

自動화社會의 犯罪樣相과 法的 對應方案

柳 仁 模*

차 례

- I. 序 言
- II. 컴퓨터 犯罪의 意義
- III. 컴퓨터 關聯犯罪의 動向變化
 - 1. 1980年代 以前의 컴퓨터 關聯犯罪
 - 2. 1980年代의 컴퓨터 關聯犯罪
 - 3. 1990年代 以後 오늘날의 컴퓨터 關聯犯罪
- IV. 法的인 對應方案
 - 1. 刑事法的 規制의 現實
 - 2. 問題點 및 補完點
 - 3. 處罰規定의 新設이나 擴大를 통한 法的 規制의 限界
- V. 社會, 技術的 對應方案
 - 1. 技術的 對應方案
 - 2. 社會的 對應方案
- VI. 結 語

* 市立 仁川大學校 法學科 教授, 法學博士

I. 序 言

19세기 후반이후 급속하게 진행된 우리사회의 발전과 그에 따른 생활 양식과 가치관의 변화는 1990년대이후 본격적인 정보화사회의 도래와 함께 더욱 가속화되었다. 컴퓨터의 보급이 일반화되고 통신기술의 비약적인 발전과 정보통신망이 국제적으로 확산되면서 지구촌의 모습이 시시각각으로 변모되어 가고 있다. 최근에는 특히 정보의 바다라고 불리는 Internet이 Database화된 음성, 화상정보의 자유롭고 신속한 교류를 가능하게 하면서 전화를 비롯한 통신매체, TV, 신문 등의 각종 미디어가 컴퓨터를 통해 통합되어 가고 있다.

요즈음 각 기관이나 기업의 활동이 컴퓨터를 통해 이루어지고 있음은 이미 논의의 여지가 없고, 게임을 즐기는 어린이로부터 학습도구로 이용하는 학생, 예술가나 의사 등의 전문가는 물론 생활정보를 필요로 하는 가정주부에 이르기까지 컴퓨터는 가장 기본적인 도구로 활용되고 있다. 이러한 사회현실에서 범죄자들이 자신들의 범죄수행을 위해 컴퓨터를 이용하기 시작했다는 일은 결코 놀라운 일이 될 수 없으며, 오히려 정보화사회의 가장 전형적이고 직접적인 역기능으로 간주되어야 할 것이다. 컴퓨터를 이용한 범죄는 자동화의 특성이 있으므로 반복성과 계속성을 가지게 되고 따라서 대규모의 경제적 손해를 수반하게 되고, 그 외에도 컴퓨터 이용의 다양화로 인해 사회적, 문화적인 영향력을 초래하게 된다.¹⁾

정보화사회가 계속 진행됨은 곧 우리 사회가 시간적·공간적으로 현실세계(Real Space)와 가상의 세계(Cyber Space)로 나뉘어 병존하게 됨을 의미하게 되고, 이는 곧 가상의 공간에서의 역기능도 현실세계에서와 마찬가지로 발생되어 현실세계로 확산될 수 있음을 의미한다고 할 수 있으며, 既存의 法制度와 司法權에 대한 새로운 도전으로 작용할 것이다. 따라서 세계각국은 정보화된 자동화사회의 폐해와 부작용을 최소화하고 순기능을 극대화할 수 있는 대책마련에 부심하고 있다.

1) 미국의 보험 서비스협회는 미국에서 컴퓨터범죄로 인한 연간 피해액이 95년에 80억 달러에 달하였고, 오는 2000년에는 200억 달러에 이를 것으로 전망하고 있다.

이하에서는 컴퓨터 관련범죄의 생성과 전개양상을 간략히 검토하고 특히 인터넷 등의 세계적인 통신망을 통해 본격적으로 자동화사회로 전개되고 있는 오늘날의 컴퓨터 관련범죄를 중심으로 그 실태와 함께 향후 전망에 대해 검토한 후 現行 法制의 문제점과 효과적인 대처를 위한 刑事法的인 대응방안과 아울러 사회적, 기술적인 대응방안을 검토해 보기로 한다.

II. 컴퓨터 犯罪의 意義

컴퓨터 범죄의 概念에 대해서는 그간 적지 않은 논의가 계속되었지만 아직까지 학문적으로 정확한 개념이 확립되지는 못하였다. 넓은 의미로 컴퓨터를 행위의 수단으로 이용하거나 컴퓨터 자체를 행위의 객체로 하는 모든 유형의 범죄라고 정의하는, 즉 컴퓨터와 관련을 가지는 가벌적 행위의 집합체라고 파악하는 廣義의 概念과²⁾ 컴퓨터의 취약성을 이용하여 컴퓨터와 관련한 정보처리기능과정에 컴퓨터의 부정한 사용형태로 인간이 불법적으로 개입하는 범죄행위이라는 좁은 개념으로 파악하는 견해,³⁾ 혹은 財産犯罪의 영역에서 발생하는 개념으로 국한해서 보기도 하는 반면, 컴퓨터 범죄란 竊盜, 詐欺, 損壞등과 같이 일반적인 구성요건의 집합체에 불과하므로 독립된 법적 개념으로 성격 규명을 할 수 없고, 일반적으로 일컬어지는 別稱에 불과하다는 주장도 있다.⁴⁾

생각건대 컴퓨터 범죄는 컴퓨터와 관련된 刑事法的인 제재의 대상이 되는 일체의 행위라고 포괄적으로 규정함이 가장 일반적인 개념이 되리라고 보지만, 하드웨어나 소프트웨어가 저장된 디스크 자체를 물리적으로 절취, 파괴하는 것과 같이 명백하게 형법상의 범죄행위에 해당하는 경우까지 컴퓨터 범죄의 범주에 넣는 것은 타당하지 않다. 따라서 컴퓨터 범죄는 적어도 컴퓨터 기술에 관한 지식을 전제로 하는 컴퓨터와 관련된 형법상의 불법행위로 그 개념을 정의하는 것이 일응 타당하리라고 본다.⁵⁾ 그러나 오늘날의 현실은

2) Sieg, *Jura* 1986, 352f.

