成均館大學校 比較法硏究所
成均館法學 第17卷 第2號 2005年 12月
SungKyunKwan Law Review
The Institute for Comparative Legal Studies
Vol. 17 No. 2 December. 2005

컴퓨터犯罪 處罰法規의 再檢討

-美國과 韓國의 立法을 中心으로-

임 석 원*

Ⅰ. 序 論
Ⅱ. 컴퓨터犯罪의 類型
Ⅲ. 컴퓨터犯罪에 대한 立法態度
Ⅳ. 立法의 改正方向
Ⅴ. 結 論

Ⅰ. 序 論

컴퓨터 정보기술의 발달은 컴퓨터를 우리사회 전반에 걸쳐 보급시켜 놓았고 언제 어디서든 컴퓨터를 접하고 만질 수 있는 상황을 만들어 놓았다. 또한 현대인들은 컴퓨터 없이는 업무를 처리할 수 없는 상황에 이르렀다. 이러한 상황은 컴퓨터에 의해 발생하는 범죄도 증가시켰다. 뿐만 아니라 컴퓨터에 의한 신종범죄도 탄생시켰다. 따라서 이러한 컴퓨터범죄에 대하여 기존의 형법으로 규율하여 형벌을 부과하기에는 한계가 있다. 그리하여 이에 대한 대처방안으로 형법은 1995년의 부분개정에서 컴퓨터범죄에 관한 처벌규정을 직접 도입하였다.[1] 그 결과 어느 정도 컴퓨터범죄를 규제

* 성균관대학교 비교법연구소 선임연구원, 법학박사.

1) 물론 1995년 이전에도 컴퓨터범죄를 규율하는 특별법제정의 움직임은 있었지만 컴퓨터범죄가 사회일부분에 국한된 특수계층을 범죄의 주체로 하는 범죄가 아니라 모든 국민이 범할 수 있는 일반적인 범죄가 되었다는 인식을 한 후에야 비로소 형법전에 컴퓨터범죄처벌규정을 두게 된 것이다.

하고 컴퓨터범죄의 일반예방효과를 거둔 것은 사실이다.

그러나 문제는 1990년대 후반부터 불기 시작한 인터넷의 사용이다. 이러한 인터넷의 사용은 1995년의 형법개정에서 마련한 컴퓨터범죄처벌법규로는 규제하기 어려운 또 다른 새로운 범죄유형을 탄생시켰다.[2] 이러한 새로운 범죄유형을 처벌하기 위하여 대처할 수 있는 대응방안은 세 가지가 있다. 그 중 하나인 형법의 개정은 시간이 많이 걸리고 기본법의 개정인 관계로 절차가 복잡하다. 이를 위한 해결방안 중에서 또 다른 하나인 현행 형법의 무리한 확장해석과 유추해석은 형법의 보장적 기능을 침해하고 이를 지키기 위한 대원칙인 죄형법정주의 원칙을 유명무실하게 할 가능성이 있다. 따라서 결국 입법자는 이에 대한 해결책으로 급하게 형사특별법을 제정함으로서 이러한 인터넷등을 이용한 신종 컴퓨터범죄[3]에 대응하게 되었다.

본 논문에서는 우선 컴퓨터범죄의 유형을 먼저 살펴보고 미국과 한국을 중심으로 현행 형법상의 컴퓨터범죄처벌법규와 형사특별법상의 컴퓨터범죄처벌법규상의 컴퓨

---

2) 예를 들면 현행형법 제319조의 주거침입죄의 객체는 사람의 주거·관리하는 건조물·선박이나 항공기 또는 점유하는 방실이다. 그러나 최근 인터넷의 발달과 대중화로 각 개인이 자신의 홈페이지를 만들어 컴퓨터와 인터넷을 통하여 스스로 관리하는 경우가 많이 있다. 이러한 개인이 관리하는 홈페이지에 침입하거나 관리자의 인터넷상의 퇴거요구를 받고도 응하지 않으면 주거침입죄가 되어야 한다. 그러나 형법의 구성요건상의 객체에 명시되어 있지 않음으로 인하여 이러한 행위를 형법으로 규제할 수 없는 문제점이 있다. 또 하나 예를 들면 형법 제309조의 출판물등에 의한 명예훼손의 구성요건적 행위수단은 신문·잡지 또는 라디오 기타 출판물에 의하여 명예를 훼손하는 것이다. 만약 인터넷으로 명예훼손을 한다면 인터넷을 출판물이라고 할 수 없으므로 구성요건적 행위수단에 포함되지 않는다. 이는 제307조의 명예훼손죄로 처벌할 수 밖에 없다. 그러나 인터넷의 공연성을 출판물등과 비교하면 오히려 더 높다고 할 수 있으므로 형벌의 불균형이 생기는 문제점이 있다.

3) 컴퓨터범죄를 명확하게 정의하여 이에 대한 처벌을 법규로서 마련하여 대응한다는 것은 상당히 어려운 일이다. 다만 간단하게 컴퓨터범죄를 정의한다면 "범죄의 수행·수사·기소를 위해서 컴퓨터 과학기술의 지식을 수반하는 형법의 위반" (Marc D. Goodman, "Why the Police Don't Care About Computer Crime", 10 Harvard Journal of Law & Technology, p .465, pp. 468~469); "컴퓨터를 이용한 반사회적 행위 및 컴퓨터의 존재에 의해 나타난 반사회적 행위"(金井 淨, 「コンピュータ犯罪の特質」, 警察學論集 第35卷 第6号, 1982年 6月, 60頁 등으로 정의할 수 있다; 한편 인터넷범죄와 컴퓨터범죄의 차이는 컴퓨터범죄의 행위범위가 인터넷범죄(혹은 사이버범죄라고도 한다)보다도 더 넓다고 보면 된다. 인터넷범죄는 컴퓨터로 범할 수 있는 범죄중의 하나이기 때문이다. 1980년대에는 인터넷을 거의 사용하지 않았기 때문에 컴퓨터범죄를 범한다 함은 주로 전산망을 통한 PC조작이 주를 이루었다. 그러나 1990년대 중반 이후부터는 PC방이 우후죽순격으로 전국각지에 생겨나고 있고 인터넷을 접속하면 세계각지 어느 곳의 홈페이지나 주소로 들어갈 수 있게 되었다. 따라서 기존의 컴퓨터의 전산망을 사용한 방법뿐만이 아닌 인터넷을 사용한 컴퓨터범죄가 주를 이루게 되었다.

터범죄를 규제하고 있는 입법태도를 살펴본다. 그 후에는 바람직한 입법의 개정방향을 구체적으로 모색해보고자 한다.

Ⅱ. 컴퓨터犯罪의 類型

컴퓨터범죄는 범죄의 행위형태에 따라서 편의상 범죄의 객체가 되는 것과 범죄의 주체로 되는 것 그리고 전통적인 범죄를 수행하는 수단으로 사용되는 것 마지막으로 컴퓨터가 범죄에 수반하는 것의 네 가지로 나누어 유형을 분류할 수 있다.[4]

1. 犯罪의 客體

이는 컴퓨터가 범죄의 객체로 되는 범죄유형을 의미한다. 곧 컴퓨터자체가 범죄의 목표가 되는 것이다. 주로 컴퓨터 자체의 절도가 이에 해당된다. 구체적인 절도의 객체로는 컴퓨터 처리장치시간(Computer Processor time)과 전산화된 용역(Computerized Services)의 절도가 대표적이다. 또한 컴퓨터에 손상을 야기시키는 경우도 이 유형에 포함된다.

