연구보고서 2004-20

인터넷을 이용한 청소년범죄의 효율적인 대처방안 연구

≪硏 究 陣≫

연 구 위 원	:이 민 식	(경기대학교 사회과학부 교수)
연 구 실 장	:김 윤 철	(총 경)
연 구 관	:백 창 현	(경 감)

목 차

표 목 차

그 림 목 차

제1장 서 론

제1절 연구의 목적

컴퓨터와 정보통신기술의 발달과 함께 사이버공간을 무대로 하는 범죄와 일탈이 급속히 증가하고 있다. 현실세계에서 일어나는 유형의 범죄와 일탈은 물론이고, 많은 새로운 유형의 범죄와 일탈이 인터넷 기술이 조성하는 가상공간에서 발생하고 있다. 사이버공간은 익명성, 자율성, 개방성, 혹은 탈공간구속성 등으로 특징지어지는 사회적 공간으로서 우리에게 무한한 가능성을 열어주는 새롭고 경이로운 세계이기도 하지만, 그러한 긍정적 특성들도 새로운 생활공간에 적합한 새로운 행동규범과 준법의식이 제때에 형성되지 못할 때는 도리어 범죄와 일탈에 유리한 장을 마련해 주고 범죄와 일탈의 기회를 높여주는 유해한 환경이 될 수 있다.

한국인터넷정보센터(KRNIC)의 최근(2004) 자료에 의하면, 2003년 12월 현재 전체 2,922만명의 인터넷 사용자의 약 37%가 20세 미만의 미성년자[1]이고, 미성년자의 인터넷 사용률은 94.8%로서 94.5%를 나타낸 20대와 함께 타 연령대에 비해 월등히 높은 비율을 보였으며,[2] 더구나 그러한 추세는 앞으로 더욱 심화될 것으로 추정되었다. 이와 같은 청소년 인터넷 사용자의 급속한 증가는 그에 비례하여 청소년들에 의한 사이버범죄의 폭증이라는 예기된 결과를 가져왔다. 더구나 사이버공간에서의 청소년 문제행동은 그 양적인 증가추세와 함께, 최근에는 매우 다양화되었으며 질적으로도 심각한 수준에 이르러 큰 사회문제가 되고 있다.

물론 청소년들에 의한 사이버범죄는 청소년기가 갖는 발달과정상의 특성과 인터넷 사용행태의 특수성[3]을 반영하듯 성인들에 의한 사이버범죄와는 다소 다른 양상을 보이는

---

1) 한국인터넷정보센터(http://www.nic.or.kr)에서는 2001년 12월의 통계자료까지는 인터넷을 이용하는 미성년자의 연령을 7~19세로 집계하였으나, 2002년부터는 인터넷 이용자층이 점차 확대되는 경향을 반영하여 취학 가능 연령인 6세부터 19세로 확대하였다.

2) 본 수치는 한국인터넷정보센터의 통계자료를 바탕으로 재구성한 것임.

3) 한국인터넷정보센터의 자료에 의하면 연령대별로 주된 인터넷 이용목적이 상이함을 알 수 있다. 예컨대, '자료/정보 검색'은 20대 이상이 목적으로 하는 경우가 많고, '이메일'은 20대가, '게임'은 19세 미만이, '쇼핑/예약'

것이 사실이다. 청소년들은 신체적 발달에 비해 정신적으로 성숙하지 못하고 감정통제가 부족하여 충동적이며 가상공간에 난무하는 각종 유해정보 및 자극으로부터 영향을 받기 쉽다. 특히 청소년들은 사이버범죄의 범죄성에 대한 인식이나 죄의식이 부족하며, 심지어 해커와 같은 사이버 범죄자에 대해서는 기성체제에 저항하는 낭만적 영웅으로 묘사하는 등, 막연한 동경심까지 가지는 경우도 있다. 흔히 볼 수 있는 청소년 사이버범죄 유형들로는 사이버성폭력(사이버성희롱, 사이버스토킹, 성차별적·성적대적 언어폭력, 음란물 불법송신 등), 사이버성매매, 사이버명예훼손·협박, 사이버이지매, (온라인게임 관련) 사이버절도, 해킹, 타인의 ID나 개인정보 도용, 자살선동 등이 있다. 이와 같이 청소년들에 의한 사이버범죄는 우선 그 동기와 원인이 다르고 범죄유형도 다르기 때문에 그것에 대한 대응해법 또한 성인들의 경우와는 달라야 한다고 본다.

본 연구는 우리 사회에서 나날이 심각도가 더해가고 있는 청소년 사이버범죄[4]에 대한 보다 근본적이고 체계적인 대응책이 절실하다는 현실적·정책적 이유에서 계획되었다. 요컨대 본 연구는 인터넷공간에서 발생하는 청소년범죄의 개별적 유형과 실태를 파악하고 그에 대한 종합적이며 효율적인 예방대책을 수립하는 것을 목적으로 한다.

제2절 연구의 범위와 방법

1. 연구범위

다음 각 장에서 다루게 될 주제들의 개괄적인 내용 및 범위는 다음과 같다.

먼저, 제2장은 사이버범죄의 원인론(etiology)을 다룬다. 흔히 사이버범죄의 원인으로는 현실공간과는 다른 가상공간이 갖는 특수성(예컨대, 가상공간은 익명성, 자율성, 개방성, 혹은 탈공간구속성 등을 특징으로 한다)이 지적되곤 한다. 물론 사이버범죄의 상당 부분은

은 20대 이상이, '오락'은 20대 미만이 각각 다른 연령층에 비해 상대적으로 많은 것으로 나타났다. 또한 '신문/뉴스/잡지'는 30대 이상이, '채팅'은 6~19세가, '인터넷 뱅킹'은 30대 이상이, '동호회' 활동은 20대가, '학습'은 19세 미만이 목적으로 하는 경우가 각각 다른 연령층에 비해 높게 나타났다(2002 한국인터넷통계집).

4) 이하에서는 '청소년 사이버범죄'란 '청소년들이 범하는 사이버범죄'를 지칭하는 용어로 사용한다.

이러한 사이버공간이 갖는 특수성에 의해서 설명될 수 있을 것이다. 그러나 그러한 설명은 범죄사건을 범죄자의 의지, 범행의 기회, 또는 범죄자와 피해자간의 역동적인 상호작용의 결과로 보는 시각, 즉 전통적인 범죄학 이론의 입장에서는 불만스러울 것이다. 따라서 본 연구에서는 사이버범죄의 발생을 사이버공간이 갖는 특수성으로 설명함과 동시에, 기존의 범죄학 및 피해자학 이론의 틀 속에서 함께 설명하고자 한다. 나아가 이러한 작업에서는 청소년들이 갖는 특성(예컨대, 인터넷 중독)이 사이버범죄의 유발에 어떠한 함의를 갖는지도 성찰의 대상이 될 것이다.

제3장에서는 사이버범죄의 유형론(typology) 및 유형별 실태의 문제를 다룬다. 최근에 사이버범죄는 양적 폭증과 함께 그 유형도 지극히 다양하여 지금도 새로운 형태의 사이버범죄가 속속 등장하고 있는 실정이다. 따라서 그처럼 다양한 사이버범죄를 누구나 공감할 수 있도록 합리적으로 분류하는 것은 결코 쉬운 일이 아니지만, 이 장에서는 논의의 편리상, 기존의 문헌에서 발견되는 몇 가지 사이버범죄 유형론을 소개하고, 그러한 유형분류 방식에 따라 공식, 비공식 통계자료 및 각종 매스컴 자료를 활용하여 사이버범죄의 실태와 사례를 살펴보기로 한다.

제4장은 현행 사이버범죄 예방·규제전략과 현황의 문제를 다룬다. 사이버범죄를 예방하고 규제하기 위한 우리사회의 활동은 다양한 주체에 의하여 이루어져 왔다. 우선 정부부문에서는 급속히 확산되고 있는 사이버범죄에 능동적으로 대처하기 위해 새로운 조직을 신설하거나 개편·확장해 왔으며, 여러 곳에 분산되어 있는 다양한 사이버범죄관련 법규들을 정비하는 노력을 해왔다. 경찰 및 검찰 등 국가형사사법기관들은 사이버범죄자의 수사 및 검거에 만전을 기해왔으며, 국가정보원, 정보통신윤리위원회, 한국정보보호진흥원 등 정보(화)관련 공공기관들은 독자적인 또는 공동의 대응을 통하여 형사사법기관의 활동을 지원해 왔다. 또한 민간부문에서는 각종 정보통신사업자 단체의 자체정화 활동과 한국사이버감시단, 한국청소년문화연구소, 학부모정보감시단, 각종 언론·사회단체의 클린인터넷 운동 등이 이어져왔다. 이 장은 그와 같은 다양한 현행 사이버범죄 예방·규제전략과 현황을 소개하기 위한 것이다.

제5장은 제4장에서 살펴 본 현행 사이버범죄 규제전략이 갖는 문제점이 무엇인지를 성찰적으로 검토하기 위한 것이다. 본 연구에서는 그러한 문제점을 크게 법적·제도적 미비점, 문제의 심각성에 대한 사회적 인식의 부족, 형사사법기관의 대응능력 부족, 총괄적

조정기관의 부족 등의 제하에 다루고자 한다.

제6장에서는 앞장에서 발견한 문제점들을 기초로 청소년 사이버범죄에 대한 효율적인 대처방안을 모색해 보고자 한다. 구체적으로는 규제법규 및 제도를 보완·정비하는 문제, 형사사법기관과 기타 공공기관의 역할의 강화, 사업자단체 및 민간의 사이버범죄 예방을 위한 자체 역량의 강화 등의 주제들을 중심으로 이 문제에 접근해 보고자 한다. 또한 이 장에서는 사이버범죄에 대한 경찰의 대응능력을 강화하고 사이버경찰을 지속적으로 발전시키기 위한 과제가 무엇인지 생각해 보는 기회도 가질 것이다.

마지막장은 사이버범죄를 예방하고 통제하기 위한 다양한 주체들의 노력을 총괄적으로 조정하기 위해 현재 우리 사회에서 이루어지고 있는 논의들을 소개하고 그러한 대책들이 실효성을 발휘할 수 있도록 하기 위해서는 어떠한 조처들이 필요할 것인지 생각해 보는 시간을 갖고자 한다.

2. 연구방법

본 연구는 청소년 사이버범죄의 원인과 실태를 진단하고 그에 대한 효율적인 대응방안을 모색하는 것을 목적으로 한다.

우선, 청소년 사이버범죄의 원인과 실태를 파악하고 현행 사이버범죄 예방·규제 전략의 현황을 개괄하기 위해서, 본 연구는 사이버범죄의 원인론에 관한 문헌을 분석하고 사이버범죄 관련 정부 및 민간 기관 - 경찰청(사이버테러대응센터 및 사이버범죄수사대), 대검찰청(인터넷범죄수사센터), 정보통신윤리위원회, 한국정보보호진흥원, 한국정보문화진흥원, 국가정보원, 한국인터넷정보센터, 청소년보호위원회, 한국형사정책연구원, 한국청소년개발원, 자녀안심운동 서울협의회, 사단법인 한국사이버감시단 등 - 으로부터의 공식통계 및 각종 유관 자료들을 분석할 것이다.

둘째는, 이러한 원인과 실태에 대한 분석을 토대로 현행 사이버범죄 규제전략이 갖는 문제점을 도출하고 청소년 사이버범죄에 대한 효율적인 대응방안을 모색하기 위해 외국의 사례에 대한 검토를 포함하여 관련 정부 및 민간기관의 전문가·실무가들로부터 폭넓은 자문을 구할 예정이다. 이러한 과정은 청소년 사이버범죄 문제에 대한 보다 효율적이고 현실성 있는 정책의 입안을 가능케 할 것으로 생각한다.

3. 기대효과 및 활용

본 연구를 통해 기대되는 효과는 다음과 같다.

첫째, 다양한 사이버범죄 중에서 특별히 청소년들에 의해서 유발되는 사이버범죄의 유형화와 원인론적 분석을 행함으로써 청소년 사이버범죄에 적합한 대응책 마련에 기여한다.

둘째, 가상공간에서의 청소년범죄를 포함하여 사이버범죄 일반에 대한 예방대책 자료로 활용될 수 있을 것이다.

제2장 사이버범죄의 원인론

제1절 사이버범죄의 개념 및 특성

1. 사이버범죄의 개념

오늘날 '가상'이라는 의미를 갖는 접두어로 사용되고 있는 '사이버(Cyber)'는 인공두뇌학으로 번역되는 '사이버네틱스(Cybernetics)'라는 용어의 줄임말이다. 80년대 중반 이후 이른바 가상현실 산업이 형성되고 '사이버네틱스'라는 용어를 상업적으로 사용하면서 인공두뇌학이라는 기술적 의미는 퇴색하고 대신 줄임말인 '사이버'가 '가상'이라는 의미를 지니게 되었다. 따라서 사이버공간(Cyberspace)이라 함은 인터넷으로 대표되는 컴퓨터 통신망, 나아가 통신망 상의 가상공간을 지칭하며, 사이버범죄란 간단히 이러한 '가상공간에서 발생하는 범죄'를 의미한다.

사이버공간에서 발생하는 범죄를 지칭하기 위해서 컴퓨터범죄(computer crime), 정보통신범죄(information & communication crime), 하이테크범죄(high-tech crime), 디지털범죄(digital crime), 인터넷범죄(internet crime), 온라인범죄(online crime) 등 다양한 용어들이 사용되어 왔다. 그러나 컴퓨터범죄는 독립적인 컴퓨터 시스템에 중점을 둔 용어로서, 인터넷이 보편화된 작금의 상황에서는 핵심적인 범죄현상을 파악하는데 무리가 있으며, 정보통신범죄 역시 컴퓨터범죄와 유사한 외연을 갖는다. 하이테크범죄는 고도의 과학기술이나 첨단기술을 이용한 범죄현상을 의미하므로 사이버공간에서의 범죄만을 내포하는 것이 아니다(강동범, 2000:69). 디지털범죄는 소위 아날로그범죄와 대비될 수 있으며, 디지털 기기나 기술을 이용한 범죄이고, 인터넷범죄는 인터넷을 매개로 하거나 그 자체를 대상으로 하는 범죄이다. 또한 온라인범죄는 오프라인범죄에 대비될 수 있는 범죄로서 이 역시 유용하게 사용된다.[5] 이처럼 각각의 용어들은 나름대로의 유용성을

5) 컴퓨터범죄, 정보통신범죄, 하이테크범죄, 디지털범죄는 다소 기술적, 하드웨어적 색채가 강한 용어인데 비해, 인터넷범죄, 온라인범죄, 사이버범죄는 소프트웨어적 색채가 강하며, 범죄의 새로운 발생공간인 가상공간(cyber space)을 강조한 용어로서 평가된다.

가지나, 최근에는 사이버범죄(cybercrime 또는 crime in the cyberspace)라는 용어가 가장 보편적으로 사용되고 있다.

최근에 Parker(1998 : 72)는 사이버범죄를 “사이버공간에 대한 특별한 지식을 이용한 범죄”라고 다소 모호하게 정의하였다. 사실 그는 사이버범죄를 단지 사이버공간이라는 새로운 도구와 목표를 사용하는, 즉 새로운 환경 속에서 발생한다는 점만 제외하면 현실세계에서 발생하는 범죄들과 본질적으로 다를 바 없는 것으로 보았다. Thomas와 Loader(2000 : 3)는 사이버범죄를 “컴퓨터와 (전지구적인) 전자 네트워크를 매개로 한 불법적이거나 불법적인 것으로 간주될 수 있는 행위 또는 활동”으로 정의하였다. 강동범(2000:69) 역시 사이버범죄를 “컴퓨터범죄를 포함하여 사이버공간에서 행하여지는 모든 범죄적 현상”을 의미하는 것으로 광의의 정의를 사용하였다. 그러나 본 연구에서는 인터넷을 매개로 하거나 그 자체를 대상으로 하는 범죄에 초점을 두어, 사이버 범죄를 ‘인터넷 사이트와 그것들을 서로 연계시키는 컴퓨터 네트워크를 수단으로 하여 특정 네티즌이나 사이트, 또는 네트워크 그 자체를 대상으로 하는 범죄를 총칭하는 개념’으로 규정하고자 한다.

본 연구는 청소년 인터넷 사용자들이 경험할 수 있는 다양한 유형의 사이버 범죄 및 일탈을 포괄적으로 다루며, 그러한 유형들 가운데는 실정법상 범죄로서 처벌받지 않는 보다 가벼운 유형의 일탈행위까지도 포함되어 있다. 그러나 이후부터는 독자들에게 혼란을 줄 수 있는 가능성을 배제하기 위하여 그와 같은 비교적 가벼운 일탈유형까지도 포괄하여 사이버범죄라는 용어로 통칭하고자 한다.

2. 사이버범죄의 특성

사이버범죄가 갖는 특성에 대한 이해는 가상공간의 특수성에 관한 지식과 함께 사이버범죄 발생원인의 파악에 도움이 될 수 있다. 사이버범죄의 특징을 조병인(1999)은 특히 그것의 수사상 난점과 관련하여 다음과 같이 정리하였다.

첫째, 사이버범죄의 경우 범행의 주체를 밝히기 곤란한 경우가 많다. 인터넷 실명제를 의무화하여도 다른 사람의 ID와 패스워드를 도용하여 범행을 저지르는 경우는 이용자의 신분을 알아낼 방법이 별로 없다. 해외에서 가명으로 국내사이트에 접속하여 범법행위를

하는 경우는 더 말할 나위가 없다.

둘째, 범행현장이 별도로 존재하지 않는다. 금융기관의 전산망에 침입해 다른 사람의 예금을 지정하는 가명계좌로 이체하고 사라지는 경우 등이 대표적인 본보기이다. 특히 외국에서 범행을 저지른 경우에는 범죄자의 위치를 지목하기가 사실상 불가능하다.

셋째, 범행의 흔적을 확인할 수 없는 경우가 많다. 컴퓨터 자료를 단지 복사만 할 경우에는 아무런 흔적이 남지 않는다. 바이러스의 경우처럼 현실적으로 피해가 발생하지 않으면 피해사실을 알기 힘든 경우도 많다.

넷째, 사이버공간에는 현실세계보다 훨씬 많은 수사 장애물이 존재한다. 사이버범죄를 규제하는 법체계의 허술함은 차치하더라도 인터넷을 오가는 무수한 메시지들을 일일이 감시할 수 없으며, 인권침해의 소지가 있는 압수수색은 더더욱 불가능하다.

다섯째, 사후적으로 범죄혐의를 입증하기가 어려운 경우가 많다. 디지털자료는 일단 저장되면 폐쇄성·은닉성·불가시성을 갖기 때문에 사후적으로 조작 등의 혐의를 밝히기가 어렵다.

그러나 이상의 수사문제와 관련한 특징 이외에 사이버범죄의 가장 큰 특징은 무엇보다도 그 피해규모가 막대하다는 것이다. 예컨대 인터넷의 대중화로 개인에 대한 허위사실이나 명예훼손적 표현 또는 컴퓨터 바이러스는 순식간에 전 세계에 유포될 수 있으며, 그로 인한 피해가 매우 광범위하게 미치게 된다. 최근에 있었던 유명인들의 사생활유포는 한 개인의 인생을 송두리째 앗아갔으며, 일련의 바이러스 사건은 전 세계에 있는 수백만 대의 컴퓨터를 작동불능 상태로 만들기도 하였다. 또한 간단한 수법의 사이버테러로 일국의 기반시설이 무용지물로 전락할 수도 있다. 해킹과 바이러스유포와 같은 사이버테러형 범죄는 일반 사이버범죄와는 달리 그 피해가 단순히 개인에게만 한정되는 것이 아니라 기업, 집단 나아가 국가와 사회 전체를 대상으로 할 수 있다는 점에서 그 폐해는 실로 대단하다고 할 것이다. 사이버테러 범죄가 우리사회에 야기하는 문제의 심각성은 과거 일련의 바이러스 사건들에 의해서도 잘 알려졌지만, 무엇보다도 지난 2003년 1월 25일에 발생한 사상 초유의 인터넷 대란 사태의 진행과정과 그에 대한 사회적 영향을 소개한 아래의 모신문 기사를 통해서 잘 드러난다.

[숨가빴던 '인터넷 대란' 22시간]

25일 오후 2시께부터 시작된 전국의 유무선 인터넷 접속이 마비되는 '인터넷 대란'은 다음날 정오께 이상철(李相哲) 정보통신부장관의 기자회견과 '대국민 행동요령' 발표로 일단 마무리됐다. 숨가빴던 22시간 동안의 긴박한 표정을 돌아본다.

◇ 25일(토)

▲ 오후 2시께 = 1천만명이 넘는 전국의 인터넷 사용자들 중 많은 수가 점점 접속 속도가 느려지면서 시간 초과로 원하는 사이트에 접속하지 못하게 되자 짜증을 내기 시작했다. 이 때 일부 ISP(인터넷 서비스 업체)에서는 일부 고객사의 특정 포트를 통해 패킷량이 급증하기 시작하자 고객사들에게 전화를 걸어 바이러스 공격 가능성을 경고하고 문제의 포트를 닫으라고 권유했다.

▲ 오후 2시 10분 = 17만명의 사용자를 가진 ISP(인터넷 서비스 업체)인 드림라인이 정보보호진흥원에 '네트워크의 트래픽이 급증하는 이상 징후가 발생했다'고 보고하면서 '대란'의 징후가 최초로 포착되면서 CERT(침해사고대응팀)라는 위기대책팀이 가동돼 원인분석에 들어갔다.

▲ 오후 2시 44분 = 컴팩 서버 10대, IBM 서버 2대로 구성된 혜화전화국의 DNS(도메인네임시스템) 서버에 해외로 전송되는 이상 패킷이 다량 유입되자 우리나라 최대의 초고속인터넷사업자인 KT에 대구 지역을 시작으로 민원이 접수되기 시작하면서 각 ISP에 전국적으로 엄청난 수의 민원이 몰려들었으며 이에 따라 장애 상황을 통보하는 등 조치가 시작됐다. 비슷한 시각에 24대로 구성된 하나로통신의 DNS 서버와 백본망 라우터 10대도 트래픽 과다로 마비 상태에 빠졌으며, 두루넷, 케이알라인 등도 마찬가지 장애를 겪었다. 이때 SK텔레콤, KTF, LG텔레콤 등 무선인터넷 사업자들의 망도 급속한 트래픽 증가를 겪으며 모두 마비상태에 빠진 상태였다.

▲ 오후 3시께 = 국제관문국인 혜화전화국 DNS 서버가 사실상 다운 상태에 놓인 사실이 확인되자 각 ISP의 네트워크 팀들은 '호떡집에 불난 듯' 화급하게 움직였다. 각 ISP는 급증하는 트래픽에 대처하기 위해 효과적인 분산 및 우회 수단을 찾는 한편 자체 망으로 들어오거나 나가는 패킷을 면밀히 분석하기 시작하는 한편 다른 ISP들과도 시시각각 정보를 주고받으며 문제 해결에 골몰했다.

▲ 오후 3시 44분 = KT는 일단 국제 라우터와 지역노드 라우터에서 이상 패킷이 발생하는 포트를 닫아 버린 뒤 트래픽 과다로 다운된 혜화전화국 DNS 서버 대신 구로전화국 DNS로 우회토록 조치했다. 이때쯤 이상철(李相哲) 정보통신부 장관은 집에서 쉬고 있다가 보고를 받고 황급히 자택을 나서 정보통신부로 향했으며 정통부 직원들은 비상근무 체제에 돌입했다.

▲ 오후 4시 = 구로전화국 DNS 서버에도 과부하가 발생, 접속 성공률이 10%대로 하락하면서 사실상 마비상태가 지속되고 있는 가운데 정통부는 사태의 원인이 MS-SQL 서버의 보안 취약성을 이용한 웜의 침투 및 확산임을 파악하고 각 ISP에 문제의 포트를 닫으라고 촉구했다.

▲ 오후 7시 = 국내 제2위의 초고속 인터넷 사업자인 하나로통신의 망과 서버가 복구됐다. 110여만 명의 회원을 가진 3위 업체 두루넷은 이보다 30분 전에 복구를 끝낸 상태였다. 일단 급한 불은 껐지만 트래픽 증가에 따른 속도 지연 및 접속시간 초과에 따른 불통 현상이 계속돼 밤늦게까지 인터넷 사용자들은 답답함을 느껴야 했다. KT, 하나로통신 등 ISP들은 메가패스, 하나포스닷컴 등 자신들의 사이트에 MS-SQL 서버의 취약점을 막기 위한 보안패치나 서비스 팩을 내려받으라고 촉구하는 내용의 공지사항을 올렸다.

▲ 오후 11시 = 트래픽이 다소 줄어들면서 네트워크가 어느 정도 정상을 되찾기 시작했으나 부분적인 망 접속 장애는 계속됐다.

◇ 26일(일)

▲ 오전 9시 = 이상철 장관, 정보통신부 간부들과 각 ISP 대표 등이 긴급회의를 갖고 대책을 숙의하는 한편 '대국민 행동요령'을 채택했다.

▲ 오전 11시 20분 = 이상철 장관은 기자회견을 갖고 "우리나라의 인터넷이 전국적으로 마비된 데 대해 국민들에게 송구하게 생각한다"며 대국민 사과를 발표하면서 "정확한 원인을 파악해 철저한 방지대책을 세우겠다"고 말했다. 피로한 표정의 이 장관은 40여분 간 진행된 기자회견에서 "이 같은 사고의 재발을 방지하기 위해 '사이버 도로교통법'에 해당하는 법률을 만들겠다"고 말한 뒤 취재기자들의 질문공세와 사진기자들의 플래시가 쏟아지는 가운데 회견장을 떠났다.

[네티즌들 "9.11 테러보다 더 충격적"]

"대한민국이 '방법'(공격을 받아 마비됐다는 뜻의 사이버 속어) 당했다" 사상 초유의 전국 인터넷 마비사태에 대해 네티즌들은 "9.11 테러사태보다 더 충격적이다. 상상조차 못 하던 일이 일어났다"고 경악했다. 특히 인터넷 의존도가 높은 많은 사람들은 인터넷이 막히자 "세상에서 단절된 것 같고 물이나 전기가 안나오는 것보다 더 답답하다"며 공포감마저 토로했다. 나우누리 사용자 이모씨는 "정말 무섭다. 시작페이지인 야후도 접속이 잘 안되고 MSN도 먹통. 늘 인터넷 붙들고 살던 나 같은 사람에게는 악몽이다"라며 "빨리 뉴스특보라도 보내 달라"고 호소했다. 다른 네티즌 신모씨는 "너무 어이없고 무슨 전쟁이 일어난 것 같다"며 "초고속통신망이 아무리 발달해도 이리 쉽게 전국적으로 순식간에 (인터넷이) 멈춰버리는데 뭐하나"고 푸념했다. 이 같은 사태가 워낙 유례없는 것이어서 최초 사태가 시작됐을 때만 해도 적지 않은 네티즌들이 개별 컴퓨터의 고장이거나 특정 통신망의 장애로 판단, 바이러스백신으로 검색하고 하드디스크를 포맷하는 등 소동을 벌였다. 프리챌 이용자 이모씨는 "인터넷이 안돼 컴퓨터 과열인줄 알고 전원을 꺼놨다 다시 켜도 안돼 하드를 포맷했는데 알고 보니 전국적 마비사태였다"며 "급하게 포맷하다 보니 미처 백업하지 못한 귀중한 자료들이 날아갔다"고 한탄했다. 그러다 인터넷이 광범위하게 불통되고 있다는 사실이 점차 퍼지면서 정보에 목마른 많은 네티즌들이 연합뉴스를 비롯한 언론사 사이트 등에 접속을 시도했으나 이들 사이트마저 일제히 멈추면서 오히려 낭패감만 가중됐다. 당황한 사람들은 주위의 친구나 친지 등에게 전화로 "그 쪽도 인터넷이 안 되느냐"고 물어보는 등 사태의 규모를 파악하려 애쓰는 모습이었다. 또 극소수 접속 가능한 사이트에는 사용자들이 몰려들어 관련 뉴스를 실시간으로 퍼 나르는 등 정보를 얻기 위해 필사적으로 노력했다. 사태가 점차 진정되면서 네티즌들은 이번 사태에 대해 "그간 '인터넷 강국'이라고 자화자찬하던 우리의 허약한 실태가 드러났다"며 당국에 대한 성토와 자성의 목소리를 높였다. 오마이뉴스에 글을 쓴 한 일본유학생은 "마이니치 신문의 인터넷 화면에 'IT 대국 한국, 인터넷 마비'라는 제목이 전면을 차지했다"며 "평소 한국의 인터넷은 대단한 자랑이었고 부러움도 많이 샀는데 이번에 망신살이 톡톡히 뻗쳤다"고 전했다. 다른 한 네티즌은 "국가 전체의 인터넷 망이 일순간에 이렇게 처참하게 무너질 수 있다는 것은 건축으로 치면 엄청난 부실공사"라며 "이런 국가적 망신의 책임을 지고 정보통신부 장관은 사임하라"고 비난했다. 이 와중에 인터넷과 달리 나우누리 등 일부 PC통신망은 정상 가동됐다는 사실이 알려지면서 사용자가 폭주해 '구닥다리' 취급을 받아오던 PC통신이 새삼 각광을 받기도 했다. 또 일부 네티즌들은 이번 사태를 '인터넷 붙박이' 생활에서 벗어나 다른 일을 하는 기회로 삼겠다는 역설적인 모습을 보이기도 했다. 나우누리 사용자 김모씨는 "MSN이 15분째 접속이 안 되고 있는데 이참에 오랜만에 '폐인' 생활을 그만두고 아는 친구들이나 만나러 나가야겠다"며 "온라인이여 바이바이. 나는 오프라인 세계로 떠나련다"고 말했다.

제2절 사이버공간의 특수성과 사이버범죄

흔히 사이버범죄의 원인으로는 현실공간과는 다른 가상공간이 갖는 특수성 - 예컨대, 가상공간은 익명성, 자율성, 개방성, 혹은 탈공간구속성 등을 특징으로 한다 - 이 지적되곤 한다. 물론 사이버범죄의 상당 부분은 이러한 사이버공간이 갖는 특수성에 의해서 설명될 수 있을 것이다. 그러나 이러한 설명은 범죄사건을 범죄자의 의지, 범행의 기회, 혹은 가해자와 피해자간의 역동적인 상호작용의 결과로 보는 시각에서는 불만스러울 것이다. 모든 사건이 다 그러한 것은 아니지만, 사이버공간 속에서도 가해자와 피해자는 서로 상호작용 하는 경우가 많기 때문에, 가상공간이 갖는 특수성만으로 사이버범죄를 설명하려는 시도는 범죄자의 범행의도와 범죄의 발생을 용이하게 하는 상황적 요소만을 고려한 반면, 피해자의 존재와 역할은 무시하는 단편적 설명으로 한계를 갖는다고 할 것이다. 따라서 본 연구에서는 사이버범죄의 원인을 사이버공간이 갖는 특수성으로 설명함과 동시에, 기존의 범죄학 및 피해자학 이론의 틀 속에서 사이버범죄(피해)를 함께 설명하고자 한다. 나아가 이러한 작업에서는 청소년들의 인터넷 사용행태가 사이버범죄의 유발에 어떠한 함의를 갖는지도 성찰의 대상이 될 것이다. 먼저 사이버공간의 특수성이 사이버범죄를 유발하는 측면을 살펴보기로 한다.

1. 비대면성 또는 익명성

사이버공간은 인터넷을 매개로 하여 형성되는 생활공간으로서 비가시적이므로 현실세계와는 달리 범죄자들이 자신의 얼굴과 정체를 노출시키지 않고 행동할 수 있다는 이점을 갖는다. 인터넷 상용서비스를 범행에 이용할 때도 타인의 ID와 패스워드를 도용하면 완벽하게 자신의 익명성을 보장 받을 수 있다. 사실 인터넷 사업자들이 의도적으로 정확한 인적사항을 요구하지 않는 경우도 많다. 이러한 비대면성과 익명성으로 인하여 사이버 범죄자들은 대면적 상황에서는 감히 하기 어려운 언행도 아무런 죄의식 없이 과감하게 하게 되는 경우가 많다. 사이버공간에서의 사회적 관계는 개인의 필요에 따라 좌우되기 때문에 공동체적 유대감를 형성하기 어렵고, 이러한 사회적 유대의 부재는 개인의 행동에 대한 내외적 통제의 약화로 이어지며, 따라서 범죄 및 일탈에 유리한 환경이 되고

있는 것이다(류승호, 1998). 이와 유사한 설명은 개인의 자아(self)에 관한 Goffman의 이론(Dramaturgy)을 통해서도 제시될 수 있다. 예컨대, 가상공간은 자아의 이기적이고, 비합리적이며, 반사회적인 부분인 '후면영역'(back stage)의 특성이 주도하기 쉬운 곳이기 때문에 범죄에 대한 친화력을 가질 수 있다(Meyrowitz, 1985).

2. 자율성

사이버공간에서는 접근가능한 누구나 자신의 목적이나 의도를 달성하기 위해 자신의 사상, 생각, 견해 등을 유포할 수 있으며, 획득할 수 있다(이재진, 2000). 따라서 자율성은 사이버공간의 가장 강력한 도덕적 원리로서, 오프라인에서의 일방향적인 소통방식과 통제기구 및 규범으로부터 벗어나 자율적인 개인들이 스스로 표현의 자유를 만끽할 수 있는 원리인 것이다. 미국에 있어서도 1996년 전자통신법(Telecommunications Act of 1996)[6]에서 사이버공간의 자율성을 규정하고 있다. 그러나 이러한 자율성은 사이버공간에서의 폭언, 허위사실의 유포, 명예훼손, 음란물 유포 및 음란사이트의 범람 등 부작용을 낳기도 하며, 사이버범죄에 보다 쉽게 접근할 수 있는 여건을 조성해 준다.

3. 개방성

혹자는 인터넷을 '무정부 공간'이라 칭하기도 한다. 이것은 어느 정도 비약된 측면도 있겠지만, 인터넷의 무한한 개방성을 염두해 둔다면 결코 지나친 표현은 아닐 것이다. 인터넷은 전 세계에 펼쳐져 있는 수많은 네트워크와 컴퓨터들이 기종에 관계없이 표준화된 규정에 따라 상호간의 접속을 허용해 주는 개방성을 제공한다.[7] 인터넷 이용자들은

6) 1996년에 제정된 전자통신법(The Telecommunications Act of 1996)은 근 62년 동안 유지해 왔던 구 전자통신법을 최초로 정비한 법이다. 同 법의 목적은 누구나 통신사업에 참여할 수 있도록 하며, 모든 통신시장에서 있을 수 있는 모든 통신사업경쟁에 대비하도록 하는 것이다. 전자통신법은 미국인들의 근무방식, 생활방식, 학업방식들을 변화시킬 가능성을 가지고 있다. 그것은 전자통신법이 전화통신서비스(telephone service), 장거리지역전화, 케이블 프로그램 편성과 기타 TV 서비스, 방송 서비스, 그리고 학교에 제공되는 서비스들에 영향을 끼칠 것이기 때문이다.

7) http://www.chungju-ch.hs.kr/teacher/%C7%CF%BC%BA%BF%EB/internet/inter14.htm.

표준화된 규정을 따를 경우 세계 각국의 어느 컴퓨터에든 접속하여 그 속에 있는 정보들을 얻을 수 있고 의사소통이 가능하다.[8] 즉 인터넷의 개방성으로 인해 원하는 사이트에 접속하며, 원하는 정보를 얻는다. 이러한 개방성은 정보의 송신자와 수신자 사이의 벽을 없애고 정보 공유를 허용하는 데서 발생한다. 이 점이 기존의 다른 매체와의 가장 큰 차이점이라고 할 수 있는 바, 개방적이지 않은 통신망은 이미 사이버공간이라고 할 수 없고 기존 매체와 차이가 없게 된다. 그러나 개방성은 본연의 순기능에도 불구하고 여타의 사이버 공간의 특성들과 마찬가지로 사이버범죄라는 부작용과 무엇보다 밀접한 관련을 맺고 있다.

4. 시·공간적 초월성 또는 탈공간구속성

인터넷은 개인용 PC와 LAN 등 기본적 장비만 있으면 언제 어디서나 접속이 가능하다. 이처럼 사이버공간에서의 삶은 시간과 공간의 개념을 무색하게 만드는 것이다. 인터넷 공간의 이러한 시공초월성은 잠재적 범죄자들에게 엄청나게 많은 범죄의 기회를 제공하고 있다. 즉 최근의 일련의 바이러스 사건(예컨대, 멜리사, CIH, 러브바이러스, 웜바이러스, 트로이 목마 등)을 통해서도 알 수 있듯이, 범죄자는 인터넷이 연결된 곳이면 세계 어느 곳에 있는 컴퓨터에라도 바이러스를 유포할 수 있고 해킹도 할 수 있다.

제3절 일반 범죄학이론과 사이버범죄

모든 범죄학 이론이 그러하듯이 특정한 이론 하나를 가지고 모든 유형의 범죄를 다 설명하기란 참으로 어려운 것이다. 특히 사이버범죄의 경우 상당히 복합적인 원인으로 발생하며, 다양한 양상을 보이기 때문에 더욱 접근하기가 까다롭다고 할 수 있다.

따라서 본 연구에서는 청소년의 인터넷을 이용한 범죄에 대하여 범죄자 중심의 설명과 피해자 중심의 설명으로 각각 나누어 설명하고자 한다.[9] 본 절에서 논의하게 될 가해자

8) http://www.itmast.com/internet/concept/ib_expa6.html.

중심의 분석에 있어서는 거시적 수준의 이론으로 Emile Durkheim의 '사회적 비규제 이론(Social Deregulation Theory)'과 미시적 수준의 이론으로 Edwin H. Sutherland의 '차별교제이론(Differential Association Theory)' 및 Gottfredson과 Hirschi의 '자기통제이론(Self-Control Theory)'을 적용하기로 한다.

1. 사회적 비규제 이론

1893년에 처음 발행된 『사회분업론(The Division of Labour in Society)』에서 E. Durkheim은 산업사회의 발달에 수반되는 사회변동의 과정을 설명하였다. 그는 원시적 형태의 사회를 '기계적(mechanical)'이라고 표현했으며, 보다 진보된 형태의 사회를 '유기적(organic)'이라고 표현하였다.

'기계적 사회'는 자급자족하는 집단들로 이루어져 각 집단의 구성원들은 서로 같은 일에 종사하며 동일한 가치관과 동일한 생활스타일을 갖고 있다. 형법은 기계적 사회의 획일성을 유지하기 위한 주요한 수단이다. 즉 규범위반자에 대한 가시적 처벌은 위반자의 열등성을 드러내고, 다수집단으로 하여금 집합의식에 더욱 전념하게 한다. 이와 같은 의미에서 범죄는 기계적 사회의 정상적인 특성인 것이다.

한편 산업화와 함께 사회는 '유기적 사회'로 나가게 되는데, 분업이 보편화되고 각기 다른 집단들이 더욱 상호의존하게 된다. 이러한 유기적 사회에서는 사회의 여러 부분들 간의 관계를 규제하는 법률의 중요성이 더욱 커지게 되며, 만약 규제가 불충분하면 범죄를 비롯한 여러 사회문제가 발생하게 된다. 그런데 중요한 것은 규제가 불충분해질 가능성은 근대화가 급속도로 이루어질 때 더 커진다는 사실이다. 그것은 급속한 사회변동기에는 새로운 통제유형이 효과적으로 발달하지 못하여 과거의 통제양식을 잘 대체하지 못하기 때문이다. 이러한 상태를 Durkheim은 '무규범' 상태라고 지적하였다.

다음으로 Durkheim은 약화된 사회적 규제가 어떻게 개인적 현상인 자살과 관련되어

9) 물론 범죄가 가해자와 피해자 간의 역동적인 상호작용의 결과인 경우가 많기 때문에 이 둘을 명확히 구분하는 것이 용이하지 않을 수도 있다. 그러나 설명의 편리를 위해, 이 절에서는 '일반 범죄학이론'의 제하에 범죄자 중심의 설명을, 그리고 다음 절에서는 '범죄피해이론'의 제하에 피해자중심의 설명을 다루기로 한다.

있는지를 연구하였는바, 그가 두 가지 비규제의 근원으로 제시하고 있는 것이 '이기주의(egoism)'와 '아노미(anomie)'이다(Liska와 Messner, 1999). 이기주의는 개인이 사회로부터 비교적 자유롭고 독립적이며 사회와 통합되지 않은 상황을 말하며, 아노미는 사회의 규범과 보편적인 이해의 붕괴를 의미하는 것이다.

Durkheim의 사회적 비규제 이론은 자살에 대한 사회학적 연구와 이론적 작업을 고무시켰을 뿐만 아니라 다른 일탈유형 및 사회적 문제행동에 대한 연구에도 다양한 적용을 가능하게 하였다.

사이버공간에서 발생하는 청소년 범죄에 대해서도 Durkheim 이론의 적용이 가능할 것이다. 정보통신기술이 조성하는 사이버공간은 단기간 내에 급속도로 확장, 발전해 왔지만, 그에 대한 사회적 통제장치, 즉 규제가 사이버 커뮤니티의 발달속도를 따라잡지 못하여 크게 불충분하다. 구체적으로 사이버윤리가 제대로 정착되지 못하였으며, 일탈행위들을 규제할 제도적 장치로서의 법률도 제대로 구성되지 못하였다. 또한 사이버공간의 특수성에서 기인하는 이기주의는 더욱 사이버공간에서의 청소년범죄를 부추기는 결과를 낳은 것이다.

2. 차별교제이론

Edwin H. Sutherland의 차별교제이론(Differential Association Theory)은 왜 특정한 사람이 일탈적 행위유형을 학습하게 되는지를 설명하는 이론으로, 범죄는 일반적인 행위와 마찬가지로 학습을 통해서 배우게 되고, 학습은 주로 친밀한 사람들과의 상호작용을 통해 이루어진다는 것이 이 이론의 핵심이다.

Sutherland는 인간 현상의 두 가지 측면을 설명하고자 하였는데, 하나는 왜 사람들의 집단에 따라 범죄율이 서로 다른가 하는 것이고, 다른 하나는 왜 대부분의 사람들은 범죄자가 되지 않는데 반해 일부 사람들은 범죄자가 되는가 하는 것이었다. 그는 이러한 질문에 대한 해답을 '차별적 교제'에서 찾고자 하였으며, 그것을 다음과 같은 9가지 가정으로 정리하였다.

① 범죄행위는 학습되는 것이다.

② 범죄행위의 학습은 사람들간의 의사소통과정을 통해 일어난다.

③ 범죄행위의 학습은 주로 친밀한 집단 속에서 잘 일어난다.

④ 범죄행위가 학습될 때, 그 학습내용에는 범죄행위의 기술뿐 아니라 동기, 충동, 합리화 방법, 태도 등을 모두 포함한다.

⑤ 범죄동기나 충동은 현행 법률을 긍정적으로 정의하느냐, 아니면 부정적으로 정의하느냐에 따라 학습된다. 즉 어떤 사람은 법률을 반드시 지켜져야 할 규칙으로 정의하는 사람들 속에 있을 수 있으며, 반면 다른 사람은 법률을 위반하는 것이 바람직하다고 정의하는 사람들 속에 있을 수 있기 때문이다.

⑥ 법 위반에 대해 비우호적인 인식보다 우호적인 인식이 앞서도록 학습된 사람은 비행으로 나아간다.

⑦ 차별적 교제는 만남의 빈도·기간·선호·강도 등에 따라 다양하게 나타난다.

⑧ 범죄적 또는 비범죄적 유형과 접촉하면서 범죄행위를 학습하는 과정은 일상생활 속에서 다른 행위의 학습과정에서 작용하는 기제들과 동일하다.

⑨ 범죄행위는 일반적인 욕구나 가치에 의해 일어나지만, 그러한 욕구와 가치가 범죄행위의 본질적 성격을 특징짓지는 않는다. 왜냐하면 비범죄적 행위도 그와 동일한 욕구 및 가치에 의해 이루어지기 때문이다.

이와 같은 차별교제이론은 특히 청소년비행을 설명함에 있어 매우 유용한 이론으로 평가되고 있으며, 본 연구가 다루는 사이버공간에서의 청소년범죄를 설명함에 있어서도 상당히 유효한 측면이 많이 있다. 청소년들은 사이버공간에서의 각종 일탈행위나 그러한 행위를 위한 기술, 동기, 합리화, 태도 등을 친구나 기타 친밀한 동년배 집단으로부터 배우게 되는 경우가 많기 때문이다.

청소년들이 주로 생활하는 학교, 그리고 적절한 여가 공간이 없어 흔히 이용하게 되는 PC방과 같은 공동의 장소는 청소년들에게 사이버범죄의 학습을 위한 주요한 공간적 배경이 되고 있는 것이다. 물론 사이버범죄의 전문적인 기술이 모두 학습된다고 보기는 어렵다. 범죄의 기술은 일정 수준이상에서는 스스로 터득하는 경우가 많기 때문이다.

하지만, 사이버범죄는 초기의 입문과정에 있어서 주로 친밀한 집단에 의해 학습되는 경향이 상당히 강한 범죄유형이라 할 수 있을 것이다.

3. 자기통제이론

Gottfedson과 Hirschi는 1990년 「범죄의 일반이론(A General Theory of Crime)」을 출판하면서 자기통제이론을 발표하였다. 이들은 고전주의 범죄학의 가정에 따라 인간의 본성을 자기이익을 추구하고 이기적인 존재로 보았다. 따라서 범죄나 비행이 행위자에게 쉽고, 즉각적이고, 확실한 이익을 제공한다고 볼 때 모든 사람은 범죄나 비행에의 동기를 가지고 있는 셈이다.[10]

이 이론은 특히 행위자의 내적 통제인 자기통제력에 초점을 맞추고 있다. 자기통제력은 순간적인 욕구와 충동을 조절할 수 있는지, 스릴과 모험을 추구하기 보다는 분별력과 조심성이 있는지, 근시안적이기 보다는 앞으로의 일을 생각하는지, 쉽게 흥분하는 성격인지 등을 말하는 것이다. 자기통제력의 주요 형성 시기인 8세까지 어린아이는 가정, 특히 부모의 통제와 감독 하에 있게 되고, 이 기간 중에 보호자의 훈육에 의해서 아이의 자기통제력이 발달하게 된다. 결국 자기통제력은 가정을 중심으로 배양되기 때문에 가정을 중심으로 한 초기 사회화는 개인의 범죄를 설명함에 있어서 그 이후의 다른 어떠한 경험들 보다 더 중요한 의미를 갖는 것이다[11].

자기통제력이 약한 사람들은 욕구를 즉각적으로 충족시키려 하고, 단순한 일을 선호한다. 또한 위험한 행동을 좋아하고, 말보다는 행동으로 스스로를 표현하며, 자기중심적이어서 다른 사람의 고통에 무신경하고, 성미가 급한 경향이 있다고 한다. 결국 자기통제력이 낮은 사람은 “지금 당장 이 자리에서(here and now)” 욕구충족을 지향하는 경향이 있는 사람이라고 한다(민수홍, 2003).

온라인상의 청소년범죄도 마찬가지이다. 자기통제력이 약한 청소년의 경우 익명성, 자율성, 탈공간구속성, 개방성 등 가상공간의 범죄친화적 특성들에 편승하여 욕구를 절제

10) http://www.survey.com/criminology/lecture/10.pdf.

11) Gottfredson과 Hirschi는 범죄나 비행을 저지름에 있어서 개인간의 차이는 인생의 초기단계에서 결정되고, 그 이후로는 한평생 안정화되는 경향이 있다고 하였다.

하지 못하고 근시안적인 관점에서 우발적, 충동적으로 비행에 빠져들 수 있는 것이다. 또한 약한 자기통제력은 타인이 입게 될 막대한 피해를 고려하지 못하게 한다. 만약 문제행동을 야기한 청소년에게 가정에서의 초기 사회화가 제대로 이루어졌다면 범행이전에 보다 효과적으로 자신을 통제할 수 있었을 것이다.

제4절 범죄피해이론과 사이버범죄

범죄의 원인을 제대로 이해하기 위해서는 범죄의 발생을 설명하는 이론과 함께 범죄피해의 발생을 설명하는 이론도 함께 고려할 필요가 있다. 사이버공간에서 발생하는 범죄피해를 설명할 수 있는 별개의 이론은 아직 나타나지 않고 있다. 따라서 이 절에서는 오프라인에서의 범죄피해를 설명해 주는 기존의 이론들의 틀 속에서 사이버공간에서의 범죄피해가 어떻게 설명될 수 있는지를 검토해 보기로 한다.

현실세계에서 범죄피해를 설명하는 이론들은 크게 두 가지 유형으로 분류될 수 있다. 첫번째 설명유형은 기회의 개념에 초점을 두며, 피해사건이 시간과 공간에 걸쳐 분포되는 방식을 이해하려 한다. 그래서 이들은 왜 어떤 사람들은 다른 사람들에 비해 범죄피해를 당할 가능성이 높은가 하는 문제를 다룬다. 이에 비해, 두번째 설명유형은 특정 피해사건에서 피해자는 어떠한 역할을 하며, 사회적 교환의 맥락에서 피해자와 가해자가 어떻게 상호영향을 주고받는 지를 밝히려고 한다. 이 절에서는 이러한 두 가지 설명유형과 그러한 이론들이 사이버공간에서의 범죄피해를 설명함에 있어서는 어떠한 함의를 지니며, 또한 어떻게 적용될 수 있는 지 등을 논의하고자 한다.

1. 범죄의 기회

범죄가 발생하기 위해서는 범죄자의 범행의도와 기회가 일치하여야 한다. 기회이론들(opportunity theories)은 범죄자들의 범행동기 또는 의도와 함께 이를 실행하기 위한 기회의 수를 증가시키거나 감소시키는 요인들에 대한 설명이 진정으로 필요하다고 주장한다. 문헌에서 발견되는 대표적인 기회이론으로는 다음 세 가지가 있다.

1) 생활양식-노출이론(Lifestyle-Exposure Theory)

이 이론은 Michael Hindelang과 그의 동료들(1978)이 발전시킨 이론이다. 이들은 사람들의 사회인구학적 특성들과 범죄피해 위험 간의 관계에 초점을 두었으며, 이 둘 간의 관계를 설명해 주는 중심개념이 "생활양식"이라고 주장하였다. 이들은 생활양식을 사람들의 일상적인 여가 및 직업활동(직장, 학교, 가사 등)의 맥락에서 정의하였다. 생활양식에 있어서의 차이는 곧 사람들이 자신의 전체 활동영역에 대해 시간과 에너지를 분배하는 양식에 있어서의 차이와 같다. 이러한 생활양식에 있어서의 차이는 사람들이 처하는 범죄피해 위험의 정도에 있어서의 차이와 연결된다. 예컨대, 잠재적 범죄자가 많이 포함된 집단과 접촉하는 사람들이나, 범죄가 자주 발생하는 시간대(늦은 밤)와 장소(유흥가, 어두운 골목 등)에서 활동하는 사람들의 경우 높은 피해율을 보인다. Hindelang과 그의 동료들은 남성들, 청년층, 그리고 소수인종집단들이 대개 위험한 생활양식을 가지고 있기 때문에 일반적으로 높은 피해를 경험한다는 것을 발견하였다.

2) 일상활동이론(Routine Activity Theory)

Cohen과 Felson(1979)은 기존의 범죄학 이론들이 범죄의 공간적 분포에만 집중하며 피해자에 대한 연구를 등한시하였다고 비판하고, 범죄자와 피해자 모두가 시간과 공간에 걸쳐 분포되는 양식과 그들의 일상활동을 고려할 것을 제안하였다. 그들은 범죄발생의 세 가지 필수요건으로서 동기화된 위반자(motivated offenders), 적절한 범행대상(suitable targets), 그리고 가용한 보호력의 부재(the absence of capable guardians)를 제시하고, 특정 범죄피해가 발생하기 위해서는 이 세 가지 요소가 모두 일정한 시간과 공간에서 수렴되어야 한다고 주장하였다. 이 세 요소가 특정 시공에서 수렴할 확률은 바로 사람들의 일상활동이 갖는 성격에 달려 있기 때문에 Cohen과 Felson은 자신들의 이론을 '일상활동이론'이라고 명명하였다.

3) 구조적 선택이론(Structural-Choice Theory)

이 이론은 Miethe와 Meier(1994)에 의해서 제안된 것으로서 앞의 두 이론의 연장으로 볼 수 있다. 이들은 기회(opportunity)란 개념을 보다 명백히 하려는 시도에서, 일상

활동이론의 두 가지 핵심 개념인 가용한 보호력(capable guardianship)과 범행대상의 매력성(target attractiveness)에다 근접성(proximity)과 노출의 정도(exposure)라는 두 가지 요인을 추가하였다. 범죄에 대한 근접성이란 잠재적 범죄자가 사는 지역과 잠재적 범행대상(사람 또는 재산)이 위치한 지역 간의 물리적 근접성을 의미한다. 노출의 정도는 표적의 가시성(visibility) 또는 표적에 대한 접근가능성(accessibility)을 나타내는 것이다. 예컨대, 밤중에 공공장소에서 많은 시간을 소비하는 사람은 대인범죄에의 노출 정도가 크며, 침입통로(문과 창)가 많으며 외진 곳에 놓인 집의 경우 밤도둑에 대한 노출 정도가 크다. Miethe와 Meier는 일상활동의 패턴이 어떤 사람이나 재산을 더 큰 위험에로 노출시키는 한편, 특정 범행대상의 선정은 그 표적를 선정함으로써 얻게 되는 보수와 그에 따르는 위험(또는 비용)에 대한 합리적인 판단에 달려있다고 전제하고, 근접성과 노출은 사람과 재산을 서로 다른 정도의 위험에 처하게 하기 때문에 "구조적 요인"들로서 고려되어야 하며, 반면에 범행대상의 매력성과 가용한 보호력은 일정한 수준의 위험을 갖는 상황 속에서 어떤 표적을 선정할 것인지를 결정해 주기 때문에 "선택적 사항"들로서 가장 잘 이해될 수 있다고 주장하였다.

2. 피해자-가해자 상호작용

범죄피해에 대한 두 번째 설명유형은 범죄사건을 피해자와 가해자 간의 일종의 사회적 교환의 산물로서 파악한다. 이들은 피해자와 가해자는 서로 고립되어 행동하지 않는다는 점을 이론의 출발점으로 삼기 때문에 대인범죄(살인, 강도, 강간 등) 피해의 설명에는 유용하나 재산범죄 피해의 설명에는 한계를 갖는다. 이러한 상호작용론은 크게 두 가지가 있다.

1) 피해자 촉발이론(Victim Precipitation Theory)

이 분야의 가장 고전적인 연구는 Marvin Wolfgang(1958)의 살인 사건에 관한 연구이다. 이 연구에서 Wolfgang은 자신이 연구한 살인 사건의 약 4분의 1에서 가해자 보다는 오히려 피해자가 먼저 무기를 휘두르거나 폭력으로 위협하는 등의 공격적 행동을

함으로써 사건의 발단을 제공하였음을 발견하였다. 요컨대, 살인 행위는 단순히 살인자의 살의의 산물이라기보다는 피해자와 가해자가 함께 연루되는 상황적 역학의 산물이라는 것이다.[12]

2) 상황적 전이행위이론(The Situated Transaction)

피해자 촉발의 논리는 피해자가 먼저 공격적인 또는 도발적인 언행을 했는지의 여부가 중요하며, 따라서 피해자에 대한 일종의 도덕적 비난을 내포할 수 있기 때문에 신중한 적용이 요구된다.[13] 그러므로 보다 합리적인 생각은 범죄사건을 단순히 가해자의 동기나 피해자의 반응의 산물이라기보다는 가해자와 피해자의 행위의 조합적 산물로서 이해하는 것이다. David F. Luckenbill은 살인에 관한 연구(1977)에서 피해자-가해자 상호작용에 대한 보다 포괄적인 이론을 제시하였다. 그는 피해자와 가해자가 구성해 나가는 상호작용의 전반적인 과정과, 피해사건을 둘러싼 상황(situation)과 목격자(audience)[14]가 그러한 상호작용 과정에 미치는 영향력에 대한 관심을 강조하였다. 이와 같이 Luckenbill은 피해사건을 "상황적 전이행위(situated transactions)"로 개념화 하였다. 그는 범죄사건을 하나의 연극에 유추하였다. 이를테면, 연극에는 무대(상황)와 관객(목격자)이 있으며 배우들(피해자와 가해자)은 대본에 따른 연기를 수행한다. 극중 배우들의 역할은 무대의 바뀜에 따라서 그리고 관객들의 반응에 따라서 가변적일 수 있다. 요컨대, 범죄피해 사건은 특정 상황 속에서 가해자와 피해자(그리고 때로는 목격자)가 구성해 나가는 역동적인 상호작용의 산물인 것이다.

---

12) 피해자 촉발이론과 유사한 한 가지 연구 경향은 범죄사건을 피해자의 불의에 대한 가해자의 응징, 자기방어, 또는 정당방위로서 이해하는 것이다(Black, 1983). 예컨대, 살인이나 폭행을 행하는 사람은 자신의 행위를 피해자가 자신에게 한 것에 대한 반응으로서, 즉 하나의 사회통제로서 이해한다는 것이다.

13) 예컨대, 피해자 촉발의 논리는 Sykes와 Matza(1957)가 제시한 중화(neutralization)의 한 가지 기법인 '피해자에 대한 부정'(denial of the victim)을 상기시킨다.

14) 물론 목격자는 존재하지 않을 수도 있다.

3. 사이버공간에서의 범죄피해와 범죄학이론

왜 사이버범죄에 의한 피해를 당하는가? 우스개 소리 같지만, 사이버범죄로 인한 피해를 당하는 가장 결정적인 이유는 인터넷을 사용하기 때문이다. 달리 표현해서, 인터넷을 사용하지 않는다면 사이버범죄로부터 피해를 당할 하등의 이유도 없는 것이다. 그러나 이렇게 말하는 것은 왜 어떤 네티즌들은 사이버범죄에 의한 피해를 당하지 않는데 비해 다른 네티즌들은 이를 경험하게 되는가, 또는 왜 어떤 네티즌들은 다른 네티즌들에 비해 사이버범죄에 의한 피해를 당할 가능성이 더 높은가 하는 물음에 대한 설명은 포기하는 셈이 된다.

1) 범죄의 기회와 사이버범죄 피해

"사이버범죄로 인한 피해를 당하는 가장 결정적인 이유는 인터넷을 사용하기 때문이다."라고 말하는 것은 곧 위에서 살펴 본 기회이론들이 사이버범죄 피해의 설명에 보다 적절할 가능성을 시사하는 것이라 하겠다. 이것은 곧 인터넷 사용을 전제로 할 경우, 사용기간이 오랠수록 그리고 평균사용시간이 많을수록 사이버공간에서 범죄피해를 당했을 가능성이 크다는 것을 의미한다.

