벌금에 처하도록 규정하고 있다. 영국의 경우 행위자에 대한 손해배상 책임을 인정하고 있다는 것이 특징이지만, 위 법조항이 사이버공간을 매개로 한다는 정확한 명시적 규정이 없어 사이버 스토킹에 대한 법률적용에 문제가 발생할 수도 있을 것이다.

일본은 2000년 11월 24일에 발효된 '스토커행위등규제에관한법률'에서 2가지 유형의 스토커 행위를 규제하고 있다. 제2조 1항은 '따라다니기 등'이라 함은 특정인에 대하여 연애 감정 등의 호의적 감정 또는 그것이 충족되지 않은데 대한 원한의 감정을 충족하기 위하여 그 특정인 또는 그 가족 등을 대상으로 행하는 행위로 규정하고 제1호에서 8호까지 8가지로 분류하고 있다. 제2조 제2항 '스토커행위'라 함은 동일한 자에 대하여 '따라다니기 등'을 반복하여 행하는 것을 말한다고 규정하고 있으며 위반시 금지명령을 행할 수 있고 이를 위반시 1년 이하의 징역 또는 100만엔 이하의 벌금이 부과된다. 이 법의 경우에도 컴퓨터통신 등의 매체를 구체적으로 지정하고 있지 않다는 점에서 사이버스토킹을 처벌하기 위한 본격적 대응법규라고 보기에는 어려움이 있다[129].

6) 사이버 명예훼손 · 모욕

비교법적으로 보면 명예훼손에 관한 죄를 범죄로 취급하여 처벌하고 있는 것이 독일, 일본, 우리나라 등 대륙법계의 입장이며, 영미법계 국가들은 이를 범죄로 취급하지 않고 단지 민법상의 불법행위로 취급하는데 그치고 있다[130].

독일 형법 제185조는 '모욕은 1년 이하의 징역 또는 벌금에 처한다. 모욕이

129) 백광훈, "사이버스토킹과 그 처벌법규 및 문제점", 사이버범죄연구회 제17회 세미나 발표자료, 2001.6; 정상훈, 전게논문, 77~78면.
130) 정영일, 「형법각론」, 박영사, 2006, 144~145면.

폭력행위를 수단으로 하여 범하여진 경우에는 2년 이하의 징역 또는 벌금형에 처한다'고 규정하고 있다. 동법 제194조에서는 명예훼손 및 모욕죄를 친고죄로 규정하고 있고(동법 제194조), 동법 제193조에서는 위법성조각사유도 적용한다. 독일 형법은 제188조의 정치인에 대한 명예훼손의 경우를 제외하고는 명예훼손 및 모욕죄에 있어서 공연성을 요구하고 있지 않고, 다만 공연히 또는 문서의 유포 또는 집회 내에서의 행위인 경우에만 그 형을 가중하고 있다(동법 제185조, 제186조, 제187조, 제190조, 제192조). 한편 독일은 정보통신 또는 이와 유사한 다른 수단을 이용하여 실행된 명예훼손 및 모욕을 처벌하는 별도의 특별법이 존재하지 않고, 일반 형법전의 규정에 따르고 있다.

일본은 형법 제34장에서 명예에 관한 죄를 규정하고 있고 모욕죄에 대하여는 '사실을 적시하지 아니하여도 공연히 사람을 모욕한 자는 구류 또는 과료에 처한다'고만 규정하고 있을 뿐이다(동법 제231조).

국회입법조사처에 따르면 중국엔 사이버검열과 관련된 법이 60개가 넘고, 그 하위 법령 중 '타인을 모욕하고 비방해서 그것이 범죄를 구성할 때에는 형사책임을 추궁받는다'는 규정이 있다고 한다[131].

7) 인터넷 사기

미국은 인터넷 사기에 대하여 연방법 제45조, 제52조 15 U.S.C. §§45, 52(불공정행위, 기망행위), 제25조, 제52조 15 U.S.C. §§25, 52(허위광고), 제1644조 15 U.S.C. §1644(신용카드 사기), 18 U.S.C. §§1028, 1029, 1030(식별문서및 정보관련사기, 접근장치관련사기, 컴퓨터관련사기), 18 U.S.C. §1345(사기금지명령) 등을 적용하고 있다.

독일은 인터넷을 통한 상거래의 사기를 포함하여 현금카드 사기, 현금 자동 입·출력기 등의 부정사용이 빈번하게 발생하고 있으며 특히 인터넷뱅킹이 증가하면서 컴퓨터를 이용한 사기 사건이 빈번하게 발생하고 있는데, 인터넷뱅킹의 경

131) 국회입법조사처, 사비버모욕죄 관련조사, 2008년 10월 17일, 4쪽. 그러나 이러한 발표 이후 중국의 고위 관계자는 이러한 결과에 대해 "중국은 반정부적인 글이나 민족의 단결을 해치는 글, 인신공격성 글은 모두 형법 등 일반법으로 다스리고 있다"면서 부인하였다. 만약 이러한 발언이 사실이라면 사이버모욕죄 규정은 우리나라가 최초로 입법화하는 셈이다. 관련기사는 한겨레신문, 장웨이창 "중국엔 사이버모욕죄 없고 필요도 없다", 2008년 11월24일자; 박혜진, "사이버모욕죄 도입에 대한 비판적 검토", 「안암법학」 28호, 안암법학회, 2009, 332~333면.

우 권한 없는 정보를 사용함으로써 이루어지게 되므로 컴퓨터사용사기죄가 적용되어 형법 제263조a에 의해서 5년 이하의 징역이나 벌금형으로 처벌된다[132].

2. 사이버범죄에 대한 국내의 법적 규제

사이버범죄에 대하여 어떠한 처벌법규가 있는지를 살펴보기 전에 사이버범죄와 컴퓨터범죄와의 구별을 통하여 정보통신망을 매개로 하지 않는 컴퓨터범죄를 사이버범죄와 동일한 형태로 간주하는 것은 다소 무리이며, 정보통신망과 무관한 컴퓨터 사기, 컴퓨터에 있는 데이터 위 · 변조, 데이터 손괴 및 컴퓨터 업무방해 등의 침해행위를 사이버범죄로 정의하는 것은 무리이며, 컴퓨터 범죄라고 개념함이 적정하다는 견해가 있다[133]. 본 견해에 의하면 정보통신망을 이용한 범죄행위를 규정하고 있는 법률들만이 사이버범죄에 관한 법규에 해당한다고 볼 여지가 있다. 그러나 사이버범죄는 기존의 컴퓨터범죄의 연속선상에서 발전되어온 개념이고, 기존의 컴퓨터범죄 관련 규정도 사이버범죄에 대처하기 위한 기본 전제가 된다는 의미에서 함께 고려할 필요가 있다 라는 주장도 제기되고 있다[134]. 또한 1995년 형법개정당시 우리나라에서 인터넷이 별로 사용되지 않았기 때문에 주로 컴퓨터범죄라는 용어들이 많이 사용되었다. 그런데 형법개정이 이루어진 1995년 이후부터 인터넷이 널리 보급됨에 따라 컴퓨터범죄의 상당부분이 인터넷을 통해 이루어지게 되었다. 인터넷 해킹을 통한 자료의 부정조작, 컴퓨터 스파이, 권한 없는 사용이나 인터넷에서의 컴퓨터 바이러스의 유포에 의한 컴퓨터 파괴 등을 그 예로 들 수 있다. 따라서 현재에는 컴퓨터범죄의 상당부분을 인터넷범죄가 차지하게 되었고 이에 따라 인터넷범죄[135] 혹은 사이버범죄라는 용어들도 사용되기 시작하였다.

1953년에 제정된 형법(1953. 9. 18. 법률 제293호)은 당시에는 제반 범죄현상을 포괄적으로 제어하기 위하여 제정되었지만, 이후 정보화 시대의 새로운 범

132) 정상훈, 전게논문, 80면.
133) 홍승희, “유비쿼터스환경과 사이버범죄”, 「형사정책연구」 제17권 제3호, 2006. 가을호, 351면.
134) 이정훈, “사이버범죄에 관한 입법동향과 전망”, 「사이버커뮤니케이션학보」 통권 제20호, 사이버커뮤니케이션학회, 2006.4, 237면.
135) 오영근, “인터넷범죄에 관한 연구”, 「형사정책연구」 제14권 제2호, 한국형사정책연구원, 2003, 300면.

죄현상에 대해서는 적절한 대응을 하지 못하였다. 또한 1970년대 이후 전산관련 정부부처별로 소관분야와 관련된 범죄현상에 대하여 개별입법이 계속되었으나, 다양한 형태로 급증한 컴퓨터관련 범죄현상을 전적으로 통제하는 것은 사실상 불가능한 실정이었다. 특히 종래 형법상의 문서에 관한 죄를 논하면서 정보의 전달과 관리, 보전방법이 통상의 문서와 전혀 달라서 그 자체로서는 비가시적, 비영구적일 수밖에 없는 전자적 기록에 대한 "문서성"의 인정문제, 그리고 재산범죄에서 전자적 정보의 "재물성"과 "점유의 이전"에 대한 개념의 해석 문제로 인해 끊임없는 논란이 있어왔다. 또한 전자자료의 위·변작이나 자료절도 등 컴퓨터 관련 범죄현상들에 대한 처벌의 필요성은 크게 요구되었으나 "죄형법정주의" 원칙상 소극적인 해석으로 사이버 범죄에 대응할 수밖에 없는 상황이었다[136]. 이러한 사정 하에 1990년대 이후 급격한 통신망의 확장과 정보전쟁의 소용돌이 속에서 고도의 지능적·기술적 수법으로 자행되고 있는 사이버 공간상의 범죄현상에 대한 법적 규제의 필요성이 한층 높아지고, 사이버공간에서 행하여지는 범죄의 대부분은 기존의 형벌법규가 전혀 예상하지 못한 불법유형이므로 "처벌법규의 공백" 상태가 나타날 수밖에 없었다. 그리하여 형법을 1995년에 일부 개정(1995. 12. 29. 법률 제5057호)한데 이어 2001년 다시 일부를 개정(2001. 12. 29. 법률 제6543호)하여 시행하고 개별적인 특별법을 제정 내지 개정하였다. 전기, 전자통신과 관련한 허위통신, 통신침해행위는 전기통신기본법, 전기통신사업법, 전파법에서 규율하고 있다. 또한 소프트웨어의 보호에 대하여는 컴퓨터프로그램보호법을 근간으로 하여 저작권법으로 이를 보충하고 있고, 특별한 펌웨어(Firmware)에 대하여는 반도체직접회로의 배치설계에 관한 법률을 바탕으로 특허법, 디자인보호법이 이를 보완하고 있으며, 도청행위에 대하여는 통신비밀보호법을 통해 규제를 하고 있다. 또한 개인의 정보를 보호하기 위하여 공공기관의개인정보보호에관한법률과 신용정보의이용및보호에관한법률을 제정하였다. 그 외에도 정보통신기반보호법, 정보통신망이용촉진및정보보호등에관한 법률, 통신비밀보호법, 공공기관의 개인정보보호에 관한 법률, 신용정보의 이용 및 보호에 관한 법률, 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률, 전자상거래등에서의소비자보호에 관한 법률 등이 그것이다[137].

136) 박성택, 전게논문, 71~72면.

그리고 정부는 기존에 여러 법률들에 산재되어 있던 사이버범죄들에 대한 처벌법규들을 통합하는 입법작업을 추진하여 정보통신망이용촉진등에관한법률을 개정하면서, 전기통신법, 전기통신사업법에 산재되어 있던 사이버범죄 관련 조항을 통합시켜 2001년 1월 16일 법률 제6360호로 정보통신망이용촉진및정보보호등에관한법률을 개정하고, 사이버테러리즘으로부터 정보통신기반을 보호하기 위하여 같은 날짜에 법률 제6383호로 정보통신기반보호법을 제정하였으며, 2001년 12월 31일자로 전자서명법(1999. 2. 5. 제정)을 개정하는 등 일련의 법제 정비작업을 마쳤다[138].

본 논문에서는 형법전에 명시된 관련 규정과 여러 특별법들 중 사이버범죄에 대한 기본법이라고 불러도 부족함이 없을 정도로 사이버범죄에 대한 처벌규정을 망라하고 있는 정보통신망이용촉진및정보보호등에관한법률에 나타난 법적 규제 방법을 살펴보기로 한다.

(1) 형법

1995년 12월 29일 국회에서는 3년에 걸친 심의 끝에 정보화 사회의 신종범죄를 규율하기 위한 형법개정안이 통과되었다. 이 개정형법은 그동안 종래 형법의 재산범죄 규정에서 “재물”, “업무”, “문서”의 개념에 컴퓨터 관련 범죄현상으로 인한 행위를 포함할 수 없었던 결함을 입법으로 해결한 것으로서 컴퓨터 관련 업무방해죄와 컴퓨터 사용사기죄 등을 신설하고, 재산범죄 중 일부 규정을 개정하였다[139]. 이후 2001년에는 형법 제347조의 2(컴퓨터등 사용사기)를 개정하여 무권한자의 정보 입력 · 변경에 의한 사기도 처벌할 수 있도록 하였다[140].

1) 전자기록에 대한 위작 · 변작 등의 죄

컴퓨터 이용의 일반화와 정보통신기기 및 시설의 보급 확대 등으로 컴퓨터에서 사용되는 전자기록이 문서와 더불어 또는 문서를 대신하여 사회적으로 중요

137) 강동범, 전게논문, 2007, 36~37면.
138) 박성택, 전게논문, 72~73면.
139) 김형준, “사이버범죄와 현행 형법의 대응”, 「인터넷법률」 제10호, 법무부, 2002, 24면.
140) 박성택, 상게논문, 73면.

한 사항에 대하여 증명기능을 담당하고 있고 아울러 정보의 기록보존기능을 하고 있기 때문에 그것의 이용가치도 보호할 필요가 있다. 그러나 전자기록 등 특수매체기록을 종래의 문서의 개념으로 포섭하기 어렵고 또한 이것에 기록된 자료만을 독립된 재물로 인정할 수 없다는 한계가 있었다. 즉 문서는 계속적 기능, 증명적 기능 그리고 작성명의 확인 기능을 가져야 하는데 전자기록은 시각적 인식이 가능한 상태로 유체물에 고착되어야 하는 계속적 기능이 결여되어 있을 뿐 아니라, 전자기록은 다수인에 의하여 만들어지는 경우가 많으므로 명의가 없거나 분명하지 않은 경우가 있어서 작성명의 확인기능(보장적 기능)을 결여하는 경우가 많다는 것이었다. 이러한 문제를 해결하기 위하여 현행 형법은 제227조의 2(공전자기록 위작 · 변작), 제232조의 2(사전자기록 위작 · 변작)을 신설하였고, 제228조(공정증서원본등의 부실기재), 제229조(위조 등 공문서의 행사), 제234조(위조사문서등의 행사), 제141조(공용서류등의 무효, 공용물의 파괴) 제1항과 제366조의 행위객체에 '전자기록 등 특수매체기록'을 추가하여 문서죄 및 손괴죄의 행위객체로 규정하여 전자기록의 위작 · 변작 및 손괴행위를 처벌할 수 있는 근거를 마련하였다.

2) 컴퓨터 등 사용사기죄

컴퓨터사용사기죄(제347조의 2)는 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 함으로써 성립하는 범죄이다. 여기서 정보처리장치란 통상적으로 컴퓨터 외에도 현금자동지급기, 신용카드조회기 등 컴퓨터를 이용한 장비를 의미한다[141]. 특히 은행업무를 비롯한 여러 거래분야에서 채권채무의 관리 · 결제 · 자금의 이동 등 재산권의 득실 · 변경의 사무가 컴퓨터에 의하여 전자기록을 사용하여 사람의 개입 없이 기계적 · 자동적으로 처리되는 상황이 증가하고, 재산권이 표창된 전자기록(선불카드, 전화카드, 전철표 등)의 사용이 늘어남에 따라 이를 악용하여 불법한 재산상의 이익을 얻는 행위도 증가하고 있음에도 불구하고 이들 행위는 사람에 대한 기망행위나 재물의 점유이전을 수반하지 않기 때문에 종래의 사기죄나 절도죄에 의해서는 적절하게 대응할 수 없었

141) 허만영 · 홍진표, 전게보고서, 65면.

다. 이에 따라 이러한 부정행위를 사기죄의 한 유형으로 파악하여 처벌하고자 컴퓨터 등 사용사기죄(제347조의 2)를 신설하였다. 본 조문은 정보통신망을 통하여 이루어지는 대금결제시스템이나 서비스에 있어서도 권한 없이 정보를 입력하여 재산상 이익을 취득하는 대부분의 사이버사기에 대처할 수 있는 규정이기도 하다[142].