2. 犯罪의 主體

컴퓨터가 범죄의 주체가 되는 경우의 범죄유형을 의미한다. 이 경우에 컴퓨터는 범행의 물질적 장소가 되거나 독특한 형태의 자산손실의 원인이나 근거가 된다. 이 범주에 속하는 유형은 네 가지가 있다. 우선 대표적인 유형으로 바이러스(Viruses)[5]가 있다. 컴퓨터 바이러스는 자기 스스로 복제하면서 컴퓨터시스템 또는 네트워크를 통하여 퍼져나가는 것이다. 바이러스는 긍정적일수도 있으나 파괴적일수도 있다. 이는 특히 범죄의 주체로서 사용되었을 때 매우 파괴적이다. 어떤 것은 이메일(E-mail)등을 통하여 예상치 못한 화면출력표시(Screen displays)의 원인이 될 수도 있으며, 컴퓨터 파일을 지워 없애기도 하고 잘못된 정보를 창조하기도 한다. 또는 회사내부전산망의

4) 이하의 유형의 분류는 Eric J. Bakewell/ Michelle Koldaro/ Jennifer M. Tjia, “Computer Crimes”, American Criminal Law Review, VOL .38 SUMMER 2001, pp. 484~486의 분류방식과 내용을 따랐다.

5) 한편 Worm도 바이러스와 유사한 유형이다. 그러나 이는 사용자전송파일 없이 컴퓨터내부전산망 안으로 직접 침입할 수 있다는 것이 바이러스와의 차이점이다 (Ibid., p. 485).

컴퓨터 정보처리능력을 없애기도 한다. 이처럼 바이러스는 컴퓨터 파괴의 주된 원인이다.

또 다른 유형으로 트로이의 목마(Trojan horses) 가 있다. 트로이의 목마는 겉으로 보았을 때는 아무런 이상이 없는 프로그램이다. 그러나 이 프로그램은 자유로운 접근이 허용되는 사용자로서 가장된 또 다른 목적을 소지하고 있는 프로그램이다. 따라서 진정한 실제 사용자가 컴퓨터 스크린에 접속했을 때 트로이의 목마 프로그램은 사용자의 이름과 암호를 절도해 간다.

다른 유형으로 논리폭탄(Logic bombs)이 있다. 이는 어느 일정한 때에 또는 특정상황아래에서 데이터를 손상하도록 고안된 프로그램이다. 이 프로그램은 컴퓨터범죄의 주체로서 매우 파괴적이다.[6]

마지막으로 탐지기(Sniffers)가 있다. 탐지기는 전산망분석기라고도 한다. 이는 컴퓨터 네트워크를 보여주거나 네트워크 사이의 연결을 수리하기 위하여 사용되는 하드웨어 장치이다. 이러한 탐지기도 컴퓨터범죄의 주체로서 사용되었을 때는 매우 파괴적이다.[7]

3. 犯罪의 手段

컴퓨터범죄가 더욱 복잡한 방법으로 수행되지만 컴퓨터는 기존의 형법각칙에 규정되어 있는 범죄들 즉 절도죄·사기죄·횡령죄·손괴죄·폭행죄 등의 전통적인 범죄를 수행하는 수단이 될 수 있다. 예컨대, 미국에서 컴퓨터는 전화통신조직의 무권한 사용을 목적으로 한 전화통신암호를 탐지하기 위하여 이용되어 질 수 있다.

4. 犯罪에의 隨伴

마지막으로 컴퓨터가 범죄에 수반하는 경우는 컴퓨터가 어느정도 범죄활동에 연관되어 있기는 하지만 컴퓨터의 사용이 범죄를 범하는데 반드시 요구되지는 않는 경우를 의미한다. 예를 들면 "금융기록같은 증거정보가 마약거래상의 컴퓨터에 저장되어

---

6) 그러나 논리폭탄은 컴퓨터 소프트웨어 회사에 의해 개발된 프로그램 면허협정(licensing agreements)의 침해에 대한 보호를 위하여 일반적으로 사용되기도 한다. 또한 면허의 침해가 발생했다는 경고를 이메일로 보냄으로서 긍적적인 기능을 수행하기도 한다 (Ibid., p. 486).

7) 탐지기역시 네트워크 고안자들이 네트워크에 발생한 문제를 찾고 해결하는 것을 도와주는 작용을 하기도 한다. 이는 긍정적인 면으로 사용되는 면을 보여주는 것이다 (Ibid., p. 486).

지는 것" 등을 의미한다.

Ⅲ. 컴퓨터犯罪에 대한 立法態度

컴퓨터범죄를 규제하기 위한 입법은 다음과 같이 형법에 따른 규제와 형사특별법에 따른 규제의 두 가지 형태로 입법을 제정하고 컴퓨터범죄의 유형에 따라서 각각 다르게 규제해 왔다.

1. 刑 法

(1) 미 연방(聯邦)형법의 입법태도[8)]

미 연방에서의 컴퓨터범죄에 관한 형법의 입법태도는 1984년 의회가 「1984년의 위조접근수단 및 컴퓨터사기·남용법 (The Counterfeit Access Device and Abuse Law in 1984)」을 통과시킨 이래 명백한 연방범죄로서 컴퓨터범죄를 다루어 왔다. 그리고 이러한 입법은 컴퓨터 관련 범죄의 새로운 유형에 따른 양적증가에 따라 이의 규제를 위하여 크게 확대되어 왔다. 그러나 인터넷의 발달에 따른 컴퓨터범죄의 범위가 또 다시 넓어짐에 따라서 미연방은 1994년 「컴퓨터남용 수정법 (Computer Abuse Amendment Act of 1994)」[9)]을 제정하였다. 그러나 이 법도 현실적인 컴퓨터범죄를 모두 다 규제하기에는 중요한 틈새를 내포하였다.

따라서 미연방은 급증하고 있는 컴퓨터범죄를 처벌하기 위한 입법의 범위를 더 늘이기 위하여 기존의 법률에 중요한 변화를 포함한 1996년 「국가정보기반 보호법 (National Information Infrastructure Protection Act of 1996)」[10)]을 통과시켰다. 1996년

---

8) 이하의 미국의 연방형법에 관한 규제법규의 입법형태와 내용에 관해서는 Ibid., pp. 486~491.

9) 1994년의 컴퓨터남용수정법은 그 전의 1986년의 "컴퓨터사기 및 남용법 (Computer Fraud and Abuse Act of 1986)"에 대한 비판점들을 수용하고 이들을 다루려고 시도하였다. 이 법은 연방관계 컴퓨터(Federal interest computers)에 권한없는 접근을 하는 것을 금지하고 있다. 이러한 1994년 컴퓨터남용수정법은 모두 6가지 유형의 컴퓨터관련 불법행위들을 규정하고 있다. 이 법에 관한 자세한 내용은 Xan Raskin/ Jeannie Schaldach-Paiva, 'Computer Crimes', American Criminal Law Review, VOL .33 SPRING 1996, pp. 544~549.