구체적으로, 사회인구학적 특성, 생활양식과 범죄피해 위험간의 관계에 대한 Hindelang과 그의 동료들(1978)의 논의를 사이버범죄 피해에 연장시켜 보자. Hindelang은 생활양식을 사람들이 자신들의 전체 활동영역에 대해 시간과 에너지를 분배하는 양식에 있어서의 차이로 규정하였다. 이러한 규정을 사이버공간에 적용한다면 네티즌들이 가장 자주 사용하는 인터넷의 용도로써 사이버커뮤니티에서의 생활양식을 파악해 볼 수 있을 것이다. 이러한 사용용도에 있어서의 차이는 네티즌들이 경험하는 사이버범죄의 피해유형에 있어서의 차이와 상관될 가능성이 크다. 예컨대, 전자상거래를 자주 하는 네티즌들의 경우 다른 네티즌들에 비해 전자상거래에 의한 피해를 당할 개연성이 크며, 인터넷으로 금융 및 경제활동을 자주 하는 네티즌들의 경우 다른 네티즌들에 비해 신용카드, 사이버증권, 사이버뱅킹 등의 금융피해를 당할 가능성이 크며, 채팅을 많이 하는 네티즌들의 경우 다른 네티즌들에 비해 사이버 성희롱이나 성폭행, 사이버스토킹,

인신공격・언어폭력・협박, 허위사실유포・명예훼손 등에 의한 피해를 당할 개연성이 크다. 또한 온라인 게임을 하지 않는 사람의 경우 게임아이템 절도와 같은 피해를 당할 하등의 이유도 없을 것이다. 사회인구학적 특성과 범죄피해 위험간의 관계의 맥락에서는 현실세계에의 경우와 유사한 결과를 상정해 볼 수 있을 것이다. 예컨대, 현실세계에서 범죄피해의 가능성이 가장 높은 인구집단이 남성과 청년층 (그리고 소수인종집단들) 이었듯이 사이버공간에서도 남성 또는 청년층이 상대적으로 사이버범죄에 의한 피해를 당할 가능성이 클 것으로 생각된다. 그것은 이들 인구집단의 인터넷 사용량이 절대적으로 큰 것도 한 가지 이유이지만, 동시에 이들 인구 집단이 질적으로 위험한 인터넷 사용패턴을 가질 가능성이 크기 때문이다. 예컨대, 채팅이나 전자상거래, 사이버금융활동, 온라인게임 등의 주 사용인구는 남성 또는 청년층이며, 따라서 이들은 여성 또는 중장년층에 비해 더 큰 범죄피해의 위험에 노출되어 있다고 할 것이다.[15]

일상활동이론의 요체는 특정 범죄피해가 발생하기 위해서는 잠재적 범죄자와 적절한 범행대상, 그리고 가용한 보호력의 부재가 일정한 시간과 공간에서 수렴되어야 한다는 것이다. 사이버공간에서는 항상 동일한 ID나 패스워드를 사용하는 사람, 자신의 성별을 노출시키는 ID나 대화명을 사용하는 사람,[16] 자신의 개인정보를 무분별하게 제공하는 사람, 전자상거래나 사이버금융거래를 자주하는 사람, 채팅이나 동호회 활동을 빈번히 하는 사람, 무료 프로그램이나 파일을 함부로 다운 받는 사람, 온라인 게임을 즐기는 사람 등이 동기화된 범죄자에게 매력적인 범행대상으로 인식될 수 있을 것이다. 현실세계에서 범죄의 억제력으로 작용하는 가용한 보호력은 주로 경찰의 치안활동이라고 할 수 있을 것이다. 실제로 경찰의 가시성(police visibility) 내지는 경찰력의 크기가 범죄를 억제하거나 범죄에 대한 사람들의 두려움을 약화시키는 효과는 여러 연구에서 검증된바 있다(Baker et al., 1983; Baumer, 1985; Box et al., 1988; Lee, 2000; Maxfield, 1987). 그러나 현실세계와는 달리, 사이버공간에서는 잠재적인 범죄의 발생을 억제할 수 있는 가시적인 보호력이 거의 존재하지 않는다. 물론 상당수의 상업용 사이트들이 고객들의

15) 네티즌들의 사회인구학적 특성과 인터넷 이용행태의 관계에 관한 보다 풍부한 논의는 한국인터넷정보센터가 발간한 2002년도 인터넷 이용자수 및 이용행태에 관한 설문조사 결과보고서를 참조 바란다.

16) 1998년 말의 천리안 “화냥년 ID사건”이 한 가지 좋은 예가 될 수 있다. 이 ID의 사용자는 익명의 네티즌들로부터 무수한 사이버 성폭력을 경험하였다.

사이버범죄 피해를 예방하기 위한 자체 차원의 노력을 하고 있으며,[17] 사이버테러대응센터 또는 사이버범죄수사대 등 소위 사이버경찰들이 활동하고 있으나, 그들의 활동은 대개 제한적이고 비가시적이며 특정 범죄가 발생한 연후에 사후 대응하는 등 범죄예방을 위한 효율적인 억제력으로 작용하지 못하고 있다.

일상활동이론은 또한 상기한 범죄피해의 요소들이 반드시 일정한 시간과 공간에서 수렴할 것을 주장하며, Miethe와 Meier의 구조적 선택이론은 잠재적 범죄자와 범행대상 간의 물리적 근접성과 그 대상에 대한 접근가능성을 범죄피해를 결정하는 중요한 요소로서 고려하고 있다. 이 점에서 사이버공간은 범죄의 발생에 매우 유리한 환경이 되고 있다. 예컨대, 사이버공간은 시공초월성을 그 주요한 특성으로 갖기 때문에 잠재적 범죄자들에게 표적에 대한 무한한 접근가능성을 부여해 줌으로써 엄청나게 많은 범죄의 기회를 제공해 준다고 할 것이다.

2) 피해자-가해자 상호작용과 사이버범죄 피해

범죄사건을 피해자와 가해자 간의 역동적 상호작용의 산물로서 보는 시각은 폭력범죄를 설명함에 있어서는 대단히 유용하나, 재산범죄의 설명에는 한계를 갖는다. 유사한 평가가 사이버공간에서 발생하는 피해사건을 설명함에 있어서도 마찬가지로 적용될 수 있을 것이다. 예컨대, 피해자 촉발론이나 상황적 전이행위론은 전자상거래나 인터넷 사기피해, 개인신용정보 도용에 의한 피해, 사이버절도 피해, 전자문서의 도용・변조・파괴 피해, 컴퓨터 바이러스나 스팸메일에 의한 피해 등(이것들은 오프라인에서의 재산범죄와 유사하다)을 설명하는 데는 부적절하다. 왜냐하면 그러한 피해유형들에서는 피해자와 가해자가 서로 고립되어 행동하기 때문이다. 그러나 사이버 성희롱・성폭행, 사이버스토킹, 허위사실유포・명예훼손, 인신공격・언어폭력・협박 등(이것들은 오프라인에서의 폭력범죄와 유사하다)의 피해유형에서는 비록 직접적이며 대면적인 접촉은 아니더라도 최소한 피해자와 가해자가 서로 고립되어 행동하지는 않기 때문에 상호작용이론들이 부분적인 설명력을 가질 수 있다고 본다. 예컨대, 채팅을 할 때나 토론방에서 피해자의 네티켓에

17) 예컨대, 최근에는 상당수의 상업용 사이트들이 사이버 성폭력, 언어폭력, 스팸메일 등의 사이버범죄를 예방하기 위한 자체 신고센터를 운영하고 있다.

반하는 도발적 언행은 잠재적 가해자로부터 일탈적 반응을 유발할 수도 있다. 한편 사이버범죄의 경우 현실세계와는 달리 피해사건을 둘러싼 상황과 목격자가 개입할 수 있는 여지가 거의 없기 때문에 그러한 요소들이 피해자-가해자 상호작용에 미치는 영향력은 상정하기 어렵다고 하겠다.

제5절 인터넷 중독과 사이버범죄

일반적으로 인터넷은 성인 보다는 청소년들의 생활이나 의식에 많은 영향을 미친다고 알려지고 있다. 청소년들은 입시위주의 교육으로 인해 문화·여가생활을 위한 시간적·정신적 여유를 갖지 못하기 때문에 인터넷은 그들에게 있어 단순한 정보습득의 수단이 아닌 하나의 욕구충족의 공간이 되고 있는 것이다(이종원, 2001).

그러나 인터넷은 성장기에 있는 청소년들에게 종래에 가져왔던 일상생활 패턴의 변화를 초래할 수 있으며, 긍정적·부정적인 영향을 동시에 미칠 수 있다. 우선 긍정적인 측면으로, 청소년들은 인터넷을 이용하여 광범위하게 언어를 사용하고 문제를 해결한다. 인터넷게임의 경우, 그것을 학습자료로 이용해서 공간지각력 내지는 정신적 조작능력의 향상을 도모할 수 있다. 또한 인터넷의 사용은 청소년의 인지발달과 사회적 관계도 확장시켜 나갈 수 있다(정보통신윤리위원회, 2004). 그러나 인터넷은 청소년에게 여러 가지 문제를 야기하기도 하는데, 대표적인 부작용 중의 하나가 인터넷 중독이다.

인터넷 중독 현상은 통상 인터넷 증후군(Internet Syndrome), 웨바홀리즘(Webaholism) 혹은 인터넷 중독장애(IAD: Internet Addiction Disorder) 등의 용어로 표현된다(황상민·한규석, 1999).

Goldberg(1996)는 인터넷 중독이라는 용어를 처음 제안하면서 "인터넷의 과다한 사용으로 현실생활에 지장을 받을 정도의 신체적, 정신적 이상현상을 경험하는 것"으로 정의했다(이종원, 2001:11). 또한 Goldberg는 그 진단기준으로서, 인터넷을 더 많이 사용해야 만족을 느끼게 되는 '내성', 인터넷 사용을 중단하거나 감소하면 나타나는 정신운동성 초조나 불안, 혹은 인터넷에 대한 강박적 사고나 환상과 같은 증상이 일어나는 '금단', 이와 함께 인터넷 사용을 위해서 중요한 사회적·직업적 활동을 포기하는 사태가

발생할 시에 이를 '인터넷 중독증'이라 지칭했다. Kimberly Young(1994)은 정신의학적 약물의존도를 측정하는 도구를 사용하여 인터넷 중독 여부를 조사하였다(이종원, 2001). 그의 연구는 총 8가지의 측정도구[18]를 이용, 이 중에서 5가지를 충족시키는 사람을 인터넷 중독자로 분류하였다.

이러한 것을 종합해 보면, 인터넷 중독이란 과다한 인터넷의 사용과 몰입으로 인하여 현실사회에 투자하는 시간이 줄어들게 되고, 이로 인해 대인관계가 위축되어 사회·경제적인 활동 및 일상생활에서의 장애가 유발되며, 수면부족으로 인한 심각한 신체적 장애, 정동 및 정서장애, 인지왜곡, 과도한 집착, 내성(tolerance) 및 금단(withdrawal symptoms), 자기조절의 실패 등이 나타나는 현상이라 할 수 있다.

그런데 문제는 이러한 인터넷 중독이 그 자체의 부정적 영향과 함께 청소년들의 사이버범죄 및 일탈의 중요한 원인이 될 수 있다는 점이다. 예컨대, 이종원(2001)은 인터넷 중독자는 "자신의 생활을 인터넷에만 국한시켜 사회적으로 고립되고, 기계조작으로 인한 쾌감을 즐기면서 통제력이 약화되고, 사이버 폭력에 무감각해져 현실에서도 폭력적이 되는 등, 정상적인 사회생활을 영위하기 어렵게 되는 것"으로 보았다.[19] 정보통신 인프라가 풍부하고 청소년들의 인터넷 이용이 보편화된 한국의 경우 청소년들의 인터넷 중독은 사이버범죄의 직접적 원인은 아닐지라도 청소년 비행의 중요한 간접 요인으로서 더 이상 간과할 수 없는 심각한 사회문제로 대두되고 있다고 할 것이다.[20]

---

18) 8가지의 측정기준은 다음과 같다: ① 점점 오랜 시간동안 온라인 접속을 해야 직성이 풀린다. ② 인터넷을 접속하지 않았을 때에는 금단증상이 나타난다(초조, 불안, 강박적 사고, 환상이나 꿈, 우울증 등). ③ 의도했던 것 보다 자주 오랫동안 인터넷상에서 장시간을 소모한다. ④ 통신접속을 줄이려 했으나 실패했다. ⑤ 온라인 접속시간을 늘리기 위해 여러 시도를 한다. ⑥ 사회생활, 직장생활 또는 여가활동에 흥미를 상실한다. ⑦ 인터넷 사용 때문에 여러 가지 문제가 생겼거나 더 나빠졌어도 인터넷을 계속 사용한다. ⑧ 인터넷을 사용하지 않을 때에는 빨리 접속해보고 싶은 마음에 사로잡힌다.

19) 또한 정보통신윤리위원회(2004)도 보라.

20) Rauschenberger(1995)는 인터넷 중독자들에게서 정상인들에 비해 훨씬 더 많은 정신병리가 존재한다고 주장하였다.

제3장 인터넷을 이용한 청소년범죄의 주요 유형과 실태

제1절 사이버범죄의 유형과 실태

1. 사이버범죄 유형론

사이버범죄 또는 컴퓨터범죄의 유형을 분류하는 문제에 관해서는 지금까지 다양한 견해가 제시되어 왔으나, 아래에서는 그러한 논의들을 종합하여 크게 세 가지로 나누어 보기로 한다.

먼저, Sieber(1986)는 컴퓨터범죄를 그 피해법익을 기준으로 하여 컴퓨터 관련 경제범죄(컴퓨터조작사기, 컴퓨터스파이, 소프트웨어절도, 컴퓨터사보타지, 컴퓨터의 무권한 사용, 전통적인 경제범죄에의 컴퓨터 이용 등), 개인적 권리에 대한 컴퓨터 관련 범죄(프라이버시 침해 등), 그리고 초개인적 법익에 대한 컴퓨터 관련 범죄(국가전산망 해킹 등)의 세 가지 유형으로 구분하였다. Wasik(1991)은 컴퓨터범죄를 컴퓨터 오용(misuse)이란 맥락에서 정의하고, 위반자에 초점을 두어 컴퓨터 오용의 세 가지 수준을 구분하였다. 첫번째는 법인범죄의 경우로서, 이 경우는 컴퓨터 오용이 회사 정책의 한 중심적 부분이 되며, 회사 내에서 중요한(structural) 직책을 차지하는 사람에 의해서 자행된다. 두번째 수준은 직업범죄의 경우인데, 이것은 회사 컴퓨터의 하드웨어를 훔치거나 사기를 치는 등, 피고용인이 자신의 고용주 또는 회사에 대하여 범죄를 저지르는 경우이다. 세번째 수준은 외부인이 불법적인 액세스 또는 해킹을 통해 사기를 획책하거나 컴퓨터에 저장된 프로그램이나 데이터에 해를 입히는 등의 경우이다.[21] Duff와 Gardiner(1996) 역시 컴퓨터범죄라는 용어를 사용하였으며, 그것을 크게 두 가지 유형으로 구분하였다.

21) 이렇게 세 가지 수준을 구분한 후에 Wasik(1991)은 컴퓨터 오용을 구체적으로 다음의 다섯 가지로 분류하였다: ① 허가 없이 남의 컴퓨터에 액세스 하는 행위, ② 컴퓨터 사기(computer fraud), ③ 허가 없이 남의 자료나 프로그램을 삭제하는 행위, ④ 컴퓨터 시간(computer time) 또는 시설을 허가 없이 사용하는 행위(예컨대, 근무시간에 회사의 컴퓨터를 사용하여 주식거래를 하거나 게임을 하는 등, 타인 소유의 컴퓨터를 허가 없이 사적인 용도로 사용하는 것을 말함), ⑤ 컴퓨터 하드웨어를 파괴하거나 손상시키는 행위.

그들이 사용한 분류기준은 컴퓨터가 범행의 도구(예컨대, 인터넷사기)로서 사용되어졌는가 아니면, 컴퓨터나 시스템 그 자체가 범행의 대상(예컨대, 불법적 액세스, 자료변조·파괴 또는 전용, 바이러스 유포 등)인가 하는 것이다. 이상의 학자들의 견해는 모두 인터넷 사용이 보편화되기 이전에 또는 그 이후에라도 컴퓨터 자체를 수단 내지 대상으로 하는 범죄를 컴퓨터범죄라고 파악하던 시대의 분류기준이라는 점에서 그 유용성을 결여하고 있다고 할 것이다.[22)]

두 번째 유형론은 사이버공간을 이용한 전통적인 범죄군과 사이버공간의 등장으로 새롭게 발생하는 범죄군으로 나누는 입장이다(김종섭, 2000; 양근원, 1999; 허만형, 1999). 전자는 전통적인 범죄행위가 사이버공간이라는 새로운 생활공간에서 행해지는 경우를 말하며, 그 예로서는 인터넷사기, 사이버성희롱, 사이버스토킹, 사이버명예훼손, 사이버협박, 인터넷 음란물 배포 및 판매, 사이버도박, 저작권침해, 사이버테러 등이 있다. 후자는 사이버공간이라는 새로운 생활공간이 등장하면서 비로소 나타나게 된, 전통적 범죄와는 다른 새로운 유형의 범죄를 말하며, 그 예로서는 해킹, 바이러스 제작·유포, 다른 사이트나 홈페이지의 무단복제 등이 있다.

한편 강동범(2000)은 사이버공간의 등장으로 새롭게 발생하는 범죄군을 보다 세분화하여 사이버공간에서의 새로운 범죄유형과 사이버공간에서만 특유한 불법유형으로 이분화하였다. 전자는 위(김종섭, 2000; 양근원, 1999; 허만형, 1999)와 동일하나, 사이버공간에서만 특유한 불법유형으로서는 도메인 주소를 훔치거나 사이버상의 아이템을 훔치거나 사이버캐릭터를 침해하는 행위를 말한다고 하였다. 그는 또한 전자의 사이버범죄는 현실세계와 관련된 것이지만 후자의 사이버범죄는 사이버세계에서만 관계된 것이라고 규정하고 있다. 그러나 현실세계와의 관련성을 따질 때, 현실세계와 전혀 무관한 사이버범죄를 생각하기는 어렵다. 예컨대, 도메인 주소나 게임아이템을 훔치는 행위가 현실세

22) 최근에 Parker(1998)도 이와 유사한 도식을 사용하였다. 그는 사이버범죄라는 용어를 사용하였으나, 이를 정보체계에 대한 지식의 사용을 수반하는 정보 남용(abuse)과 정보 오용(misuse)을 포괄하는 개념으로 채택하였다. 정보남용은 정보에 대하여 행해지는 범죄로서, 그것은 정보가 갖는 유용성, 완전성(integrity), 그리고 확실성을 해치는 것이다. 이에 비해 정보오용은 정보를 이용한 범죄로서, 그것은 정보의 가용성, 소유권, 그리고 비밀성을 상실케 하는 것이다. 그러나 이러한 분류는 그가 구분의 기준으로서 컴퓨터나 네트워크 보다는 지나치게 정보자체를 강조하였기 때문에 사이버범죄 보다도 정보범죄에 더 적합한 것이라고 할 것이다.

계의 이익과 관련되는 경우는 흔히 찾아볼 수 있기 때문이다.

사이버범죄를 분류하는 세 번째 방식은 해킹을 기준으로 하여, 해킹기술을 통해 범행이 구현되는 경우와 해킹기술과 무관한 경우로 구분하는 입장이다(조병인 외, 2000). 해킹기술을 통해 범행이 실행되는 경우로는 사이버스파이, 사이버테러, 폰프리킹, 홈뱅킹사기, 홈페이지훼손 등이 있고, 해킹과 무관한 경우로는 인터넷을 통한 불량정보유통, 판매사기, 저작권침해, 도박사이트운영, 매매춘알선, 명예훼손, 스토킹, 성희롱, 음란사이트운영, 마약밀매, 통신방해, 서비스거부 등이 있다. 해킹기술의 개입 여부에 따라 사이버범죄를 양분하는 이러한 견해는 흥미로운 것이다. 그러나 현실은 그리 간단한 것 같지 않다. 예컨대, 이 견해가 인정하고 있듯이, 해킹기술과 무관한 악성바이러스를 유포하거나 고성능 전자폭탄을 보내는 방법으로 테러목적을 달성하는 경우도 있으며, 해킹기술과 무관한 경우의 예로 든 저작권침해, 명예훼손 등이 해킹에 의하여 일어나는 경우도 있음을 부정할 수 없을 것이다.

이상에서 살펴 본 바와 같이, 사이버범죄의 유형을 분류하는 문제는 결코 간단치 않다. 그것은 아마도 첫째, 사이버범죄의 개념 자체가 아직까지는 모호한 상태로 남아있으며, 둘째, 사이버범죄의 경우 종종 여러 가지 유형들이 결합된 형태로 범해지는 경우가 많으며, 셋째, 지금도 끊임없이 새로운 형태의, 새로운 기술의 사이버범죄가 발견되고 있으며 앞으로도 그러할 것이 기대되기 때문이다. 따라서 사이버범죄에 관한 한 완벽한 분류기준을 찾으려는 노력은 적어도 현재로서는 무모한 짓인지도 모른다.

본 연구에서는 사이버범죄를 아래와 같이 11가지 유형으로 분류하여 그 실태 및 사례들을 살펴보기로 한다.[23]

---

23) 참고로, 미국 법무부의 컴퓨터범죄 및 지적재산 분과(Computer Crime and Intellectual Property Section, CCIPS)는 인터넷 관련 범죄를 다음과 같은 12가지로 분류하고 있다: ① 컴퓨터 침해(해킹 등), ② 패스워드 불법거래, ③ 저작권 침해(소프트웨어, 영화, 음악 등), ④ 업무상 비밀의 절도, ⑤ 상표위조, ⑥ 통화위조, ⑦ 아동포로노그라피 또는 착취, ⑧ 메일연계를 갖는 아동착취 및 인터넷 사기, ⑨ 인터넷 사기, ⑩ 인터넷을 통해 타인을 괴롭히는 행위, ⑪ 인터넷 폭탄 협박, ⑫ 인터넷상에서 폭발물, 무기 등의 불법거래 (출처: http://www.cybercrime.gov/reporting.html). 우리나라 경찰청의 경우는 사이버범죄를 크게 사이버테러형 범죄와 일반사이버범죄로 양분하며, 그에 대한 대응도 이원화되어 있다. 사이버테러범죄는 ① 해킹과 ② 바이러스유포 범죄를 말하고 본청의 사이버테러대응센터(http://www.ctrc.go.kr)가 전담하고 있으며, 일반사이버범죄는 ① 개인정보침해, ② 전자상거래사기, ③ 온라인게임범죄, ④ 불법복제, ⑤ 위법·유해사이트, ⑥ 사이버도박, ⑦ 사이버명예훼손·협박, ⑧ 사이버스토킹·성폭력, ⑨ 음란물유포 등으로 분류하여 각 지방경찰청 사이버수사대가 전담하고 있다. 또한, 우리나라 대검찰청 인터넷범죄수사센터(http://www.icic.sppo.go.kr)는 컴퓨

① 단순 해킹
② 전자상거래 관련 범죄・인터넷사기
③ 사이버성범죄(성희롱, 성폭력, 스토킹, 매매춘 제의, 음란물 송신 등)
④ 허위사실유포・명예훼손
⑤ 사생활유포(몰래카메라 등)
⑥ 인신공격・언어폭력・협박
⑦ 개인신용정보의 도용 또는 도용을 통한 범죄(신용카드, 사이버증권・뱅킹 등)
⑧ 사이버절도(게임아이템 절도 등)
⑨ 전자문서(웹콘텐츠 포함)의 도용・변조・파괴
⑩ 컴퓨터바이러스 유포
⑪ 스팸메일 유포.

물론 이러한 분류가 어떤 확립된 기준에 따라 이루어진 것은 아니다. 그러나 그렇다고 하여 단순히 자의적으로 선정된 것 또한 아니다. 위에서 나열된 유형들은 일차적으로는 인터넷범죄(또는 인터넷을 이용한 사이버범죄)라는 용어로 포괄될 수 있는 것들이다. 다만, 인터넷범죄에도 수 없이 많은 종류의 범죄가 있기 때문에, 본 연구는 그것들 중에서도 개인 인터넷 이용자들이 비교적 빈번히 경험할 수 있는 유형들로 한정한 것이다. 따라서 이상의 11가지 사이버범죄의 유형들을 굳이 앞에서 검토한 유형론(typology)의 기준에서 평가한다면, 두 번째(즉, 사이버공간을 이용한 전통적인 범죄군과 사이버공간의 등장으로 새롭게 발생하는 범죄군으로 나누는 입장)와 세 번째(즉, 해킹기술을 통해 범행이 구현되는 경우와 해킹기술과 무관한 경우로 구분하는 입장)의 논의들이 조합하여 적용될 수 있다고 할 것이다.

터범죄를 그 처벌법규를 중심으로 13가지로 분류・집계하고 있다: ① 공용전자기록손상등, ② 전자문서관련죄, ③ 전산업무방해, ④ 전자기록비밀침해, ⑤ 컴퓨터사용사기, ⑥ 전자기록손괴, ⑦ 정보통신망법상 명예훼손, ⑧ 정보통신망법상 개인정보누설등, ⑨ 정보통신망법상 정보통신망침해등, ⑩정보통신망법상 음란물유포 등, ⑪ 개인정보보호법위반, ⑫ 여신전문금융업법위반, ⑬ 기타.

<표 3-1> 사이버범죄의 분류

	사이버공간을 이용한 전통적 범죄유형	사이버공간에서의 새로운 범죄유형
해킹과 유관한 범죄유형	유형 I : 개인신용정보의 도용	유형 III : 단순해킹 사이버절도(게임아이템 등) 전자문서의 도용・변조・파괴
해킹과 무관한 범죄유형	유형 II : 전자상거래범죄・인터넷사기 사이버성범죄(성희롱・성폭력・스토킹 등) 허위사실유포・명예훼손 사생활유포 인신공격・언어폭력・협박	유형 IV : 컴퓨터바이러스 스팸메일

예컨대, <표 3-1>은 본 연구에서 다룰 11가지 사이버범죄 유형들을 앞의 두 가지 기준을 조합하여 분류해 본 것이다. 먼저, 유형I은 사이버공간을 이용한 전통적 범죄유형들 중에서 해킹기술과 관련 있는 것으로서 개인신용정보 도용에 의한 범죄를 포함한다. 유형II는 사이버공간을 이용한 전통적 범죄유형들 중에서 해킹기술과 무관한 것으로서 전자상거래범죄・인터넷사기, 사이버성범죄, 허위사실유포・명예훼손, 사생활유포, 인신공격・언어폭력・협박을 포함한다. 유형III은 사이버공간의 등장과 함께 새롭게 발생하는 범죄유형들 중에서 해킹기술과 유관한 것으로서 단순 해킹, 사이버절도, 전자문서의 도용・변조・파괴가 이에 해당된다. 마지막으로, 유형IV는 사이버공간에서의 새로운 범죄유형들 중에서 해킹기술과 무관한 것으로서 컴퓨터바이러스와 스팸메일 유포가 이에 해당된다. 그러나 이러한 분류방식은 현재까지의 모든 시도들이 그러하였듯이 어디까지나 시론적인 것이며 계속적인 보완이 필요한 것이다. 이를테면, 해킹기술과 무관한 범죄유형으로 분류된 허위사실유포 및 명예훼손이 해킹과 관련되는 경우도 전혀 없지는 않으며, 해킹과 유관한 것으로 분류된 개인신용정보의 도용이 해킹과 무관하게 이루어지는 경우도 흔히 있다. 또한 컴퓨터바이러스 유포의 경우 대부분이 전자메일을 그 경로로 하기 때문에 해킹과 무관한 범죄유형으로 분류되었으나, 그것 역시 해킹을 전후로 하거나 해킹과 동시에 이루어지는 경우도 있다.

참고로, 사단법인 한국사이버감시단(http://www.wwwcap.or.kr)은 2001년도에 출간한 「한국사이버범죄백서」에서 사이버범죄를 ① 전산망범죄, ② 불건전정보범죄, ③ 영상미디어범죄, ④ 기타 사이버범죄의 네 가지로 대분류한 후, 그것을 다시 14가지로 소분류하였다(<표 3-2> 참조).

<표 3-2> 사단법인 한국사이버감시단의 분류 (출처: 2001 한국사이버범죄백서)

대 분 류	소 분 류	세 부 유 형	
(1) 전산망 범죄	해 킹	전산망해킹 / 개인PC해킹 / 아이디와 비밀번호 도용, 주민등록번호 및 개인신상 해킹 / 인터넷 도·감청 해킹 / 허위 주민등록번호·신용카드번호 제조와 해킹 / 주식·사이버머니 해킹	
	바이러스제작·유포	운영체제별 분류	DOS바이러스 / Windows바이러스 / Linux바이러스 / Palm바이러스 / Unix바이러스
		감염영역별 분류	부트바이러스 / 파일바이러스 / 부트·파일바이러스 / 매크로바이러스
		기타	웜바이러스 / 트로이목마
	개인정보침해	수집 및 침해	이용자의 동의 없이 개인정보를 수집한 경우 등
		이용·제공	제공받은 목적 외로 이용자의 개인정보를 사용한 경우 등
		이용자권리	이용자의 개인정보 삭제요구에 불응한 경우 등
		비밀 등의 보호	타인의 개인정보를 훼손하거나 비밀을 침해·도용·누설한 경우
		스팸메일	원치 않는 영리목적의 광고성 메일을 전송한 경우
	전자상거래범죄	판매사기	통신판매사기 / 경매·역경매사기 / 직거래사기 / 피라미드식 및 다단계판매 / 홈쇼핑 상품도용 및 사기 / 환불·교환지연 및 거부, 불공정행위 / 허위·과장광고 / 무료 인터넷 서비스 사기(경품사기)
		금융사기	인터넷금융피라미드사기 / 인터넷주식·공모사기
(2) 불건전정보 범죄	음란물과 폭력물	음란물의 제작, 유포 및 판매 / 음란홈페이지 및 게시물 / 사이버윤락알선 / 음란성인방송	
	소프트웨어 저작권 침해	불법복제물 유통·판매 / 와레즈사이트 / 메신저프로그램 및 PNP(P2P) / 크랙	
	사이버폭력	사이버스토킹 / 사이버성폭력 / 사이버언어폭력 / 사이버명예훼손 / 허위사실유포 / 악성루머	
	사이버공해	스팸메일 / 스팸성게시물	
(3) 영상미디어 범죄	채 팅	원조교제(청소년성매매) / 언어폭력 / 음란채팅 / 채팅에 의한 오프라인상에서의 범죄	
	온라인게임	아이디 및 아이템절도·사기 / 계정 및 아이템 불법거래 사기 / 온라인게임상의 폭력	
	사이버도박	-	
	인터넷성인방송	-	
(4) 기타사이버 범죄	반사회적 정보제작 및 유포	자살·폭탄사이트 / 반사회적 사이트	
	반사회적 사이버범죄	사이버돈세탁 / 사이버마약거래 / 사이버고리대금 / 사이버선거운동	

2. 공식통계에 나타난 사이버범죄의 실태

우리나라에서 발생하는 사이버범죄의 실태를 파악할 수 대표적인 공식통계로는 경찰청 사이버테러대응센터(CTRC)의 자료, 대검찰청 인터넷범죄수사센터의 자료, 기타 정보통신윤리위원회와 국가정보원의 자료 등이 있다.

1) 경찰자료

경찰청 사이버테러대응센터의 자료에서는 사이버범죄 유형별 발생현황 및 검거현황과 사이버범죄의 연령별 현황을 파악할 수 있다.

(1) 사이버범죄의 유형별 발생현황

<표 3-3>에서 전체 사이버범죄의 발생현황을 살펴보면 2000년도에 2,444건이었던 것이 2003년도에는 68,445건으로 무려 28배나 증가한 것으로 나타났다. 물론 단 3년 만에 사이버범죄가 그렇게 폭증했다고는 볼 수 없을 것이다. 2000년도에 발생건수가 2,444건에 불과하였던 것은 우리사회가 사이버범죄의 문제를 그다지 심각하게 인식하지 않음으로써 신고율이 낮았던 점과 경찰 또한 초기에는 사이버범죄를 적극적으로 단속하지 않았던 탓에 기인한다고 볼 수 있겠지만, 그러한 점을 감안하더라도 여전히 놀라운 증가속도임에는 틀림이 없다. 사이버범죄의 세부 유형별 발생현황을 보면, 해킹의 경우 449건에서 14,159건으로 약 32배, 바이러스는 3건에서 82건으로 약 27배, 일반사이버범죄는 1,992건에서 54,204건으로 역시 약 27배 증가한 것으로 나타났다.

한편 2003년도의 경우 전체 68,445건에서 일반사이버범죄[24]가 79%를 차지하였으며, 그 다음은 해킹이 20%, 그리고 바이러스가 채 1%가 안돼는 정도의 비율을 보였다.

24) '일반사이버범죄'란 사이버 공간을 이용한 일반적인 불법행위로서 사이버도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보유출 등의 사이버범죄를 말한다.

<표 3-3> 사이버범죄 유형별 발생현황(단위: 건)

구 분	해 킹	바이러스	일반 사이버범죄	계
2000년	449	3	1,992	2,444
2001년	10,562	112	22,651	33,325
2002년	14,065	94	45,909	60,068
2003년	14,159	82	54,204	68,445

(출처: 경찰청 사이버테러대응센터)

(2) 사이버범죄의 유형별 검거현황

경찰청 사이버테러대응센터에서 발표한 사이버범죄의 유형별 검거인원을 살펴보면, 2003년도의 경우 전체 51,722건으로 56,724명의 사이버범죄자를 검거하였는바, 이는 2003년도 전체 발생건수 68,445건의 75.6%에 해당하는 수치이다.

<표 3-4>에서 세부유형별 검거현황을 살펴보면, 해킹의 경우 2003년도에 8,844건으로 9,992명 검거, 바이러스는 47건으로 55명, 일반사이버범죄는 42,831건으로 46,677명을 검거한 것으로 나타났다.

<표 3-4> 사이버범죄 유형별 검거현황(단위: 건(명))

구 분	해 킹	바이러스	일반 사이버범죄	계
2000년	275(360)	3(3)	1,437(1,827)	1,715(2,190)
2001년	7,512(8,004)	83(95)	15,098(16,356)	22,693(24,455)
2002년	9,650(10,689)	57(73)	32,193(36,490)	41,900(47,252)
2003년	8,844(9,992)	47(55)	42,831(46,677)	51,722(56,724)

(출처: 경찰청 사이버테러대응센터)

(3) 연령별 사이버범죄 현황

<표 3-5>과 <그림 3-1>은 연령별 사이버범죄 현황을 나타낸 것으로 10~20대의 범죄율이 가장 높다는 사이버범죄의 특징을 단적으로 보여주고 있다. 2001년도와 2002년도의 경우 10대는 각각 전체의 43.4%와 37.6%로 가장 높은 구성비를 보여주었다. 그리고 2003년

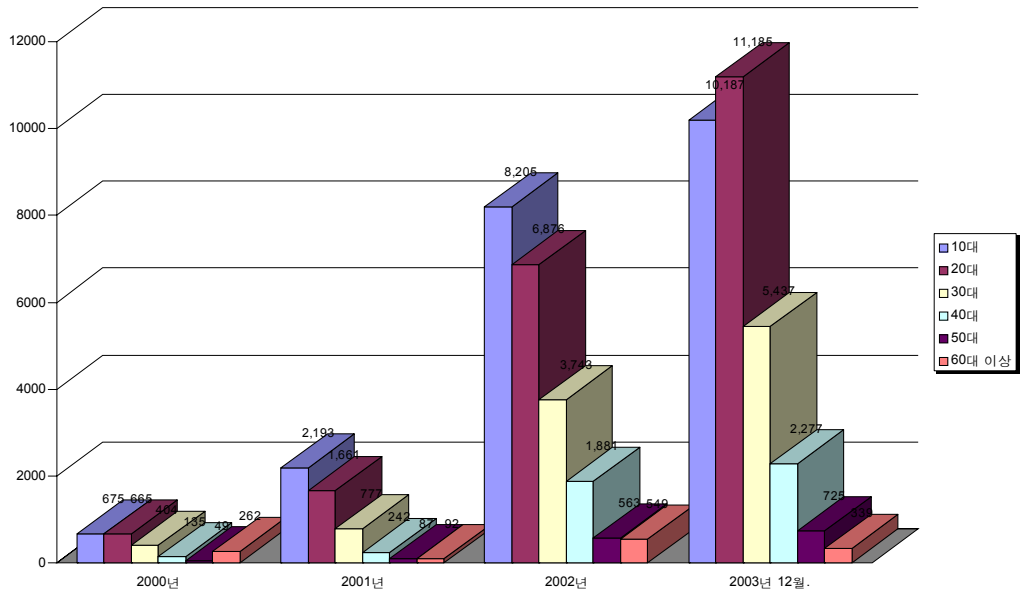
도 12월 현재의 경우에도 비록 20대가 가장 높은 비율을 보이고 있기는 하지만, 10대 또한 10,187명으로 전체의 33.8%에 해당하는 높은 비율을 차지하고 있다. 이러한 점은 사이버범죄의 경우 10대의 범죄율이 오프라인 범죄에 비하여 월등히 높다는 것을 말해준다.

<표 3-5> 연령별 사이버범죄 현황

구 분	10대	20대	30대	40대	50대	60대 이상	계
2000년	675	665	404	135	49	262	2,190
2001년	2,193	1,661	777	242	87	92	5,052
2002년	8,205	6,876	3,743	1,881	563	549	21,817
2003년 12월	10,187	11,185	5,437	2,277	725	339	30,150

(출처 : 경찰청 사이버테러대응센터: 단위및<표 3-4>와의 수치상 차이는 미상)

<그림 3-1> 연령별 사이버범죄 현황



2) 검찰자료

검찰자료는 대검찰청 인터넷범죄수사센터에서 제공하고 있으며, 컴퓨터범죄의 연도별 처리현황 및 연령별 현황에 관해 이용가능하다. 검찰은 1997 - 2003년도까지의 연도별 컴퓨터범죄 처리현황을 공용전자기록손상등, 전자문서관련죄, 전산업무방해, 전자기록비밀침해, 컴퓨터사용사기, 전자기록손괴, 정보통신망법, 개인정보보호법 등으로 구분하여 제시하고 있다.

(1) 연도별 컴퓨터범죄 처리현황

① 공용전자기록손상 등

<표 3-6>은 공용전자기록손상 등에 관한 범죄 처리현황을 보여준다. 공용전자기록손상등과 관련된 범죄는 1997년 집계가 시작된 이래 2002년까지 발생하지 않았으나, 2003년도에 와서 처음으로 2건(피의자 4명)이 집계되었다.

<표 3-6> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 공용전자기록손상등

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	0	0	0
1998	0	0	0
1999	0	0	0
2000	0	0	0
2001	0	0	0
2002	0	0	0
2003	2	4	0
계	**2**	**4**	**0**

(출처: 대검찰청 인터넷범죄수사센터)

② 전자문서관련죄

전자문서관련죄에 해당하는 범죄(<표 3-7>과 <그림 3-2>)는 1997년부터 지속적으로 증가하여 2002년도의 경우 241건, 2003년도에는 516건이 발생하였다. 특히 2001년 이후에는 범죄 처리건수 및 피의자수, 구속자수가 2~3배 이상 폭등하는 양상을 보이고

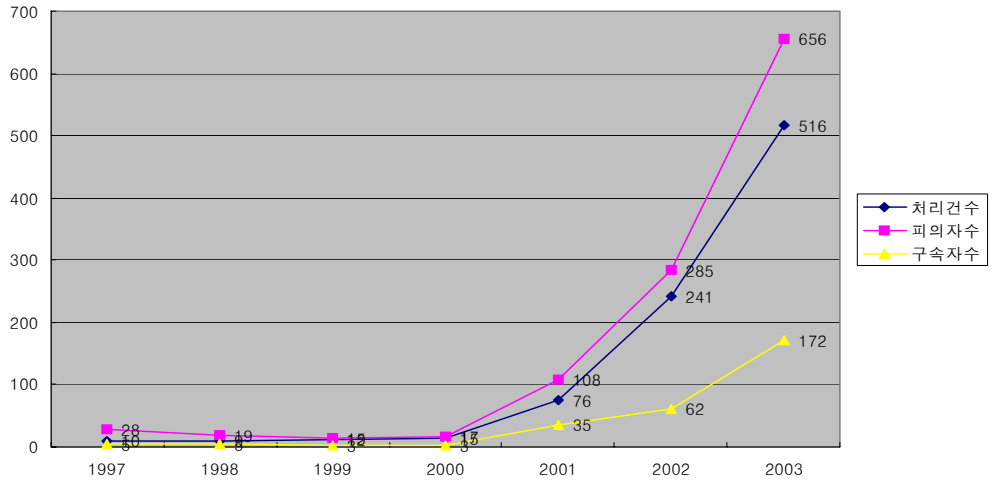
있어 향후 지속적인 증가가 예상되는 범죄유형이다. 이와 같은 양상은 전자정부의 구현 및 각종 전자상거래의 확대 및 그로 인한 전자문서의 사용 증가로 인해 발생하는 현상이라 유추할 수 있다.

<표 3-7> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 전자문서관련죄

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	10	28	5
1998	9	19	5
1999	12	15	3
2000	15	17	3
2001	76	108	35
2002	241	285	62
2003	516	656	172
계	**879**	**1,128**	**285**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-2> 연도별 컴퓨터범죄 처리현황 - 전자문서관련죄



③ 전산업무방해

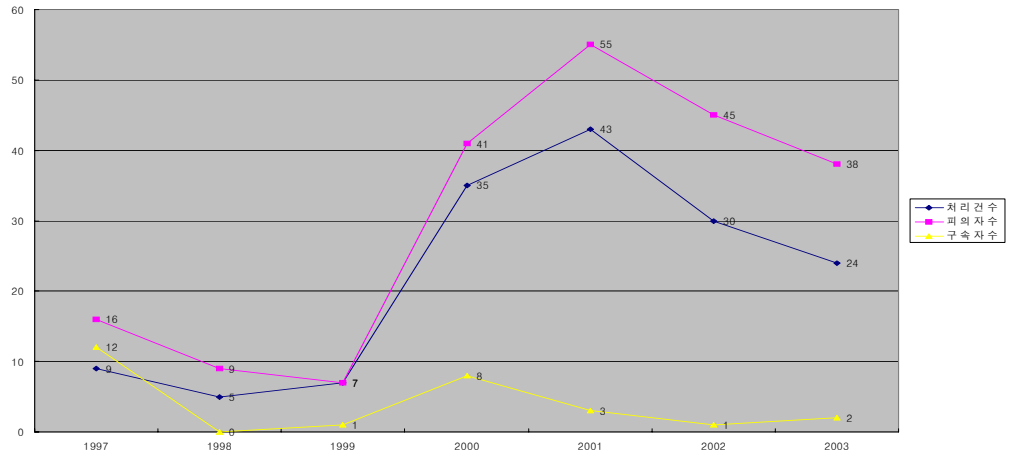
<표 3-8>과 <그림 3-3>에서 알 수 있는 바와 같이 전산업무방해는 증가일변도인 他컴퓨터범죄와는 달리 2001년의 43건을 기점으로 2002년도 30건, 2003년도 24건으로 점차 감소하는 경향을 보이고 있다. 이러한 변화는 공공기관과 기업체, 또는 개인에 있어서 최근의 보안의식의 강화 추세와도 관련 있는 것이라 생각된다. 또한 처리건수나 피의자 숫자에 비하여 구속자 숫자가 적은 것이 특징적인데, 이는 전산업무방해가 주로 경미한 수준에서 발생하고 있는 것을 시사하는 것이라 하겠다.

<표 3-8> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 전산업무방해

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	9	16	12
1998	5	9	0
1999	7	7	1
2000	35	41	8
2001	43	55	3
2002	30	45	1
2003	24	38	2
계	**153**	**211**	**27**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-3> 연도별 컴퓨터범죄 처리현황 - 전산업무방해



④ 전자기록비밀침해

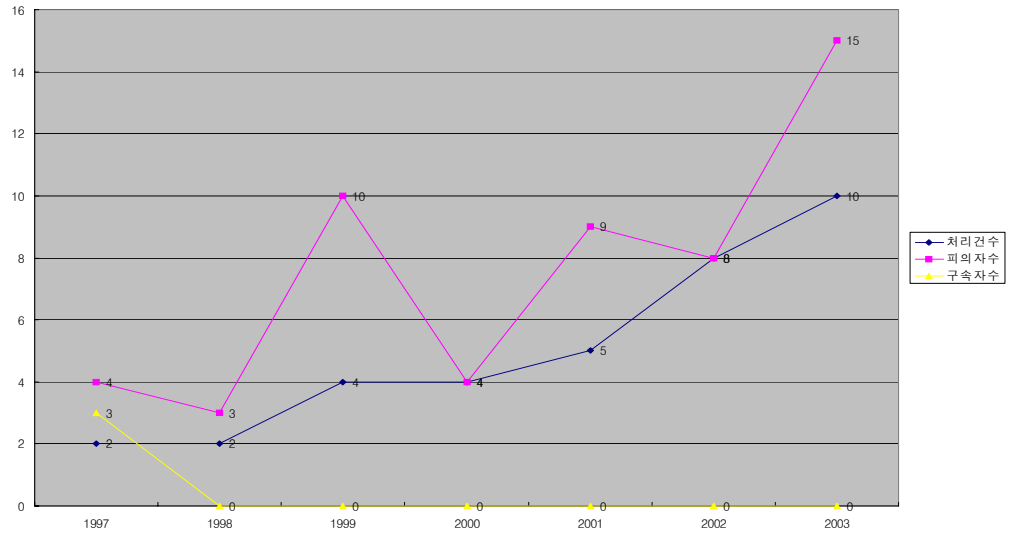
전자기록비밀침해 또한 발생률이 낮은 형태의 컴퓨터범죄이다. 비록 1998년도 이후 발생빈도가 증가하고는 있지만, 처리건수가 10건 미만이며 구속자수 또한 1998년도 이후에는 한명도 없어 매우 드물게 나타나는 범죄유형이라 할 수 있다(<표 3-9>와 <그림 3-4>).

<표 3-9> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 전자기록비밀침해

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	2	4	3
1998	2	3	0
1999	4	10	0
2000	4	4	0
2001	5	9	0
2002	8	8	0
2003	10	15	0
계	35	53	3

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-4> 연도별 컴퓨터범죄 처리현황 - 전자기록비밀침해



⑤ 컴퓨터사용사기

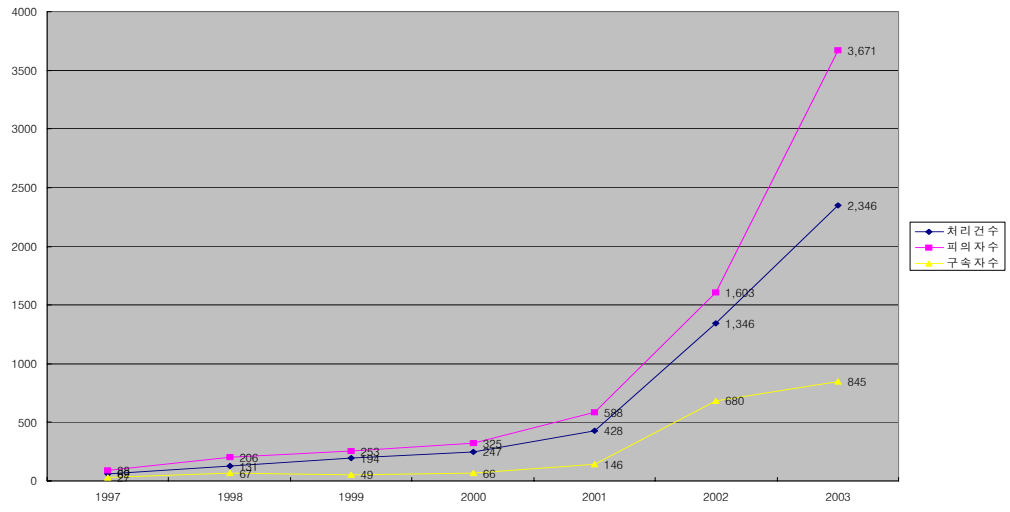
컴퓨터사용사기는 최근에 그 발생건수가 폭발적으로 증가하고 있는 범죄유형이다. <표 3-10>과 <그림 3-5>를 보면, 1997년에 62건이던 처리건수가 2003년도에는 무려 38배인 2,346건으로 증가하였다. 특히 2002년도에 구속자수가 전년도에 비해 약 4.7배나 증가한 것은 놀라운 일이며, 이는 사이버범죄 특히 컴퓨터사용사기범죄에 대한 검찰의 엄벌주의 정책을 반영한 것으로 보인다.

<표 3-10> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 컴퓨터사용사기

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	62	88	27
1998	131	206	67
1999	194	253	49
2000	247	325	66
2001	428	588	146
2002	1,346	1,603	680
2003	2,346	2,671	845
계	**4,754**	**5,734**	**1,880**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-5> 연도별 컴퓨터범죄 처리현황 - 컴퓨터사용사기



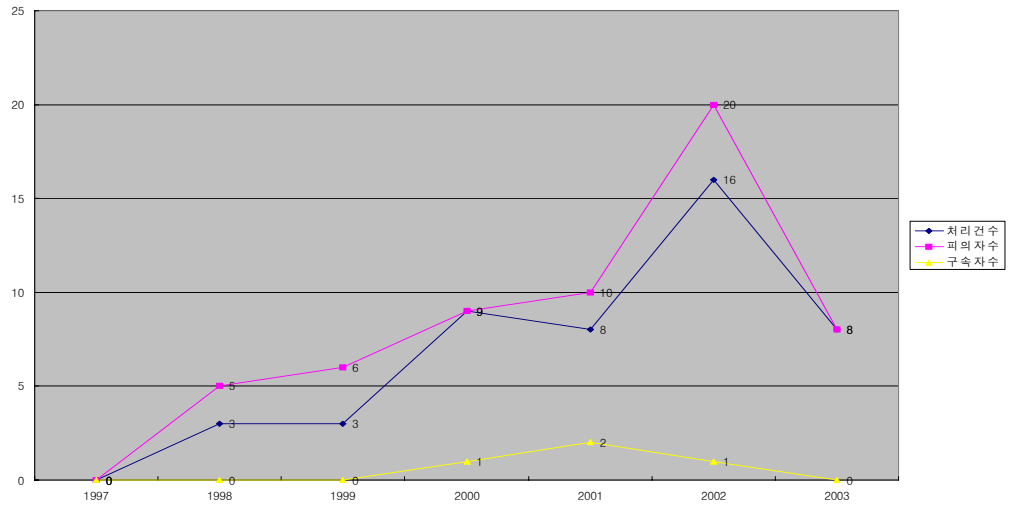
⑥ 전자기록손괴

전자기록손괴는 <표 3-11>과 <그림 3-6>에서 보는 바와 같이 2000년도 이후에는, 2002년도를 제외하고는, 거의 같은 발생건수를 보이고 있으며, 구속자도 거의 발생하지 않고 있다.

<표 3-11> 연도별 컴퓨터범죄 처리현황 - 전자기록손괴

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	0	0	0
1998	3	5	0
1999	3	6	0
2000	9	9	1
2001	8	10	2
2002	16	20	1
2003	8	8	0
계	47	58	4

<그림 3-6> 연도별 컴퓨터범죄 처리현황 - 전자기록손괴



⑦ 정보통신망법

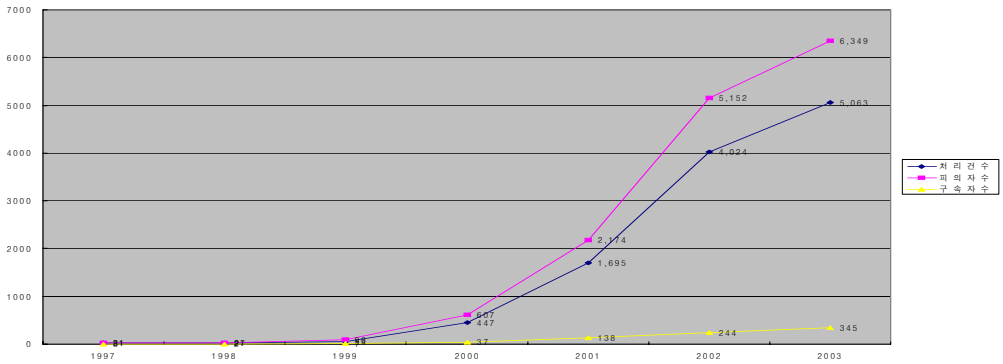
앞서 언급한 컴퓨터사용 사기와 더불어 정보통신망법 위반은 2001년 이후 급증하고 있는 범죄 유형으로 컴퓨터범죄에 있어서 가장 큰 비중을 차지하는 범죄유형이다. <표 3-12>와 <그림 3-7>에서 볼 수 있는 바와 같이 정보통신망법 위반건수는 2000년을 기점으로 대폭 상승하였다. 1999년도에 54건에 불과하던 처리건수는 이듬해인 2000년도에 447건, 2001년도에는 1,695건, 2002년도에는 4,024건, 2003년도에는 5,063건으로 지속적으로 크게 증가하는 추세를 보이고 있다. 또한 피의자수 대비 구속자수의 비율도 비교적 높게 나타나고 있다. 이러한 경향은 정보통신망법에 저촉되는 범죄유형인 해킹, 바이러스 및 스팸메일 유포 등의 행위들이 일상적으로 발생하고 있으며, 그에 대한 형사사법기관의 대응 역시 강화되고 있는 추세를 보여주는 것이라 하겠다.

<표 3-12> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 정보통신망법

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	21	31	5
1998	21	27	2
1999	54	96	7
2000	447	607	37
2001	1,695	2,174	138
2002	4,024	5,152	244
2003	5,063	6,349	345
계	**11,325**	**14,436**	**778**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-7> 연도별 컴퓨터범죄 처리현황 - 정보통신망법



⑧ 개인정보보호법

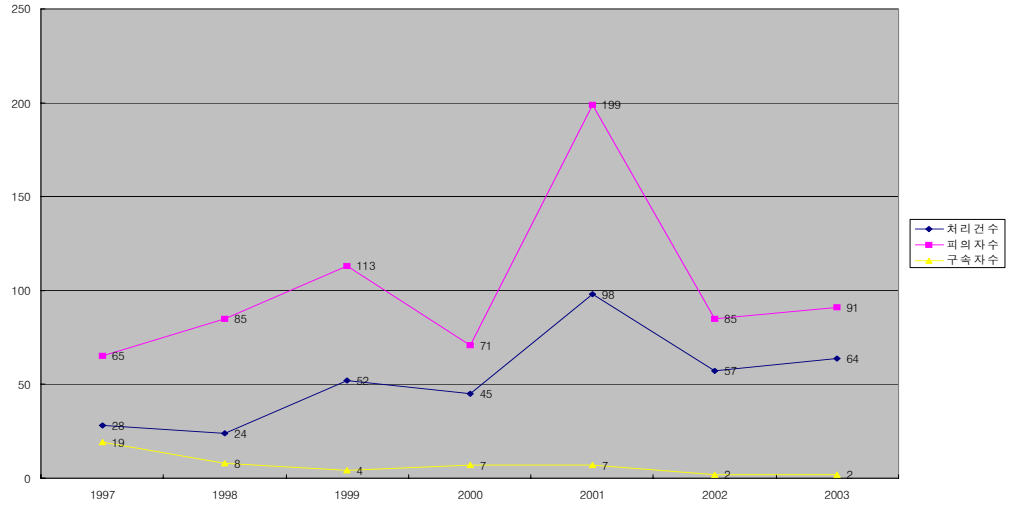
개인정보보호법 위반 범죄는 주로 개인의 정보를 무단으로 도용하는 경우이다. <표 3-13>과 <그림 3-8>에서 그 처리건수를 보면, 2000년 45건에서 2001년 98건으로 2배 이상 급등하는 양상을 보이기는 했으나, 2002년도에는 다시 57건으로 감소하였으며, 전체적으로 큰 변화를 보이지는 않고 있다. 오히려 구속자수는 1997년 이후 지속적으로 감소하는 현상을 나타내고 있다.

<표 3-13> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 개인정보보호법

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	28	65	19
1998	24	85	8
1999	52	113	4
2000	45	71	7
2001	98	199	7
2002	57	85	2
2003	64	91	2
계	**368**	**709**	**49**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-8> 연도별 컴퓨터범죄 처리현황 - 개인정보보호법



⑨ 연도별 전체 컴퓨터범죄 처리현황

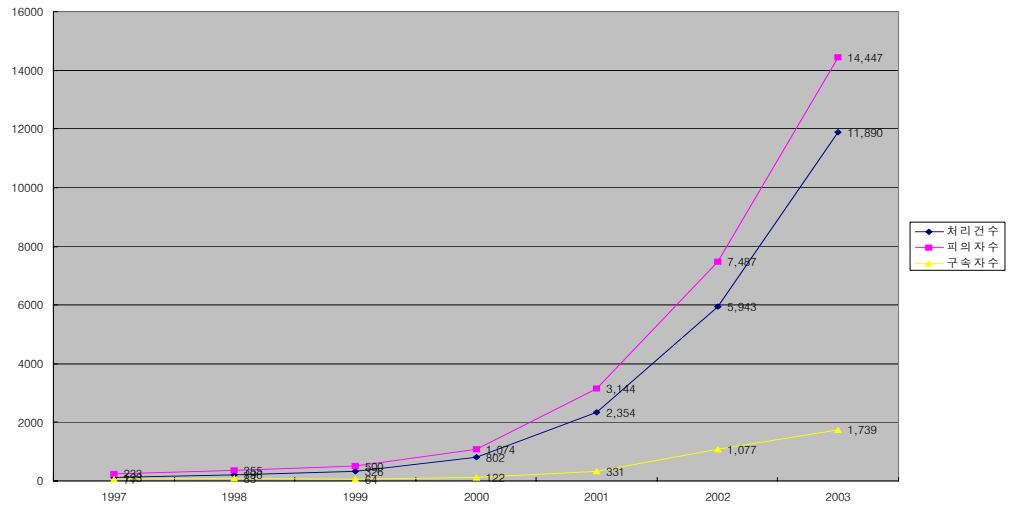
<표 3-11>에서 보는 바와 같이 컴퓨터범죄는 1997년 이후 급속히 증가하고 있다. 특히 2000년대에 접어들어 인터넷 사용이 보편화되면서 2000년도의 802건 이후 2001년도에는 2,354건, 2002년도에는 5,943건, 2003년도는 11,890건으로 매년 대폭 상승하고 있다. 또한 구속자 숫자도 2002년도에 1000명을 돌파한 이래 2003년도에는 1,739명으로 크게 증가하고 있다.

<표 3-14> 연도별 컴퓨터범죄 처리현황(1997 - 2003) - 전체

구 분	처 리 건 수	피 의 자 수	구 속 자 수
1997	133	233	71
1998	196	355	83
1999	326	500	64
2000	802	1,074	122
2001	2,354	3,144	331
2002	5,943	7,487	1,007
2003	11,890	14,447	1,739
계	**21,644**	**27,240**	**3,417**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-9> 연도별 컴퓨터범죄 처리현황 - 전체



(2) 연령별 컴퓨터범죄 처리현황

① 공용전자기록손상등

2003년에 검찰이 공용전자기록손상등과 관련해 처리한 컴퓨터범죄는 단 2건에 불과하며, 구속자도 없는 것으로 나타났다. 피의자도 20대와 40대가 각 2명으로써, 이 유형의 범죄는 청소년이라는 지위와는 직접적인 관련이 없는 것으로 보인다(<표 3-15>).

<표 3-15> 연령별 컴퓨터범죄 처리현황(2003년도) - 공용전자기록손상등

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	0	0	0
30세미만	1	2	0
40세미만	0	0	0
50세미만	1	2	0
50세이상	0	0	0
계	**2**	**4**	**0**

(출처: 대검찰청 인터넷범죄수사센터)

② 전자문서관련죄

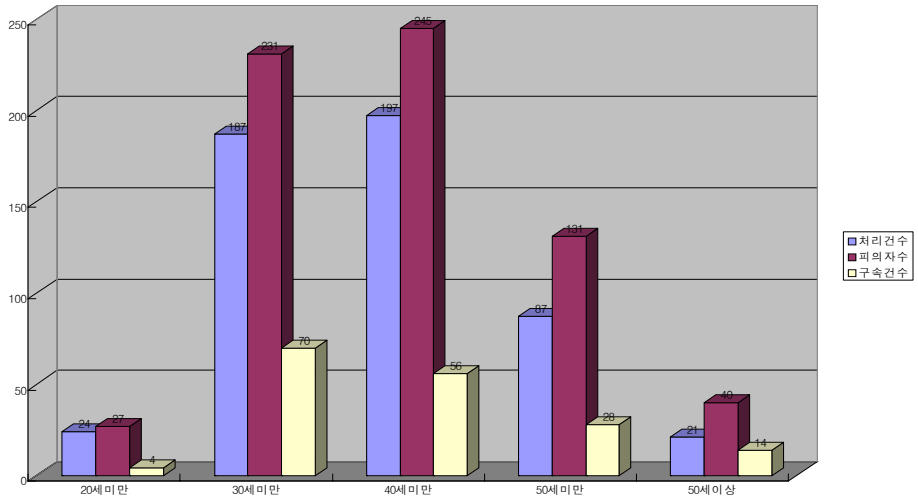
<표 3-16>과 <그림 3-10>에서 볼 수 있는 바와 같이, 2003년도에 전자문서관련죄의 처리건수는 총 516건이며 구속자수는 172명에 이르고 있다. 연령별 분포를 보면, 가장 큰 비중을 차지하는 연령대는 20대와 30대로서 전체 처리건수의 약 74%를 차지하고 있다. 10대 청소년의 경우 50세 이상 연령대 범죄자와 더불어 가장 낮은 비율을 보임으로써, 이 유형의 범죄는 청소년과는 관련성이 낮은 것임을 알 수 있다.