3) 업무방해죄

형법 제314조 제2항의 '컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타의 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해하는 것'은 동조 제1항의 '기타 위계'에 포함될 수 없는 업무방해 방법이다. 개정형법에서는 이러한 컴퓨터에 의한 업무방해를 새로운 업무방해죄의 유형으로 동조 제2항에 신설한 것이다[143]. 컴퓨터의 보급에 의해 개인의 사무처리는 물론 금융기관이나 행정관청 등의 사무처리가 급속히 자동화되고, 그 업무범위가 현저하게 확대됨에 따라 종래 사람에 의해 처리되었던 사무의 대부분이 컴퓨터에 의해 처리되게 되었다. 그 결과 컴퓨터시스템을 파괴하거나 기타 불법적인 방법으로 정보처리에 장애를 발생시키는 행위는 현행형법의 업무방해죄와 그 본질은 동일하지만 위계 · 위력이 사람을 전제하기 때문에 컴퓨터에 대한 가해행위에 의한 업무방해를 처벌하는 별개의 구성요건을 신설한 것이다[144]. 본죄의 행위객체는 사람의 업무이며, 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록 또한 업무방해를 위한 행위수단으로서 행위객체로 볼 수 있다. 이러한 정보처리장치나 특수매체기록의 손괴 또는 정보처리장치에 의해 허위의 정보나 부정한 명령의 입력, 기타의 방법으로 정보처리에 장애를 발생시키는 일체의 행위는 본죄의 구성요건적 행위가 된다. 정보처리장치나 특수매체기록의 손괴는 물리적 파손 외에 그 효용을 해하는 일체의 행위를 포함한다. 정보처리장치에 허위의 정보나 부정한 명령을 입력시키는 것은 정보처리에 장애를 발생시키는 방법의 예시가 된다.

142) 이정훈, 전게논문, 238~239면.
143) 박성택, 전게논문, 74면.
144) 이정훈, 상게논문, 239면.

그밖에 기타의 방법으로 정보처리에 장애를 발생시키는 경우로는, 전원이나 통신회선의 절단, 동작환경의 파괴 또는 컴퓨터 바이러스를 침투시키거나 처리 불능의 대량의 정보를 입력시키는 경우 등이 있다. 또한 컴퓨터 해킹을 통하여 타인의 업무정보에 접근하는 행위는 중대하고 심각한 업무방해의 위험을 초래할 수 있다[145]. 본 규정은 최근의 DDos공격과 같이 인터넷을 통하여 회사의 홈페이지 서버를 다운시키거나 과부하 장애를 일으켜 업무를 방해한 경우에도 적용된다.

4) 비밀침해죄

비밀침해죄는 봉함 기타 비밀장치한 사람의 편지 · 문서 · 도화를 개봉하거나(제316조 제1항), 봉함 기타 비밀장치한 사람의 편지 · 문서 · 도화 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아냄(제316조 제2항)으로써 성립하는 범죄이다. '기술적 수단을 이용하여 그 내용을 알아낸 행위'란 Password Cracking이나 시스템보안장치 버그를 이용한 Root권한의 획득, 암호처리가 되어있는 데이터 파일에서 암호 루틴을 해제하는 방법 또는 암호해독장치를 이용하여 암호를 풀어내는 방법 등 어떠한 방법에 의하든 모두 여기에 해당한다. 다만 공무원이 그 직무에 관하여 봉함 기타 비밀장치란 문서 · 도서 또는 전자기록 등 특수매체기록을 개봉 내지 기술적 수단을 이용하여 그 내용을 알아낸 경우에는 형법 제140조의 공무상 비밀침해죄에 해당한다. 이 비밀침해죄는 고소가 있어야 공소를 제기할 수 있는 친고죄(형법 제318조)이다[146].

(2) 정보통신망이용촉진 및 정보보호 등에 관한 법률

1995년의 형법개정을 통한 컴퓨터범죄 관련 규정들은 현재의 사이버범죄에 대한 기본적인 대처법규로서 기능하고 있기는 하지만 인터넷이라는 사이버공간에서 발생하는 새로운 범죄유형에 대처하는 것에는 미흡한 점이 없지 않았다. 예컨대, 기존의 형법은 유체물에 한정된 법해석을 유지하고 있었기 때문에 이른바 사이버포르노에 대응할 수 없었고[147], '전자기록'이라는 구성요건을 추가하였음

145) 박성택, 전게논문, 75면.
146) 박성택, 상게논문, 73~74면.

에도 불구하고 정보통신망을 통해 전송되는 데이터 침해에 대해서 적절히 대응할 수 없었다[148]. 아울러 해킹이나 바이러스에 의한 불법행위에는 더더욱 현행 형법으로 대처하기에는 한계가 존재하였다[149]. 기존의 정보통신망이용촉진등에 관한법률이 정보통신망이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법이라 함)이라는 명칭으로 개정되어 2001년 7월 1일부터 시행되고 있다. 개정 법률에서는 기존 법률에 처벌조항이 없었던 정보통신망이용 명예훼손, 바이러스 등 악성프로그램 전달 · 유포, 서비스거부공격, 사이버스토킹 행위 등에 대한 처벌조항이 신설되었다[150]. 신설당시 제61조에서 제65조에 규정되었던 벌칙조항은 2007. 12. 21. 개정으로 제70조 이하로 변경되었다. 그 주요내용은 다음과 같다.

1) 정보통신망을 통한 명예훼손에 관한 규정(제70조)

신설당시 제61조에서 2007.12.21 개정을 통하여 제70조로 이동하여 현재 동법 제70조에서는 정보통신망을 통한 명예훼손죄를 규정하여 인터넷상의 명예훼손행위를 규제하고 있다. 그 내용은 제1항에 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처한다. 제2항에 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다. 제3항에는 제1항과 제2항의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다고 규정하고 있다. 사이버 명예훼손은 인터넷의 높은 전파성과 지속성이 출판물에 의한 명예훼손죄(형법 제309조)와 유사함에도 불구하고 인터넷게시판 등은 형법 제309조의 '신문 · 잡지 · 라디오 · 기타 출판물'에 해당하지 않으므로 제307조로 처벌할 수 밖에 없다는 점을 고려하여 정보통신망 명예훼손죄가 신설된 것이다. 동죄는 출판물에 의한 명

147) 인터넷상의 사이버음란물이 형법의 적용대상이 아니라고 한 대법원 1999.2.25. 선고 98도3140판결.
148) 전자기록은 해석상 데이터와 매체를 구별할 수 없는 개념으로서 데이터(정보)가 일정한 매체에 화체되어 있는 상태를 의미하므로 전송중인 데이터는 형법의 포섭대상이 되지 않는다.
149) 이정훈, 전게논문, 239~240면.
150) 박성택, 전게논문, 79면.

예훼손죄와는 달리 '공연성'을 요하므로, 공연성이 없는 1 : 1대화방이나 1 : 1 메일의 경우에는 설령 '비방의 목적으로 정보통신망을 통하여' 사실을 적시 하였더라도 동죄가 성립하지 않는다[151]. 물론 '비방의 목적이 없는' 사이버 명예훼손은 공연성이 있는 경우에 형법상의 명예훼손죄로 처벌되며[152], 사이버모욕죄와 관련하여 판례는 인터넷게시판에 타인을 비방하는 글을 게시한 행위에 대하여 형법상의 모욕죄(제311조)가 성립한다고 하였다[153].

2) 개인정보에 대한 규정(제71조 제1호, 3호, 6호, 제72조 제2호)

동법 제71조의 1호와 3호는 정보통신서비스제공자와 이용자의 개인정보를 취급하거나 취급하였던 자는 개인정보를 훼손 · 침해 또는 누설하여서는 아니 된다고 명시하고, 제72조의 2호에는 분쟁조정위원회의 분쟁조정 업무, 정보보호관리체계 인증업무, 정보보호시스템의 평가업무, 정보보호 안전진단 업무, 명예훼손분쟁조정부의 분쟁조정 업무에 종사하거나 종사하였던 자의 직무상 알게 된 개인정보에 대한 누설이나 직무상 목적 외에 이를 사용한자에 대한 규정을 두어 업무상 비밀침해죄에 대해 규정하고 있다. 그러나 이는 일정한 업무에 종사하거나 종사하였던 자들이 주체가 되는 신분범의 성격을 띠고 있는 범죄로서 오프라인에서도 이루어질 수 있는 범죄이고 반드시 인터넷을 통하여 행해지는 것은 아니다. 따라서 전형적인 인터넷범죄에 속한다고 보기는 어려운 점이 있다. 그리고 제71조의 11호에는 정보통신망에 의하여 처리 · 보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해 · 도용 또는 누설한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 명시하여 개인정보에 대한 정보훼손 및 비밀침해죄를 규정하고 있다. 형법 제316조 제2항의 비밀침해죄의 객체가 전자기록 등 특수매체기록이어서 전송중인 데이터는 객체가 될 수 없는데, 본죄는 전송중인 데이터도 비밀침해의 객체로 하여금 범죄규정을 확장한 것이다. 또한 내

151) 공연성이 없으므로 명예훼손죄(형법 제307조)도 성립하지 않는다.
152) 대법원은 '직장의 전산망에 설치된 전자게시판에 타인의 명예를 훼손하는 내용의 글을 게시한 행위가 명예훼손죄를 구성한다'고 판시하였다(대판 2000.5.12 99도5734).
153) 대법원은 '모욕죄는 사람의 외부적 명예를 저하시킬 만한 추상적 판단을 공연히 표시하는 것으로 족하므로, 표시 당시에 제3자가 이를 인식할 수 있는 상태에 있으면 되고 반드시 제3자가 인식함을 요하지 않으며, 피해자가 그 장소에 있을 것을 요하지도 않고 피해자가 이를 인식하였음을 요하지도 않으므로, 행위자가 피해자를 대면할 때만 모욕죄가 성립한다는 상고이유 주장은 받아들일 수 없다'고 판시하였다(대판 2004.6.25. 2003도4934).

용을 알아내지 않고 정보를 훼손하거나 침해하는 행위는 형법상 비밀침해죄에 해당하지 않는데, 이를 범죄로 규정한 것이다[154]. 제74조 5호에는 인터넷 홈페이지 운영자 또는 관리자의 사전 동의 없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램 그 밖의 기술적 장치를 이용하여 전자우편 주소를 수집 · 판매 · 유통 또는 정보전송에 이용한 자를 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다고 명시하였다. 이것은 2002년 12월 개정 시에 신설된 것으로 스팸메일을 규제하기 위한 것이라고 할 수 있다.

3) 악성프로그램의 전달 · 유포에 관한 규정(제71조 제9호)

제71조 제9호는 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손 · 멸실 · 변경 · 위조 또는 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하는 행위를 처벌하는 규정이다. 악성프로그램을 전달 또는 유포하여 업무를 방해하는 경우 형법 제314조 제2항의 업무방해죄가 성립할 수 있고, 컴퓨터나 데이터 또는 프로그램을 훼손한 경우에는 형법 제366조의 손괴죄가 성립할 수 있다. 그러나 본 죄는 업무방해를 초래하지 않거나 손괴의 결과를 발생하지 않더라도 악성프로그램을 전달 또는 유포하는 행위 그 자체를 범죄로 규정한 것이다.

4) 정보통신망 장애 · 침입에 대한 규정(제71조 제10호, 제72조 제1항 제1호)

제71조 제10호는 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 자에 대한 규정으로 업무방해나 손괴의 정도에 이르지 않더라도 정보통신망에 장애를 발생하게 하는 행위 자체를 벌하는 규정인 것이다. 제72조 제1항 제1호에는 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입함으로써 성립하는 범죄를 규정함으로써 해킹에 대한 처벌규정을 명시하여 정보통신망의 장애나 업무방해가 발생하지 않았더라도 단순히 침입만 하더라도 범죄가 성립될 수 있도록 하였다.

154) 오영근, 전게논문, 308~309면.

5) 음란 및 청소년 유해정보에 관한 규정(제74조 제1항 제2호, 제73조 제2호, 제3호)

현행 형법 해석상 사이버상의 음란물에 대하여는 음란물죄가 적용되지 않는 결과 대부분의 음란물이 인터넷을 통하여 유포되고 있는 현실을 감안하여 제74조 제1항 제2호에서는 '정보통신망을 통하여 음란한 부호 · 문언 · 음향 · 화상 또는 영상을 배포 · 판매 · 임대하거나 공공연하게 전시한 자'를 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하는 규정을 두고 있다. 동법 제42조(청소년유해매체물의 표시)는 '전기통신사업자의 전기통신역무를 이용하여 일반에게 공개를 목적으로 정보를 제공하는 자(이하 "정보제공자"라 한다) 중 「청소년보호법」 제7조 제4호에 따른 매체물로서 같은 법 제2조 제3호에 따른 청소년유해매체물을 제공하려는 자는 대통령령으로 정하는 표시방법에 따라 그 정보가 청소년유해매체물임을 표시하여야 한다'고 규정하고 있다. 동법 제73조 제2호는 이에 위반하여 청소년유해매체물임을 표시하지 아니하고 영리를 목적으로 제공한 경우 2년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있다. 또한 제42조의2(청소년유해매체물의 광고금지)는 '누구든지 「청소년보호법」 제7조제 4호에 따른 매체물로서 같은 법 제2조 제3호에 따른 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호 · 문자 · 음성 · 음향 · 화상 또는 영상 등의 형태로 같은 법 제2조 제1호에 따른 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시하여서는 아니된다'고 규정하고 제73조 제3호에 이를 위반하여 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시한 자 대하여 2년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 규정하고 있다.

6) 사이버스토킹 행위에 관한 규정(제74조 제1항 제3호)

제74조 제1항 제3호는 정보통신망을 통하여 공포심이나 불안감을 유발하는 부호 · 문언 · 음향 · 화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자를 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하되, 제2항에서 이를 반의사불벌죄로 규정하고 있다. 이는 소위 사이버스토킹을 범죄화한 것으로 사이버스

토킹은 성적접근과 무관하며, 1회의 행위만으로는 성립할 수 없다는 점에서 사이버성폭력과 구별된다[155].

(3) 사이버범죄의 유형별 처벌규정

1) 해킹

해킹이란 타인의 전산망에 부정접속 내지 부정접근 또는 무단침입 행위를 의미한다. 현행 형법상 국가 기업의 공공전산망에 침입해 정보를 파괴하는 행위에 대하여는 공전자기록과 사전자기록 위작 · 변작죄(제227조의 2, 제232조의 2), 전자기록 손괴죄(제316조 제1항), 업무방해죄(제314조 제2항)등으로 처벌할 수 있으며, 전산망에 특별한 피해를 주지 않는 단순 해킹행위도 업무방해죄나 비밀침해죄(제316조 제2항)로 처벌할 수 있다. 그러나 형법상의 비밀침해죄는 특수한 보호조치를 취한 개인의 비밀을 보호하는 규정이므로 암호조치를 해 놓은 컴퓨터상의 전자기록에 접근하여 그 내용을 알아낸 경우에는 본죄에 해당하지만 별도의 보안대책을 강구하지 않은 데이터베이스에 대한 무단접근행위에는 적용될 수 없다. 또한 내용이 '전자기록'의 형태로 저장된 것이어야 하는데, 전송중인 자료나 정보는 영속성이 없어 이에 해당하지 않으므로 컴퓨터통신에 의하여 교환되는 비밀을 해킹에 의하여 알아내는 행위에 대해서는 형법에 의하여 처벌할 수 없다. 다만 이에 대하여는 통신비밀보호법 제16조 제1항, 제3조, 정보통신망법 제72조 제1항 제1호, 제48조 제1항에 의하여 처벌할 수 있으며, 미수범도 처벌된다(동조 제2항). 또한 물류전산망의 보호조치를 침해하거나 훼손하는 행위는 물류정책기본법(구 화물유통촉진법:2007.8.3개정) 제54조의 4에 의해 처벌된다.

그리고 현행 형법상의 비밀침해죄는 타인의 전자기록 등 특수매체 기록에 담겨진 비밀을 기술적 수단을 이용하여 알아낸 행위만을 처벌하도록 규정하고 있어 '단지 타인의 시스템에 침입만 하고 그 내용은 알아내지 못한 행위'에 대하여는 처벌할 수 없다. 그러나 이에 대하여는 특별법인 정보통신망법 제72조 제1항 제1호, 제48조 제1항에 의하여 처벌하는 것이 가능하다[156]. 판례도 "정보통신망

155) 강동범, 전게논문, 2007, 38면.
156) 김희준, 전게논문, 460면.