10) 1996년의 국가정보기반보호법은 1984년의 "위조접근장치와 컴퓨터사기 및 남용에 관한 법률 (Counterfeit Access Device and Computer Fraud and Abuse Act)"을 수정한 내용을 포함하고 있다. 이 두 법의 관계에 대하여는 Eric J. Bakewell/ Michelle Koldaro/ Jennifer M. Tjia, op. cit., p. 488.

에 통과된 이 법의 중요한 특징은 기존의 1994년의 컴퓨터남용 수정법하에서는 주와 주 사이에서 발생한 컴퓨터범죄에 대해서만 연방형법이 효력을 가졌지만 1996년의 법은 한 개의 주 내부에서 일어난 컴퓨터범죄에 대해서도 효력을 가지게 되었다. 따라서 같은 주에 위치하고 있는 컴퓨터들 사이에서 발생한 컴퓨터범죄라 할지라도 규율할 수 있는 효력을 가지게 된 것이다.

이 법은 모두 컴퓨터관련범죄의 특별한 행위에 초점이 맞혀져 있으며 일반적으로 컴퓨터파일에 권한없이 접근하거나 권한의 범위를 넘어서 접근하는 것을 모두 범죄로 규정하고 있다. 그리고 정부분류정보를 연속적으로 전송하는 것도 범죄로 하고 있다. 내용을 살펴보면 국가정보기반보호법 제1030조 (a)는 다음과 같은 7개의 주요한 내용을 포함하고 있다. 그 자세한 내용은 다음과 같다.

우선 제1030조 (a) (2)는 권한없이 또는 권한을 초과하여 미국정부의 금융기관 혹은 통상을 위하여 사용되는 사기업체의 컴퓨터로부터 정보를 얻는 것을 금지하고 있다.

제1030조 (a) (3)은 허가없이 미국정부의 각 부서나 국의 개인컴퓨터에 의도적으로 접근하는 것을 금지하고 있다. 이 조문은 미국정부나 혹은 미국정부의 부서는 사적(私的)인 측면에서 컴퓨터를 사용하지 않기 때문에 (즉 공적인 측면에서만 컴퓨터를 사용한다) 불법적인 접근은 정부의 사용에 영향을 미칠 수 밖에 없어서 규제를 가해야 한다는 것을 규정한다.

제1030조 (a) (4)는 어떠한 가치를 획득하거나 기망하려는 의도를 지니고 권한없이 혹은 권한을 초과하여 "보호된 컴퓨터(Protected Computer)"에 접근하는 것을 금지한다. 다만 여기에는 피고가 연간 5,000달러 이하의 가치를 획득하는 것은 제외한다.

제1030조 (a) (5)는 컴퓨터 해킹(Computer Hacking)을 규제하고 있다.[11] 이 조항은 과거의 제1030조 (a) (5)를 개정한 1994년 '컴퓨터남용수정법'에 의해 야기된 많은 문제점들을 해결하였다. 가장 대표적인 해결은 해킹에 관하여 주와 주 사이 통상(Interstate commerce)이나 의사전달을 목적으로 사용되는 컴퓨터에만 규제를 가함으로서 1994년의 법에서 규제되었던 주내부의 기구와 금융기관 컴퓨터에 대한 해커의 공격은 비범죄화하였다. 즉 1996년의 국가정보기반보호법은 주와 주사이·정부·금융기

11) 해킹은 일반적으로 해커(Hacker)의 인터넷상의 범죄행위로 이해되고 있다. 이러한 해커는 컴퓨터 시스템에 권한없이 접근하고자 하는 컴퓨터사용자에게 일반적으로 적용되는 용어이다. 전통적으로 일반적인 해커는 이러한 시스템에 접근할 수 있는 권한을 가지고 있지 않다. 해킹에 관한 자세한 개념과 규제법규에 관해서는 류석준, 「해킹에 대한 규제법규에 관한 연구」, 비교형사법연구 제6권 제2호 , 2004, 189면 이하 참조.

관 컴퓨터들만을 '보호된 컴퓨터'에 포함시킴으로 인하여 이러한 문제를 해결하였다.

과거 1994년 '컴퓨터남용수정법'은 구성요건에서 침입요구를 제거하고 고의나 중과실에 의한 컴퓨터의 침입을 추가하였다. 그러나 이 법의 수정안은 과실에 의한 컴퓨터에 대한 침입자를 규제하지는 못하였다. 1996년 국가정보기반보호법은 이러한 차이점(문제점)을 제1030조 (a) (5) (C)를 추가함으로서 해결하였다. 이 제1030조 (a) (5) (C)는 컴퓨터에 끼친 손해가 무모하게 야기되었던 그렇지 않든 상관없이 '손해(Damage)'[12]를 야기하는 권한없는 접근을 모두 금지하고 있다.

또한 제1030조 (a) (5) (A)는 프로그램·암호·명령의 고의적 전송과 그 결과로서 고의적으로 '보호된 컴퓨터'에 손해를 야기하는(컴퓨터에 대한 접근권한 유무에 상관없이) 행위를 범죄화하고 있다. 그리하여 회사내부직원들과 접근이 허용된 사용자라 하더라도 '보호된 컴퓨터'에 고의적으로 손해를 야기한 것에 대하여 책임을 지울 수 있다. 이 조항은 접근권한 없이 보호된 컴퓨터에 의도적으로 접근하는 것과 무모하게 혹은 과실 기타의 행위의 결과로서 손해를 야기하는 것을 모두 금지한다. 즉 이 규정은 악성 소프트웨어의 전송을 야기하는 해커같은 권한없는 사용자들에 대하여 비록 그 전송이 고의가 아니라 단지 무모함 때문 혹은 과실때문이라고 할지라도 책임을 지우고 있는 것이다.

제1030조 (a) (6)은 주와 주사이 혹은 외국과의 통상에 영향을 끼치거나 정부 컴퓨터에의 권한없는 접근을 허용하는 암호를 제조하여 이용함으로서 거래하는 사기의 고의를 가진 자를 처벌한다.

마지막으로 1996년 국가정보기반보호법에 의해 추가된 제1030조 (a) (7)은 주와 주사이 혹은 외국과의 통상에서 어떠한 가치를 왜곡시키려는 의도로서 '보호된 컴퓨터'에 손해를 야기하는 고의를 가지고 위험을 전송하는 것을 불법으로 규정한다. 즉 이 조항은 회사의 정보를 암호화하거나 그 암호를 푸는 열쇠를 댓가로 돈을 요구하고, 주어진 시스템에 대한 처분특권이 부여되지 않았는데도 그 시스템을 파괴하는 해커와 같은 그러한 범죄들을 규제한다.

1996년의 국가정보기반보호법의 특징은 단순히 권한없는 접근을 포함하는 행위와 피고가 금전적인 목적으로 컴퓨터에의 접근을 이용하는 행위를 세분화하여 구별하고 있다는 데에 특징이 있다. 그 근거는 획득한 정보의 가치가 5,000달러를 초과하거나 혹은 범죄행위 또는 불법행위의 범위 내에서 접근에 의한 침해가 금전적인 획득을

12) 컴퓨터범죄에서 손해의 개념정의는 Eric J. Bakewell/ Michelle Koldaro/ Jennifer M. Tjia, op,cit., p. 490 supra note 4).

목적으로 범하여진다면 경범죄가 중범죄로 바뀌는 것을 중요한 내용으로 하는 데에서 알 수 있다.