<표 3-16> 연령별 컴퓨터범죄 처리현황(2003년도) - 전자문서관련죄

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	24	27	4
30세미만	187	231	70
40세미만	197	245	56
50세미만	87	113	28
50세이상	21	40	14
계	**516**	**656**	**172**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-10> 연령별 컴퓨터범죄 처리현황(2003년도) - 전자문서관련죄



③ 전산업무방해

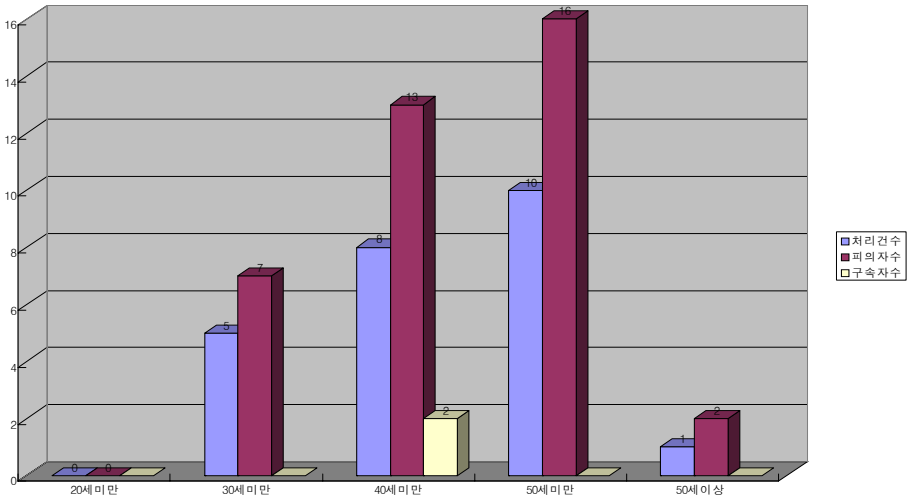
전산업무방해범죄는 2003년도에 총 24건이 처리되었으며, 이 중에서 40대와 30대가 차지하는 비율이 18건(75%)으로서 대부분이다. 그러므로 전산업무방해는 주로 30~40대가 많이 저지르는 범죄유형임을 알 수 있다. 구속자 2명은 모두 30대에서 나왔으며, 10대 청소년의 경우 전산업무방해로 처리된 경우는 한건도 없다(<표 3-17>, <그림 3-11>).

<표 3-17> 컴퓨터범죄 연령별 현황(2003년도) - 전산업무방해

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	0	0	0
30세미만	5	7	0
40세미만	8	13	2
50세미만	10	16	0
50세이상	1	2	0
계	**24**	**38**	**2**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-11> 컴퓨터범죄 연령별 현황(2003년도) - 전산업무방해



④ 전자기록비밀침해

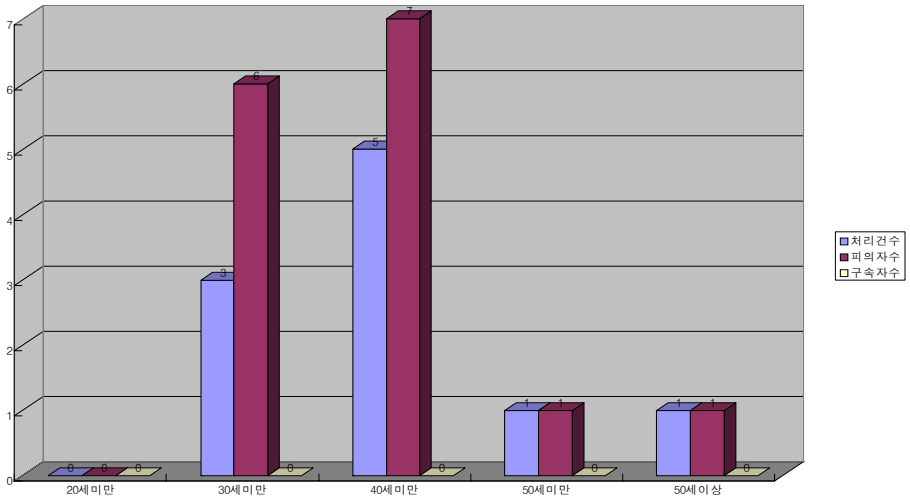
전자기록비밀침해도 2003년도에 총 10건이 발생하여 발생빈도가 많지 않은 컴퓨터범죄 유형이다. 이 범죄는 <표 3-18>에서 보는 바와 같이 주로 20, 30대에서 많이 발생하고 있으며, 10대 청소년의 경우 한 건도 없다. 피구속자도 한 사람도 없다.

<표 3-18> 컴퓨터범죄 연령별 현황(2003년도) - 전자기록비밀침해

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	0	0	0
30세미만	3	6	0
40세미만	5	7	0
50세미만	1	1	0
50세이상	1	1	0
계	**10**	**15**	**0**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-12> 컴퓨터범죄 연령별 현황(2003년도) - 전자기록비밀침해



⑤ 컴퓨터사용사기

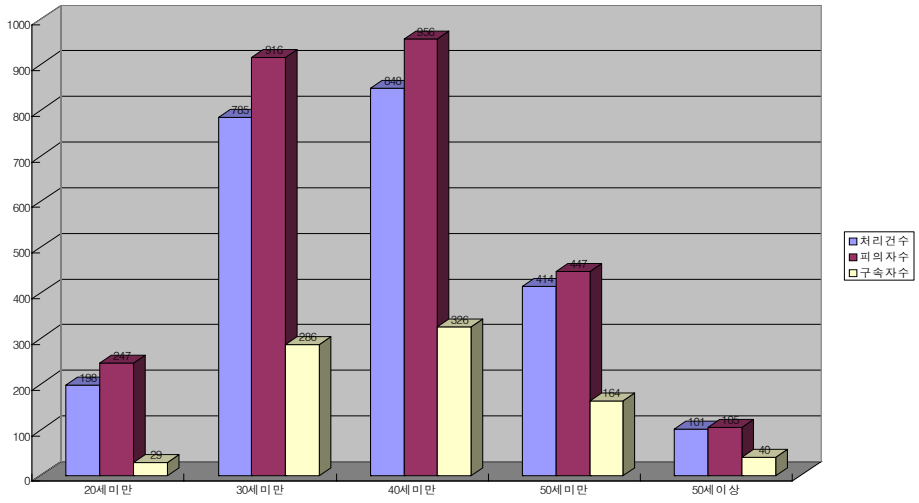
컴퓨터사용사기도 20-30대가 많이 저지르는 사이버범죄이나, 타 범죄에 비해 비교적 다양한 연령층에서 발생하고 있으며, 청소년들도 상대적으로 빈번히 범하는 범죄유형이다. <표 3-19>에서 30대는 전체 처리건수의 약 36%(848건)를 차지하였고, 20대는 전체의 33.4%(785건)을 차지하였다. 10대 청소년의 경우 피의자수가 247명으로 전체의 약 9.2%를 차지하고 있으나, 구속자수는 29명으로서 3.4%에 불과하다. 이는 곧 청소년 사범의 경우 성인사범에 비해 형사사법기관으로부터 관대한 처분을 받는 경향이 있음을 의미하는 것이다.

<표 3-19> 컴퓨터범죄 연령별 현황(2003년도) - 컴퓨터사용사기

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	198	247	29
30세미만	785	916	286
40세미만	848	956	326
50세미만	414	447	164
50세이상	101	105	40
계	**2,346**	**2,671**	**845**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-13> 컴퓨터범죄 연령별 현황(2003년도) - 컴퓨터사용사기



⑥ 전자기록 손괴

전자기록손괴의 경우도 전체 처리건수가 8건에 불과하며, 주로 20 - 30대에 의해서 범해지고 있다. 10대 청소년들의 경우 한건도 없다(<표 3-20>).

<표 3-20> 컴퓨터범죄 연령별 현황(2003년도) - 전자기록손괴

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	0	0	0
30세미만	3	3	0
40세미만	4	4	0
50세미만	1	1	0
50세이상	0	0	0
계	**8**	**8**	**0**

(출처: 대검찰청 인터넷범죄수사센터)

⑦ 정보통신망법

2003년도에 정보통신망법 위반 범죄의 전체 처리건수는 5,063건이며, 이 중에서 10대 청

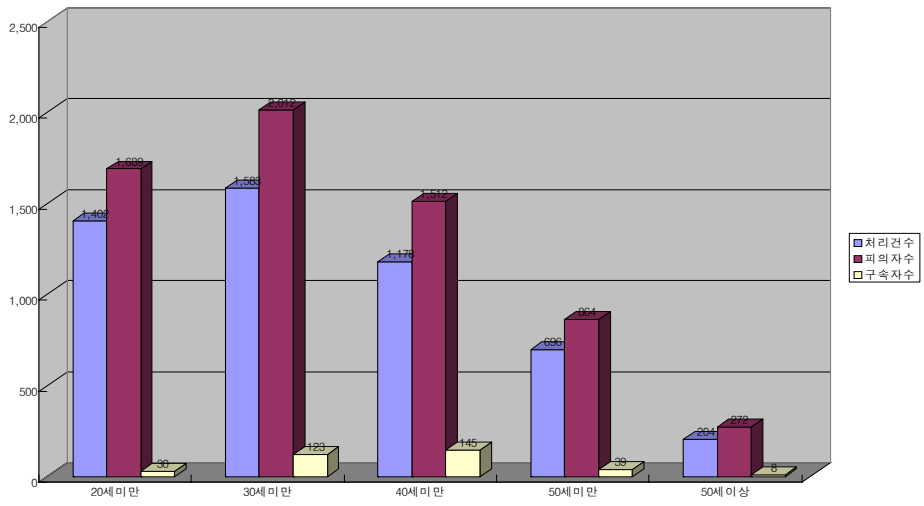
소년들이 차지하는 비중은 20대(31.3%) 다음으로 높은 27.7%(1,402건)이다. 하지만 10대의 경우 피의자수 대비 구속자수의 비율은 상대적으로 낮아서 1.8%에 불과하다. 이 비율은 40대의 9.6%나 30대의 6.1%에 비교하면 크게 낮은 수치이다(<표 3-21>과 <그림 3-14>).

<표 3-21> 컴퓨터범죄 연령별 현황(2003년도) - 정보통신망법

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	1,402	1,689	30
30세미만	1,583	2,012	123
40세미만	1,178	1,512	145
50세미만	696	864	39
50세이상	204	272	8
계	**5,063**	**6,349**	**345**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-14> 컴퓨터범죄 연령별 현황(2003년도) - 정보통신망법



⑧ 개인정보보호법

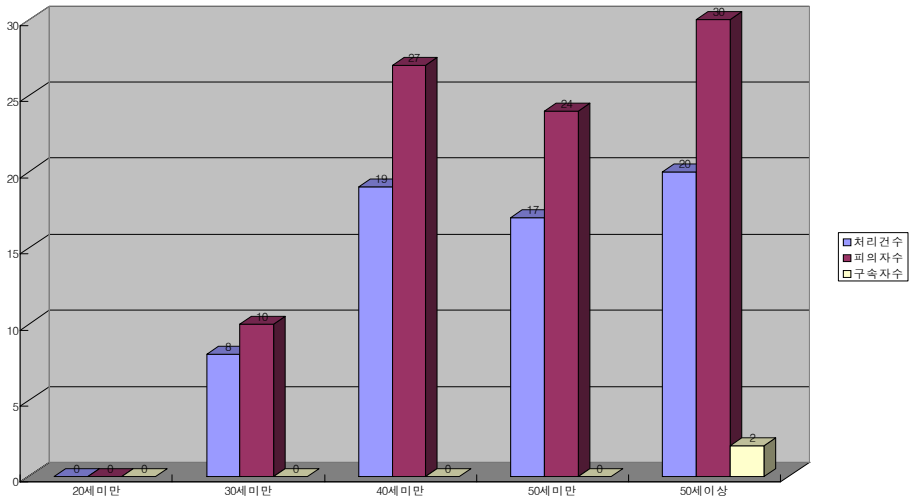
개인정보보호법 위반 범죄는 특이하게도 20대 이상에서 연령대가 증가할수록 처리건수 및 피의자수도 증가하는 양상을 보인다. 이 범죄유형과 관련한 10대 청소년피의자는 1명도 없는 것으로 나타났다. 이러한 점은 개인정보보호법 위반이 주로 개인적 차원에서 일어나는 범죄가 아니라 기업적, 상업적 차원에서 일어나는 경향이 있음을 보여주는 것이라 하겠다(<표 3-22>과 <그림 3-15>).

<표 3-22> 컴퓨터범죄 연령별 현황(2003년도) - 개인정보보호법

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	0	0	0
30세미만	8	10	0
40세미만	19	27	0
50세미만	17	24	0
50세이상	20	30	2
계	64	91	2

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-15> 컴퓨터범죄 연령별 현황(2003년도) - 개인정보보호법



⑨ 전체 컴퓨터범죄 연령별 현황

<표 3-23>은 앞에서 본 컴퓨터범죄 유형별 연령분포를 합한 것이다. 2003년도의 경우 전체 11,890건의 컴퓨터범죄가 발생하였으며, 구속자수도 1,739명에 달하고 있다. 이 자료에 의하면 컴퓨터범죄를 가장 많이 범하는 연령대는 20대로서 전체의 33.9%(4,032건)를 차지하며, 그 다음은 10대가 25.5%(3,032), 30대가 24.1%(2,871)인 것으로 나타났다. 다만 10대의 경우 피의자수 대비 구속자수는 타 연령대에 비해 현저하게 낮아서 5.2%에 불과하였다. 이러한 비율은 30대의 17.2%나 20대의 12.8%에 비하면 크게 낮은 수치이며, 이는 곧 소년사범에 대한 형사사법기관의 관대한 처분 경향을 보여주는 것이라 하겠다.

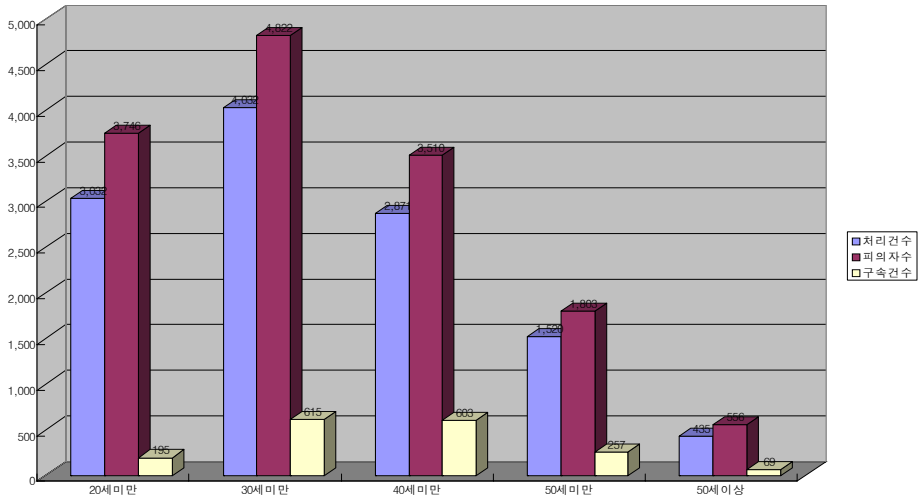
이상에서 우리는 사이버범죄의 현황에 대한 경찰 및 검찰의 공식통계자료를 검토하였다. 우리사회에서 발생하는 사이버범죄의 총량에 대한 두 형사사법기관의 통계자료는 상당한 편차가 있으나 이는 사이버범죄의 경우 상당량이 청소년들에 의해 저질러지는 것이어서 경찰단계에서 훈방조치 되는 등 검찰에 송치되지 않는 경향이 많기 때문으로 당연한 것이라고 하겠다. 연령별 분포 또한 경찰과 검찰의 자료간에 다소의 차이가 있으나, 10대 청소년의 비율이 20 - 30대에 못지않게 높게 나타나고 있다는 점에서는 동일하다.

<표 3-23> 컴퓨터범죄 연령별 현황(2003년도) - 전체

구 분	처 리 건 수	피 의 자 수	구 속 자 수
20세미만	3,032	3,752	195
30세미만	4,032	4,822	615
40세미만	2,871	3,510	603
50세미만	1,520	1,803	257
50세이상	435	560	69
계	**11,890**	**14,447**	**1,739**

(출처: 대검찰청 인터넷범죄수사센터)

<그림 3-16> 컴퓨터범죄 연령별 현황(2003년도) - 전체



3) 기 타

(1) 정보통신윤리위원회

정보통신윤리위원회(http://www.icec.or.kr)는 전기통신사업법 제53조의2에 근거하여 설립된 정보통신부 산하 기관으로서, 불법통신의 근절 및 건전정보유통의 활성화를 위해 전기통신회선을 통하여 일반에게 공개를 목적으로 유통시키는 정보에 대한 심의 및 시정요구를 하고 있다. 따라서 정보통신윤리위원회가 제공하는 통계자료는 경찰이나 검찰이 제공하는 자료와는 그 성격이 다른 것이다.

2003년도에 불법·청소년유해정보에 대한 정보통신윤리위원회의 심의건수는 79,134건으로 전년도의 32,221건에 비해 약 2.5배 증가하였다. 시정요구건수도 전년도에 비해서 63% 증가하였으나, 심의건수 대비 시정요구건수의 비율은 과거 연도에 비해 오히려 크게 감소한 것으로 나타났다. 이는 과거에 비해 불법유해 정보에 대한 심의를 보다 적극적이고 광범위하게 한 결과로 볼 수 있을 것이다.

<표 3-24> 불법·청소년유해정보에 대한 심의·시정요구 실적(1995 - 2003)

(단위 : 건)

구 분	1995	1996	1997	1998	1999	2000	2001	2002	2003	합 계
심 의	2,032	5,655	14,016	17,108	29,607	23,477	25,210	32,221	79,134	228,460
시정요구	598	2,137	6,346	12,682	19,729	15,440	21,502	11,033	18,031	107,498

(출처:정보통신윤리위원회, 「2003 정보통신윤리백서」, 정보통신윤리위원회, 2004. p.121.)

정보통신윤리위원회는 불법·청소년유해정보신고센터를 설치하여 일반 정보이용자들로 구성되는 '사이버패트롤'을 운영, 불건전정보에 대한 적극적인 신고를 유도하고 있다. 또한 네티즌들의 신고를 간편화하기 위해 불건전정보 자동신고 프로그램인 「인터넷 파랑새」를 보급·권장하고 있으며, 핫라인 실무협의회 운영을 통해 사법기관·수사기관 등과의 수시협조 체제를 구축하고 있다.

이러한 제도적인 운영을 통하여 2003년도에 불법·청소년유해정보신고센터로 신고된 정보는 음란, 37,751건(51.4%), 명예훼손 806건(1.1%), 폭력·잔혹·혐오 448건(0.6%), 사행심조장 966건(1.3%), 사회질서위반 5,733건(7.9%), 그리고 비심의대상 27,767건(37.8%)으로 나타났다.

<표 3-25> 불법·청소년유해정보신고센터 신고현황(2002 - 2003)

(단위 : 건)

구 분	음 란	명예훼손	폭력·잔혹·혐오	사행심조장	사회질서위반	비심의대상	합 계
2002	9,326	96	765	240	5,673	2,167	18,267
2003	37,751	806	448	966	5,733	27,767	73,511

(출처:정보통신윤리위원회, 「2003 정보통신윤리백서」, 정보통신윤리위원회, 2004. p.125.)

한편 정보통신윤리위원회는 <표 3-26>에서 보는 바와 같이 신고와 자체인지 등으로 심의한 유해정보들에 대하여 청소년유해매체물로 결정하고, 이를 청소년보호위원회를 통해 고시 요청하고 있다. 청소년유해매체물의 결정 고시는 1997년부터 시작하였으며, 2003년 12월말 현재 6,287건이 결정되었고, 504건이 결정취소 되었다.

<표 3-26> 청소년유해매체물 결정 및 고시 추진현황(1997 - 2003)

(단위 : 건)

구 분	청소년유해매체물		매 체 별			
			인 터 넷		PC 통 신	
	결 정	취 소	결 정	취 소	결 정	취 소
1997	607	0	0	0	607	0
1998	755	0	0	0	755	0
1999	69	5	13	0	56	5
2000	95	0	42	0	53	0
2001	400	14	393	14	7	0
2002	816	470	816	35	0	435
2003	3,524	13	3,524	13	0	0
합 계	**6,287**	**504**	**1,440**	**504**	**1,478**	**440**

(출처:정보통신윤리위원회, 「2003 정보통신윤리백서」, 정보통신윤리위원회, 2004. p.208.)

⑵ 국가정보원

국가정보원(http://www.nis.go.kr)에서는 사이버침해사고에 대한 실태를 파악하고 방지대책을 마련하는 일을 하고 있다. 국가정보원의 자료(<표 3-27>)에 따르면, 2003년도의 경우 모두 27,502건의 사이버침해사고가 발생하였으며, 이 가운데 국가·공공기관에서 발생한 것이 1,323건으로 전체의 4.8%를 차지하였으며, 민간분야에서는 26,179건이 발생, 사고의 대부분(95.2%)를 차지하였다. 민간부문의 이 수치는 전년도에 비해 10,987건이 증가한 것으로, 약 72%의 증가세를 보이고 있다.

<표 3-27> 최근 5년간 사이버 침해사고 발생현황

연 도	1999년	2000년	2001년	2002년	2003년	합 계
공공분야	18	102	613	1,315	1,323	**3,371**
민간분야	572	1,943	5,333	15,192	26,179	**49,219**
합계	**590**	**2,045**	**5,946**	**16,507**	**27,502**	**52,590**

(출처 : 국가정보원, 「2003 사이버 침해사고 사례분석집」, 국가정보원, 2004, p.115.)

이처럼 민간분야에서의 사이버침해사고 발생률이 높은 것은 공공기관에 비해 침입차단시스템이나 백신프로그램 보급률이 저조한 개인이나 소규모 단체에 대한 사이버침해 사례가 증가했기 때문이다. 한편 국가정보원에 따르면 통상 피해기관(업체)이 사고사실을 숨기거나 인지하지 못하는 경우가 많기 때문에 실제사고 건수는 공식통계보다 훨씬 많을 것으로 예측하고 있다.

제2절 인터넷을 이용한 청소년범죄의 주요 유형과 실태·사례

앞 절에서는 형사사법기관 및 기타 정부기관의 공식통계를 이용하여 우리사회에서 발생하는 다양한 사이버범죄의 실태를 포괄적으로 살펴보았다. 이제 이 절에서는 <표 3-1>에서 제시한 사이버범죄 유형론에 의거하여 개별적인 사이버범죄 유형별로 그 실태와 사례들을 검토하기로 한다.

1. 유 형 Ⅰ:

1) 개인신상정보의 도용

(1) 개인신상정보도용의 개념

인터넷을 통한 각종 상거래의 급속한 확산과 더불어 회원가입을 의무로 하는 회원제 사이트가 증가하면서 자신도 모르는 사이에 주민등록번호나 아이디 등의 신상정보가 무단으로 도용되어 각종 피해가 급증하고 있다.

인터넷상의 개인신상정보에 대하여 공정거래위원회에서는 크게 신상정보(나이, 성별, 직업, 직책, 가족, 기호, 취미, 주소, 전화번호, 이메일), 거래정보(거래품목, 거래정도, 자주 이용하는 거래처, 좋아하는 색상 등), 신용정보(소득, 재산정도, 연체사실, 보증 등), 지불정보(신용카드번호, 지로번호 등), 그리고 기타정보(의료·건강정보, 노동력정보) 등으로 구분하고 있다.[25]

일반적으로 개인신상정보의 도용이라는 것은 위와 같은 특정한 개인의 정보에 대하여 동의 없이 무단으로 도용하여 자신의 소기의 의도를 달성함과 동시에 피해자에게는 막대한 피해를 입히는 행위라 할 수 있다. 이러한 개인신상정보의 도용은 개인의 프라이버시를 침해하는 것은 물론 개인 권익의 손실을 유발할 수 있고, 궁극적으로 인간의 존엄성 침해를 가져올 수 있을 만큼 파급 효과가 큰 범죄 행위이다.[26]

(2) 개인신상정보도용의 실태

개인신상정보의 침해와 관련하여 2004년 1분기에 개인정보분쟁조정위원(http://www.kopico.or.kr)에 접수된 개인정보침해관련 민원은 모두 469건으로 이는 지난해 같은 기간의 250건보다 88% 증가한 수치이며, 지난 2003년 1년간 접수된 845건의 54%에 달한다. 유형별로는 '법정대리인의 동의가 없는 아동의 개인정보 수집'이 237건으로 절반이 넘는 55.5%를 차지했으며, 그 다음으로 '타인정보의 훼손, 침해, 도용'이 15.1%인 71건, '고지, 명시 범위를 넘어선 이용이나 제3자 제공'이 11%인 50건, '동의철회, 열람 또는 정정요구 불응'이 6.3%인 30건으로 집계됐다.[27]

또한 국가인권위원회가 '함께하는 시민행동'(http://www.ww.or.kr)과 함께 2003년 5월부터 5개월간 네티즌 1,000여명을 대상으로 조사한 결과 응답자의 26%가 자신의 주민등록번호를 도용당해 인터넷 사이트에 회원으로 가입하지 못한 경험이 있다고 응답했다.[28]

한편 김성언(2001)은 2001년 9월 현재 서울시에 거주하는 20세 이상 60세 미만의 성인남여 1,050명을 대상으로 개인정보침해에 관해 조사하였는데, 조사결과, 인터넷에서 발생하는 7가지 유형의 개인정보 침해 중, ID나 패스워드 도용피해를 경험한 비율이 21.3%로 가장 높았고, 그 다음은 누군가가 자신의 개인정보를 이용하여 특정 사이트에 가입(19.5%), 전자문서(웹콘텐츠 포함)의 도용·변조·파괴(7.2%), 허위사실 유포에 따른 명예훼손(5.3%), 몰래카메라에 의한 사생활 침해(4.4%), 신용카드의 도용(4.1%), 사이버뱅킹이나 사이버증권상의 개인정보 침해(3.8%)의 순으로 나타났다.

---

25) 본 분류 방식은 공정거래위원회 소비자종합 홈페이지(http://www.consumer.go.kr)를 참조한 것임.
26) 정완, "전자상거래 관련범죄의 규제에 관한 연구", 한국형사정책연구원 연구보고서, 2000. p. 10.
27) 연합뉴스, 2004년 5월 27일자.
28) YTN, 2003년 12월 18일.

(3) 청소년의 개인신상정보도용 실태

청소년들의 개인신상정보 도용은 청소년들의 컴퓨터 관련 지식이 성인에 비해 뒤지지 않는 것과 마찬가지로 매우 지능화, 대규모화 되고 있다. 과거 10대 청소년에게 있어 개인신상정보의 도용이 주로 발생한 경우는 타인의 아이디로 사이버머니를 가로채는 경우나 성인대상 회원제 사이트에의 접속을 위한 것이 대부분으로 파악되었으나, 최근에는 금융거래나 개인정보 도용을 통한 금품의 요구 등 점차 성인들의 그것과 유사한 양상으로 변모하고 있는 것으로 나타났다.[29)]

청소년들의 개인신상정보 도용과 관련한 이종원(2001)의 연구에서는 전체 조사대상 청소년 1,309명 중 11.8%를 차지하는 154명의 청소년이 개인신상정보를 도용해본 적이 있다고 응답했다.

2. 유 형 Ⅱ :

1) 전자상거래범죄(인터넷사기 등)

(1) 전자상거래범죄의 개념

전자상거래(EC: Electronic Commerce)란 상품이나 서비스에 대한 정보제공 및 수집, 주문, 접수, 대금결제, 상품발송 등 일련의 상거래 흐름이 기존의 서류에 의존하지 않고 인터넷이라는 정보통신기술에 의해 이루어지는 것을 의미하며, 전자상거래의 과정에서 일어나는 불법적인 행위들을 전자상거래 범죄라 한다.

전자상거래의 유형은 기업간, 기업과 개인, 개인과 개인, 기업과 정부, 개인과 정부, 정부와 정부 등 6가지 형태로 볼 수 있는데, 이러한 전자상거래에 있어 발생할 수 있는

---

29) 다음의 2가지 사례는 청소년들의 개인신상정보도용 수준이 성인범에 근접하고 있음을 단적으로 보여주고 있다.: (1) 사례 1: 경찰청 사이버테러대응센터는 자신이 개발한 'IP 스캐너'라는 프로그램을 이용하여 국내 46개 인터넷 사이트를 해킹, 무려 630여만 명의 회원정보를 빼낸 뒤 해당 사이트 운영자에게 금품을 요구한 K군을(17, 대전 A 상고) 검거함(동아일보, 2000년 12월 16일자). (2) 사례 2: 서울경찰청 사이버범죄수사대는 2000년 4월 25일 상습적으로 서울 신길동 PC방 컴퓨터 12대에 해킹 프로그램인 '백오리피스'를 설치한 뒤 PC방 이용자들의 ID와 비밀번호를 알아내어 인터넷 유료서비스에 접근하고, 주식·은행거래, 인터넷 쇼핑 등을 한 장모군(18)에 대해 구속영장을 신청하고 이모군(17)에 대해서는 불구속 입건함(국민일보, 2000년 4월 26일자).

피해로 인터넷사기, 내부자 정보남용, 해킹, 전자우편의 오남용, 개인정보의 유출 등이 있다(한국사이버감시단, 2001).

그러나 전자상거래에 있어 특히 중요한 점은 소비자, 즉 네티즌이 피해를 볼 수 있는 요소가 곳곳에 산재해 있어 실제로 다양한 피해사례가 속출하고 있는 실정이며, 피해의 영향은 개인뿐만 아니라 사회적, 경제적으로 심각한 영향을 미치고 있다는 점이다.

(2) 전자상거래범죄의 실태

우리나라는 인터넷 강국답게 초고속인터넷 서비스 보급률이 세계 1위이며 이용자도 3천만명을 돌파하는 등 인터넷 이용자가 크게 늘어나면서 사이버공간에서의 각종 사기사건 등 전자상거래 관련 범죄 또한 크게 증가하고 있다. 전자상거래 관련 범죄 현황을 컴퓨터사용 사기건수로 발표하고 있는 대검찰청의 자료에 따르면 전자상거래범죄는 2001년 428건에서 2002년 1,346건, 2003년 2,346건으로 크게 증가하는 추세를 보이고 있다.

대표적인 전자상거래범죄 유형은 판매사기와 금융사기이다. 판매사기의 경우 통신판매사기,[30] 경매·역경매사기,[31] 개인간 직거래 혹은 이벤트사기,[32] 피라미드식 다단계사기,[33] 홈쇼핑 상표도용 및 사기, 환불·교환 지연 및 거부, 불공정행위, 허위·과장광

30) 통신판매사기는 가장 전형적인 전자상거래 범죄의 유형이다. 공정거래위원회는 지난 5월 10일 물건을 사고자 하는 고객이 결제를 하면 이 돈을 금융기관 등 제3자에 예치한 후 배송 확인을 거쳐 판매업체에 지급하는 '결제대금 예치제(에스크로)' 도입을 의무화하는 '전자상거래소비자 보호법' 개정안을 마련, 입법예고 하였다. 따라서 앞으로 통신판매사기는 다소 위축될 것으로 예상되며, 보다 지능적인 전자상거래 관련 범죄가 등장할 것으로 예상된다.

31) 서울지검 컴퓨터수사부는 2003년 9월 27일 인터넷 경매 사이트를 운영하면서 허위 입찰한 회사 내부자가 낙찰받도록 하는 방법으로 회원들로부터 입찰 참가비를 편취한 혐의로 인터넷 경매업체인 모회사대표 허모씨 등 3명을 구속했다. 허모씨 등은 2003년 6월부터 인터넷에서 최저가로 단독 입찰한 회원이 낙찰받는 방식의 경매쇼핑몰을 운영하면서 직원들의 친인척 명의로 1원 단위로 금액을 올려 입찰하는 소위 '깔기' 방식을 이용해 낙찰받는 수법으로 최근까지 입찰에 실패한 회원 만2천여명으로부터 입찰참가비 2억7천여만원을 챙겼다(연합뉴스, 2003년 9월 27일자).

32) 최근 이벤트 당첨을 미끼로 한 인터넷 사기수법이 기승을 부리고 있다. 구체적으로는 사기 온라인게임 아이템이나 사이버머니 제공 또는 이벤트 당첨 등을 미끼로 미성년자를 유혹해 전화번호를 알아낸 뒤 전화결제용 번호인 060-XXX-YYYY로 전화를 걸게 해, 정보이용료는 미성년자의 부모 등이 부담케 하고 캐쉬 등을 차지하는 사기행위가 나타나고 있다(edaily, 2004년 2월 9일자).

33) 서울경찰청 사이버범죄수사대는 2001년 7월 18일 개인 인터넷쇼핑몰을 분양해주겠다며 인터넷을 통해 회원들을 모집, 5만5천여 명에게서 4백50억원을 챙긴 인터넷쇼핑몰 대표 김모(30)씨 등 4명을 방문판매 등에 관한 법률위반 혐의로 구속하고 이 회사 관계자 27명을 같은 혐의로 구속 입건했다(한국경제, 2001년 7월 18일자).

고[34] 등이 자주 발생하고 있다. 또한 금융사기의 경우로는 인터넷 금융 피라미드 사기,[35] 인터넷 신용카드사기, 인터넷 주식 사기, 그리고 최근에 성행하고 있는 속칭 '피싱'사기 수법[36] 등이 흔히 발생하고 있다.

(3) 청소년의 전자상거래 범죄

전자상거래 범죄는 청소년들에 의해서도 적지 않게 발생하는 사이버범죄 유형이지만, 청소년들에게 있어서는 범죄유형의 폭이 성인들에 비해 좁은 편이며, 범행 액수 또한 성인범에 비해 적은 편이다. 청소년들이 저지르는 전자상거래 관련 범죄는 허위광고와 연계된 인터넷게임 아이템판매 관련 사기, 통신판매사기 등이 대부분이다. 특히 인터넷게임 아이템을 판다고 허위광고를 한 후 타인 명의로 개설된 통장에 입금을 하게한 뒤 가로채는 수법,[37] 또래 청소년들의 사행심을 불러일으킬 수 있는 각종 물품을 판다고 속여 대금을 가로채는 경우[38]가 많이 발생하고 있다.

---

34) 재택부업을 원하는 주부 등을 상대로 핸드폰 판매용 홈페이지를 개설만 하면 매달 수십만원의 고정수익을 올릴 수 있다고 속여 총 수십억원을 가로챈 일당이 검찰에 적발됐다. 서울중앙지검 컴퓨터수사부는 2004년 5월 2일 주부 및 실직자 등 피해자 2천6백여 명으로부터 휴대폰 판매용 홈페이지 제작비 명목으로 1인당 1백59만원씩, 총 30억8천여만 원을 가로챈 혐의(특정경제범죄가중처벌법상 사기)로 인터넷 쇼핑몰 실운영자 전모씨(34세)등 6명을 구속기소하고 사장인 신모씨(30세)등 4명을 불구속 기소했다(한국경제, 2004년 5월 2일자).

35) 검찰은 2002년 12월 29일 전형적인 인터넷 쇼핑몰로 위장, 벤처투자 명목으로 1천억원대의 자금을 끌어모으는 등의 전형적인 인터넷 금융 피라미드 수법 행각을 벌인 비즈앤퍼슨스 대표등 14명을 적발하여, 이 중 8명을 구속하였다. 서울지검 컴퓨터수사부(한봉조 부장검사)는 29일 금융피라미드업체 (주)비즈앤퍼슨스 대표 이모(34)씨 등 8명을 사기 등 혐의로 구속기소했다. 또 해외로 도주한 이 회사의 대주주이자 오너인 정모(38)씨를 인터폴을 통해 지명 수배하고 정씨의 측근 5명을 불구속 기소했다(한국경제, 2002년 12월 29일).

36) 인터넷상의 신종 사기기법인 '피싱'은 불법적으로 개인정보를 얻으려는 자(phisher)가 불특정 다수의 이메일 사용자에게 신용카드나 은행계좌 정보에 문제가 발생해 수정이 필요하다는 거짓 이메일을 발송, 가짜 웹사이 트로 유인하는 등의 방법으로 신용카드 정보나 계좌정보 등을 빼내는 수법이다.

37) 전남 목포경찰서는 인터넷 게임 아이템을 판다며 9백여만원을 받아 가로챈 혐의로 17살 류모군에 대해 구속영장을 신청했다. 류군은 지난해 7월, 남의 명의로 은행 계좌를 개설한 뒤 온라인게임 리니지 아이템을 판다고 허위 광고를 내 이를 보고 돈을 송금한 23살 김모씨 등 90여명으로부터 모두 9백여만원을 받아 가로챈 혐의를 받고 있다(YTN, 2004년 6월 5일).

38) 청소년들에게서 가장 일반적으로 나타나는 전자상거래 범죄 유형으로는 다음의 2가지 사례가 대표적이다. (1) 서울 청량리 경찰서는 인터넷사이트에 물건을 판다고 글을 올린 뒤 물건값만 입금 받아 챙긴 혐의로 15살 박모군 등 10대 3명에 대하여 구속영장을 신청했다. 박군 등은 인터넷 매매 사이트에 액세서리를

경찰청 자료를 인용한 언론보도에 의하면 2003년도의 경우 인터넷 게임 사기 등의 사이버범죄로 벌금형 이상을 선고받아 전과자가 된 청소년이 1만명을 넘어섰으며, 이 중 아이템 관련 사기나 아이템 해킹 관련 범죄가 70%에 달하는 것으로 나타나고 있다.[39]

2) 사이버성범죄(사이버성폭력)

(1) 사이버성폭력의 개념

'사이버성폭력'은 '성폭력'의 개념 자체가 갖는 애매함 외에 '사이버'라는 공간적 배경이 갖는 모호함이 더해짐으로써 간단히 규정하기 어려운 지극히 다차원적이며 논쟁적인 개념이다. 실제로 실무계와 학문공동체의 논의에서는 사이버성폭력이 구체적으로 무엇을 지칭하는 것인가에 대해 아직까지 뚜렷한 개념적 합의를 보지 못하고 있다. 다만, 현재까지 나타난 논의들을 종합해 보면 사이버성폭력을 규정함에 있어서는 두 가지 지배적인 관점이 있음을 알 수 있다(정진수 외: 2000:23~25).

첫 번째 관점은 오프라인에서의 성폭력에 대한 법률적 이해와 유사하게 사이버성폭력을 "인간의 성(sexuality)적 온전성(또는 자아)에 대한 온라인상의 침해행위"로 다루는 입장으로서, 이러한 관점은 「성폭력범죄의처벌및피해자보호등에관한법률」 제14조(통신매체이용음란죄) - "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 자 ... " - 에서 찾아 볼 수 있다. 요컨대, 이 관점에서 사이버성폭력은 "인터넷, 이메일 등 정보통신수단을 이용하여 다수 또는 특정인을 성적으로 괴롭히는 행위(성적 수치심, 공포심 및 불안감 유발)"로 규정된다.

판다는 허위광고를 올린 뒤 이를 보고 연락한 17살 윤모군으로부터 14만원을 입금받아 챙기는 등 모두 110여 차례에 걸쳐 천여만원을 받아 챙긴 혐의이다(YTN, 2004년 6월 5일). (2) 전남 무안경찰서는 2004년 6월 26일 인터넷 물품매매 사이트에 허위광고를 낸 뒤 거액의 대금을 받아 챙긴 홍모군(18. 전남 목포시) 등 4명에 대해 상습사기 혐의로 구속영장을 신청했다. 홍군 등은 지난해 12월 27일 오후 5시께 목포시내 모 PC방에서 인터넷 물품거래사이트 게시판에 '오토바이와 휴대폰 등을 싸게 팔겠다'는 글을 올린 뒤 구매를 원하는 박모군(18)으로부터 100만원을 송금받아 가로채는 등 최근까지 200여 차례에 걸쳐 8000여만원 상당을 편취한 혐의다(뉴시스, 2004년 6월 26일자).

39) 중앙일보. 2004년 5월 21일자.

두 번째 관점은 주로 여권운동단체나 여성학계에서 주장하는 것으로서, 사이버성폭력을 “여성에 대한 폭력”이란 시각에서 다룬다. 예컨대, (사)한국성폭력상담소에서는 사이버성폭력을 “원치 않는 성적인 언어 - 외모와 성적 취향, 음담패설 등 - 나 이미지를 사용함으로써 위협적, 적대적, 공격적인 통신환경을 조성하여 상대방의 통신환경을 저해하거나 현실공간에서의 피해를 유발한 경우 ..., 또한 명시적으로 성적인 접근이나 제안이 아니더라도 성적인 은유나 암시로 상대방으로 하여금 불쾌감을 느끼게 한 경우”로 규정하고 있다.[40]

이러한 두 가지 관점 중 전자는 ‘성’(sexuality)에 초점을 두는 비교적 엄밀한 개념인데 비해, 후자는 ‘성차’(gender difference)에 초점을 두는 비교적 광의의 개념으로서 이성(주로 여성)에 대해 적대적인 욕설・비속어・언어폭력 그리고 단순히 불쾌감을 주는 성적 메시지까지도 사이버성폭력의 범주에 포함시켜야 한다는 입장이라 하겠다. 본 연구에서는 이러한 후자의 견해에 따라 사이버성폭력을 “사이버공간에서 발생하는 성 및 성차와 관련한 이성에 대한 다양한 불법적인 행위유형”으로 광의로 정의하고자 한다.

(2) 사이버성폭력의 유형

사이버성폭력의 유형을 살펴보면, 한국성폭력상담소에서는 사이버성폭력을 다음과 같은 다섯 가지 유형으로 분류하고 있다: ① 성에 관한 원치 않는 대화 요청이나 성적인 메시지 전달, ② 성에 관한 원치 않는 전자우편이나 쪽지(memo) 발송, ③ 성에 관한 개인의 사적인 자료를 게시판 등에 공개, ④ 게시판을 통해 상대방의 동료나 친구 또는 아는 사람에게 상대방의 성에 관해 이야기 하는 것, ⑤ 사이버성폭력의 연장으로서, 우편이나 전화를 통해 오프라인에서의 접근을 시도하는 행동. 이 유형화의 특징은 앞에서 언급한 바와 같이 사이버성폭력을 상당히 포괄적으로 규정하여 오프라인에서 우편이나 전화를 통해 접근을 시도하는 행동까지도 하나의 사이버성폭력 형태로 인정하고 있다는 것이다.[41]

그리고 정진수 외(2000)의 연구에서는 사이버성폭력을 성과 관련한 괴롭힘이나 성가심 문제로서 ① 사이버성희롱과 ② 사이버스토킹을, 성차와 관련한 문제로서 ③ 이성에 대한 언어폭력(성차별적・성적대적 플레임), ④ 사이버매매춘, ⑤ 사이버음란물의 상업적

40) http://www.sisters.or.kr/menu5/cyber.html.
41) http://www.sisters.or.kr/typical/cyber.html.

유통을 구분하고, 사이버성희롱을 다시 '채팅과정에서 상대방의 의사를 무시하고 음담패설이나 성적인 언사로 희롱,' '원치 않는 음란물 또는 성적 메시지(글, 음향 및 동영상 파일) 전달 및 게시,' '일방적으로 성적 대화(컴섹)나 성적 만남(번섹[42])을 강요'의 세 가지 하위 유형으로 나누었다.

한편 이민식(2003)은 경험적 조사를 통해 사이버성폭력의 유형을 다음과 같이 8가지로 분류하였다. ① 음담패설 또는 성적 언사로 희롱함, ② 성차별적·성적대적 언어폭력, 협박, ③ 폰섹, 컴섹 또는 번섹 제의, ④ 매매춘 또는 원조교제 제의, ⑤ 대화 중 또는 메일을 통해 음란물(음향, 화상, 동영상 등) 송신, ⑥ 화상채팅 도중 자신의 성기 또는 자위행위를 보여 줌, ⑦ 광고 또는 판매를 위한 음란물 송신, ⑧ 사이버스토킹(성적인 것에 한정).

한편 사이버성폭력을 이렇게 다양한 하위유형들로 구분함에 있어서는 몇 가지 유의해야 할 사항이 있다.

첫째는 전술한 분류가 분석상의 목적에서 유용할지는 모르나 실제 상황에서는 여러 가지 하위 유형들이 복합적으로 동시 다발적으로 나타나는 경우가 많다는 것이다. 예컨대, 음담패설 또는 성적 언사의 희롱은 성차별적·성적대적 언어폭력, 폰섹·컴섹 또는 번섹 제의 등의 전단계로서 발생할 수 있다. 초기의 성희롱에 대한 강력한 대응은 상대방으로부터 성차별적·성적대적 언어폭력을 유발할 수 있으며, 반대로 소극적인 대응은 폰섹·컴섹 또는 번섹 제의를 유도할 수도 있는 것이다.

둘째, 매매춘 또는 원조교제의 제의는 부당한 금전적 이득을 목적으로 하는 전문적인 알선조직에 의한 경우도 적지 않지만, 그 상당 부분은 실제로 실행할 의도를 가지고 행하였다기 보다는 단순히 장난기 또는 호기에서 비롯된 것임을 감안해야 한다.

셋째, 광고 또는 판매를 목적으로 한 음란물의 수신은 이메일을 사용하는 사람치고 경험해 보지 않은 사람이 없을 정도로 일상적인 것이다. 사이버음란물의 상업적 유통은 불평등한 성문화를 반영한 것임에는 틀림없지만, 대부분의 여성 네티즌들이 이를 하나의 성폭력피해로 심각하게 인식하지 않는다는 점에서 그것을 사이버성폭력의 한 가지 유형으로 여과 없이 받아들일 수 있는가 하는 점에는 논란의 여지가 없지 않다.

---

42) 번섹은 통신속어로서 '번개섹스'의 줄임 말이다. 채팅을 하거나 메모(쪽지)를 주고 받다가 상대방을 오프라인에서 직접 만나는 것을 '번개'라고 하고, 이러한 단순한 만남에서 성행위까지 가는 것을 '번섹'이라고 한다.

(3) 사이버성폭력의 실태

<표 3-28>은 이민식(2003)이 2000년도 8월 인터넷 서베이를 통해 수집한 자료[43]를 토대로 응답자들이 구체적으로 진술한 사이버성폭력 피해의 내용을 분석하여 유형화한 것이다. 또한 이 표에는 각각의 피해유형별로 대표적인 사례가 하나씩 제시되어 있다.

이 자료에 의하면 피해경험이 있는 774명중 응답자들이 가장 빈번히 경험한 사이버성폭력 피해유형은 '성차별적·성적대적 언어폭력 및 협박'으로서 전체의 33.6%인 260명의 응답자가 이를 경험한 것으로 나타났다. 두 번째로 높은 빈도를 차지한 피해유형은 '음담패설 또는 성적언사로 희롱함'으로서 전체의 25.1%인 194건이었다. 나머지는 '매매춘 또는 원조교제 제의'(9.1%), '컴섹, 폰섹, 또는 번섹 제의'(9.0%), '사이버스토킹'(8.4%), 그리고 '음란물송신 또는 음란 사이트 자동 링크'(7.3%)가 서로 비슷한 수준으로 발생하였다. '광고 또는 판매를 위한 음란물 송신'은 채팅이나 대화 도중 상대방이 음란물을 보내거나 올리는 것과는 달리 상업적인 목적을 가지고서 행해지는 것으로서 실제로 인터넷을 사용하는 사람치고 경험해 보지 않은 사람이 없을 정도로 흔히 발생하는 일이다. 그러나 또한 바로 그 점에서 네티즌들은 그것을 하나의 사이버성폭력으로 인식하지 않는 경우가 많으며, 따라서 이 연구에서는 그러한 피해를 자신의 자아에 상처를 줄 정도로 심각하게 인식하였던 사람들만이 사이버성폭력으로 보고하였다(3.2%).

성폭력이란 개념의 다의성 그 자체가 시사하는 바와 같이 사이버성폭력은 다양한 하위유형들을 포괄하는 개념이다. 이민식(2003)의 연구에서는 그러한 행위를 비록 8가지 하위유형으로 구분하였지만, 그것은 어디까지나 분석상의 편리함을 위한 것이지, 실제에 있어서도 그들 간의 차이가 명확히 드러나는 것은 아니다. <표 3-28>에서 제시된 '혼합된 유형들'이 시사해 주는 바와 같이 실제의 사이버성폭력은 다양한 하위유형들이 복합적으로 중첩되어 발생하고 있음을 알아야 할 것이다.

한편 최근의 조사자료로서 안산 YMCA가 안산지역의 20대 이상 여성 네티즌 345명을 대상으로 사이버성폭력 피해 실태조사를 한 결과, 71%에 해당하는 246명의 여성 네티

43) 본 연구의 원자료인 인터넷 서베이는 국내 최대의 무료 인터넷 포털서비스업체인 '다음커뮤니케이션(Daum Communications Co.)'의 협조를 얻어 실시한 것으로, 2000년 8월 4일부터 8월 10일까지 7일간에 걸쳐 실시되었다.

즌들이 각종 사이버성폭력의 피해를 경험한 것으로 나타나는 등 사이버성폭력 범죄는 매우 심각한 문제로 대두되고 있다.[44]

<표 3-28> 사이버성폭력 피해의 유형과 실태

구 분	빈도	%	사 례
1) 음담패설 또는 성적 언사로 희롱함	194	25.1	"제가 이혼녀들의 까페를 운영하고 있습니다. 그러다 보니, 고1 남자라는 둥, 중년의 남자라는 둥 그런 사람들이 남의 아뒤를 가지고 멜을 보냅니다. 섹스를 하고 싶다, 당신들은 좀 편할 것 같다(왜냐면 이혼녀니까), 남자에게 몸 달아 있는 여자를 소개시켜 달라는 둥의 이상한 멜을 보냅니다."
2) 성차별적·성적대적 언어폭력, 협박	260	33.6	"대화방에서 실명을 밝히지 않은 남자가 들어와서 온갖 상스런 이야기를 하였고, 그것에 대해 반발하자. XX년 지랄하고 있네. 등 온갖 욕설을 퍼붓고 나갔다."
3) 컴섹, 폰섹, 또는 번섹 제의	70	9.0	"인터넷 채팅 중에 컴섹이나 폰섹을 하자구 자꾸 그러더라구요.. 그래서 그게 뭔지 잘 몰라서 뭐냐구 물어봤더니, 설명해주는데.. 상대방의 언행이.. 저에겐,, 충격적이었고.. 그런 얘기를 한다는 것에 너무 놀랐었습니다."
4) 매매춘 또는 원조교제 제의	71	9.1	"채팅을 하는데 같은 나이의 남자 애와 일대일 대화를 할 기회가 생겼다. 계속 대화하다 보니 이상한 점을 느껴 물어보았더니 나중에서야 10대가 아닌 원조를 원하는 30대 후반의 아저씨였던 것이다."
5) 음란물(음향, 화상, 동영상 등) 송신 또는 음란사이트 자동 링크	56	7.3	"대화방에서 애기를 하던 중 한 사람이 메모를 보내왔고, 여자가 확실하냐고 물어보며 재미난 그림을 보여주겠다며 파일을 보내주었는데, 그 장면은 변태적 행위와 관련된 것이었다. 왜 나에게 그걸 보내느냐고 물어보니 그냥 재밌으니까 라고 대답했다."
6) 화상채팅 도중 자신의 성기 또는 자위행위를 보여 줌	5	0.6	"화상채팅 중에 어떤 사람이 들어오더니 (남자) 아랫 부분을 비추더니 자기의 생식기를 보여줬다 ㅠ.ㅠ"
7) 광고 또는 판매를 위한 음란물 송신	25	3.2	"항상 메일로 정체불명의 음란물 구입을 강요하는 메일이 온다. 정말 불쾌하고 제목이 또 안녕 이런거면 누가 보낸거지 하면서 열어보게 되는데, 열리는데 엄청난 시간이 지나서 완료된다. 한참을 기다리곤 하는데 정말 짜증난다."
8) 사이버스토킹 (성적인 것에 한정)	65	8.4	"대부분의 사이트에서 아이디가 '세라야'인데 어떤 이상한 넘이 사이트마다 따라다니면서 사귀자고 쪽지 보내고.. 밤에 만나자는 등.. 이상한 내용의 메모나 메일 마구 보내고.. 하여튼 왕짜증이었는데..그 사이트 관리자에게 신고를 해도 다른 아뒤로 다시 그러고..."
이들의 혼합된 유형*	28	3.6	-
합 계	**774**	**100.0**	-

* 혼합된 유형: 2)번 유형+기타(17명), 5)번 유형+기타(11명),
3)번 유형+기타(9명), 4)번 유형+기타(9명), 1)번 유형+기타(6명)

44) YTN, 2003년 12월 12일.

⑷ 청소년의 사이버성폭력 실태

청소년들이 사이버공간의 주축으로 자리잡아가고 있지만, 사이버공간의 유해환경은 청소년을 성폭력에 부방비로 노출시키고 있다. 10대 청소년들에게 있어서 사이버성폭력은 성인들과 거의 같은 형태로 이루어지고 있지만, 가해자와 피해자가 동시에 대량 양산되고 있는 점이 큰 문제이다.

2003년에 한국교육학술정보원(KERIS)에서 전국의 중학교 3학년과 고교 1학년 2,509명을 대상으로 연구한 결과에 따르면, 인터넷상의 사이버성폭력 경험여부에 대하여 23.5%가 '조금 또는 자주 있다'라고 응답하였다.[45] 또한 대구 카톨릭대학교 사회과학연구소가 2001년 2월부터 11월까지 대구시내 25개 중고교의 2,600명을 대상으로 조사한 결과 대구지역 중고생의 35%가 인터넷 등의 사이버상에서 성폭력 피해 경험이 있는 것으로 조사됐다.[46]

3) 허위사실유포・명예훼손

사이버공간이 갖는 표현의 자유, 광범위한 전파성, 저렴한 비용 등의 특성들은 인터넷을 통한 허위사실의 유포와 명예훼손의 기회를 극대화 시키고 있다.

명예훼손과 허위사실유포는 상호관련된 개념이기는 하지만, 명예훼손이 한 사람 또는 일부 특정인 등의 명예실추나 사회적인 매장을 노린 범죄라면,[47] 허위사실의 유포는 다수에게 왜곡된 정보를 유포함으로써 혼동을 초래하거나 집단간, 지역간, 또는 국가간의 갈등을 조장하는 범죄행위를 말한다. 따라서 허위사실의 유포는 개인적 차원이 아닌 사회적, 국가적으로 큰 피해를 입힐 수 있는 범죄행위로 인식할 필요가 있다.[48]

---

45) 경향신문, 2003년 3월 12일자.

46) 국민일보, 2001년 12월 11일자.

47) 충남지방경찰청 사이버수사대는 2004년 5월 31일 인기 여가수 이효리를 비방하는 인터넷 카페를 운영한 혐의(정보통신망이용촉진및정보보호에관한법률 위반)로 유모씨(29)를 불구속 입건했다. 유씨는 2003년 12월 16일 이효리를 비방하는 인터넷 안티 카페를 개설한 후 지난 29일 폐쇄할 때까지 이효리의 사진에 '안 벗으면 못 사는 여자'라는 비난 글을 합성해 올려놓는 등 명예를 훼손한 혐의다(일간스포츠, 2004년 6월 1일자).

48) 허위사실유포와 관련, 개정된 선거법에 따르면 앞으로 각종 인터넷과 언론, 포털사이트 등의 게시판과

최근에는 주로 증권관련 혹은 정치인이나 연예인 등 사회적 공인들을 대상으로 하는 악성루머가 빈번하게 나타나고 있다.[49] 악성루머는 인터넷의 게시판이나 정보통신을 이용하여 수많은 네티즌에게 무작위로 배포되어 대량의 피해를 초래한다.

4) 사생활유포

인터넷을 이용한 개인의 사생활 유포는 종래에는 연예인 등 특정인에게 집중되는 경향을 보였으나, 최근에는 일반인들에게까지 그 대상이 확대되는 경향을 보이고 있으며, 인터넷 자체가 타인의 사생활을 엿보고 감시하는 수단으로 전락하고 말았다.

최근 해킹기법의 발달로 타인의 이메일을 해킹하고 공개하여 사생활이 심각하게 침해당하고 있다. 그리고 사생활을 몰래 촬영한 비디오를 인터넷에 공개하여 한 개인에게 씻을 수 없는 모욕과 수치를 주기도 한다.[50] 최근에는 10대 청소년이 특정 연예인의 사생활을 담은 비디오를 인터넷에 공개하여 구속되는 일이 발생하는 등 사생활유포는 청소년들에게도 예외가 아닌 현상으로 나타나고 있다.[51]

이처럼 사생활유포는 게시판의 작성글 뿐만 아니라 이메일의 공개, 사진 및 몰래촬영한

대화방에서 정치적 의견을 밝히기 위해서는 인터넷 아이디가 아닌 실명을 써야한다. 이러한 선거법의 개정에 대하여 시민단체 등은 선거법이 전과자를 양산한다며 강력히 반발하고 있다.

49) 서울지검 컴퓨터수사부는 2003년 8월 7일 주가분석 방송에서 허위정보를 유포, 주가를 조작해 총 1억2천2백여만원의 부당이득을 챙긴 혐의(증권거래법 위반)로 안모씨(30) 등 사이버 '고수' 5명과 모 케이블 TV PD 등 7명을 불구속 기소했다. 검찰에 따르면 이들 사이버 고수는 지난해 4월 주가분석 방송에 출연하면서 총 22차례에 걸쳐 방송에서 추천할 종목을 방송 1-2일전에 미리 사놓고 방송 당일 허위정보를 흘려 주가를 끌어올린 뒤 주식을 비싼 값에 팔아 시세차익을 챙긴 혐의다. 이들은 주가조작 대상으로 삼은 종목에 대해 방송 전에 다량의 허수 주문을 내 거래가 활발한 것처럼 가장하는 등 일반 투자자들을 속이기 위해 치밀한 준비작업까지 한 것으로 드러났다(YTN, 2003년 8월 7일자).

50) 서울지법 민사합의 43부는 2003년 5월 27일 미스코리아 출신 탤런트 성모씨(28)가 수의(囚衣)를 입은 자신의 사진을 인터넷을 통해 유포해 심각한 사생활 침해를 당했다는 이유로 교도소 경비교도원 정모씨와 국가를 상대로 낸 손해배상청구소송에서 "정씨와 국가는 성씨에게 각각 2000만원과 1000만원을 지급하고 정씨는 성씨에게 반성문도 제출하라"며 강제조정 결정을 내렸다. 정씨는 H교도소 교도원으로 근무하던 지난해 3월 마약복용 혐의로 수감돼 있던 성씨의 미결수 사진을 몰래 빼낸 뒤 인터넷에 유포한 바 있다(동아일보, 2003년 5월 28일자).

51) 서울지검 북부지청 형사3부는 2000년 11월 30일 사회적 파문을 일으키고 있는 일명 '백지영 비디오' 파일을 자신의 인터넷 홈페이지에 올린 혐의(전기통신기본법 위반 및 명예훼손)로 원모(17. 무직)군에 대해 구속영장을 청구했다. 원군은 2000년 11월 27일부터 자신의 홈페이지 게시판에 이 파일을 올려 15만여명의 네티즌들이 복사할 수 있게 한 혐의다(중앙일보, 2000년 12월 1일자).

비디오의 공개 등 매우 광범위한 방법으로 인터넷상에서 이루어지고 있다. 한편 최근 법무부가 2006년 시행을 목표로 확정한 민법개정안에 따르면 '사적자치'(私的自治)조항을 신설하여 허가 없이 타인의 사진을 게제하거나 인터넷상에 유포한 경우 상응하는 대가를 치르도록 함으로써 사생활유포의 경우 앞으로 보다 엄격한 처벌이 예상된다.

5) 인신공격・언어폭력・협박

사이버공간에서는 비대면성의 특성으로 인해 인신공격・언어폭력・협박이 난무하고 있다. 이와 같은 유형의 행위는 주로 홈페이지 게시판이나 이메일, 대화방, 채팅, 쪽지 등을 통하여 상스러운 욕설과 함께 인신공격 혹은 허위・비방, 그리고 협박하는 글들을 올리는 방식으로 이루어진다.

한 여중생이 채팅과정에서 당한 성적 수치심을 이기지 못해 자살한 사건, 또한 최근에 일어난 온라인 욕설이 오프라인 폭력으로 변한 사건 등을 종합해 보면, 사이버공간에서의 인신공격・언어폭력・협박 등은 이미 위험수위를 지나쳐 피해 당사자에게 씻을 수 없는 상처를 주는 범죄행위가 되고 있다.[52] 특히 청소년들의 경우 네티켓이 성숙하지 못하고, 심리적인 자제력이 충분하지 못하기 때문에 쉽게 인신공격・언어폭력・협박의 가해자 혹은 피해자가 될 수 있다.

3. 유 형 Ⅲ :

1) 단순 해킹

(1) 해킹의 개념

'해킹(hacking)'은 사이버공간에서 공공기관이나 기업, 그리고 개인의 정보에 불법적으로 접근하여 치명적인 피해를 야기하는 범죄이다.[53]

---

52) 서울경찰청 사이버범죄 수사대는 2004년 6월 11일 인터넷 카페에서 만난 동호회원들과 변태 성행위 등을 한 뒤 "가족에게 이 사실을 알리겠다"고 협박해 돈을 뜯어내려한 혐의로 백모씨(27)를 구속했다(헤럴드 경제, 2004년 6월 11일자).

사전적 의미로서의 해킹이란 컴퓨터 시스템에 불법적으로 접근하여 데이터를 빼내거나 파괴하는 행위이다. 구체적으로는, 컴퓨터를 이용하여 다른 사람의 정보처리장치 또는 정보처리조직에 침입하거나 기술적인 방법으로 다른 사람의 정보처리장치가 수행하는 기능이나 전자기록에 함부로 간섭하는 일체의 행위를 말한다(백광훈, 2000:59).