이용촉진 및 정보보호 등에 관한 법률 제48조 제1항은 구 전산망 보급확장과 이용촉진 등에 관한 법률 제22조 제2항 및 구 정보통신망 이용촉진 등에 관한 법률 제19조 제3항과 달리 정보통신망에 대한 보호조치를 침해하거나 훼손할 것을 구성요건으로 하지 않고 '정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입'하는 행위를 금지하고 있으므로, 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 그 보호조치에 대한 침해나 훼손이 수반되지 않더라도 부정한 방법으로 타인의 식별부호(아이디와 비밀번호)를 이용하거나 보호조치에 따른 제한을 면할 수 있게 하는 부정한 명령을 입력하는 등의 방법으로 침입하는 행위도 금지하고 있다고 보아야 한다"고 하고 "이용자가 자신의 아이디와 비밀번호를 알려주며 사용을 승낙하여 제3자로 하여금 정보통신망을 사용하도록 한 경우라고 하더라도, 그 제3자의 사용이 이용자의 사자 내지 사실행위를 대행하는 자에 불과할 뿐 이용자의 의도에 따라 이용자의 이익을 위하여 사용되는 경우와 같이 사회통념상 이용자가 직접 사용하는 것에 불과하거나, 서비스제공자가 이용자에게 제3자로 하여금 사용할 수 있도록 승낙하는 권한을 부여하였다고 볼 수 있거나 또는 서비스제공자에게 제3자로 하여금 사용하도록 한 사정을 고지하였다면 서비스제공자도 동의하였으리라고 추인되는 경우 등을 제외하고는, 원칙적으로 그 제3자에게는 정당한 접근권한이 없다고 봄이 상당하다. 따라서 피고인이 업무상 알게 된 직속상관의 아이디와 비밀번호를 이용하여 직속상관이 모르는 사이에 군 내부전산망 등에 접속하여 직속상관의 명의로 군사령관에게 이메일을 보낸 사안에서, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조 제1항에 규정한 정당한 접근권한 없이 정보통신망에 침입하는 행위에 해당한다[157]"고 판시하였다. 즉, 정보통신망의 보호조치에 대한 침해나 훼손 없이 부정한 방법으로 타인의 아이디와 비밀번호를 이용하거나 보호조치에 따른 제한을 면할 수 있게 하는 부정한 명령을 입력하는 등의 방법으로 침입하는 행위도 본죄에 해당한다고 보았다. 또한 해킹에 의해 타인의 PC뱅킹 등 사이버거래에 필요한 비밀번호 등을 알아낸 뒤 이를 이용하여 타인계좌의 예금을 이체하거나 은행의 프로그램을 변경하여 자신의 계좌에 일정액 이하의 이자가 자동으로 이체되도록 하는 방법 등에 의해 재물이나 재산상 이익을 취득하는 경우, 현재 해킹

157) 대법원 2005.11.25. 2005도870.

에 의한 재산취득에 적용될 수 있는 구성요건은 형법에 규정된 컴퓨터 사용사기죄(형법 제347조의 2)이다[158]. 개인정보침해와 관련하여 재물이나 재산상의 이익 취득 목적으로 다른 사람의 주민번호 등 개인정보를 도용하여 회원으로 가입한 경우에는 주민등록법 위반이 적용될 수 있다.

2) 바이러스 전달 및 유포

정보통신망법은 정보통신시스템, 데이터 또는 프로그램 등을 훼손, 멸실, 변경, 위조 또는 그 운용을 방해할 수 있는 프로그램을 악성프로그램이라고 표현하고 이를 전달 또는 유포하여서는 아니된다(제48조 제2항)고 규정하고 제71조 제9호에 이를 위반한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 규정하였다. 또한 정보통신기반보호법은 컴퓨터바이러스라는 용어를 직접적으로 사용하고 있다(제2조 제2호[159], 제12조 제2호[160]).

3) 스팸메일

스팸메일(spam mail)이란 수신자가 원하지 않는 정보를 영리목적으로 반복하여 전송하는 메일로서 반복성이 있으며, 영리목적을 갖고 불특정 또는 다수인을 대상으로 하고 있다. 정보통신망법 제50조 제1항은 누구든지 명시적인 수신거부의사에 반하는 영리목적의 광고성 정보전송을 금지함으로써 옵트인(Opt-in)방식을 취하고 있다. 즉 영리목적의 광고성 정보를 전송하고자 하는 경우에는 수신자의 사전동의를 얻어야 한다(동법 제50조 제2항). 스팸메일의 형사처벌 여부에 대해 논란이 있는데, 정보통신망법 제76조 제1항 제7호는 영리목적의 광고성 정보를 전송한 자를 형벌이 아닌 행정벌(3천만원 이하의 과태료)에 처하도록 하였다. 만약 특정인에게 다량의 스팸메일을 전송하여 정보통신망에 장애를 발생하게 하면 정보통신망장애죄(제71조 제10호)를 구성한다. 또한 전자상거래등에서의 소비자보호에관한법률 제45조 제1항 제6호는 소비자에게 구매권유 광고를 송신한

158) 강동범, 전게논문, 2000, 84~85면.
159) "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다.
160) 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위.

자를 1천만원 이하의 과태료에 처하도록 하였다[161]. 최근 미국, 일본을 비롯한 대부분의 외국에서 모두 형사처벌을 통해 강하게 규제하는 등 형사처벌의 필요성이 제기됨에 따라 우리나라도 이러한 스팸발송에 대한 형사처벌을 통해 불법 스팸메일발송에 대한 경각심을 높여, 기하급수적으로 증가하고 있는 스팸으로부터 피해를 최소화하자는 여론이 반영된 것으로 볼 수 있다[162].

4) 사이버 폭력

사이버상의 각종 폭력행위는 물리적인 폭력을 동반하지는 않지만 심리적으로 상당한 압박을 가하는 것이 사실이며 건전한 사이버 생활을 방해한다는 점에서, 또한 상대방의 의사를 무시하고 일방적으로 지속적으로 행해질 수 있다는 점에서 문제가 되고 있어 관련 처벌규정이 마련되어 있다. 특히 오프라인공간에서의 단순 스토킹 행위에 대해서는 형사처벌을 할 수 없는 반면, 사이버스토킹에 대해서는 처벌규정이 마련되어 있다[163]. 사이버스토킹은 사이버공간에서 공포심이나 불안감을 유발하는 부호 · 문언 · 음향 · 화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 것을 말하며, 이러한 행위는 정보통신망법 제74조 제1항 제3호(정보통신망 이용 공포심 유발 정보전달죄)에 의해 처벌된다. 사이버스토킹은 성적접근과 무관하며, 1회의 행위만으로는 성립할 수 없다는 점에서 사이버성폭력과 구별된다[164]. 다만 이 규정은 반의사불벌죄로서 피의자의 명시적 의사에 반하여 처벌할 수 없다.

사이버 성폭력, 즉 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화 · 우편 · 컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 성폭력범죄처벌및피해자보호등에관한법률 제14조(통신매체이용음란)에 의해 2년 이하의 징역 또는 500만원 이하의 벌금에 처해진다. 또한 최근 몰래카메라 등을 통해 촬영된 동영상 파일이 인터넷에서 유포되어 문제를 야기하고 있는데 카메라, 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또

161) 강동범, 전게논문, 2007, 43면.
162) 홍승희, 전게논문, 2006, 367~368면.
163) 양근원·임종인, 전게논문, 95~96면.
164) 강동범, 상게논문, 2007, 38면.

는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영하거나 그 촬영을 반포 · 판매 · 임대 또는 공연히 전시 · 상영한 자는 성폭력처벌법 제14조의 2(카메라등 이용촬영)에 의하여 5년 이하의 징역 또는 1천만원 이하의 벌금에 처해진다. 따라서 피해자의 동의하에 촬영한 경우에는 본죄의 구성요건에는 해당하지 않으며, 제14조의 통신매체이용음란죄와는 달리 친고죄가 아니다. 이는 몰래카메라의 촬영행위가 여관이나 화장실 혹은 목욕탕 등에서 불특정 다수인을 상대로 하는 경우가 많아 피해자를 특정하기 어렵다는 현실적인 이유를 고려한 것[165]으로 볼 수 있다. 또한 동법 제14조의 2 제2항에서는 영리목적으로 제1항의 촬영물을 정보통신망을 이용하여 유포한 자는 7년 이하의 징역 또는 3천만원 이하의 벌금에 처한다고 규정하여 최근 몰래카메라를 이용, 이를 촬영하여 영리목적으로 인터넷에 게시하는 행위에 대하여도 처벌이 가능하다.

5) 사이버 명예훼손

형법에는 타인의 명예훼손, 출판물에 의한 명예훼손죄 등이 규정되어 있어서(형법 제309조) 종래에는 사이버상의 명예훼손죄에도 형법의 규정을 적용하여 왔으며, 특별히 사이버상의 명예훼손에 대하여는 지난 2001년 정보통신망법 개정시 '사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 정보통신망법 제70조 제1항이 적용되어 3년 이하의 징역이나 금고 또는 2천만원 이하의 벌금에 처해진다' 라고 규정하였다. 또한 제70조 제2항에 허위의 사실을 유포하는 경우, 즉 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처해짐으로써 가중 처벌된다. 그리고 비방의 목적이 없는 정보통신망을 통한 명예훼손은 형법 제307조 제1항 소정의 명예훼손죄의 성립 여부가 문제될 수 있고 이에 대하여는 다시 형법 제310조에 의한 위법성 조각 여부가 문제될 수 있다[166].

165) 김희준, 전게논문, 462~463면.
166) 대판 2003. 12. 26. 선고 2003도6036.

6) 사이버 사기

전자상거래가 활성화되면서 그 부작용도 적지 않은데, 예컨대 주문한 물건이 배달되지 않고 해당 사이트가 폐쇄되거나, 일부만 배달되는 등 사기 판매나 사기 경매 등 다양한 형태의 사이버사기가 발생하고 있다. 사이버사기는 형법상의 사기죄(제347조)로 처벌된다. 그리고 '컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력 · 변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 때'에는 컴퓨터사용사기죄(형법 제347조의 2)가 성립한다[167]. 또한 최근 온라인게임에서 사이버머니나 아이템 등을 매개로 하는 게임을 중심으로 이를 얻기 위한 각종 불법행위들이 많이 발생하고 있다. 아이템이나 사이버캐릭터 또는 사이버머니는 정보통신망법상의 정보[168]에 해당하므로, 이것들을 타인의 계정으로부터 자기 또는 제3자의 계정으로 옮기는 행위는 정보통신망 정보훼손죄로 처벌[169]될 수 있다. 나아가 이러한 유형의 전자정보를 재산범죄의 객체인 재물이나 재산상 이익에 해당하느냐가 문제된다. 하급심은 타인의 게임아이템을 무단으로 자신의 계정으로 이전한 경우[170], 피해자를 폭행하고 게임아이템을 빼앗은 경우[171], 게임에서 자신을 이긴 피해자를 찾아가 상해를 가하고 아이템을 빼앗은 경우[172]에 재산범죄의 성립을 인정하였다. 하지만 이러한 전자정보가 유체물이 아님은 분명하며, 정보는 관리할 수는 있으나 동력은 아니므로 재물이라고 할 수 없다[173]라고 하였다. 그러나 재산상의 이익은 재물 이외에 재산적 가치가 있는 일체의 이익을 말하며, 재산적 가치는 객관적 가치는 물론 주관적 가치도 포함한다고 보아

167) 강동범, 전게논문, 2007, 39~40면.

168) 정보란 특정목적을 위하여 광 또는 전자적 방식으로 처리하여 부호 · 문자 · 음성 · 음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식을 말한다(국가정보화기본법 제3조 제1호, 정보통신망이용촉진및정보보호등에관한법률 제2조 제2항).

169) PC방의 컴퓨터를 이용하여 게임사이트에 접속하여 권한없이 알고 있던 피해자의 아이디와 비밀번호를 입력하고 피해자의 계정에 등록되어 있던 게임속 화폐와 아이템을 자신의 계정으로 옮긴 피고인을 정보통신망 정보훼손죄로 처벌한 하급심 판례(서울지법 2003.6.3. 2003고단3578;탁희성, 전자정보 침해의 실태와 법적 규제, 한국형사정책연구원, 2005, 80면).

170) 부산지법 2004.10.7. 2004고단3425, 4613(병합) 판결은 재산상 이익을 취득하였다고 하여 컴퓨터사용사기죄를 인정하였다.

171) 서울고법은 게이머들 사이에 실제로 고액에 거래되고 있으므로 강도죄의 객체인 '재산상 이익'에 해당한다고 판시하였다(2001.5.8. 2000노3478).

172) 서울서부지법은 2000.11.8 선고한 판결에서 게임아이템이 현실공간의 이용자 사이에 돈으로 거래되고 청소년 사이에서는 선물로도 주고받는 점에 비춰 재물성이 인정된다며 상해죄와 공갈죄를 적용하여 처벌하였다.

173) 대법원 2002.7.12. 2002도745.

야 하므로 경제적 가치가 있는 전자정보는 재산상 이익에 해당한다고 본다. 따라서 경제적 가치가 있는 전자정보, 즉 아이템 · 캐릭터 · 사이버머니 등에 대하여 재산범죄의 성립이 가능하다[174]는 견해가 있다.

7) 불법복제

컴퓨터프로그램이나 기타 저작물 또는 유용한 정보가 저장되어 있는 컴퓨터 디스켓, CD, 비디오테이프 등을 무단으로 복제하여 이용하거나 다른 사람의 홈페이지에 게시된 자료를 복제하여 자신의 창작물이나 그 소유물인 것으로 위장하려는 행위가 증가하고 있다. 저작권법 제4조에 의하면 인터넷상의 각 페이지의 글, 그림, 영상 및 프로그램 등은 언어저작물, 음악저작물, 미술저작물, 사진저작물, 영상저작물 및 컴퓨터프로그램저작물에 해당한다고 할 수 있다. 이에 의하면 원칙적으로 인터넷의 개별 홈페이지의 글이나 사진 등은 저작권법상의 대상이 된다. 따라서 저작권법 제136조 제1항에 의하여 저작재산권 그 밖에 이 법에 따라 보호되는 재산적 권리(제93조의 규정에 따른 권리를 제외한다)를 복제 · 공연 · 공중송신 · 전시 · 배포 · 대여 · 2차적저작물 작성의 방법으로 침해한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다.

8) 기타

사이버상에서 재물을 걸고 도박행위를 하는 자에 대해서는 형법 제246조(도박, 상습도박)가 적용되어 500만원 이하의 벌금 또는 과료에 처해진다. 또한 영리의 목적으로 사이버도박장을 개장한 자는 형법 제247조(도박개장)가 적용되어 3년 이하의 징역 또는 2000만원 이하의 벌금에 처해진다. 도박죄는 재물죄이므로 단순히 사이버머니를 매개로한 사이버도박 게임행위에 대해서는 본 규정을 적용할 수 없을 것이나 신용카드 등을 사용하여 현금이 오고가는 형식을 취한다면 사이버도박죄가 적용될 수 있다[175].

사이버음란물유포는 정보통신망법 제74조 제1항 제2호에 의해 처벌된다. 동죄

174) 강동범, 전게논문, 2007, 45~46면.
175) 양근원·임종인, 전게논문, 97면.

는 '음란한 부호 · 문언 · 음향 · 화상 또는 영상'을 객체로 하므로 유체물이 아닌 컴퓨터 프로그램 파일 등을 컴퓨터 통신망을 통하여 전송하는 방법으로 판매한 행위에 대하여 적용되며, 음란한 CD나 비디오테이프를 인터넷을 통하여 유포하거나 판매하는 행위는 동죄가 아닌 형법상 음화반포죄(제243조)로 처벌된다[176]. 다만 자신의 인터넷게시판이나 홈페이지에 음란사이트를 링크시켜 놓거나 음란사이트의 주소를 게시해 놓는 행위가 정보통신망법이나 형법의 '공연히 전시하는 것'에 해당하는가는 해석상 다툼이 있다[177]. 또한 음란한 동영상을 인터넷게시판에 올려 이를 다운로드 받을 수 있게 하거나 음란인터넷사이트를 개설하여 이 사이트에 접속하게 한 행위를 형법 제243조의 음란물죄로 처벌할 수 있느냐에 대하여 판례는 '형법 제243조는 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자에 대한 처벌 규정으로서 컴퓨터 프로그램파일은 위 규정에서 규정하고 있는 문서, 도화, 필름 기타 물건에 해당한다고 할 수 없으므로, 음란한 영상화면을 수록한 컴퓨터 프로그램 파일을 컴퓨터 통신망을 통하여 전송하는 방법으로 판매한 행위에 대하여 전기통신기본법 제48조의2의 규정을 적용할 수 있음은 별론으로 하고, 형법 제243조의 규정을 적용할 수 없다'[178]고 판시하였다. 이러한 대법원의 입장에 반대하는 견해[179]도 있다. 문리해석이 아니라 목적론적 해석을 해서 '기타 물건'은 '예시된 방법 이외에 음란한 내용을 전달할 수 있는 모든 매체'로 보는 것이 옳다는 것이다. 그러나 대법원의 입장이 옳다고 보는 견해에서는 형법을 입법할 당시의 대중매체 수단이 한정되어 있었기 때문에 형법 제243조의 대상은 유형적 음란물이고, 정보통신망법 처벌규정의 대상은 무형적 음란물, 곧 사이버음란물이라고 이해하는 것이 옳다고 본다[180]. 따라서 이에 대하여는 형법 제243조로 처벌하는 것은 불가

176) 대법원 1999.2.24. 98도3140.
177) 대법원은 "음란한 부호 등이 불특정·다수인에 의하여 인식될 수 있는 상태에 놓여 있는 다른 웹사이트를 링크의 수법으로 사실상 지배·이용함으로써 그 실질에 있어서 음란한 부호 등을 직접 전시하는 것과 다를 바 없다고 평가되고, 이에 따라 불특정·다수인이 이러한 링크를 이용하여 별다른 제한 없이 음란한 부호 등에 바로 접할 수 있는 상태가 실제로 조성되었다면, 그러한 행위는 전체로 보아 음란한 부호 등을 공연히 전시한다는 구성요건을 충족한다고 봄이 상당하다"고 판시하였다(2003.7.8. 2001도1335);강동범, 전게논문, 41면.
178) 대법원 1999. 2. 24. 98도3140.
179) 배종대, 형법각론(제6전정판), 홍문사, 2006, 130/6. 이와 유사하게 컴퓨터 프로그램을 기타 물건에 포함시키는 견해도 있다(박상기, 형법각론, 박영사, 2008, 580면 이하).
180) 윤동호, 전게논문, 224~225면.