한편 제1030조 (g)는 고의적인 컴퓨터범죄의 희생자들에 대한 민사상 구제책을 부여함으로서 컴퓨터에 관계된 범죄를 보고하도록 하는 유인책을 규정한다.

또한 컴퓨터에 대한 접근권한을 가진 다른 기관에서와 마찬가지로 미국의 비밀첩보국(The United States Secret Service)에 수사권한을 부여하는 것을 내용으로 하고 있다.

⑵ 미 각 주(州)형법의 立法態度[13]

1978년에 미국의 각 주의회(State legislatures)들은 애리조나(Arizona)주와 플로리다(Florida)주를 시작으로 하여 컴퓨터범죄를 규율하는 법률을 입법하기 시작했다.[14] 그 이후로 모든 주들은 컴퓨터범죄에 관한 특별형법을 제정하였다.[15] 대략 각 주들의 반가량이 1977년 혹은 1979년의 "연방컴퓨터시스템보호법(Federal Computer Systems Protection Act)"에 근본적으로 근거를 두고 그들의 제정법의 모범으로 삼았다. 반면에 나머지 반 정도의 주들은 앞서의 연방입법과는 큰 관계없는 포괄적인 컴퓨터범죄 관련법규를 제정하였다. 이러한 각 주(州)형법의 규정은 컴퓨터범죄에 관한 정확한 정의와 형벌을 명시적으로 다루고, 그에 따라서 컴퓨터안전의식을 증진시키며 범죄억제를 고양시키는 것을 주요한 내용으로 하고 있다. 또한 컴퓨터범죄에 대한 기소를 더 용이하게 함으로써 일반적인 연방형법규범에 비하여 중요한 사명을 가지고 있다.

---

13) 이하의 미국의 주(州)형법에 관한 규제법규의 입법형태와 내용에 관해서는 Ibid., pp. 516~518; 한편 주 형법전이 다루는 컴퓨터범죄관련영역은 다음과 같은 10개의 영역으로 구분할 수 있다. 이는 어느 한 주석자가 구분한 것이다. ①전통적인 재산개념의 컴퓨터를 포함하는 개념으로의 범죄객체확대 ②컴퓨터 파괴 ③컴퓨터를 도구로 한 방조 및 교사 ④지적재산권 침해범죄 ⑤고의적·무권한 사용 ⑥무권한 복제 ⑦有權限 컴퓨터사용의 방해 ⑧컴퓨터의 불법적인 삽입 또는 훼손 ⑨무권한 접근에 의한 컴퓨터 엿보기 ⑩컴퓨터시스템에 대한 내용물등의 소유물 탈취 의 10개의 영역이 그것이다. 여기에 대한 자세한 내용설명은 Xan Raskin/ Jeannie Schaldach-Paiva, op. cit., pp. 565~566 supra note 9)

14) 이는 아마도 미 연방형법전의 제정으로 인한 컴퓨터범죄의 규제가 성공을 거두지 못했기 때문이라고 생각된다 (Ibid., pp. 562~564).

15) 많은 주 형법에서 나타나는 한 가지 특징은 컴퓨터범죄를 일반적인 유형으로 나눈다. 이는 앞에서 언급한 컴퓨터범죄의 유형의 분류와 거의 같다. "컴퓨터가 범죄의 행위객체(Target)가 되는 경우와 컴퓨터가 범죄의 수단(Tool)이 되는 경우 그리고 컴퓨터가 범죄에 수반(Incidental)하는 경우"의 세 가지로 유형을 구분한다.

또한 각 주의 컴퓨터범죄에 관한 제정법규의 최근의 개혁은 컴퓨터범죄에 관련된 재산을 몰수하는 권한을 각 주에 부여하여 범죄에 사용된 컴퓨터장비의 몰수를 확장하는 규정을 포함한다.

이밖에도 어떤 주는 "일반적인 전화폭력법(General telephone harassment statutes)" 안에 전자통신장치와 컴퓨터를 통합시킴으로서, 그리고 반스토킹법규(Anti-stalking statutes)안에 "동의받지 않은 접촉(unconsented contact)"하의 전자통신을 포함시킴으로서 온라인상의 협박을 범죄화 하여 증가하는 온라인폭행에 대한 우려에 대응하기 시작하였다.

또 다른 주는 컴퓨터범죄자들을 체포하고 기소하는 것이 컴퓨터범죄를 예방하는 것보다 더 어렵다는 것을 인정한다. 따라서 네브라스카(Nebraska)주의 컴퓨터범죄관련 법규는 잠재적인 컴퓨터범죄의 희생자들이 그들 스스로의 안전조치를 실행하는 것을 허용한다. 그리고 로드 아일랜드(Rhode Island)주와 오클라호마(Oklahoma)·조오지아(Georgia)주를 포함한 몇몇 주들은 전보손해배상을 위한 민사소인(Civil cause of action)을 규정함으로서 컴퓨터범죄 피해자들이 스스로 적극적으로 나서게끔 용기를 북돋워 주고 있다.

⑶ 우리형법의 입법태도

우리형법은 1995년의 형법개정이 있기 전까지는 컴퓨터범죄에 대한 대책과 처벌이 필요하다는 것을 인식은 하였으나 이를 직접 형법에서 입법으로 반영하려는 움직임은 보이지 않았다. 그러다가 1995년의 형법개정에 의해서 비로소 컴퓨터범죄를 처벌하기 위한 규정을 신설·보완하였다. 이 때 신설한 조항은 다음과 같다.

첫째, 문서에 관한 죄에서 제227조의 2와 제232조의 2를 신설하여 公電磁記錄僞作·變作의 죄와 私電磁記錄僞作·變作의 죄[16]를 신설하였다. 신설취지는 다음과 같다.

우선 기존의 문서에 관한 죄의 행위객체인 문서는 가독성·가시성이 있었다. 그러나

16) 이 죄의 형법전상의 행위객체는 "공무원 또는 공무소의 전자기록등 특수매체기록"(공전자기록)과 "권리·의무 또는 사실증명에 관한 타인의 전자기록(사전자기록)등 특수매체기록이다. '전자기록'이라함은 일정한 매체에 전자방식이나 자기방식으로 저장된 기록을 의미한다. 전자방식은 帶電시키는 방식으로 이에는 반도체기억집적회로(IC)에 의한 것이 있고 자기방식이란 磁化시키는 방식으로 이에는 자기디스크나 자기테이프에 의한 것이 있다. 즉 전자방식에 의한 것이 컴퓨터내의 ROM·RAM등의 기록이고, 자기방식에 의한 것이 현금카드·전화카드·지하철티켓등의 자기띠부분을 의미하는 것이다 (강동범, 「형법상 컴퓨터범죄규정의 개정방안」, 형사법연구 제22호 (2004년 겨울 특집호), 779면).

전자문서의 일종인 전자기록등은 가독성·가시성이 없을 뿐만 아니라 기록과정에서 기존의 문서처럼 한사람만 참여해서 완성하여 명의인을 남기는 것이 아니라 여러사람이 관여했을 가능성이 농후하다. 결국 일반서면문서에서와 같은 작성명의를 명백하게 얻기가 어려워 문서에 해당한다고 할 수 없다. 따라서 이러한 전자기록을 보호하기 위한 형법적 입법조치가 요구되었다. 이에 형법은 기존의 문서에 관한 죄의 문서를 공문서와 사문서로 나눈 것에 대비해서 공전자기록과 사전자기록으로 나누고 위조·변조및 동행사죄를 처벌하는 기존형법규정에 발맞추어 이의 위작·변작및 동행사(제229조·제234조)를 처벌하도록 입법화한 것이다.