3) 최완진, “컴퓨터범죄에 관한 小考”, 성시탁교수화갑기념논문집, 1993년, 797면.

4) Haft, *NStZ* 1987, 6f.

5) 줄고, “형법개정안의 비범죄화와 범죄화에 대한 연구”, 인천대학교 평화통일연구소 논문집 99면 참조; 같은 취지, 신각철, 『컴퓨터와 법률문제』, 법영사, 1993, 210면.

컴퓨터의 사용이 나날이 일반화 되어 가고 있어 심지어 창작적인 예술의 영역이나 육체적인 활동, 스포츠의 영역에 이르기까지 사실상 오히려 컴퓨터를 이용하지 않는 영역을 찾기가 그리 쉽지 않다고 할 만큼 광범위하게 활용되고 있고, 컴퓨터 자체는 원래 목적상 범죄적인 것이 아니고 컴퓨터와 관련된 법익침해행위가 컴퓨터 범죄의 내용이 될 수 있는 것이므로 컴퓨터를 이용한 일체의 유형이 컴퓨터 범죄로서 정의될 수 있다고 전제할 때 오늘날 컴퓨터 범죄라는 개념은 점차 무의미한 개념이 되어 가는 듯한 느낌이 든다. 컴퓨터가 전문인의 전유물이 아닌 일반생활의 도구로 전환되는 것에 비례하여 컴퓨터 범죄의 전문성도 희석된다고 하지 않을 수 없을 것이고, 따라서 독립된 법적 개념으로서의 컴퓨터 범죄개념은 과도기적인 개념으로 더 이상 불필요한 것으로 보아야 할 것이다. 다만 컴퓨터를 통해 이루어지는 범행이 전통적인 범죄와 구분되는 몇 가지 특성들, 즉 영속적이고 반복적인 범행, 또한 공간적 제한 없이 광역성을 가지고 있기 때문에 커다란 범죄적 영향력을 가지고 있으면서도 범죄의 적발과 증거가 대단히 곤란하고, 컴퓨터 범죄가 대부분 영웅심의 발로나 단순한 유희에서 비롯되어 범죄의식이 희박하다는 점 등이 공통적으로 나타나 있으므로 컴퓨터 기술의 이용을 전제로 재산권, 인격권, 국가적 법익에 대한 침해행위를 넓게 컴퓨터 관련범죄라고 유형화하는 것이 바람직하게 생각된다.

Ⅲ. 컴퓨터 關聯犯罪의 動向變化

컴퓨터 관련범죄는 컴퓨터 기술의 발전 양상과 보급정도에 비례하여 그 유형이 변화되어 왔는데 1960, 70년대에는 대형 컴퓨터를 중심으로, 1980년대에는 개인용 PC를 이용한 컴퓨터 범죄유형이 생겨나기 시작하였으며, 90년대에는 데이터베이스 산업과 통신망의 발전에 따른 네트워크 범죄로 그 양상의 변모를 가져왔다.

1. 1980年代 以前의 컴퓨터 關聯犯罪

1980년대 이전에는 컴퓨터의 사용이 극소수의 전문가에게 제한되어 있었고 일반인의 인식 속에 자리잡은 컴퓨터란 대단히 신비스런 기계라는 정도이

었으므로, 컴퓨터 범죄의 개념을 외부에서 인식하기조차 어려운 시기였다. 따라서 이 시기의 컴퓨터 범죄는 극소수의 내부전문가에 의해서만 자행될 수 있는 대표적인 화이트칼라범죄로서 암수율도 대단히 높았을 뿐 아니라 경제 분야를 중심으로 제한적으로 발생될 수 밖에 없었다. 우리 나라 최초의 컴퓨터 범죄로 기록된 1973년 10월 과학기술처 중앙전산실의 프로그래머가 서울 반포의 AID차관 아파트 입주 추첨과 관련하여 프로그램을 조작한 사건이래 주로 내부전문가에 의한 컴퓨터스파이와 컴퓨터의 부정조작범죄(Computer-manipulation)를 중심으로 유형화된다.

2. 1980年代의 컴퓨터 關聯犯罪

1980년대는 컴퓨터 기술의 질적인 변화를 경험한 시기였다. 1970년대 후반부터 개발되기 시작한 개인용 PC는 1980년 IBM PC가 개발되어 전세계적으로 급속하게 확산되고 일반인의 활용이 폭발적으로 늘어나면서 컴퓨터의 개념에 대한 수정과 함께 일반인을 대상으로 한 컴퓨터 범죄의 개념이 비로소 형성되게 된다. 뿐만 아니라 컴퓨터의 기술을 응용한 기기들이 무수히 개발되면서 컴퓨터 범죄의 특징이 만들어지고, 컴퓨터 범죄도 프로그램의 무단 복제, 컴퓨터 파괴, 개인용 데이터의 무권한 이용, 부정조작을 통해 증명력 있는 정보의 위작, 변작과 같은 데이터의 불법한 변경, 컴퓨터 바이러스의 사용과 데이터의 삭제등과 같은 손괴등의 유형과 이들 유형을 통해 이루어지는 데이터의 부정한 출력과 개인정보침해, 재산상의 이익의 취득을 내용으로 하는 컴퓨터사기등의 재산범죄 및 Computer Sabotage와 같은 업무방해, 신용카드 남용 등의 내용으로 유형화할 수 있다. 또한 이러한 범죄유형과 특성에 따른 법적인 대처방안들이 논의되기 시작하고 각국이 앞다투어 법적인 보완장치들을 마련하게 됨으로서 형사법분야에도 컴퓨터 범죄라는 새로운 장르가 생기게 된다.