능하며, 성폭력범죄의처벌및피해자보호등에관한법률 제14조의 통신매체이용음란죄로 처벌하는 것이 가능하다.

해킹, 바이러스, 개인정보침해, 인터넷사기, 유해사이트, 인터넷명예훼손, 사이버성폭력, 저작권침해, 스팸메일, 사이버성매매 등 각종 사이버범죄의 유형별로 관련 규제 법률의 현황을 예시하면 다음 표 3-1과 같다.

<표 3-1> 사이버범죄의 유형별 규제 법률

유형	관련법률
해킹	▪ 정보통신기반보호법 제28조, 제12조 ▪ 물류정책기본법 제33조, 제71조 ▪ 정보통신망법 제72조, 제48조
바이러스	▪ 정보통신기반보호법 제28조, 제12조 ▪ 정보통신망법 제71조, 제48조
비밀침해	▪ 정보통신망법 제72조, 제48조, 제49조 ▪ 형법 제316조, 제318조 ▪ 통신비밀보호법 제16조, 제3조 ▪ 주민등록법 제37조 ▪ 공공기관의개인정보보호에관한법률 제23조 제2항 ▪ 부정경쟁방지및영업비밀보호에관한법률 제18조
전자기록 손괴	▪ 형법 제366조
전자기록 위작·변작	▪ 형법 제227조의 2, 제232조의 2
정보통신망 정보훼손	▪ 정보통신망법 제49조, 제71조 11호
업무방해	▪ 형법 제314조 제2항 ▪ 정보통신망법 제48조, 제71조 10호
인터넷 사기	▪ 형법 제347조, 제347조의 2, 제348조, 제352조 ▪ 여신전문금융업법 제70조
유해사이트	▪ 정보통신망법 제74조 ▪ 형법 제246조, 제247조, 제248조, 제225조, 제229조, 제347조, 제252조, 제250조, 제260조 ▪ 총포·도검·화약류 등 단속법 제70조, 제71조 ▪ 마약류관리에관한법률 제60조, 제4조, 제91조, 제95조 ▪ 상표법 제93조 ▪ 폭력행위등처벌에관한법률 제3조, 제4조 ▪ 여신전문금융업법 제70조 ▪ 성매매알선등행위의처벌에관한법률 제20조
인터넷명예훼손	▪ 정보통신망법 제70조
사이버성폭력	▪ 정보통신망법 제74조 ▪ 성폭력범죄의처벌및피해자보호등에관한법률 제14조, 제14조의2
저작권 침해	▪ 저작권법 136조 ▪ 온라인디지털콘텐츠산업발전법 제22조, 제18조
스팸메일	▪ 형법 제314조 ▪ 정보통신망법 제48조 제3항, 제71조 5호, 제76조 제1항 제7호, 제50조, 제50조의 2 ▪ 정보통신망장애죄 제71조 제10호 ▪ 전자상거래등에서의소비자보호에관한법률 제45조 제1항 제6호
사이버성매매	▪ 형법 제242조 ▪ 아동복지법 제40조, 제29조 ▪ 성매매알선등행위의처벌에관한법률 제4조, 제19조

IV. 사이버범죄에 대한 현행법상의 문제점과 개선방안

1. 현행 형법과 관련 특별법규의 문제점과 개선방안

전술한 바와 같이 사이버범죄는 다양한 특성을 지니고 있기 때문에 일반적으로 특정할 수 있는 한 두 개의 유형만으로는 규율할 수가 없다. 왜냐하면 종래의 전통적 범죄가 단순히 사이버공간에서 일어난 경우에는 종래의 형법에 의한 해결방안을 고려해 볼 수 있으나, 사이버범죄의 다른 일부는 사이버 공간에서만 가능한 범죄적 행위들로 종래의 형법체계로는 해결이 쉽지 않은 새로운 유형의 범죄적 행위들도 존재하기 때문이다. 따라서 기존의 형법을 개정하여 컴퓨터 관련 범죄 조항을 일부 삽입하고 또한 관련 특별법을 제정하여 사이버 범죄에 대응을 하고 있는데, 이 역시 많은 문제점을 노출하고 있는 실정이다.

(1) 형법과 특별법

현행 형법전에 규정되어 있는 처벌법규는 1980년대의 PC중심의 컴퓨터범죄 유형에 대한 대책으로 입법화된 것으로, 오늘날인 2000년대에 본격적으로 인터넷 중심의 범죄에 대해 적절한 대책이 될 수 없다. 더구나 사이버범죄는 컴퓨터나 인터넷의 발전 추이에 따라 급격히 변화하는 데 반해서, 정적인 성격이 강한 형법전으로는 인터넷관련 반사회적 행위들에 대해 유효한 대응을 하기 어렵다. 그렇기는 하지만 사이버범죄는 현재 사이버공간에서 대부분의 경우 전통적인 범죄의 형식(예컨대 사기나 명예훼손 등)으로 이루어지고 있으며, 비록 사이버공간이 형성됨으로써 비로소 이루어지는 반사회적 행위라 할지라도 따지고 보면 전통적인 형법으로 대응할 수 있는 여지가 전혀 없는 것은 아니다. 예를 들면 해킹이나 컴퓨터 바이러스를 이용하여 타인의 컴퓨터나 홈페이지에 들어가 거기에 수록된 정보를 파괴하는 행위 등은 형법상 재물손괴죄[181], 업무를 방해한 경우

181) 제366조 (재물손괴등)
타인의 재물, 문서 또는 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 기 효용을 해한 자는 3년 이하의 징역 또는 700만원 이하의 벌금에 처한다.

업무방해죄[182]를 적용할 수 있다. 또한 게임아이템이나 사이버머니 등도 비록 사이버공간에서만 존재한다 할지라도 관리가 가능하고 재산가치가 인정될 경우에 그것을 재물이라고 판단할 수 있는 것으로, 이처럼 형법상으로 처벌할 수 있다는 점을 고려해 본다면 일부 사이버범죄는 현행법상으로도 적절한 대응이 가능하다. 그러나 이상과 같은 일부의 범죄를 제외하고는 전반적인 사이버범죄를 현행 형법만으로 규율하기에는 현실적으로 무리가 따른다는 것은 부인할 수 없는 사실이다. 급격하게 변화하고 있는 사이버공간의 특성상 현재의 형사법적 대응방식만으로는 한계가 존재할 수 밖에 없는 것이다.

현재 사이버범죄와 관련된 특별법들은 각 부처 간에 독자적이고 부분적인 입법에 그치고 있어 사이버범죄의 처벌과 관련하여 형법의 일반원리와 당벌성 그리고 다른 범죄들과의 형평성 등의 내용들이 구체적으로 고려되기 보다는 신속한 형사법적 대응이 필요하다는 점과 발생하는 법익침해가 막대하다는 점만이 전면에 등장하다보니 중첩적인 처벌규정들과 엄격한 규정들을 생산하여, 결국 사이버범죄에 대한 형사법적 규제는 과잉범죄화와 과잉형벌화의 문제를 지니게 되었다. 즉 동일한 구성요건 행위가 다양한 법률에 중복 또는 중첩적으로 규정되어 중복적용문제로 인한 문제가 과잉범죄화[183]를 야기하고 있으며, 동일한 내용의 불법행위가 사이버공간과 오프라인에서 발생한 경우 그에 대한 처벌규정이 각기 존재하는 경우 사이버공간에서의 법정형이 일반범죄에 대한 법정형과 비슷하거나 다소 높아 과잉형벌화[184]를 야기하고 있는 것이다. 물론 해킹이나 악성프로그램 유포 등과 같은 일부 범죄는 일반범죄에 비하여 정보통신망에 대한 신뢰성과 안전성을 위태롭게 하거나 범죄의 피해와 전파성의 정도가 매우 크다는 점에서 정당화 되어질 수 있다. 그러나 이러한 경우를 제외하고는 유사한 범죄행위가 오프라인에서 행해졌느냐 정보통신망을 통해 수행되었는가에 따라 법정형에서

182) 제314조 (업무방해)
①제313조의 방법 또는 위력으로써 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천500만원 이하의 벌금에 처한다
②컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형과 같다.

183) 이에 대하여는 본 논문의 2. 유형별 처벌법규의 문제점과 개선방안의 3) 자료손괴와 자료조작 참조

184) 이에 대하여는 본 논문의 2. 유형별 처벌법규의 문제점과 개선방안의 2) 비밀침해와 (4) 사이버스토킹 참조.

상당한 차이가 나는 것은 형평성의 견지나 과잉금지의 원칙에 비추어 처벌이 조정되어야 할 것이다[185].

형벌법규는 보호법익을 기준으로 처벌대상이 되는 행위를 유형화하여 구성요건을 형성하여야 하는데, 서로 상이한 법익을 침해하는 행위(예컨대 재산적 가치를 침해하는 정보훼손과 증명적 기능을 침해하는 자료변경)를 하나의 조문에 규정한 것은 타당하지 않다. 또한 이미 확립된 형법상의 용어가 있음에도 동일 내지 유사한 행위를 규제하는데 서로 상이하거나 생소한 용어(예컨대 위조 · 변조와 위작 · 변작, 훼손 · 침해 · 말소 · 삭제)를 사용함으로써 해석상의 어려움을 초래하여 형벌법규의 체계적 이해를 곤란하게 하고 있다[186]. 현재 우리나라 특별법의 상당수는 반드시 특별법으로 규율하여야 할 뚜렷한 이유 없이 주로 입법의 편의나 가중처벌을 위해 특별법의 형태로 만들어지고 있다. 이러한 사정은 사이버범죄의 경우에도 동일하여 형법에 규정하는 것이 가능한 구성요건들이 각종 특별법에 산재하여 있어 법률전문가들조차 그것을 찾아내기 쉽지 않은 실정이다. 물론 정부에서도 이러한 현실을 인식하고 2001년 1월 16일 법률 제6360호로 정보통신망이용촉진및정보보호등에관한법률로 개정하여 여러 법률들에 산재되어 있던 사이버 범죄들에 대한 처벌법규들을 통합하는 입법 작업을 추진하였고, 정보통신기반보호법을 제정하는 등 일련의 법제 정비작업을 마쳤다. 그러나 이들 법률 역시 하루가 다르게 증가하고 있는 사이버범죄를 효과적으로 규율하는 데는 한계를 보이고 있다[187].

(2) 실체법의 개선방안

앞서 언급한 바와 같이 우리나라의 사이버범죄 관련법규는 형법, 정보통신망법, 정보통신기반보호법 등 여러 특별법들에 산재되어 있어 이들 법규 가운데는 상호 중복되거나, 동일한 개념에 대하여 법규간 다른 용어를 사용하는 등의 문제점을 가진 법규도 적지 않다. 유사한 불법행위임에도 법정형에 현저한 차이가 있

185) 전지연, "사이버범죄의 과거, 현재 그리고 미래", 「형사법연구」 제19권 제3호, 한국형사법학회, 2007 가을호, 18~21면.
186) 허일태, 전게논문, 81면; 강동범, 전게논문, 2007, 47면.
187) 박성택, 전게논문, 87~88면; 강동범, 상게논문, 2007, 46면.

거나, 불법성에 상당한 차이가 있음에도 법정형이 유사하여 보호법익의 가치관계가 제대로 반영되어 있지 않은 경우가 많다. 법률 특히 형사처벌과 관련된 법률은 단순하고도 명확하게 규정될 필요가 있으며 가급적 일원화된 체제로 정비되어야 예측가능성을 높일 수 있다. 특별법 처벌규정은 일반법 규정이 감당할 수 없는 특별한 경우에 예외적으로 인정되는 것이 타당하다. 미국의 사이버범죄 관련 실체법적 규정을 보면 1984년에 제정된 컴퓨터 사기 및 부정이용에 관한 법을 기본으로 하여 시대적 상황을 반영하여 조문 개정작업을 거쳐 오늘날 사이버범죄에 대응하고 있는 것은 시사하는 바가 크다. 그에 반해 우리나라의 경우 컴퓨터범죄 현상과 관련한 규정을 1995년 형법 개정시 반영하였으며 기타의 사이버범죄 관련 실체법들은 기존의 형법규정을 개정하기 보다는 새로운 법을 만들어 특별법의 특별법 역할을 하게 하는 등 법적 안정성, 예측 가능성, 체계성을 크게 훼손하고 있는 것으로 판단된다.

사이버범죄에 대한 형법적 규정의 정비방안으로 사이버범죄특별법과 같이 사이버범죄의 처벌규정을 모두 하나의 특별법 규정으로 포섭하는 방안[188]과 사이버범죄의 처벌을 원칙적으로 형법에 두고 특별히 특별법에 두어야 할 필요성이 있는 경우에 한하여 특별법으로 처벌하는 방안[189]이 대립하고 있다. 사이버범죄는 이미 우리 사회에서 일반적인 현상이 되어가고 있으므로 원칙적으로 형법의 제정과 개정을 통하여 형법전으로 편입시킴으로써 해당행위에 대한 처벌의 정도를 다른 범죄들과 비교·검토함으로써 처벌범위에 대한 정당성을 획득하고 체계 및 형평성을 유지하여야 하며, 기존 범죄와 다른 유형을 가지는 특유한 형태의 사이버범죄에 대한 규정을 특별법으로 처리하는 것이 타당하다고 본다.

2. 유형별 처벌법규의 문제점과 개선방안

(1) 해킹

해킹의 처벌규정은 해킹의 유형이나 행위에 따라 처벌법규가 달라지는데 유형별

188) 원혜욱, 전게논문, 113면.
189) 강동범, 전게논문, 2007.12, 49~50면.

로 문제점을 살펴보면 다음과 같다.

1) 단순해킹

형법상 단순해킹의 처벌에 관한 찬반양론이 대립하고 있는데 형법상 단순해킹을 처벌할 경우 그 범위의 확정이 광범위해 질수 있기 때문에 단순해킹의 처벌에 문제가 있다[190]는 주장의 가장 기본적인 논거가 된다. 즉 기존의 형법적인 법익의 침해를 수반하지 않는 한 유형의 침해의 전단계로서의 해킹행위 자체는 가벌성을 인정할 수 없다는 것이다. 그러나 정보통신망 자체가 형법상 보호법익으로서의 가치를 가지고 있다는 점, 해킹기술이 점점 다양화되고 지능화 되어가고 있다는 점에서 단순해킹의 경우에도 전산망의 안정성을 침해하는 중요한 범죄이고 나아가 국가안보 위험까지 고려해야 할 것이다. 그러나 우리 형법은 단순해킹을 처벌하는 규정이 없으며, 단지 정보통신망법 제48조의 1항이나 제72조 1항 1호에 의하여 처벌할 수 있다. 그러나 해킹의 기술적 특성으로 단순 접근만으로도 해당 정보를 열람할 수가 있고 나아가 타인의 시스템과 정보통신망에 장애를 일으킬 수 있으므로 단순 해킹에 대한 형법적인 가벌성 인정여부와 확대해석이 필요하다고 생각된다.

2) 비밀침해

사이버비밀침해에 대하여 비밀침해죄(형법 제316조)[191], 정보통신망비밀침해죄(정보통신망법 제49조및 제71조 11호)[192], 전기통신감청죄(통신비밀보호법 16조)[193]가 중첩적으로 적용될 수 있을 뿐만 아니라, 행위의 불법성 정도에 비추어

190) 전지연, 전게논문, 19~20면.

191) 제316조 비밀침해 ①봉함 기타 비밀장치한 사람의 편지, 문서 또는 도화를 개봉한 자는 3년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
②봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다.

192) 제49조 (비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.
제71조 (벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
11. 제49조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자

193) 제3조 (통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.
제16조 (벌칙) ①다음 각호의 1에 해당하는 자는 10년 이하의 징역과 5년 이하의 자격정지에 처한다.