다만 한 가지 특이한 것은 같은 목적범이면서도 기존의 문서의 죄는 "행사할 목적"을 구성요건으로 하고 있는데 반해 공전자기록및 사전자기록 위작·변작의 죄는 "사무처리를 그르치게 할 목적"을 구성요건으로 하고 있다. 이는 전자기록의 특성상 단순한 사용 및 행사의 목적보다는 '증명작용에 實害를 발생시킬 목적'이 있는 경우로 한정하여 해석하려는 취지이다. 이는 데이터를 기존의 방식과 다른 방식으로 저장하기 위하여 기존 데이터에 수정·변경을 가하거나 기존의 데이터처리방식보다 능률적인 사무처리를 위해 데이터에 변경을 가한 경우는 행사할 목적은 있으나 사무처리를 그르치게 할 목적이 없으므로 여기에 해당하지 않는다는 것을 의미한다.[17]

둘째, 제347조의 2에서 컴퓨터등 사용사기죄를 신설하였다. 이 죄는 그 후 시대의 흐름에 맞추어 2001년 12월 29일에 다시 한번 개정되었다. 최근 금융을 비롯한 거래분야에서 대출금의 관리를 비롯한 재산에 관련된 업무가 사람의 개입없이 컴퓨터등 정보처리장치에 의하여 처리되고 재산권이 누적된 전자기록의 사용이 늘어남에 따라서 이를 이용하여 재산상의 이익[18]을 얻는 행위가 증가하게 되었다. 이를 규제하기 위하여 기존의 절도죄나 사기죄를 적용하여 대응할 수는 없다. 이들 행위가 사람에 대한 기망행위나 직접적인 재물의 점유이동을 수반하지 않기 때문에 절도죄나 사기죄를 적용하여서는 처벌할 수 없기 때문이다. 본조는 이러한 범죄행위를 사기죄의 일유형으로 파악하여 처벌하고자 하는 목적에서 신설한 조항이다. 이러한 취지를 살리기 위하여 사기죄의 구성요건인 기망과 착오 그리고 처분행위대신에 '허위의 정보 또는 부정한 명령을 입력하거나 권한없이 정보를 입력·변경[19]하여 정보처리를 하게 함

17) 정성근/ 박광민, 형법각론, 삼지원, 2002, 585면.

18) 사기죄의 객체가 재물과 재산상의 이익인 것과는 달리 본죄의 객체는 '재산상의 이익'에 한정되어 있으므로 본죄는 순수한 이득죄에 해당한다. 재물을 제외한 이유는 기존의 처벌규정인 "절도죄"에 의해서 충분히 처벌이 가능하기 때문에 기존형법의 규정으로는 처벌할 수 없는 경우만을 예상한 것이라고 생각된다 (강동범, 「형법상 컴퓨터범죄규정의 개정방안」, 784면).

으로서' 라는 구성요건을 신설하여 입법화하고 있다.

셋째, 제314조 제2항에서 컴퓨터손괴등으로 인한 업무방해죄를 신설하였다. 신설취지는 컴퓨터의 보급으로 인한 시스템의 확장등으로 인하여 컴퓨터의 중요성이 부각되게 되었다는 데에 있다. 이에 따라서 이러한 컴퓨터시스템을 파괴하거나 기타 불법적인 방법으로 정보처리에 장애를 발생시키는 행위가 빈번하게 되었다. 이를 규제하기 위하여 기존의 업무방해죄를 적용할 수도 있다. 그러나 기존 업무방해죄는 구성요건으로서 '허위의 사실유포및 기타 위계 또는 위력'으로 행위태양이 사람에 대한 직접적 행위형태로 제한되어있다. 따라서 '컴퓨터등의 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타방법으로 정보처리에 장애를 발생하게 하여'라는 행위태양은 처벌이 불가능하였다. 따라서 이러한 행위태양을 처벌하기 위하여 컴퓨터에 대한 가해행위로서 타인의 업무를 방해하는 행위를 처벌하기 위하여 별개의 구성요건을 신설하게 된 것이다.[20]

넷째, 기존의 입법을 보완한 조항으로서는 우선 제141조 제1항에서 공용서류등의 무효죄에서의 범죄의 객체와 제366조 재물손괴등의 죄의 범죄의 객체에 '전자기록등 특수매체기록'을 범죄의 객체로서 추가한 것을 들 수 있다. 최근 전자기록등 특수매체기록은 문서에 대신하여 사회적 증명기능을 하고 있을 뿐만 아니라 정보의 기록·보존기능을 하고 있기 때문에 이용가치를 보호할 필요가 있다. 그러나 전자기록등 특수매체기록을 문서로 보기는 어렵다. 또한 형법상의 재물이 되려면 유체물과 관리가능한 동력이 되어야 하는데 이러한 자료자체를 유체물이라고 할 수 없고, 물리적으로 관리가능한 동력이라고 할 수도 없다. 따라서 이러한 경우의 처벌을 위하여 형법상의 재물과는 별도로 '전자기록등 특수매체기록'을 행위객체로 규정하여 전자기록등의 손괴행위를 처벌할 수 있는 근거를 마련하여 입법화하게 된 것이다.

이 밖에도 역시 기존의 입법을 보완한 조항으로서 제140조 제3항에서 비밀표시무효죄와 제316조 제2항의 비밀침해죄의 객체에 '전자기록등 특수매체기록'을 구성요건에 추가하였다. 그리하여 기술적 수단을 이용하여 그 내용을 알아내는 것을 처벌하는

19) 권한없이 정보를 입력·변경하는 것은 진실한 자료를 권한없이 입력하거나 변경하는 것을 의미한다. 이는 타인의 현금카드를 습득한 자가 비밀번호를 알아내어 자기계좌나 제3자의 계좌로 이체시키는 행위를 처벌하기 위한 것으로 2001년 12월 29일 개정으로 추가된 구성요건상의 행위유형이다.

20) 본죄에 해당하는 행위는 정보통신기반보호법 제28조와 제12조 그리고 정보통신망이용촉진및정보보호등에관한법률 제62조 제5호와 제48조 제3항에 의해서도 처벌된다.

규정을 마련하여 보완하였다. 또한 제48조 제3항에서의 몰수의 객체로서 '전자기록등 특수매체기록'인 경우를 객체에 추가하였고, 제228조 제1항에서 공정증서원본등의 부실기재죄의 객체에 '전자기록등 특수매체기록'을 범죄의 객체로서 추가하였다.

2. 刑事特別法

(1) 미 聯邦 형사특별법[21]

미 연방에서의 형사특별법의 제정은 미 연방형법에서의 적용범위밖에서 일어나는 컴퓨터관련 범죄를 기소하기 위하여 제정하였다. 컴퓨터관련범죄는 미 연방형법의 범위를 벗어났다하더라고 약 40개정도의 연방 형사특별법하에서 처벌될 수 있다. 이러한 범죄의 범위는 컴퓨터소프트웨어절도에서부터 손해를 야기함이 없는 컴퓨터시스템의 무권한 접근에 이르기까지 다양하다. 구체적인 미 연방형사특별법의 종류와 내용은 다음과 같다.