3. 1990年代 以後 오늘날의 컴퓨터 關聯犯罪

1990년대에 들어오면서 컴퓨터기술은 통신망과 각종 미디어의 통합과정을 통해 또 한번 질적인 변화를 경험하게 된다. 사회의 정보화가 급속히 이루어지고 데이터베이스 산업의 비중이 커지면서 개인용 컴퓨터와 각 기관과 기업

의 대형컴퓨터가 연결되게 되고 대형시스템에 수록된 데이터베이스가 개방화 되게 되었고, 세계적인 통신망의 연결을 통한 정보의 바다 Internet이 일반화됨으로서 점차 컴퓨터 사용의 핵심이 정보매체, 정보전달자의 기능을 중심으로 형성되게 되었다.

전 세계적으로 Internet을 사용하는 사람은 이미 4,000만명을 넘었고, 인터넷을 통한 경제교류도 연간 7억달러, 오는 2000년에는 20억달러에 달할 것이라고 한다.⁶⁾

따라서 컴퓨터 범죄의 양상도 데이터베이스범죄, 네트워크범죄의 형태로 나타나게 되면서 대표적인 범행으로 Computer Hacking, Computer Virus, 도청의 수법들이 단독 또는 결합적인 형태를 띄고 나타나게 된다. 뿐만 아니라 Internet을 통한 범죄유형들은 전통적인 범죄영역으로 확산되어 점차 일반 범죄화하는 내용으로 변모하게 된다.

(1) Computer Hacking

컴퓨터 해킹이란 권한없이 데이터의 탐지, 사용, 파괴 혹은 시스템의 부정 조작을 통해 정상적인 작동을 방해하거나 재산상의 이득을 취할 목적으로 타인의 컴퓨터 시스템이나 데이터에 침입하는 행위를 의미하는데 데이터베이스 산업의 비약적인 발달과 통신망의 확산으로 인해 오늘날 가장 중심적인 형태의 컴퓨터 관련범죄라고 할 수 있다. 해킹은 60,70년대의 내부 전문가에 의해 자행되던 것이 90년대에 오면서 개인용 PC의 보급이 급속히 가속화되고, Network의 연결을 통해 일반인에게까지 확대된 것으로 정보전달매체의 기능을 중심으로 컴퓨터의 활용이 이루어지는 현실에 비추어 볼 때 앞으로도 더욱 다양한 형태의 침투가 예상된다.

해킹은 통신망의 운영체제나 소프트웨어의 하자를 이용하는 방법과 해킹 프로그램을 별도로 개발하여 행하는 두 가지의 방법이 있는데 최근에는 보안 시스템과 하자보완방법이 발달하여 전자의 방법보다는 의도적으로 전문적인 기술을 통해 통신망에 도전하는 방법이 널리 행하여진다. 뿐만 아니라 최근의 동향을 보면 System의 침입을 전제로 한 패스워드의 분석이 아닌 보완

6) *Die Welt*誌 1996년 2월 28일자 참조: 이 통계수치는 나날히 폭발적으로 증가하고 있고, 또한 인터넷의 분산적인 구조로 인해 정확히 계산을 하기는 무척 어렵다.

프로그램 자체에 대한 도전을 감행함으로써 영웅심을 발휘하려는 유형의 해커들도 다수 발견된다.⁷⁾

컴퓨터 해킹은 범죄의 특성상 광역화된 형태를 띠게 되고, 국제적인 범행으로 나타나는 경우가 많을 뿐만 아니라, 고도의 지능범에 의해 전문적으로 이루어지는 경우가 많아 그 적발과 추적이 매우 어렵기 때문에 이에 대한 대책이 시급한 실정이다.⁸⁾

Internet을 통해 최근에 일어났던 해킹의 국내의 사례를 살펴보면 가장 유명한 사건은 “빠꾸기 알(The Cuckoo’s Egg)” 사건으로 1988년 독일의 한 대학생이 대학의 Internet망을 이용하여 1년여 동안 미국의 방위산업체 전산망에 침투한 다음 군사비밀에 해당하는 각종 정보를 입수하여 소련 KGB에 넘겨주고 그 대가로 마약을 받아왔던 일이 있었고, 통신망에 바이러스를 침투시켜 2000여대의 컴퓨터를 정지시킨 Internet Worm 사건, 은행의 시스템에 침투하여 거액을 부당인출하려했던 CITI Bank사건 등이 있고, 국내에서도 1992년에 해킹을 통한 청와대사칭 사기사건을 비롯하여 최근의 KAIST 대학원생들이 포항공대 시스템의 데이터를 삭제한 사건에 이르기까지 해커들의 활동무대가 점점 확산되고 있다.⁹⁾

(2) Computer Virus

컴퓨터 바이러스는 1985년 처음 출현한 이후 1990년에는 1000여개, 1993년 3000여종이 발견되었고, 1995년 말에는 7400여종에 이르는 바이러스가 세계적으로 발견되었으며, 국내에서도 약 200여종의 바이러스가 발견되고 있다.¹⁰⁾

컴퓨터 바이러스는 생물학적인 세균은 아니지만 프로그래머의 악의에 의해

7) 최영호, 『컴퓨터범죄에 관한 사회제도적 대처방안』, 1996, 형사정책연구원 세미나 자료(정보사회와 범죄), 20면 참조.