법정형이 적정한 균형을 이루고 있지 못하다. 예컨대 비밀장치(보호조치)를 해놓은 컴퓨터에 기록되어 있는 비밀을 알아낸 경우에는 형법상의 비밀침해죄와 정보통신망법의 비밀침해죄에 해당하며, 컴퓨터통신망을 이용하여 전송되는 타인의 비밀을 취득하거나 그 내용을 공개 또는 누설하는 경우에는 통신비밀보호법과 정보통신망법이 중첩적으로 적용된다. 그런데 특별히 비밀장치(보호조치)를 해놓은 비밀에 대한 침해행위(형법 제316조 제2항(비밀침해죄) : 3년 이하의 징역이나 금고 또는 5백만원 이하의 벌금)의 법정형이 보호조치가 없는 자료나 정보(다만 송수신되는 것에 한정됨)에 대한 침해행위(통신비밀보호법 등 특별법)의 법정형보다 낮은 것이나, 전기통신의 '일반적인 자료 내지 정보'의 탐지(통신비밀보호법 제16조 : 10년 이하의 징역과 5년이하의 자격정지)가 '정보통신망 비밀'의 탐지(정보통신망법 : 5년이하의 징역 또는 5천만원 이하의 벌금)보다 중한 것도 문제가 된다. 따라서 해킹에 의한 비밀침해행위를 형법이나 정보통신망법으로 일관화하거나 통신비밀보호법 위반죄의 형량을 조정할 필요가 요구된다. 이러한 법정형의 현격한 차이는 특별법의 과잉을 보여주고 형평성의 원칙에 어긋나는 것이므로 처벌규정의 일관화 및 형량을 비교 · 검토하여 과잉형벌에 대한 문제를 해소해야 할 것이다. 또한 비밀의 침해를 정보의 훼손과 함께 하나의 조문에 규정한 것은 적절하지 않다. 왜냐하면 양자는 보호법익이 전혀 상이하기 때문이다[194].

미국의 컴퓨터사기및부정이용에관한법의 제1030(a) (1)항은 컴퓨터를 이용한 비밀정보에 대한 첩보행위를 규제하기 위한 것이다. 본 규정은 본 규정은 비밀로 분류되거나 제한된 정보를 취득하기 위해 '고의로 컴퓨터에 침입'하거나 '침입을 시도'하는 자를 '그 행위만으로도 처벌'할 수 있는 근거를 마련하고 있다. 이는 우리 정보통신망법 제72조 제1항 제1호와 같은 맥락이지만 우리나라에는 간첩행위를 위한 해킹행위를 처벌하는 입법은 마련되어 있지 않고 단지 형법의 간첩죄(제98조)[195]를 적용할 수 있을 뿐으로 그 적용에 한계가 있는 것이다.

---

1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자
2. 제1호의 규정에 의하여 지득한 통신 또는 대화의 내용을 공개하거나 누설한 자

194) 강동범, 전게논문, 2007, 47~48면; 정상훈, 전게논문, 100면.

195) 제98조 (간첩)
①적국을 위하여 간첩하거나 적국의 간첩을 방조한 자는 사형, 무기 또는 7년 이상의 징역에 처한다.

3) 자료손괴와 자료조작

사이버자료손괴의 경우 형법의 재물손괴죄[196]의 규정에서 '전자기록 등 특수매체기록'에 대한 효용을 해하는 경우를 처벌하고 있으며, 정보통신망법에서는 정보통신망에 의하여 보관되는 정보를 훼손하는 경우[197]를 처벌하며, 나아가 정보통신망에 의하여 처리 또는 전송되는 정보를 훼손한 경우를 처벌한다. 또한 해당 정보가 공공기관에서 처리하고 있는 개인정보의 경우에 이를 공공기관의 개인정보처리업무를 방해할 목적으로 개인정보를 말소한 경우에는 공공기관의개인정보보호에관한법률[198]에 의해 처벌되며, 물류전산망에 의하여 처리·보관 또는 전송되는 물류정보를 훼손한 경우에는 물류정책기본법[199]에 의해, 신용정보전산시스템의 정보를 삭제 기타 이용 불능케 하는 행위는 신용정보의이용및보호에관한법률[200]에 의해 처벌된다. 이와 같이 해당 자료의 종류에 따라 다양한 법률에 중첩적으로 규정되어 있다.

사이버자료조작은 자료의 정확성과 증명가치를 해하는 것으로 정보훼손이나 비밀침해에 해당하지 않기 때문에 정보통신망 정보훼손죄나 비밀침해죄로 처벌

---

②군사상의 기밀을 적국에 누설한 자도 전항의 형과 같다.

196) 형법 제141조 (공용서류등의 무효, 공용물의 파괴)
①공무소에서 사용하는 서류 기타 물건 또는 전자기록등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
제366조 (재물손괴등) 타인의 재물, 문서 또는 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 기 효용을 해한 자는 3년이하의 징역 또는 700만원 이하의 벌금에 처한다.

197) 제48조 (정보통신망 침해행위 등의 금지)
② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.
제71조에서 이를 위반한 경우 5년이하의 징역 또는 5천만원 이하의 벌금에 처한다.

198) 제23조 (벌칙)
①공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 자는 10년 이하의 징역에 처한다.

199) 제71조(벌칙)
① 제33조제1항을 위반하여 전자문서를 위작 또는 변작하거나 그 사정을 알면서 위작 또는 변작된 전자문서를 행사한 자는 10년 이하의 징역 또는 2억원 이하의 벌금에 처한다. 이 경우 미수범은 본죄에 준하여 처벌한다.
② 제33조제2항을 위반하여 종합물류정보망 또는 국가물류통합데이터베이스에 의하여 처리·보관 또는 전송되는 물류정보를 훼손하거나 그 비밀을 침해·도용 또는 누설한 자는 5년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

200) 제50조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
3. 권한 없이 제19조제1항에 따른 신용정보전산시스템의 정보를 변경·삭제하거나 그 밖의 방법으로 이용할 수 없게 한 자 또는 권한 없이 신용정보를 검색·복제하거나 그 밖의 방법으로 이용한 자

할 수 없으므로, 형법상 전자기록위작 · 변작죄에 해당하는 경우에만 처벌이 가능하지만 처리 · 전송중인 자료를 변경하는 행위(자료의 증명력을 변경시키는 행위)에 대하여는 처벌의 공백이 있다. 또한 전자기록등 특수매체기록에는 '사무를 그르치게 할 목적으로'를 구성요건으로 하고 위작 · 변작이라는 용어를, 공문서 및 사문서에는 '행사할 목적으로'를 구성요건으로 위조 · 변조라는 용어를 사용함으로써 구성요건에 대한 법적 판단이 모호하고 용어의 사용에 있어 문서범죄와의 통일적 · 체계적인 해석을 어렵게 하는 문제가 있다. 그리고 형법상의 문서나 전자기록의 위조 · 변조에 대한 처벌은 공문서[201]의 경우와 사문서[202]의 경우의 법정형에 차이가 있으나, 물류정책기본법 제71조에 의하면 '전자문서를 위작 또는 변작하거나 그 사정을 알면서 위작 또는 변작된 전자문서를 행사한 자는 10년 이하의 징역 또는 2억원 이하의 벌금에 처한다' 라고 하여 형법의 공문서와 관련된 법정형보다 다소 중하게 처벌되며 그 정보의 중요성의 가치가 매우 큰 신용정보의 이용 및 보호에 관한 법률에서 제50조에서는 '권한 없이 신용정보전산시스템의 정보를 변경·삭제하거나 그 밖의 방법으로 이용할 수 없게 한 자 또는 권한 없이 신용정보를 검색·복제하거나 그 밖의 방법으로 이용한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다' 라고 하여 법정형의 차이를 보이고 있다. 또한 정보 등의 변경과 삭제(말소)(공공기관의개인정보보호에관한법률, 신용정보의이용및보호에관한법률)를 하나의 조문에 규정하고 있는 것도 적절하지 않다. 정보의 변경은 정보의 정확성과 증명력을 보호하는 규정이고, 정보의 삭제는 재화로서의 정보의 가치를 보호하는 규정이기 때문이다.

따라서 해킹에 의한 사이버 자료손괴(정보훼손) · 자료조작 · 비밀침해 행위 등에 대하여 특별법에 산재되어 있는 해당조문을 정리하여 각각의 해당 행위들이 가지는 처벌의 필요성과 다른 범죄와의 형평성 및 다른 법률들과의 관련성 등을 검토하여 정보통신망법이나 형법전에 편입시키거나 통합하여 법정형을 조정할 필요가 있으며, 위조 · 변조 또는 행사할 목적으로 등과 같이 용어를 통일시켜 구성요건에 대한 모호성을 줄일 수 있도록 하는 등의 작업을 할 필요가 있다.

---

201) 형법은 제225조(공문서의 위조·변조)와 제227조의 2(공전자기록의 위작·변작)죄에 대하여는 10년이하의 징역에 처한다.

202) 형법은 제231조(사문서 등의 위조·변조)와 제232조의 2(사전자기록의 위작·변작)죄에 대하여는 5년이하의 징역 또는 1천만원이하의 벌금에 처한다.

(2) 바이러스 유포행위

바이러스의 유포행위는 형법 제314조 제2항(컴퓨터손괴 등 업무방해죄)에 해당한다. 또 형법 제316조 제2항(비밀침해죄)과 정보통신망법 제48조에 의해서도 처벌될 수 있다. 그러나 바이러스 제작과 유포는 바이러스가 활동하여 비로서 법익침해가 발생해야 처벌이 가능하다는데 문제가 있다. 즉 바이러스 제작당시 잠복기를 두어 미래에 활동하거나 특정한 이벤트를 요구하는 경우 사용자가 활동기에 이르지 않거나, 특별한 이벤트를 발생시키지 않으면 아무런 증상이 나타나지 않으며 법익침해 역시 없다. 따라서 법익침해를 목적으로 제작하고 유포하였지만 미수로써 끝나 미수범 처벌규정이 있지 않는 한 사실상 처벌되지 않는다. 바이러스 외에도 보안상 취약점이나 암호해독 알고리즘의 공개, 컴퓨터 통신에 사용되는 비밀번호의 제공 등 범행원인을 제공하는 행위에는 규제가 없다[203].

따라서 정보통신망 자체를 위협하고 나아가 국가안보의 위험성을 내포하고 있는 해킹과 바이러스 제작 및 유포 행위는 개인적 법익침해의 대응체계가 아닌 국가 보호법익으로 하는 강력한 대응체계가 마련되어야 하며, 특히 바이러스 제작 · 유포행위는 법익침해가 발생해야 처벌이 가능하므로 법익침해를 목적으로 제작하고 유포하였지만 미수로써 끝나 미수범 처벌규정이 있지 않는 한 사실상 처벌되지 않는다. 따라서 형법전의 314조에 해킹이나 악성코드나 바이러스 제작 · 유포행위에 대한 미수범 처벌규정을 두어 단순해킹 행위와 법익침해가 발생되지 않은 바이러스 제작 · 유포행위에 대하여 가벌성을 인정하고 이를 처벌할 수 있도록 명시적으로 규정해야 할 것이다.

(3) 사이버사기

사이버사기에 적용될 수 있는 컴퓨터사용사기죄와 관련하여 현금의 인출이나 대출이 재산상 이익의 취득에 해당하느냐에 대하여 해석상 다툼[204]이 있다. 이

203) 정상훈, 전게논문, 140면; 신현정, 전게논문, 73면.
204) 대법원은 현금인출을 재산상 이익의 취득이 아니라고 판시하였다(대판 2003.5.13. 2003도1178).

는 동죄가 매우 빈번하게 발생하는 현금취득을 처벌하기 위한 규정임에도 불구하고 재산상의 이익만을 객체로 규정하고 있기 때문이다. 이와 더불어 최근 인터넷 게임상의 아이템이 사이버공간에서 재산적 가치를 지닌 화폐나 신용거래의 수단으로 이용되고 있다. 이러한 게임 아이템 거래의 위법성 여부에 대한 논란이 소송분쟁으로까지 확대되어 진행되었지만 아직까지도 아이템 거래의 적법한 인정을 꺼리고 있는 실정이다. 현재 게임 아이템은 게임회사의 저작물로써 현금거래에 있어서 약관의 규제를 받지만, 현실적으로 게임회사들은 게임사용료나 아이템 구매의 이익을 위하여 계정간의 양도를 허용하고 은밀한 거래를 묵인하고 있는 것이다. 게임 아이템의 재물성 인정여부[205]와 더불어 아이템 거래가 불법임에도 처벌법규의 근거를 마련하지 못하고 있으며 상호 거래에서의 신뢰위반으로 생기는 인터넷 사기 등의 재산범죄에 소극적으로 대처하고 있는 것은 명백한 법률체계의 문제라고 할 수 있을 것이다.

따라서 형법에서 재산죄의 객체를 재물과 재산상의 이익으로 나누어 규정하고 있으므로 형법상 컴퓨터사용사기죄(제347조의 2)의 객체에 재물을 추가하고, 최근 급증하고 있는 정보 · 사이버머니 · 게임 아이템의 재물성을 인정하는 법적 규정이 필요하다. 또한, 불법임에도 불구하고 빈번하게 발생하고 있는 게임 아이템 거래와 같은 특별한 유형의 행위에 대한 불법성이나 사회유해성의 실증적 분석을 통한 처벌법규의 근거마련을 위해 정부는 2006년 4월 게임산업진흥에관한법률[206]을 제정한 것은 매우 바람직한 일이라 할 것이다.

(4) 사이버스토킹

사이버스토킹은 정보통신망법(제74조 제1항 제3호)에 의해 1년 이하의 징역이나 1천만원 이하의 벌금에 처해지는데, 현실공간에서의 스토킹은 경범죄처벌법

205) 게임 아이템은 재물의 개념을 유체성설 뿐만 아니라 통설인 관리가능성설을 따른다 하여도, 아이템은 재산죄의 객체로서 재물개념에 포섭되기는 어렵다. 그러나 아이템은 현실사회에서 현금거래의 객체가 되고 있고 온라인 경제시장에 있어서도 그 거래비중이 급속히 확대되고 있으므로, 경제적 재산개념에 입각하여 경제적 가치가 있는 재산상의 이익으로 파악하는 것이 타당하다고 본다; 전지연, 전게논문, 32면.

206) 게임산업진흥에 관한 법률 제32조 제1항 7호는 '누구든지 게임물의 이용을 통하여 획득한 유·무형의 결과물(점수, 경품, 게임 내에서 사용되는 가상의 화폐로서 대통령령이 정하는 게임머니 및 대통령령이 정하이와 유사한 것을 말한다)을 환전 또는 환전 알선하거나 재매입을 업으로 하는 행위'를 규정하고 이를 위반하는 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하고 있다.

에 의해 10만원 이하의 벌금, 구류 또는 과료의 형으로 처벌(제1조 24호 및 제53호)되는 것과 비교하여 현저히 균형을 상실한 것으로 보인다.

따라서 사이버스토킹행위에 대해 정보통신망법에 의한 처벌과 경범죄 처벌법에 의한 스토킹 사이의 법정형의 현저한 불균형은 시정되어야 할 것으로 보인다. 스토킹 행위에 대한 기본적인 개념 정립과 실태 및 불법성에 대한 형법의 태도를 정립할 필요성이 있다.

(5) 사이버명예훼손

명예훼손 행위에 대하여는 형법 제307조와 제309조에 의하여 처벌되며, 사이버명예훼손 행위는 정보통신망법 제70조 제1항과 제2항에 의하여 처벌될 수 있다. 정보통신망을 이용한 명예훼손은 사이버공간의 빠른 전파성과 2차 · 3차 명예훼손 발생 가능성 등 피해의 심각성과 피해자의 법익침해가 크고 출판물에 의한 명예훼손의 규정으로는 사이버공간에서의 명예훼손을 처벌할 수 없다는 입법상의 미비를 보완하기 위한 것으로 매우 타당하다고 판단된다. 그러나 비방의 목적이 없는 정보통신망을 통한 명예훼손은 형법 제307조 제1항 소정의 명예훼손죄의 성립 여부가 문제될 수 있고 이에 대하여는 다시 형법 제310조에 의한 위법성 조각 여부가 문제될 수 있다. 또한 사이버공간에서 흔히 볼 수 있는 악의적 댓글처럼 심한 모욕성을 띠고 있는 내용의 경우 정보통신망법상의 명예훼손죄가 아닌 형법상 제311조의 모욕죄가 적용되어야 하지만 정보통신망법상에서는 모욕죄를 규정하고 있지 않다. 이 때문에 법의 균형차원에서 타당하지 않다고 하여 사이버모욕죄 신설에 관한 논의가 있었지만 표현의 자유에 대한 지나친 규제라는 반대의견과 대립하고 있는 실정이다. 명예훼손에 관한 죄를 범죄로 취급하여 처벌하고 있는 것이 독일, 일본, 우리나라 등 대륙법계의 입장이며, 영미법계 국가들은 이를 범죄로 취급하지 않고 단지 민법상의 불법행위로 취급하는데 그치고 있다. 독일은 형법에서 명예훼손 및 모욕죄에 관해 규정하고 있다. 우리나라와 달리 독일은 명예훼손 및 모욕죄를 친고죄로 규정하고 있고(동법 제194조), 위법성조각사유도 적용한다는 점에서 차이가 있다(동법 제193조). 독일 형법은 제188조의 정치인에 대한 명예훼손의 경우를 제외하고는 명예훼손 및 모욕죄에

있어서 공연성을 요구하고 있지 않고, 다만 공연히 또는 문서의 유포 또는 집회 내에서의 행위인 경우에만 그 형을 가중하고 있다(동법 제185조, 제186조, 제187조, 제190조, 제192조). 따라서 공연성을 인정하고 있는 우리의 경우 독일보다 형법상 명예훼손 및 모욕의 범위가 더 좁게 된다고 볼 수 있다. 한편 독일은 정보통신 또는 이와 유사한 다른 수단을 이용하여 실행된 명예훼손 및 모욕을 처벌하는 별도의 특별법이 존재하지 않고, 일반 형법전의 규정에 따르고 있다. 일본은 형법 제34장에서 명예에 관한 죄를 규정하고 있고 우리나라와 달리 출판물에 의한 명예훼손죄나 정보통신망을 통한 명예훼손죄에 대해 가중처벌을 하고 있지 않고 있다. 우리나라와의 공통점은 공연성을 요구한다는 것인데 상대적으로 낮은 형벌을 부과하고 있을 뿐만 아니라 명예훼손죄 및 모욕죄 모두 친고죄라는 점에서 차이가 있다(동법 제232조).