일반적으로 해킹은 전산망 해킹, 개인 PC 해킹, 아이디와 비밀번호, 주민등록번호의 도용을 위한 해킹, 인터넷 도·감청 해킹, 허위 주민등록번호와 신용카드번호 생성을 위한 해킹, 주식·사이버머니 해킹 등으로 분류된다(사단법인 한국사이버감시단, 2001).

⑵ 해킹피해 현황

현재 해킹과 관련된 피해사례는 기하급수적으로 증가하고 있으며, 공공기관이나 기업뿐만 아니라 보안성이 취약한 윈도우 운영체제를 주로 사용하는 개인 네티즌들의 피해가 크게 늘어나고 있는 실정이다.

해킹피해와 관련된 문제가 본격적으로 논의되기 시작한 1996년의 경우 147건에 불과하던 해킹피해 건수는 2000년 1,943건을 기점으로 하여, 2001년 5,333건, 2002년 15,192건, 2003년 26,719건으로 해마다 급속하게 증가하고 있는 실정이다.[54] 아래의 <표 3-29>는 연도별 해킹피해 현황을 보여주고 있다.

<표 3-29> 연도별 해킹피해 현황(1996 - 2003)

연 도	1996	1997	1998	1999	2000	2001	2002	2003
건 수	147	64	158	572	1,943	5,333	15,192	26,719

(출처 : 한국정보보호진흥원)

53) 최근 국내에서 발생한 해킹사례로는 2004년 7월 2일 저녁 서울시청 홈페이지를 대학생 장모씨(23)가 해킹하여 관리자 권한으로 서울의 버스운영체계개편에 대한 여론조사를 임의로 실시한 사건, 2004년 6월 국방연구원, 국방과학연구소, 원자력연구소, 해양수산부, 해양경찰청, 중소기업청 등 6개 정부기관이 해킹 프로그램에 감염된 사건, 2004년 3월 이라크 전쟁 반대 등 반전을 표방하며 국내 60여개 사이트를 포함, 전세계적으로 1,000여개의 사이트를 해킹한 브라질의 해킹조직 '사이버로드스' 사건 등이 대표적이다.

54) 해킹피해와 관련된 통계수치는 일반해킹을 포함하여 일반 웜, 스펨릴레이 등 해킹과 관련된 사항을 통합하여 나타낸 수치이다.

한편 <표 3-30>에서 보는 바와 같이, 해킹범죄는 대학, 기업, 연구소 및 비영리단체, 그리고 개인 등에 대해서 무차별적으로 이루어지고 있는 실정이다. 특히 개인은 전체 해킹피해 건수의 대부분을 차지할 정도로 해킹에 거의 무방비 상태로 노출되어 있다고 할 수 있다.

<표 3-30> 기관별 해킹피해 현황(2001~2003)

기 관	도메인	2001	2002	2003
대 학	ac	937	1,812	2,416
기 업	co	308	716	705
비영리	or	32	154	126
연구소	re	7	22	14
네트워크	ne	0	4	32
기타(개인)		1,243	3,736	9,058
총 계		2,527	6,444	12,351

(출처: 한국정보보호진흥원)

⑶ 청소년의 해킹범죄 실태

해킹범죄의 특성은 컴퓨터와 인터넷 등에 대한 전문적인 지식을 요한다는 점이다. 따라서 해킹을 행하는 청소년들의 경우 또래집단 보다 컴퓨터와 인터넷 등에 대한 풍부한 지식을 소유하고 있는 경우가 많다. 그러나 성인과 동일하게 전문적 기술을 요함에도 불구하고 청소년들이 저지르는 해킹범죄는 성인들의 경우와는 다른 양상을 보이는바, 청소년들의 해킹범죄는 주위에 자신의 실력을 뽐내기 위한 과시형 해킹의 경우가 많으며, 해킹범죄를 저지르고 난 후에도 특별한 죄의식을 느끼지 못하는 경우가 많다.

청소년들이 많이 범하는 해킹의 유형으로는 게임 아이디와 패스워드 해킹, 주민등록번호와 이메일 해킹 등이 있으며, 주로 게임중독[55]이나 유료콘텐츠 사업의 성장을 배경으로 하여 나타나는 게임 아이템이나 아바타(avatar)[56] 등에 대한 소유욕구, 그리고 특정

55) 게임중독이란 과도한 게임으로 정신적, 육체적, 물질적으로 생활에 지장을 받고 있는 상태를 말한다. 특히 온라인게임은 컴퓨터와 인간이 아닌 사람과 사람이 경쟁, 협력하는 게임으로 중독성이 더 강하다. 게임중독 증상은 스스로 통제가 불가능하며 일상생활이 어려워지고 대인기피증을 보인다. 증상이 심하면 가출해 PC방을 전전하기도 하고 학교, 직장을 그만두기도 한다.

56) 아바타란 간단히 표현하자면, 사이버공간에서 자신을 나타내는 캐릭터 분신이다. 최근 이러한 아바타를 구입하기 위해 발생하는 청소년 문제가 심각하게 대두되고 있다. 실제로 아바타를 구입하기 위해 6개월

대상물이나 특정인에 대한 호기심을 바탕으로 하여 일어나는 경우가 많다.

게임중독의 경우 본인 혹은 피해자 중 어느 한쪽이 게임에 중독 되어 해킹을 통하여 아이템을 취득하거나, 또는 해킹으로 취득한 아이템을 다른 청소년들에게 되파는 형식, 그리고 그에 동반되어 나타나는 인터넷 사기의 형태로 발생하고 있다.[57] 그리고 대부분의 인터넷 사이트가 유료로 제공하고 있는 아바타는 지나치게 높은 가격(1개당 100 - 12,000원)으로 과소비(1인 평균 5,000~30,000원/월)를 조장해 어린 네티즌들이 거액을 낭비하게 하고, 지불능력이 없는 청소년들이 그러한 돈을 마련하기 위한 수단으로 다시 해킹을 하게하는 경우가 많다(공병철, 2003). 또한 성인사이트 등에 대한 접속을 위해 주민번호를 해킹한 후 도용하거나, 연예인이나 관심이 있는 또래의 이성이나 동성의 이메일, 아이디, 패스워드를 해킹하여 사생활에 대한 호기심을 충족시키는 등의 해킹 유형이 많이 발생하고 있다.

2) 사이버 절도

(1) 사이버절도의 개념

온라인 게임을 즐기는 네티즌 사이에서 흔히 발생하는 사이버절도는 그 개념을 별도로 명문화하고 있지 않으므로 기존의 절도죄와 결부시켜 파악할 수 있다. 즉 광의의 사이버절도는 타인의 컴퓨터에 저장된 파일을 몰래 자신의 공CD에 복사하는 행위, 컴퓨터 등의 정보처리장치와 관련한 절도행위 등을 포함한 사이버상에서 벌어지는 모든 절도행위를 말할 수 있지만, 일반적으로 논의되는 협의의 사이버절도는 인터넷상에서 발생하는 온라인게임 아이템 절도, 정보통신시스템의 내부 절도, 컴퓨터 프로그램 절도, 개인정보의 도용과 관련된 절도행위 등을 말한다.

사이버절도의 대표적인 형태인 아이템 절도에는 아이디나 아이템 판매와 관련된 절도

간 170만원을 썼던 13세의 초등학생이 부모의 꾸중이 두려워 2003년 5월 자살하는 사건이 발생하기도 했다(미디어오늘, 2003년 8월 1일자).

57) 일간스포츠, 2004년 6월 3일자; 경찰청 사이버테러대응센터의 분석에 따르면 2003년도 한해 동안 발생한 청소년들의 사이버범죄 중 해킹과 인터넷 사기가 전체의 70%를 차지하고 있으며, 이러한 수치는 하루 평균 28명이 사이버범죄 전과자로 전락하는 것이다.

혹은 사기, 그리고 해킹을 이용한 아이디 및 아이템 절도행위가 있다.

첫 번째, 아이디·아이템 판매와 관련된 절도 및 사기 행위로는 아이디나 아이템을 판매한다고 광고를 한 후 돈을 입금하면 잠적해 버리는 경우, 아이디나 아이템을 서로 교환하자고 유도한 후 자신의 아이디와 아이템은 주지 않고 상대방의 아이디와 아이템을 가로채는 경우, 다른 사람의 아이디나 또는 유사한 아이디로 접근하여 친구나 잘 아는 사람처럼 속여서 아이디나 아이템을 절도하는 행위, 운영자를 사칭하여 상대방의 비밀번호를 요구하여 아이디와 아이템을 절도하는 경우 등이 있다.

두 번째 유형인 해킹을 이용한 아이디·아이템 절도행위로는 온라인 게임업체에서 제공하는 게임 중 특정 프로그램을 이용하여 아이디를 크래킹하여 그 아이디와 아이템을 절도하는 행위, 온라인상에서 정보를 제공하여 준다고 현혹하여 상대방에게 해킹툴을 보내어 그 프로그램을 이용하여 상대의 아이디와 아이템을 절도하는 행위, 남이 가지고 있는 좋은 아이템을 빼앗기 위해 스스로 플레이어킬러(PK: 살인자)가 되어 아이디와 아이템을 절도하는 행위가 있다(한국사이버감시단, 2001:423-424).

⑵ 사이버절도의 실태

사이버절도에 있어서 두드러진 양상은 온라인 게임업체가 늘어나고 그 이용자도 폭발적으로 증가함에 따라 게임 아이디나 게임상의 가상 아이템이 게임을 하는 네티즌들에게는 현실의 아이템 만큼이나 값진 것이 되어버렸고, 그로 인하여 이러한 아이템 절도가 과거에 비해 급속히 증가하고 있다는 점이다.

사이버절도의 보편적인 유형은 개인신상정보를 도용해 포털사이트에 가입하여 타인의 사이버머니를 훔쳐 부당 이득을 취한 후 다른 네티즌에게 되파는 형태이다. 그러나 이러한 고전적 유형의 사이버절도가 사법당국에 의하여 적발된 후 처벌되는 사례가 빈발하자,[58] 최근에는 사이버절도가 상당히 기발한 형태의 지능형 범죄로 발전하고 있다.

---

58) 서울지법 형사2 단독 염기창(廉基昌)판사는 30일 타인의 주민등록번호를 이용해 게임사이트 회원으로 가입한 뒤 사이버 게임에 사용되는 사이버 머니를 빼내 판매한 혐의(정보통신망이용촉진등에관한법률 위반) 등으로 기소된 컴퓨터 프로그래머 金모(25)씨 등 4명에게 각각 징역 1-2년을 선고했다(중앙일보, 2001년 10월 30일자).

즉 이전의 단순한 게임아이템 등의 절도 방식에서 벗어나 일반주택의 유선전화를 이용하여 사이버머니를 훔치거나,[59] 운영자를 사칭하여 아이디와 패스워드를 알아낸 뒤 사이버머니와 아이템을 절도하는 등 점차 지능형 범죄로 발전하고 있다.

(3) 청소년의 사이버절도 실태

청소년들에 의한 사이버절도도 성인범과 마찬가지로 날로 지능화, 다양화되어 가고 있다. 최근에 일어난 청소년 사이버절도 사례를 보면, 성인범과 같이 해킹프로그램을 통하여 타인의 게임 아이디와 비밀번호를 알아낸 뒤 아이템을 훔치는 경우가 가장 빈발하게 발생하고 있다. 예컨대, 부산지방경찰청 사이버범죄수사대는 2000년 14일, 해킹프로그램으로 남의 인터넷 게임 아이디(ID)와 비밀번호를 알아낸 뒤 그 사람의 게임 전리품을 훔친 혐의(정보통신망이용촉진등에관한법률 위반)로 부산 모 중학교 3학년 권모군(15. 부산시 사상구 학장동)을 불구속 입건했다. 권군은 지난 6일 부산시 서구 서대신동 모 게임방의 컴퓨터 2대에 해킹프로그램을 미리 설치해 그 컴퓨터로 '어둠의 전설'이란 인터넷 게임을 즐긴 이모씨(23)의 아이디와 비밀번호를 알아낸 뒤 지난 10일까지 7차례에 걸쳐 이씨의 아이디로 게임망에 접속, 이씨가 6개월간 다른 사람과의 게임에서 이겨 획득한 각종 무기 등 전리품을 훔친 혐의이다(중앙일보, 2000년 1월 14일자).

3) 전자문서의 도용・변조・파괴

일반적인 의미로서의 전자문서는 전자서명을 통해 종이문서의 효력을 갖게 되는 것을 말한다. 전자문서에는 인터넷을 통해 발급되는 모든 문서가 포함된다고 할 수 있다.

현재 사이버공간에서는 전자상거래의 발달, 전자정부의 구현, 전자문서이용촉진법의 제정으로 각종 전자상거래 뿐만 아니라 금융거래, 그리고 정부기관의 각종 공문서도 전자문서로 발급되는 등 전자문서의 사용이 급격히 증가하고 있다. 특히 새로 제정된 전자

---

59)) 다세대주택 1,600여 가구의 유선전화를 무차별 도용, 현금 5천여만원 상당의 사이버머니를 챙긴 신종 '전화요금 도둑'이 붙잡혔다. 범인인 강모씨(29)와 배모씨(28)는 'ㅅ' 포털사이트에서 알아낸 연체자들의 인적사항을 이용하여 아이디를 만든 후 1,650가구의 유선전화를 도용하였으며, 가로챈 돈은 모두 유흥비로 탕진한 것으로 드러났다(경향신문, 2003년 12월 5일자).

문서이용촉진법은 전자상거래의 활성화를 위해 기존의 종이문서 이외에 전자문서의 효력인증을 강화하는 것을 골자로 하고 있다.[60]

그러나 사이버공간에서는 전자문서의 사용증가에 따른 역기능으로 전자문서의 도용·변조·파괴라는 새로운 형태의 사이버범죄가 증가하고 있다.[61] 각종 공문서의 위·변조는 물론이고, 특히 전자상거래에 있어서는 모든 거래가 비대면으로 이루어지기 때문에 관련 전자문서에 대한 위조·변조·파괴가 흔히 나타나고 있다. 따라서 전자문서의 도용·변조·파괴를 막기 위해 사이버공간의 인감도장이라 할 수 있는 '전자서명제도'를 도입하고 있다.[62]

한편 청소년에게 있어서는 전자문서의 위조·변조·파괴는 상대적으로 적게 발생하는 범죄유형이다.

4. 유 형 Ⅳ:

1) 컴퓨터바이러스 유포

(1) 컴퓨터바이러스의 개념

인터넷을 통한 정보의 유통이 보편화됨에 따라 컴퓨터 바이러스 또한 인터넷 경로에 편승하여 그 감염경로를 확대하고 있다. 컴퓨터 바이러스(computer virus)란 컴퓨터 프로그램이나 실행 가능한 부분을 변형시켜 여기에 자신 또는 자신의 변형물을 복사하여 컴퓨터 작동에 피해를 주는 명령어들의 조합을 말하며, 생물학적인 바이러스가 생물체에

---

60) 전자문서이용촉진법은 기존의 상법 등 116개 개별법상에서 종이문서를 의무사용토록 한 규정을 전자문서로 대체하며 또한 전자문서를 집중 관리하는 공인 전자문서보관소에 대한 신설조항을 마련하였다.

61) 2001년 76건에 불과하던 전자문서관련 범죄의 처리건수는 2002년 241건, 2003년에는 561건으로 대폭 증가하고 있는 실정이다.

62) '전자서명'이란 서명 또는 날인의 전자적인 대체물로서, 펜 대신에 컴퓨터를 매개로 하여 생성되는 정보가 송신자의 것임을 보증하고, 내용이 변조되지 않았음을 증명한다. 1024비트의 공개키 방식 암호화 기술이라는 고도의 암호화 기술을 사용해 보안 기능이 가능하다. 공개키 방식이란 송신자가 자신의 비밀키로 정보를 암호화하고 수신자는 송신자의 공개키를 이용해서 이를 해독하는 것. 인터넷 뱅킹이나 온라인 주식거래에 필요한 공인인증서는 국가가 지정한 공인인증기관에서 발행하고 공개키를 관리하는 대표적인 전자서명이다.

침투하여 병을 일으키는 것처럼 컴퓨터 내에 침투하여 자료를 손상시키거나 다른 프로그램들을 파괴하여 작동할 수 없도록 하는 컴퓨터 프로그램의 한 종류이다(한국사이버감시단, 2001).

바이러스의 발생 기원은 1949년 J. 폰 노이만이 발표한 논문에서 프로그램이 자기 자신을 복제함으로써 증식할 수 있다는 가능성을 제시한 것으로부터 유래한다. 실제로 미국에서는 1985년 프로그램을 파괴하는 악성 컴퓨터 바이러스가 처음 보고 되었고, 한국에서는 1988년 (C)BRAIN이란 컴퓨터 바이러스가 처음으로 보고 되었다.

컴퓨터 바이러스가 출현하게 된 경위는 자신의 능력을 과시하기 위하여 만들었다는 설, 불법복제를 막기 위하여 만들었다는 설, 소프트웨어의 유통경로를 알아보기 위하여 유포시켰다는 설, 경쟁자 또는 경쟁사에게 타격을 주기위하여 만들었다는 설 등 다양하다. 그러나 은밀하게 유포되고 있기 때문에 확실한 경위는 밝혀지지 않고 있지만 복합적인 원인 때문일 것으로 추정된다.[63]

안철수연구소에서는 컴퓨터 바이러스의 유형을 크게 두 가지 기준에서 구분하고 있는바, 첫 번째는 감염부위에 따른 분류로써 부트 바이러스(boot virus), 파일 바이러스(file virus), 부트/파일 바이러스(multipartite virus), 매크로 바이러스(macro virus)등이 포함되며, 두 번째 분류방식은 운영체제에 따른 분류로써 도스 바이러스(dos virus), 윈도우 바이러스(window virus), 애플리케이션 파생 바이러스, 유닉스, 리눅스, 맥, OS/2 바이러스, 자바 바이러스(java virus)등이다.[64]

(2) 바이러스 유포의 실태

컴퓨터 바이러스에 감염될 경우 단순히 컴퓨터의 속도가 떨어지는 가벼운 증상이 나타나는 경우도 있고, 소위 악성 바이러스의 경우 컴퓨터의 동작을 중지시키거나 하드디스크의 모든 자료를 삭제하기도 한다. 최근 들어 컴퓨터 바이러스는 마이크로소프트 오피스에서 지원하는 배우기 쉽고 프로그래밍하기 쉬운 매크로 언어를 사용하여 제작할 수 있게 되어 더욱 많은 종류의 바이러스들이 제작·유포되고 있는 추세이다. 특히 인터

63) http://onyu.net/data/virus1.htm#①.

64) http://opendic.naver.com/100/entry.php?entry_id=69643.

넷이 일반화되면서 이메일로 전염되는 바이러스들이 속속 제작되고 있기 때문에 컴퓨터 바이러스의 감염속도와 피해규모가 대형화되고 있다.

한국정보보호진흥원(KISA)에 따르면, 2003년의 경우 지속적으로 Dumaru 웜 바이러스에 의한 피해가 속출하였으며, 2004년도 현재까지의 경우 영문으로 대량 메일을 발송하는 Nesky, Dumaru, Bagle 바이러스 등이 전체의 90% 가량을 차지하고 있다. 이것은 PC 사용자들이 실제 메일과 패치관련 바이러스 메일을 잘 구분하지 못하여 발생하는 피해라 볼 수 있다. 다음 <표 3-31>은 2001년부터 2004년 6월까지 신종바이러스의 출현건수 및 국내의 바이러스 피해신고 접수건수를 나타낸 것이다. 표를 보면 2002년에 신종바이러스 출현건수가 가장 많았으나, 국내의 전체 바이러스 신고건수는 오히려 2003년에 85,023건으로 가장 많았으며, 특히 2004년의 경우 6월까지의 집계임에도 불구하고 72,225건에 달하는 등 최근 바이러스가 광범위하게 유포되고 있음을 알 수 있다.[65]

<표 3-31> 신종바이러스 출현 건수 및 바이러스 피해신고접수 건수

구 분	2001년	2002년	2003년	2004년 6월 현재
신종출현건수	194	232	108	9
피해신고접수건수	65,033	38,677	85,023	72,225

(출처 : 한국정보보호진흥원)

2) 스팸메일 유포

스팸메일(spam mail)은 광고를 목적으로 불특정 다수에게 전달되는 인터넷 전자메일로써, 무작위적으로 추출한 이메일 주소 목록을 이용하여 네트워크를 통해 불특정 다수에게 유포된 광고성 메일을 가리키는 용어이다. 정크 메일(junk mail) 또는 벌크 메일(bulk mail)이라고도 한다.

스팸메일은 크게 상업성 메일, 불법유통물 광고메일, 폭탄메일, 체인메일[66] 등의 4가

65) 이는 또한 네티즌들의 사이버범죄의 심각성에 대한 인식이 증가한 결과일 수도 있다.
66) 체인메일이란 같은 내용의 메일을 무작위로 보내거나 피라미드 형식으로 배포하는 것을 말한다.

지로 구분되며, 주로 개인이나 기업이 불특정 다수에게 광고를 전달하기 위한 방법으로 작게는 수십명, 많게는 수백만명에게 동시에 메일을 발송하여 원하지 않는 사람에게까지 보내어지거나 국가전산망에 부하를 주는 등 인터넷상에서의 쓰레기 정보로 전체 인터넷 이용자들에게 좋지 않은 영향을 준다.

정보통신부가 2003년 발표한 통계보도자료[67]에 따르면, 2001년도에는 불법 스팸메일 전송으로 단 2개의 업체만이 행정처분을 받았던 것에 비해, 2002년에는 총 815개 업체가 과태료(24개) 및 시정명령(791개)을 받은 것으로 나타났다. 구체적으로는 수신자가 수신거부의사를 표시했음에도 불구하고 스팸메일을 재전송하여 총 22개 업체가 과태료 처분을 받았으며, 광고메일 전송시 메일 제목란에 표시해야 하는 '(광고)'문구를 표시하지 않았거나 변칙표시 등을 하여 총 793개 업체가 시정명령 등 처분을 받았다. 그리고 스팸메일을 대량 살포한 업종으로는 인터넷쇼핑몰이 총 593개로 가장 많았으며, 컴퓨터, 영어교육 학원이 총 52개로 그 다음으로 많았다. 성인사이트(48개), 통신사업자(45개), 보험, 신용카드회사 등 금융업체(36개)가 그 뒤를 이었으며, 이메일주소추출기 판매업체도 12개가 있었다. 하지만 이와 같은 행정처분에도 불구하고 스팸메일은 더욱 대량살포되고 있어 공정거래위원회 등 관련기관들은 대책마련에 부심하고 있다.[68]

5. 기 타

1) 불건전(음란, 자살 등) 사이트 운영

당국의 지속적인 단속과 근절대책에도 불구하고 음란사이트 및 자살사이트와 같은 유해 사이트는 독버섯처럼 번지고 있다. 음란사이트는 음란한 사진이나 동영상, 문서 등을 보유하여 접속자에게 자료를 열람하게 하거나 배포하는 사이트로써 현재 인터넷상의 곳

67) http://www.spamcop.or.kr/upload/spam_bb.hwp.

68) 실제로 공정거래위원회는 2004년 7월 6일 무차별적으로 살포되는 스팸메일로부터 네티즌을 보호하기 위해 내년부터 기업들이 광고성 이메일이나 휴대전화 문자메시지를 보내기 전에 반드시 공정거래위원회의 광고메일·메시지 수신 거부자 명단을 확인해야 하며, 수신 거부자로 등록된 사람에게 광고메일을 보냈다가 적발되면 1000만원의 과태료 처분을 받게 되는 '전자상거래소비자보호법' 개정안을 가을 정기국회에 제출할 계획이라고 밝혔다(중앙일보, 2004년 7월 6일자).

곳에 퍼져있으며, 유료 또는 무료로 운영되고 있다. 특히 최근에는 꾸준한 단속을 벌이고 있는 당국의 눈길을 피해 해외를 근거지로 하는 사이트를 개설해 국내 네티즌들에게 유료로 공급하고 있는 실정이다.

인터넷상에서 청소년들은 음란물에 무방비로 노출되어 있다고 해도 과언이 아닐 것이다. 이들은 주로 정보공유를 목적으로 하는 P2P 사이트에 접속하여 음란물을 공유하거나[69] 아이디나 주민등록번호의 해킹, 그리고 성인인증을 거치지 않는 무료 사이트를 통하여 자유롭게 음란사이트에 접속하고 있다. 그리고 각종 포털사이트에서도 쉽게 음란물을 접촉하고 있는바, 그것은 포털사이트들이 금칙어를 지정하지 않거나, 금칙어를 지정하였으나 미흡하게 지정한데서 비롯된 것이다.[70]

한편 자살사이트는 당초 자살을 생각하는 사람들의 고민을 상담해주고 서로 의견을 주고받아 자살을 방지한다는 목적으로 개설된 홈페이지나 게시판이었으나, 최근 들어 이러한 게시판에는 자살방법과 같은 자살에 관한 정보들이 다양하게 소개되어 오히려 자살을 조장하는 결과를 낳고 있다.[71] 그러나 무엇보다 중요한 점은 정신적 미성숙 단계로 입시에 대한 스트레스, 가정내 불화, 이성문제 등 다양한 문제에 노출되어 있는 청소년들에게 자살사이트는 그야말로 무서운 인터넷 공간이 될 수 있다는 것이다.[72]

---

69) 실제로 P2P(커뮤니티 파일공유 사이트)사이트는 청소년들이 음란물과 접할 수 있는 가장 손쉬운 접근방법이다. 국무총리 산하 청소년보호위원회의 조사 결과에 의하면 2004년 6월 한 달 동안 청소년들이 자주 접하는 포털사이트 10곳과 P2P 사이트 4곳을 모니터한 결과 P2P 사이트에서 유통되는 자료의 절반 이상이 음란물이었다고 한다(국민일보, 2004년 7월 7일).

70) 청소년보호위원회의 조사보고서에 따르면 유명 포털사이트 중에서 싸이월드와 드림위즈는 검색과정에서 금칙어 지정이 전혀 안 돼 있다는 점이 큰 문제로 지적되었다. 나름대로 금칙어를 지정한 네이버, 다음 등과는 달이 이들 사이트에서는 '섹스'라는 단어를 입력하면 관련 클립이 쉽게 검색된다는 것이다(전자신문, 2004년 7월 8일자).

71) 자살사이트를 통해 자살을 공모하고 동반 자살하는 경우가 많이 발생하고 있다. 올해의 경우에도 전북 무주의 20대 남녀 3명의 음독자살(자살방조 2명 검거), 강원도 강릉 여관에서의 20대 남녀 음독자살, 강원도 홍천에서의 남성 3명의 차량내 자살기도 등외에 여러 사건 모두가 자살사이트를 통해 자살을 기도한 사건들이다.

72) 인터넷상의 자살 사이트가 독버섯처럼 청소년들을 유혹하고 있다. 이들 사이트는 아직 이성적인 사고가 확립되지 않아 새로운 것을 무비판적으로 받아들이기 쉬운 청소년들에게 직접적인 위해를 끼칠 수 있다는 점에서 사회문제로 부각되고 있다. 2001년 2월 6일 전남 목포시와 충북 청주시에서 평소 자살사이트에 접속했던 것으로 알려진 초등 초등학생과 중학생이 스스로 목숨을 끊었다. 2001년 2월 6일 오후 9시경 전남 목포시 상동 B아파트 뒤편 화단에 이 아파트에 사는 초등학교 6년생 A군(13)이 떨어져 숨져 있는 것을 이 아파트 주민이 발견, 경찰에 신고했다. A군은 평소 학교생활에 별다른 문제는 없었으나

2) 신종사이버범죄 - '인터넷 방법'

인터넷상에 등장한 신종 사이버범죄의 한 가지 유형으로 '인터넷 방법'이 있다. 인터넷 방법이란 다수의 네티즌들이 한 대상에 대하여 집중적으로 공격하는 것을 말하는 것으로, 사회적으로 큰 이슈에 있어서만이 아니라 부당한 판매행위를 알려 소비자 권익을 보호하는 등 개별적인 사안에도 광범위하게 이루어지고 있다. 이러한 인터넷을 통한 집단적 여론표출은 소비자의 주권을 신장시키고 참여민주주의를 발전시키는 긍정적인 측면도 있지만, 때로는 '왕따 동영상'[73]이나 '안티 문희준 사건'[74]처럼 '방법'을 당하는 대상에게 치명적인 결과를 초래하기도 한다.

PC방을 즐겨 드나들었으며, 친구들에게 '자살사이트에 접속해 보았다'고 말한 것으로 알려졌다. 그는 유서에서 "죽고싶다. 사후세계도 궁금하다"고 밝혔다(동아일보, 2001년 2월 7일자).

73) 한 중학교에서 같은 반 친구를 왕따시키며 폭행하는 장면을 학생들이 촬영해 유포한 사건으로 학교 교장이 자살한 사건이다.

74) 가수 문희준에 대한 네티즌의 인신모독성 공격, 허위사실의 유포로 인하여 네티즌을 고소한 사건이다.

제4장 현행 사이버범죄 예방·규제 전략과 현황

제1절 개 관

21세기 지식정보사회의 부산물인 사이버범죄를 예방·규제하고 정보통신윤리를 확립하기 위한 우리사회의 노력은 정부 및 형사사법기관, 정보화 관련 공공기관, 정보통신사업자단체, 시민단체 및 언론기관 등 다양한 주체들에 의해 다양한 방법으로 진행되어 왔다.

우선 정부는 국가 IT전략과 함께 정보화의 역기능에 대응하여 정부조직을 개편하는 등 다양한 정책을 추진하고, 사이버범죄를 규제하기 위한 특별법을 제정하거나 개정하는 등 법제정비 작업을 해왔다. 경찰, 검찰 등 국가형사사법기관들은 사이버범죄를 전담하기 위한 부서 및 조직을 새로 구성하거나 확대개편하고 전담 수사인력의 양성과 국제공조에 주력해 왔다. 한국정보보호진흥원, 한국정보문화진흥원 등 정보화관련 공공기관들은 정보통신부 및 국가정보원을 중심으로 해킹, 바이러스 등 사이버침해사고에 대응한 체제정비 및 기술개발을 위해 노력해 왔다. 특히 1995년에 발족한 정보통신윤리위원회는 각종 윤리강령을 제정·선포하고 정보통신윤리 교육을 실시함으로써 사회일반의 정보통신윤리 의식을 고양·정착시키기 위한 많은 노력을 기울여왔다.

한편 정보화 역기능의 해소와 사이버범죄의 예방은 정부 및 공공기관의 노력만으로는 불가능하다. 이점에서 정보통신사업자단체, 시민단체, 언론단체 등 민간의 자체적 노력이 필수적이다. 특히 사업자단체들의 자율정화활동은 인터넷 환경이 그 특수성(개방성·가변성·쌍방향성)으로 인하여 기존의 공적규제만으로는 규제의 실효성을 달성하기 어렵다는 점에서 의의가 있다고 할 것이다. 마지막으로 인터넷 역기능의 예방과 청소년선도 및 사회정의의 실현을 목적으로 하는 다양한 시민단체와 언론단체의 참여가 이어졌는데, 이들의 노력은 인터넷이 가져온 거대한 변화의 소용돌이 속에서 건전한 사이버문화를 만들어 가는데 중요한 역할을 담당하고 있다고 할 것이다.

제2절 정부부문의 대응

1. 사이버범죄에 대응한 정부조직의 개편

21세기 지식정보사회로의 급속한 변화와 새로운 경제 패러다임의 등장은 인터넷 시대에 보다 적합한 새로운 대응전략을 요구하였다. 이에 우리나라도 1990년대부터 세계 각국의 IT전략에 적극 대응하여 미래 지식정보사회를 향한 범국가적인 정보화를 추진하였으며, 그 결과 세계적인 초고속 정보통신 인프라를 구축하게 되었다.

그러나 정보화의 진전에 따라 인터넷상에 유통하는 불건전정보가 급증하고, 해킹 사고 및 바이러스 유포, 개인정보 침해 등 정보화 역기능 문제가 사회문제로 대두되었고, 정보통신부는 정보보호 및 정보화 역기능 문제에 종합적으로 대처하기 위해 관련 업무를 전문적으로 추진할 전담조직이 필요하다고 인식하였다.

정부조직측면에서 이루어진 그 동안의 변화를 살펴보면, 국가전략사업으로 초고속정보통신기반 구축사업을 추진하기 위해 1994년 8월 체신부에 초고속망구축기획단을 설치하고, 1994년 12월 정부조직 개편시에 체신부를 정보통신부로 확대 개편하여 산업자원부, 과학기술부, 공보처 등에 분산되어 있던 정보통신 및 방송관련 업무를 정보통신부로 일원화하였다.

또한 1996년 5월 대통령 주재 정보화추진확대 보고회의에서 대통령은 범국가적인 정보화 추진을 위해 정부내에 정보화 전담조직을 만들 것을 지시하여 1996년 6월 정보통신부내에 정보화기획실을 신설하였다.

정보화촉진정책의 효율적 추진을 위하여 정보통신정책실의 정보화 관련기능을 신설된 정보화기획실로 이관하고, 기획총괄과, 정보화제도과, 정보화지원과, 초고속망기획과, 초고속망구축과 및 정보보호과를 두고 분산되어 있는 정보화 및 정보통신망 관련기능과 초고속정보통신기획단을 흡수 통합하였다.

정보화기획실은 국가사회 정보화 정책 및 시책의 수립·시행에 관한 실무를 총괄하여 최고심의기관인 정보화추진위원회의 운영을 실질적으로 뒷받침하고 있다. 주요업무로는 정보화촉진기본계획 수립을 중심으로 국가사회의 정보화 확산, 정보화관련 법·제도 정비와 정보문화 확산, 분야별 정보화사업 지원업무와 정보기술의 조사·보급, 인터넷 기

본정책 수립 및 기반확충, 초고속국가정보통신망 구축계획 수립·추진 및 이용제도 수립, 정보보호 및 정보화 역기능에 관한 대책 수립 추진과 정보통신기반의 보호, 정보이용의 보호와 개인정보의 보호, 정보보호 기술개발 및 정보보호산업의 육성 등을 들 수 있다.

한편 정보화의 진전에 따른 정보화 역기능 문제가 사회문제로 대두되면서 정보통신부는 이러한 정보보호 및 정보화역기능 문제에 종합적으로 대처하기 위해 정보보호 업무를 전문적으로 추진할 전담조직이 필요하다는 점을 인식하고, 1999년 10월 22일 국무회의에서 '정보화역기능 방지를 위한 정보보호 종합대책'을 보고하면서 정보통신부를 포함한 관계부처의 정보보호 전담 조직 보강의 필요성을 보고하고, 2000년 1월 28일 정보화기획실 소속으로 국장급 정보보호심의관과 3개의 과를 신설하여 그 정원은 30명으로 하였다.

구체적인 구성을 살펴보면, 당초 정보화기획실에 설치되었던 정보보호과를 정보보호기획과로 개편하여 정보보호기본정책 수립, 해킹 바이러스 대응, 전자서명 및 암호이용 활성화, 주요정보통신기반보호에 대한 보호정책의 수립·추진, 한국정보보호진흥원 지원·육성 관련 업무를 담당케 하고, 정보이용보호과에서는 불건전정보 유통방지, 정보통신망을 통한 사생활침해 방지, 인터넷을 이용한 불법행위 및 사회적·개인적 역기능 방지, 사이버 공간에서의 이용자 권익보호, 개인정보 보호, 스팸메일 최소화 등의 업무를 담당케 하였으며, 정보보호산업과에서는 정보보호 산업육성, 정보보호관련 기술개발 및 표준화 추진, 인력양성, 정보보호 관리체계 인증 및 정보보호전문업체 지정제도 운용, IC카드, 전자지불 정책 추진, 정보보호시스템의 평가 및 제도개선 정책 시행 등의 업무를 수행토록 하여, 불건전정보 유통 단속 및 건전한 사이버문화 정립 관련 업무는 정보이용보호과에서 담당하게 되었다.

특히 2003년 1·25 인터넷 침해사고를 계기로 정보보호 강화대책을 적극적으로 추진하기 위하여 인터넷침해사고 발생 시 신속한 대응과 원인분석 등을 위해 네트워크를 24시간 모니터링 하는 인터넷침해사고대응지원센터를 구축하고 인터넷대응지원팀을 구성, 운영하고 있다.

2. 정책추진현황

정보화와 관련된 1990년대 중반까지의 정부정책은 주로 정보통신 인프라의 고도화에 집중되어 있었으나, 1990년대 후반 정보화의 역기능 문제가 심각하게 대두되자 각종 불법·유해정보로부터 정보이용자를 보호하기 위한 정책이 추진되었다.

1) 1990년대의 정책추진현황

1990년대에 있어서의 정부의 정책추진 현황을 보면, 1995년 4월 정보통신서비스를 이용한 불건전정보의 유통을 방지하고, 건전한 정보이용문화를 확립하기 위해 전기통신사업법에 제53조의2를 신설하여 정보통신윤리위원회를 법정위원회로 설치하였다.

이후 1996년에 접어들면서 PC통신, 국제폰팅, 국내폰팅, 700번 전화정보서비스 등이 활성화되어, 동 서비스를 이용한 불건전정보의 유통, 사생활 침해 등 정보화 부작용이 사회적인 문제로 대두되기 시작하면서 건전한 정보이용문화 확립, 불건전정보 단속을 위한 정책을 수립하였으며, 전기통신기본법 제48조의2를 신설하여 정보통신망을 통하여 음란한 정보를 유통하는 행위를 처벌할 수 있는 법적근거를 마련하였다.

또한 1997년에는 전기통신사업법 시행령을 개정하면서 제16조의4를 신설하여 정보통신윤리위원회의 시정요구 기능을 추가함으로써 온라인상의 불건전정보에 대해 즉각적으로 대응할 수 있는 근거를 마련하였다.

이어 1999년에는 4월 초순 한국정보보호센터(2001년 7월 한국정보보호진흥원으로 개칭), 한국전자통신연구원, 정보통신정책연구원, 한국전산원 등의 전문가로 『정보화역기능 방지 전담반』을 구성하여 '정보화역기능 방지를 위한 종합대책'의 마련에 착수하였고, 동년 4월 11일 국무회의에서 정보통신부장관은 인터넷에서 유통되는 정보의 10%가 음란물 등 불건전정보로 추정됨에 따라 정보화역기능 방지를 위한 종합적이고 근본적인 대책을 수립하겠다고 밝혔다.

따라서 1999년 7월에는 '정보화역기능 방지를 위한 종합대책' 초안이 마련되었으며, 8월부터 9월까지 관계부처 의견수렴 및 공청회 개최를 통하여 관계 전문가들의 의견을 수렴, 10월 22일 '정보화역기능 방지를 위한 종합대책'을 국무회의에 최종 보고하여 확정하였다.

2) 2000년대의 정책추진현황

2000년대에는 전국 어디에서나 인터넷의 사용이 가능해지고, 인터넷 사용자가 급증함에 따라 그에 따른 역기능이 더욱 심화되었다. 따라서 정부는 이러한 문제들에 대한 대응책을 다각도로 모색하기 시작하였다.

이와 같은 정책의 일환으로 2000년도에는 불건전정보의 단속과 함께 건전한 정보통신윤리 확산에 기여하기 위하여 「청소년권장사이트제도」를 도입하였으며, 2000년 5월에는 사이버성폭력신고센터(www.gender.or.kr)를 정보통신윤리위원회 내에 설치하여 사이버성폭력 피해신고 접수 및 법률자문 등의 상담을 하고, 사이버성폭력 예방수칙 및 대응요령 등에 대한 교육 및 홍보, 사이버 성폭력 정보에 대하여 정보통신윤리위원회가 심의할 수 있도록 하는 역할을 수행하였다.

한편 2001년도에는 인터넷상의 자살, 폭탄제조, 아동포르노 등 불법·유해정보가 더욱 심각한 사회문제로 대두되자 동년 2월 '불법·유해정보에 대한 종합대책'을 수립하여 불법·유해정보의 단속, 시민단체의 민간감시망 구축지원, 사업자단체의 자율규제 지원, 유관기관과의 협력체계 강화 등을 추진하였다.

2002년도에는 6월 27일 헌법재판소가 전기통신사업법 제53조(불온통신의 단속) 및 동법시행령 제16조에 대하여 명확성 원칙, 과잉금지원칙, 포괄위임입법금지원칙에 위배되어 헌법에 위반된다고 판결함에 따라 동 조항에 대한 개정을 추진하여 2002년 12월 동법을 개정·시행하였다. 또한 정보이용자의 권익보호를 위하여 2001년 11월 확대 개편한 「사이버인권침해방지지원센터」를 2002년 10월 「사이버명예훼손·성폭력상담센터」로 명칭을 변경하여 운영의 효율성을 제고하였다.

2003년도의 경우 크게 세 가지의 방향에서 정책을 추진하였다. 첫째, 불법·유해정보 유통확산, 인터넷 오·남용 등 인터넷 역기능 방지를 위해 관련 정부기관, 민간단체, 사업자 등이 참여하는 범사회적 「민·관 합동 스팸메일 대책위원회」를 구성, 운영하여 불건전정보 유통방지를 위한 범사회적 공감대를 조성하였다. 또한 동년 5월에는 「청소년유해매체물표시방법 고시」개정을 통하여 청소년들이 자신의 의사와 무관하게 초기화면에서 청소년유해매체물을 접하게 되는 경우를 차단하였다.

두 번째의 정책추진 방향으로 민간 자율의 정화 활동을 강화하였다. 민간자율규제 활

성화를 위하여 민간단체 실무자 모니터링 전문교육, ISP사업자의 한글제공 불법사이트 차단활동 지원 등의 민간자율규제활동 지원사업을 추진하였으며, 해외 서버를 이용한 한글불법사이트를 국제 관문에서 전기통신서비스사업자가 원천차단할 수 있도록 DB를 제공하고, 인터넷 유해정보로부터 청소년보호를 위한 초고속통신망사업자의 유해정보차단 서비스 확대를 유도하고 있다.

셋째, 건전한 사이버문화 조성을 위하여 『e-Clean Korea』캠페인, 정보통신윤리 홍보대사 위촉 등의 교육·홍보활동을 강화하였으며, 학부모 인터넷교실 운영, 청소년 특강 등 다양한 형태의 정보윤리 교육을 실시하였다(정보통신윤리위원회, 2002, 2003).

제3절 사이버범죄 규제법제

현행 사이버범죄 또는 컴퓨터범죄 규제법규는 단일 법령으로 통일되어 있지 않고 매우 다양한 법령에 분산되어 있다. 이 절에서는 그러한 법령들 중에서 먼저 정보통신윤리 관련 법령과 형법 및 형사특별법을 간단히 개요한 후, 주요 사이버범죄의 유형별로 그 처벌조항을 살펴보기로 한다.

1. 정보통신윤리 관련 법제[75]

정보통신윤리와 관련된 법제는 정보화촉진기본법, 전기통신기본법, 전기통신사업법, 정보통신망이용촉진및정보보호등에관한법률 등에 규정되어 있다. 정보화촉진기본법에는 건전한 정보통신윤리 확립을 위한 기본적인 내용이 규정되어 있고, 전기통신사업법에는 불온통신의 개념과 정보통신부장관의 취급거부명령권, 정보통신윤리위원회 관련 내용이 규정되어 있으며, 전기통신기본법에는 음란물 유포에 대한 처벌사항이, 그리고 정보통신망이용촉진및정보보호등에관한법률에는 정보통신망에서의 청소년보호에 관한 사항과 사이버명예훼손에 대한 처벌, 정보통신서비스제공자에 대한 정보이용자의 정보삭제요구권 등에 대해 규정되어 있다.

75) 정보통신윤리위원회(2002, 2003).

1) 정보화촉진기본법

정보화촉진기본법은 국가의 정보화를 촉진하기 위한 기본법으로, 정보문화 및 정보통신윤리와 관련하여서는 1995년 제정(법률 제4969호) 당시에 동법 제12조(정보문화의 확산)에서 정보화촉진 등이 활성화될 수 있도록 홍보 및 교육의 확대 등을 규정하였고, 1999년 1월 21일 개정(법률 제5669호)시에 건전한 정보통신윤리 확립을 위하여 제12조의2(건전한 정보통신윤리의 확립)를 신설하여 미풍양속을 해치는 불건전한 정보의 유통을 방지하고 건전한 국민정서를 함양하며 불건전한 정보로부터 청소년을 보호하기 위하여 필요한 시책을 강구하도록 하였고, 동법 시행령 제11조의2(건전한 정보통신윤리의 확립)를 신설하여 청소년이 정보통신서비스를 건전하게 이용하게 하기 위하여 필요한 관리적·기술적 조치 등에 관한 기준을 정하여 권고할 수 있도록 하였다.

2) 전기통신기본법

전기통신기본법은 전기통신정책을 종합적으로 수행할 수 있도록 하기 위해 전기통신 각 분야에 공통으로 적용되는 기본적이고 종합적인 사항을 규정한 법으로, 정보통신윤리와 관련하여서는 1996년 12월 30일 개정(법률 제5219호)시 전기통신사업법에서 규정하고 있는 불온통신 단속의 운영상 미비점 및 전기통신역무 이용자의 권익보호를 위하여 제48조의2(벌칙)를 신설하여 '전기통신역무를 이용하여 음란한 부호·문언·음향 또는 영상을 판매 또는 임대하거나 공연히 전시한 자는 1년 이하의 벌금에 처한다'고 규정하였다. 그러나 동규정은 관련규정을 종합적으로 규정하기 위하여 2001년 1월 16일 정보통신망이용촉진및정보보호등에관한법률 전문개정시 동법에 관련규정을 신설하면서 전기통신기본법에서는 삭제되었다.

3) 전기통신사업법

전기통신사업법은 전기통신서비스의 이용과 관련된 법으로 정보통신윤리와 관련하여 1991년 8월 10일 전문개정(법률 제4394호)을 하면서 법 명칭을 공중전기통신사업법에서 전기통신사업법으로 변경하였고, 전기통신의 건전한 발전과 이용을 도모하기 위하여 제

53조(불온통신의 단속)를 신설하여 공공의 안녕질서 또는 미풍양속을 해하는 것으로 인정되는 통신을 금지하고, 이러한 통신에 대하여는 정보통신부장관이 전기통신사업자로 하여금 그 취급을 거부·정지 또는 제한할 수 있도록 규정하였다. 또한 동법 시행령 제16조(불온통신)에서는 불온통신의 개념을 구체화하여 범죄를 목적으로 하거나 반국가적 행위의 수행을 목적으로 하는 경우 및 선량한 풍속 기타 사회질서를 해하는 내용의 전기통신으로 규정하였다. 그러나 2002년 6월 27일 헌법재판소가 전기통신사업법 제53조(불온통신의 단속) 및 동법시행령 제16조에 대하여 명확성 원칙, 과잉금지원칙, 포괄위임입법금지원칙에 위배되어 헌법에 위반된다고 판결함에 따라 동 조항을 개정하였다. 주요 개정내용은 금지대상을 불온통신에서 음란한 정보유통, 명예훼손, 스토킹, 해킹, 바이러스 유포, 사행심 조장 등 9개 항목으로 분류한 현행법상 불건전정보로 한정하여 명확히 하였다. 또한 정보통신부장관의 명령권 행사의 대상이 되는 전기통신사업자 및 전기통신이용자에게 행정절차법상 사전에 의견을 제출할 수 있는 권한을 명시적으로 보장하였고, 정보통신부장관의 불법정보에 대한 시정명령권행사는 정보통신윤리위원회의 전심절차를 거치도록 규정하고 있다. 이와 함께 공청회를 통하여 제기된 의견을 반영하여 정보통신윤리위원회의 위원을 위촉하는 때에는 법조계 인사 및 이용자단체 인사가 각각 위원 총수의 5분의 1 이상이 되도록 위촉하여 위원회의 전문성을 유지할 수 있도록 하였다.

4) 정보통신망이용촉진및정보보호등에관한법률

1999년 2월에는 기존의 전산망보급확장과이용촉진에관한법률(1986년 제정)이 정보통신망이용촉진등에관한법률(법률 제5835호)로 전문개정 되면서 정보통신망 이용의 활성화, 개인정보보호 등 정보이용 질서에 관한 내용을 신설하여 재구성되었다. 정보통신망이용촉진등에관한법률은 2001년 1월 16일 정보통신망의 이용촉진 등에 관한 사항에 정보통신서비스 이용자의 개인정보보호제도에 관한 사항이 대폭 규정됨에 따라 법률의 명칭을 정보통신망이용촉진및정보보호등에관한법률(법률 제6360호)로 변경하여 전문 개정되었다. 이 법에서는 정보통신서비스 이용자의 개인정보를 보호하기 위하여 정보통신서비스 제공자에 대한 규제를 강화함과 아울러 인터넷상의 음란·폭력정보로부터 청소년을

보호하고 사이버상의 건전한 정보유통을 위해 사이버 명예훼손 등에 대한 관련규정이 대거 신설되었다.

구체적으로 보면, 인터넷상의 불건전정보로부터 청소년을 보호하기 위하여 '제5장 정보통신망에서의 청소년 보호 등'을 신설하였다. 제5장 제41조(청소년 보호를 위한 시책의 마련 등)에서는 내용선별S/W의 개발 및 보급, 청소년 보호를 위한 기술 개발 및 보급, 교육 및 홍보 등을 규정하였고, 청소년·이용자 관련단체의 청소년 보호활동을 지원할 수 있는 근거를 마련하였으며, 제42조(청소년유해매체물의 표시)에서는 청소년보호법에 의한 청소년유해매체물에 대하여 대통령령이 정하는 방법으로 표시를 하도록 하였다. 또한 건전한 정보유통을 촉진하고, 사이버 명예훼손 등의 피해를 최소화하기 위해 동법 제44조(정보의 삭제요청 등)에서 일반에게 공개를 목적으로 제공된 정보로 인해 법률상 이익이 침해된 자의 경우 정보통신서비스 제공자에게 당해 정보의 삭제 또는 반박내용의 게재를 요청할 수 있도록 하였으며, 요청받은 사업자는 지체 없이 필요한 조치를 취하도록 하였다(제9장 벌칙에 관한 사항은 다음 절: '사이버범죄의 주요 유형별 처벌조항'에서 다룸). 한편 불건전정보의 단속과 별도로 정보이용자에게 유익한 정보의 공급을 확대하기 위해 동법 제10조(정보내용물의 개발지원)에서 정부가 공익을 증진하기 위하여 정보통신망을 통하여 유통되는 정보내용물을 개발하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있도록 하였으며, 국경이 없는 인터넷의 특성을 반영하여 동법 제53조(국제협력)에서 정보통신망에서의 청소년 보호를 위하여 국가 또는 국제기구와 상호협력하도록 규정하였다.

2. 형법 및 형사특별법

1) 형 법

형법 제243조[음화반포등]는 "음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자"에 대한 처벌규정으로서, 컴퓨터 프로그램파일은 위 조문에서 규정하고 있는 문서, 도화, 필름 기타 물건에 해당한다고 할 수 없으므로 음란한 영상화면을 수록한 컴퓨터 프로그램파일을 컴퓨터 통신망을 통하여 전송하는

방법으로 판매한 행위에 대하여 전기통신기본법 제48조(벌칙)의2의 규정을 적용할 수 있음은 별론으로 하고 형법 제243조의 규정을 적용할 수 없다"고 판결한 대법원 판례(98도3140, 99년 2월 24일)가 있다.

2) 성폭력범죄의처벌및피해자보호등에관한법률

성폭력범죄의처벌및피해자보호등에관한법률 제14조(통신매체이용음란)는 "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 자"에 대해 처벌할 수 있다고 하고 있으나, 동법 제15조에서 제14조를 친고죄로 규정함으로써 음란물로부터 피해를 입은 당사자가 고소를 한 경우에만 처벌이 가능하다.

3) 청소년보호법

청소년보호법은 제7조(매체물의 범위) 제4호에서 청소년유해매체물로 심의·결정될 수 있는 매체물의 범위에 전기통신사업법 및 전기통신기본법의 규정에 의한 전기통신을 통한 음성정보, 영상정보 및 문자정보를 포함시키고 있어 정보통신윤리위원회의 심의·결정과 청소년보호위원회의 고시를 통해 청소년유해매체물을 고시하고 있다.

4) 청소년의성보호에관한법률

청소년의성보호에관한법률 제8조(청소년이용음란물의 제작·배포 등)에서는 청소년을 대상으로 한 음란물을 제작·수입·수출하거나 영리를 목적으로 청소년 이용 음란물을 판매·대여·배포하는 행위, 청소년을 청소년이용 음란물의 제작자에게 알선하는 행위에 대하여 규제하는 등 청소년을 이용한 행위에 대해 특별히 단속하고 있다.

3. 사이버범죄의 주요 유형별 처벌조항[76]

사이버범죄의 유형별 처벌조항은 해킹, 바이러스유포, 전자메일관련 범죄, 개인비밀침해, 음란물관련 범죄, 명예훼손, 몰래카메라, 컴퓨터사용사기 등 8가지 주요 인터넷범죄 유형들에 대하여 소개한다.

1) 해 킹

① 정보통신망침해행위금지

제63조(벌칙) 다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 1. 제48조제1항[77]의 규정을 위반하여 정보통신망에 침입한 자. [정보통신망이용촉진및정보보호등에관한법률 제63조 (벌칙)]

② 전자기록 손괴·정보처리장애 업무방해

컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형[78]과 같다. [형법 제314조제2항 (업무방해)]

③ 공용전자기록등의 무효

공무소에서 사용하는 서류 기타 물건 또는 전자기록등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. [형법 제141조제1항 (공용서류 등의 무효, 공용물의 파괴)]

---

76) http://icic.sppo.go.kr

77) 제48조(정보통신망 침해행위 등의 금지) ①누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 아니된다.

78) 5년 이하의 징역 또는 1천500만원 이하의 벌금.

④ 전자기록등의 무효

타인의 재물, 문서 또는 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 그 효용을 해한 자는 3년 이하의 징역 또는 700만원 이하의 벌금에 처한다. [형법 제366조 (재물손괴 등)]

⑤ 데이터부정조작·변작

제227조의2 (공전자기록위작·변작) 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 전자기록등 특수매체기록을 위작 또는 변작한 자는 10년 이하의 징역에 처한다. 제232조의2 (사전자기록위작·변작) 사무처리를 그르치게 할 목적으로 권리·의무 또는 사실증명에 관한 타인의 전자기록등 특수매체기록을 위작 또는 변작한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. [형법]

⑥ 정보통신기반시설 교란·마비·파괴

제12조[79]의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. [정보통신기반보호법 제28조제1항 (벌칙)]

2) 바이러스

① 전자기록 손괴·정보처리장애 업무방해

컴퓨터등 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. [형법 제314조제2항(업무방해)]

79) 제12조 (주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다. 1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위. 2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위. 3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위.

② 공용 전자기록등의 무효

공무소에서 사용하는 서류 기타 물건 또는 전자기록등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. [형법 제141조제1항 (공용서류등의 무효, 공용물의 파괴)]

③ 전자기록등의 무효

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

④ 정보통신기반시설 교란·마비·파괴

제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. [정보통신기반보호법 제28조제1항 (벌칙)]

⑤ 악성프로그램 전달·유포 금지

다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 1.... 4. 제48조제2항[80]의 규정을 위반하여 악성프로그램을 전달 또는 유포한 자. [정보통신망이용촉진및정보보호등에관한법률 제62조(벌칙)]

3) 이메일

① 타인간의 대화등 내용 녹음, 청취, 공개, 누설

다음 각호의 1에 해당하는 자는 7년 이하의 징역에 처한다. 1. 제3조[81]의 규정에 위

80) 제48조 (정보통신망 침해행위 등의 금지) ②누구든지 정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램(이하 “악성프로그램”이라 한다)을 전달 또는 유포하여서는 아니된다.

81) 第3條 (通信 및 對話秘密의 보호) ①누구든지 이 法과 刑事訴訟法 또는 軍事法院法의 規定에 의하지 아

반하여 우편물의 검열, 전기통신의 감청 또는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하거나 그 취득한 통신 또는 대화의 내용을 공개하거나 누설한 자. 2..... [통신비밀보호법제16조 (벌칙)]

② 전자기록 손괴·은닉

컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형과 같다. [형법 제314조제2항(업무방해)]

③ 정보통신기반시설 교란·마비·파괴

제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. [정보통신기반보호법 제28조제1항 (벌칙)]

니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 公開되지 아니한 他人간의 對話를 녹음 또는 聽取하지 못한다. 다만, 다음 各號의 경우에는 당해 法律이 정하는 바에 의한다. <개정 2000.12.29, 2001.12.29, 2004.1.29> 1. 還付郵便物등의 處理:郵便法 第28條·第32條·第35條·第36條등의 規定에 의하여 爆發物등 郵便禁制品이 들어 있다고 의심되는 小包郵便物(이와 유사한 郵便物을 포함한다) 을 개피하는 경우, 受取人에게 配達할 수 없거나 受取人이 受領을 거부한 郵便物을 發送人에게 환부하는 경우, 發送人의 住所·姓名이 漏落된 郵便物로서 受取人이 受取를 거부하여 환부하는 때에 그 住所·姓名을 알기 위하여 개피하는 경우 또는 유가물이 든 還付不能郵便物을 처리하는 경우. 2. 輸出入郵便物에 대한 檢査:관세법 제256조·제257조 등의 規定에 의한 信書외의 郵便物에 대한 通關檢査節次. 3. 拘束 또는 服役중인 사람에 대한 通信:刑事訴訟法 第91條, 軍事法院法 第131條, 行刑法 第18條·第19條 및 軍行刑法 第15條·第16條등의 規定에 의한 拘束 또는 服役중인 사람에 대한 通信의 관리. 4. 破産者에 대한 通信:破産法 第180條의 規定에 의하여 破産者에게 보내온 通信을 破産管財人이 受領하는 경우. 5. 混信除去등을 위한 電波監視:電波法 제49조 내지 제51조의 規定에 의한 混信除去등 電波秩序維持를 위한 電波監視의 경우. ②우편물의 검열 또는 전기통신의 감청(이하 "통신제한조치"라 한다)은 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다. <신설 2001.12.29>. ③누구든지 단말기기 고유번호를 제공하거나 제공받아서는 아니된다. 다만, 이동전화단말기 제조업체 또는 이동통신사업자가 단말기의 개통처리 및 수리 등 정당한 업무의 이행을 위하여 제공하거나 제공받는 경우에는 그러하지 아니하다. <신설 2004.1.29>

④ 통신비밀침해, 누설

다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 6. 제54조제1항[82]의 규정에 위반하여 전기통신사업자가 취급 중에 있는 통신의 비밀을 침해하거나 누설한 자. [전기통신사업법 제70조(벌칙)]

⑤ 정보통신망 장애발생행위 금지

다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 1... 5. 제48조제3항[83]의 규정을 위반하여 정보통신망에 장애를 발생하게 한 자. [정보통신망이용촉진및정보보호등에관한법률 제62조(벌칙)]

4) 개인비밀침해

① 타인의 정보 훼손, 침해, 도용

다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 6. 제49조[84]의 규정을 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 자. [정보통신망이용촉진및정보보호등에관한법률 제62조 (벌칙)]

② 비밀침해

봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아 낸 자도 제1항의 형[85]과 같다. [형법 제316조제2항 (비밀침해)]

---

82) 第54條 (通信秘密의 보호) ①누구든지 電氣通信事業者가 취급중에 있는 通信의 秘密을 침해하거나 누설하여서는 아니된다.

83) 제48조 (정보통신망 침해행위 등의 금지) ③누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하여서는 아니된다.

84) 제49조 (비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니된다.

85) 제316조【비밀침해】1)봉함 기타 비밀장치한 사람의 편지, 문서 또는 도화를 개봉한 자는 3년이 하의 징역이나 금고 또는 500만원이하의 벌금에 처한다.

③ 개인정보 변경·말소·누설·처리·제공

① 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 자는 10년 이하의 징역에 처한다. ② 제11조[86]의 규정을 위반하여 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. ③ 사위 기타 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받은 자는 2년 이하의 징역 또는 700만원 이하의 벌금에 처한다. [공공기관의개인정보보호에관한법률 제23조(벌칙)]

④ 개인정보의 전용, 제3자에게 제공 및 누설

다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 1. 제24조제1항[87](제58조[88]의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 개인정보를 제22조제2항[89]의 규정에 의한 고지의 범위 또는

---

86) 제11조 (개인정보취급자의 의무) 개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 개인정보의 처리업무를 위탁받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니된다.

87) 제24조 (개인정보의 이용 및 제공 등) ①정보통신서비스제공자는 당해 이용자의 동의가 있거나 다음 각호의 1에 해당하는 경우를 제외하고는 개인정보를 제22조제2항의 규정에 의한 고지의 범위 또는 정보통신서비스이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공하여서는 안된다. 1. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 2. 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우 3. 다른 법률에 특별한 규정이 있는 경우.