8) 미국 FBI 컴퓨터 범죄반의 분석에 의하면 전체 발생하는 컴퓨터 시스템 침입범죄 가운데 약 90% 이상이 적발되지 않고 있다고 추정하고 있고, 미국 국방성의 주관하에 실시한 침입실험의 통계는 침입을 시도한 실험중 95%가 성공한 것으로 나타나 있다.

9) 정진섭, “인터넷과 컴퓨터 범죄 동향변화”, 1996, 형사정책연구원 세미나자료, 63면 이하 참조.

10) 중앙일보 1996년 2월6일, 28면 참조.

오동작을 발생시키고, 데이터손괴 등의 침해를 수반하는 대표적인 컴퓨터 범죄의 범행도구로서 마치 병적인 현상을 일으키는 세균과도 같은 효과를 만들어 내는 것을 의미하는데, 초창기에는 프로그램의 불법복제를 방지하기 위하여 혹은 프로그래머의 장난으로 가벼운 경고적 효과를 내는 것이었으나, 최근에는 엄청난 피해를 주고 있는 심각한 형태의 바이러스 프로그램들이 등장하고 있다.

바이러스 종류가 다양한 만큼 그 침해적 현상도 다양하지만 대개 다음의 3가지 유형으로 구분되는데 컴퓨터에 수록된 데이터를 파괴하는 유형과 운영체계의 작동을 방해하는 유형, 그리고 메모리에 상주하여 자기복제기능과 각종 장애를 지속적으로 반복하는 유형 등이 있으며, 최근에는 3가지의 유형이 복합된 형태로 나타나는 바이러스도 발견된다. 뿐만 아니라 컴퓨터의 활용범위가 넓어지고 운영체계가 다양화되면서 바이러스의 출현양상도 복잡해지고 있다.¹¹⁾ CD-ROM이나 MODEM을 통한 감염과 윈도우 운영체계에서 작용하는 바이러스등 신종 바이러스의 출현은 컴퓨터 사용의 대단한 위협요인으로 등장하고 있다. 뿐만 아니라 Network와 Internet 등으로 PC간의 교류방법이 다양해지면서 바이러스에 의한 피해는 더욱 확산될 것이 예상된다.¹²⁾

한편 바이러스의 퇴치를 위한 연구도 활발히 진행되어 미국과 독일 등의 대학에서 바이러스 연구소를 설치하여 바이러스의 도전에 대해 응전을 하고 있지만 특별한 예방이 아닌 하자 치유의 방법으로 밖에는 대응이 되지 않으므로 여전히 어려운 문제로 남아있다.¹³⁾ 더욱이 우리 나라의 경우는 개인차원의 대처밖에는 이루어지지 않는 점을 감안할 때 국가적 차원에서 체계적인 대처방법을 연구하여야 할 필요성이 강하게 대두된다.

(3) 盜 聽

도청은 흔히 음성에 대한 도청으로 인식되지만 비음성정보의 감청도 중요한 침해의 내용이 된다. 음성에 대한 도청으로는 전화도청외에도 무선송신기

11) Brunnstein, Klaus: *Computer Viren: Stand der Bedrohung, Erkennung, Gegenmassnahmen, Rechtsprobleme*: in jur-PC 1996, S.115f.

12) Brunnstein, a.a.O.

13) Brunnstein, a.a.O.

나 이동전화에 대한 도청이 있고, 비음성정보의 감청으로는 Telex, 무선전신, Faximilie 등 통신자료의 도청과 컴퓨터 네트워크에 대한 도청이 있다. 특히 컴퓨터가 음성, 화상정보를 전달하는 모든 미디어의 통합기능을 가지고 통신망과 연결되게 되면서 컴퓨터통신을 통한 도청, 감청은 더욱 기승을 부리고 있다.

도청은 첩보전이나 상업적인 경쟁의 과정에서 종래에도 성행해 왔던 것이지만 컴퓨터를 통한 통신의 역할이 비약적으로 증대한 현실에서는 개인의 사생활은 물론 산업정보, 국가안보에 관한 정보들까지도 인공위성을 이용한 영상확대장치 등 최첨단 장비에 의해 중요한 침해의 대상이 될 것이다.

한국의 고속철도 수주와 관련하여 독일의 ICE가 프랑스의 TGV에 패배한 이유가 독일의 판매정보를 프랑스 첩보기관에 도청당하였기 때문이라는 주장도 있고, 국내에서도 며칠전 휴대폰의 비밀번호를 통해 통화내용이 모두 도청된다는 사실이 보도되기도 하였다. 또한 작년 10월 러시아에서 인질로 잡혔던 현대전자 직원들을 구출하는데도 최신의 도청장치가 큰 공헌을 하였다고 한다.¹⁴⁾

(4) 인터넷을 통해 확산되는 傳統的인 犯罪領域

모든 종류의 정보유통이 자유자재로 이루어지는 가상공간인 Internet을 중심으로 이루어지는 오늘날의 컴퓨터 관련범죄는 단순히 특정한 영역에 국한되지 않고 전통적인 범죄영역으로까지 점차 확산되어 기존범죄체계에 대한 도전이 되고 있다. 그러나 전세계적인 통신망을 통해 쉽게 익명적으로 이루어질 수 있는 Internet상의 행위들을 추적하여 효과적으로 제재하기란 무척 어려운 실정이고 따라서 Internet을 통해 형성된 가상세계(Cyberspace)는 자유로운 범죄영역이 되어 가는 듯한 인상을 준다. 물론 인터넷은 법으로부터 자유로운 영역은 결코 아니다.¹⁵⁾ 이하에서는 Internet상의 범죄와 관련된 몇 가지만 살펴보기로 한다.