사이버명예훼손죄는 이미 일반화된 범죄행위가 되었고 사이버 명예훼손행위가 출판물에 의한 명예훼손행위와 입법취지나 불법내용에 있어 유사하므로 특별법에 두기보다는 형법 제309조 출판물에 의한 명예훼손죄에 정보통신망을 포섭하여 함께 규정하는 것이 바람직하다고 판단된다. 악성댓글과 같은 유형의 모욕에 관하여 사이버모욕죄의 신설을 주장하는 견해[207]도 있으나, 입법 취지의 정치성이나 범죄자-피해자의 특정화 · 표적화, 표현의 자유에 대한 심각한 침해 등의 우려가 크므로 사이버모욕죄에 대한 도입은 고려되어야 할 것[208]으로 판단된다. 타인을 비방할 목적의 고의가 배제된 일시적인 감정에 의한 의사표현일 수도 있으며, 사이버공간의 개방적인 특성으로 사회이슈에 대한 거침없는 대화의 장이 열릴 수 있는 표현의 자유가 충분히 보장되어야 한다고 생각한다. 따라서 제도적 규제보다는 일반 인터넷 이용자를 대상으로 인터넷 이용 의식을 개선하기 위한 홍보 · 교육활동 강화 및 자율정화운동을 통한 인터넷 윤리교육을 강화하고, 형사처벌은 악의적이고 계속적인 명예훼손 및 모욕행위가 이루어질 때 명예훼손죄의 적용이 가능할 수 있다고 생각된다.

(6) 사이버음란물 유포

207) 정완, 전게논문, 2009, 212~214면;정상훈, 전게논문, 147면.
208) 박혜진, 전게논문, 2009, 334면 이하.

사이버 음란물 유포행위에 대하여 문제가 되고 있는 것은 인터넷의 링크 기능을 이용하여 그래픽이나 텍스트를 이용하여 음란사이트로 이동하는 서비스를 할 경우 처벌이 가능한 것인가이다. 이 경우 링크자체의 음란성은 인정되지 않지만 링크를 클릭하여 열리게 되는 사이트가 음란사이트라는 점에서 음란부호로 볼 것인가에 관하여 단순한 그래픽이나 텍스트일 경우에는 음란성이 인정되지 않아 처벌할 수 없다는 문제가 발생한다. 실제 대부분의 이용자들이 음란사이트에 접근하기 위하여 포털서비스의 검색엔진이나 사이트 링크를 이용하기 때문에 이러한 음란사이트의 알선 · 중개하는 행위에 대한 입법적인 대응이 요구된다. 특히, 미국이나 영국, 독일 등 선진 각국들은 아동과 관련된 음란물에 대한 다양한 법규정 및 자율기구들을 두어 적극적으로 대응하고 있는 반면 우리의 경우에는 아동복지법, 청소년보호법 등 선진각국과 비교하여 볼 때 소극적 대응에 따른 많은 한계점을 가지고 있다. 또한 서버에 음란한 동영상을 올리는 행위는 그 서버의 소재지와 관계없이 정보통신망법으로 처벌이 가능하나, 외국에 있는 서버에 올려진 사이버음란물은 우리나라에 있는 사람이 보거나 내려받기를 해서 저장하는 것은 정보통신망법의 처벌규정으로도 처벌하기 어렵다. 따라서 사이버공간의 특성상 사이버음란물의 수출입을 규제하거나 처벌해야할 필요성이 더 크므로 사이버음란물수출입죄의 신설이 필요하다는 견해[209]와 뜻을 하지만, 단순한 내려받기인지 배포의 목적이 있는지에 대한 가벌성의 기준과 판단이 문제가 될 수 있을 것이다.

또한 사이버공간에서의 네트워크서비스제공자(IP), 온라인서비스제공자(OSP), 또는 인터넷서비스제공자(ISP) 등은 홈페이지를 비롯한 각종 상업용 사이트들의 물리적 공간계정의 할당이라는 막강한 권한을 가지고 있기 때문에 인터넷에서 성행하는 불법 서비스 및 각종 위법한 행위에 대하여 행위자를 개별적으로 규제하기 보다는 원초적인 사이트 개설과 폐쇄의 권한을 가진 서비스제공자의 규제를 촉구하고 있으며 우리나라 정보통신망법 제44조의 2(정보의 삭제 요청 등)도 이를 규정하고 있다. 그러나 이러한 강력한 통제에 대하여 위헌적 요소가 등장할 뿐만 아니라 수많은 사이버공간에서 실시간으로 일어나는 정보의 변화에 대한

209) 윤동호, 전게논문, 227면 이하.

위법성 여부를 서비스제공자가 모두 통제하기란 불가능하고 또 개별적인 이용자와의 계약관계에 놓인 이들이 이용자를 통해 발생하는 수입의 영향을 감수하면서까지 적극적으로 대처할지는 의문이다. 서비스 제공자의 형사책임을 인정할 수 있는 가에 대해서도 민사책임과 달리 형사책임에서는 직접위반의 고의를 전제로 하기 때문에 이론적으로 그 적용이 어렵다[210].

따라서 사이버음란물 유포행위의 문제에 관하여는 사회적 유해성 및 가벌성의 정도가 형법(제243조)과 정보통신망법(제44조의 7, 제74조)가 유사하므로 이를 형법 제243조에 정보통신망을 포함시켜 포괄적으로 규제하고, 모든 음란사이트의 최상위 페이지에는 음란성 게시물을 표시하지 못하도록 규제하고 포털서비스의 음란사이트 접속시 반드시 최상위 페이지만을 표기하도록 의무화하며, 링크서비스도 최상위페이지만 나타나도록 제한하도록 규정함으로써 ISP의 자율적 규제와 책임을 강화하는 것이 타당하고 생각된다.

(7) 사이버도박

미국의 경우에는 1998년 인터넷 도박 금지를 명문화한 '인터넷도박방지법(Internet Gambling Prohibition Act)'를 통과시켜 도박업자뿐 아니라 도박을 즐기는 개인도 처벌하고 ISP에게 도박사이트의 접속을 금지하도록 명령할 수 있게 하였다.

현재 사이버도박은 형법상의 도박죄[211]와 도박개장죄[212], 게임산업진흥에관한 법률[213]로 처벌되고 있지만 형법상 도박죄의 구성요건은 인터넷이 없던 시대에 만들어진 것이며, 대규모 포털사이트들이 게임사이트를 운영하여 도박을 조장하고 막대한 이익을 챙기고 있으며, 불법 포커, 경마, 경륜 등 다양한 도박 사이트

---

210) 정상훈, 전게논문, 96~98면.
211) 제246조 (도박, 상습도박)
①재물로써 도박한 자는 500만원 이하의 벌금 또는 과료에 처한다. 단, 일시오락정도에 불과한 때에는 예외로 한다.
②상습으로 제1항의 죄를 범한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
212) 제247조 (도박개장)
영리의 목적으로 도박을 개장한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
213) 제44조 (벌칙)
①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. 제28조제2호의 규정을 위반하여 도박 그 밖의 사행행위를 하게 하거나 이를 하도록 방치한 자

들이 생겨나고 있다. 이 중 특히 문제가 되는 것이 사이버머니에 대한 불법 환전으로 그 피해의 규모가 더욱 커지고, 이들 대부분이 교묘히 법망을 피해거나 가벼운 처벌로 끝나기 때문[214]에 문제의 심각성은 더욱 커지고 있는 것이다. 특히 사이버도박의 경우 일반 도박에 비해 그 중독성과 피해규모가 매우 크다는 점을 고려해 볼 때 형법의 법정형이나 게임산업진흥에관한법률의 법정형을 조정하여 그 폐해를 감소시킬 수 있도록 하는 방안이 요구된다.

3. 정책상의 문제점과 개선방안

(1) 국제적 공조체제의 확립

인터넷의 공간적 무제약성으로 인해 한 국가에서 발생하는 컴퓨터범죄뿐만 아니라 국가간에 걸쳐 범죄가 발생하는 경우, 행위자를 특정하기 어렵고 행위자의 국적에 따라 또는 범죄행위지 또는 결과발생지를 기준으로 관할권에 관한 문제가 발생한다. 특히 도박과 음란물과 같이 해당국가의 단속을 피하기 위해 적법한 나라에 서버를 두고 서비스를 실행하는 추세가 보편화 되고 있다. 이와 같이 전세계 이용자를 대상으로 하는 상업적 음란물과 도박사이트들이나 외국에서의 해킹 등에 대하여 효율적으로 대처하기 위하여는 각국의 형법의 적용범위가 속인주의 · 속지주의 · 보호주의 여부에 따라 관할권이 달라지게된다. 또 관할권이 적용된다 하더라도 범죄인의 인도와 처벌에 대하여 국제적인 보호주의 원칙 등으로 해결할 수 있을 것이나 그러한 원칙이 적용되지 않는 경우에는 각국간의 조약이나 협조를 통해서만 가능한 경우가 있어 문제가 된다[215]. 이와 더불어 사이

214) 온라인 고스톱과 포카 등 이른바 `고포류` 게임을 둘러싼 논란이 국정감사 도마 위에 오른다.(중략) 이경재 의원실에 따르면, NHN 한게임은 고포류 게임 덕에 하루 평균 매출이 10억원을 넘어섰다. 올해 1분기 한게임 매출액 1164억원 중에 고포류 등 웹보드게임 비중은 88% 1024억원인 것으로 밝혀졌다.(중략) 반면 게임사를 탓할 게 아니라 사이버머니를 불법으로 환전해주는 불법 환전상들이 사행화를 조장한다는 시각도 있다. 지난 2008년 5월 경기지방경찰청 수사를 살펴보면, 검거된 불법환전상들의 경우 거래규모가 약850억원, 부당이익 규모가 45억원에 이르는 등 불법환전상을 통한 거래시장 규모는 대규모 시장으로 추정된다. 하지만 `2008범죄백서`에 따르면, 도박으로 단속돼 검찰송치된 경우는 연간 3만2000건에 이르는 반면, 불법환전으로 검찰송치된 경우는 연간 245건에 지나지 않는 것으로 나타났다. 이들 환전업자에 대한 처벌이 강화됐다고 하지만 대부분 재판과정에서 비교적 가벼운 벌금형으로 처벌을 받고 있는 것으로 알려졌다 ;이데일리, 2009.10.16.

215) 최영호, "개정형법과 컴퓨터관련 범죄현상(下)", 「법조」 478호, 법조협회, 1996, 67~68면;정상훈, 상게논문, 140~144면; 신현정, 전게논문, 76~77면.

버공간에서의 행위들에 대한 법적 구성요건이 국가마다 다르므로 구체적 상황들에 대해 국가마다 다른 시각이 존재할 경우 국가 간에 긴밀한 협력을 기대하기가 원칙적으로 어렵다. '국제형사사법조약' 및 '범죄인인도조약'이 체결된 상태라 하더라도 '자국민 불인도원칙', '정치범 불인도원칙'이 사이버범죄의 단속수사에도 그대로 적용되어 국제공조가 제한되는 원인으로 작용한다. 이와 같은 국제사회의 복잡성 · 국가간의 이해관계 등 여러 가지 복합요인에 의하여 국제공조수사 체계가 한계에 부딪히고 있다. 특히 외교부를 경유하여 국가간 형사사법공조관계를 통한 공조절차가 통상 1개월 이상의 기간이 소요되어 순식간에 범죄가 이루어지고 증거확보가 쉽지 않은 사이버범죄에 대한 신속한 대처가 어려운 현실이다. 현재 사이버범죄와 관련해 현존하는 다자간 국제협약은 '유럽평의회의 사이버 범죄조약'이다. 지난 2001년 완성된 이 조약에는 EU 회원국 등 47개국이 가입하고 있다. 이 조약은 국내법으로 반드시 규정해야할 사이버범죄 범위를 명확히 하고 수사시 갖춰야할 수사절차, 국제형사사법공조 절차를 규정, 사이버범죄 수사에 대한 모든 절차를 망라하고 있다. 이밖에 사이버범죄를 조직범죄의 한 유형으로 파악하고 일반규정을 적용하는 차원으로 'UN 반초국가조직범죄조약'이 있다. 이 조약은 대상국가가 190여국에 이르고 현재 가입 · 비준절차를 완료한 국가만도 147개국에 달해 유럽평의회 등에 가입돼 있지 않더라도 이 조약에 가입한 국가와의 공조에서 효용가치가 크다. 우리나라의 경우 유럽평의회에는 가입돼 있지 않고, UN 반초국가조직범죄 조약에는 가입했으나 비준절차가 남아 있어 사이버범죄 다자조약에 적극적이지 못한 실정이다[216]. 경제협력개발기구(OECD) 등이 우리나라의 형사사법공조제도 등을 검토해 내놓은 개선안 보고서는 긴급한 경우 공조요청을 이메일이나 팩스를 통해 할 수 있도록 한 다음 추후 정식 요청서를 접수하는 방식을 도입할 것을 권고하기도 했다. OECD는 또 다자간 조약가입과 양자조약 확대도 권고했다. 물론 법무부가 국제다자조약 가입국과 접촉하며 국내법 정비방안에 대한 논의를 거듭하고 있으며, 사이버 범죄에 관한 유일한 국제협약인 '유럽평의회(Council of Europe)' 가입절차도 검토하는 등 대응책 마련에 고심하고 있으나 하루라도 빨리 신속대응이 가능한 절차를 도입해 국제공조수사가 이루어질 수 있도록 해야 할 것이다. EU의 사이버범죄조약에서 제시하고

216) 인터넷법률신문, 2009.8.12.

있는 것과 같이 저장된 컴퓨터 자료의 신속한 보존, 저장된 컴퓨터 자료의 접속에 관한 공조, 저장된 자료의 초국경적 접속, 전송자료의 실시간 수집에 관한 공조, 콘텐츠자료의 감청에 관한 공조, 1주일 24시간 네트워크 24/7 Network구축 등의 조항은 전 세계가 사이버테러라는 초국경적 범죄에 공동으로 대응하기 위해 필수적으로 필요한 국제공조 수단들이므로 이에 대한 규정은 우리나라 법제도에도 반영되어야 할 것이다.

(2) 인터넷서비스제공자의 책임 및 P2P서비스의 규제 강화

인터넷을 통하여 발생되는 사이버범죄에 대한 효과적인 규율방안으로 논의되고 있는 것이 인터넷서비스제공자(ISP)의 책임이다. 또한 최근 음란물이나 불법복제물 유통의 근거지로 활성화 되고 있는 것이 P2P를 이용함으로써 이들 서비스제공자에 대한 책임을 강화시킬 필요가 있는 것이다. 특히 이들 인터넷서비스제공자는 접속계정의 부여와 통신망 이용의 매개자 역할을 하기 때문에 직접적이고 강력하게 ISP를 통한 규제가 필요하다. 대부분의 국가에서 ISP에 대한 일정한 책임을 규율하고 있지만 개별사안에 대하여 판례가 통일되지 못하고 있는 실정이다. 독일의 경우 1997년 7월 22일 '정보통신서비스법'을 제정하고 인터넷서비스제공자의 일정한 책임을 부과하고 있다. 따라서 불법 · 유해정보 유통과 관련한 사업자에 대한 명확한 책임규정을 마련하고 인터넷서비스제공자의 기술적 대응방안에 대하여도 그 책임을 명확하게 법제화 할 필요가 있다. 우리나라의 경우 2008년 7월 24일에 국회 진성호의원 대표발의로 국회에 접수된 법률[217] 중 불법복제물에 대한 강도 높은 대책을 마련하기 위하여 저작권법에 특수한 유형의 온라인서비스제공자에「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제9호의 게시판을 영리를 목적으로 운영하는 온라인서비스제공자를 추가

217) 제안이유:2007년 저작권침해방지 연차 보고서에 의하면 2006년 기준 P2P, 웹하드, UCC 및 포털 등 인터넷을 통해 국내에서 유통된 불법 복제 음악은 약 185억 4,413만곡, 영상은 총 114억 3,483만편, 출판물은 총 100억 456만편이 유통된 것으로 조사되었고, 이 같은 불법 복제물 유통과 이용에 지불된 금액은 음악과 영상부문에서만 약 2조 7천억원에 달하며, 피해금액은 약 2조 191억원으로 나타났음. 이처럼 인터넷상에서 상습적으로 발생하는 불법복제물의 유통을 포함한 불법 정보의 유통을 근절하기 위하여 정보통신서비스 제공자에게 정보통신망의 이용질서를 심각하게 훼손하는 불법 정보의 유통을 방치 또는 관리·운영하는 게시판 관리·운영자에 대하여 그 관리 및 운영의 정지 또는 해지를 명할 수 있는 규정을 신설하여 인터넷 이용자들에게 건전한 인터넷 문화를 향유할 수 있도록 하려는 것임.