88) 제58조 (정보통신서비스제공자외의 자에 대한 준용) 제22조 내지 제32조의 규정은 정보통신서비스제공자외의 자로서 재화 또는 용역을 제공하는 자중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에 이를 준용한다. 이 경우 "정보통신서비스제공자" 또는 "정보통신서비스제공자등"은 "재화 또는 용역을 제공하는 자"로, "이용자"는 "재화 또는 용역을 제공받는 자"로 본다.

89) 제22조 (개인정보의 수집) ②정보통신서비스제공자는 제1항의 규정에 의한 동의를 얻고자 하는 경우에는 미리 다음 각호의 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시하여야 한다. 1. 개인정보관리책임자의 성명·소속부서·직위 및 전화번호 기타 연락처 2. 개인정보의 수집목적 및 이용목적 3. 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용 4. 제30조제1항·제2항 및 제31조제2항의 규정에 의한 이용자 및 법정대리인의 권리 및 그 행사방법 5. 그 밖에 개인

서비스 이용약관에 명시한 범위를 넘어 이용하거나 제3자에게 제공한 자. 2. 제24조제2항[90](제58조의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 이용자의 개인정보를 제공받은 목적외의 용도로 이용하거나 제3자에게 제공한 자. 3. 제24조제4항[91](제58조의 규정에 의하여 준용되는 경우에 해당되는 자를 포함한다)의 규정을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자. [정보통신망이용촉진및정보보호등에관한법률 제62조 (벌칙)]

⑤ 통신비밀침해, 누설

다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 6. 제54조제1항의 규정에 위반하여 전기통신사업자가 취급 중에 있는 통신의 비밀을 침해하거나 누설한 자. [전기통신사업법 제70조(벌칙)]

⑥ 타인간의 대화 등 내용 녹음, 청취, 공개, 누설

다음 각호의 1에 해당하는 자는 7년 이하의 징역에 처한다. 1. 제3조의 규정에 위반하여 우편물의 검열, 전기통신의 감청 또는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하거나 그 취득한 통신 또는 대화의 내용을 공개하거나 누설한 자. 2..... [통신비밀보호법제16조 (벌칙)]

⑦ 신용정보업자 등 업무상 비밀침해

다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 9. 제27조[92]의 규정을 위반한 자. [신용정보의이용및보호에관한법률 제32조제2항(벌칙)]

정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항.

90) 제24조 (개인정보의 이용 및 제공 등) ②정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 당해 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니된다.

91) 제24조 (개인정보의 이용 및 제공 등) ④이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니된다.

92) 제27조 (업무목적외 누설금지등) ①신용정보업자등과 제16조제2항의 규정에 의하여 신용정보의 처리를 위탁받은 자의 임원 및 직원이거나 이었던 자(이하 “신용정보업관련자”라 한다)는 업무상 알게 된 타인

5) 음 란

① 음란물반포, 판매, 임대, 전시

전기통신역무를 이용하여 음란한 부호·문언·음향 또는 영상을 반포·판매 또는 임대하거나 공연히 전시한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. [전기통신기본법 제48조의2(벌칙)]

② 통신매체이용음란

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 1년 이하의 징역 또는 300만원 이하의 벌금에 처한다. [성폭력범죄의처벌및피해자보호등에관한법률 제14조]

③ 음란화상, 영상 등 전시

다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 1... 2. 정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시한 자. [정보통신망이용촉진법 제65조제1항(벌칙)]

6) 명예훼손

① 정보통신망이용 명예훼손

의 신용정보 및 사생활등 개인적 비밀을 업무목적외로 누설 또는 이용하여서는 아니된다. ②다음 각호의 1에 해당하는 경우에는 제1항의 규정에 의한 업무목적외 누설 또는 이용으로 보지 아니한다. 이 경우 신용정보제공·이용자간 또는 신용정보제공·이용자와 신용정보업자간에 제공된 신용정보의 보안관리대책을 포함한 계약을 체결하여야 한다. <신설 97·8·28> 1. 신용정보제공·이용자가 다른 신용정보제공·이용자의 업무에 활용하도록 하기 위하여 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공하는 경우 2. 신용정보제공·이용자가 신용정보업자의 수집에 응하여 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공하는 경우 ③신용정보업관련자로부터 신용정보를 제공받은 자는 타인에게 그 신용정보를 제공하여서는 아니된다. 다만, 이 법 또는 다른 법률의 규정에 의하여 제공이 허용되는 경우에는 그러하지 아니하다.

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. [정보통신망이용촉진및정보보호등에관한법률 제61조(벌칙)]

② 명예훼손

① 공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다. ② 공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처한다. [형법 제307조]

③ 통신매체이용음란

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 한자는 1년 이하의 징역 또는 300만원 이하의 벌금에 처한다. [성폭력범죄의처벌및피해자보호등에관한법률 제14조]

④ 공포심, 불안감유발

다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 1... 3. 정보통신망을 통하여 공포심이나 불안감을 유발하는 말, 음향, 글, 화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자. [정보통신망이용촉진법 제65조제1항(벌칙)]

7) 몰래카메라

① 카메라 등 이용 촬영

카메라 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영한 자는 5년 이하의 징역 또는 1천만원이하의 벌금에 처한다. [성폭력범죄의처벌및피해자보호등에관한법률 제14조의2]

② 음란물반포, 판매, 임대, 전시

전기통신역무를 이용하여 음란한 부호·문언·음향 또는 영상을 반포·판매 또는 임대하거나 공연히 전시한 자는 1년 이하의 징역 또는 1천만원이하의 벌금에 처한다. [전기통신기본법 제48조의2(벌칙)]

8) 컴퓨터사용사기

① 사 기

① 사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. ② 전항의 방법으로 제삼자로 하여금 재물의 교부를 받게 하거나 재산상의 이익을 취득하게 한 때에도 전항의 형과 같다. [형법 제347조].[93]

② 컴퓨터 등 사용사기

컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. [형법 제347조의2][94]

93) 통신망에 물건을 판다고 게시물을 올려 입금만 받고 도주하는 경우가 이에 해당한다(http://icic.sppo.go.kr /b_1_8.htm).

94) ATM기에서 타인의 카드로 돈을 빼내거나 인터넷홈뱅킹을 통해 타인의 계좌에서 돈을 빼돌리는 경우가 이에 해당한다(http://icic.sppo.go.kr/b_1_8.htm).

제4절 형사사법기관의 대응

1. 경찰청 사이버테러대응센터(CTRC)

1) 설립목적

경찰청 사이버테러대응센터(CTRC)는 21세기 첨단 정보통신 시대에 발맞추어 최첨단 해킹수사 장비들을 보완하여 세계제일의 수사능력을 갖추고자 사이버범죄수사대를 확대, 개편한 것이다.

CTRC는 사이버공간내의 정보이용 방해, 정보오용, 인터넷을 이용한 범죄 등 모든 사이버테러를 방지하고 있으며, 명실 공히 사이버공간의 첨병으로서 사이버세계의 안전을 확보하고 국민들이 안심하고 정보를 이용할 수 있는 정보사회를 구축하고자 설립되었다.

2) 연 혁

사이버테러대응센터는 1995년 10월 발족한 외사관리청 소속의 해커수사대가 그 전신이다. 이후 1997년 8월 4일 형사국 지능과 소속의 컴퓨터범죄수사대, 1997년 12월 23일 수사국 지능과 소속 사이버범죄수사대를 거치면서 2000년 7월 11일 수사국 소속으로 69명 4개 팀으로 구성된 사이버테러대응센터로 변모하였으며, 2002년 1월 28일 3계 1실로 개편되었다.

(1) 해커수사대

- 발대 : 1995. 10
- 소속 : 외사관리관
- 구성 : 2개팀(수사팀, 분석팀)

(2) 컴퓨터범죄 수사대

- 발대 : 1997. 8. 4

- 소속 : 형사국 지능과
- 인원 : 10명
- 구성 : 수사팀, 협력관

(3) 사이버범죄 수사대

- 발대 : 1997. 12. 23
- 소속 : 수사국 지능과
- 인원 : 16명
- 구성 : 수사1반, 수사2반

(4) 사이버테러 대응센터

- 발대 : 2000. 7. 11
- 소속 : 수사국
- 인원 : 69명
- 구성 : 4개팀

(5) 사이버테러 대응센터 개편

- 개편 : 2002. 1. 28
- 소속 : 수사국
- 인원 : 69명
- 구성 : 3계 1실

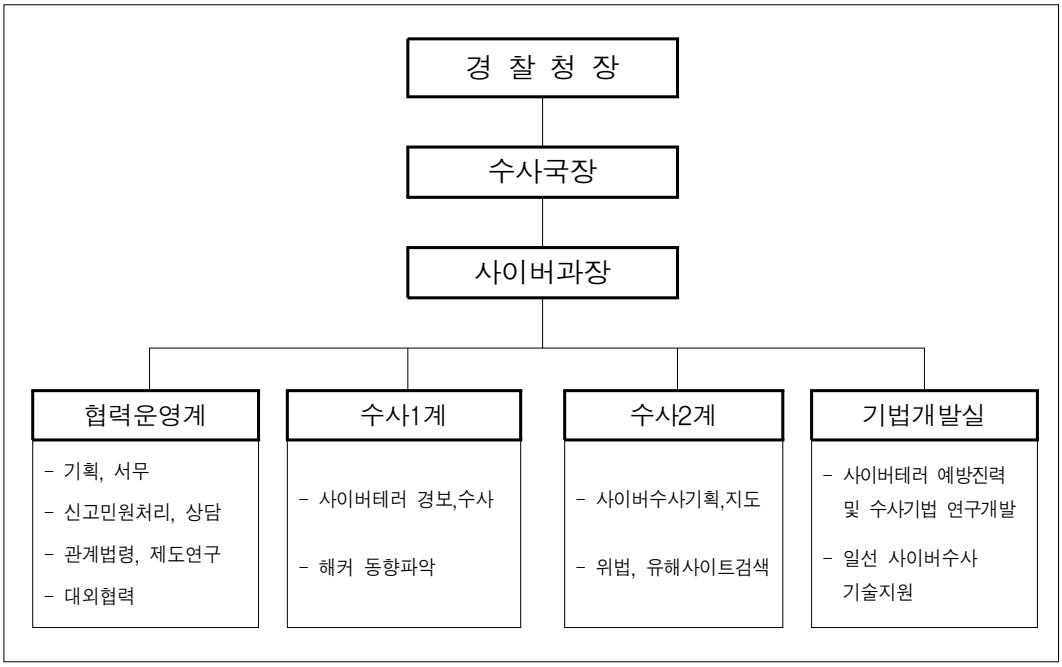
3) 조직 및 기능

사이버테러대응센터는 경찰청 수사국내에 편재되어 있다. 수사국내 협력운영계, 수사1계, 수사2계의 3실과 기법개발실의 1실로 구성되어 있는데, 협력운영계에서는 기획·서무 및 신고민원처리 상담, 관계법령·제도연구의 기능을, 수사1계에서는 사이버테러경보

및 수사, 해커동향 파악을 담당하고 있으며, 수사2계에서는 사이버수사기획 및 지도, 위법·유해사이트 검색을 담당하고 있다. 한편 기법개발실에서는 사이버테러 예방전력 및 수사기법의 연구개발, 그리고 일선 사이버수사에 대한 기술지원의 기능을 수행하고 있다.[95]

사이버테러대응센터의 조직 및 기능은 다음 <그림 4-1>과 같다.

<그림 4-1> 사이버테러대응센터(CTRC)의 조직 및 기능



(출처 : 경찰청 사이버테러대응센터(http://www.police.go.kr/ctrc))

4) 향후 개편계획

현재 수사국내에 69명의 직원, 3계 1실로 운영되고 있는 사이버테러대응센터에 대하여 경찰청은 최근 일어난 국방연구원 등 6개 국가기관 해킹사건과 관련, 2004년 하반기 중 사이버테러대응단을 창설키로 했다.

경찰청은 기존 사이버테러대응센터 내 4개 팀을 과로 승격시켜 4개 과를 갖춘 사이버

95) http://www.police.go.kr/ctrc.

테러대응단을 출범시킬 방침이며, 경무관을 단장으로 하는 110명 규모의 대규모 조직으로 각 과는 사이버테러 예방, 해킹 대응기술 개발 , 그리고 인터넷범죄 수사 및 국제공조 등 전문영역을 갖게 된다.[96]

2. 지방경찰청 사이버범죄수사단 - 사이버방범단(Cyber Watchman) 운영

서울경찰청 사이버범죄수사단은 사이버범죄예방 및 깨끗한 인터넷 환경조성에 동참할 뜻이 있는 전국의 대학생들을 모집, 사이버방범단을 구성하여 운영 중이다. 아래에서는 이를 간단히 소개하기로 한다.

1) 사이버방범단이란?

인터넷 기술 환경과 사회 기반시설의 급속한 발전에 따라 가정과 학교, PC방 등에서 언제든지 누구나 인터넷의 무한한 정보를 접할 수 있게 되면서 정보화의 역기능 또한 빠른 속도로 증가 하였다. 사이버 공간의 팽창과 함께 인터넷 인구 또한 기하급수적으로 증가함에 따라 그릇된 사이버 윤리의식을 가진 네티즌이나, 가치관 정립이 제대로 되지 않은 상태에서 인터넷의 유해 정보에 노출된 어린 학생들이 죄의식을 느끼지 않고 범죄를 행하게 되는 경우가 많이 발생하고 있다.

이에 서울경찰청 사이버범죄수사대는 수사능력의 강화와 함께 깨끗한 인터넷을 만드는데 동참할 진취적이고 활동적인 대학생을 모집하여 사이버공간을 위한 자정노력과 함께 사이버범죄 예방 및 사이버공간 곳곳에서 자행되는 사이버범죄의 신속한 발견과 조치로 피해를 줄여 건전한 인터넷 문화 형성에 중추적 역할을 할 수 있도록 지원하고자 하고 있다. 자발적이고 적극적이며 건전한 사고를 가진 전국의 대학생들로 구성된 이들은 자신의 방범분야를 해킹, 사이버금융, 전자상거래, 지적재산권, 개인정보보호, 불법유해사이트, 인터넷게임 등에서 자유로이 선택하여 활동하며, 이들을 서울경찰청 사이버범죄수사대 사이버방범요원이라 칭하고 그 모임을 사이버방범단으로 명하고 있다.

---

96) 세계일보, 2004년 6월 25일자.

2) 사이버방범요원의 권리와 의무

(1) 권 리

사이버방범요원으로 선정된 학생들은 서울청 사이버범죄수사대 “사이버방범단” 운영에 직·간접적으로 참여할 수 있으며, 사이버방범단의 활동 목적과 법에 위배되지 않는 한 사이버 방범활동에 필요하다고 생각되는 사항을 건의할 수 있다. 그리고 사이버방범요원으로 선정된 학생들은 웹서핑 중 불법유해사이트나 불건전한 정보를 제공하는 자에게 서울경찰청 사이버범죄수사대 사이버방범요원의 이름으로 경고 또는 항의메시지를 보낼 수 있으며, 방범단 활동 목적을 해치지 않는 한도 내에서 자체적으로 다양한 사이버 문화와 관련된 동호회, 소모임을 결성하여 활동할 수 있다.

(2) 의 무

사이버방범요원은 방범활동에 적극적으로 참여하여야 하며, 사이버방범요원은 자신이 선택한 방범분야의 인터넷 사이트를 모니터링 하여 범죄의 우려가 있거나 그러한 사실을 인지하였을 경우 본 사이버범죄수사대에 신속히 통보하여야 한다. 그리고 방범활동 보고서를 제출하는 경우에는 반드시 해당사이트, 날짜, 작성자를 밝혀야 하며, 사이버공간에서 발생하는 불법, 부당행위에 대한 감시를 소홀히 해서는 안된다. 끝으로 방범활동 시 항상 네티켓을 준수하여 사이버방범요원으로서의 명예를 지켜야 한다.

3) 사이버방범단의 활동

사이버방범요원은 방범활동을 수행한 후 결과를 보고서로 작성하여 활동보고 게시판에 게시한다. 이때, 실명을 밝히지 않아도 무방하며, 단 그런 경우 아이디는 필히 기재하여 작성자를 알 수 있도록 한다. 방범요원 자유게시판은 본 수사대 사이버방범요원으로 인증된 학생들과 수사대 직원만 접근이 가능하므로 자유로이 글을 기재하여도 무방하다. 사이버방범단장과 각 분야별 팀장으로 선정된 학생들은 본 수사대와 밀접한 연락관계에 있어야 하며, 수사대에서 행하는 행사에 1차적으로 우선권을 부여한다.

3. 대검찰청 인터넷범죄수사센터(ICIC)

1) 설립목적

검찰에서는 21세기 지식·정보화 선진국에 장애가 되는 해킹, 바이러스 유포, 전자상거래 사기 등 첨단 컴퓨터범죄에 대응하기 위한 최선의 노력을 기울이고 있으며, 이러한 노력의 일환으로 대검찰청 인터넷범죄수사센터(ICIC)를 설립하였다.

중점 단속분야로는 통신, 에너지, 운송, 자원 등 국가기반 정보통신시설을 대상으로 이루어지는 사이버테러 행위, 그리고 전자상거래사기 및 개인정보침해, 불건전정보유포 등 국민 생활과 직결된 컴퓨터범죄이다. 또한 중점 추진시책으로는 첨단 컴퓨터범죄에 대하여 신속·능동적으로 대처할 수 있도록 수사제도 및 효율적 수사기법 개발, 유관 민간단체·기업 및 국가기관과의 긴밀한 협조망을 구축하고, 미국 법무부 등 16개국이 참여하고 있는 '국제하이테크범죄 24시간 수사협조체제'의 대한민국 Contact Point로 활동하고 있다.

검찰의 인터넷범죄수사센터는 대검찰청과 서울지검에 각각 설치되어 있으며, 대검찰청 중앙수사부 컴퓨터수사과와 서울지검 컴퓨터수사부에서 이를 각각 운영하고 있다.

2) 연 혁

대검찰청 및 서울지방검찰청, 21개 지방검찰청 및 지청의 인터넷범죄수사센터의 연혁은 다음과 같다.

(1) 대검찰청

- 1996. 6. 3. 중앙수사부 수사기획관실내 '정보범죄대책본부' 설치
- 1999. 4. 1. 정보범죄대책본부를 '컴퓨터범죄전담수사반'으로 개칭
- 2000. 2. 21. 중앙수사부내 '컴퓨터수사과' 신설
- 2001. 2. 15. 대검찰청인터넷범죄수사센터 설치

(2) 서울지방검찰청

- 1995. 4. 10. 특별수사2부내에 '정보범죄수사센터' 설치
- 2000. 2. 21. '컴퓨터수사부' 신설
- 2001. 2. 15. 서울지검인터넷범죄수사센터 설치

(3) 21개 지방검찰청 및 지청

- 1997. 4. 부산, 대구, 광주, 대전지검 '컴퓨터수사반' 설치
- 1998. 6. 인천, 수원, 청주, 창원, 전주지검 '컴퓨터수사반'설치
- 1999. 6. 춘천, 울산, 제주지검, 서울동부, 서부, 북부지청 '컴퓨터수사반' 설치
- 2000. 7. 서울남부, 의정부, 성남, 부천, 부산동부지청 '컴퓨터수사반' 설치
- 2002. 12. 수원지검 안산지청 '컴퓨터수사반' 설치

3) 조직 및 기능

대검찰청에서는 인터넷범죄수사센터, 서울지방검찰청에서는 컴퓨터수사부, 그리고 21개 지방검찰청 및 지청에서는 컴퓨터수사반에서 관련 업무를 담당하고 있다.

(1) 대검찰청 인터넷범죄수사센터

① 컴퓨터 등 정보처리장치 및 정보통신매체를 사용한 범죄사건에 대한 검찰사무의 지휘·감독; ② 컴퓨터 등 정보처리장치 및 정보통신매체와 관련된 증거자료에 대한 압수·수색 및 분석 등의 지원; ③ 위 사건에 규정된 사건에 관한 범죄현상의 분석·연구·수사지침수립 및 국내외 중요사건 사례연구집 발간.

(2) 서울지방검찰청 컴퓨터수사부

① 검사장이 지정하는 컴퓨터 등 정보처리장치 및 정보통신매체를 사용한 범죄사건의 수사; ② 위 사건에 관련된 정보 및 자료의 수집·정비에 관한 사항; ③ 컴퓨터 등 정보처리장치 및 정보통신매체와 관련된 증거자료에 대한 압수·수색 및 분석.

(3) 일선청 컴퓨터범죄수사반

① 컴퓨터 등 정보처리장치 및 정보통신매체를 이용한 범죄사건의 수사 및 처리; ② 컴퓨터 등 정보처리장치 및 정보통신매체와 관련된 증거자료에 대한 압수·수색 및 분석.

제5절 정보(화) 관련 공공기관의 대응

국제경쟁력 강화를 위해 IT산업을 집중 육성하면서 한국은 세계 초일류 정보화 산업의 인프라를 구축한 국가가 되었다. 하지만 이에 따라 나타나는 문제점들은 단순한 역기능의 차원을 넘어 하나의 큰 사회문제가 되고 있다.

사이버범죄 및 정보화의 역기능에 대처하기 위해 정부 산하 정보화 관련 공공기관들은 다양한 대책마련과 함께 활발한 정화운동을 벌이고 있다. 현재 설치되어 있는 대표적인 정보화관련 공공기관으로는 정보통신윤리위원회(ICEC), 한국정보보호진흥원(KISA), 한국정보문화진흥원(KADO), 국가정보원내에 설치된 국가사이버안전센터(NCSC) 등이 있다.

정보통신윤리위원회(ICRC)는 전기통신사업법 제53조의2를 근거로 하며, '정보통신윤리강령'과 '네티즌윤리강령'을 제정·선포하고 '정보통신윤리 교육'과 같은 사업을 전개하여 사업자와 이용자뿐 아니라 정책 입안자들과 일반 국민들에게 정보통신윤리 의식을 고양, 정착시키기 위해 설립된 기관이다.

한국정보보호진흥원(KISA)은 신속한 인터넷 침해사고 대응지원, 주요 정보통신기반시설 취약점 분석·평가, 스팸메일 대응 및 개인정보보호 활동, 전자서명인증, 정보보호산업 지원, 정보보호정책 개발 및 교육홍보 등 IT발전에 따른 정보화 역기능의 예방에 중점을 두고 활발히 활동하고 있는 기관이다.

정보격차해소에관한법률 제16조에 의해 설립된 기관인 한국정보문화진흥원은 국내·외 정보격차 해소를 종합적으로 지원하기 위한 국가 정보격차해소 전담기관으로서 장애인과 노인, 저소득층, 농어촌 지역주민 등 정보소외계층에게 정보통신서비스에 대한 자유로운 접근과 정보이용을 보장함으로써 이들의 삶의 질을 향상시키고 균형 있는 국민경

제의 발전에 이바지하고 있다.

한편 2004년 2월 20일 개소한 국가정보원 산하 국가사이버안전센터(NCSC)는 사이버테러를 막기 위한 국가 차원의 종합적이고 일원화된 대응체계 마련을 위해 설립된 기관이다.

이하에서는 이러한 정보화관련 공공기관의 종류와 각 기관별 설립목적 및 연혁, 기능 및 분장 사무에 대하여 살펴보기로 하겠다.

1. 정보통신윤리위원회(ICEC)

1) 설립목적

인터넷 이용자수가 기하급수적으로 늘어나고 인터넷의 시공을 초월한 편리함을 이용해 상업성이 개입되면서 불건전정보의 유통이 날로 심화되었다. 이처럼 정보통신윤리 문제가 중요한 사회적 과제로 떠오르게 됨에 따라, 정보통신부는 1995년 전기통신사업법 제53조의 2를 근거로 정보통신윤리위원회를 설립하였다. 정보통신윤리위원회는 '정보통신윤리강령'과 '네티즌윤리강령'을 제정·선포하고 '정보통신윤리 교육'과 같은 사업을 전개해 사업자와 이용자뿐 아니라 정책 입안자와 일반 국민들에게 정보통신윤리 의식을 고양시키고 정착시키기 위해 노력해 왔다.

2) 연 혁

정보통신윤리위원회는 1995년 4월 13일 제1기 위원회가 발족한 이래 2003년 현재 제5기 위원회가 구성되어 활동하고 있다. 자세한 연혁은 다음과 같다.

- 1995. 1. 5 정보통신윤리위원회 설립 법적 근거 마련(전기통신사업법 개정)
- 1995. 4. 13 정보통신윤리위원회 발족
- 1995. 6. 7 정보통신윤리강령 선포
- 2000. 4. 1 청소년권장사이트제도 운영
- 2000. 5. 3 사이버성폭력피해신고 접수처리

- 2000. 6. 15 네티즌윤리강령 선포
- 2001. 9. 24 인터넷내용등급서비스 개시
- 2002. 4. 19 사이버패트롤네티즌(자원봉사자)발족
- 2002. 5. 20 불법·청소년유해정보신고 '인터넷119'개설
- 2002. 10. 1 사이버명예훼손·성폭력상담 제공
- 2003. 4. 13 제5기 정보통신윤리위원회 구성
- 2003. 5. 15 국제인터넷핫라인협회(INHOPE)회원 가입
- 2003. 10. 1 기구개편 및 강화(불법·청소년유해정보신고센터, 사이버명예훼손·성폭력분쟁조정센터 설치)

3) 조직 및 기능

(1) 조 직

정보통신윤리위원회의 조직은 1실 2단 9팀 2센터로 구성되어 있다. 1실은 사업지원실이며, 사업지원실은 기획팀, 총무팀, 기술지원팀으로 구성되어 있다. 2단은 심의조정단, 협력사업단인바, 심의조정단에는 심의조정1팀, 심의조정2팀, 심의조정3팀이 있으며, 협력사업단은 협력지원팀과 교육홈보팀으로 구성되어 있다.

한편 2센터는 불법·청소년유해정보신고센터와 사이버명예훼손·성폭력분쟁조정센터이다.

(2) 기 능

정보통신윤리위원회는 전기통신사업법에 따라 불법·청소년유해정보 모니터링 및 심의·의결, 불법·청소년유해정보신고센터(인터넷 119) 운영, 인터넷 민간자율규제활동 지원, 인터넷 내용등급서비스 제공, INHOPE 회원활동 및 국제협력체제구축, 정보통신윤리교육·홍보 프로그램 운영, 청소년권장사이트 선정·보급, 정보통신윤리 관련 정책연구 및 논의 활성화, 사이버명예훼손·성폭력분쟁조정센터 운영 등 건전한 정보문화의 창달 및 전기통신의 올바른 이용환경 조성을 위한 활동을 전개하고 있다. 정보통신윤리위원회의 기본적인 임무는 다음과 같다.[97]

<표 4-1> 정보통신윤리위원회의 임무

· 정보통신윤리에 대한 기본강령의 제시 · 전기통신회선을 통하여 일반에게 공개를 목적으로 유통되는 정보 중 전기통신사업법 및 대통령령이 정하는 정보의 심의 및 시정요구 · 전기통신회선을 이용하여 유통되는 정보의 건전화를 위한 대책수립 건의 · 불법·청소년유해정보 신고센터의 운영 · 건전한 정보문화 창달을 위하여 필요한 활동 · 건전한 정보의 유통 활성화와 관련하여 정보통신부장관이 위탁하는 사항

2. 한국정보보호진흥원(KISA)

1) 설립목적

정보통신망이용촉진및정보보호등에관한법률 제52조[98]를 근거로 하여 설립된 한국정보보호진흥원(KISA)는 신속한 인터넷 침해사고 대응지원, 주요정보통신기반시설 취약점 분석·평가, 스팸메일 대응 및 개인정보보호 활동, 전자서명인증, 정보보호산업지원, 정보보호정책 개발 및 교육홍보 등 IT발전에 따른 정보화 역기능의 예방에 중점을 두고 있다.

2) 연 혁

한국정보보호진흥원은 1995년 8월 정보화촉진기본법(법률 제4969호)이 공포되면서 한국정보보호센터로 출발하였으며, 2001년 7월 한국정보보호진흥원으로 승격되었다. 자세한 연혁은 아래와 같다.

- 1995. 8 정보화촉진기본법 공포(법률 제4969호)
- 1996. 4 한국정보보호센터 설립(설립근거: 정보화촉진기본법 제14조의2)
- 1996. 11 한국정보통신망침해사고대응팀협의회(CONCERT) 발족

---

97) http://www.icec.or.kr/.

98) 【정보통신망이용촉진및정보보호등에관한법률 제52조】 정부는 정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위하여 한국정보보호진흥원(이하 "보호진흥원"이라 한다)을 설립한다.

- 1997. 1 정보보호 전문교육과정 개설
- 1997. 8 온라인 보안점검서비스 개시
- 1998. 1 국제침해사고대응팀협의회(FIRST) 가입
- 1998. 2 침입차단시스템 평가시행
- 1999. 7 전자서명인증관리센터 개설
- 2000. 4 해킹바이러스상담지원센터 개설, 개인정보침해신고센터 개설
- 2001. 1 설립근거 및 명칭 변경(법 제52조), 정보통신망이용촉진및정보보호 등에관한법률 공포 (법률 제6360호)
- 2001. 7 한국정보보호진흥원으로 승격

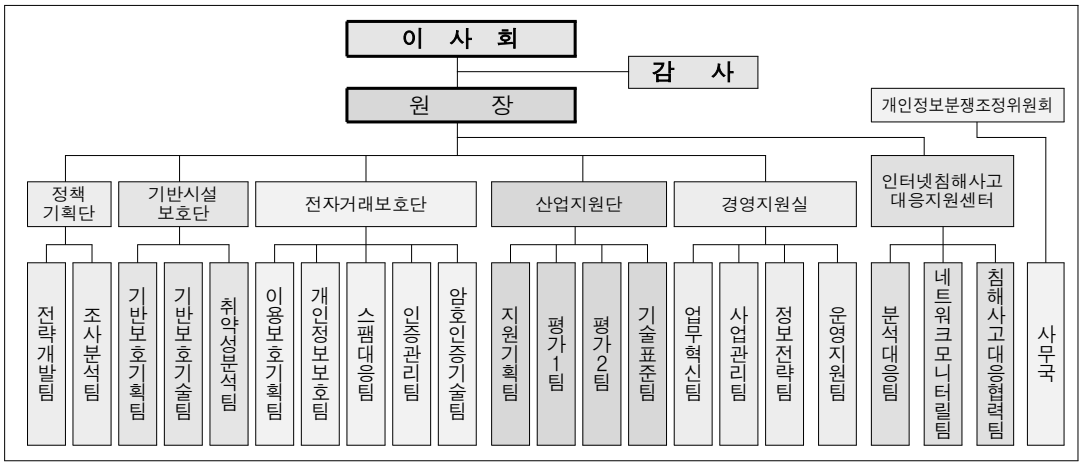
3) 조직 및 기능

(1) 조 직

한국정보보호진흥원은 원장 이하 정책기획단, 기반시설보호단, 전자거래보호단, 산업지원단, 경영지원실로 구성되어 있다. 또한 인터넷침해사고대응지원센터가 개설되어 있는 바, 이 센터는 침해사고대응협력팀, 네트워크 모니터링팀, 분석대응팀으로 구성되어 있다. 그리고 별도의 기관으로 개인정보 분쟁조정위원회가 설치되어 있다.

<그림 4-2>는 한국정보보호진흥원의 조직도이다.

<그림 4-2> 한국정보보호진흥원 조직도



(2) 기 능

정관 제4조에 규정된 한국정보보호진흥원의 주요임무는 다음의 <표 4-2>와 같다.

<표 4-2> 한국정보보호진흥원의 주요임무

1. 정보보호를 위한 정책 및 제도의 조사·연구
2. 정보보호 기술 개발
3. 정보보호시스템의 연구·개발 및 시험·평가
4. 정보보호에 관련된 표준 및 기준 연구
5. 정보화 역기능 분석 및 대책연구
6. 정보보호에 관한 홍보 및 교육훈련
7. 정보보호에 관한 기술지원 및 자문
8. 전자서명법 제25조제1항의 규정에 의한 전자서명 인증관리
9. 개인정보보호를 위한 대책연구
10. 정보시스템 침해사고 처리 및 대응체계 운영
11. 개인정보분쟁조정위원회사무국 운영
12. 기타 법령에 의하여 보호진흥원의 업무로 정하거나 위탁한 사업 또는 국가로부터 위탁받은 사업 및 제1호 내지 제12호의 사업에 부수되는 사업

4) 부속기관 및 분장사무

(1) 개인정보침해신고센터

개인정보침해신고센터는 「정보통신망이용촉진등에관한법률」상의 개인정보 보호규정이 이행되는지 여부를 감시하는 임무를 수행하며, 정보보호진흥원 내에 설치되어 있다. 개인정보를 침해당한 경우에는 누구든지 신고센터에 소정의 양식에 따라 신고할 수 있으며, 또한 개인정보보호와 관련된 궁금한 사항이나 자신의 권익내용에 관한 사항을 상담받을 수 있다. 신고 접수된 사항은 정보통신부의 조사계획에 의거 당사자를 조사하게 되며, 법규위반 여부 결정 및 위반사항 정도에 따라 과태료 부과 및 수사 의뢰를 한 후, 조치 결과를 신고자에게 통보하게 된다.[99]

(2) 개인정보분쟁조정위원회

최근에 개인신상에 관한 정보 유출이나 오용에 대한 염려가 커짐에 따라 2001년 12월 정보통신망이용촉진및정보보호등에관한법률 제33조에 의거하여 분쟁해결 전문기관인 개인정보분쟁조정위원회가 설립되었다. 이 위원회는 인터넷 이용자와 사업자 사이의 개인정보분쟁조정 뿐 아니라 교육과 홍보를 통한 피해예방 활동, 법제도 개선 건의, 기업의 거래 행태나 약관의 시정권고, 위법사실 처리 등의 각종 재발방지조치를 통해 국민의 권리를 보호하고 있다.[100]

(3) 전자서명인증관리센터

전자서명인증관리센터는 전자서명을 안전하고 신뢰성 있게 이용할 수 있는 환경을 조성하고 공인인증기관을 효율적으로 관리하기 위한 기관으로 전자서명법 제25조를 법적 근거로 하여 1999년 7월 7일에 설립되었다. 주요 추진 업무로는 공인인증기관에 대한 공인인증서 발급·관리 등 인증업무, 공인인증기관 실질심사 및 정기점검, 전자서명인증 관련 기술개발·보급, 전자서명인증 관련 제도 연구 및 상호인증 등 국제협력 지원, 전자서명 이용활성화 추진 등이 있다.[101]

(4) 정보보호관리체계인증제도

인터넷의 확산으로 인한 새로운 보안위협의 증가에 따라 정보보호에 관한 종합적이고 체계적인 정보보호 관리 및 인증의 필요성이 대두되면서 미래의 시큐리티라운드(Security Round)에 대비하여 국내 대응역량 배양의 필요성이 증가하였다. 그러나 정보통신서비스제공자 및 정보통신서비스를 제공하기 위한 물리적 시설을 제공하는 자와 같은 관련 조직의 정보보호대응능력 전반을 객관적으로 심사하여 고객·이용자에게 올바른 정보를 제공할 수 있는 적절한 평가메커니즘이 부재한 상황에서 등장하게 된 것이 정보보호관리체계인증제도이다.

---

99) http://www.cyberprivacy.or.kr/index_1.html.
100) http://www.kopico.or.kr/.
101) http://www.rootca.or.kr/.

정보보호관리체계인증제도는 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립·문서화하고 지속적으로 관리·운영하는 시스템, 즉 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책 구현, 사후관리 등의 정보보호관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계에 대하여 제3자의 인증기관(한국정보보호진흥원)이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도이다.[102]

(5) 정보보호산업지원센터

정보보호제품의 연구개발을 지원하기 위하여 정보보호업체, 학계 및 연구기관이 공동으로 이용할 수 있는 인프라를 구축·운영함으로써 정보보호산업 발전을 위한 기초 여건을 조성하기 위하여 설립된 기관이다. 정보보호산업지원센터에서는 정보보호제품의 연구개발을 위한 Test Lab과 정보보호 전문교육 및 제품이용교육을 위한 교육시설을 제공하고 있으며, 정보보호기술·시장 동향 제공을 위한 정보자료실을 운영하고 있다.[103]

(6) 불법스팸대응센터

불법스팸대응센터는 국민의 스팸관련 상담 및 불법스팸 신고를 원활히 처리하기 위하여 2003년 1월 24일 한국정보보호진흥원내 개설되었다. 당 센터는 일반 국민에게 스팸차단 방법 등을 안내하고, 「정보통신망이용촉진및정보보호등에관한법률」에서 정하고 있는 불법스팸의 신고를 연중 접수하여 처리하고 있다. 이외에도 스팸피해를 사전에 예방하기 위한 각종 인식제고 활동들을 벌이고 있으며, 스팸방지 프로그램을 개발 배포하는 등의 기술적인 대책 마련에도 주력하고 있다. 또한 스팸규제 강화를 위한 법 제도 개선 방안을 연구하고, 스팸방지대책을 수립, 시행하는 한편, 한국발 스팸문제를 해소하기 위해 외국의 스팸대응기구와의 국제협력도 추진하고 있다.[104]

---

102) http://www.kisa.or.kr/isms/.
103) http://www.kisis.or.kr/.
104) http://www.spamcop.or.kr.

(7) 보호나라(정보보호포털사이트)

보호나라(www.boho.or.kr)는 정보통신부가 '21세기 가장 무서운 적은 정보 유출'이라는 구호 아래 2002년 개설한 정보보호 포털 사이트로 해킹, 바이러스 등 사이버 공격과 관련된 정보를 한 눈에 알 수 있다. 보호나라는 해킹, 바이러스, 정보자료실, 신고하기, 관련 사이트, 네티즌 마당 등의 코너로 구성돼 있다. 해킹 코너에는 찾고자 하는 각종 바이러스를 검색할 수 있는 데이터베이스와 예방 및 대처법 등이 담겨 있다. 또한 한국정보보호진흥원 등에서 제공하는 해킹, 바이러스경보를 바로 바로 게시하고 있으며, 각종 보안업체 등과도 연결돼 있다. 그리고 개인정보침해신고센터 등 관련 사이트와 연결된 '신고하기'를 통해 개인정보 침해, 새로 발생한 바이러스, 스팸메일, 청소년 유해정보 등을 신고할 수 있다.[105]

(8) 인터넷보안기술포럼

국내에서도 국제 표준화 동향에 대응하며 국내에 적합한 사실 표준 제정을 위해서는 민간 업체의 표준화에 대한 관심을 고조시킬 수 있는 정보교류의 장이 필요하다는 인식 아래 정보통신부가 전략적으로 민간 포럼의 구성을 추진하였으며, 이러한 노력의 일환으로 설립된 것이 인터넷보안기술포럼이다. 주요 추진사업은 인터넷 보안기술 관련 최신 기술정보의 수집, 분석, 보급 및 활용촉진, 인터넷 보안기술 관련 국내 표준 개발, 인터넷 보안 관련 제품 상호운용성 항목 발굴 및 상호운용성 시험, 인터넷 보안기술 관련 세미나, 워크샵 등 행사 개최, 인터넷 보안기술 관련 국제 표준화회의, 국제포럼 등에의 참여 지원 등이다.[106]

(9) 한국PKI포럼

PKI(Public Key Infrastructure: 공개키 기반구조)[107] 이용의 활성화를 촉진하고

105) http://www.boho.or.kr/.

106) http://www.istf.or.kr/intro.html.

107) PKI란 전자서명과 같은 정보전자거래의 환경구축을 위한 핵심기술로 안전성과 신뢰성을 바탕으로 정보전자거래의 선진화를 기할 수 있는 기술이다. 현재 세계 각국이 도입하고 있으며, 현재 우리나라의 PKI 기술에 대한 개발은 지속적으로 이루어지고 있다.

PKI 사업환경의 기반을 구축하여 정보산업의 건전한 발전을 도모하기 위해 설립된 한국PKI포럼은 PKI 사업환경 기반 구축, 전자서명 활성화를 위한 활동, PKI의 인식확산을 위한 교육·홍보활동, 국내 PKI의 제도발전을 위한 연구활동, 아시아 PKI 포럼 활동, 국외 PKI 관련 기관·단체와의 협력활동, 기타 포럼의 목적달성에 필요한 사업 등에 활발한 활동을 하고 있는 단체이다.[108]

3. 한국정보문화진흥원(KADO)

1) 설립목적

한국정보문화진흥원은 정보격차해소에관한법률 제16조에 의해 설립된 기관이다. 본 기관은 국내외 정보격차 해소를 종합적으로 지원하기 위한 국가 정보격차해소 전담기관으로 장애인과 노인, 저소득층, 농어촌 지역주민 등 정보소외계층에게 정보통신서비스에 대한 자유로운 접근과 정보이용을 보장함으로써 이들의 삶의 질을 향상시키고 균형 있는 국민경제의 발전에 이바지함을 그 목적으로 하고 있다.

이를 위하여 정보사회 미참여 계층을 위한 정보접근 환경조성, 정보격차해소관련 기술 및 콘텐츠 개발·지원, 국가간 정보격차해소를 위한 국제협력, 정보이용능력 배양을 위한 국민정보화교육, 정보격차해소를 위한 사회인식 확산 및 홍보, 국민의 생산적 정보활용 촉진 및 오·남용 예방, 정보격차해소 정책개발 지원 및 조사연구 등 7대 핵심과제를 중점 추진해 나가고 있다.

2) 연 혁

한국정보문화진흥원은 1984년 11월 전신인 (재)정보통신훈련센터(ITTC)가 발족하면서 그 활동이 시작되었으며 현재에까지 이르고 있다.

- 1984. 11 (재)정보통신훈련센터(ITTC)설립
- 1988. 1 전남고흥에 국내 최초 농어촌컴퓨터교실 개소

108) http://www.pki.or.kr/.

- 1988. 6 정보문화의 달 제정(매년 6월)
- 1989. 1 강남정보문화홍보관 개관
- 1992. 2 전산망보급확장과이용촉진에관한법률(법률 제4439호)에 의거 한국정보문화센터로 개관
- 1992. 6 정보화추진협의회 발족
- 1994. 5 지역정보화사업 전담기관으로 지정
- 1994. 11 초고속정보통신 전시관 건립 전담기관 지정
- 1994. 12 초고속정보통신 홍보전담기관 지정
- 1996. 6 초고속정보통신 전문인력양성 전담기관 지정
- 1997. 1 부설 정보기술교육원 개원
- 1997. 4 정보화상담실 개소
- 1997. 11 정보공동체포럼 서비스 개시
- 1998. 5 정보나라(초고속정보통신 전시관)기공
- 1998. 6 한국정보문화운동협의회 발족
- 1999. 1 한국전산원 부설 한국정보문화센터로 발족
- 2000. 4 강서 정보문화홍보관 개관
- 2000. 10 정보나라 초고속정보통신 전시관 개관
- 2002. 4 인터넷중독예방상담센터 개소
- 2003. 1 한국정보문화진흥원(KADO)으로 확대 개편(정보격차해소에관한법률 제16조에 의한 특별법인)

3) 조직 및 기능

한국정보문화진흥원은 원장 이하 1실 4단으로 구성되어 있다. 1실은 기획관리실이며, 4단으로는 정보접근지원단, 정보화교육사업단, 정보생활진흥단, 국제협력단이 있다. 본 기관이 수행하는 기능 및 역할을 살펴보면, 정보소외계층이 차별 없는 정보화의 혜택을 향유할 수 있는 보편적 정보접근·활용 환경 조성, 국민 모두의 디지털 역량 극대화 및 생산적 정보활용 촉진을 통한 창조적이고 건전한 국민 정보생활 정립, 국가간의 정보격차해

소 교류·협력 확대를 통한 정보화 선도 국가로서의 위상 수립이라는 세 가지 측면의 기능을 수행함과 동시에, 정보소외계층을 위한 정보접근 환경조성, 정보격차해소기술 및 콘텐츠 개발·지원, 국가간 정보격차 해소를 위한 국제협력, 정보이용능력 배양을 위한 국민 정보화교육, 정보격차해소를 위한 사회인식 확산 및 홍보의 역할을 수행하고 있다.[109]

4. 국가정보원 - 국가사이버안전센터(NCSC)

1) 설립목적

2004년 2월 20일 개소한 국가정보원 산하 국가사이버안전센터(NCSC)는 사이버 테러를 막기 위한 국가 차원의 종합적이고 일원화된 대응체계의 마련 필요성에 의해 설립된 기관이다. 특히 MS-SQL서버의 취약점을 이용한 '슬래머 웜바이러스'로 국내 8천800여 대의 서버가 감염돼 수많은 전산시스템이 일제히 마비된 2003년의 '1.25 인터넷 대란' 이후 최근에는 웜바이러스의 감염속도가 가속화되면서 그 필요성이 더욱 크게 제기되어 설립되었다. 국가사이버안전센터는 국내 정보통신망에 대하여 국내외로부터의 사이버 위협을 24시간 모니터링 하여 각종 보안위해 및 공격유형 등을 종합적으로 분석, 사이버 공격 징후를 사전에 탐지해 각급기관에 지원하는 일을 하고 있다.

2) 연 혁

국가사이버안전센터는 2003년 7월 24일 대통령의 재가를 받아 설립 추진이 본격화되어 2004년 2월 20일 개소를 하게 되었다.

- 2003. 7. 24 「국가사이버테러대응체계 구축 기본계획」대통령 재가.
- 2003. 12. 18 국가사이버안전센터 설립
- 2004. 2. 20 국가사이버안전센터 개소

109) http://www.kado.or.kr/.

3) 기능 및 역할

국가사이버안전센터의 기능 및 역할을 구체적으로 살펴보면, 본 기관에서는 사이버 위협을 평시(녹색)-주의(청색)-경고(황색)-위험(적색) 등 4단계로 나눠 예·경보를 발령하고 각종 보안권고문과 보안뉴스, 보안기술자료 등을 민·관·군에 전파해 보안대책을 강구할 수 있도록 지원하며, 피해발생시 사고원인의 규명과 함께 긴급복구를 돕는다. 이와 같은 대응을 위해 센터에서는 시간별로 정보통신망의 상태를 파악하고 정상상태와 비교를 통해 위험도를 파악하고 있다. 또한 '국가사이버안전매뉴얼'을 배포해 정보통신망을 안전하게 관리하고 단계별 대응방법을 알리며, 외국의 사이버 보안기구 및 침해사고대응기구와 협력도 강화해 나가는 것은 물론 국가정보통신망에 대한 사이버위협의 유형을 분석한다. 사이버테러가 우리 사회의 전 영역을 포괄한다는 점에서 동 센터는 국정원을 축으로 재정경제부, 국방부, 행정자치부, 정보통신부, 대검찰청, 경찰청 등 유관부처와 한국정보보호진흥원, 국가보안기술연구소 등 전문 인력이 합동 근무하는 체제로 운영되고 있다. 특히 이 센터의 운영지침을 비롯한 사이버상의 안전에 대한 정책은 국가안전보장회의(NSC)가 담당하고 있다.

제6절 정보통신사업자 및 사업자단체의 대응

1990년대 중반부터 정보통신 이용환경이 PC통신에서 인터넷으로 옮겨가기 시작하면서 포털(Portal), 채팅, ISP(Internet Service Provider: 인터넷서비스제공자) 및 성인정보제공 사업자 등 다양한 인터넷 사업자가 나타나기 시작하였다. 더불어 인터넷 사용자가 급격히 증가하기 시작하였고, 정보화의 역기능이 점차 사회문제화 됨에 따라 공적규제와 함께 민간영역에서의 자율규제활동의 필요성이 대두되기 시작하였다. 이는 인터넷 환경의 개방성·가변성·쌍방향성으로 인하여 기존의 공중파 매체처럼 공적규제만으로는 정보건전화를 위한 규제의 실효성을 달성하기 어렵기 때문이다. 사업자 또는 사업자단체의 자율규제활동은 사업자(단체)가 핫라인을 구축하여 신고·처리시스템을 운영하거나, 행동강령 또는 약관제정, 자체모니터링 및 신고센터 운영, 캠페인 등 사업자 스스로

정보건전화를 위한 다양한 활동을 추진하는 것이라 할 수 있다.[110]

사업자들은 인터넷을 통한 불법정보의 유통방지, 특히 어린이・청소년들이 성인정보나 청소년 유해정보에 노출되는 것을 방지하기 위한 활동들을 실시하고 있다. 섹스, 포르노, 스와핑과 같은 키워드 검색시 성인인증절차의 실시, 광고성・음란성 스팸메일에 대한 수준별 필터링, 스팸차단 환경설정, 음란스팸잡이 프로그램 다운로드 등 지원, 어린이가 회원에 가입할 경우 부모 또는 법정대리인의 동의절차 실시, 어린이 전용 포털사이트 및 이메일 서비스 제공 등이 그 예라 할 수 있다(정보통신윤리위원회, 2003). 아래에서는 주요 정보통신사업자단체들의 자율규제활동들을 살펴보기로 한다.

1. 한국인터넷방송협회

(사)한국인터넷방송협회(www.korwa.or.kr)는 인터넷방송의 올바른 이해와 보급 및 바람직한 인터넷문화상을 제시하고, 인터넷방송의 다양한 비즈니스 모델을 모색하여 인터넷방송의 산업화에 기여함을 목적으로 1998년에 설립되었다.

정보통신윤리와 관련하여 이 협회가 그 동안 추진한 기능 및 주요사업은 다음과 같다: ① 공익성 콘텐츠 DB화 및 방송, ② 인터넷 성인채널에 대한 민간차원의 자율모니터링 실시, ③ 인터넷방송 관련 저작권 문제 상담, ④ 웹캐스팅 관련 신규・전문인력 양성, ⑤ 우수 콘텐츠・기술 발굴 및 시상(인터넷방송대상 시상), ⑥ 디지털콘텐츠 사업 시장동향 조사 및 정책연구를 위한 실태조사 사업, ⑦ 웹캐스팅 관련 교육교재 개발 및 수강생 모집, 홍보.

---

110) 예컨대, 하나로통신은 초고속인터넷서비스 가입자에게 인터넷 유해사이트 접속을 차단하는 서비스(서비스명: 하나포스 가디언)를 2003년 12월부터 제공하고 있다. 하나포스 가디언은 원하는 희망자만이 가입할 수 있으며, 가입자에게는 데이터베이스화된 유해정보목록은 접속이 금지되는 블랙리스트 방식의 차단 기능을 갖고 있다. 여기에 사용하는 유해정보 데이터베이스는 음란, 폭력, 도박, 자살사이트 등 미성년자에게 해로운 정보를 제공하는 자가 '청소년 이용불가'임을 명시적으로 표시한 사이트, 위원회에서 정한 인터넷 유해사이트 기준에 해당되는 사이트 및 청소년유해매체물 관련 법규에 근거하여 하나로통신에서 자체적으로 분류한 인터넷 사이트 등으로 구성되어 있다.

2. 한국콘텐츠산업연합회

사)한국콘텐츠산업연합회(www.kiba.or.kr)는 정보사업의 자율적 정화 및 심의제도 정착을 통한 건전한 정보문화 확산, CP 창업지원 등을 통한 정보제공사업영역의 인터넷 기반으로의 확장, 콘텐츠사업자들의 권익증진 및 협조체계 강화, 온라인 콘텐츠산업의 사업환경 개선, 콘텐츠산업발전을 통한 21세기 지식정보사회의 기반 조성 등을 위하여 설립되었다(전신인 한국전화정보통신협회는 1997년 3월에 설립됨). 주요 기능 및 사업으로는 ① 자율심의 활동, ② 저작권특별위원회 활동, ③ 디지털콘텐츠산업 인력양성 사업, ④ 유망CP 멀티채널 지원, ⑤ 국내디지털콘텐츠산업 시장조사가 있다.

3. 한국인터넷성인문화협회

(사)한국인터넷성인문화협회(www.kiaca.com)는 2001년 1월 성인콘텐츠 사업자를 대상으로 한 검찰의 대대적인 단속 이후, 성인문화 정보제공 사업자들의 자정노력과 올바른 성인문화 정착을 위한 취지로 설립되었다.

이 협회가 그 동안 추진한 정보통신윤리 관련 주요사업은 다음과 같다: ① 음란물로부터 청소년 보호를 위한 제도적 장치마련을 위한 공청회 개최(2002. 9), ② 합동자율지도위원회 발족(2003. 10), ③ 청소년유해매체물 목록표시 통보(2004. 5), ④ 자율심의위원회 운영 및 모니터링 활동.

4. 한국게임산업연합회

한국게임산업연합회(www.kgia.org)는 게임사업자 뿐만 아니라 이용자, 정부 및 공공영역의 상호 이익을 도모함은 물론, 서로 협력하고 경쟁하는 가운데 게임산업의 육성과 건전한 게임문화의 성장을 촉진하기 위하여 2000년 9월 설립되었으며, 정보통신윤리와 관련해서는 사업자 자율규제 시스템을 구축·운영하고 건전한 게임문화의 정착을 위한 다양한 사업을 하였다.

5. 이메일환경개선추진협의체

이메일환경개선추진협의체(www.antispam.or.kr)는 무분별한 스팸메일과 개인정보 침해 등 정보사회의 역기능을 방지하고 법제도 및 정책개선 연구를 도모하는 한편, 이해관계에 있는 각 기업간의 조정기구로서의 역할을 목적으로 2002년도에 출범하였으며, 협의체 사무국은 (사)한국인터넷기업협회(www.kinternet.org)에 있다.

협의체의 기능 및 주요사업으로는 ① 이메일 환경 개선을 위한 공동사업의 발굴 및 시행, ② 불법메일의 방지와 자율적인 이메일 환경개선 준수규정 제정, ③ 불법메일의 방지를 위한 기업윤리강령 제정, ④ 기업인증마크제 도입, ⑤ 불법메일 및 발송자에 관한 규제방안 연구, ⑥ 불법메일 근절을 위한 법제도 개선 세미나 개최, ⑦ 이메일 환경 개선을 위한 공익광고·캠페인 전개, ⑧ 이메일 정책에 관한 공청회 및 여론조사 실시, ⑨ 스팸메일 신고센터 운영, ⑩ 기타 이메일 환경 개선을 위한 사업 추진 등이 있다.

제7절 민간의 대응

현실공간의 청소년·여성·미디어·환경문제 등 사회정의 실현에 관심을 가지고 활동해오다 사이버공간의 각종 역기능이 사회문제화 되자 이에까지 활동의 영역을 확대하는 민간단체들이 증가하고 있다. 기독교윤리실천운동, YWCA, 한국여성단체협의회, 미디어세상 열린사람들 등이 그러한 대표적인 단체라고 할 수 있다.

그러나 출발부터 사이버공간에서 발생하는 각종 역기능에 대응하고 인터넷을 보다 유용하고 안전하게 사용할 수 있는 환경으로 조성하려는 단체들도 속속 생겨나고 있는바, 한국사이버감시단과 '안전한 온라인을 위한 민간네트워크' 등이 그러한 단체이다.

특히 청소년들의 인터넷 사용이 급증하자 기존의 청소년 보호 및 선도를 목적으로 하는 시민단체들이 인터넷 역기능 문제의 해소에 노력하는 경우도 많다. 한국청소년문화연구소, 한국청소년마을, 네스튜, 학부모정보감시단 등이 그러한 단체이다.

또한 최근에는 건전한 정보통신윤리의 확립과 올바른 정보이용 문화의 확산을 위한 주요 언론사들의 캠페인 활동이 돋보인다. 여러 신문사들이 주도하고 있는 '클린 인터넷

운동'이 대표적이다.

이상의 시민단체들은 인터넷이 가져온 어마어마한 변화의 소용돌이 속에서 건전한 사이버문화를 만들어 가는데 일익을 담당하고 있다. 시민단체들의 활동은 현재는 유해정보 모니터링, 건전한 정보이용 교육 등에 머물러있지만, 앞으로는 인터넷중독 예방과 치료 상담, 현실성 있는 정책제안 등을 통해 보다 내실 있고 깊이 있는 활동을 전개해 나갈 것으로 기대된다.

1. 사이버범죄일반의 예방을 목적으로 하는 시민단체: 한국사이버감시단(KCGA)

(사)한국사이버감시단은 급변하는 정보화 사회에 급격히 증가하는 사이버공간에서의 네티즌피해를 최소화하고 네티즌들의 권리는 네티즌 스스로가 지켜가자는 취지에서 2000년 2월에 설립된 민간단체이다.

한국사이버감시단의 활동은 매우 다양하다. 우선, 한국사이버감시단은 사이버범죄 또는 정보화의 역기능을 줄여나가기 위해 노력한다. 인터넷 사기, 소프트웨어의 불법복제 및 불법거래, 불법음란물 및 음란정보, 원조교제, 온라인 도박, ID도용, 사이버언어폭력 및 성희롱, 해킹 & 바이러스피해, 인터넷중독 등 사이버상의 유해 요소를 추방하는데 노력한다. 둘째는 청소년들의 올바른 사이버문화와 윤리의식의 함양을 위한 활동이다. 이를 위하여 한국사이버감시단은 정보통신윤리 교육(네티켓)및 홍보(캠페인)와 출판활동 등을 기본 업무로 하며, 특히 오천여 명의 모니터요원들을 바탕으로 청소년에 유해한 불법·불건전 정보에 대한 조사 및 계도(모니터링) 활동을 전개한다. 셋째, 한국사이버감시단은 전자상거래시 발생하는 소비자피해 및 분쟁에 대한 조정을 통해 사이버소비자 피해구제 활동도 한다. 넷째, 한국사이버감시단은 또한 온라인피해신고센터를 운영하고 있다. 온라인상에서 발생하는 전산망범죄(컴퓨터 바이러스 및 해킹 피해, 개인정보 유출 및 침해), 불건전정보범죄(음란 사이트, 불법소프트웨어 제작 및 유포, 사이버성폭력 피해), 영상미디어범죄(온라인게임피해, 채팅 사이트 등에서 일어나는 원조교제, 음란정보 공유)에 의한 네티즌들의 피해신고를 받아 상담, 조정, 해결하는 일을 한다. 마지막으로 한국사이버감시단은 올바른 인터넷문화의 발전을 위해 노력한다. 온라인에서의 유해요소에 대한 다양한 대처방법을 연구·개발·보급하여 '건전한 사이버문화'와 '푸른 사이버세

상'을 만들어가기 위해 노력하며, 네티즌이 안심하고 인터넷을 이용할 수 있도록 '민간자율정화시스템'을 널리 확대하기 위한 민간협력 및 국제협력 활동도 한다.

2. 청소년보호 및 선도를 목적으로 하는 민간단체

1) 한국청소년마을

한국청소년마을(www.kyvillage.org)은 청소년들에게 체험위주의 조화로운 활동기회를 제공하여 국가와 사회발전에 필요한 올바른 청소년 육성에 기여하고, 청소년에 관한 사회적 관심을 드높여 밝고 건전한 사회건설에 이바지하기 위해 1989년에 설립된 단체이다. 본 단체의 주요사업은 청소년 정보문화 창달과 국제화 적응능력 배양 관련 사업, 문화적 감성배양과 잠재력 개발 관련사업, 수련 및 여가활동 관련사업, 지도자 육성에 필요한 강습(연수)회 개최 등으로, 특히 청소년의 정보문화 창달과 국제화 적응능력 배양을 위해 청소년 사이버문화 경진대회, 청소년 인터넷학교 등을 진행하여 청소년들의 정보화능력 배양과 더불어 건전한 정보윤리를 가질 수 있도록 하고 있다.

2) 한국청소년문화연구소(청소년정보감시단; 청소년정보문화공동체)

청소년 스스로 인터넷 공간을 정화하고 건강한 인터넷 문화를 만들자는 취지아래 탄생한 단체가 (사)한국청소년문화연구소(www.youth.re.kr)에서 발족시킨 청소년정보문화공동체(Cyber Youth Culture Community)이다. 청소년정보문화공동체는 청소년 자원봉사 프로그램의 일환으로서 1997년 문화관광부의 후원으로 설립된 청소년정보감시단(Cyber Youth Cap)을 2002년에 확대 개편한 것으로, 온라인상의 유해정보를 감시·정화하는 활동과 청소년 스스로 주체가 된 다양한 정보 문화 동아리활동을 해왔다.