14) 최영호, 전계논문, 34면 이하 참조.

15) Wenning, Rigo: *Das Internet: ein rechtsfreier Raum?*; in jur-PC 1995, S.3321f.

가. 음란물 문제

인터넷의 정보 중에는 아무런 제한 없이 누구나 접속할 수 있는 정보들 가운데도 음란정보를 수록한 뉴스그룹이나, 전자음란잡지 혹은 음란 사이트가 개설되어 있는 경우가 무수히 많다. 뿐만 아니라 세계각국의 음란정보를 제한 장치 없이 청소년들에게까지 무분별하게 제공함으로써 청소년의 정서를 피폐하는 수단으로 전락하고 있다. 따라서 세계각국은 기술적인 차단방법과 법적인 규제방법을 논의하고 있지만 애로점이 많은 것이 사실이며,¹⁶⁾ 우리나라에도 통신비밀보호법에 범죄 수사를 위한 감청이 인정되고는 있으나 음란물이나, 폭력물에 대한 온라인 감청은 불가능하게 되어 있어 문제점이 되고 있다.¹⁷⁾

나. 컴퓨터도박

최근 인터넷에 개장된 도박장에서 전자화폐를 이용하여 국제적인 도박이 성행하고 있지만, 각국마다 도박에 대한 처벌규정이 다르고 단속법규가 없는 국가도 있어 현실적인 규제가 용이하지 않은 현실이다. 뿐만 아니라 도박자체가 익명으로 이루어지는 경우가 많아 속임수 행위를 통해 손해가 발생하더라도 이를 해결하거나 중재할 방법이 없는 경우마저 있어 역시 문제점이 되고 있다.¹⁸⁾

다. 자금세탁의 문제

인터넷의 전자화폐를 통한 대금결재를 통해 마약거래등 불법거래의 대금결재나, 뇌물의 공여를 함으로서 자금원에 대한 추적을 불가능하게 하는 사례들이 발생하고 있다. 전자화폐는 디지털 서명에 의해 거래 상대방의 신원을 노출시키지 않고 금융거래를 가능하게 하는 기술로서 범죄행위를 통해 취득한 금전의 자금세탁의 중요한 수단으로 전락해 가고 있다.¹⁹⁾

16) 독일 검찰은 최근 200여개 이상의 해외 음란사이트에 대한 국외 차단을 요청하였고, 미국은 통신순화법을 제정하여 컴퓨터 관련정보뿐 아니라 영화나 TV 프로그램에 이르기 까지 음란, 폭력성의 정도에 따라 시청등급을 정하고 V칩과 같은 제한수신장치를 부착하도록 하고 있다.

17) 최영호, 전계논문, 16면 참조.

18) Collardin, Marcus: *Straftaten im Internet-Fragen zum internationalen Strafrecht: in Computer und Recht* 1995, S.618ff.

상기한 분야 이외에도 인터넷에 의한 거래를 통한 조세포탈, 컴퓨터 통신을 이용한 명예훼손이나 모욕 등과 같이 컴퓨터를 이용하여 전통적인 범죄를 전개하려는 기도는 계속 광범위하게 확산될 것이다.

IV. 法的인 對應方案

컴퓨터의 등장으로 인해 발생하는 여러 가지 법적인 문제들의 해결을 위해서는 모든 법분야에서 새롭게 규정, 개정의 필요성이 제시되겠지만 이하에서는 범죄현상에 대한 형사법적인 대응방안에 국한하여 간략히 검토하기로 한다. 뿐만 아니라 이와같이 다양화되고 변모된 컴퓨터 관련범죄에 적절하게 대응하기 위해서는 법적인 대응책 이외에도 나날이 모습을 바꾸어 가는 컴퓨터 기술의 습득을 전제로 한 기술적인 대처방안과 사회제도적인, 또한 컴퓨터 범죄에 대한 사회적인 인식재고를 위한 사회교육적인 대처방안등이 함께 병행되어야 한다. 이하에서는 형사법적인 규제의 현실과 문제점 등을 중심으로 점검해 보고자 한다.

1. 刑事法的 規制의 現實

우선 지난해 12월 부분개정되어 1996년 7월 1일부터 시행되고 있는 현행 형법에서는 컴퓨터 관련 범죄현상의 중요한 부분에 대한 처벌규정을 신설하였다. 개정형법은 종래 형법 규정으로는 죄형법정주의에서 파생된 유추해석 금지의 원칙상 컴퓨터 관련 범죄현상으로 인한 행위들을 포함할 수 없었거나, 논란의 대상이 되어왔던 “재물”, “업무”, “문서” 등의 개념을 새로이 확장적으로 첨가 내지 수정함으로서 이를 입법적으로 해결하는 것에 그 주안점을 두었다고 할 수 있다.

그 내용을 살펴보면 사람을 기망하는 사기죄에 컴퓨터의 부정조작을 통해 재물이나 재산상의 이익을 취하는 컴퓨터사기가 새로이 규정되었고, 문서성의 인정여부와 논란이 되었던 전자기록에 대한 전자기록위작변작죄등이 규정되었고, 재물손괴유형의 일환으로 컴퓨터데이터파괴죄와 업무방해의 유형에

19) Sieber Ulrich, *Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen(1)*; in JZ 1996, 428ff.