(안 제104조제1항)하고, 저작권법 133조의 2[218]와 3[219]을 신설하여 P2P를 포함한 불법복제물을 유통하는 자와 온라인서비스제공자의 정보통신망의 관리 및 운영 정지와 시정조치에 대한 근거를 마련하였고 정보통신망법 제44조의 7 제4항[220]에 정보통신서비스제공자에 대한 책임 근거를 강화하는 것은 매우 바람직

---

218) 제133조의2(불법 복제물의 삭제 및 운영 정지 명령 등) ① 문화체육관광부장관은 정보통신망을 통하여 저작권 그 밖에 이 법에 따라 보호되는 권리를 침해하는 복제물, 저작권 등을 침해하는 정보를 제공하는 게시판 및 기술적 보호조치를 무력하게 하는 프로그램 등(이하 "불법복제물 등"이라 한다)이 전송 또는 제공되는 경우에 위원회의 심의를 거쳐 대통령령이 정하는 바에 따라 온라인서비스제공자에게 다음 각 호의 조치를 명할 수 있다.
1. 불법복제물 등의 복제·전송 및 정보 제공자에 대한 경고
2. 불법복제물 등의 삭제 또는 전송 및 정보 제공의 중단

② 문화체육관광부장관은 제1항제1호의 경고를 받은 복제·전송 및 정보 제공자가 3회 이상 반복적으로 불법복제물 등을 복제·전송 및 정보를 제공하는 경우에 위원회의 심의를 거쳐 대통령령으로 정하는 바에 따라 온라인서비스제공자에게 해당 복제·전송 및 정보 제공자의 계정(온라인서비스제공자가 이용자를 식별 관리하기 위하여 사용하는 이용권한 계좌를 말한다)을 정지 또는 해지할 것을 명할 수 있다. 이 경우 온라인서비스제공자는 해당 복제·전송 및 정보 제공자가 다른 계정의 신설을 허용하여서는 아니 된다.

③ 문화체육관광부장관은 온라인서비스제공자에게 정보통신망에 개설된 영리를 목적으로 운영하는 게시판(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제9호의 게시판을 말한다. 이하 같다) 중 제1항제2호의 명령이 3회 이상 내려진 게시판에 대하여 위원회의 심의를 거쳐 온라인서비스제공자에게 해당 게시판을 폐지할 것을 명할 수 있다.

④ 문화체육관광부장관은 온라인서비스제공자가 다음 각호의 어느 하나에 해당하고, 해당 서비스의 형태, 전송되는 복제물의 양이나 성격, 제공되는 정보의 침해 정도 등에 비추어 해당 서비스가 저작권 등의 이용질서를 심각하게 훼손한다고 판단되는 경우에는 위원회의 심의를 거쳐 대통령령으로 정하는 바에 따라 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호의 정보통신서비스 제공자를 말한다)에게 해당 온라인서비스제공자에 대한 관리·운영을 정지 또는 해지할 것을 명할 수 있다.

1. 제104조제1항에 따른 필요한 조치를 하지 아니하며 제142조제1항에 따른 과태료 처분을 2회 받고 다시 과태료 처분의 대상이 된 경우
2. 제1항제2호, 제2항 또는 제3항의 명령을 이행하지 아니하여 제142조제1항제2호에 따른 과태료 처분을 3회 받고 다시 명령의 대상이 된 경우

⑤ 온라인서비스제공자 또는 정보통신서비스제공자는 제1항부터 제4항까지의 규정에 따른 명령을 받은 경우에 명령을 받은 날부터 3일 이내에 그 조치 결과를 대통령령으로 정하는 바에 따라 문화체육관광부장관에게 통보하여야 한다.

⑥ 문화체육관광부장관은 제1항부터 제4항까지의 규정에 따른 명령 대상이 되는 온라인서비스제공자, 복제·전송 및 정보 제공자 또는 정보통신서비스제공자에게 처분 전에 의견 제출의 기회를 주어야 한다.

⑦「행정절차법」 제22조제4항부터 제6항까지 및 제27조의 규정은 제5항의 의견 제출에 관하여 이를 준용한다.

219) 제133조의3(시정 권고) ① 위원회는 불법복제물 등이 정보통신망을 통하여 복제·전송 또는 정보가 제공된 경우에 이를 심의하여 온라인서비스제공자에 대하여 다음 각 호에 해당하는 시정조치를 권고할 수 있다.

1. 불법복제물 등의 복제·전송 또는 정보 제공자에 대한 경고
2. 불법복제물 등의 삭제 또는 전송 및 정보 제공의 중단
3. 반복적으로 불법복제물 등을 복제·전송 및 정보를 제공하는 자의 계정 정지 또는 해지

② 온라인서비스제공자는 제1항에 따른 권고를 받은 경우에는 권고를 받은 날부터 3일 이내에 그 조치 결과를 위원회에 통보하여야 한다.

③ 위원회는 온라인서비스제공자가 제1항에 따른 권고에 따르지 아니하는 경우에는 문화체육관광부장관에게 제133조의2제1항 및 제2항에 따른 명령을 하여 줄 것을 요청할 수 있다.

④ 제3항에 따라 문화체육관광부장관이 제133조의2제1항 및 제2항에 따른 명령을 하는 경우에는 의견 제출의 기한을 두지 아니하고 위원회의 심의를 거쳐 처분할 수 있다.

220) 제44조의 7 제4항 신설; ④ 방송통신위원회는 제1항제1호부터 제7호까지의 정보에 대하여 정보통신망

한 일이라 할 것이다. 또한 영국과 같이 사이버공간의 이용자인 서비스제공자와 콘텐츠제공자 등에게 일정한 권한을 위임하고 그들로 하여금 일정한 자율통제권을 부여하여 운영자와 회원준수사항에 공동 가이드라인을 마련하고 상호협력 체계의 구축을 통한 사이버윤리의 자율적 강화가 이루어질 수 있도록 하는 것이 바람직하다고 할 것이다.

(3) 인터넷 실명제의 확대 실시

사이버공간의 익명성으로 인한 책임의식의 결여로 악성댓글, 명예훼손 등 사이버범죄가 증가하고 있다. 우리나라는 2005년 8월 4일 개정된 '공직선거법'에서 처음으로 인터넷 게시판에 글을 게시할 경우 실명을 확인받도록 법으로 규정하였는데, 이는 인터넷언론사가 선거운동기간 중 게시판, 대화방 등에서 정당 및 후보자에 대한 지지·반대 글을 게시할 경우 실명을 확인받도록 하는 기술적 조치를 취할 것을 명시한 것이다. 본격적인 본인확인제는 인터넷 익명성을 악용한 사이버 폭력 등 사이버 역기능을 방지하고자 2007년 7월부터 실시하였고 현재 정보통신망법 44조의 5(게시판이용자의 본인확인) 제1항에 의해 하루 이용자 10만명 이상의 정보통신서비스제공자와 공공기관 게시판 이용자의 경우 본인확인 조치를 시행하고 있다[221].

국회 입법조사처 현안보고서 제3호는 실명제와 관련하여 모든 인터넷 게시물에 실명을 입력하는 포괄적인 인터넷 실명제는 표현의 자유 침해라는 견해가 전반적으로 설득력이 있는 상황이며 '인터넷 본인확인제' 확대 실시에는 적용범위와 방식, 규제의 강도에 관한 보다 심층적인 논의가 있어야 한다고 밝히고 있다.

국회입법조사처 현안보고서의 자료에 따르면 외국의 경우에는, 중국을 제외하고는 OECD 회원국을 비롯한 해외 주요국에서는 인터넷 실명제와 같은 적극적인 게시판 이용 규제를 시행하고 있지 않다. 중국의 경우 거의 모든 분야에서 인터넷 실명제를 시행하고 있는데, 특히 대학 교육 네트워크에서 실명제를 강화하고

의 이용질서를 심각하게 훼손한다고 판단되는 경우에 심의위원회의 심의를 거쳐 정보통신서비스 제공자에게 해당 게시판 관리·운영자에 대한 관리·운영을 정지 또는 해지할 것을 명할 수 있다.

221) 2008년 현재 본인확인제 적용대상 사업자는 포털 16개, 인터넷언론 15개, UCC사업자 6개이다.

있으며, PC방 이용 시에도 반드시 신분증을 제시하고 실명을 등기하도록 하고 있다. 반면 미국의 경우 익명적 커뮤니케이션을 인정하는 사례들에서 볼 수 있듯이 익명표현의 자유를 소중하게 생각하며 실명제를 강제하는 법은 표현의 자유에 대한 제한으로 본다. 물론 익명에 의한 온라인 명예훼손 등에 소송을 제기할 수는 있지만 인터넷 실명제와 같은 적극적인 정책을 통해 사전에 규제하지는 않고 있다. 유럽연합의 경우는 인터넷 역기능에 대한 규제강도가 미국보다 강한 편으로 정부규제와 자율규제의 절충방식을 취하고 있는데, 인터넷 게시판에 대한 규제보다는 보편적인 안전한 인터넷 환경 구축과 불법 및 유해 콘텐츠에 대처하는 등의 정책을 지향하고 있다. 특히 개인정보보호와 프라이버시권 보장 등을 목적으로 EU회원국 간의 상이한 법체계를 정비하여 국가간 공조를 통해 온라인 명예훼손 등의 문제에 대응하고자 한다. 예를 들어, EU SIP(Safe Internet Plus)2005-2008은 핫라인, 필터링, 대중교육 부문을 지원하고 인터넷 역기능에 관한 캠페인을 전개하는 등 일반대중 및 민간영역의 적극적인 참여를 유도하고 있다. 그러나 미국을 비롯한 해외 주요국의 경우 비영리 뉴스그룹 등을 통해 주로 학술적 목적의 인터넷 토론문화가 있어 왔으며 최근 유투브, 구글 등을 중심으로 일부 게시판에서 댓글 사용이 늘어나는 추세이다. 또한 홈페이지 구축시 게시판 기능이 필수기능으로 포함되어 있지 않는 경우가 많으며 게시판 기능이 있는 경우에도 제한적으로 글쓰기를 허용하는 등 인터넷 게시판에서의 글쓰기와 댓글 달기가 우리나라처럼 대중화되지는 않은 상황이다. 인터넷 실명제 실시와 관련한 효과에 대해서는 논란의 여지가 많지만 학술적 목적이나 건전한 토론문화가 활성화 될 수 있는 게시판의 활용에서 실명제에 대한 논란은 그리 크지 않을 것이다. 가장 큰 문제가 되고 있는 것은 포털이나 개인 미니홈피에 대한 악성 댓글이다. 이미 싸이월드에서는 미니홈피의 댓글을 실명화하였으며, 지난 2009년 2월부터 SK커뮤니케이션즈는 기존의 포털인 네이트와 엠파스를 통합한 새로운 네이트를 서비스하면서 모든 뉴스서비스의 댓글작성자를 실명화하기로 하였다[222]. 물론 인터넷 실명제를 실시한다고 해서 악성댓글이 완전히 사라지는 것

222) SK커뮤니케이션즈(SK컴즈)가 인터넷 포털 업계에서 최초로 완전실명제를 시행한다. SK컴즈는 기존 인터넷 포털 네이트와 엠파스 콘텐츠를 통합한 새로운 '네이트'를 28일부터 공식 서비스한다고 25일 밝혔다. 이 회사는 네이트 뉴스서비스에서 댓글 작성자의 실명을 공개하기로 했다. 현재 모든 포털은 댓글 작성자의 ID만을 공개하는 제한적 본인확인제를 시행하고 있는데, 완전실명제 시행은 이번이 처음이다. SK

은 아니며, 분명히 기본권을 침해하는 요소가 있다. 하지만, 의사표현의 자유는 자신의 신상을 밝히느냐 밝히지 않느냐와는 별도 차원의 문제라고 생각한다. 인터넷 실명제가 심리적인 부담이 될 수는 있지만 의사표현의 자유의지를 침해하는 것은 아니며 오히려 자신의 실명이 공개되는 만큼 자신의 말에 그만큼 강한 의지와 책임을 포함시키는 효과가 있을 것으로 생각된다.

따라서 인터넷 실명제에 대한 적용범위와 방식, 그리고 규제의 강도에 대한 심층적인 분석을 통하여 사이버공간의 역기능에 대처할 수 있는 명확한 근거를 가지고 확대실시 되어야 할 것이며, 더불어 어린이나 청소년을 포함한 네티즌을 대상으로 건전한 사이버문화 형성을 위한 예방교육과 같은 정책적 방안이 병행되어야 할 것이다.

(4) 사이버범죄 대응조직의 강화

사이버범죄에 효과적으로 대응하기 위해서는 사이버범죄를 전담하는 부서의 조직과 위상을 강화시킬 필요가 있다. 또한 사이버범죄에 효과적으로 대응하기 위하여 컴퓨터와 정보통신기술에 능통한 고도의 전문지식과 기술을 가진 전문가들을 체계적으로 확보해야 한다. 더불어 날로 지능화 되고 있는 신종범죄에 대처하기 위한 전문지식과 컴퓨터 기술을 신속하게 습득하는 것은 물론 사이버범죄에 대한 인식을 바꿀 수 있는 교육과 연구를 강화시켜야 한다. 사이버범죄가 어느 한 분야에서만 발생하지 않으므로 경찰과 검찰, 국가정보원, 한국인터넷진흥원, 정보통신윤리위원회 등 사이버범죄와 관련된 여러 기관들이 유기적으로 협조할 수 있는 공조체제가 원활하게 이루어질 수 있는 방안이 마련되어야 할 것이다.

컴즈는 "'제한적 본인확인제'가 법적으로 문제가 되는 수준의 댓글을 규제하는 수단으로 작용했다면, 댓글 실명제는 토론 문화를 해치는 무의미한 '악플'(악성 댓글)을 제한해 악의적인 이슈 재생산을 막는 데 효과가 있을 것"이라고 설명했다; donga.com, 2009.2.26.

V. 결론

본 논문에서는 정보통신기술의 발달과 더불어 컴퓨터와 인터넷상에서 발생하고 있는 각종 범죄의 유형들을 사이버범죄의 개념으로 포섭하여 구분하고 정리하고 이에 따르는 국내 · 외의 법제도적 문제점과 개선방안을 고찰하였다. 종래의 전통적 범죄와는 달리 사이버범죄는 사이버공간상의 특성으로 인하여 기존의 법률체계의 대응으로는 한계가 있고 사이버범죄의 특성상 범죄의 발각과 입증이 쉽지 않고 수사와 처벌에 어려움이 존재하고 있다.

사이버범죄의 유형을 분류함에 있어 끊임없이 변화하고 새로운 형태가 나타나는 특성으로 인해 명확하게 분류하기는 어려우나, 사이버공간을 수단으로 하는 범죄의 특성을 고려하여 진정사이버범죄와 부진정사이버범죄로 분류하여 형법의 해석과 정책에서 사이버공간의 특성을 반드시 고려해야 하는 경우와 그렇지 않아도 되는 경우로 구별하였다. 진정사이버범죄는 사이버공간내에서만 가능한 범죄행위로서 해킹, 악성프로그램 및 바이러스 유포, 스팸메일 등이 이에 해당하고, 부진정사이버범죄는 사이버공간을 이용하는 범죄행위로서 전자상거래 사기, 불법복제, 사이버폭력, 사이버음란물 유포 등의 불법유해사이트, 개인정보침해, 사이버도박 등을 들 수 있다.

최근 들어 사이버범죄는 단순한 웜 · 바이러스는 감소하지만 금전적 목적의 악성코드 유포와 해킹으로 개인정보 유출 피해가 지속적으로 증가하고 조직적이고 지능화된 사회공학적 기법을 이용하여 그 양상 및 피해규모는 점점 증가하고 있는 실정이다. 오늘날 사이버범죄의 심각성은 현실공간에서의 범죄에 비하여 결코 덜하지 않으므로 사이버공간을 범죄로부터 보호하여야 한다는 점은 자명하다. 사이버공간을 이용하는 새로운 범죄의 대부분은 기존의 형벌법규가 전혀 예상하지 못한 불법적인 유형들이기 때문에 당연히 처벌에 있어 공백이 생길 수밖에 없다. 그리하여 세계 각국에서는 사이버범죄에 대처하기 위하여 새로운 처벌법규를 신설하거나 기존의 처벌법규를 보완하는 입법을 한 바 있다.