청소년정보문화공동체의 활동은 크게 네 가지로 나누어진다. 첫째는 청소년 사이버정보감시단의 운영이다. 사이버정보감시단은 사이버상의 유해정보나 사이트를 감시・신고・적발하는 일을 수행한다. 감시단이 신고한 유해정보 사이트나 스팸메일 등은 정보통신윤리위원회에 신고조치하며, 자율적인 감시체제를 구축하여 보다 맑고 깨끗한 사이버 세

상 만들기에 앞장선다. 둘째, 청소년 사이버글짱 대회를 개최한다. 짱 문화가 새로운 아이콘으로 떠오른 지금 자칫 시각적이고 감각적으로만 보여 질 수 있는 요즘의 짱 문화를 사이버글짱 대회를 통해 청소년들의 정서함양과 감성증진 도모에 주안점을 두며 청소년들의 새로운 문화코드를 보다 바람직한 형태로 발전시켜 나갈 수 있는 기회를 제공한다. 셋째는 청소년 모바일 유해환경 사진전 의 개최이다. 이는 사진을 통해 오프라인에서의 청소년 유해환경을 고발하고 그 심각성을 알리기 위한 행사이며, 사진을 통하여 청소년들의 윤리의식을 고취시키고 문화생산자로서의 경험과 전문지식을 습득케 하는데 그 주안점을 둔다. 넷째는 정보윤리 포럼의 운영이다. 청소년들에게 이슈가 될 수 있는 주제를 선정하여 그들의 생각과 의견을 발표하도록 하여 토론경험이 부족한 청소년들에게 자기의 생각을 발표케 하고 타인의 의견도 존중 할 수 있는 계기를 마련하여 청소년들의 상호이해를 증진시킨다.

3) 네스튠

네스튠(www.nestune.com)은 인터넷 음란물의 직접적인 피해자가 청소년인 점을 감안, 청소년들 스스로가 자신들의 인터넷 이용 권익을 지키기 위해 무엇인가 해야 한다는 생각으로, 2001년 1월 평택 청담정보통신고의 김성진, 김동현, 최기선 학생 등이 만든 단체이다.

이 단체는 주로 15-19살의 청소년들로 구성되며, 인터넷사이트를 수시로 돌아다니며 음란사이트를 찾아내 폐쇄를 유도하는 일을 주로 하고 있다. 즉 전자우편으로 해당 사이트에 폐쇄하라는 설득 메시지를 전달하고, 여의치 않으면 정보통신윤리위원회 등 관련기관에 신고하는 일을 하고 있다. 이와 같은 일을 한 덕분에 2002년 2월 네스튠 홈페이지가 올바른 인터넷 문화를 확산하는데 기여한 공로로 네띠앙이 주관하는 '휴먼 사이트'로 선정되었고, 2002년 6월 보험회사에서 주최한 전국 중고생 자원봉사대회에서 은상을 수상하면서 이 상금으로 그 동안 국내에 공개된 유해사이트 차단 프로그램을 모아서 CD에 담아 200여명의 학부모들에게 무료로 배포하였다. 특히 2003년 6월 정보문화의 달 기념식에서 건전한 인터넷 문화 확산에 기여한 공로로 김성진 군이 국무총리 상을 받기도 했다. 한편 네스튠 대표 김성진 군은 본인이 만든 청소년유해정보 차단 프로그램 '모야'를 업그레이드하여 학부모정보감시단과 청소년보호위원회에서 내려받을 수 있도록 하고

있다. 그리고 사이버 지킴이로 선정된 네스튜 회원들은 소속 학교나 지역에서 실시하는 강의를 통해 유해사이트의 폐해와 올바른 인터넷 이용에 대한 정보를 제공하고 있다(정보통신윤리위원회, 2002).

4) 학부모정보감시단(PUN)

학부모정보감시단(www.cyberparents.or.kr)은 1998년 9월 100명의 학부모가 결성하여 탄생한 단체로서, 인터넷이 이미 청소년들의 생활의 일부가 되어버린 상황에서 더 이상 인터넷상의 문제들을 방치할 수 없다는 학부모들의 절박한 심정에서 비롯되었다.

학부모정보감시단의 주요 활동은 우선, 인터넷상에서 건전한 사이트를 발굴하여 보급·육성하는 일을 한다. 건전한 정보통신 이용 문화 확산을 위해 어린이·청소년, 부모별로 이들이 이용해도 좋을 건전한 정보를 발굴하여 소개하고 있다. 뿐만 아니라 청소년 유해매체에 대한 정보를 수집하고 검색하여 시정을 요구하며, 시민의 정보능력 향상을 위한 정보통신 교육, 학부모들의 정보통신 이용 능력을 향상시키기 위한 부모 대상 컴퓨터 교육을 실시하고 있으며, 청소년 유해정보 유통을 방지하기 위해 청소년유해정보신고센터를 운영하고 있다. 그리고 네티켓을 비롯해 정보통신을 올바르게 이용할 수 있는 정보통신윤리교육, 교재개발, 교육지원 활동을 하며, 음란물 추방 캠페인 등 청소년 보호를 위한 각종 캠페인, 세미나, 조사활동을 한다. 또한 학부모정보감시단은 국경 없는 인터넷상에서 청소년들의 안전을 지키기 위해 해외단체와의 정보 교류 및 협력도 추구하고 있다.

3. 기타 사회정의 실현을 목적으로 하는 민간단체

1) 기독교윤리실천운동

기독교윤리실천운동(www.cemk.org)은 1987년 12월에 출범하여 지난 16년 동안 국내외 19개 지부가 결성되어 전국에 8천여 명의 기독교인들이 회원으로 가입하는 등 전국적 규모로 성장하였다. 이 단체는 교회의 도덕적 힘을 강화시키고 기독교 신앙을 바탕으로 교회를 바로 세우며 건강한 시민사회를 형성하는 것을 사명으로 건강가정운동, 생

활신앙운동, 건강교회운동, 사회정의운동, 문화소비자운동 등 5대 운동을 전개하고 있다. 이중에서 정보통신윤리 문제는 문화소비자운동 영역에서 다뤄지고 있다.

문화소비자운동은 여러 문화현상들을 관찰, 분석, 진단하여 적절한 대안을 제공함으로써 건전한 사회형성에 기여하며, 이를 위해 교회가 해야 할 일을 지원하는 것을 사명으로 한다. 그래서 문화소비자운동본부에서는 청소년과 학부모를 위한 미디어 교육, 목회자를 위한 미디어 아카데미, 청소년 영상미디어제작 캠프, 청소년 유해환경감시단 운영, 컴퓨터 음란·스팸메일 차단 및 추방을 위한 법조인모임, 스포츠신문 등 간행물 감시, 불건전 방송·광고 감시 및 항의, 로또 등 불법 도박산업 추방, 청소년유해매체 지정 및 포장판매전개, 불건전 전화정보 서비스 추방 캠페인 등과 같은 사업을 추진해왔다. 또한 깨끗한 미디어를 위한 교사운동(이하 깨미동) 분과모임과 영락교회 '저동문화교실'과 연계하여 교회 내 주부이자 학부모인 세대와 청소년들에게 유해한 비디오, 노래 등을 모니터하여 교회 내외적으로 세미나를 통해 알려 활동 영역을 넓혀가고 있다.

2) 서울YWCA

YWCA(Young Women's Christian Association)는 1922년에 설립된 단체로서, 각종 사회봉사활동 및 계몽활동과 더불어 인터넷 유해환경으로부터 청소년을 보호하기 위한 활동을 전개하고 있다.

2003년도의 경우 YWCA는 인터넷 서핑, 게임, 채팅 등 중독현상으로부터 청소년들을 보호하고 인터넷으로부터 유익한 정보를 취사선택할 수 있는 능력함양 교육과 인터넷 유해정보에 대한 모니터링, 청소년 대상 정보통신윤리교육, 청소년대상 우수 커뮤니티 시상식 및 사례발표회 등을 전개하였다. 모니터링 활동은 교사, 중학생, 대학생 등으로 구성된 모니터 요원들이 인터넷상의 정보들을 모니터링하여 청소년 스스로 유익한 정보를 선택할 수 있는 계기를 마련하였으며, 청소년에게 유해한 정보에 대한 고발 접수 및 처리 활동을 하였다. 청소년 대상 정보통신윤리교육은 서울시내 중, 고교생 920명을 대상으로 실시하였으며, 5월과 11월에 약 1,800명이 참석한 가운데 청소년 유해환경감시단 활동 및 인터넷유해사이트 정화활동을 홍보하고, 불건전정보 유통실태, 인터넷 중독 자가진단 등의 다양한 주제로 거리 캠페인을 전개하였다.

3) 한국여성단체협의회

한국여성단체협의회(www.iwomen.or.kr)는 여성단체들 간의 협력과 친선을 도모하고, 여성단체의 발전과 복지사회를 이룩하는 일에 여성이 적극 참여하도록 권장하며, 여성단체의 의견을 정부 및 사회에 반영하기 위한 목적에서 1959년 발족하여 현재 60여 개의 (협동)회원단체들로 구성된 대표적인 여성단체이다.

이 단체의 정보통신윤리 관련 사업의 핵심은 사이버성폭력 문제에 대응하기 위한 인터넷 모니터링 팀의 활동에 있다. 사이버 모니터링 팀은 2000년 사이버 성폭력과의 전쟁을 치르면서 '인터넷 지킴이'로 나서게 되었다. 이들은 사이버공간에서 벌어지는 성폭력의 심각성을 공론화시키고, 이를 막기 위해 다양한 활동을 전개하였으며, 이들의 활동은 사이버 성폭력에 대한 인식제고와 함께 여성단체로 구성된 '사이버 성폭력 네트워크'를 조직하는 결과를 이끌어냈다. 모니터링 팀은 또한 인스턴트 메신저의 대화방에서 생기는 문제와 스팸메일을 막기 위한 캠페인을 실시하였다. 이들은 스팸메일을 방지하는 방법과 대처요령을 담은 포스터를 제작하여 전국에 배포하는 등 스팸메일과의 전쟁을 전개하였다.

4) 미디어세상 열린사람들

2000년 9월에 발족한 미디어세상 열린사람들(www.mediayolsa.or.kr)은 비대화·상업화된 제도언론의 본질을 이해하고 개혁하며, 능동적이고 적극적인 미디어 활용자로서의 권리를 찾음으로써 건전하고 밝은 미디어 문화를 만들어 가고자 설립되었다.

미디어세상 열린사람들은 원래 오프라인 미디어 중심의 모니터링 활동을 해왔으나, 온라인 영역의 확대에 따라 현재는 사이버환경에도 많은 관심을 가지고 연대활동을 전개하고 있다. 구체적으로, 온라인상에서 네티즌을 보호하고 건전한 온라인 문화를 형성하기 위해 정보통신윤리위원회의 후원을 받아 정보통신윤리 교육 및 기술교육을 실시하고 있다. 교육의 내용은 온라인 자율정화활동을 위한 민간단체 실무자들의 정보통신윤리 교육, 유해정보 감시활동을 위한 온라인 교육 등이며, 그밖에도 국내외 관련법 등의 이론

교육, 각 단체별 홈페이지 개설과 운영 관리를 위한 이론 및 기술 교육 등이다. 이와 같은 온라인 미디어 교육은 온라인에 대한 전반적인 이해를 높이고, 기술 교육을 통해 온라인 감시활동을 하는 민간단체의 기반 형성 및 실무자의 전문성과 경쟁력을 높이는 데 많은 도움을 주고 있다.

또한 미디어세상 열린사람들은 전자상거래 시장이 성장함에 따라 발생되는 관련 소비자 피해를 줄이고 안심할 수 있는 전자상거래 환경을 만들고자 유명 포탈사이트 및 쇼핑몰 사이트를 대상으로 사업자 자신에 관한 정보표시 여부, 재화 및 거래조건 등 정보 관련 사항, 대금지급 방법, 개인정보 사항, 약관, 부당 광고 등에 대해 현황조사를 실시하기도 하였다.

4. 사이버범죄와 언론의 역할

전술한 바와 같이, 사이버공간의 건전화를 위한 노력은 사회 다방면에서 활발하게 진행되고 있다. 그러나 앞에서 언급한 정부·공공기관, 사업자단체 및 시민단체의 활동 외에 또 하나 중요한 역할을 담당하는 기관이 언론이다. 언론은 사회전반에 큰 영향을 미칠 뿐만 아니라 특히 청소년의 건전한 윤리의식 함양에 있어 절대적인 위치를 차지한다고 할 수 있다. 따라서 건전한 정보통신윤리의 확립과 올바른 정보이용 문화가 정착되기 위해서는 언론의 적극적인 활동이 필요할 것이다.

그동안 진행되어온 언론의 활동으로는 2001년 3월 내외경제신문의 '사이버 건전문화 캠페인'을 필두로 대한매일의 '클린 사이버 2001', YTN의 '건전한 정보 이용 만들기 캠페인', 조선·중앙일보의 '클린 인터넷 운동', 동아일보의 '건강한 인터넷' 등이 있다. 아래에서는 몇몇 주요 언론사의 캠페인 추진활동을 살펴보기로 한다.

1) 조선일보 - 클린넷

조선일보는 어린이들을 보호하고, 인터넷을 건강하고 안전하게 지키며 성숙한 인터넷 시민의식을 정착시키기 위해 각계인사들을 기획위원으로 하여 2003년 3월 '클린넷' 운동을 발족하였으며, 이 운동의 하나로 정보통신부를 비롯하여 정보보호실천협의회와 정보

보호산업협회 등 보안 관련단체와 엠파스・한국마이크로소프트・프리챌・두루넷・인터파크・CJ홈쇼핑・벅스뮤직・KT・데이콤・하나로통신・드림라인・온세통신・넷시큐어테크놀러지 등 13개사와 공동으로 민・관 합동정보보호운동 캠페인을 벌였다. 또한 4월에는 스팸메일을 자동차단하는 안티스팸 서비스를 무료로 제공하였으며, 5월에는 클린넷 시민포럼을 개최하여 학부모・학생・인터넷 업계 및 정부관계자 등이 참석한 가운데, 인터넷이 청소년 심리에 끼치는 부정적 영향과 음란, 폭력물로부터의 청소년 보호방안을 논의하였다.

2) 동아일보 - '건강한 인터넷'

동아일보는 2003년 4월 15일 창간 83주년 기념사업의 하나로 인터넷의 역기능을 줄이기 위한 '건강한 인터넷' 캠페인을 펼쳤다. 정보통신부의 후원 아래 연중 캠페인으로 추진된 이 운동에는 정보보호실천협의회, 학부모정보감시단 등 4개 기관과 KT, KTF, 다음커뮤니케이션, NHN 등 15개 기업이 참여하였으며, 개발연구협의체(CODS) 등 비정부기구(NGO)도 참여하였다. 2003년 6월에는 정보통신윤리위원회가 운영하는 '건강한 인터넷' 캠페인 공식 홈페이지를 열어 그동안 언론보도와 오프라인 행사에 머물렀던 캠페인에 네티즌이 직접 참여할 수 있는 장을 마련했다. 또한 동아일보는 정보격차로 인한 불평등을 줄이기 위한 노력을 전개하며, '건강한 인터넷' 캠페인의 일환으로 다양한 기획기사를 연재하기도 하였다.

3) 중앙일보 - 클린 인터넷

중앙일보는 2003년 3월 클린인터넷 국민운동본부와 함께 건전하고 안전한 인터넷 환경을 구현하기 위해 협력하기로 양해각서를 체결하는 등 유해 콘텐츠와 불법적인 인터넷 사용을 추방하기 위해 자율 규정을 정해 전파하기 위한 노력을 전개하였다. 이러한 노력의 일환으로 중앙일보는 2003년 6월 재단법인 클린인터넷 국민운동본부와 공동으로 '사이버중독, 어떻게 대응할 것이가' 라는 주제의 클린 인터넷 제2차 국민 대토론회를 주최하였다. 또한 중앙일보는 클린인터넷 국민운동본부 및 한국정보보호진흥원과 함께

음란, 스팸메일 차단 소프트웨어 1백만개를 무료로 배포하였다. 소프트웨어와 함께 배포된 '부모와 자녀가 함께 보는 클린 인터넷 자료집'은 가정에서 올바른 인터넷 사용을 위한 교재로 꾸며져 매우 유용한 자료로 평가받았다.

4) 국민일보 - '음란물, 자녀의 미래를 망칩니다'

국민일보는 온·오프라인을 통해 음란물과 유해정보가 어린이나 청소년들에게 무차별적으로 배포됨으로써 범죄나 일탈현상이 일어나는 심각한 사회현실에 대한 대책으로 2003년 7월초 '음란물, 자녀의 미래를 망칩니다'라는 캠페인을 시작하였으며, 7월 11일부터는 '음란물로부터 자녀의 미래를 보호합시다'라는 장기 기획 시리즈를 관련기관·단체와 연계해 보도하였다.

5) 한겨레신문 - '청소년 넷사랑! 아빠와 함께'

한겨레신문사는 2003년 7월 2일 한국언론회관 국제회의장에서 '청소년 넷사랑! 아빠와 함께' 캠페인 선포식을 가졌다. 7월부터 6개월 동안 청소년보호위원회와 함께 진행한 이 행사는 '아버지와 함께하는 인터넷 교육', '아빠와 함께하는 정보검색대회', '인터넷 상시 모니터링' 등 아버지와 청소년 자녀가 함께 인터넷 음란물에 대처하도록 하는 다양한 프로그램으로 꾸며졌다(정보통신윤리위원회, 2004).

5. 사이버범죄 예방을 위한 시민운동·단체의 연합 - 안전한온라인을위한민간네트워크(SON)

안전한온라인을위한민간네트워크(안전넷: www.safeonline.or.kr)는 온라인상에서의 불법·유해 정보가 심각한 사회문제로 확대되는 것을 막고, 보다 성숙한 정보통신 문화를 만들어 가기 위하여 2001년 5월에 22개의 민간단체가 참여하여 발족하였다(공동사무국: 기독교윤리실천운동, 한국사이버감시단).

안전넷은 인터넷 불건전정보에 대한 민간영역의 자율정화능력을 배양하고 민간감시단

체들 간의 상호협력을 체계화하는 “민간온라인감시단체네트워크” 구축을 목적으로 현재 40여개 단체가 활동하고 있다. 안전넷은 민간감시단체가 가지고 있는 독특성과 장점을 살려 정부로부터 상대적으로 독립적이며 자발적인 활동을 통해 여론의 지지를 이끌어내고 있다. 안전넷은 온라인상의 많은 시민운동 과제들을 공동으로 수행하면서 자연스럽게 연대의 필요성을 확인하고, 사안별 연대를 통해 단체들 상호간의 이해와 신뢰를 구축해 나가면서 네트워크 조직을 만들어가야 한다는 원칙을 가지고 활동한다. 감시활동 분과, 교육홍보 분과, 조사연구 분과 등 3개의 분과가 있어 참여하는 회원단체는 적어도 한 개 이상의 분과에 소속하여 활동하고 있으며, 단체간의 원활한 의사교환 통로와 중재 역할을 담당하는 운영위원회를 두고 있다. 발대식을 겸하여 민간차원의 감시활동을 수행하는 단체 실무자들의 전문성 확보를 위한 “안전한 정보통신문화 발전을 위한 포럼”을 시작으로 본격적인 온라인 정화활동을 전개하였다. 또한 정보사회에 대한 이해를 넓히고 연대를 통한 시민운동전개를 위한 기법을 배우며, 인터넷 교육 홍보활동 전략 점검, 인터넷 모니터링 방법론 습득, 실무자들의 협력증진 방안 모색 등을 위한 워크숍을 개최하여 민간단체 실무자들의 전문성을 개발하고 단체들 간의 연대활동이 긴밀해질 수 있도록 하였다. 그리고 청소년 보호는 도외시한 채 수익창출에만 열을 올리고 있는 세이클럽의 경영형태가 인터넷 콘텐츠 업계의 성공적인 수익모델로 칭송받고 마치 닷컴의 모범답안인 것처럼 인식되고 있는 우려를 바로잡기 위하여 세이클럽을 집중 모니터링하였으며 성명서[111]를 발표하였다. 성명서 발표이후 세이클럽에서는 청소년 보호를 위한 대책을 마련하고 700ARS서비스를 통해 청소년에게 부과되었던 요금을 감면해 주는 결과를 가져왔다. 안전넷 회원단체와 국내 민간단체 실무자들이 모여 인터넷상에서의 ‘표현의 자유’와 불법·유해정보로부터 정보이용자 보호 및 안전한 인터넷을 만들기 위한 좋은 방향을 모색하기 위해 “안전한 인터넷 이용과 표현의 자유에 대한 토론회”를 개최하기도 하였다.

111) ① 세이클럽은 세이캐시제도를 개편하여 청소년이 이용하기에 적절한 가격을 책정, 청소년용 세이캐시제도를 도입할 것을 요구한다. ② 세이클럽내에서 청소년간의 경쟁심리와 사치심리를 조장하는 행위를 중단할 것을 요구한다. ③ 700ARS서비스를 통해 과도한 요금이 부과된 청소년과 소비자에 대해서 보상대책과 방안을 강구하여, 언론 및 자사사이트, 회원공지 등을 통하여 이를 공지하고 보상할 것을 요구한다.

제5장 현행 사이버범죄 규제전략이 갖는 문제점

앞 장에서 본 바와 같이 사이버범죄를 예방·규제하고 정보통신윤리를 확립하기 위한 우리사회의 노력은 정부 및 형사사법기관, 정보화 관련 공공기관, 정보통신 사업자단체, 시민단체 및 언론기관 등 다양한 주체들에 의해 다양한 방법으로 진행되어 왔다. 그러나 이러한 노력들에도 불구하고 우리사회 사이버범죄는 폭발적으로 증가하고 있는 실정이다. 게다가 최근에 발생한 일련의 사이버범죄를 살펴보면 그 범죄성향이 현행 규제전략으로는 도저히 감당할 수 없을 정도로 지능화, 광역화, 대량화, 다양화, 저연령화 되었다는 것을 알 수 있다. 특히 외국의 서버를 기초로 국내의 인터넷서버를 마비시키는 바이러스유포, 공공기관 및 기업에 대한 해킹, 각종 불법·음란 사이트, 인터넷사기 및 개인정보침해와 같은 중대한 사이버범죄에 의한 피해사례는 거의 매일 매스컴을 장식하고 있다고 해도 과언이 아닐 것이다.

이 장과 다음 두 장에서는 우리나라의 현행 사이버범죄 규제전략이 갖는 문제점들을 진단해 보고, 그러한 진단을 바탕으로 하여 인터넷을 이용한 청소년범죄에 대한 효율적인 대처방안을 모색해 보고자 한다. 먼저, 본 장에서는 현행 사이버범죄의 규제전략이 갖는 문제점을 법적·제도적 측면, 사이버범죄 문제의 심각성에 대한 사회적 인식의 측면, 형사사법기관들의 대응능력 측면, 그리고 총괄적 조정기관의 부재라는 측면에서 평가해 보기로 한다.

제1절 법적·제도적 미비점

1. 법적 미비점

1) 처벌법규의 혼재 및 중복

현재 사이버범죄와 관련된 법령은 통합된 법률 없이 형법 및 청소년보호법, 성폭력범

죄의처벌및피해자보호등에관한법률, 청소년의성보호에관한법률과 같은 형사특별법, 그리고 정보화촉진기본법, 전기통신기본법, 전기통신사업법, 정보통신망이용촉진및정보보호등에관한법률 등과 같은 정보통신윤리 관련 법제가 혼재해 있다.

그런데 이렇게 처벌법규가 일원화되지 못하고 혼재되어 있는 경우 범죄행위에 상응하는 형사처벌에 대한 예측가능성이 떨어지게 된다. 또한 사이버범죄 처벌을 위한 법규정이 상황에 따라 부처별로 제정·보완됨으로써 동일한 법익을 침해하는 행위에 대해 여러 가지 처벌법규가 중복 적용되는 경우가 많을 뿐 아니라, 같은 행위를 규제하는데 있어 서로 다른 용어를 사용함으로써 처벌대상을 확정하는데 어려움을 겪게 되는 수가 많다.

2) 처벌법규의 부재 및 불명확

인터넷 등 사이버공간은 이전과는 비교할 수 없을 정도로 광역화, 다양화되고 있으며, IT산업의 비약적인 발전으로 나날이 새로운 유형의 사이버범죄가 발견되고 있다. 그러나 우리사회의 법률체계는 이러한 변화를 제때 따라가지 못하며, 개별 범죄행위에 대해서도 그 구성요건의 불명확으로 인해 처벌하지 못하는 경우가 많이 발생하고 있다.

형법의 경우 특성상 과거 50, 60년대에 제정된 조항이 대부분이기 때문에 최근 인터넷상에서 발생하는 신종 범죄행위들에 대해서는 적용이 어려운 경우가 많다. 또한 특정 법률에 있어 처벌요건이 불명확한 경우가 많다. 예를 들어, 최근 인터넷상에서 범죄의 온상이 되고 있는 사이버머니의 경우 형법상의 '재물'로 볼 수 없기 때문에 도박이나 절도사건, 사기사건에 적용시키기가 어렵다. 그리고 특정 홈페이지에 무단으로 게시물을 수백, 수천 건 올려 서버자체를 마비시켜 버리는 속칭 '게시판 도배'와 같은 테러행위에 대해서도 직접적으로 시스템상의 통신운영을 방해했다는 것을 입증하지 못한다면 처벌을 할 법규가 없다.

이와 같이 타인에게 피해를 입히고 명백히 범죄행위임에도 불구하고 처벌법규가 미비하여 처벌하지 못하는 사례가 다수 발생하고 있는 점은 사이버범죄를 더욱 양산하는 결과로 나타나고 있다.

3) 정보통신사업자에 대한 직접적 규제법률의 미비

흔히 사이버공간에서 불건전정보의 3주체를 정보통신사업자(ISP), 정보제공자(information provider, IP), 정보이용자(end-user)라 한다. 이 중에서 정보통신사업자(ISP)는 일반인에게 인터넷에의 접속을 가능하게 해주는 상업적 사업자를 말한다. 그러나 이러한 정보통신사업자들은 상업성에 치우친 나머지 정보통신윤리를 망각하고 오히려 사이버범죄를 부추기는 경우도 있다. 문제는 정보통신사업자 스스로가 불건전·유해매체물을 유포한 상황에서는 직접적인 제재가 가능하지만, 자신들이 제공하는 인터넷서버를 통해 불건전·유해매체물이 유포될 경우에는 처벌이 이루어질 수 없다는 점이다. 물론 이와 같은 문제는 인터넷상의 표현의 자유와 상충되어 논란의 소지가 있는 부분이다.

인터넷 등 정보통신사업자들에게는 원칙적으로 자율성이 존중되어 왔으며, 불건전정보에 대해서도 자신들이 직접 유포하지 않은 한 면책을 누리는 경우가 많았다. 그러나 인터넷 기술의 발달과 함께 불건전정보의 유통이 불러일으키는 사회적 문제가 심각해짐에 따라 이러한 전통적인 관행이 점차 바뀌어 인터넷서비스제공자들을 상황에 따라 어느 정도 규제하려는 움직임이 나타나고 있는 것이다. 이러한 정부의 규제 움직임에 대하여 정보통신사업자들은 자율정화라는 자구책을 내놓고 있지만, 장기적으로 볼 때 자율정화는 한계를 드러낼 수밖에 없으며, 따라서 이들에 대한 보다 직접적인 규제 장치가 미비한 것은 큰 문제점이 아닐 수 없다.

특히 영국과 독일에 있어서도 원칙적으로는 자율성을 보장하지만, 정보통신사업자가 자신의 서비스망에서 불법적이거나 불건전한 정보가 유통되는 것을 스스로 인지하였거나 제3자로부터 제보를 받고 또 그것을 제거할 수 있는 기술적인 방법이 있을 경우, 우선 일차적으로 정보제공자에게 통보하여 자발적으로 그 정보를 제거하도록 권유하고, 정보제공자가 이를 거부할 경우 정보통신사업자가 이를 제거하여야 한다고 규정하고 있을 만큼 정보통신사업자의 역할을 중시하고 있다.[112] 이들 국가에서는 정보통신사업자가 이러한 노력을 기울일 경우에 한해, 만일에 뒤따를 수 있는 법적 책임추궁에서 선처를 바랄 수 있다는 것을 볼 때 한국에 있어서도 좋은 제도적 시사점이 될 수 있을 것이다.

---

112) http://www.icec.or.kr/.

4) 사이버범죄와 연계된 법률의 미비

사이버범죄에 대한 처벌에 있어서 또 하나의 중요한 사실은 사이버범죄가 그것과 직접적으로 관련된 법률 외에 다른 일반 법률들과 연계되어 발생하는 경우가 많다는 점이다. 사이버범죄는 이와 같은 연계 법률이 명확히 구성되어 있고, 처벌규정 또한 명확할 때 보다 확실하게 근절될 수 있는 것이다. 그러나 실제로는 사이버범죄와 연계되는 법률의 미비로 솜방망이식 처벌에 그치는 경우가 많고, 심지어 명백한 범죄행위임에도 불구하고 관련 조항이 없어 처벌하지 못하는 경우가 많아 문제가 된다.

대표적인 경우가 주민등록번호 위조에 따른 개인정보의 도용이다. 인터넷상에는 주민등록번호 생성기로 만들어진 주민등록번호와 실명이 아주 싸게 거래되고 있고, 이에 따른 신분증의 위·변조 및 도용으로 피해자에게 막대한 경제적, 정신적 피해를 입히고 있다. 그러나 이 부분에서 문제가 되는 것은 첫째, 피도용자에게 직접적인 경제적 피해가 없으면 처벌할 수 없다는 점과 둘째, 현행 주민등록법상 '재산상의 이익'을 목적으로 도용되는 경우에만 처벌이 가능하도록 되어 있어,[113] 인터넷상의 주민등록번호 생성기를 통해 만들어진 주민등록번호가 재산상의 이익 외에 사용될 때는 처벌이 어렵다.

또 다른 경우는 인터넷에 범람하고 있는 불법·음란물의 유통과 관련된 것으로, 최근 성인전용 PC방이 범람하면서 이곳이 불법·음란물의 주요 루트가 되고 있다는 점은 관계당국에서도 인지하고 있는 사실이다. 그러나 PC방은 업종 분류상 자유업으로 분류되어 있기 때문에 사업자 등록만 하면 누구든지 운영할 수 있고, 단속기준도 일반 PC방과 같아서 실질적인 단속이 어렵다.

이와 같이 사이버범죄는 직접적으로 영향을 미치는 법률 외에 기타 주변 법률과도 밀접한 관련이 있다. 따라서 연계 법률의 미비는 사이버범죄자에게 있어 하나의 탈출구가 되고 있는 실정이다.

---

113) 지난 2001년 1월 26일 개정된 주민등록법의 제21조9항에는 '다른 사람의 주민등록번호를 자기 또는 다른 사람의 재물이나 재산상의 이익을 위해 사용한 자'에 한해 3년 이하 징역이나 1000만원 이하의 벌금에 처하도록 규정돼 있다. 따라서 인터넷 사이트에 가입하거나 서비스를 이용해도 '공짜'인 경우 이 규정을 적용할 수 없다는 것이다.

2. 제도적 미비점

1) 사이버범죄 신고처리체제의 분산

사이버범죄가 급속도로 확산되는데 비하여 사이버범죄에 대한 신고 및 처리창구는 제대로 알려져 있지 않다. 대체로 일반적인 사건 및 피해 신고처인 경찰청, '사이버 118 해킹신고센터'를 운영하며 관련 사건의 신고를 접수처리하고 있는 한국정보보호진흥원, 정보통신윤리위원회, 국가정보원 및 한국소비자보호원 등이 주된 신고처가 되곤 하지만 사례별로 처리기관이나 절차가 다르기 때문에 다른 기관으로 다시 연락을 하거나 신고자나 피해자가 인터넷 홈페이지를 뒤져야 하는 경우가 태반이다.

예컨대, 정보통신서비스 일반의 신고와 관련해서는 정보통신부 민원서비스가, 개인 및 고객 정보 누출피해 일반에 대해서는 한국정보보호진흥원의 정보보호상담실이나 개인정보침해신고센터가, 해킹·바이러스는 한국정보보호진흥원이나 정보보안사업자(안철수랩 등)의 해킹・바이러스상담지원센터, 경찰청 사이버테러대응센터, 국가정보원 등이, 그리고 사이버성폭력, 사이버명예훼손 등 일반 사이버범죄는 경찰청 사이버테러대응센터나 사이버범죄수사대 또는 정보통신윤리위원회 등이, 전자상거래피해나 인터넷사기는 한국소비자보호원 등이 담당하고 있다.

이렇듯 사이버범죄와 관련한 신고는 사이버범죄의 다양성에 비례하여 많은 기관에서 분산하여 이루어지기 때문에 시민들은 신고기관의 연락처나 신고방법을 쉽게 인지하지 못하며, 신고처리도 중복되거나 지나치게 많은 시간이 소요되는 등 비효율성을 면치 못하고 있다. 그러므로 차제에 사이버범죄와 관련된 신고창구를 현재의 다원화된 신고처리체계에서 하나의 창구로 통합함으로써 사이버범죄 신고처리의 효율성을 확보하는 것이 절실히 요구된다고 하겠다.

2) 청소년유해매체물에 대한 이중규제

청소년유해매체물과 관련하여 현행 제도상 가장 큰 문제점은 청소년유해물에 대한 이중규제이다. 청소년유해매체물은 게임, 영상물, 도서 등 다양한 루트를 통해서 양산되고 있다.

그러나 청소년유해매체물은 복수의 법률과 복수의 기관에 의해 규제가 이루어지고 있기 때문에 규제의 실효성이 떨어지고 정보통신사업자들의 불만을 초래하는 요인이 되기도 한다.

이를테면, 영상물등급위원회가 '음반·비디오물및게임물에관한법률'에 따라 사전에 청소년 이용 등급을 매겨놓은 것을 나중에 정보통신윤리위원회가 '정보통신망이용촉진및정보보호등에관한법률' 등으로 다시 청소년유해매체물 여부를 판정하는 식이다. 얼핏 두 기관의 역할분담이 잘돼 있는 것처럼 보이지만, 내부를 들여다보면 심의기준과 내용이 서로 다르고 법적의무도 판이하다는 것을 알 수 있다.

청소년들이 즐기는 온라인게임의 대표격인 '리니지'가 관련 규제제도가 이원화되어 있는 대표적인 사례이다. 즉 문화관광부 산하의 영상물등급위원회가 게임물 사전·사후 심의권을 갖고 있고, 정보통신부 산하 정보통신윤리위원회도 사후 심의를 하고 있는 상황이다. 이러한 이중규제의 결과로 영상물등급위원회는 '리니지'에 대하여 '18세 이상 이용'의 규정을 적용하였는가 하면, 정보통신윤리위원회는 '19세 이상 이용'을 적용하여 양자를 모두 표시해야 하는 등 규제의 혼선을 가져옴과 동시에 관련 업계의 강한 반발을 사고 있다.[114]

특히 문제가 되는 것은 청소년 기준연령을 두 기관이 서로 다르게 잡고 있는 점이다. 물론 이러한 것은 성년의 하한 연령을 20살로 정한 현행 민법에 대한 해석의 차이일 수도 있으나, 관련 기업의 입장에서는 수익과 직결되는 것이며, 청소년유해매체물의 범람을 막을 수 있는 기준 자체가 모호해져 자칫 역효과를 가져올 수 있어 18세에서 19세 사이 연령층에 대한 '규제의 사각지대'를 만드는 결과도 되고 있다.[115]

3) 사이버범죄 피해자에 대한 구제제도 부족

114) 이러한 이중적 규제에 대한 경종을 울리는 법원 결정이 나왔는바, 정보통신윤리위원회(정통윤)가 엔씨소프트의 온라인게임 '리니지2'를 청소년유해매체물로 판정한 데 대해 법원이 효력정지 결정을 내린 것이다. 이번 결정은 "정통윤 결정이 영상물등급위원회(영등위)가 리니지2에 대해 18세 이상 이용가 판정을 내린 것과 어긋나고, 18세 회원에 대한 서비스 여부 등에 대해 많은 혼란을 낳고 있다."는 엔씨소프트의 주장을 법원이 받아들인 것으로 풀이된다. 특히 이번 결정에 따라 가뜩이나 영등위와 온라인게임 중복심의 논란을 빚고 있는 정통윤의 입지가 적지 않은 영향을 받을 것으로 보인다(스포츠서울, 2004년 7월 21일자).

115) 전자신문, 2004년 6월 4일자.

날로 증가하고 있는 사이버범죄 건수와 맞물려 사이버범죄 피해자의 숫자도 크게 증가하고 있다. 특히 사이버성폭력, 사이버명예훼손, 인터넷사기 및 전자상거래 관련 범죄 피해가 심각한 문제로 대두하고 있다. 현행법상 사이버명예훼손 및 사이버성폭력 피해자의 경우 '정보통신망이용촉진및정보보호등에관한법률' 등으로 가해자에 대한 처벌과 피해구제가 가능하기 때문에 일단 정보통신윤리위원회내 사이버명예훼손·성폭력분쟁조정센터(www.cyberhumanrights.or.kr)로 상담을 요청할 수 있으며, 동 센터에서는 상담서비스와 법률자문을 제공하고 있다. 그리고 인터넷사기 및 전자상거래관련 피해는 소비자보호원 등에 문의한 후 경찰청에 신고할 수 있으며, 사기로 인한 피해금액은 피해구조신청 등을 통해 관할 지방검찰청에서 구제받을 수 있다.

그러나 사이버범죄에 대한 피해자구제에 있어서는 몇 가지 해결해야 할 문제가 있다. 첫째는 피해자구제를 위한 전담기관이 없다는 것이다. 사이버범죄의 대응에 있어서도 일괄적 통제기구가 없는 것처럼 피해자의 구제에 있어서도 전담 기관이 없는 것이 문제이다. 사이버범죄 피해자의 경우 대부분 구제 방법에 대한 법률적 지식이 없는데 반하여 관련 구제기관은 피해 유형에 따라 세분화되어 있어 피해를 입고서도 쉽게 구제를 요청할 수 없는 경우가 많다.

둘째는 현재 활발히 시행되고 있는 소송 이외의 분쟁해결제도에 관한 문제점이다. 정보통신윤리위원회는 2003년 10월부터 사이버명예훼손·성폭력분쟁조정센터를 개설하여 피해자와 가해자간의 원만한 합의를 유도하고 있으며, 한국전자거래진흥원 산하 전자거래분쟁조정위원회에서도 전자상거래 관련 분쟁 조정 업무를 시행하고 있다.[116] 그러나 분쟁해결제도는 그 본연의 취지와는 달리 아직 업무실적이 미미한 수준이며, 특히 당사자간의 합의를 통해 분쟁의 재연을 사전에 방지하고 법적 절차를 통하지 않고서도 신속히 사건이 종결될 있는 사이버명예훼손·성폭력분쟁에 관한 부분은 2003년도부터 꾸준히 설치논의는 있어왔지만, 아직도 조정센터에 머물고 있어 피해구제제도의 기능을 다하지 못하고 있다. 따라서 사이버범죄 피해자의 실질적인 구제를 위하여 사이버범죄 피해와 관련된 각종 분쟁조정위원회의 설치 및 기능강화가 시급하다 하겠다.

116) http://www.hackersnews.org/data/2003/04/0414_23.html.

4) 유관기관간 협력체제 미비

사이버범죄는 범죄 그 자체의 특성과 수사상 어려움으로 인해 하나의 특정 기관만의 노력으로는 해결할 수 없고, 범국가적 차원에서 유관기관들이 상호협력하여 해결할 수밖에 없는 것이다. 그러나 그동안 관계 당국 및 정보통신사업자, 그리고 민간단체 등은 상호유기적 협력을 통하여 문제해결에 접근하기보다는 각자 독자적으로 사이버범죄 문제해결에 대처하였던 것이 사실이다. 이와 같은 문제로 인하여 그동안 업무의 중복과 처리의 지연, 비효율성이 지속되어 왔던 것이다.

최근 정보통신부 산하 정보통신윤리위원회는 보도자료에서 경찰청과의 핫라인 활성화를 통하여 사이버범죄에 대응한다고 발표한 바 있다. 그러나 사이버범죄의 대응에 있어서 그 두 기관이 주축기관임에는 이론의 여지가 없지만, 보다 근본적으로 사이버범죄의 문제에 대처하기 위해서는 모든 주체들의 참여가 필요하다. 요컨대, 상기 두 기관을 포함하여 기타 정보화 공공기관, 정보통신사업자, 그리고 민간감시단체가 모두 참여하는 유기적 공조체제가 구성될 필요가 있는 것이다. 또한 사이버범죄자에 대한 사후처리과정과 재범방지도 중요하다. 이점에서 사전예방 및 감시, 진압기관인 경찰과 검찰, 정보통신부 산하 기관들, 이미 사이버범죄 피의자 신분으로 구속, 불구속 처리된 사람들에 대한 재범방지 대책으로서의 사회봉사와 수강명령 등을 집행하는 보호관찰기관의 상호 협력체제의 구축도 중요하다고 할 것이다.

제2절 문제의 심각성에 대한 사회적 인식부족

현행 사이버범죄 규제전략이 실효성을 거두고 있지 못하는 또 한 가지 중요한 이유는 우리 사회가 아직도 사이버범죄의 문제를 그다지 심각하게 받아들이지 않는 경향이 있는 탓이기도 하다.

사이버공간에서의 각종 범죄행위들은 정보화 사회의 미래에 암울한 그림자를 던지는 중대한 도전이며, 따라서 이에 대한 효과적인 대응은 형사사법기관들의 노력만으로는 부족하며, 사회일반의 높은 신고 및 참여의식이 담보되어야 한다. 이를 위해서는 우선 일

반 네티즌들이 사이버범죄 문제의 심각성을 제대로 인식할 필요가 있을 것이다. 그러나 아직 우리사회의 현실은 그렇지 않은 것 같다. 사이버범죄 피해를 경험하지 않은 사람들은 차치하더라도 피해경험자들 조차도 상당수는 사이버범죄 문제의 심각성을 제대로 인식하고 있지 않은 것 같다. 심지어 일부 청소년들을 중심으로는 여전히 사이버범죄자(예컨대, 해커)에 대한 긍정적 내지는 낭만적인 이미지를 가지고 있는 것도 사실이다. 이러한 사실은 사이버범죄가 갖는 높은 암수와 지극히 낮은 신고율에 의해서도 입증된다.

이 절에서는 지난 2000년도에 한국형사정책연구원에서 실시한 「사이버공간에서의 범죄피해 조사」[117]에서 나타난 피해신고와 관련한 몇 가지 조사결과를 살펴보면서 이 문제를 생각해 보기로 한다.

이 조사에서는 우선 사이버범죄로 인한 피해를 실제로 경험하였는지 여부와는 상관없이 일반 네티즌들을 대상으로 인터넷 사용 중에 범죄(피해)를 유발할 가능성이 있는 유해한 정보나 사이트를 발견하게 될 때 이를 검찰이나 경찰, 혹은 기타 신고센터에 신고할 의향이 있는지를 물었다. 이에 대한 대답이 <표 5-1>에 나와 있다. 이 자료에 의하면 그러한 상황에 처할 경우 '적극적으로 신고할 것'이라고 답한 사람이 전체의 16.1%이고, '상황이 허락한다면 신고할 것'이라고 답한 사람이 57.5%로서 신고여부에 대해 긍정적으로 답한 사람이 절대 다수인 73.6%나 되었다.

<표 5-1> 신고의지에 관한 질문

분 류	빈 도	%
적극적으로 신고할 생각이다	1158	16.1
상황이 허락한다면 신고할 것이다	4143	57.5
신고할지 않을지 잘 모르겠다	1783	24.8
신고하지 않을 것이다	116	1.6
계	**7200**	**100.0**

117) 이민식, 「사이버공간에서의 범죄피해」, 한국형사정책연구원 연구보고서, 2000.

그러나 이와 같은 결과는 사람들이 막연히 사회적으로 바람직한 방향으로 답하는 경향(social desirability)에 의한 것일지 모른다. 예컨대, 이 조사에서는 실제 사이버범죄 피해를 당한 경험이 있는 사람들을 대상으로 그들이 자신이 당한 피해를 형사사법당국이나 기타 피해신고센터에 신고하였는지 여부를 물어보았는데, 그 결과는 사람들의 일반적인 신고의지와는 달리 피해경험자의 극히 일부분(4.9%)만이 신고를 한 것으로 나타났다(<표 5-2>). 이러한 결과는 결국 대부분의 피해자들이 사이버범죄 피해를 별로 심각치 않은 일로 치부해 버리는 경향이 있음을 의미하는 것이라고 하겠다. 실제로 이 연구에서는 전체 피해경험자의 절대 다수인 약 88%의 응답자들이 자신들이 당한 피해를 '별로 심각치 않았다'거나 '약간 심각하였다'라고 답하였다.

<표 5-2> 피해신고 여부

분 류	빈 도	%
신 고 함	263	4.9
신고하지 않음	5059	95.1
계	5322	100.0

다음으로 사이버범죄 피해를 경험하고도 피해를 신고하지 않은 사람들을 대상으로 신고를 하지 않은 가장 큰 이유가 무엇인지를 물었다. <표 5-3>에 그 결과가 나와 있다.

<표 5-3> 피해를 신고하지 않은 이유

분 류	빈 도	%
피해가 경미하여	1,591	37.0
스스로 해결할 수 있는 일이라서	863	20.1
충분한 증거를 확보하지 못하여서	449	10.4
신고절차가 복잡하여	234	5.4
신고해도 이해하지 못할 것 같아서	231	5.4
신고해도 잡지 못할 것 같아서	488	11.3
기 타	447	10.4
계	4,303	100.0

위의 자료에 의하면, 신고를 하지 않은 가장 큰 이유는 '피해가 경미하여'로서 전체 미신고자의 37%나 된다. 두 번째로 큰 미신고 사유로서는 '스스로 해결할 수 있는 일이라서'로서 20.1%이며, 그 다음은 '신고해도 잡지 못할 것 같아서'(11.3%), '충분한 증거를 확보하지 못해서'(10.4%), 그리고 '신고절차가 복잡하여'와 '신고해도 이해하지 못할 것 같아서'(각각 5.4%)의 순으로 나타났다. 요컨대, 미신고의 일차적 이유는 피해자들이 그러한 피해를 그다지 심각하게 받아들이지 않기 때문이며, 그 다음으로는 사이버범죄에 대한 형사사법기관의 대응력과 형사사법적 절차에 대한 신뢰의 부족[118]도 중요한 몫을 차지하는 것으로 나타났다.

제3절 형사사법기관의 대응능력 부족

사이버범죄의 대응에 중추적인 역할을 담당하고 있는 형사사법기관인 경찰청 사이버테러대응센터(또는 사이버범죄수사대)와 검찰청 인터넷범죄수사센터에서는 사이버범죄 문제의 해결을 위해 다각적인 노력을 전개하고 있다. 그러나 이러한 노력에도 불구하고 사이버범죄에 대한 대응은 만족할 만한 효과를 거두지 못하고 있는 것으로 평가되는데, 그것은 이들 기관의 인적 자원의 부족 및 전문성 부족에서 기인하는 바가 크다고 할 수 있다.

경찰과 검찰에서는 장기적인 대책을 수립하여 전담부서로 하여금 지속적인 단속업무

118) 다음은 전체 연구대상자에게 '사이버범죄에 대한 형사사법기관들의 대응력에 대한 신뢰의 정도'를 물은 결과이다. 이 자료에 의하면 '전혀 신뢰하지 않는다'고 답한 사람이 14.9%, '대체로 신뢰하지 않는다'고 답한 응답자가 57.6%로서 절대 다수인 72.5%가 형사사법기관들의 사이버범죄에 대한 대응력을 불신하고 있는 것을 알 수 있다.

분 류	빈 도	%
전혀 신뢰하지 않는다	1076	14.9
대체로 신뢰하지 않는다	4144	57.6
잘 모르겠다	322	4.5
대체로 신뢰한다	1591	22.1
전적으로 신뢰한다	67	0.9
계	7200	100.0

를 수행토록 하고 있으며, 자체직원을 선발하여 교육을 시키고 이들을 사이버범죄수사 전문요원으로 활용하고 있다. 하지만 자체 선발된 직원들이 사이버범죄를 수사할 수 있는 전문요원이 되기까지에는 상당한 시간이 소요되며 사이버범죄자들의 범죄능력 향상 속도에 대응할 수 있는 지식이 짧은 시간에 습득되기 어려운 점을 감안한다면, 좀더 현실적이며 적극적인 대책의 입안과 실행이 필요하다고 할 것이다.

1. 경찰의 대응능력 및 전문성 부족

경찰에서는 사이버테러대응센터가 사이버범죄에 대한 대응을 주도하고 있다. 사이버테러대응센터는 현재 70여명의 인력으로 구성된 한국에서 가장 중추적인 사이버범죄 대응기관이다. 그러나 본 기관의 내실은 그 이름에 걸맞지 않다. 인력의 측면에서 볼 때 사이버테러대응센터의 인원 70여명 중 사이버보안업무 종사자는 30여명에 불과하여 실질적으로 절반이상이 전문가라 할 수 없다.[119]

이러한 인력 및 전문성의 부족은 하급기관인 지방경찰청 사이버범죄수사대나 일선 경찰서 사이버수사반의 경우 더욱 심각하게 나타나고 있다. 지방경찰청 사이버수사대에서는 주로 간단한 해킹사건이나 개인정보침해, 음란물유통, 사이버명예훼손등과 같은 '일반 사이버범죄'를 취급하고 있으나, 그 인적 자원과 예산 및 시설·장비 등 물적 여건이 본청 사이버테러대응센터에 비하면 현저히 낮아 문제가 되고 있다. 특히 단순히 인력면만 보더라도 2003년 11월 현재 서울지방경찰청 29명, 부산지방경찰청 12명, 경기지방경찰청 11명, 그리고 기타 지방경찰청은 5~11명으로 전문성은 차치하더라도 턱없이 부족한 인원으로 구성되어 있으며, 일반적으로 사이버범죄 담당 경찰관이 내근, 외근을 모두 소화한다고 볼 때 이와 같은 인력은 정말 심각한 수준이라 하지 않을 수 없다.

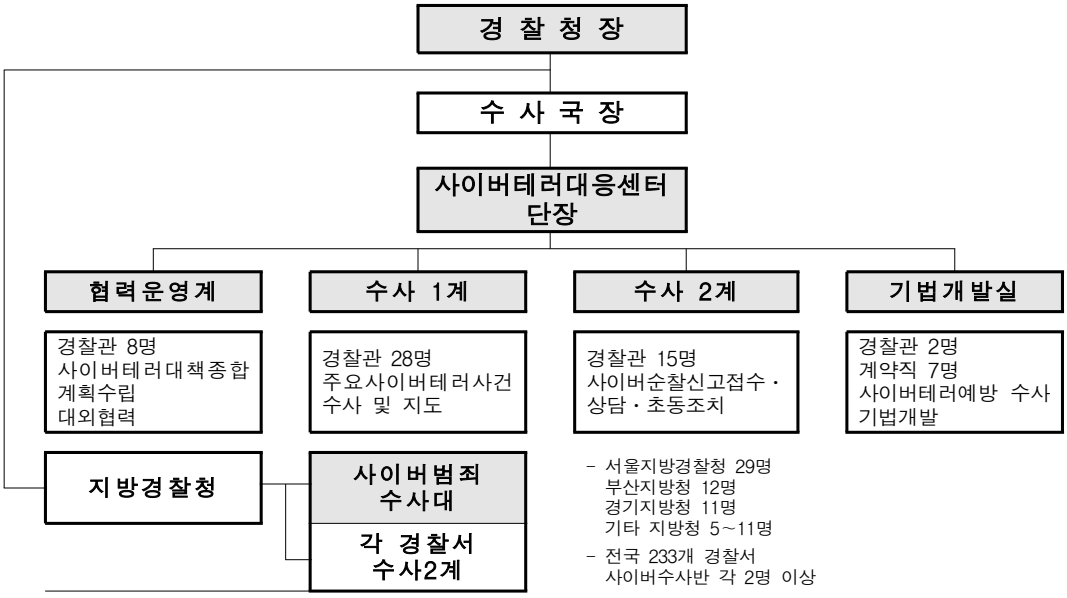
또한 사이버범죄 수사에 있어 최하부 조직이라 할 수 있는 일선 경찰서내의 수사2계에 편성된 사이버수사반의 경우 사이버범죄 담당경찰관이 2명이상이라고 규정하고는 있으나, 실질적으로 1-3명에 불과하고 그나마도 컴퓨터운영체제 및 인터넷 사용 등에 관

119) 서울신문, 2004년 7월 15일자에서는 경찰청 사이버테러대응센터의 인력 및 예산의 측면을 꼬집은 바 있다. 절반 이상의 인력이 보안전문가가 아니기 때문에 해킹 등에 적절한 대응을 하지 못하고 있으며, 2004년도 예산의 경우는 미국 관련기관의 5%에 불과한 19억원에 그치고 있다는 것이다.

련된 전문지식이 부족하거나, 적절한 교육을 통해 수사기법을 수시로 향상시킬 수 있는 체제가 이루어지지 못해 최근의 급변하는 사이버 범죄에 대한 수사를 제대로 하기가 사실상 힘든 상황이다. 그리고 경찰서 수사2계는 전통적으로 기획사건을 중심으로 수사를 해왔기 때문에 사이버범죄에 대한 중요성은 반감될 수밖에 없으며, 일련의 사건들에서 나타나는 범죄의 강력화 경향에 따라 수사조직이 강력범죄 위주로 움직이고 있어 사이버범죄의 대응능력이 강화되지 못하고 있다.[120] 따라서 현재의 일선 경찰서 수사2계는 단순히 고소, 고발, 진정 등의 창구로서의 역할에 그치고 있는 실정이다.

아래의 <그림 5-1>은 경찰청 사이버테러대응센터 및 지방경찰청 사이버수사대, 그리고 일선 경찰서의 사이버범죄 대응체계를 나타낸 것이다.[121]

<그림 5-1> 경찰의 사이버범죄 대응체계



120) 그러나 최근 경찰의 수사대응능력 강화를 위해 일선 경찰서 조직을 개편함에 있어 시범 경찰서로 선정되어 관심을 모았던 일산경찰서의 경우 죄종별 수사조직체제로 개편하면서 사이버범죄에 대한 부분은 업급하지 않고 있다. 일산경찰서는 수사2계를 각종 비리사건과 환경, 시위, 사회적 이목을 끌 수 있는 사건 등의 전담 체제로 전문화했으며, 형사과의 경우 강력사건만을 전담하도록 했다. 이러한 수사전문화 방안에 있어서의 개편은 일련의 사건에서 나타나는 강력범죄에 대응하기 위한 조치로 인식되나, 사이버범죄의 중요성은 상대적으로 반감되는 측면을 낳고 있다(연합뉴스, 2004년 7월 11일자).

121) 경찰청 내부문서 참조.

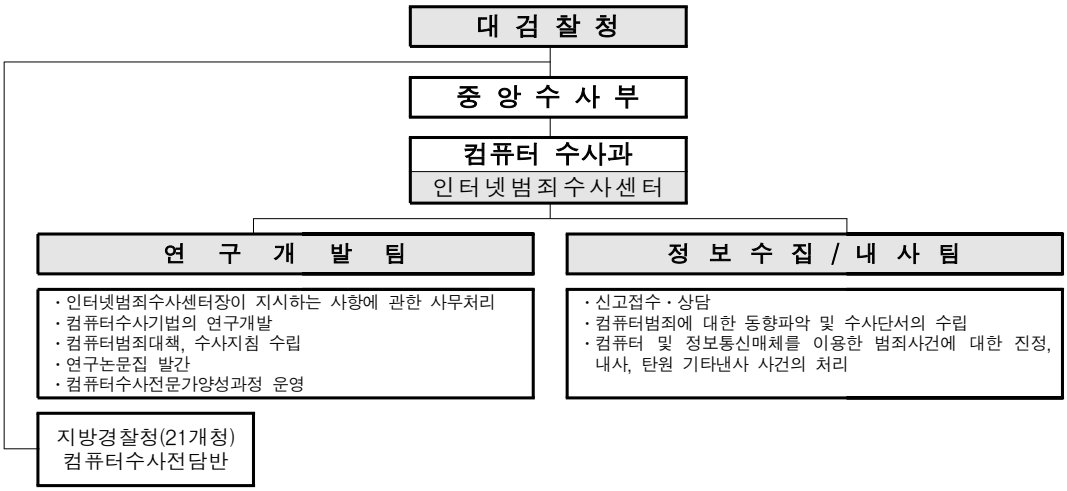
한편 사이버범죄 수사인력의 전문화를 위해 마련된 경찰청의 사이버범죄 수사기법 교육으로는 경찰수사보안연수소에서 행하여지는 '사이버범죄수사과정'(고급과 중급, 연 240명)이 있다. 그러나 본 과정은 1회당 40명을 대상으로 년 4회 실시하며 교육기간도 2주에 불과해 실질적인 효과를 거두지 못하고 있다. 그리고 소수 정예화 프로그램으로 사이버수사의 첨단기술을 선도하는 요원을 양성하기 위하여 민간 전문교육기관에 1개월에서 5개월 정도의 장기 위탁교육을 시키고 있으며 연 20-30명의 인력이 교육을 받고 있지만, 전문성을 확보하기에는 미흡한 교육기간이다. 또한 외국의 첨단수사기법을 배우기 위한 해외 위탁 교육프로그램도 있으나 그 기간이 1-2주 내외에 그쳐 실질적인 효과를 거두기 어려운 실정이다.

2. 검찰의 전문성 부족과 구조적 모순

검찰의 경우 대검찰청에 컴퓨터수사과를 그리고 각 지방검찰청에 컴퓨터수사부(반)를 설치하여 사이버범죄를 전담수사하고 있다.[122] 2001년 2월 대검찰청 컴퓨터수사과와 서울지검의 컴퓨터수사부내에 설치한 '인터넷범죄수사센터'는 사이버 스페이스 순찰 및 단속의 성격을 가진 조직으로 검찰의 사이버범죄 대응에 있어 중요한 역할을 담당하고 있다.

아래의 <그림 5-2>는 대검찰청 인터넷범죄수사센터의 조직과 관장업무를 나타낸 것이다.

<그림 5-2> 대검찰청 인터넷범죄수사센터의 조직과 관장 업무



122) http://www.dci.sppo.go.kr.

서울지방검찰청의 경우는 2001년 2월부터 '서울지검인터넷범죄수사센터'를 설치·운영하고 있다. 또한 전국 20개 지방검찰청 및 지청에 '컴퓨터수사반'을 설치하여 운영하고 있으며, 전국 22개청에 컴퓨터 수사검사 27명과 컴퓨터 수사전담요원 73명을 배치하고 있다(이경훈, 2002).

검찰은 사이버범죄에 대응하기 위한 전문화교육의 일환으로 2001년 1월부터 6개월 과정의 '컴퓨터수사전문가양성과정'을 대검찰청 인터넷범죄수사센터에 개설하여 수도권 검찰청의 컴퓨터수사요원을 대상으로 보안업체 전문강사를 초빙하여 유닉스 등 운영체제와 해킹수사에 관한 전문교육을 실시하고 있다.

그러나 중요한 점은 주로 기소 업무와 일반범죄 수사 영역에서 활동하던 검사 및 검찰수사요원들이 사이버범죄에 대하여 얼마나 전문적인 지식을 습득하고 전문적인 수사활동을 전개해 나갈 수 있는지가 의문이며, 교육 내용자체가 해킹 등의 특정한 유형에 국한된 사이버범죄에 대한 사후진압적인 측면이 강해 사이버범죄를 사전예방 하는 등의 종합적 대응과는 거리가 멀다는 것이다.

또한 검찰의 사이버범죄 대응체제는 경찰의 그것과 중복되기 때문에 오히려 형사사법적 자원의 낭비를 초래할 수 있다. 이점은 공소제기 및 유지라는 검찰본연의 임무와 관련하여 생각해 볼 수 있다. 사이버범죄에 대한 대응은 단순히 수사와 진압의 측면이 아닌 사전 예방적 기능을 중시해야 하며, 양대 기관에서 공히 같은 역할을 수행하는 조직을 두고 있다는 것은 극히 비효율적인 일이기 때문이다. 예컨대, 대검찰청 인터넷범죄수사센터의 경우 사이버상의 예방순찰과 연구개발 등이 주된 업무로 경찰청 사이버테러대응센터 수사2계 또는 기법개발실과 그 기능이 중복되고 있는 실정이다.

이와 같은 관점에서 사이버범죄에 대한 보다 효과적인 대응을 위해서는 검찰 사이버수사 인력의 일정 부분을 경찰로 옮겨 사전 예방적 활동과 수사 기능을 모두 경찰에서 수행토록 하고, 검찰에서는 필요한 최소한의 요원으로 사이버범죄 피의자에 대한 보강수사와 공소제기 및 유지의 업무를 담당하는 체제를 고려해 볼 수도 있을 것이다.

제4절 총괄적 조정기관의 부재

현재 우리나라의 사이버범죄에 대한 대응에 있어서 가장 큰 문제점 중의 하나는 사이버범죄를 사전에 예방하고, 일단 사이버범죄가 발생하였을 경우 신속하게 대응할 수 있는 총괄적 조정기능을 가진 전담 기관이나 조직이 부재하다는 것이다. 물론 지난 2004년 2월 국가정보원이 창설한 국가사이버안전센터(NCSC)가 그와 같은 총괄적 기능을 수행하고자 창설되었지만, 이는 주로 해킹·컴퓨터바이러스 유포 등 사이버테러 공격으로부터 국가의 전산망을 보호할 목적에서 설립된 조직이기 때문에 소위 '일반사이버범죄'와는 거리가 멀다고 할 수 있다.