컴퓨터업무방해죄가 새로이 규정되었으며, 데이터탐지죄가 비밀침해, 컴퓨터 스파이범죄의 범주에 속하는 것으로서 규정되었다. 또한 특별법을 통해서도 전기, 전자통신과 관련한 통신침해 행위는 전기통신기본법, 전기통신사업법, 전파법등에서 규율하고 있고, 소프트웨어나 데이터베이스의 보호에 대하여는 컴퓨터 프로그램보호법을 근간으로 하여 저작권법으로 이를 보충하고 있다. 또한 도청에 대해서는 통신비밀보호법에서 처벌규정을 마련하고 있고, 해킹에 대해서는 1986년에 제정되고 1992년에 개정된 전산망보급확장과이용에 관한법률에 별도로 처벌조항을 마련하여 대응함으로써 컴퓨터 범죄에 대한 직접적인 처벌규정이 어느 정도 정비되었다고 할 수 있다.

따라서 해킹의 방법에 의해 권한없이 비밀장치한 타인의 System에 침입하는 침해행위 자체만으로도 형법 제316조의 데이터탐지죄가 적용될 수 있고, 데이터를 복제, 열람하는 경우에는 컴퓨터프로그램보호법이나 저작권법에 따라 처벌될 수 있다. 또한 개인이나 기업, 국가기밀에 속하는 데이터를 탐지하는 경우에는 비밀침해의 구성요건에 해당될 수 있다. 또한 해킹을 통해 System의 정상적인 작동을 방해하는 경우,²⁰⁾ 또는 업무방해의 위험성이 있는 사람에게 권한없이도 시스템을 사용할 수 있도록하여 주는 경우등은 형법 제314조제2항의 규정에 의해 업무방해죄로 의율할 수 있으며, 해킹의 방법으로 재산상의 이득을 취득한 경우에는 신설된 형법 제347조의2 규정에 의해 컴퓨터사기죄로 처벌이 가능하게 되었다.²¹⁾

또한 고의로 바이러스를 침투시켜 정상적인 정보처리과정에 장애를 초래하게 하는 경우 역시 업무방해죄의 적용이 가능하여졌으며, Data를 손괴하는 경우 형법 제229조제1항에 의해 전자기록 손괴죄에 의한 처벌이 가능하게 되었다. 다만 막대한 피해를 줄 수 있는 컴퓨터 바이러스 프로그램을 제작하는 행위나 이를 제3자에게 공개하거나 전송하는 등의 배포행위에 대하여서는 손괴의 고의를 인정하기 어려운 실정이며, 특히 불법복제 등의 범죄행위의 수행을 조건으로 작동하는 바이러스의 경우는 현행법에 의한 처벌이 불가능

20) 예컨대 System file을 임의로 조작하여 컴퓨터의 작동이 안되게 하거나 논리폭탄 등을 설치하여 일정한 조건하에서 오동작을 발생하게 하는 경우 등을 들 수 있다.

21) 기타 자세한 것은 최영호, “개정형법과 컴퓨터관련 범죄현상”, 법조 1996년 5월호, 50면 이하; 1996년 6월호, 39면 이하 참조.

하다고 할 것이다. 따라서 컴퓨터 사용자의 대부분이 이를 경험하고, 엄청난 피해를 초래하는 바이러스의 제작, 배포행위 등의 위험한 예비행위에 대한 처벌규정도 시급히 마련되어야 할 것이다.²²⁾

2. 問題點 및 補完點

그러나 형법적인 규제의 내용을 살펴보면 몇 가지 문제점과 보완점이 지적된다.

첫째, 실제 발생하는 컴퓨터 관련 범죄현상에 대한 실증적이고 경험적인 연구가 부족한 상태에서 컴퓨터 관련범죄현상에 대한 법률적인 규제를 국가의 기본법인 형법을 중심으로 해결하려고 한 결과 중요한 범죄현상에 대한 규제가 미흡하게 된 점이 있다.

둘째, 컴퓨터의 보안과 관련된 특별법들은 행정부처간의 독자적이고 부분적인 입법이어서 효율적인 대처가 미흡할 뿐 아니라 형법도 체계적이고 통일적인 규제법률로서는 대단히 미흡한 실정이다. 따라서 규제법령의 수는 많아도 법적용을 할 수 없는 범죄행위가 발생하는 허점이 생기게 된다.²³⁾

셋째, 오늘날 컴퓨터 관련범죄의 핵심적인 형태인 해킹에 대해서는 형법 제316조제2항의 데이터탐지죄와 전산망보급확장과이용에관한법률 제22조제1항에서 전산망사업자에게 전산망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 강구할 의무를 부과하고, 이를 침해하거나 훼손하는 자에 대하여는 3년이하의 징역 또는 1천만원이하의 벌금에 처한다고 규정함으로써 일단 전산망을 이용하여 타인의 정보를 절취, 변경, 파괴한 자에 대하여 처벌을 할 수 있는 법적 장치는 갖추었다고 할 수 있다. 그러나 이의 처벌에는 전산망의 보안장치를 할 것이 전제되어 있기 때문에 보호장치가 없이 자신의 비밀을 보관하는 경우는 이 법에 의한 규제대상이 될 수 없다. 이는 마치 봉합되지 않은 편지에 대하여 편지개봉죄를 구성하지 않는 것과 같다. 그러나 컴퓨터의 이용과 정보보완은 항상 반비례관계에 있으므로 지나친 전산보완은

22) 영국이나 스위스에서는 컴퓨터바이러스퇴치법(Anti Viren Gesetz)을 제정하여 이러한 예비행위 등을 처벌하고 있다. 기타 자세한 내용은 Brunstein, *a.a.O.*, 116면 이하 참조.

23) 최영호, 전게논문(컴퓨터범죄에 대한 사회제도적 대처방안), 40면.