우리나라에서도 산업화 · 정보화의 추세에 따른 컴퓨터범죄 등의 신종범죄에 효율적으로 대응하기 위해 1995년 12월 형법개정을 통하여 컴퓨터관련 범죄를

형법으로 처벌할 수 있도록 하였으며, 2001년 12월 다시 형법의 일부를 재개정하여 1995년 당시 파악하지 못했던 '권한없이 정보를 입력 · 변경하여 정보처리를 하게 하는 행위양태'를 구성요건에 새로이 추가함으로써 법률의 흠결을 보완하였다. 사이버범죄에 대한 형사법적 규제는 형법뿐만 아니라 다양한 특별법에 의하여 이루어지고 있다. 사이버범죄를 특별법 중심으로 규제하게 된 이유는 사이버공간에서 나타나는 일탈행위에 신속하게 대응할 필요성이 있어서 그때그때마다 입법이 필요하다고 판단하여 이를 특별법으로 포섭하였다. 그리고 또한 사이버공간에서 발생하는 일탈행위와 관련하여 직접적으로 이해관계가 있다고 보여지는 정보통신망업체, 컴퓨터관련기관 그리고 이를 담당하는 정부기관들의 시각에 의하여 처벌의 유형과 대상 그리고 법정형들이 정해지고 이것이 형사규제로 입법화되었다. 그 결과 사이버범죄의 처벌과 관련하여 형법의 일반원리와 당벌성 그리고 다른 범죄들과의 형평성 등의 내용들이 구체적으로 고려되기 보다는 신속한 형사법적 대응이 필요하다는 점과 발생하는 법익침해가 막대하다는 점만이 전면에 등장하였다. 또한 검찰과 경찰에서도 사이버범죄 전담수사팀을 설치하여 사이버범죄에 대처하고 있다. 그러나 정부의 이러한 법적 · 제도적인 조치에도 불구하고 사이버범죄의 발생빈도는 높아지고 있다. 그 이유는 사이버범죄 그 자체가 교묘하게 이루어지고 있을 뿐만 아니라 점차 다양화되고 있지만 그에 대한 예방 및 규제대책이 제대로 뒤따르지 못하고 있기 때문이다.

따라서 형법과 정보통신망법을 비롯한 법률에 처벌규정을 보완(신설 또는 개정)한 것은 적절하다고 할 것이다. 그러나 특별법은 일반형법에 비해 법률제정이 덜 엄격함으로써 졸속으로 제정될 위험이 높고, 특별법의 대부분이 긴급조치의 목적으로 제정됨으로써, 과잉범죄와와 과잉형벌화, 법률제정상 남용과 졸속의 문제, 법률형식상의 법률효과의 불명확성과 법률명칭의 비통일성, 범죄의 실효성 등 많은 문제점을 가지고 있다. 이는 특별법의 성격상 형법 및 형사소송법의 일반원칙이 배제된다는 근본 문제점을 지적할 수 있으며, 이로부터 특별법의 규정들은 일반 형법에 비해, 손쉽게 개정되고 폐지될 가능성이 높아 특별법에 규정된 사이버범죄 제재조치는 불완전하고 불안정한 지위를 가질 수밖에 없다. 최근 일부에서는 '정보형법'과 '사이버범죄특별법' 등이 거론되고 있는데 새로운 법을 제정하기 보다는 산재되어 있는 여러 특별법들을 사이버범죄의 큰 맥락으로 묶어

관리할 수 있는 체계가 필요하다는데 공감한다. 따라서 외국과 같이 충분한 기본 법률의 제정비로 새로운 범죄현상에 대응하는 체계가 필요하리라 생각된다.

미국의 경우처럼 컴퓨터범죄에 대해서는 혁신적인 법집행기술을 요구하면서 계속 출현하고 있는 기술의 남용에 대처할 수 있도록 고안된 새로운 법률의 요구에 의해 1984년 연방법에 컴퓨터사기 및 부정이용에 관한 법을 제정하여 기본법규로 삼고 이를 수차례 개정하며 인터넷 관련 범죄들에 적극적으로 대처할 필요가 있는 것이다.

해킹과 같은 범죄는 국가기반 정보통신망의 안전성을 해할 수 있는 위험이 있으므로 단순해킹이나 바이러스 제작 · 유포와 같은 범죄행위는 형법전에 미수범의 처벌규정을 신설하는 것이 바람직할 것으로 생각된다. 특히 사이버범죄 중에서도 이미 형법에 그 처벌규정이 마련되어 있고 우리 사회에서 일반화된 범죄행위가 된 명예훼손이나 음란물 유포 같은 경우에는 형법전으로 편입시키고 그 피해의 규모나 중독성 · 파급효과 등 사회적 유해성이 매우 큰 인터넷을 이용한 도박은 형법이나 게임산업진흥에관한법률의 처벌규정을 상향조정하여 처벌을 강화시킬 필요가 있으며, 기존의 특별법에 중복 규정되어 있는 처벌법규들은 해당행위에 대한 처벌의 정도를 다른 범죄들과 비교 · 검토함으로써 일관화하여 처벌범위에 대한 정당성을 획득하고 체계 및 형평성을 유지하여야 하는 것이 타당하다고 생각된다. 이와 더불어 인터넷을 통한 불법 · 유해정보의 유통과 관련하여 인터넷서비스제공자나 P2P서비스의 규제를 강화해야 할 필요가 있으며, 논란의 여지는 있으나 무의미한 악성댓글이나 명예훼손 등을 감소시키고자 하는 방안으로 인터넷 실명제의 확대실시를 적극 검토해 보아야 할 것이다.

정보대국인 미국의 경우에는 법무성 산하에 사이버범죄대책반(컴퓨터범죄 및 지적재산권 담당국:Computer Crime and Intellectual Property Section -CCIPS)을 구성, 종합보고서를 제출하고 있으며, 그 실천을 위한 입법과정에 들어가 있는가 하면, 일본의 경우에는 기존의 형법규정의 확대해석 내지는 유추해석의 가능성까지도 심각하게 고려하고 있는 실정이다. 뿐만 아니라, 유럽의 경우에는 아예 일정한 범위 내에서 정보통신서비스제공자의 편집권을 인정하면서 그에 대한 법적 책임을 추궁할 수 있는 여지를 부여하는 형태로 사이버범죄의 유통을 차단하는 장치를 실시하고 있다.

우리나라도 외국의 다양한 입법례를 고려하여 한국적 현실과 관련하여 그 적실성을 추구해야 할 것이다. 그 외에도 IT환경이 무선인터넷 중심으로 변화하고 모바일에 이러한 인터넷 기능이 확장되면서 모바일 관련 범죄가 빠르게 진행하고 있다. 이러한 의미에서 장래의 사이버범죄는 모바일범죄로 변화될 것이며, 이를 포괄적으로 수용할 수 있어야 할 것이다. 또한 건전한 사이버문화 조성을 위한 예방적 차원의 윤리교육을 의무화하고 사이버범죄를 사전에 예방할 수 있는 제도와 재범방지를 위한 효과적인 제재수단을 연구·개발하여야 할 것이다.

참고문헌

<단행본>

강동범, 「컴퓨터범죄시론」, 경진사, 1989.

박상기, 「형법각론」, 박영사, 2008

배종대, 「형법각론(제6전정판)」, 홍문사, 2006.

이철, 「컴퓨터범죄와 소프트웨어보호」, 박영사, 1995.

정영일, 「형법각론」, 박영사, 2006.

최영호, 「컴퓨터와 범죄현상」, 컴퓨터출판사, 1995.

<논문>

강동범, “컴퓨터범죄와 개정형법”, 「법조」 491호, 법조협회, 1997.

강동범, “사이버범죄와 형사법적 대책”, 「형사정책연구」 제11권 제2호, 한국형사정책연구원, 2000.

강동범, “사이버범죄 처벌규정의 문제점과 대책”, 「형사정책」 제19권 제2호, 한국형사정책학회, 2007.12.

김수정, “지식정보사회에서의 사이버범죄”, 「교정복지연구」 창간호, 한국교정복지학회, 2005

김종세, “사이버범죄의 법적 쟁점에 관한 고찰”, 「경찰연구논집」 제2호, 한국경찰이론과 실무학회, 2008.

김종섭, “사이버범죄의 현황과 대책”, 「형사정책」 제12권 제1호, 한국형사정책학회, 2000.

김형준, “사이버범죄와 현행 형법의 대응”, 「인터넷법률」 제10호, 법무부, 2002.1.

김희준, “사이버범죄의 개념과 대응방안”, 「해외연수검사연구논문집」 제18집, 법무연수원, 2003.

남재도, “중국내 사이버범죄 실태 및 한중간 효과적인 공조방안 연구”, 행정안전부 교육훈련정보센터 국외훈련보고서, 2009,

박성택, “사이버 범죄의 현황과 대응방안”, 영남대학교 행정대학원 석사학위논문, 2004.8.

박혜진, “사이버모욕죄 도입에 대한 비판적 검토”, 「안암법학」28호, 안암법학회, 2009.

백광훈, “인터넷을 이용한 범죄의 유형과 처벌법규”, 2003년 한국범죄방지재단 세미나 자료집, 한국범죄방지재단, 2003.

백광훈, “사이버스토킹과 그 처벌법규 및 문제점”, 사이버범죄연구회 제17회 세미나 발표자료, 2001.6.2.

백광훈, “정보통신범죄의 개념과 유형 및 분류”, 사이버범죄연구회 제23회 세미나 발표자료, 2001.10.13.

신현정, “사이버범죄에 관한 고찰”, 서강대학교 공공정책대학원 석사학위논문, 2005. 6.

양근원, “사이버범죄 현황과 대책”, 「21세기 도전과 사이버스페이스」, 사이버커뮤니케이션학회 ‘99추계학술대회 자료집, 1999.11.

양근원, 「사이버테러의 실태와 법적 대응에 관한 연구」, 경희대학교 국제법무대학원 석사학위 논문, 2003.8.

양근원 · 임종인, “사이버범죄분석과 법률적 대응방안”, 「과학사상」 통권49호, 범양사, 2004.

오영근, “인터넷범죄에 관한 연구”, 「형사정책연구」제14권 제2호, 한국형사정책연구원, 2003 여름호.

우제태, “사이버범죄의 대응방안에 관한 연구”, 「경찰연구논집」제1호, 한국경찰이론과 실무학회, 2007.

유석준, “사이버범죄에 대한 외국의 입법례”, 「영산법률논집」 제15권 제1호, 영산대학교 법률연구원, 2008.9.

윤동호, “사이버공간에서 관세법의 금지품수출입죄의 해석과 정책”, 「법조」 통권639호, 법조협회, 2009.12.

이수현, “인터넷범죄의 실태와 대응방안”, 「법학논고」 제25집, 경북대학교 법학연구소, 2006. 12.

이정훈, “사이버범죄에 관한 입법동향과 전망”, 「사이버커뮤니케이션학보」통권

제20호, 사이버커뮤니케이션학회, 2006.4.
이천현, “사이버범죄의 개념-일반적 개념정의에 대한 비판적 관점에서”, 사이버범죄연구회 제18회 세미나, 2001. 6.16.
원혜욱, “인터넷범죄의 특징과 범죄유형별 처벌조항”, 「형사정책연구」 제11권 제2호, 한국형사정책연구원, 2000 여름호.
장영민 · 조영관, 「컴퓨터범죄에 관한 연구」, 한국형사정책연구원, 1993.
전지연, “사이버범죄의 과거, 현재 그리고 미래”, 「형사법연구」 제19권 제3호, 한국형사법학회, 2007 가을호.
정상훈, 「사이버범죄에 관한 연구」, 공주대학교 대학원 석사학위논문, 2007.2.
정완, “사이버범죄의 주요동향과 형사정책적 과제”, 「형사정책연구」 제18권 제3호, 한국형사정책연구원, 2007 가을호.
정완, “사이버범죄의 실태와 동향 및 대응책”, 「홍익법학」 제10권 제1호, 홍익대학교 법학연구소, 2009.
정재봉, 「사이버 범죄의 실태와 대책에 관한 연구」, 원광대학교 행정대학원 석사학위논문, 2007.10.
조병인, “하이테크범죄의 실태와 대책”, 한국공안행정학회 국제범죄 학술세미나 발표논문, 1999.9.17.
조병인·정진수·정완·탁희성, 「사이버범죄에 관한 연구」, 한국형사정책연구원 연구보고서, 2000.
조성택, “사이버 범죄의 규제에 관한 연구:사이버 음란물을 중심으로”, 「한국지역정보화학회지」 제9권 제2호, 한국지역정보화학회, 2006.12.
최정호, “일반 사이버범죄 법규의 문제점”, 「경찰법연구」 제6권 제2호, 한국경찰법학회, 2008.
최영호, “개정형법과 컴퓨터관련 범죄현상(下)”, 「법조」 478호, 법조협회, 1996.
허만영 · 홍진표, 「사이버스페이스의 범죄현황과 경찰의 대응방안」, 치안정책연구소 연구보고서, 치안정책연구소, 2005.
허일태, “사이버 범죄의 현황과 대책”, 「동아법학」 제27호, 동아대학교 법학연구소, 2000.

홍승희, “정보통신범죄의 전망”, 「형사정책」 제19권 제1호, 한국형사정책학회, 2007.

홍승희, “유비쿼터스환경과 사이버범죄”, 「형사정책연구」 제17권 제3호, 한국형사정책연구원, 2006 가을호.

<기타>

경찰청, 「2009 경찰백서」.

국가정보원, 「2003 국가정보보호백서」.

국가정보원, 「2005 국가정보보호백서」.

국가정보원, 「2006 국가정보보호백서」.

국가정보원, 「2007 국가정보보호백서」.

국가정보원, 「2008 국가정보보호백서」.

국가정보원, 「2009 국가정보보호백서」.

법무부, http://www.moj.go.kr

http://www.cybercrime.gov/

Convention on Cybercrime, http://www.iwar.org.uk/law/resources/eu/cybercrime-final-notes.htm

Weiser, M., http://www.ubiq.com/weiser

한국인터넷진흥원 인터넷통계정보시스템 참조 http://isis.nic.or.kr

경찰청 사이버테러대응센터 http://www.ctrc.go.kr

대검찰청 첨단수사과 인터넷범죄수사센터 http://www.spo.go.kr

ABSTRACT

A Study on Cyber Crimes

Eun-Ju Lee
Department of Law
Graduate School
Jeju National University

Modern society, called the Information Society, is changing at too high speed based on high information technologies to predict our future, and cyber space keeps expanding further and it is being given a great deal of weight in the information era, accordingly.

This study aims to describe the development progress of computer crimes and cyber crimes under the title, 'Cyber Crimes'. It also examines the general idea of computers, which is a major object of computer crimes, and its meaning in the criminal context and considers cyber crime as a comprehensive criminal act that is constituted in cyber space.

The characteristics of cyber space are anonymity, non face-to-face communication and those of cyber crime are the seriousness of infringement of people's rights, a lack of feeling guilty, crimes of deception, high frequency of criminals and complicity in crimes.

There are a lot of theories of the classification criteria of cyber crimes and it is found difficult to firmly establish them. This study classifies cyber crimes into the essential type crime and unessential cyber crime by the media of cyber space . Essential cyber type refers to possible within the cyber space itself such as hacking, malwares distribution, spam-mail and Denial-of-Service attacks. On the other hand, unessential cyber crime refers to crime that uses cyber space as a tool, for example Internet auction fraud, piracy, service of illegal contents, defamation, cyber stalking, cyber gambling, exchange of prohibited product, etc.

This paper lays a finger on problems with countermeasures for the current controversial cyber crimes and punitive regulations in force in current legal system by conducting an analysis of other countries' lawmaking cases and countermeasures, and suggests better solution for cyber crimes.

The government adopted a special law to correspond to the adverse effect of the public Internet use from the middle of 1990's, instead of applying criminal law.

Legislation that criminalizes certain acts thus is commonly applied to cyber criminals by police as follows :

- Criminal Act
- Act on Promotion of Information and Communications Utilization and Information Protection, etc.
- Information Communication Infrastructure Protection Act
- Protection of Communications Secrets Act
- Framework Act on Telecommunications
- Telecommunications Business Act
- Location Information Protection Act
- Copyright Act
- Radio Waves Act
- Digital Signature Act
- Computer Programs Protection Act

By this government's countermeasures, some problems such as penalty unbalance among several laws, legal system inconsistency, and similar rules dispersed in many special laws occurred.

As it is shown in the American and Germany legal system where cyber crimes are being addressed in the positive manner regarding the application of a criminal law in countries, it is found that they are trying to make a practical study on the means best suited for their system and public order by applying the existing laws to cyber crimes extensively.

In conclusion, this study summarizes the improvement plans for the regulations of criminal laws and special laws by types of cyber crimes, and strengthening internet service provider's liability, promoting cooperation between the administrative machinery and puts an emphasis on the necessity of voluntary control, an indirect regulation of cyber crimes.