첫째, 저작권법(Copyright Act)이 있다. 이 법은 불법적으로 소프트웨어를 복제하거나 배포하는 자는 형사상 저작권침해에 대한 처벌을 받을 수 있음을 규정하고 있다. 이러한 형사상의 저작권침해법은 저작권의 침해와 저작권의 침해에 대한 고의적 실행 그리고 이로 인해 상업적인 이익 또는 개인적인 금융이익을 도모할 것의 3가지 요건을 충족해야만 처벌이 가능하다. 이 중 저작권침해의 요건은 컴퓨터소프트웨어의 단순한 무권한 복제에 의해 충족될 수 있지만 나머지 두 가지 요소는 증명하기 어려울 가능성이 높다.

둘째, 국가도품법(National Stolen Property Act)이 있다. 이 법은 5,000달러 이상의 재화를 범죄의 객체로 하고 있다. 내용은 절취되었거나 사취된 것으로 밝혀진 재화·상품·증권·금전을 州 間의 통상에서 수송하는 행위를 금지한다. 또한 이 법은 허위로 전산화된 자금이체(Transfers of funds)를 포함한, 다양한 컴퓨터범죄들의 처벌에 그 조문이 적용되어 왔다. 미국법원은 만일 컴퓨터 프로그램들이 단지 무형의 형태로 존재한다면 국가도품법하에서 컴퓨터 소프트웨어는 재화나 상품을 구성하지 않는다고 판결해왔다. 그러나 법원은 유형의 하드웨어는 국가도품법에 의하여 보호되는 것으로서 재화와 상품을 구성한다고 결정하면서 소프트웨어절도를 유형의 하드웨어 절도와 구별해 왔다.

---

21) 이하의 미연방형사특별법의 규제법규에 관한 자세한 내용에 대해서는 Eric J. Bakewell/ Michelle Koldaro/ Jennifer M. Tjia, op. cit., pp. 495 ~ 507 supra note 4).

셋째, 우편 및 전신사기법(Mail and Wire Fraud)이 있다. 이 법은 금전이나 재산을 획득할 목적으로 사기 계획을 진척시키기 위하여 州 間 전신통신 및 우편을 이용하는 것을 금지하고 있다. 이러한 법들은 州 間의 전신·우편 또는 연방보증은행(Federally insured bank)의 범죄에의 이용을 수반한 컴퓨터보조절도(Computer-aid theft)를 차단하는데에 중요한 역할을 수행한다. 이는 무형의 컴퓨터 프로그램의 무권한 복제물을 획득하려는 시도는 우편 및 전신사기법의 적용을 받을 수 있다는 것을 의미한다. 그러나 지방법원에서는 전신사기법이 저작권부 자료(Copyrighted material)에 적용될 수 있는지에 대한 문제에 관하여 견해가 갈린다.[22]

넷째, 전자통신 사생활법(Electronic Communications Privacy Act)이 있다. 1986년에 제정된 이 법은 컴퓨터통신의 무권한 방해를 금지하기 위해서 전신 및 전자통신 방어에 관한 연방법을 개정한 것이다. 더욱이 이 법은 해당시설에의 의도적이고 권한없는 접근을 통하여 시설내의 전자적으로 저장된 자료를 획득·변경하거나 유권한 접근을 방해하는 것을 금지하는 것을 내용으로 하는 새로운 범죄에 대한 처벌법규를 만들어 냈다. 또한 이 법은 개인사생활보호의 확장과 전자감시법을 통해서 처벌될 수 있는 범죄의 수를 확장함으로 인해서 해커들의 컴퓨터통신 방해를 차단하는 역할을 행하고 있다.

다섯째, 1996년의 통신예절법(Communications Decency Act of 1996)과 1998년의 온라인상의 아동보호법(Child Online Protection Act of 1998)이 있다. 미 의회는 1996년 통신예절법과 1998년의 온라인상의 아동보호법을 제정함으로서 인터넷상의 언론의 내용을 규제함에 의해 인터넷상으로 미성년자에게 특정물을 전송하는 것을 막기 위하여 노력하였다. 이 법은 통신의 수신자를 의도적으로 괴롭히기 위한 컴퓨터의 고의적 이용뿐만 아니라 음란물을 미성년자에게 제공하기 위한 컴퓨터의 고의적 이용을 규제하고 있다. 즉 통신예절법에서는 인터넷을 통해 미성년자에게 부적절하고 외설적이며 명백하게 불법인 자료를 전송하는 것을 금지한다. 또한 미 의회는 온라인상의 아동보호법을 통과시켰다.

---

22) 이 의견대립은 컴퓨터프로그램은 비록 무형이지만 그래도 "재산"이고, 그에 따라 저작권법과 전신사기법 양자에 의해 기소될 수 있는 것이라는 판례와 부분적으로 전신사기법이 저작권부 자료에 적용되도록 하는 명백한 입법적 의도가 없기 때문에 저작권부 소프트웨어의 불법복제를 용이하게 하는 컴퓨터게시판의 이용에 전신사기를 이유로 한 기소는 허용될 수 없다는 판결이 대립하고 있다 [United Ststes v. Wang, 878 F. Supp. 758, 759(D. Colo. 1995): United Ststes v. LaMacchia, 871 F. Supp 535, 540~544 (D. Mass. 1994)]; 여기에 대해서는 Xan Raskin/ Jeannie Schaldach-Paiva, op. cit., p. 551 supra note 9).

마지막으로, 1996년의 아동포르노예방법(Child Pornography Prevention Act of 1996)이 있다. 1996년에 미 의회는 컴퓨터상에서 어린이의 성적인 표현을 나타내는 것들의 수령과 배포 그리고 생산을 금지하기 위하여 아동포르노예방법을 통과시켰다. 이 법은 미성년자의 성적인 묘사를 만들어내기 위하여 전자적으로 혹은 기계적으로 창조되거나 변화되는 성적 이미지의 수령과 배포 그리고 생산을 범죄화하고 있다. 즉 이 법은 어린이를 묘사한 애로물의 컴퓨터상의 전송을 금지하고 있다.

⑵ 우리나라의 형사특별법

우리나라에서 컴퓨터범죄에 관한 처벌규정을 두고 있는 형사특별법은 대부분이 현행 형법규정에서 처벌하지 못하는 컴퓨터상의 불법행위를 처벌하기 위하여 급하게 제정되었다는 데에 그 특징이 있다. 여기에 해당하는 법률은 여러 가지가 있으나 그 중 가장 대표적인 법률로서 '정보통신망이용촉진및정보보호등에관한법률'이 있다. 그 외에 '정보통신기반보호법'이 있고, '화물유통촉진법'과 '무역업무자동화촉진등에관한법률'이 컴퓨터범죄 중 전자문서 또는 정보의 위작·변작에 대해 처벌규정을 두고 있다.[23]

이 중 '정보통신망이용촉진및정보보호등에관한법률'과 '정보통신기반보호법'은 신종 컴퓨터범죄에 대처하기 위한 처벌규정으로서 2001년 7월 1일에 정부가 제정하고 시행하였다.[24] 여기에서는 '정보통신망이용촉진및정보보호등에관한법률'중 컴퓨터범죄와 관련된 처벌(벌칙)조항을 중심으로 살펴보기로 한다. 이는 다음과 같다.