상업성을 띤 정보의 이용을 위해 장애가 될 수 있고 따라서 정보에의 접근이 허용되어 있는 경우가 적지 않은 현실에서 보완장치를 전제로 한 규정은 커다란 허점이 되지 않을 수 없다.²⁴⁾

넷째, 컴퓨터 바이러스의 제작과 배포, 통신망의 보안상 취약점이나 암호 해독 알고리즘의 공개, 컴퓨터 통신에 사용되는 비밀번호의 양도 등에 대한 규제 등이 누락됨으로서 현존하는 위험을 제공하는 행위나 정보처리장치의 부정사용에 직접적인 수단을 제공하는 관련자들의 배신행위를 방치하고 있다는 점이다.

따라서 오늘날 실제 발생하는 컴퓨터 관련범죄에 대한 경험적인 연구를 통해 보다 철저한 규정의 보완과 함께 체계적이고 통일적인 규제법의 제정이 필요하며, 이를 통해 압수, 수색, 전자추적의 절차, 전자적 증거자료의 증거 능력과 증명력 등 수사상의 어려움을 해결하기 위한 배려가 함께 이루어져야 할 것이다.

3. 處罰規定의 新設이나 擴大를 통한 法的 規制의 限界

그러나 법적 규제의 내용도 처벌규정의 신설이나, 확장에 국한할 수는 없다. 왜냐하면 상기한 바와 같이 컴퓨터 기술의 비약적이고 지속적인 발달은 범죄의 양상을 나날이 변모시키고 있기 때문이다. 실제로 지난해의 개정을 통해 형법전에 새로이 규정된 범죄유형은 이미 80년대 컴퓨터 범죄유형이 대부분을 이루고 있고, 새로운 범죄현상에 대한 규제는 미흡한 현실을 경험하고 있다. 또한 최근의 컴퓨터 관련범죄의 유형이 형법상의 모든 전통적인 범죄영역으로 확대되고 있음을 부인하기 어렵다. 따라서 컴퓨터 범죄는 더 이상 특수한 영역으로 간주되어 특수한 대응을 하려고 해서는 안될 것이다. 우선 컴퓨터 범죄의 일반화를 개념적으로 실현하고 컴퓨터 범죄라는 개념을 부정한 채 기존 법규정 전반에 걸쳐 컴퓨터 마인드를 해석론으로 실현하여야 하리라고 본다. 따라서 현실의 문제를 직접적으로 규율해야 하는 형법의 과제가 컴퓨터 범죄에 대한 구성요건의 신설만으로서 해결되리라고 기대한다면 이는 대단히 시대착오적인 발상이 될 것이며, 형법학자들과 법조인들의 법해

24) 장영민, 『정보통신망발전에 따른 개인정보보호』, 형사정책연구원 세미나자료(정보사회와 범죄), 1996, 83면 참조.

석의 새로운 기준을 마련하는 작업이 반드시 병행되어야 할 것이다.

정보화사회로 일컬어지는 오늘날 많은 재산적 가치를 지닌 자료들이 온라인 시스템에 의해 공유되는 현실에서 이는 곧 재산상의 침해로 직결되므로 재산범죄의 성립을 배제한 처벌은 의미가 없게 된다. 예를 들어 ID를 우연히 알게 되어 유료정보를 몇 시간 동안 사용하여 진정한 사용자가 사용료를 부과하게 되는 경우에는 재산범죄, 특히 재물을 그 객체로 하는 재산범죄의 성립여부가 문제된다. 컴퓨터의 사용시간은 재산가치를 가지며, 시간의 도용은 귀중한 재산가치의 절도라는 의미에서 소위 시간의 절도(Zeitdiebstahl)라는 개념이 사용되고 있기도 하다.²⁵⁾ 이 경우 정보의 재물성이 문제가 될 수 있다. 형법상 재물의 개념은 본래 민법상의 물건, 가동물건, 유체물의 의미로 파악되다가, 전기의 등장과 함께 도전의 문제가 제기되면서 제346조의 주의규정을 두어 관리가능한 동력도 재물로 간주한다는 규정을 두어 입법적인 해결을 하였다. 그러나 그 후 재물의 개념에 대해 통설적인 개념은 유체물의 개념뿐 아니라 관리가능한 동력을 포함하는 개념으로 변천되었고, 따라서 제346조의 규정은 단순히 주의 규정적인 성격을 갖게 되었다. 그러나 재물의 개념을 관리가능한 동력이란 개념으로 한정할 결과, 정보는 자산가치가 큰 관리가능한 대상임에도 불구하고 재물성을 인정할 수 없다고 보는 것이 지배적인 견해이다.²⁶⁾

물론 정보라는 재화가 물체의 이전을 통해 가치가 함께 이전되는 다른 재물과는 다른 독특한 성격을 가지고 있기는 하지만, 정보화 사회에서 무한한 자산가치를 가지고 있는 정보의 도용문제를 재산적인 침해로 보지 않는다는 것은 커다란 오류라고 할 것이다. 따라서 기존의 재물의 개념 속에 정보를 포함시킬 수 있는 해석이 가능하도록 하던지 아니면 별도의 규정을 신설하여 보호하는 방안이 필요하다. 그러나 새로운 현상이 발생할 때마다 입법적인 해결을 하려고 한다면 형법은 늘 범죄의 뒤를 따라 다니고, 새로운 범죄를 처벌할 수 없는 공백상태를 반복적으로 맞이하게 될 것이다. 따라서 재물의

25) Lenckner, *Computerkriminalität und Vermögensdelikte*, S.25f.

26) 이재상, 『형법각론(新訂版)』, 1996, 228면, “재물은 동력에 제한 되므로 동력이 아닌 정보(Information)는 재물이 될 수 없고 따라서 정보를 알아내거나, 문서를 복사하여 원본은 두고 복사본만 가져간 때에는 절도죄가 될 수 없다.” 고 하였다.