그동안 우리나라의 사이버테러 및 공격에 대한 대응은 국가정보원, 정보통신부 및 산하기관, 행정자치부, 국방부, 경찰, 검찰, 정보보안사업자 등 다양한 기관들에 의해 중구난방으로 이루어져 왔으나, 다행이 금번 국가사이버안전센터의 설립으로 체계화를 위한 토대가 마련되었다고 하겠다. 그러나 문제가 되는 부분은 정보보안체계에 대한 범죄 외의 일반 사이버범죄에 대한 대응체계가 지나치게 분산되고 세분화되어 있으며, 총괄적인 조정기능을 수행할 수 있는 전담기관이 아직까지 마련되어 있지 않다는 점이다. 전술한 바와 같이 사이버범죄에 대한 신고처리체계의 분산, 청소년유해매체물에 대한 이중규제, 유관기관별 협조체제의 미비 등의 문제도 모두 이러한 총괄적 조정기능을 가진 전담기관이 부재하기 때문에 발생하는 문제점이다.

한편 이러한 상황에서 최근 불거져 나온 정보통신부의 사이버범죄에 대한 수사권요구는 그렇지 않아도 대응주체의 지나친 분화로 자원이 비효율적으로 운용되고, 업무가 중복되며, 결과적으로 원활한 대응을 어렵게 하는 현실을 더욱 가중시킬 수 있는 발상이라 귀추가 주목된다. 정보통신부는 지난 2004년 3월 사이버명예훼손, 해킹, 바이러스 유포, 음란물 유포, 스팸메일 등 신종첨단 컴퓨터범죄에 대해 정통부가 직접 수사할 수 있도록 '사법경찰관리의직무를행한자와그직무범위에관한법'을 개정해줄 것을 법무부에 요청하였다. 만약 이 법률이 그렇게 개정된다면 정보통신부는 사이버범죄의 80-90%를 수사기관에 별도로 고발조치하지 않고 단독으로 강제수사 할 수 있게 된다.[123] 정보통신부는 급

123) 한국일보, 2004년 5월 7일자.

증하는 사이버공격에 효과적으로 대응하기 위해서는 전문성 있는 정통부 직원들에게 사법경찰권을 부여하는 것이 효율적이라는 논리로서 위와 같은 요청을 하였다.[124]

그러나 이와 같은 정보통신부의 요청은 여러 가지 문제점을 내포하고 있다. 그것은 첫째, 정보통신망법상 첨단범죄, 신종컴퓨터범죄, 재래적인 인터넷범죄 등을 구별하기가 어려워지는 현실에서 기관별 대응 범죄유형을 분리하는 것 자체가 무리라는 것이다.[125] 예를 들어, 컴퓨터를 이용한 사기의 경우 인터넷을 이용하여 범죄가 저질러진다는 특징은 있지만, 사기의 기법과 수단은 전통적 사기와 일치하는 양상이며, 청소년성매매의 경우도 인터넷은 하나의 매개체가 될 뿐 직접적인 위법행위는 오프라인에서 이루어지기 때문이다. 둘째, 수사권이 정보통신부에까지 확대되는 것은 자칫 경찰권이 확대되어 경찰국가화 될 우려가 있다는 것이다. 이는 작은 정부라는 정부의 정책기조에도 부합되지 않는 논리이며, 경찰권을 축소하는 현대국가의 개념에도 맞지 않는 것이다. 셋째, 심각한 인권침해를 조장할 우려가 있다. 많은 시민단체에서도 주장하는 바와 같이 민간인인 정보통신부 직원이 수사권을 행사할 경우 심각한 인권침해는 물론 개인정보유출 등 더 큰 문제점을 야기할 수 있다. 넷째, 자원의 비효율적 운용이다. 현재도 사이버범죄에 대한 수사 및 대응체계가 경찰과 검찰로 양분되어 있어 인력과 예산의 낭비가 심한 상황에서 정보통신부에까지 수사권을 준다면 그것은 비효율적인 중복투자에 지나지 않는 것이다 (총괄적 조정기관에 관한 보다 구체적 사항은 제7장 결론부에서 다시 논의하기로 한다).

124) 정보통신부는 현재 소프트웨어 불법 복제 등 제한된 분야에서 사법경찰권을 행사하고 있다.
125) 연합뉴스, 2004년 5월 8일자.

제6장 인터넷을 이용한 청소년범죄에 대한 효율적 대처방안

제1절 규제법규 및 제도의 보완·정비

1. 사이버범죄 관련 특별법의 제정

사이버범죄와 관련된 법률은 형법과 성폭력범죄의처벌및피해자보호등에관한법률, 청소년보호법, 청소년의성보호에관한법률 등의 형사특별법, 그리고 정보화촉진기본법, 전기통신기본법, 전기통신사업법, 정보통신망이용촉진및정보보호등에관한법률 등의 정보통신 관련 법률을 포함하여 모두 25여 가지에 이르며, 세부 시행령까지 포함하면 실로 다양한 법률이 사이버범죄와 관련되어 있다고 할 수 있다. 그래서 특정 사이버범죄 유형과 관련된 법률도 다양하고 그 결과 범죄의 규정 또는 구성요건이 불명확해지고 이에 따라 범죄에 대한 억제효과도 기대하기 어려운 실정이다. 따라서 갈수록 심각해지고 새로워지고 다양화되는 사이버범죄에 보다 효과적으로 대처하기 위해서는 기존의 법들을 개정하거나 땜질식 보완을 하기 보다는 가칭 '사이버범죄특별법'과 같은 보다 종합적인 특별법의 제정이 필요하다고 본다.

사실 2001년 1월 16일 전문 개정된 정보통신망이용촉진및정보보호등에관한법률이 그와 같은 사이버범죄에 관한 기본법적 성격을 갖고 출발하였지만, 이 역시 기존의 정보통신망 이용촉진 등에 관한 사항에 정보통신서비스 이용자의 개인정보보호제도에 관한 사항을 추가한 것에 불과하다. 또한 정보통신부는 최근에도 사이버범죄에 대한 보다 효과적인 대처를 위해 정보통신망법 개정안을 마련하였지만, 이 역시 포괄적인 특별법적 기능을 가진 법률안이 아닌 특정 세부범죄 유형에 대한 미봉책에 불과한 것이라 할 수 있다. 이와 같은 형태로 이루어지는 각 부처와 관련된 영역에서의 소규모 법률개정은 기관별 관장 사항 및 처벌규정의 상이함으로 동일한 법익을 침해하는 행위에 대해 여러 처벌법규가 중복 적용되고, 같은 행위를 규제하는데 있어서도 서로 다른 용어를 사용하며, 처벌규정 또한 상이하기 때문에 사이버 범죄에 대하여 효과적인 대응을 가로막고 처벌

의 신속성과 형평성을 저해하는 요인이 되고 있는 것이다.

따라서 이러한 폐단을 수정하기 위해서는 사이버범죄를 총괄할 수 있는 가칭 '사이버범죄특별법'의 제정이 필요한바, 동 법률은 대부분의 사이버범죄 유형들을 포괄함과 동시에 관련범죄에 있어서의 적정한 수사절차를 정하여 무리한 수사로 인한 인권침해의 소지를 막아야 할 것이다. 또한 실체적 구성요건과 압수, 수색 등의 절차와 방법 등을 총 망라하는 법률로써 제정되어야 할 것이다.

2. 정보통신사업자에 대한 직접적 규제법률 마련

앞서 언급한 바와 같이 사이버공간에서의 불건전정보의 3주체는 정보통신사업자(ISP), 정보제공자(information provider, IP), 인터넷이용자(end-user)이다. 그런데 이러한 3주체에 대하여 그동안 정보통신 관련 국가기관과 사법당국은 불건전유해매체물과 관련하여 정보통신사업자(ISP)보다는 정보제공자(information Provider, IP)에게 더 주목하여 이들에 대한 수사와 검거에 집중하여 왔던 것이 사실이다.

이것은 정보통신사업자들에게는 원칙적으로 자율성이 존중되어야 한다는 선진국의 사례와 법률적 규정을 바탕으로 형성된 논리이지만, 최근에는 일부 정보통신사업자들이 스스로의 의무를 방기한 채 불건전유해매체물을 오히려 방조하는 행태를 보이고 있기 때문에 문제가 되는 것이다.

현재 관계당국은 인터넷 서비스제공업자들에 대하여 자율정화라는 명목으로 자율성을 부여하고 직접적인 규제법률의 적용에 소극적인 자세를 보이고 있다. 그러나 앞서 제5장에서 지적한 바와 같이, 영국과 독일 등에서는 원칙적으로 정보통신사업자에게 자율성을 부여하고, 불건전유해매체물의 제공자에게 일차적인 책임을 묻지만, 정보통신사업자가 불건전유해매체물에 대한 관리, 감독 및 수정 조치를 소홀히 할 경우에는 단호한 조치를 취하도록 규정하고 있다.

독일의 경우 구체적인 입법 규정으로 1997년 '정보및커뮤니케이션서비스법: 정보 및 커뮤니케이션 서비스의 일반조건을 성립시키는 연방법'을 제정하여 ISP는 직접 작성한 컨텐츠에 대하여 책임을 질뿐만 아니라, 유해컨텐츠의 게시여부에 대하여 알고 있고, 유해컨텐츠의 유통을 방지하기 위한 기술을 가지고 있음에도 불구하고 그것을 방치했을

경우 ISP에게 책임을 지우고 있다. 또한 아동에게 유해한 정보에 대하여 동법은 “컨텐츠제공자는 ‘... 연방심사위원회’가 분류한 청년에게 유해한 출판물이 아동에게 배급되지 않도록 하여야 한다” 그리고 “(유해한) 컨텐츠의 유통을 제한하기 위한 공학기술을 채택하여야 하며, 이를 게을리 하는 자는 제재를 받는다” 라고 규정하고 있다.[126]

하지만 반대로 미국의 통신품위법(Communication Decency Act of 1996)의 ‘선한 사마라아인’ 조항에서는 구체적으로 ① 제230조 (c) (1)에서 “쌍방향 컴퓨터서비스 제공자나 이용자는 다른 정보·콘텐츠 제공자가 제공한 정보에 대하여 그 발행자 또는 송신자적 입장에 있는 것으로 취급되지 아니 한다”; ② 제230조 (c) (2) (A): “쌍방향 컴퓨터서비스 제공자나 이용자는 음란하거나 외설적인 정보, 선정적이거나 비속한 정보 또는 과도한 폭력성을 내포하거나 타인을 괴롭히는 내용의 정보 기타 문제 있는 정보에의 접근을 제한하기 위하여 선의를 가지고 행한 자발적인 조치를 이유로 법적인 책임을 지지 아니 한다”; ③ 제230조 (c) (3): “위 서비스제공자에 대하여 본 조항에 반하는 주법, 기타 지방공공단체가 제정한 법령을 근거로 소송을 제기하거나 법적 책임을 부과하는 것은 허용되지 않는다”라고 규정하고 있다. 이러한 통신품위법(Communication Decency Act of 1996)을 근거로 美 연방 제4항소법원은 Zeran vs AOL 사건[127]에서 정보통신

126) 정완, “사이버공간에서의 규제와 자율”, 형사정책연구, 제12권, 제3호, 한국형사정책연구원, 2001, pp. 258~259.

127) Zeran vs AOL 판결은 다음과 같은 전개과정을 거쳐 성립된 것이다: 본 사건은 1995년 4월 25일 익명의 사람이 America Online, Inc(AOL)의 게시판에 "Naughty Oklahoma T-Shirts"를 광고하는 메시지를 투고하면서 시작되었다. 그 투고는 1995년 4월 19일 발생한 오클라마시의 Alfred P. Murrah 연방빌딩 폭발에 관한 불건전한 슬로건이 적힌 셔츠 판매를 알리는 것이었다. 그런데, 이 게시판에 적힌 내용은 셔츠를 구입하고자 하는 사람은 워싱턴주 시애틀에 있는 Kenneth M. Zera의 자택전화번호의 "Ken"에게 전화를 걸라는 것이었다. 그 결과 Zeran에게 많은 양의 전화가 걸려왔는데, 그것은 주로 분노에 가득찬 내용이었고, 그 중에는 살해하겠다고 위협하는 내용도 들어있었다. 하지만, Zeran은 자신의 전화번호를 변경할 수 없었다. 그 이유는 사업상 집에서 일반인의 전화를 받을 필요가 있었기 때문이다. 그날 늦게 Zeran은 AOL에 연락하여 자신의 어려움을 호소하였으나, AOL은 Zeran에게 그 투고를 제거할 수 없다고 설명하였다. 양당사자는 언제 AOL이 게시판에서 투고를 제거할 것인지를 두고 다툼을 벌이게 된다. 다음날인 4월 26일에도 익명의 사람이 오클라마시 폭파사건에 관한 새로운 불건전한 슬로건이 게재된 셔츠를 다시 광고하는 메시지를 투고하였다. 이번에도 구매하고 싶은 사람은 Zeran의 전화번호에 걸어 "Ken"을 호출하라는 것이었는데, 그 후 협박적인 전화가 더욱 격화되었다. 4일간에 걸쳐 지속적으로 불상자는 AOL의 게시판에 메시지의 투고를 계속하였다. 이 기간 중에 Zeran은 반복하여 AOL에 전화하였으나, AOL로부터 그 메시지를 투고한 개인의 계좌를 물을 수 없도록 폐쇄 되어 있다는 내용을 통보받았다. Zeran은 또한 이 사건을 시애틀에 있는 FBI에 보고하였다. 4월 30

사업자에게 완전한 면책을 인정한바 있다.[128]

결국 독일과 미국의 입법례는 '법익보호 및 사이버범죄의 방지'라는 측면과 '표현의 자유'가 상충하는 부분이라 할 수 있다. 한국의 경우에는 현재 '표현의 자유'를 우선시하여 정보통신사업자들에게 자율규제 권한을 부여하여 불건전유해매체물에 대한 규제를 하고 있다. 그러나 사이버범죄가 급증하고 있고 청소년들이 불건전유해매체물에 거의 무방비로 노출되어 있는 현실에서는 표현의 자유를 과도하게 해치지 않는 범위내에서 독일과 같은 직접적 규제가 필요하다고 본다. 다시 말해서, 자율규제를 실시하되, 이와 병행하여 자율규제가 드러내는 한계점이 명확해진다면 집적적인 규제를 가할 수 있는 법적·제도적 장치도 마련해 볼 필요가 있다는 것이다.

3. 사이버범죄 연계 법률의 정비

사이버범죄는 관련된 법률이 상당히 많은 것과 동시에 범죄 자체가 온라인 혹은 오프라인을 넘나드는 경우가 많아 사이버범죄자를 처벌함에 있어 일반 법률과 연계되는 경

일까지 Zeran은 2분에 1회 정도 매도하는 내용의 전화를 받았다. 그 사이에 오클라마시 라디오 방송국인 KRXO의 아나운서는 최초로 AOL에 투고된 내용을 1통을 전달받아 5월 1일 메시지의 내용을 방송하고, Zeran의 전화번호가 "Ken"이라고 하면서 청취자에게 그 번호에 전화할 것을 촉구하였다. 이 방송 후 Zeran은 끊임없는 살해위협, 기타 두려운 전화를 오클라마시 주민으로부터 받았다. 그 후 수일간에 걸쳐 Zeran은 KRXO 및 AOL의 사원과 통화하였다. 그는 또한 경찰에 신고하여 경찰이 가택감시를 하기도 하였다. 이후 지속적으로 5월 14일까지 오클라마시의 신문이 메시지의 광고가 악의에 찬 것이라는 내용의 폭로기사를 게재하였고, KRXO가 사죄의 방송을 한 후 Zeran의 자택으로 걸려오는 전화의 수는 1일 15회 정도로 감소하였다. 하지만 Zeran은 이에 대하여 1996년 1월4일 오클라마주 서부지구 연방지방법원에 KRXO을 상대로 소를 제기하였다. * 사건의 쟁점 - 이 사건에서 쟁점이 된 것은 CDA(Communication Decency Act of 1996) 제230조가 정보발행자(publisher)의 면책을 인정하는 규정은 두고 있으나, 배포자(distributor)로서의 책임을 면제한다는 명문규정이 없으므로 원고가 주장하는 것처럼 피고가 배포자로서의 책임을 지는가 하는 것이었다. 이 사건의 판결은 "선한 사마리아인 조항"이 포함된 CDA가 발효한 이후에 미국연방 제4항소법원이 Zeran v. AOL사건에서 "선한 사마리아인조항"의 '발행자'는 불법행위법에서 말하는 '발행자' 뿐만 아니라 '배포자'도 포함하는 개념이라고 하여 "쌍방향 컴퓨터서비스"를 제공하는 네트워크의 정보중개자는 이 조항에 의하여 '발행자'로도 '배포자'로도 인정되지 않아 명예훼손에 관한 불법행위 책임으로부터 면책된다는 판단을 내린 사건이다 (http://www.kolis/DNlawinfo/casestudy/read.html).

128) 서보학, "인터넷상의 정보유포와 형사책임", 형사정책연구, 제12권, 제3호, 한국형사정책연구원, 2001, pp. 334-34.

우가 많다. 앞서 언급한 바와 같이 주민등록법, 저작권법 등이 대표적인 관련 법규인데, 이러한 법률이 상호 연계되어 정비되어야만 사이버범죄에 대한 보다 효과적인 대응이 가능할 것이다.

특히 주민등록법상의 개인정보 도용에 있어서 인터넷을 통해 개인정보를 도용해 거래를 하더라도 피도용자에게 직접적인 경제적 피해가 없으면 처벌할 수 없다는 점과 '재산상의 이익'을 목적으로 도용되는 경우에만 처벌이 가능하기 때문에[129] 인터넷상의 주민등록번호 생성기를 통해 만들어진 주민등록번호가 재산상의 이익 외의 목적으로 사용될 때에는 처벌이 어렵다는 점은 반드시 수정될 필요가 있다. 즉 도용자체만으로도 명확한 처벌이 필요한 것이다.

그리고 '반의사불벌죄'의 요소가 포함되는 친고제 관련 법률의 개정 역시 필요하다. 즉 현행 컴퓨터프로그램보호법과 저작권법은 친고죄에 해당해 저작권자의 고소가 없이는 처벌이 불가능한 법률이다. 따라서 관계기관이 불법복제된 소프트웨어를 단속하더라도 처벌을 위해서는 저작권자의 고소를 기다려야 하는 실정이며, 직접적인 고소가 없을 경우 처벌이 불가능한 상황이다.

그러므로 사이버범죄의 효과적인 예방을 위해서는 온라인상에서 직접적으로 이루어지는 사이버범죄 외에 간접적으로 연계된 범죄행위에 대해서도 정확히 처벌할 수 있도록 관련 규정을 조속히 정비해야 할 것이다.

4. 사이버범죄 미수범에 대한 처벌 강화

사이버범죄는 이미 범죄를 저질러 범죄자로 양산된 경우도 많지만, 사전에 발각되는 등의 원인으로 미수범에 그치는 경우도 많기 때문에 이들에 대한 처리문제도 간과할 수 없는 부분이다. 특히 미수범의 경우 범행의 성공을 위해 재차 불법적인 행위를 저지를 위험이 있기 때문에 사전 대응이 절실하다고 할 수 있다.

---

129) 지난 2001년 1월 26일 개정된 주민등록법 제21조9항에는 '다른 사람의 주민등록번호를 자기 또는 다른 사람의 재물이나 재산상의 이익을 위해 사용한 자'에 한해 3년 이하 징역이나 1000만원 이하의 벌금에 처하도록 규정돼있다. 따라서 인터넷 사이트에 가입하거나 서비스를 이용해도 '공짜'인 경우 이 규정을 적용할 수 없다는 것이다.

2004년 1월 29일 개정된 정보통신망법 제63조에서는 사이버범죄에 대한 형사처벌의 범위를 확대하여 사이버범죄 중 해킹과 관련한 미수범에 대해서는 3년 이하의 징역이나 3,000만원 이하의 벌금에 처하도록 규정하고 있다.[130] 하지만 정보통신망법은 해킹 외에 기타 사이버범죄 미수범에 대해서는 처벌조항을 두고 있지 않아 기타 미수범에게는 처벌근거를 제시하지 못하고 있다. 그래서 직접적으로 범죄행위가 성립되지 않아 미수에 그치는 전자상거래, 바이러스 유포, 사이버 성관련 범죄 등에 대한 미수범 처리는 제대로 이루어지지 못하고 있는 실정이다. 그러므로 현재의 정보통신망법을 개정하여 사이버범죄 미수범에 대한 포괄적인 처벌규정을 마련함과 동시에 사이버범죄 실행자에게는 보다 엄격한 처벌을 가하고, 미수범의 경우 차후의 사이버범죄를 예방할 수 있도록 사회내처우를 강화할 필요가 있다고 하겠다.

현재 한국정보보호진흥원에서는 서울보호관찰소 남부지원과의 협력하에 사이버범죄로 기소되어 보호관찰 처분을 받은 범죄자를 대상으로 다양한 사회내처우를 실시하고 있으며, 이에 대한 성과도 긍정적으로 나타나고 있다.[131] 특히 청소년의 경우 성인범과는 처벌을 달리하여 징역이나 벌금 등의 공식적 처벌 보다는 보호관찰이나 사회봉사제도, 그리고 수강명령 등을 활용하여 사이버범죄에 대한 경각심을 일깨워줌과 동시에 재범을 방지할 수 있도록 하는 것이 보다 효과적인 대응방안일 것이다.

5. 사이버범죄 신고처리체제의 일원화

사이버범죄 피해의 경우 신고기관 연락처, 신고방법, 처리절차 등이 상당히 세분화되어 있고, 그에 대한 홍보도 제대로 되지 않아 피해를 입은 사람들이 제대로 피해 구제

130) 2004년 1월 29일 개정된 정보통신망법에서 미수범 관련 부분은 제63조로서 내용은 다음과 같다. 제63조 (벌칙) ① 다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 1. 제48조제1항의 규정을 위반하여 정보통신망에 침입한 자, 2. 제57조의 규정을 위반하여 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적외에 이를 사용한 자, ② 제1항제1호의 미수범은 처벌한다.<신설 2004. 1. 29.>

131) 한국정보보호진흥원에서는 서울보호관찰소 남부지소와 협력하여 인터넷중독성검사 지원을 시작으로 시범사업을 추진하고 있으며 사회봉사명령대상자를 중고PC 정비 및 사랑의 PC보내기 사업에 투입하여 정보소외계층 대상 정보격차해소사업에 동참시키고 있다(http://cybercrime.kado.or.kr/cyb/cyb_aft01.asp).

를 받지 못하는 사례가 많다. 특히 피해사례에 따라 경찰, 정보통신윤리위원회, 한국정보보호센터, 한국소비자보호원 등 다양한 기관으로 신고처리체제가 분산되어 있는 점은 신속하고 정확한 사이버범죄 처리를 가장 크게 저해하고 있는 부분이다.

그러므로 전체적인 사이버범죄를 포괄할 수 있는 신고 및 처리체계의 일원화가 필요하다. 즉 화재신고의 119나 범죄신고의 112처럼 사이버범죄를 당한 사례가 발생한 경우 지체 없이 신고할 수 있는 일원화된 신고처리체계가 그것이다. 물론 사이버범죄가 가지는 다양성과 광범위성 때문에 경찰 혹은 정보통신관련 기관, 상거래 및 소비자 피해 관련 기관이 분화될 수밖에 없다는 논리도 가능하나 이것은 피해자의 입장을 고려하지 않은 지나친 행정편의주의적 사고에 지나지 않는다.

신고처리체계 일원화의 구체적인 방안으로는 여러 번호로 나뉘어 있는 신고번호를 하나로(예를 들어 118) 통일한 뒤 음성안내시스템을 통하여 피해유형별로 피해자가 세부코드를 눌러 신고할 수 있는 체계의 구축이다. 이와 같은 체계에는 주로 해킹 및 바이러스 신고만을 담당하고 있는 현재의 '사이버 118', 불건전정보의 신고만을 담당하는 '인터넷 119'와는 달리 전자상거래, 개인정보침해, 성관련 범죄, 사기범죄 등 모든 유형의 사이버범죄를 총괄할 수 있는 것이어야 한다.

그런데 중요한 점은 이러한 총괄적 신고체계를 담당할 기관을 어디로 정하느냐의 문제인바, 이는 각 부처별 이해관계에 따라 쉽게 논의될 수 있는 사안은 아니다. 하지만 정보통신관련 기관과 소비자관련 기관은 수사권을 소유하고 있는 기관이 아니며 처벌권한도 극히 제한되어 있기 때문에 사이버범죄에 대한 직접적인 수사를 담당하고 있는 경찰의 주도아래 관련 기관이 공동 참여하는 형식으로 동 체제가 구축되어야만 가장 효율적인 시스템으로 운용될 수 있을 것이다.

6. 청소년유해매체물 제도 강화 및 이중규제의 개선

청소년유해매체물제도는 청소년들에게 유해하다고 판단되는 정보에 대하여 청소년보호법에 의해 '청소년유해매체물'로 결정하여 청소년유해매체물 표시와 함께 청소년들에게 접근을 금지 하도록 하는 제도이다.[132] 본 제도는 음성매체물[133]과 문자영상매체물[134]을 대상으로 이루어지며, 이러한 매체물에 대하여 청소년유해매체물로 표시하여 청

소년의 접근을 원천적으로 차단하는 것이다.

그런데 이러한 청소년유해매체물제도에 대하여 일부에서는 인터넷상에서의 '표현의 자유'를 침해한다고 하여 제도 자체에 대한 회의적인 시각을 드러내고 있다. 하지만 정보통신윤리위원회의 '2003년 정보통신윤리 관련 종합통계'에 따르면 국내 인터넷상에 청소년들에게 무분별하게 노출되는 음란 정보의 경우, 그 증가세가 두드러져 지난 2002년에 18,941건이었던 심의 건수가 49,482건으로 크게 뛴 것으로 나타났다.

유해매체물로부터 청소년을 보호하기 위하여 다각도로 예방 노력이 확대되고 있는 현실에서의 이러한 증가추세는 불건전한 정보의 유통을 근본적으로 감소시킬 대응책을 절실히 요구하고 있는 것이다. 특히 최근에는 신종 수법을 동원한 불법 사이트가 판을 치면서 사전감시와 사후제재만으로는 한계가 뚜렷하게 나타나고 있다.

따라서 일각에서 제기하고 있는 청소년유해매체물제도에 대한 회의적 시각 보다는 오히려 청소년유해매체물에 대한 심의기준을 강화하여 유해매체물이 청소년들에게 유입될 수 있는 경로를 보다 강도 높게 차단해야 할 필요가 있는 것이다. 또한 관련 처벌법규를 강화하여 변칙적 방법으로 청소년에게 유해매체물을 제공하는 제공자에 대해서는 강력한 처벌이 따라야 할 것이다.

한편 온라인 게임 '리니지'와 관련하여 대두된 문화관광부의 '영상물등급심의위원회'와 정보통신부의 '정보통신윤리위원회'의 게임 및 영상물과 관련한 청소년유해매체물에 대한 이중규제는 하나의 매체가 두개의 법률, 두개의 심의기관에 의해 규제되는 결과를 초래하는 것이다.

이러한 현실에서는 18세, 19세라는 연령 차이를 악용해 유해매체물이 청소년들에게 보다 손쉽게 유입될 수 있으며, 심의기준의 혼선을 초래하여 제대로 된 유해매체물 지정이

---

132) 관련 법규로는 【전기통신사업법】제53조, 제53조 제2항 및 동법시행령 제16조 내지 제16조 제3항, 【정보통신망이용촉진및정보보호등에관한법률】 제42조, 제64조 및 동법시행령 제21조, 【청소년보호법】 제8조, 제14조, 제17조, 제22조, 제50조, 제51조 및 동법시행령 제13조, 제14조, 제16조 등이다.

133) 음성매체물에 대해서는 사전에 음성으로 "이 정보내용은 청소년유해매체물로서 정보통신망이용촉진및정보보호등에관한법률 및 청소년보호법의 규정에 의하여 19세 미만의 청소년이 이용할 수 없습니다"라고 음성표시를 한다.

134) 문자영상매체물에 대해서는 "이 정보내용은 청소년유해매체물로서 정보통신망이용촉진및정보보호등에관한법률 및 청소년보호법의 규정에 의하여 19세 미만의 청소년이 이용할 수 없습니다" 라고 표시함과 동시에 컬러매체의 경우 적색 테두리의 원형마크 안에 '19'라는 숫자를 흑색으로 표시하여야 한다.

어려워질 수밖에 없다. 따라서 궁극적으로는 '영상물등급위원회'나 '정보통신윤리위원회' 두 가지 심의창구를 하나로 단일화하는 것이 필요하다고 본다.

7. 사이버범죄 피해자에 대한 구제 강화

사이버범죄 발생량의 증가에 비례하여 사이버범죄 피해자 역시 증가하고 있다. 그러나 사이버범죄 피해자에 대한 전담 구제기구가 없으며, 분쟁해결제도도 미비한 상황에서 피해자에 대한 구제는 극히 제한적으로 이루어질 수밖에 없다. 따라서 사이버범죄 피해자에 대한 구제를 강화하기 위해서는 구제를 돕기 위한 전담기구의 설치가 필요하며, 피해자들은 그러한 전담기구를 통하여 유·무형의 보상을 받을 수 있어야 할 것이다.

그리고 정보통신윤리위원회에서 설치한 '사이버명예훼손·성폭력분쟁조정센터'와 한국전자거래진흥원 산하 '전자거래분쟁조정위원회' 등의 조정 기능을 한층 강화하여 피해자의 보상이 신속하게 이루어지고, 가해자와 피해자 사이의 원만한 합의를 이룰 수 있도록 도와야 할 것이다. 또한 명예훼손과 성폭력, 전자상거래에 국한되어 설치된 조정위원회를 각종 사이버범죄 유형별로 세분화하여 강화하는 방안도 필요하다.

한편 사이버범죄는 국내에서만 일어나는 범죄가 아니라 세계 각지에서 일어날 수 있는 광역성을 가진 범죄이기 때문에 피해자 구제를 위한 국제적인 협조체제를 강화하고, UNESCO 등 국제기구를 통한 사이버범죄 피해자 구제에도 힘을 쏟아야 할 것이다.

8. 기타 제도의 도입 및 개선

1) 인터넷 내용등급제의 강화

인터넷 내용등급제는 인터넷을 통하여 유통되는 정보가 청소년에게 유해한지를 선별하여 여과할 수 있는 장치로서 정보이용자의 의도와는 관계없이 불건전 정보에 접촉될 수 있는 여지를 사전에 차단하는 제도이다. 인터넷 내용등급제는 음란(형법 제243조, 전기통신기본법 제48조의2, 청소년보호법 제10조), 불온(전기통신사업법 제53조, 전기통신사업법 시행령 제16조), 미풍양속(정보통신이용촉진에관한법률 제20조)등의 기준규정에

의하여 시행되고 있는 제도로서, 정보 이용자에게 인터넷 컨텐츠의 종류와 수준을 선택할 수 있는 권리를 부여하고자 시행되고 있다. 따라서 본 제도에서는 정보내용에 대하여 선정성, 폭력성, 언어 등의 일정한 범주별로 등급을 설정하게 되는 것이다.

인터넷 내용등급제는 세계적으로 활발히 시행되고 있는 제도이다. 물론 미국의 경우 대부분의 불법·유해 콘텐츠가 자국내에 존재하여 우리와 현실이 다르지만, 대부분의 불법·유해 콘텐츠가 국외에 존재하여 우리와 상황이 비슷한 일본과 유럽, 그리고 호주의 사례는 우리에게 많은 시사점을 주고 있다.

유럽에서는 정보통신관련 대기업 연합체인 ICRA(Internet Content Rating Association)가 실질적으로 등급제를 추진하고 있다. 2003년까지 약 14만개 사이트 또는 페이지에 등급을 부여하였으며 월 평균 4000여 사이트 또는 페이지에 추가로 등급이 부여되고 있다. 운영경비는 ICRA 회원사들이 연간 25,000달러의 회비를 납부해 충당하고 있다.

일본은 정보통신사업자단체 기구인 전자네트워크협의회(ENC)에서 등급제를 추진하고 있는데 ENC에는 정부기관과 민간기업의 연구원 등이 회원으로 참여하고 있다. 이 등급제는 학교 인터넷망이 주요 대상으로 화상인식 로봇을 이용, 매일 약 1000여개 사이트에 등급을 부여한다. ENC가 사업을 제안하고 정부가 자금을 지원하고 있다.

호주는 지난 99년 개정된 온라인서비스법을 통해 영화등급 방식에 의한 등급제(PG, M, MA, R, X 5등급)를 도입, 유통금지 등급을 받은 콘텐츠의 유통을 막고 있다. X등급이나 R등급을 받은 인터넷 콘텐츠는 청소년 접속제한 시스템을 마련해야 하고 호주 외의 다른 국가에서 호스팅 되는 인터넷 콘텐츠가 R이나 X로 분류되면 금지콘텐츠가 된다.[135]

우리나라도 현재 실시하고 있는 인터넷 내용등급제를 강화하여 영리목적의 정보제공자 중 청소년유해정보를 제공하는 경우에는 더욱 강력한 등급표시 의무를 부과해야하며, 등급조정위원회는 정보이용자와 정보통신서비스제공자, 감시단체 등의 신청을 받아 정보내용의 등급조정을 더욱 엄격하게 해야 할 것이다. 또한 등급표시의무대상자가 등급을 표시하지 않거나 악의로 허위의 등급을 표시한 경우에는 형사처벌을 포함하여 강력하게 처벌해야 할 것이다.

---

135) http://kin.naver.com/browse/db_detail.php?d1id=7&dir_id=701&docid=317741.

2) 청소년권장 사이트제도의 활성화

청소년권장사이트제도는 인터넷의 음란·폭력물 등 각종 불건전정보로부터 청소년을 보호하고 청소년의 건전한 인터넷 이용을 돕기 위해 마련한 것으로, 매달 유익한 정보를 제공하는 인터넷 사이트를 발굴하여 시상하는 것을 말한다.

본 제도는 정보통신윤리위원회가 자체적으로 인지하거나 홈페이지 '청소년권장사이트'로 일반인들이 추천한 사이트 중 청소년들에게 건전하고 유익한 정보를 제공하는 국내 사이트를 심사대상으로 3, 6, 9, 12월 각 분기별로 시상하고 있다. 특히 영리목적의 회원가입사이트의 경우 개인정보보호정책의 시행여부 및 아동 가입시 부모동의절차의 존재여부가 선정기준이 되어 청소년들의 무분별한 사이트 가입으로 인해 발생하는 부작용을 막고 있다.

청소년권장사이트제도는 인터넷 내용등급제와는 반대로 청소년에게 건전한 사이트를 소개하는 제도이기 때문에 활성화되어야 할 필요가 있다. 구체적으로 청소년권장사이트 지정 대상의 폭을 확대하고, 나아가 이렇게 선정된 사이트에 대해서는 금전적인 면 등의 실질적인 혜택이 주어질 수 있도록 하는 제도적 장치를 마련해 건전 사이트를 정보통신사업자 스스로가 활성화할 수 있는 동기부여를 해야 할 것이다.

3) 최소한의 인터넷게시판 실명제 실시

4) 옵트 인(opt-in)방식의 도입

스팸메일과 관련한 문제는 어제오늘의 일이 아닌 지속적으로 제기되어온 문제이다. 스팸메일과 관련하여 현재 우리나라는 정보통신망법 제50조 제1항을 통하여 '옵트 아웃(opt-out)'방식의 태도를 취하고 있으나, 정보통신부 등 관계 부처에서는 '옵트 인(opt-in)'방식의 도입을 골자로 하는 스팸메일 방지대책을 추진 중에 있다.

'옵트 아웃'이란 발신자의 권리를 중시하여 수신자가 수신거부 의사를 밝힌 경우 이외에는 광고성 정보를 전송할 수 있도록 허용하는 것으로 대표적인 실시국가는 미국이다. 반면에 '옵트 인' 방식이란 수신자의 권리를 중시하여 수신자가 동의를 한 경우에만 광고성 정보의 전송을 허용하는 제도로서 EU 국가에서는 대부분 이러한 방식을 사용하고 있다.[136]

그런데 '옵트 아웃'방식의 경우 스팸메일을 규제할 수 있는 장치로서의 기능을 사실상 상실했다고 볼 수 있다. 옵트아웃 방식은 수신거부의 의사가 표시되기 전까지는 얼마든지 스팸메일을 발송할 수 있다는 점에서 심각한 문제를 내포하고 있다. 또한 불필요한 네트워크 자원을 소모하고 이메일 마케팅 효과를 저하시키며, 나아가 청소년들에게 유해한 불건전 광고의 무차별적 유통을 사실상 허용하는 것이나 마찬가지이다. 이러한 측면에서 날로 교묘해져가고, 불법적, 무차별적으로 유포되고 있는 광고성, 유해성 스팸메일에 대응하기 위해서는 법률개정을 통한 '옵트 인'방식의 조속한 도입이 필요하다고 하겠다.

제2절 정부 및 공공기관의 역할

1. 건전한 사이버문화 확립을 위한 정보통신윤리 교육 및 계몽활동의 강화

현재의 추세와 같이 인터넷 이용자는 앞으로도 계속 빠른 속도로 증가할 것이고, 활용분야도 다양해져 사이버공간이 인간에게 있어 주된 활동무대가 될 것은 분명한 사실이다. 아니 인터넷은 이미 우리들 삶의 핵심영역이라고 말하는 것이 더 정확할 것이다. 아무튼 이처럼 중요한 인터넷공간을 그 본래 의도한 바대로의 순기능을 다하도록 하기 위해서는 관련 공공기관과 정보통신사업자, 민간단체와 네티즌 등 관련 주체들의 공동의 노력이 필요하며, 무엇보다 네티즌 스스로의 의식과 문화, 도덕적 규범이 건강해져야 한다. 요컨대, 건전한 사이버문화 확립을 위해서는 정보통신윤리교육 및 계몽활동이 광범위하고 지속적으로 실시되어야 한다. 특히 청소년들의 사이버범죄가 증가하고 있는 현실은 그만큼 사이버공간에서의 윤리교육이 제대로 이루어지지 못했다는 반증이기도 하다.

미국의 경우 정보통신윤리교육이 가급적 조기에 시작되어야 한다는 판단 아래 유치원 및 초등학생을 위한 정보통신윤리교육 프로그램들을 개발하여 보급하고 있다. 그 실례를 살펴보면, 초등학교 3-4학년에 이미 프라이버시란 주제로 교육을 실시하여 어린이들이 사적인 정보를 확인하고 부모나 선생님의 허락 없이 사이버 공간에서 개인정보를 함부

136) http://blog.naver.com/vsunna.do?Redirect=Log&logNo=100001643717.

로 누설해서는 안 된다는 사실을 인식시키며, 사이버공간에서 프로젝트 수행을 위해 학생들이 서로 협동할 수 있는 방법을 이해시킨다.[137]

미국의 경우와 같이 우리나라에서도 정보통신윤리관련 교육과 계몽활동은 초등학교 저학년부터 조기에 정해진 프로그램에 따라 정기적으로 실시하여야 하며, 사이버범죄에 관한 비디오 등 홍보물을 개발해 청소년의 사이버범죄를 미연에 방지할 수 있도록 해야 한다. 또한 이들에게 적절한 사이버윤리를 주지시킬 수 있는 역량 있는 교사의 양성도 시급하다.[138]

---

137) 미국에서 초등학교 3-4학년 단계에서 실시되는 구체적인 지도과정은 다음과 같다. ① 교사는 학생들이 이야기를 만들어내기 위해 서로 협력할 수 있는 상황을 조성한다. 교사는 학생들에게 "두 남매가 가족들과 함께 해변에 있다. 둘이 해변을 달리며 놀던 중에 여동생이 모래 위로 어떤 것이 지나가는 것을 보았다."라고 말한다. 그 후에 교사는 학생들이 자원하여 한 문장씩 덧붙임으로써 이야기를 구성하게 한다. 교사는 인터넷을 이용하여 멀리 떨어진 곳에 살고 있는 학생들에게 이야기를 말해줄 수 있다는 것을 학생들에게 자세하게 설명해 준다. ② 교사는 학생들에게 '활동지 A'를 나누어준 후에 서로 토의하게 한다. 이 때 교사는 프라이버시에 포함되는 여러 유형의 개인 정보를 학생들이 이해하는 데 초점을 맞춘다. ③ 교사는 사이버 공간에 들어가는 것이 현실 세계에서 여행을 하는 것과 마찬가지임을 학생들에게 설명한다. 거리에서 만난 낯선 사람에게 개인 정보를 알려주어서는 안 되는 것과 마찬가지로, 사이버공간에서 웹사이트나 타인들에게 함부로 개인 정보를 주어서는 안 된다는 사실을 교사는 학생들에게 주지시킨다. ④ 교사는 '활동지 B'를 나누어준다. 교사는 학생들로 하여금 10-15분 정도 자유롭게 인터넷 서핑을 하게 한 후에, '활동지 B'에 제시된 질문에 답하게 한다. 교사는 학생들이 기록한 것을 발표하게 한다. ⑤ 교사는 학생들에게 "학교에서 안전하게 지내기 위해 우리가 지켜야 할 규칙에는 어떤 것이 있을까?" 라고 질문한다. 그 후에 교사는 학생들에게 "사이버 공간에서 우리가 안전하게 지내기 위해 지켜야할 규칙에는 어떤 것이 있을까?"라고 질문을 한다. 교사는 활동지 안의 안전 규칙에 따라 사이버 공간에서 행동하는 것이 바람직함을 학생들에게 다시 한번 강조한다. ⑥ 수업을 마무리하면서 교사는 학생들에게 다음과 같은 질문을 한다. "여러분이 사이버 공간에 들어 갈 때에 여러분에게 사적인 것에는 어떤 것이 있을까?", "사이버 공간에서 여러분의 개인 정보를 알려 줄 때 유의해야 할 점은 무엇인가?", "사이버 공간에서 이야기를 만들어 서로 공유하는 방법에는 어떤 것이 있을까?" (http://cafe.naver/digitalforensic.cafe?iframe_url=/BoardRead.do%3Farticleid=37). 또한 초등학교 4~5학년 단계에서의 구체적인 지도과정은 다음과 같다. ① 교사는 학생들에게 "사이버 공간에서 여러분 자신에 대한 정보를 공개하도록 요구받은 경험이 있습니까?"라고 질문을 한다. 그 후에 교사는 오늘 수업에서 그런 상황에서의 안전 규칙에 대해 학습하게 될 것임을 상세하게 설명한다. ② 교사는 학생들에게 활동지를 나누어준다. 교사는 학생들이 활동지를 읽은 후에, 활동지에 기술된 시나리오에 따라 역할놀이를 하게 한다. 그런 후에, 교사는 학생들에게 다음과 같은 질문을 한다. "이 상황에서 개인 정보를 공유하는 것이 괜찮다고 생각되는 단서는 무엇인가?"교사는 그러한 단서가 부모님과 함께 있을 때, 부모님이 사이트를 소개시켜 주었을 때, 부모님이 그 상황 속의 모든 사람들을 알고 있을 때 등임을 설명해 준다. ③ 학생들이 개인 정보를 의미하는 개별 항목을 이해했다고 여겨지면 박스 안의 개인 정보 유형에 대하여 토의한다. 이 때 교사는 교사, 부모, 혹은 성인 안내자의 일차적인 허락 없이 초등학생들이 개인정보를 함부로 타인에게 누설하는 것은 바람직하지 못함을 학생들에게 주지시킨다 (http://cafe.naver/digitalforensic.cafe?iframe_url=/BoardRead.do%3Farticleid=37).

그리고 이미 인터넷에 익숙해진 기성세대들에 대한 재교육도 병행하여 불법적인 행위들의 명확한 규정을 이해시키고 성인들이 주도적으로 건전한 사이버문화를 정착시킬 수 있도록 해야 할 것이다. 특히 정보통신윤리위원회[139]와 한국정보보호원, 경찰청과 '학부모정보감시단' 등의 민간단체, 그리고 정보통신사업자들은 공동의 노력으로 새로운 윤리교육 프로그램을 개발함과 동시에 정기적으로 꾸준히 네티즌 대상의 계몽교육을 실시하고, 지속적인 캠페인을 통하여 건전한 사이버문화 정착에 앞장서야 할 것이다.

2. 신유형 및 해외유입 불건전정보에 대한 대책 수립

전세계적으로 인터넷 이용자수가 급증하면서 사이버공간에는 국경의 개념을 초월한 하나의 글로벌공동체가 형성되었다. 이에 따라 다양한 새로운 유형의 범죄는 물론이고, 음란·도박 등 각종 불건전정보가 급속히 확산되고 있다. 특히 해외 한글불법 정보 중 음란 및 도박정보의 경우 내국인 정보이용자들의 접근이 용이해 다양한 사회문제를 야기 시키고 있으며, 해외 음란사이트에는 개인의 프라이버시를 침해하는 몰래카메라, 미성년자를 성적유희의 대상으로 이용한 로리타, SM(sadism-masochism: 변태성욕), 라이브 포르노 등 각종 불법 포르노 매체물이 제공되고 있어 성인뿐만 아니라 청소년들의 건전한 인격형성에 장애가 되고 있다.[140] 또한 사행심을 조장하는 해외도박 인터넷정보의 경우 해당사이트 가입비, 도박비용 등이 일반적으로 신용카드로 결제되고 있어 외화유출이 심각한 상황이다.

그런데 현실적인 문제는 이렇게 해외에 서버를 두고 한글로 제공되는 신유형의 해외유입 불건전정보에 대해서는 국내의 현행 법규에 의한 규제가 법률상으로는 가능할지

138) 청소년들에게 올바른 사이버문화를 정착시킬 수 있도록 한국정보보호원에서는 초, 중, 고교 교사들을 대상으 로 원격교육을 실시하고 있다. 교육 내용은 사이버문화와 N세대의 특징, 인터넷 중독, 저작권과 정보보안, 엽 기문화와 안티문화, 불건전 유해정보와 사이버 성폭력 등으로 일선 학교에서의 접근방식에 대한 사례 중심으로 이루어져있다(http://blog.naver.com/comsnake.do?Redirect=Log&logNo=80002236580).

139) 정보통신윤리위원회는 2004년 상반기 중 네티즌 33,543명을 대상으로 정보통신윤리교육을 실시하였다 (전자신 문, 2004년 7월 22일자).

140) 과거의 경우 국내에 서버를 두고 한글 포르노물을 유포하는 사업자가 많았으나, 최근 관계당국의 지속적인 단속이 있자 해외에 서버를 두고 한글자막 및 음성으로 제작하여 국내 이용자에게 유료로 유포하는 경우가 많아지고 있다.

몰라도 규제의 실효성을 확보하기는 쉽지 않다는 것이다. 따라서 이러한 한계를 감안하고도 궁극적으로 해외유입 불건전정보를 조기에 차단할 수 있는 강력한 '유입차단조치'가 필요한 것이며, 이를 위해서는 다음과 같은 몇 가지 사항을 생각해 볼 수 있을 것이다.

첫째, 국제사법공조체제의 구축을 통하여 해외유통 불건전정보에 대한 정보를 상호간에 교류하며, 불건전매체 차단기술의 공동개발 등 실질적인 차단 노력을 해야 한다.

둘째, 해외불법정보 이용대금의 결제를 억제하는 방안이 필요하다. 이러한 방식은 해외서버를 통해 국내로 유입되는 불건전정보에 대한 대금지급을 억제함으로써 불건전정보의 유입을 원천적으로 차단하는 것이다. 예를 들어 지급결제에 있어 계약관계나 거래관행상 지급결제 대행업자에 대하여 감독권 등 사실상 지배권을 행사할 수 있는 것이 카드사이기 때문에 금융감독기구가 여신전문금융업자인 카드사에 대하여 금융감독권을 행사함으로써 간접적인 규제가 가능하도록 하는 것이다. 그러나 이와 같은 방안은 자칫 외교적 마찰의 소지가 있기 때문에 제도적 개선이 선행되어야 하며, 이를 위해 정보통신부와 경찰, 검찰, 정보통신사업자, 한국여신금융협회, 신용카드사 등 관련 기관의 공동의 노력이 필요하다.

셋째, 해외불법정보에 대한 차단기술의 개발 및 보급이 필요하다. 현재 해외 불건전정보의 차단은 URL단위와 IP주소 단위로 ISP업체의 협조에 따라 이루어지고 있다. 해외 불건전정보제공자 및 사이트 운영자는 국내에서 음란·도박정보의 유통이 불법이라는 사실을 인지하여 수 개의 IP를 연결·활용하거나 IP를 손쉽게 변경하여 국내에서의 라우터 차단 등을 회피한다. 이에 비해 국내에서는 URL단위나 IP주소단위 중 1개의 단위만으로 차단하거나 이를 병행하여 차단하는 등 ISP업체마다 다른 차단방식을 이용하고 있어 차단기술의 일관성을 유지하는데 한계가 있다. 따라서 ISP업체의 라우터 시스템 및 서비스이용 제한을 최소화 할 수 있는 기술개발이 이루어져야 한다(정보통신윤리위원회, 2004).

넷째, 해외 불법정보제공자 및 이용자에 대한 형사적 제재를 강화해야한다. 기존에는 해외에 서버를 두고 한글로 제공되는 인터넷상의 불건전정보에 대하여는 처벌할 수 없다는 논리가 지배적이었으나, 최근에는 해외의 불법정보제공자 및 이용자들에 대하여도 관계당국이 형사처벌을 하는 추세이다. 따라서 향후에도 해외 불건전정보제공자가 반드시 처벌된다는 점을 환기시켜 불건전정보가 해외에서 유입될 수 없도록 해야 한다.

3. 정보・네트워크 보호산업 및 인력의 육성

오늘날 국제사회는 정보능력에 따라 국가의 안위가 결정될 만큼 정보보호의 중요성은 날이 갈수록 커지고 있다. 따라서 작게는 사이버범죄를 예방하고 크게는 국가안보를 위해서도 정보 및 네트워크 보호산업 관련 인력의 육성은 시급하다.

우리나라의 경우 정보보호산업이 첨단산업으로 각광을 받으면서 정보보호분야에 대한 관심이 높아지고는 있으나, 기본적으로 정보보호산업 관련 인력육성에 대한 투자가 현재보다는 더욱 활발히 이루어져야 한다고 본다. 최근의 조사에서 나타난 사항, 즉 대부분의 정보통신사업자들이 가장 기본적인 대응책이라 할 수 있는 침입차단시스템조차 설치하지 않고 있어 보안서버 보급비율이 OECD 가입 국가 중에서 매우 낮은 수준으로 나타난 것 등이 이를 반증한다.

그러므로 지속적으로 정보보호 분야의 전문 인재를 양성하는 한편 핵심기술개발을 적극적으로 추진해 사이버 범죄에 대응할 수 있는 인프라를 구축해야한다. 구체적 방안으로, 정부 및 정보통신사업자, 그리고 학교에서는 기술개발과 산업인력양성을 위해 지속적으로 노력해야 하며, 대학의 관련 전공을 신설・확대하고 지원을 아끼지 말아야 할 것이며, 그 외에도 정보보호관련 전문교육기관을 운영하고, 정보보호관련 자격제도를 활성화하는 등의 방안이 활발하게 이루어져야 할 것이다.

특히 정보보호를 위하여 최근 각국에서 해커를 활용하는 사례가 늘어나는 점도 주목할 필요가 있다.[141] 우리나라의 경우 정보통신산업의 수준이 최고라고 해도 과언이 아니

141) 세계 각국은 당초 해커들로부터 전산망을 보호하는 보안설비 시스템 구축에 주력했으나 지난 90년대 중반 이후 해킹과 바이러스를 담당하는 해커부대를 양성하는 등 공격형 사이버전에 나서고 있다. 국가가 타국의 기밀과 군사 및 기업정보를 훔치거나 파괴하고, 컴퓨터시스템에 타격을 주기 위해 전문 해커집단을 관리·교육하고 있는 것이다. 사이버전에 본격 대비해온 나라는 현재 타의 추종을 불허하고 있는 미국 외에 북한과 중국, 일본, 영국, 프랑스, 러시아, 이스라엘, 쿠바, 리비아 등 20여개국에 이른다. 미국은 99년 적국의 데이터·군사·금융체계를 파괴하는 합동작전 부대를 창설, 적의 지휘·명령·통신·컴퓨터 및 정보체제(C4&I)와 작전 소프트웨어를 마비시키는 훈련을 해오면서 자료와 프로그램을 파괴하는 바이러스인 '논리폭탄'과 에너지를 방출해 전자장비 를 마비시키는 전자폭탄 등 사이버무기들을 선보였다. 미 국방부는 지난해에만 사이버전력 강화에 3천만 달러의 예산을 썼으며, 2천500만대에 달하는 군사용 컴퓨터의 보안을 위해 매년 10억 달러 이상을 투입하고 있다. 100만명이 넘는 해커를 보유한 중국은 97년 컴퓨터바이러스부대를 조직한 뒤 지역사령부 단위까지 사이버부대를 편성, 해킹전쟁 훈련을 반복해왔다. 또 '방화벽 만리장성'이라는 정보방어 프로젝트에 집중하면서 해킹, 암호해독, 바이러스

지만, 정보보호에 있어서는 관련 인력이 부족하여 정보보호를 위한 효과적인 대응을 하지 못하고 있다. 따라서 정보통신에 대한 전문적인 지식을 습득하고 있는 해커들을 활용하는 방안도 고려해볼만 하다. 물론 이들이 불법적인 행위를 할 경우 처벌은 당연하지만, 이들을 긍정적인 방향으로 활용한다면 귀중한 정보보호자원이 될 수 있을 것이다. 최근 우리나라의 주요 국가기관 해킹사건의 주범이 중국 인민해방군 산하 해킹부대라는 논란[142]과, 유명 포털사이트 '다음'이 해커 전문가 그룹과 공식적인 업무제휴 협약을 체결하여 100% 안전하지 못한 자신들의 서비스 문제점을 해결하기로 하였다는 사례는 해커의 중요성을 잘 나타내주는 것이다. 그러므로 우리나라도 해커를 이용하여 사이버범죄에 대응할 수 있는 방안을 검토해볼만하며, 장기적으로는 해커들을 활용한 '사이버방위군', '사이버보안군' 등의 국가안보를 위한 국가적 부대 창설도 검토해볼만 하다.

제3절 사업자(단체)의 역할

1. 자율규제활동의 강화

정보통신서비스를 제공하는 사업자측에서의 자율규제활동은 포털서비스 등을 제공하는 개별 사업자의 경우와 유관 사업자들로 구성된 사업자단체의 경우로 나누어 생각해 볼 수 있다.

제작은 물론 전자충격을 일으켜 전자 무기·장비를 파괴하는 전자기 진동 미사일탄두 등 다양한 디지털 공격무기를 개발 중이다. 일본은 98년 자국의 한 컴퓨터를 경유한 이스라엘 해커가 미 해군 전산망에 침입한 사건을 계기로 국토방위의 개념을 오프라인에서 온라인으로 확대, 국가전산망 보호에 나섰다. 2000년 군·경합동 사이버테러 대응조직을 만들고, 2001년엔 컴퓨터 보안체계 구축을 위해 129억엔의 예산을 처음으로 특별 편성한데 이어 오는 2006년 목표로 사이버 전투부대 창설을 준비하고 있다. 북한도 예외가 아니다. 지난 2004년 5월 국군기무사 발표에 따르면 북한군은 미 중앙정보국(CIA)과 맞먹을 정도의 해킹능력을 가진 부대를 통해 남한 정보를 수집하고 있다. 컴퓨터 수재들을 선발해 인민무력부 정찰국 예하 해킹부대의 군관으로 발령하는 등 매년 전문인력 100명을 양성하고 있다 한다(부산일보, 2004년 7월 22일자).

142) 2004년 7월 우리 국가기관을 해킹한 중국인 해커가 현역 중국 인민해방군인 것으로 알려져 파문이 확대되고 있다. 또 중국 해커에 의해 해킹 피해를 입은 우리 국가기관이 당초 알려진 국회 등 10곳 외에 주한미군 사령부 등 해외주둔 미군사령부 5곳도 중국 해커에 의해 해킹 피해를 입은 것으로 확인됐다(경향신문, 2004년 7월 15일자).

정보통신사업자들은 유해정보의 유통방지, 스팸차단, 음란메일에 대한 수준별 필터링, 어린이 회원 가입시 부모의 동의절차 등 개별 사이트별로 다양한 규제활동을 실시하고 있으며, 정보통신사업자단체에서는 단체에 소속된 개별 사업자들을 대상으로 심의 및 시정요구를 하고 있다.

인터넷공간은 근본적으로 '자율' 이라는 이념 하에 표현의 자유가 중시되고 자유롭게 활동하는 공간이므로 유해환경도 공식적인 통제에 의해서보다는 정보제공자와 정보통신사업자들이 자율적으로 규제하는 것이 이상적이다. 그러나 최근에 급증하고 있는 각종 역기능 현상들은 인터넷 공간을 더 이상 자율에만 맡겨둘 수 없는 지경에 이르게 하였다. 그러한 원인의 상당 부분은 지나치게 상업성에 치우쳐 몸집 불리기에만 급급한 개별 정보통신사업자들과 단체 본연의 임무인 소속업체에 대한 심의활동을 소홀히 한 정보통신사업자단체에 있는 것이다. 이미 인터넷 내용등급제가 실시되고 있는 것과 같이 더 이상 정보통신사업자가 자율규제활동을 간과한다면 인터넷상의 자율은 갈수록 그 입지가 좁아질 수밖에 없을 것이다.

따라서 정보통신사업자와 사업자단체들은 보다 명확한 규제기준을 설정하고, 기준을 위반한 사용자에 대해서는 사용금지 또는 관계당국에 고발조처하고, 사업자단체는 소속 사업자에 대해 자체적으로 강력한 징계를 내리는 등 건전한 사이버공간을 만들기 위한 자발적인 노력을 강화해야 한다.

2. 자체모니터링의 강화

사이버테러나 불건전유해매체물의 유포 등을 막기 위한 신종 네트워크 기술이 개발되고 있기는 하지만, 모니터링(monitering)도 신속정확하고 엄격한 규제가 이어질 경우 이러한 사이버범죄를 막기 위한 효과적인 대응수단의 하나이다.

사이버범죄를 막기 위한 모니터링 활동도 정보통신부와 경찰 등 관계기관, 정보보호관련 기업, 시민단체 및 일반 네티즌에 이르기까지 다양한 주체들에 의해서 이루어지고 있지만, 근본적으로 정보통신사업자들의 협조 없이는 소기의 성과를 거두기가 어렵다.

포털사이트의 경우 국대 5대 사이트에서는 자체 심의 기준을 통해 수시로 모니터링하고 직권으로 사이트 등록을 해지한다고 밝히고 있으나, 최근의 조사결과에 의하면 모니

터링 활동은 극히 저조하여 각종 음란사이트가 버젓이 공개되고 있는 것으로 나타났다.[143]

따라서 정보통신사업자들이 모니터링 인력을 증원하고 사전모니터링 등을 통해 불건전정보가 유통되는 것을 막기 위해 자체정화활동을 강화하도록 하기 위한 정부차원의 제도적 장치도 필요하다. 또한 정보통신사업자들은 24시간 실시간으로 사이버 공격 및 범죄행위에 대한 조기탐지와 신속대응체계를 구축하고 인터넷데이터센터(IDC)의 보안을 강화하는 등의 시스템 구축에 심혈을 기울여야 할 것이다.

3. 처벌가능성의 경고와 신고의 의무화

정보통신사업자들이 운영하고 있는 각종 사이트에서는 회원가입을 요구하는 경우 약관에 동의하도록 하고 있으며, 약관 위반 시 형사책임이 따르게 된다는 사실을 공지하고 있다. 그러나 자신들의 사이트와 직결되지 않는 부분에 있어서는 인터넷 이용자들이 쉽게 찾아볼 수 있을 정도의 각종 처벌가능성에 대한 경고표시가 제대로 표시되지 않고 있어 다수의 청소년들이 자신들의 행위를 위법한 행위로 인식하지 못한 채 사이버범죄자로 전락하는 경우가 많다.

따라서 정보통신사업자 측에서는 사이버범죄의 가능성이 있는 사이트의 메인창, 게시판 혹은 채팅창, 전자상거래 관련 창에 집중적으로 사이버범죄에 대한 처벌가능성을 경고하는 내용의 문구를 만들어 누구나 쉽게 볼 수 있도록 해야 한다. 또한 구체적인 처벌조항을 링크시켜 사이버범죄에 대한 경각심을 일깨워 줄 필요가 있다.