---

23) 이러한 형사특별법으로는 가장 중요한 위의 법규 이외에도 정보화촉진기본법,전산망보급확장과이용촉진등에관한법률,통신비밀보호법,공공기관의개인정보보호에관한법률,신용정보의이용및보호에관한법률,컴퓨터프로그램보호법,신용카드업법 등이 있다. 그러나 이 법규들이 컴퓨터범죄를 규율하기 위한 대표적인 법규라고는 할 수 없으므로 지면관계상 '정보통신망이용촉진및정보보호등에관한법률'을 제외한 나머지 법규는 본 글에서는 자세히 다루지 않기로 한다; 한편 형사특별법 전체의 문제점과 정비방안에 대해서는 박기석, 「형사특별법의 구성요건 및 법정형의 문제점과 정비방안」, 법조 2004년 11월(통권 제578호), 법조협회, 143~166면 참조.

24) 당시 정부의 이러한 대처태도는 컴퓨터와 통신기술 발전속도를 감안할 때 형법의 개정은 상대적으로 매우 긴 시간을 요구하는 작업이라는 우려에서 기인하는 것으로 보여진다. 이는 현행 형법의 규정과 해석을 통한 문제해결을 너무 쉽게 포기하고 행정편의적인 발상에서 여러 가지 문제점의 지적에도 불구하고 계속적인 특별법의 제정을 강행한 정부의 태도는 법적용의 통일성과 헌법상 비례의 원칙, 형법의 비범죄화의 요청, 형법의 보충성의 원리에 비추어서 부당하다고 보여진다 (류석준, 「해킹에 대한 규제법규에 관한 연구」, 188면).

① 제61조에서 “사람을 비방할 목적으로 정보통신망을 통하여 공연히 사실 혹은 허위의 사실을 적시하여 타인의 명예를 훼손한 자”를 처벌함으로서 인터넷상의 명예훼손죄에 대한 처벌규정을 마련하고 있다.

② 제62조 제1호 내지 제3호와 제63조 제2호에서 “인터넷정보통신서비스제공자 및 정보의 제공을 매개하는 업무에 종사하거나 종사하였던 자”가 주체가 되어 행하는 개인정보에 대한 침해범죄에 대해 형법에서의 업무상 비밀누설죄에 준하는 처벌규정을 마련하였다.

③ 제62조 제6호에서는 “정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하는 행위”를 정보훼손 및 비밀침해죄로서 처벌하고 있다.[25]

④ 2002년 12월 18일 개정시에 신설된 조항으로서 스팸메일을 규제하기 위해 제65조의 2 제3호에서 스팸메일 발송을 위한 예비행위를 처벌하는 규정을 마련하였다. 즉 “인터넷 홈페이지 운영자 또는 관리자의 사전동의없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램 그 밖의 기술적 장치를 이용하여 전자우편주소를 수집·판매·유통 또는 정보전송에 이용하는 행위”를 처벌하고 있다.

⑤ 악성프로그램의 전달 또는 유포하는 행위와 타인의 정보훼손 그리고 타인의 비밀침해·도용·누설을 처벌하기 위하여 제62조 제4호와 제5호에서 “정당한 사유없이 정보통신시스템, 데이터 또는 프로그램등을 훼손·멸실·변경·위조 또는 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하는 행위”와 “정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하는 행위”를 처벌하고 있다.[26]

⑥ 제63조 제1항 제1호에서 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하는 것을 처벌하는 규정을 입법화하였다. 또한 제2항에서 이러한 정보통신망침입행위의 미수를 처벌하는 규정을 신설하였다.[27]

---

25) 이 규정은 우리형법 제316조 제2항의 비밀침해죄의 객체가 전자기록등 특수매체기록이어서 전송중인 데이터는 객체가 될 수 없다는 점, 그리고 내용을 알아내지 않고 정보를 훼손하거나 침해하는 행위를 처벌하기 위한 보완규정으로 생각된다; 同旨 오영근, 「인터넷범죄에 관한 연구」, 형사정책연구 제14권 제2호(제54호), 한국형사정책연구원, 2003, 308~309면.

26) 이는 형법 제314조 제2항의 업무방해죄및 제366조의 손괴죄로 처벌할 수 없는 행위 즉 업무방해를 초래하지 않거나 손괴의 결과를 발생시키지 않더라도 단지 위험을 발생시키는 자체만으로 처벌할 수 있는 근거를 마련하기 위해 제정된 것으로 보인다; 同旨 오영근, 「인터넷범죄에 관한 연구」, 309면.

⑦ 제65조 제1항 제2호에서 "정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시한 자"를 처벌하는 규정을 두었다.[28]

⑧ 제64조 제1호와 제2호는 "정보제공자가 청소년유해매체물임을 표시하지 아니하고 영리를 목적으로 제공하는 경우와 청소년유해매체물을 광고하는 내용의 정보를 청소년에게 전송하거나 청소년접근을 제한하는 조치없이 공개적으로 전시한 자에 대해 처벌하는 규정을 마련하고 있다.

⑨ 제65조 제1항 제3호와 제2항은 "정보통신망을 통하여 공포심이나 불안감을 유발하는 말, 음향, 글, 화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자"를 처벌하고 이를 반의사불벌죄로 처리하는 규정을 마련하고 있다.[29]

한편 정보통신기반보호법은 제12조와 제28조에서 권한없이 주요정보통신기반시설에 접근하여 시설을 교란·마비 또는 파괴한 자를 처벌하고 있다.[30]

---

27) 이는 형법 제319조 제1항 의 주거침입죄로 처벌할 수 없는 행위인 해킹과 그에 대한 미수를 범죄화하여 처벌하는 법규를 마련한 것이다. 형법상의 주거침입죄가 미수범처벌규정을 두고 있으므로(제332조) 이에 대응하여 해킹의 미수도 처벌하는 규정을 신설한 것으로 보인다; 다만 이 법규에 대하여는 정보통신망 보호조치 침해행위에 대해 우리형법상의 업무방해죄와 비밀침해죄가 미수를 처벌하지 않음에도 불구하고 이러한 보호조치침해행위의 미수를 처벌하는 것은 가벌성의 지나친 확장이라는 비난이 있다 (류석준, 「해킹에 대한 규제법규에 관한 연구」, 202면).

28) 이는 형법 제243조의 음화유포등의 죄로는 인터넷상의 음란물을 규제할 수 없기 때문에 이를 보완하기 위하여 마련한 규정이다; 同旨 오영근, 「인터넷범죄에 관한 연구」, 320면.

29) 이는 "사이버스토킹"을 처벌하기 위한 법규라고 할 수 있다.