개념을 관리가능한 동력에 국한하지 않고, 재산적인 가치를 가지는 관리가능한 재화라는 개념으로 확대하는 것이 타당하다고 할 것이다.²⁷⁾

이와 같이 법적인 규제의 내용도 새로운 범죄유형에 대한 새로운 처벌이라는 국지적인 대응이 아닌 죄형법정주의가 침해당하지 않는 범위에서 총론적인, 해석론적인 해결을 함께 도모하여야 한다.

V. 社會, 技術的 對應方案

1. 技術的 對應方案

법적인 대응과 함께 병행되어야 할 것은 기술적인 대처방안이다. 처벌규정이 존재한다고 항상 실제로 처벌이 가능한 것은 아니기 때문이다. 해커를 처벌하고 싶어도 아무런 흔적이 남지 않는다면 형사소송법의 증거법의 원칙상 처벌이 불가능함은 자명한 일이다.²⁸⁾ 범행의 적발이 5%도 안되는 현실에서 처벌규정의 존재를 주장함은 무의미하다. 따라서 다각적이고 효율적인 보안 기술의 개발이 무엇보다 시급한 과제이다.

해킹에 대해서는 암호체계와 암호화 기법에 대한 개발을 통해 보호조치를 파괴하는 범죄자보다 기술력에서 우위를 확보함으로써 컴퓨터 해킹에 대한 장기적이고 본질적인 방어대책을 수립하여야 한다. 도청의 원리를 과학적으로 면밀히 분석하여 도청에 대한 감지기술 개발을 위한 노력을 하여야 하고, 컴퓨터 바이러스의 퇴치를 위한 컴퓨터 바이러스의 연구도 개인의 흥미차원이 아닌 국가 정책적으로 심도있게 진행되어야 할 것이다.

2. 社會的 對應方案

컴퓨터 범죄에 대한 또 하나의 효과적인 대응방안은 사회적인 측면에서 제기된다. 우선 Internet을 중심으로 한 Network형태의 범죄는 그 특성상 광역화, 국제범죄화가 불가피한만큼 유관기관의 긴밀한 공조, 관련기관의 연계활동과 국제적 공조의 필요성이 무엇보다도 중요하다. 따라서 필요한 경우

27) 줄고, 상계논문, 100면 참조.

28) 장영민, 전계논문, 83면 참조.

입법을 통해 국제적 사법공조에 관한 별도의 법적 규제가 마련되어야 한다.²⁹⁾

둘째로 컴퓨터 관련범죄에 대한 범죄의식을 확산시키기 위한 노력이 병행되어야 한다. 컴퓨터 범죄를 범하는 자들은 대부분 연령층이 낮고, 범죄의식이 희박하다. 해커들의 경우 그 범행동기가 전통적인 범죄와는 달리 자신의 지식수준을 자랑하려는 잘못된 영웅심의 발로이거나 단순한 유희에서 비롯되는 경우가 많다. 또한 컴퓨터의 조작기술을 즐긴다는 의도 속에 전통적인 범죄에서와 같은 도의적인 자책감이 결여되기가 쉽다. 청와대의 System에 침입했던 해커나, 포항공대와 KAIST 대학원생간의 시스템 침입 해킹사건의 경우에서 보듯이 피해를 본 회사에서조차 그를 영웅시하고 서로 스카웃하려는 현실이다. 심지어 최근에는 해커를 대상으로 놀이마당을 만들어 이벤트 형식으로 상설화하여 침입에 성공한 해커들에게 상금을 지급하는 등 해킹을 양성화하는 경우도 있다고 한다.³⁰⁾ 따라서 해킹이나 컴퓨터 바이러스의 침투등의 컴퓨터 범죄에 대한 사회적인 인식을 전환하고 정보윤리의 확립을 위한 노력이 절실함을 새삼 실감하게 한다.³¹⁾

마지막으로 우수한 수사관의 확보를 통한 범죄의 적발과 추적을 실제로 가능하도록 하여야 한다. 수사기관과 정보통신부 등 유관기관에 해커수사대, 정보보호센터 등의 컴퓨터관련범죄 전담부서가 만들어지고 있지만 컴퓨터마인드와 법적인 지식을 겸비한 유능한 수사관과 전문적인 법조인의 확보는 그리 용이한 일이 아니다. 이를 위해서는 법학을 교육하는 과정에서부터 컴퓨터마인드를 자연스럽게 함양할 수 있는 기회가 확대될 수 있도록 적극적인 고려가 되어야 할 것이다.

VI. 結 語

본격적인 정보화 사회로 들어가는 길목에서 Internet을 통한 가상세계의 범죄들이 현실적으로 나타나기 시작하는 상황을 경험한다. 그러나 법적인 규

29) 장영민, 전계논문, 83면.

30) 조선일보 Good Morning Digital 1996년 8월 24일, 6면 참조.

31) Johnson, Deborah G., *Computer Ethics*, 1994, p.112.

제는 실증적이고 경험적인 연구의 토대위에서 비로소 가능해진다. 나날이 그 모습을 바꾸는 컴퓨터 관련범죄에 대한 법적인 대응방안은 컴퓨터 기술의 발전속도에 비례해서 동적으로 전개되어야 한다.

法理가 절대성을 추구하는 眞理와는 달리 현실적인 규제를 전제로 한 可變的인 합리성을 추구해야 한다면 정보화 사회의 확산으로 형성되게 될 Cyber Space의 법리는 情報法學의 신선한 論理로서 대체되지 않으면 안될 것이다.

따라서 법정보학적인 방법론과 정보법학의 법리들은 새로운 영역의 신선함으로 우리에게 던져진 명제가 아니라 어느새 우리법학의 한가운데로 현실적인 필요성과 함께 성큼 다가와 있음을 감지하게 한다.