한편 정보통신사업자들이 모니터링 등을 통해 사이버범죄를 인지한 경우에는 지체 없이 관계당국에 신고할 수 있도록 의무를 부과할 필요가 있다. 최근의 국가기관 해킹사건들을 계기로 2004년 8월부터 해킹에 대해서는 인터넷제공업체와 인터넷데이터센터 등을 대상으로 반드시 신고를 하도록 하는 '신고의무화제도'가 실시된다. 그러나 이러한 정보

143) 유명 포털에 등록된 성인사이트 10곳 중 9곳은 불법이거나 성인 인증장치가 없는 등 성인물 관리가 허술한 것으로 드러났다. 이에 따라 최근 인터넷 미디어를 자처해 온 포털업체들이 광고 수익에만 눈이 어두워 스스로 모니터링을 소홀히 하거나 외면하여 사회적 공기의 역할을 회피하고 있다는 지적을 받고 있다(전자신문, 2004년 4월 21일자).

통신사업자에 대한 신고의무화 제도는 해킹의 경우뿐만 아니라 전체적인 사이버범죄로 확대하는 방안을 검토해 보아야 한다. 정보통신사업자가 자체적인 모니터링을 통해 사이버범죄를 인지하거나 이용자들의 신고로 사이버범죄를 인지하는 경우 즉시 관계당국에 신고하여 수사에 착수할 수 있도록 '사이버범죄 신고의무제도'를 실시할 필요가 있다는 것이다.[144]

4. 온라인 우표제의 전면실시

온라인 우표제도는 일반 우편물처럼 온라인의 전자우편에도 요금을 부과하는 제도로서, 2002년 5월 국내 유명 포털사이트인 다음커뮤니케이션(Daum Communication Co.)이 세계 최초로 실시하였다. 이와 같은 방식은 대량으로 전자우편을 보내는 사용자에게 서버 사용료를 받는 형식으로, 다음커뮤니케이션은 2002년 12월 현재 하루 1000통 이상을 보내는 사업자에게 이 제도를 적용하고 있다.

온라인 우표제는 근본적으로 대량으로 발송되는 스팸메일의 폐단을 막자는 취지로 시행되고 있는데, 이에 대하여 시민단체에서는 온라인 우표제가 스팸메일을 방지하는 효과는 극히 미미하며, 오히려 정보통신산업의 위축을 가져오고 대형 포털사이트의 수입향상에만 기여한다고 반대를 분명히 하고 있다.

그러나 소수에서 시행중인 온라인 우표제는 스팸메일의 방지와 더불어 불건전정보의 유통을 막을 수 있는 상당히 실효성 있는 제도라고 생각된다. 일각에서 제기하고 있는 인터넷과 이메일이 표방하는 정보의 공유 및 알 권리에 위배된다는 논리는 최근에 더욱 심해지는 스팸메일의 유해성을 간과한 논리라고 보여진다.[145]

스팸메일은 비단 어제, 오늘의 문제가 아닌 인터넷이 활발해진 90년대 후반부터 끊임없이 제기된 문제이다. 특히 최근에는 청소년에게까지 음란 및 사행심조장 메일, 바이러스가 포함된 메일이 무차별적으로 살포되고 있어, 온라인 우표제에 반대의견을 가졌던

144) 특히 사이버성매매, 전자상거래사기, 명예훼손 및 허위사실유포와 같은 사이버범죄에 있어서는 정보통신사업자의 자체 모니터링에 이은 신고가 크게 효과를 거둘 수 있을 것이다.

145) 최근의 스팸메일은 메일을 열자마자 바이러스를 유포시키거나, 노골적인 성관계 동영상 배경이나 성인사이트로의 자동 이동, 거짓 허위사실의 메일 등 청소년에게는 실로 큰 해악을 끼치는 정도로 변해가고 있다.

포털사이트에서도 그 위험성을 인식, 태도를 바꾸고 있다.[146] 따라서 궁극적으로는 온라인 우표제가 전면적으로 실시되는 것이 바람직하며, 수신자의 이메일 평가에 따라 온라인 우표의 요금을 환불해주는 현재의 제도에 더하여 온라인 우표제를 통하여 얻어진 수입을 포털사이트가 독식하는 것이 아닌 사회적으로 환원할 수 있는 정책이 필요할 것이다.[147]

제4절 민간(단체)의 역할

1. 모니터링 활동의 활성화

민간단체에서 행하게 되는 인터넷상의 모니터링 활동은 주로 불건전유해매체물에 집중될 수밖에 없다. 그것은 민간단체의 전문적 지식 부족에서 기인하기도 하지만, 민간단체 자체가 학부모, 교사 등 청소년들과 직접적으로 관련되는 구성원들로 조직되기 때문이다.

그러나 이러한 민간단체의 모니터링 활동은 불건전유해매체물을 일소하는데 있어 큰 역할을 담당하고 있다. 앞서 언급한 바와 같이 현재 정부 및 공공기관, 그리고 정보통신사업자의 모니터링 활동은 인력의 부족으로 인해 크게 제약을 받을 수밖에 없다.

이러한 상황에서 불건전유해매체물에 대한 모니터링 활동을 민간단체와 공조하게 된다면 활동 자체의 효율성을 높일 수 있을 뿐만 아니라 기타 사이버범죄에 대하여 최대한의 자원을 투입하여 전반적인 사이버범죄 자체의 예방과 대응에 탄력을 받을 수 있기 때문이다.

따라서 인터넷에 대한 민간의 모니터링이 활성화되면 다음과 같은 이점을 얻을 수 있다.

---

146) 특히 대형 포털사이트인 Yahoo와 MSN을 운영하는 MS사도 온라인 우표제의 도입을 적극적으로 검토하고 있다(파이낸셜 뉴스, 2004년 2월 4일자).

147) 한편 공정거래위원회는 2003년 10월 17일 다음 커뮤니케이션의 온라인 우표제가 공정거래법을 위반했는지 여부를 전원회의가 3개월에 걸쳐 심의한 결과 법 위반 여부를 판단할 근거가 부족하다는데 의견을 모으고 심의절차를 종료하기로 최종 합의했다고 밝혔다. 공정위 사건처리절차가 규정하고 있는 '심의절차 종료'란 법 위반성이 없다는 '무혐의'와 달리, 사건의 사실관계 확인이 곤란해 법위반 여부의 판단이 불가능할 때 내려지는 것으로 1년 반이 넘는 심사기간을 거친 사건이 '심의절차 종료'결정을 받은 경우는 손을 꼽을 정도로 극히 드문 일이다.

첫째, 활발한 모니터링 활동은 궁극적으로 민간 영역의 온라인 불건전 정보 감시활동을 활성화시켜 자율적 정화 능력을 배양할 수 있는 것이다. 둘째, 모니터링 활동은 민간·공공기관·정보통신사업자와의 지속적 협력을 유도하여 인터넷 안전 네트워크를 구축할 수 있게 한다. 셋째, 공정하고 안전한 인터넷 문화를 조성할 수 있으며, 넷째, 그동안 정보화의 역기능에 익숙해진 네티즌으로 하여금 인터넷의 편리성과 안정성에 대한 인식을 제고할 수 있다.

최근 모든 공공기관의 사업에 있어 민간의 참여는 필수적인 요소로 자리잡아가고 있다. 그것은 직접적인 혜택을 받는 구성원이 자발적으로 정책에 참여할 때 그 만큼 효과를 거양할 수 있다는 것을 의미한다. 이러한 점은 사이버공간에 있어서도 마찬가지이다. 향후 모니터링뿐만 아니라 정보통신정책 전반에 있어서의 민간의 참여는 그래서 더욱 요구되는 것이다.

2. 인터넷 중독의 예방활동 강화

'중독'이라는 것은 한번 빠지면 헤어나기 어렵고, 또한 본인과 주변의 도움으로 회복되었다 하더라도 중독 되었던 시간만큼의 정신적, 시간적, 경제적 손실을 되돌릴 수 없게 되는 것이다.

인터넷 중독은 정체감 형성이 불완전한 아동과 청소년뿐만 아니라 정상적인 사회생활을 영위해야할 직장인, 주부, 남편 등 일반인에게 있어서도 매우 심각한 영향을 끼치고 있으며, 인터넷 중독의 수준에까지 다다르면 일상생활에 미치는 피해는 상상을 초월하게 된다. 따라서 인터넷 중독은 예방이 최선이자 최고의 방법이라 할 수 있다(정보통신윤리위원회, 2004).

인터넷 중독을 예방하기 위해서는 개인적 차원의 노력이 중요하지만, 무엇보다 인터넷 중독이 가져오는 폐해를 인식하게 하고, 적절한 인터넷 사용을 유도할 수 있는 교육 및 계몽활동이 필요하다.

특히 사이버공간은 공권력이 잘 통하지 않는 공간이기 때문에 민간단체는 정부나 정보통신사업자들과 달리 인터넷 중독에 대한 예방활동에 많은 기여를 할 수 있을 것이다. 따라서 현재 활발한 활동을 벌이고 있는 기존의 학부모정보감시단(www.cyberparents.or.kr), 클린

인터넷 국민운동본부(www.cleaninternet.org), 한국사이버감시단(www.wwwcap.or.kr), 안전한 온라인을 위한 민간네트워크(www.safeonline.or.kr) 등의 민간단체 외에 더욱 많은 민간의 참여가 이루어져야 하는 것이다.

물론 인터넷 중독의 예방을 민간단체의 독자적인 노력으로 한다는 것은 무리가 따른다고 볼 수 있다. 그러므로 정부의 적절한 지원 아래 정부 및 공공기관과 정보통신사업자, 민간단체 등 모든 사이버 구성원들이 참여할 수 있는 예방캠페인을 전개해야 할 것이다. 그러나 그 중에서도 특히 민간단체의 역할이 중요한 것은 자명한 사실이다.

3. 청소년에게 유익한 컨텐츠 보급 운동

현재 정보통신윤리위원회는 청소년권장사이트제도를 운영하여 청소년들에게 유익한 컨텐츠를 보급하고자 노력하고 있다. 그러나 이러한 정부주도적 노력보다는 민간에서 주도적으로 컨텐츠를 보급하는 노력이 더 큰 효과를 거둘 수 있다.

따라서 민간단체에서는 청소년들에게 보다 교육적이고 건전한 컨텐츠의 개발과 보급에 있어 주도적인 역할을 담당해야 한다. 민간단체가 참여할 수 있는 구체적인 부분으로, 민간단체는 정부로부터 예산 등의 지원을 받아 학부모 단체, 교사, 청소년전문가들과 협력하여 청소년에게 유익한 컨텐츠를 제작, 보급해야 한다.

또한 민간단체는 불건전컨텐츠에 대한 자율적인 정화활동을 보다 활발히 실시하여 불건전 컨텐츠를 모니터링하고 신고하는 등의 자정적인 정화능력을 배양해야 하며, 지속적인 건전 컨텐츠 보급을 위한 캠페인을 전개하여 인터넷의 역기능을 해소하고 건전한 사이버공간을 만들 수 있도록 해야 할 것이다.

4. 건전한 청소년 인터넷 문화의 조성

정부 주도로 이루어지던 청소년의 건전한 인터넷 문화 만들기와 관련된 운동에 있어 최근에는 민간의 참여가 다양하게 이루어지고 있다. 최근 48개 시민사회단체가 모여 구성한 '안전한 온라인을 위한 민간네트워크'는 건전한 정보 확산을 위한 문화강좌, 워크숍 등을 개최한 데 이어 온라인 게임 이용과정에서 청소년들이 입을 수 있는 피해에 대해

게임업체들의 각성을 촉구하는 성명서를 내기도 하였다. 또한 사단법인 한국사이버감시단은 정통부의 'e-Clean Korea' 캠페인의 일환인 민간단체 캠페인을 주도적으로 진행했고, 현재는 민간단체에 대한 인터넷 자율규제활동 교육을 진행 중이다.

이렇게 민간단체가 건전한 사이버공간을 만들기 위해 직접 나서게 된 것은 더 이상 인터넷이 청소년들에게 안전한 공간이 아니며, 방치할 경우 더욱 큰 문제점이 발생할 수 있다는 인식, 그리고 정부와 정보통신사업자들만의 노력으로는 이러한 문제를 해결할 수 없다는 인식에서 비롯된 것이라 할 수 있다.

따라서 민간단체는 건전한 사이버공간을 만들기 위해 향후 지속적인 노력을 전개해야 할 것이다. 특히 불건전유해매체물을 감시하고, 청소년들의 일탈을 유발할 수 있는 요소들을 제거하는 활동 등을 통해 사이버공간이 본래의 순기능대로 청소년에게 유익한 공간이 될 수 있도록 해야 할 것이다.

제5절 일반 네티즌들의 사이버범죄(피해) 예방 노력

사이버범죄는 다른 범죄와 달리 피해자의 피해예방 노력 여하에 따라 범죄를 크게 감소시킬 수도, 또는 크게 증가시킬 수도 있는 피해자의 역할이 매우 중요한 범죄유형이라 할 수 있다.

잠재적인 피해자가 사이버범죄를 줄일 수 있는 구체적인 방안으로는 첫째, 사이버범죄에 대한 의식제고이다. 앞서 문제점에서 지적한 바와 같이 우리 사회가 아직은 사이버범죄를 여타 강력범죄에 비하여 심각하게 받아들이지 않는다는 것이 큰 문제점이다. 특히 사이버범죄에 대한 신고의지는 높은 반면에 피해경험자의 극히 일부분인 4.9%만이 실제로 신고를 한다는 점은 다른 여러 가지 이유가 있을 수 있지만, 무엇보다 피해당사자의 강력한 처벌의지가 없다는 것이다. 그러므로 사이버범죄를 예방할 수 있는 가장 중요한 방법은 사이버범죄에 대한 심각성을 인식하고 그에 따라 경미한 범죄가 발생했을 때에도 철저하게 신고할 수 있는 의식전환이라 할 수 있다.

둘째, 개인의 보안의식 강화이다. 한국의 일반 네티즌들은 초고속 인터넷의 보급률에

비하여 보안의식이 상당히 낮은 수준이다. 따라서 사이버범죄 피해를 예방하기 위해서는 개인의 보안의식 강화로 개인의 PC부터 방어할 수 있는 의식의 전환이 필요하다. 보안은 편의성과 반비례하기 때문에 불편하더라도 보다 세심한 모니터링과 개인용 방화벽 설치 등이 필요하다. 또한 전자상거래를 할 때에 있어서도 온라인 정보 암호화 프로그램을 반드시 설치하고, 공인전자서명을 받아두는 등 개인적인 보안의식을 강화해야 할 것이다.

셋째, 사이버범죄와 신고절차 및 피해구제제도를 숙지해야 한다. 사이버범죄의 피해를 입은 피해자들은 자신이 입은 피해상황에 대하여 가해자의 행위가 범죄행위로 성립될 수 있는지, 처벌을 받을 수 있는지, 그리고 만약 그렇다면 신고절차는 어떻게 되는지에 대하여 숙지하지 못하고 있는 경우가 많다. 따라서 신고의지를 갖고 있어도 쉽게 신고를 하지 못하고 있으며, 피해상황에 대한 구제제도를 파악하지 못해 범죄피해를 덮어 버리는 경우가 많다. 그러나 이와 같은 태도는 자신만을 범죄피해자로 만드는 것이 아니라 또 다른 사이버범죄 피해자를 양산하는 태도이기 때문에 사이버범죄 피해발생시의 신고절차와 피해 구제제도에 숙지할 필요가 있는 것이다.

넷째, 인터넷 중독의 방지 및 적절한 인터넷 사용 노력이 필요하다. 모든 범죄가 그렇듯 범죄가 일어날 수 있는 상황에 노출되는 시간이 많을수록 범죄피해자가 되기 쉽다. 특히 인터넷 중독의 경우 하루의 대부분을 인터넷에서 보내기 때문에 본인 스스로의 문제점과 더불어 사이버범죄 피해자가 되기 쉬운 면이 있다. 그러므로 인터넷 중독의 방지를 위한 노력이 필요하며, 동시에 적절한 시간동안만 인터넷을 사용할 수 있는 스스로 통제하는 능력을 키워야 한다.

다섯째, 개인 스스로가 불건전정보나 유해매체에 접근하지 않도록 해야 한다. 사이버공간에서 범죄피해를 당하는 상당수가 스스로가 불건전 정보나 유해매체와의 접촉을 함으로써 일어나고 있다. 특히 음란스팸메일을 통한 바이러스 유포, 전자상거래 관련 사기, 게임 아이템 사기, 사이버성폭력 등 다수의 범죄들이 공식적이고 건전한 인터넷 매체가 아닌 불법적이고 유해한 매체를 통해 이루어진다. 그러므로 네티즌 스스로가 이와 같은 사이버공간에의 접촉을 자제하여 자신의 범죄피해를 예방해야 할 것이다.

제6절 경찰의 대응능력 강화

1. 대응체계 재검토

사이버범죄에 대한 현행 경찰의 대응체계는 크게 경찰청 수사국내의 사이버테러대응센터(CTRC)를 중심으로 이루어지고 있다. 그러나 정책적 지원의 부재, 전문인력의 부족과 예산, 장비 등의 부족으로 인해 보다 효과적인 대응체계를 구축하지 못하고 있다.

경찰의 사이버범죄 대응체계에 있어서 경찰청 사이버테러대응센터, 지방경찰청 사이버범죄수사대, 경찰서 전담반 체제의 조직구조는 효율적인 면을 지니고 있다. 그러나 문제는 정책적으로 사이버범죄에 대한 정부차원의 집중적 투자가 아직은 크게 부족하다는 것이다.

특히 경찰청 사이버테러대응센터가 수행하는 업무에 비해 정통부(국장급), 국정원(국장급) 등 여타 관련 부처의 기능에 비해 책임자가 총경급으로 상대적으로 약화되어 있으며, 전담인원의 숫자에 있어 상대적으로 부족한 실정이다. 따라서 경찰의 대응능력을 강화하기 위해서는 자체의 위상강화 뿐만 아니라 전문 인력의 지속적인 확보, 양성 등 적절한 인적 관리방안이 필요하며, 나아가 전문화 교육을 강화하며, 지속적으로 발달하는 사이버범죄에 효과적으로 대응하기 위한 첨단수사기법의 개발이 필요하다.

또한 그동안 효과적인 대응을 가로막았던 사이버범죄 단속여건을 현실화하는 동시에 보다 엄정한 법집행을 이룰 수 있는 제도적 장치의 마련이 필요할 것이다. 이하에서는 보다 효과적인 사이버범죄 대응을 위한 세부사항에 대하여 논의하기로 한다.

2. 대응역량 강화

1) 전담인력의 확충

경찰청 사이버테러대응센터는 70여명 규모로 국내 사이버범죄에 대한 주도적인 대응업무를 수행하고 있다. 그러나 2000년 2,444건에서 2003년 68,445건(28배 증가)으로 폭발적으로 증가하고 있는 사이버범죄에 대한 대응인원으로는 상당히 부족한 수치이다. 물

론 향후 발족될 사이버테러대응단에서는 경무관을 단장으로 하여 110명 규모로 조직이 확대된다고 하지만, 110명이라는 인원도 결코 많은 숫자라 할 수 없다.

69명이라는 숫자는 2003년도의 총 사이버범죄 발생건수와 비교해 볼 때 담당인원 1인당 991건에 해당하는 것이며, 110명이라고 가정하더라도 1인당 622건에 해당한다. 특히 이러한 인원들이 감시활동 외에 현장출동 및 사후처리의 업무까지 수행하기 때문에 상당히 과도한 업무량이라 할 수 있다.

따라서 사이버범죄에 보다 효과적으로 대응하기 위한 경찰의 가장 우선적인 개선노력은 인력의 확충일 것이다. 구체적으로 향후 경찰의 전담인력 증원숫자는 적어도 1인당 500건이 넘지 않는 범위내에서 대폭 증원되어야 할 것이다.

2) 전문화교육의 강화

전문화교육은 단순한 인력의 증원에 그치지 않고 지속적인 사후관리적 대응이라 할 수 있다. 사이버범죄에 대한 대응인력이 모두 전문가일 수 없기 때문에 이들에 대한 전문화교육은 효과적인 대응을 위한 필수적인 요소라 할 수 있다.

현재 사이버범죄 대응 경찰인력의 전문화교육은 경찰수사보안연수소에서 행하여지는 '사이버범죄수사과정'(고급과 중급, 연 240명)이 있으나, 1회당 40명을 대상으로 년 4회 실시에 교육기간도 2주에 불과해 실질적인 효과를 거두지 못하고 있으며, 민간 전문교육기관에의 위탁교육도 1개월에서 5개월 정도에 그치고 있다. 또한 해외 교육프로그램으로 외국의 첨단 수사기법을 연수하는 프로그램은 1-2주 내외의 짧은 일정에 그치고 있다.

이러한 교육과정은 지나치게 짧은 교육기간으로 실질적인 효과를 거두기가 어렵다. 특히 사이버범죄가 특정한 국경 없이 전 세계 곳곳에서 발생하고 있으며, 그 수법도 갈수록 고도화되는 현실에서 외국의 첨단 수사기법을 연수하는 과정은 반드시 필요한 것이다. 그럼에도 불구하고 이러한 과정이 1-2주에 그치고 있는 것은 연수과정 자체의 의미가 없는 것이라 해도 과언이 아닐 것이다.

그러므로 경찰의 사이버범죄 대응능력을 향상시키기 위해서는 전문교육 기간을 대폭 늘리는 것이 필요하며, 특히 활발한 해외연수 기회의 증대와 관련 기관으로의 위탁교육을 확대, 실시해야 할 것이다.

3) 첨단수사기법의 지속적 개발

사이버범죄는 범죄수법의 발달속도가 여타 범죄에 비하여 상당히 빠른 편이다. 따라서 수사기법이 범죄수법의 속도를 따라가지 못한다면 사이버범죄에 대한 대응은 더욱 어려워지는 것이다.

최근 일어난 중국 등에서의 국가기관망 해킹 사건에서 보듯이 국내의 전산망의 보안상태는 상당히 취약한 실정이며, 이들에 대한 대응에 있어서도 미흡함이 많이 드러났다. 특히 해킹과 같은 범죄에 있어서는 경찰이 '해커를 잡는 해커'가 되어야만 하는 것이다.

따라서 경찰에서는 사이버범죄 수법의 발달속도에 맞추어 그러한 범죄를 조기에 진압할 수 있는 첨단수사기법을 지속적으로 개발해야 할 것이며, 외국과의 활발한 교류, 그리고 외국의 관련기관으로의 파견 및 연수의 확대를 통하여 효과적인 수사기법을 습득할 수 있도록 해야 할 것이다.

3. 단속여건의 현실화

1) 실시간 대응 보장

사이버범죄의 수사에 있어 실시간 대응은 상당히 중요한 요소이다. 특히 접속기록을 역추적하여 범인을 검거하는 것이 보편적인 수사방식인 현실에서 실시간 대응은 수사의 성패를 가늠할 수 있는 중요한 열쇠가 되는 것이다.

그러나 서버를 역추적하는 과정은 관련기관 및 업체와의 협조미비로 인해 일일이 공식 절차를 밟아야 하는 경우가 많으며, 이에 따라 대응시간도 그만큼 길어지게 되는 것이다. 또한 경찰의 독자적인 수사권이 미비하고, 관련 법률의 미비로 인하여 실시간 대응이 이루어지지 못하는 경우도 많다.

그러므로 사이범죄의 대응에 있어 사안이 긴급성을 요함에 있어서는 경찰의 재량을 보다 확대하여 실시간으로 대응할 수 있는 체제를 구축하는 것이 바람직할 것이다.

구체적인 방안으로는 긴급상황시 경찰책임자의 독자적 판단으로 긴급압수 혹은 긴급수색을 명할 수 있는 권한을 강화해야 할 것이다. 또한 경찰관직무집행법 제7조(위험방

지를 위한 출입)에 있어 사이버범죄의 대응과 관련된 규정을 보완, 신설하여 보다 긴급한 사항에 대처할 수 있는 법, 제도적 측면에서의 지원이 필요할 것이다. 물론 이러한 경우 경찰이 개인정보를 함부로 침해할 수 없도록 하는 법률의 규정 및 제한장치를 동시에 규정해야 할 것이다(조병인, 2003).

2) 정보통신업계의 역할 및 협력 강화

앞서 언급한 바와 같이 사이버범죄는 정보통신부 관련 기관이나 기타 형사사법기관의 대응만으로는 이루어질 수 없기 때문에 경찰과 정보통신업계의 협력은 매우 중요한 요소이다.

그러나 정보통신업계와의 협력이 법, 제도적으로 정착되지 않고 자율에만 맡겨둔다면 실질적인 협력효과는 거양할 수 없을 것이다. 따라서 관련 정부부처와 정보통신업계가 실질적으로 사이버범죄에 대한 공동대응체제를 구축하기 위해서는 정보통신업계의 역할을 보다 강화하고, 강제성을 두는 방안이 필요할 것이다.

이러한 정책의 일환으로 해킹 등의 사이버범죄 피해가 국가기관은 물론 민간기업에도 확산되는 것을 방지하기 위하여 2004년 8월부터 주요 인터넷 서비스제공업체(ISP), 인터넷데이터센터(IDC) 등을 대상으로 해킹사고 신고를 의무화한 조치는 상당히 긍정적인 조치로 평가받을 수 있을 것이다.

하지만 이러한 제도적 장치가 해킹 등에 국한되어서는 안 될 것이며, 특히 개인정보의 유출방지 및 보호의무를 부과할 필요가 있다. 또한 경찰 등의 수사에 적극적으로 협조하도록 하는 의무를 부과하는 방안, 그리고 관련 통신자료를 보관해야할 의무 등도 고려해야 할 것이다.

3) 국제형사사법 공조의 강화

사이버범죄의 특성상 국제적 형사사법 공조는 사이버범죄의 대응에 있어서 매우 중요한 요소라 할 수 있다. 이에 경찰청에서는 연간 100여건에 달하는 사이버범죄를 국제적 공조를 통해 해결하고 있다.

구체적인 공조방식으로는 공식적인 루트로서 인터폴 등 각종 국제형사사법기구와 협력하고 있으며, 국제컴퓨터범죄회의의 주관 및 참여 등으로 활동무대를 넓히고 있으며, 각국의 사이버범죄 수사관과 24시간 Contact Point를 유지하고 있다. 그리고 수사관간의 상호 정보교류를 위하여 교환방문 등을 실시하고 있으며, 실제 주요사건들의 경우 수사관들이 현지를 직접 방문하여 자료교환 등을 실시하고 있다.

한편 비공식적인 루트로서는 국제회의 등을 통해 익힌 수사관간 개인 연락처를 통해 수사채널을 확보하고 있다.

그러나 경찰은 이러한 공조체제 구축에도 불구하고 아직은 국제형사사법체제에서 중요한 위치를 차지하고 있지 못하며, 정보를 제공받는 위치에 머물러 있다고 할 수 있기 때문에 보다 적극적인 태도를 통한 위상강화 및 주도적 역할의 수행이 요구된다.

따라서 우리나라의 사이버범죄 대응 위상에 걸맞게 국제사회에서의 리더역할을 수행하도록 여러 정책을 수행해야 할 것이며, 향후 국제회의에서의 사례발표를 통한 국제적 인지도 강화, 국내의 해결사례를 통한 수사기법의 전수, 타 국가의 사이버수사관 전수교육 등을 실시함으로써 단순 참여자가 아닌 리더로서의 역할을 수행해야 할 것이다.

4. 단속활동의 적정화

1) 범죄신고율 제고

모든 범죄사건이 그러하듯 사이버범죄에 있어서도 피해자 혹은 일반 시민의 신고는 범죄해결에 절대적인 역할을 차지한다. 그러나 아직까지 사이버범죄에 있어서는 높은 범죄신고율을 확보하고 있지 못하며, 이에 따라 경찰이나 관련기관의 수사에 의존하는 경향이 높다.

앞서 제5장에서 살펴본 바와 같이 사이버범죄의 피해자들이 신고를 하지 않는 이유는 대략 피해의 경미, 신고절차의 세분화로 인한 피해신고 절차에 대한 무지, 범죄구성요건에 대한 미인식 등에서 기인하는 바가 크다.

그러므로 범죄신고율을 제고하기 위해서는 이와 같은 요인들에 대한 경찰의 적절한 대책이 요구된다고 할 수 있는바, 피해자나 일반 시민에게 보다 간단하게 신고할 수 있는 절차적 개선과 함께 경미한 사이버범죄라 할지라도 시민들이 적극적으로 신고할 수 있

도록 사이버범죄의 위험성에 대한 교육 및 사이버범죄가 구성되는 요건 및 피해구제절차 등에 대한 계몽활동을 병행해야 할 것이다.

또한 앞서 언급한 바와 같이 정보통신업계에 대한 강제적 규정을 통해 신고를 의무화하도록 하여 사이버범죄를 조기에 진압할 수 있는 체제를 구축해야 할 것이다.

한편 경찰에서는 신고자에 대한 포상규정도 신설, 확대할 필요가 있다. 특히 국가기관망의 해킹이나 중요 전자상거래 관련 사기, 사이버성매매 등 중요성이 높은 범죄의 경우 경찰차원에서 신고자에 대한 적극적인 포상규정을 신설하여 신고율을 제고하는 방안도 효과적일 것이다.

2) 엄정한 법집행

사이버범죄는 일반 격정범 보다는 고의적인 의도로 지능적, 계획적으로 이루어지는 경우가 많다. 그러나 일반적으로 경찰은 오프라인상에서의 여타 강력범죄에 비하여 범죄예방에 있어 소홀히 하는 경향이 많으며, 사후 법집행에 있어서도 우선순위로 취급하지 않는 경우가 많다.

하지만 사이버공간에 있어서도 심각한 물적 피해를 가져올 수 있는 사기가 성행하고 있으며, 청소년들을 대상으로 하는 각종 성범죄가 만연하고 있다. 또한 이러한 범죄 이외에 모든 범죄의 매개체가 될 수 있는 여지를 내포하고 있기 때문에 보다 엄격하고 강력한 법집행이 요구된다고 할 수 있다.

그러므로 경찰에서는 일반 강력범죄와 마찬가지로 사이버범죄에 대하여 보다 신속하고 확실하게, 그리고 보다 엄정하게 법집행을 할 수 있는 태세를 유지해야 할 것이며, 이러한 태세를 유지할 수 있도록 각종 자원의 투입에 아낌이 없어야 할 것이다.

5. 기타 발전적 조치

1) 사이버패트롤의 강화

사이버범죄 피해자나 일반 시민들의 신고 이외에 사이버범죄에 적극적으로 대처하기

위해서 경찰은 사이버패트롤을 보다 강화할 필요가 있다. 현재 정보통신부에서는 민간의 지원을 받아 사이버패트롤제도를 활발히 시행하고 있는데 비하여 경찰은 자체 인력에 의존하여 사이버패트롤을 실시하고 있다. 따라서 경찰은 자체업무가 과중됨과 동시에 사이버 공간에서의 효과적인 순찰활동을 실시하지 못하여 사이버범죄를 미연에 방지하지 못하고 있다.

모든 범죄에 있어서와 같이 패트롤, 즉 순찰활동은 범죄예방의 중추적인 역할을 담당하는 것이며, 이러한 점은 사이버범죄에 있어서도 같은 것이다. 사이버상에 나도는 불건전 유해정보나, 각종 성매매, 그리고 해킹 등 사이버범죄를 미연에 방지하기 위해서는 경찰이 자체 인력 증원을 통한 순찰인력을 증원함과 동시에 민간부문의 역할을 증대시켜 보다 효과적인 사이버패트롤이 이루어질 수 있도록 해야 할 것이다.

2) 시민사이버경찰제도의 활성화

위에서 언급한 바와 같이 경찰의 효과적인 사이버범죄 대응을 위해서는 시민들의 참여가 절대적인 것이며, 시민들의 활발한 신고 및 순찰활동이 경찰활동에 있어 큰 보탬이 되는 것은 의심할 여지가 없을 것이다.

특히 이러한 시민참여를 유도하기 위해 경찰이 활성화시킬 수 있는 것이 '시민사이버경찰제도'이다. 이와 같은 제도는 시민에게 명예직으로서의 시민경찰관을 부여함과 동시에 제한된 부분에 있어서나마 사이버범죄를 감시할 수 있는 권한을 주어 시민들이 능동적으로 사이버범죄에 대응할 수 있는 토대를 구축해줄 수 있는 제도가 될 것이다.

특히 인터넷 사용인구가 많은 청소년들과 20대 등 젊은층을 중심으로 대단위의 시민사이버경찰관을 위촉하여 본인의 주변에서부터 미연에 사이버범죄를 예방하고 감시할 수 있는 체제를 구축해야 할 것이다.

또한 나아가 활발한 활동을 펼치는 시민사이버경찰관에게는 각종 포상과 더불어 사이버전담 경찰관으로 특별채용 할 수 있는 제도를 마련한다면 시민들의 참여는 보다 극대화될 수 있을 것이다.

제7장 결 론: 인터넷을 이용한 청소년범죄의 대응을 위한 새로운 대응체제의 모색

지금까지 본 연구에서는 인터넷을 이용한 청소년범죄에 대한 전반적인 실태와 더불어 규제현황 및 관련되는 문제점과 각 주체별 대응방안에 대하여 살펴보았다. 그러나 이러한 개별주체들이 조화될 수 있는 방안에는 아직 일치된 의견이 제시되고 있지 않다. 따라서 본 장에서는 본 연구의 결론에 부쳐, 위에서 나타난 대응실태와 문제점 및 개선방안을 중심으로 인터넷을 이용한 청소년범죄에 대응하기 위한 새로운 대응체제 개편방안에 대하여 논하고자 한다.

제1절 이원적 대응체제로의 전환

사이버범죄, 특히 청소년의 인터넷범죄를 예방하기 위해서는 새로운 대응체제로의 개편이 요구된다. 현재 개별 대응 주체들은 개별업무가 중복되고 유관기관별 공조체제가 제대로 유지되고 있지 않아 사이버범죄에 대한 대응능력의 저하와 자원의 비효율적 운용이라는 문제점을 노출시키고 있다. 그러므로 보다 강력한 대응체제 구축과 대응자원의 효율적인 활용을 위해서는 현 체제를 개편하여 보다 새로운 형태를 가진 대응체제로의 재편이 요구된다고 할 수 있다.

일각에서 제기되고 있는 대안은 전체적으로 사이버범죄 및 사이버테러 등 모든 사이버관련 불법 행위들을 총괄할 수 있는 일원화된 전담기구의 설치이며, 이와 같이 일원화해야 한다는 목소리에 대한 제도적 장치로 출범한 것이 국가정보원의 국가사이버안전센터이다. 국가사이버안전센터는 '국가사이버안전메뉴얼'을 배포, 사전 예방 활동을 강화하고 국내외 각종 위협 정보를 종합 분석하는 역할을 수행하고 있으며, 재정경제부, 국방부, 행정자치부, 정보통신부, 대검찰청, 경찰청 등 유관부처 관계자들과 한국정보보호진흥원, 국가보안기술연구소 전문 인력들이 합동 근무하는 체제로 운영되고 있다. 따라서 국가정보원의 국가사이버안전센터는 그야말로 사이버테러 방지를 위한 국가적 역량을

총괄적으로 이끌어낸 조직이라 할 수 있다.

그러나 국가정보원의 국가사이버안전센터는 주로 안보 및 공공부문 등 국가전체의 사이버테러와 관련된 측면의 역할을 수행하고 있다는 점에서 또 다른 대책이 요구된다고 할 수 있다. 물론 최근 일어난 정부 및 각종 공공기관 해킹 사건으로 인해 국가적 위기감이 감돌았고, 따라서 이에 대한 총괄적인 대응체계로서의 국가사이버안전센터의 역할은 적절한 것이다.

하지만 국가사이버안전센터에서 가지고 있는 중요한 문제점은 해킹과 바이러스 유포 등의 네트워크와 관련된 부분의 사이버범죄가 아닌 일반 사이버범죄 전체를 포괄하지는 못하고 있다는 점이다.

이러한 원인에 기인하여 현재 일반 사이버범죄의 경우 경찰, 검찰, 정보통신부 산하기관, 민간단체 등 수 많은 기관에서 담당하고 있으며, 이에 따라 신고창구도 분산되어 효과적인 대응을 저해함은 물론 사이버범죄 피해자가 구제받을 수 있는 제도적 장치의 마련이 어려운 실정이다.

한편 경찰은 사이버범죄에 대한 대응을 위하여 2004년 10월 현 '사이버테러대응센터'를 '사이버테러대응단'으로 확대 개편하여 보다 강력한 사이버범죄 대응체계를 구축하고자 하는 노력을 보이고 있다. '사이버테러대응단'은 경무관을 단장으로 하는 110명 규모의 대규모 조직으로 각 과는 사이버테러 예방, 해킹 대응기술 개발, 인터넷범죄 수사, 국제공조 등 전문영역을 갖게 되어 사이버범죄에 보다 효과적인 대응체제를 갖게 된다.

따라서 결론적으로 본 항에서 논하고자 하는 새로운 체제의 핵심 사항은 사이버범죄 대응체제를 현재의 다원적 대응체제에서 이원적 대응체제로 전환하는 것으로써, 이러한 이원체제는 현 상황에 비추어 경찰과 국가정보원을 중심으로 이루어지는 것이 효과적이라 할 수 있는 것이다.

미국의 경우에는 사이버범죄에 대응하여 여러 기관이 있기는 하나 주로 CIA와 FBI 내에 설치된 'NIPC'(국가기반시설보호센터, National Infrastructure Protection Center)가 주도적인 역할을 담당하고 있다. NIPC는 1998년 2월 대통령 행정명령 제63호로 발령된(PDD-63) '중요기반구조에 대한 클린턴 행정부의 보호정책'에 의하여 창설되었다. 미국내 국가의 주요기반시설을 대상으로 이루어지는 사이버 공격 및 물리적 공격을 탐지·예방하고 그 취약점을 평가·경고하는 업무와 범죄행위가 구체적으로 발생

할 때 수사하는 것을 주요 임무로 하고 있다.

이와 같은 NIPC는 FBI가 주축이 되고 USSS(United States Secert Service)와 국방성을 비롯한 각 연방기관에서 파견된 컴퓨터 수사전문가로 구성되어 있는 합동기구이며, 국가기반을 운영하는 정부의 각 기관이나 민간기업·단체와 긴밀한 연락망을 구축하고 있어 사이버범죄에 있어서의 중추적인 역할을 담당하고 있다.

이와 같이 미국은 우리와 같이 다양한 기관에서 사이버테러 및 범죄와 관련된 역할을 수행하지만, 중심적인 기능은 소수의 기관에서 담당하고 있다. 따라서 한국에 있어서도 이원화된 중심체제로의 개편이 필요한 것이다.

전술한 바와 같이 경찰은 '사이버테러대응단'을 창설할 예정이며, 인원도 대폭 확충하고 전문성을 높여 사이버범죄에 대한 효과적 대응을 위한 인프라를 구축하고 있다. 반면 국가정보원은 사이버테러에 있어서의 국제적 대응체제를 구축하고 있다. 그렇다면 현재의 체제를 개편해야 한다는 일관된 요청 속에서 나올 수 있는 대안은 사이버범죄 대응에 있어서의 경찰과 국가정보원으로의 '이원화' 이다.

제2절 이원화 체제의 구체적인 모형

현재 다원화되어 있는 사이버범죄에 대한 대응체계를 이원화한다는 것은 상당히 어려운 일이 될 것이다. 특히 이원화에 따른 관련 기관의 반발이 예상되며, 이원화되는 양 기관, 즉 국가정보원과 경찰의 업무배분에 있어서도 상당한 마찰이 생길 것이 분명하기 때문이다. 그러나 사이버범죄에 대하여 전체적인 사항을 포괄할 수 있는 체제, 즉 현실적으로 일원화가 어렵기 때문에 이원화해야 한다면 다음과 같은 모형으로 설치될 수 있을 것이다.

1. 사이버테러 및 국가기간망 보호를 위한 국가사이버안전센터

먼저 국가정보원의 국가사이버안전센터는 국가전반의 기간망 보호를 위한 각종 해킹 및 바이러스에 대한 정보수집 및 대응, 그리고 향후 치열할 것으로 예측되는 '사이버戰'을 대비

한 국가적 역량강화 노력 등에 집중하게 된다. 따라서 국가사이버안전센터는 국내 보다는 주로 국제적인 측면의 사이버테러 방지 업무를 수행하게 되는 것이다. 특히 이와 같은 점은 국정원이 궁극적으로 나아가야 할 방향인 해외정보수집 업무에 치중하게 된다는 점과 일맥상통하게 되어 오히려 국정원 본연의 임무에 보다 부합되는 것일 것이다.

2. 사이버범죄 대응을 위한 경찰 중심의 새로운 대응체제

국가정보원의 국가사이버안전센터의 경우 본연의 역할 범위 안에서 조금 축소된 역할을 수행한다는 점에서 이원화에 따른 부작용을 최소화할 수 있을 것이다. 그러나 문제는 경찰 중심의 새로운 대응체계가 어떻게 이루어지느냐에 대한 점이다. 이에 대한 구체적 방안은 다음과 같다.

1) 전담기구로서의 사이버테러대응단

본 연구에서 논하고자 하는 새로운 체제에 있어 경찰의 사이버테러대응단(출범예정)은 현재 정보통신부 산하 관련 기관인 정보통신윤리위원회, 한국정보보호진흥원 등 사이버범죄와 관련된 기능을 수행하고 있는 정보통신 관련 기관의 사이버범죄 대응 역할을 흡수하게 되는 것이다. 물론 이러한 경우 조직 자체를 흡수하는 것은 아니다. 다만 관련 인력과 장비 및 기술력을 제공받고 사이버테러대응단 내에서 함께 대응체제를 갖추게 되는 것이다. 따라서 사이버테러대응단은 국내 및 국내와 해외가 연계되어 일어나는 사이버범죄에 대한 총괄적인 대응업무를 수행하게 되는 기구로 변모하는 것이다.

2) IT산업 발전과 관련된 역할의 정보통신부 산하 기관

사이버테러대응단의 업무 확장에 따라 정보통신부 산하 기관은 현재 그들 기관에서 주장하고 있는 수사권 등 사법경찰의 임무가 주어지는 것이 아닌 국내의 IT산업 발전과 관련된 인터넷 침해사고 대응지원, 주요 정보통신기반시설 취약점 분석·평가, 스팸메일 대응 및 개인정보보호 활동, 전자서명인증, 정보보호산업지원, 정보보호정책 개발 및 교육홍보 등의 역

할과 건전한 사이버문화조성을 위한 활동, 불건전유해정보에 대한 모니터링 및 감시활동, 그리고 경찰의 사이버범죄 대응에 필요한 정보제공과 인력, 장비, 기술제공의 역할을 수행하는 것이다. 특히 정보통신부 산하기관의 인력이 파견직으로 근무하는 것은 한계가 있기 때문에, 이들이 정규 경찰관으로 임직할 수 있도록 현재 조금씩 이루어지고 있는 사이버범죄 전담요원으로의 특별채용과 같은 제도적 장치의 마련이 이루어져야 할 것이다.

3) 공소의 제기와 유지 기능의 검찰

현재 대검찰청 인터넷범죄수사센터 등에서 사이버범죄 대응 기능을 수행하고 있는 검찰은 검찰 본연의 임무인 공소제기 및 유지의 임무를 수행하는 체제로 변모하여야 한다. 앞서 언급한 바와 같이 검찰은 현재 신종 사이버범죄 및 고도의 지능형 사이버범죄를 전담한다고 공표하고 있으나 실제로는 경찰과 별다른 차이점이 없으며, 오히려 업무의 중복과 인력의 낭비를 초래하고 있다. 그러므로 현행 수사권과 관련된 현실상 검찰은 수사의 지휘는 하되, 사이버범죄에 수사에 필요한 자원은 경찰에 지원하고, 궁극적으로는 경찰에 수사를 일임하는 형태가 바람직할 것이다. 따라서 검찰은 사이버범죄자에 대한 공소제기 및 유지에 있어 필요한 최소한의 대응인력만을 유지하는 체제로 만들어야 한다.

4) 총괄기구 편성에 따른 획일화된 신고체제 구축

사이버범죄 대응과 관련하여 중복되고 있는 대표적 기관인 정보통신부 산하기관과 경찰이 하나의 기관을 중심으로 재편되면서 이에 따라 단일화된 신고체제가 구축된다. 즉 현재 사이버범죄 유형에 따라 여러 신고체제로 나뉘어 있는 신고번호가 하나의 핫라인 번호로 통합되고,[148] 이에 따라 사이버범죄 신고에 대한 대응도 통일적으로 사이버테러 대응단에서 하게 되는 것이다.

이렇게 될 경우 사이버범죄 피해자의 혼선을 피하고 대응에 있어서도 보다 신속성을 기할 수 있게 될 것이다. 또한 별도의 일원화된 피해구제 창구를 만들어 사이버범죄 피

148) 물론 핫라인 번호 안에서는 음성안내 및 상담원 안내를 통하여 보다 세분화된 사이버범죄 상담 및 신고를 할 수 있는 기술적인 체제로 운영되어야 한다.

해자에 대한 구제활동이 활발하게 이루어지도록 해야 할 것이다.

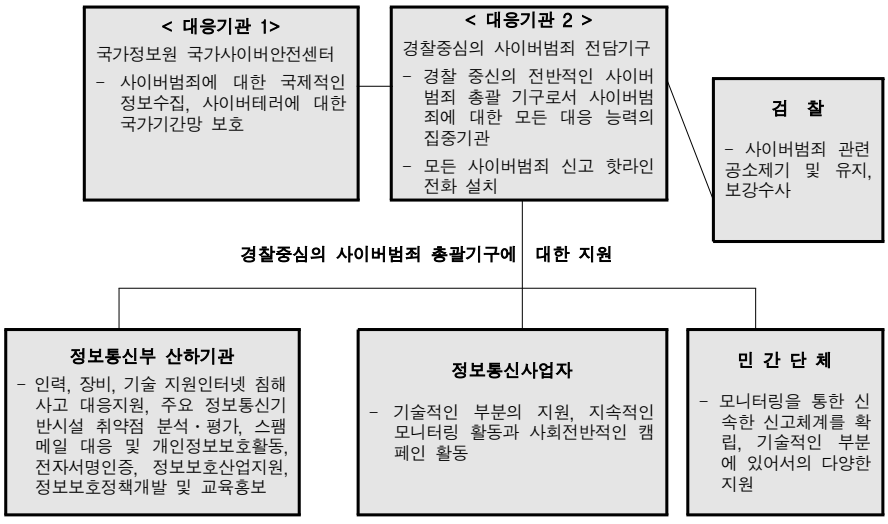
5) 사이버테러대응단과 정보통신사업자 및 민간단체와의 공조체제 구축

사이버범죄를 위한 이원화체제로의 개편에 있어 또 하나의 중요한 부분은 정보통신사업자 및 민간단체와의 협력이다. 현행 대응체제에 있어서도 이들은 중요한 역할을 담당하고 있지만, 만약 대응체제가 이원화될 경우 그 중요성은 더욱 커지게 된다. 특히 경찰을 중심으로 하는 대응기구에는 모든 사회적 역량이 총동원되어야만 그 기능을 제대로 수행할 수 있기 때문이다.

구체적으로 이들의 역할을 살펴보면, 정보통신사업자의 경우 해킹, 바이러스 뿐 만 아니라 모든 사이버범죄에 대한 모니터링을 통한 신속한 신고체계를 확립하고, 기술적인 부분에 있어서도 다양한 지원을 해야 할 것이다. 민간단체의 경우에는 기술적인 부분의 지원과 함께 지속적인 모니터링 활동과 사회전반적인 캠페인 활동을 활발히 하여 사이버범죄에 대한 경각심과 예방 및 대응에 힘써야 할 것이다.

한편 이와 같은 이원화체제로의 개편에 있어서의 구체적인 조직 모형은 다음의 <그림 7-1>과 같다.

<그림 7-1> 사이버범죄 대응을 위한 이원화체제의 모형



제3절 이원화 체제에 따른 양 기관의 인력 증원 및 전문성 제고 방안

사이버범죄에 대한 대응체계를 이원화로 개편함에 있어 핵심적인 부분은 총괄기구의 인력 및 전문성과 관련된 부분이다. 현재 정보통신부가 요구하고 있는 사이버범죄 수사권과 관련하여 정보통신부의 가장 큰 논리적 근거는 경찰의 전문성이 떨어진다는 것이다. 따라서 이원화 체제에 있어 가장 중요한 부분은 총괄기구의 인력증원과 전문성 제고에 관련된 부분일 것이다.

먼저 인력충원과 관련된 부분에 있어 2004년 10월로 개편예정인 경찰청 사이버테러대응단의 인력 110명으로는 현실적으로 총괄적 기능을 수행하기가 어렵다. 따라서 상당히 많은 인력 증원이 필요할 것이다. 그러나 단순한 인원의 증원이 아닌 전문성을 제고한 인력증원이 필요하다. 그러므로 전문성을 기함과 동시에 인력을 증원하기 위해서는 정보통신부 산하 각 기관에 배치되어 있는 컴퓨터 전문가를 본인이 원할 경우 사이버 전담 경찰관으로 특별채용하는 방안이 필요하다.

또한 현재 사이버테러대응단에 소속되어 있는 경찰관들에 대하여 정보통신부 산하 교육기관에서 정보통신 관련 교육을 이수하게 함으로써 전문성을 제고할 필요가 있다. 한편 정보통신부에서 경찰청 직원으로 편입되는 사이버전문요원의 경우 중앙경찰학교에서 소정의 경찰 관련 교육을 받게 한 후 사이버전문요원으로 근무하게 하는 것이 바람직할 것이다. 그리고 본 기관에서 근무하게 될 특별채용외의 신규채용자에 대해서는 초기 입직경로에 있어서 일반 경찰과는 다르게 컴퓨터 관련 수험과목을 채택하여 애초 전문지식을 가진 인원을 선발한 후 별도의 교육기간을 거쳐 채용하는 것이 바람직할 것으로 본다.

제4절 이원화체제의 기대효과

사이버범죄에 대한 대응체계가 현재의 다원화 체제에서 이원화된다면 현재 보다 훨씬 효과적이고 신속한 대응체계를 구축할 수 있을 것이다. 구체적인 내용은 다음과 같다.

첫째, 사이버범죄에 대한 이원화된 대응체계는 현재 보다 전문성을 높일 수 있으며, 보다 신속하게 대응할 수 있을 것이다. 그것은 정보통신 전문가 그룹과 형사사법 전문가

그룹의 결합으로 보다 효과적인 범죄대응이 가능하기 때문이다.

둘째, 자원의 효율적 활용이 이루어진다. 현재 사이버범죄와 관련하여 다수 기관의 업무가 중복되고, 인원과 장비, 예산이 비효율적으로 운용되고 있는 현실에서 국가정보원의 국가사이버안전센터 외의 사이버범죄를 총괄할 수 있는 총괄기구가 신설된다면 현재의 자원을 보다 효과적으로 운용할 수 있을 것이다.

셋째, 통일된 신고체계를 통하여 신고율을 높이고, 이에 따라 적절한 대응을 할 수 있게 된다. 현재의 신고체계는 핫라인 번호 등 신고체계가 분산되어 사이버범죄 피해를 당한 피해자의 입장에서는 신고방법을 몰라 신고하지 못하는 경우가 빈번하게 발생하고 있다. 또한 관련 기관의 대응에 있어서도 같은 사안을 놓고 중복되게 대응하는 경우가 많다. 그러므로 경찰중심의 새로운 총괄기구로 신고창구를 일원화한다면 보다 신고율을 높일 수 있고, 그에 따라 효과적인 대응을 할 수 있을 것이다.

넷째, 사이버범죄 피해자에 대한 구제를 보다 활발히 할 수 있다. 총괄기구에는 반드시 피해자 구제기관이 포함되어야 한다. 피해자에 대한 피해구제가 적절히 이루어지지 못하고 있는 현실에서 총괄기구가 새로이 만들어진다면 피해자에 대한 구제장치가 일원화되고 그에 따라 피해자 구제가 제도적으로 정착될 수 있을 것이다.

참고문헌

1. 국내문헌

강동범. 2000. “사이버범죄와 형사법적 대책.” 사이버범죄의 실태와 대책: 제25회 형사정책세미나. 한국형사정책연구원.

공병철. 2003. “청소년의 인터넷 유료정보 이용에 대한 온라인 결제 문제의 고찰”, 청소년관련 온라인 결제방식 현황 및 개선방안 세미나 발표문, 온라인게임문화포럼.

국가정보원, 『2003 사이버 침해사고 사례분석집』, 국가정보원, 2004.

김성언. 2001. 『개인정보 침해에 관한 조사연구』, 한국형사정책연구원.

김종섭. 2000. “사이버범죄 현황과 대책.” 한국형사정책학회 2000년 동계학술회의 자료.

김준오외. 2003. 『청소년비행론』. 청목출판사, 2003.

류승호. 1998. “정보사회의 윤리: 정보공간의 일탈과 규제.” 정보사회학회편. 정보사회의 이해. 나남출판.

민수홍. 2002. ‘여자청소년의 자기통제력이 비행에 미치는 영향’, 『형사정책연구』 제13권 제1호, 한국형사정책연구원.

백광훈. 2000. 『인터넷범죄의 규제법규에 관한 연구』, 한국형사정책연구원. 사단법인 한국사이버감시단, 2001 한국사이버범죄백서.

서보학. 2001. “인터넷상의 정보유포와 형사책임”, 『형사정책연구』 제12권 제3호, 한국형사정책연구원.

양근원. 1999. “사이버범죄 현황과 대책.” 사이버커뮤니케이션학회. 21세기 도전과 사이버스페이스. ‘99추계학술대회 자료집.

이경훈. 2002. “세계각국의 검퓨터 수사기관의 현황과 역할”, 『컴퓨터 수사와 정보보호』, 대검찰청 중앙수사부 컴퓨터 수사과.

이민식. 2000. 『사이버공간에서의 범죄피해』, 한국형사정책연구원.

이재진. 2000. “사이버공간에서의 표현의 자유와 인격권 보호”. 언론중재 2000년 겨

울호. 언론중재위원회 web zine.

이종원. 2001.「청소년의 인터넷관련 문제행동 실태분석」, 한국청소년개발원.

장상희 역. 2001.「일탈과 범죄사회학」. 도서출판 경문사.

정보통신윤리위원회. 2004. 2003 정보통신윤리백서.

정완. 2000.「전자상거래 관련범죄의 규제에 관한 연구」, 한국형사정책연구원.

정완. 2001. “사이버공간에서의 규제와 자율”, 「형사정책연구」제12권 제3호, 한국형사정책연구원.

정진수 외. 2000.「신종 성폭력 연구 -사이버 성폭력의 실태 및 대책을 중심으로 -」, 한국형사정책연구원.

조병인 외. 2002. “사이버범죄에 관한 연구”, 한국형사정책연구원.

한국 인터넷 통계집. 2002.

허만형. 1999. “사이버범죄에 대한 국가의 정책적 대응방안.” 사이버커뮤니케이션학회. 21세기 도전과 사이버스페이스. ‘99추계학술대회자료집.

황상민・한규석. 1999.「사이버공간의 심리」, 박영사.

2. 외국자료

Cohen, L. E. and M. Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review 44:588-608.

Duff, L. and S. Gardiner. 1996. "Computer Crime in the Global Village: Strategies for Control and Regulation." International Journal of the Sociology of Law 24:211-228.

Hindelang, M. J. et al. 1978. Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Crime. Cambridge, MA: Ballinger.

Kiesler, S. et al. 1984. "Social Psychological Aspects of Computer-Mediated Communication." American Psychologist 39-10.

Luckenbill, D. F. 1977. "Criminal Homicide as a Situated Transaction." Social Problems 25:176-186.

Meyrowitz, J. 1985. No Sense of Place: The Impact of Electronic Media on Social Behavior. New York: Oxford University Press.

Miethe, T. D. and R. F. Meier. 1994. Crime and Its Social Context. Albany, NY: SUNY Press.

Parker, Donn B. 1998. Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley and Sons, Inc.

Sieber, Ulrich. 1986. The International Handbook on Computer Crime. New York:
John Wiley and Sons, Inc.

Thomas, Douglas and Brian D. Loader. 2000. Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. New York: Routledge.

Vold. George B & . Bernard. Thomas J & . Snipes. Jeffery B. 2002. Theoretical Criminology(5th ed.), New York : Oxford University Press.

Wasik, Martin. 1991. Crime and the Computer. Oxford: Clarendon Press.

Wolfgang, M. 1958. Patterns in Criminal Homicide. Philadelphia: University of Pennsylvania Press.

3. 신문기사 등

edaily, 2004년 2월 9일자.

YTN, 2003년 12월 12일, 2003년 12월 18, 2004년 6월 5일.

경향신문, 2003년 12월 5일자, 2003년 3월 12일자, 2004년 7월 15일자.

국민일보, 2001년 12월 11일자, 2000년 4월 26일자, 2004년 4월 14일자.
2004년 5월 30일자, 2004년 7월 7일자.

뉴시스, 2004년 2월 28일자, 2004년 6월 26일자.
동아일보, 2000년 12월 16일자, 2001년 2월 7일자, 2003년 5월 28일자.
매일경제, 2003년 12월 29일자.
미디어오늘, 2003년 8월 1일자.
서울경제신문, 2004년 4월 7일자.
서울신문, 2004년 7월 15일자
세계일보, 2004년 6월 25일자.
스포츠서울, 2004년 7월 21일자.
연합뉴스, 2003년 9월 27일자, 2004년 5월 27일자, 2004년 5월 8일자,
2004년 7월 11일자.
일간스포츠, 2004년 6월 1일자, 2004년 6월 3일자.
전자신문, 2003년 12월 19일자, 2004년 4월 21일자, 2004년 6월 4일자.
2004년 7월 22일자, 2004년 7월 8일자.
조선일보, 2004년 2월 1일자.
중앙일보, 2000년 12월 1일자, 2000년 1월 14일자, 2001년 10월 30일자.
2003년 12월 25일자, 2004년 7월 6일자, 2004년 5월 21일자.
파이낸셜 뉴스, 2004년 2월 4일자.
한국경제, 2001년 7월 18일자, 2002년 12월 29일자, 2004년 5월 2일자.
한국일보, 2004년 5월 7일자.
헤럴드 경제, 2004년 6월 11일자.

4. 인터넷 등

http://health2u.wo.to .
http://www.dci.sppo.go.kr .
http://www.spamcop.or.kr/upload/spam_bb.hwp .
http://blog.naver.com/comsnake.do?Redirect=Log&logNo=80002236580.
http://blog.naver.com/gripis24.do?Redirect=Log&logNo=20003437677.

http://blog.naver.com/vsunna.do?Redirect=Log&logNo=100001643717.

http://cafe.naver/digitalforensic.cafe?iframe_url=/BoardRead.do%3Farticleid= 37.

http://cybercrime.kado.or.kr/cyb/cyb_aft01.asp.

http://icic.sppo.go.kr /b_1_8.htm.

http://kin.naver.com/browse/db_detail.php?d1id=7&dir_id=701&docid=317741.

http://kin.naver.com/browse/db_detail.php?dir_id=710&docid=26740.

http://onyu.net/data/virus1.htm#①.

http://opendic.naver.com/100/entry.php?entry_id=69643.

http://www.antispam.or.kr.

http://www.boho.or.kr/.

http://www.chungju-ch.hs.kr/teacher/%C7%CF%BC%BA%BF%EB/internet/inter 14.html.

http://www.cybercrime.gov/ reporting.html

http://www.cyberparents.or.kr.

http://www.cyberprivacy.or.kr/index_1.html.

http://www.dci.sppo.go.kr/ introdci.htm.

http://www.fkii.or.kr.

http://www.hackersnews.org/data/2003/04/0414_23.html.

http://www.icec.or.kr/.

http://www.istf.or.kr/intro.html.

http://www.itmast.com/internet/concept/ib_expa6.html.

http://www.kado.or.kr/.

http://www.kait.or.kr.

http://www.kiaca.com.

http://www.kiba.or.kr.

http://www.kisa.or.kr/isms/.

http://www.kisis.or.kr/.

http://www.kispa.or.kr.

http://www.kolis/DNlawinfo/casestudy/read.html.

http://www.kopico.or.kr/.

http://www.korwa.or.kr/.

http://www.ktoa.or.kr.

http://www.nic.or.kr..

http://www.pki.or.kr/.

http://www.police.go.kr/ctrc.

http://www.rootca.or.kr/.

http://www.sisters.or.kr/menu5/cyber.html.

http://www.sisters.or.kr/typical/cyber.html.

http://www.spamcop.or.kr.

http://www.survey.com/criminology/lecture/10.pdf.

연구보고서 2004-20

인터넷을 이용한 청소년 범죄의 효율적 대처방안 연구

2004년 9월 발행
2004년 9월 인쇄

발행인 : 류 정 선
발행처 : 치 안 연 구 소
경기도 용인시 구성읍 언남리 88번지
인쇄처 : 대 한 문 화 사
(TEL : (02)2268-0458)