30) 이외의 형사특별법으로서 화물유통촉진법은 형법이 전자기록 보호면에서 해결하지 못하고 있는 공백을 해소하고 있다. 형법은 1995년 형법개정 당시에 제정된 법률로서 제227조의 2와 제232조의 2를 신설하여 公電磁記錄僞作·變作의 죄와 私電磁記錄僞作·變作의 죄를 처벌하는 규정을 마련하였다. 그러나 앞에서도 언급했듯이 전송중인 데이터를 보호하는 입법은 형법에서 마련하지 못하였다. 이에 화물유통촉진법은 제54조의 2 제1항과 제2항에서 "물류전산망에 의한 전자문서(여기서의 전자문서는 화물유통촉진법 제2조 제11호에 의해서 처리 또는 보관중인 것 뿐만 아니라 전송중인 것도 포함한다)를 위작 또는 변작하거나 그 사정을 알면서 위작 또는 변작된 전자문서를 행사한 자와 그 미수범"을 처벌하는 규정을 마련하여 해결하였다. 그러나 이 법규에 대하여는 전송중인 공전자문서를 본 규정의 전자문서에 포함시킬수 없다는 점과 물류전산망 사전자 문서를 제외한 다른 사전자문서에 대해서는 여전히 형벌의 공백이 존재한다는 점, 형법의 규정과 비교해 보았을 때 형벌의 불균형등의 문제점을 지적하는 견해가 있다 (류석준, 「전자기록위작·변작행위의 규제법규에 관한 연구 -문제점을 중심으로-」, 형사법연구 제23호(2005년 여름호), 148~150면); 또한 무역업무자동화촉진에관한법률 제25조 제1항에서는 "지정사업자·무역업자·무역유관기관및 대행처리사업자의 컴퓨터파일에 기록된 전자문서 또는 데이터베이스에 입력된 무역정보를 위조 또는 변조하거나 이를 행사한 자는 1년 이상 10년이하의 징역 또는 1억원이하의 벌금에 처한다"라고 규정하고 있다. 이는 컴퓨터범죄의 객체가 무역업무에 종사하는 기관및 사람들의 컴퓨터파일이

Ⅳ. 立法의 改正方向

1. 刑 法

위에서 컴퓨터관련 범죄를 규율하기 위한 형법에서의 입법태도를 살펴보았다. 주목할 첫 번째 사실은 우선 미연방 형법전의 탄력적인 입법태도를 들 수 있다. 우리형법이 1997년의 형법개정에서 비로소 컴퓨터범죄를 처벌하기 위한 조문을 신설하였으나 이는 늦은 감이 있다. 또한 그 후 에도 변화하는 신종컴퓨터범죄를 처벌하기 위하여 2001년의 개정에서 컴퓨터등 사용사기죄의 일부구성요건을 추가하여 대처하였다. 그러나 점점 발달하는 인터넷과 컴퓨터정보기술의 발전은 기존의 거의 모든 범죄를 온라인상에서 범할 수 있는 날도 머지않았음을 암시한다. 급격한 사회의 변화에 맞추어 컴퓨터관련범죄에 대해 탄력적인 법운용을 행하는 것이 세계적 추세이다. 이에 맞추어 우리형법도 신속한 대응이 요구된다. 이를 위하여는 더 조직적이고 체계적인 입법의 정비가 요구된다고 할 것이다. 그러나 우선 시급하게 우리형법이 나아가야 할 개정방향을 제시하면 다음과 같다.

첫째, 우리형법상의 컴퓨터범죄처벌법규에서 과실범처벌규정의 신설이다. 컴퓨터범죄는 특성상 확정적인 고의를 지니고서 범하는 범죄도 있겠지만 과실에 의해서(특히 인식있는 과실)범하여지는 경우가 상당히 많다고 생각되어진다(가령 해킹의 경우가 그 대표적이다. 이 때 해커는 자신의 행위가 정당하다는 확신을 가지고 행하는 경우가 많을 것이다). 그럼에도 불구하고 현행 우리형법에서는 과실로서 컴퓨터에 접근하여 악성소프트웨어의 전송을 야기하는 행위와 역시 과실로서 해킹을 통해 업무방해의 결과를 야기한 자를 처벌하는 법규를 마련해두고 있지 않다. 만약 다른 고의범죄를 범하기 위한 수단으로서 악성소프트웨어를 전송했다면 처벌할 수 있다. 그러나 그러한 전송이 고의가 아니라 순수한 과실로서 행하여지고 그 결과를 처벌할 수 있

므로 일반형법상의 공·사전자기록 위작·변작의 죄보다 형벌을 가중하여 부과하려는 취지의 법규로 보여진다. 다만 이 법규에 대하여는 역시 ① 형법과 달리 공·사전자기록의 구분없이 같은 조항에서 규정하면서 동일한 법정형을 부과하는 것은 사전자기록의 경우를 공전자기록의 경우보다 가볍게 처벌하고 있는 형법의 태도와 배치된다는 점 ② 규정의 법문의 구조상 위조·변조된 전자문서나 무역정보의 행사를 처벌할 수 없게 된다는 점 ③ 전송중인 전자문서나 무역정보에 대해서는 대처할 수 없다는 점 ④ 허위공전자문서작성행위에 대한 형벌의 공백을 내포하고 있는 점 의 문제점을 제기하고 있는 비판이 있다 (류석준, 「전자기록위작·변작행위의 규제법규에 관한 연구 -문제점을 중심으로-」, 151~153면).

는 과실범처벌규정이 없다면 이러한 범죄는 처벌이 불가능해진다. 이는 과실로서 행하여지는 행위이기 때문에 처벌규정을 마련하기가 곤란하다고 할 수도 있다. 그러나 과실범도 처벌의 필요성이 있다면 처벌해야 한다. 거의 모든 국민이 컴퓨터와 인터넷에 접속하는 것이 생활화되어있는 현대에는 더욱 더 이러한 불법전송행위와 그로 인한 피해, 그리고 과실에 의한 업무방해의 결과에 대한 처벌규정의 필요성이 절실하다 할 것이다.

둘째, 컴퓨터범죄의 잠재적 피해자들을 위하여 그들의 법익을 좀 더 철저히 보장해 줄 필요가 있다. 이를 위한 한 가지 방안으로서 총칙규정에서 위법성조각사유의 제한을 어느정도 완화시켜 주기위해 규정을 보완할 필요가 있다. 컴퓨터범죄의 경우에는 과실에 의한 범죄행위가 특성상 많을 수밖에 없다. 따라서 이러한 과실에 의한 컴퓨터범죄에 대해서 피해자가 컴퓨터상에서 그때마다 조치를 취하는 위법성조각사유인 정당방위는 현재성의 요건을 완화하여 줄 필요가 있다. 이는 고의범에 있어서도 마찬가지이다. 컴퓨터등 사용사기죄를 예로 들었을 때 컴퓨터에 부정한 명령 또는 허위의 정보를 입력하거나 권한없이 정보를 입력·변경하여 정보처리를 하게 함으로서 재산상의 이익을 취득하는 것을 막기 위하여 잠재적 컴퓨터파괴장치를 하고 이러한 범죄행위가 실행에 착수되었을 때에는 범죄행위자의 컴퓨터가 손괴되는 장치의 부착을 허용하는 것등이 한가지 방법이 될 수 있을 것이다. 이는 이론적 해석에 의한 해결도 가능할 수 있겠지만 총칙에서 입법을 보완할 필요가 있다. 보완규정의 주요내용은 컴퓨터범죄의 잠재적 피해자들 즉 형법상 컴퓨터범죄의 보호법익의 대상이 되는 사람들이 그들의 보호법익을 지키기 위한 안전장치를 행함에 있어서 위법성조각사유의 현재성의 요건을 완화해 주는 것이 그것이다. 컴퓨터범죄는 장래에 나타나는 침해에 대해서도 위법성조각사유를 인정해줄 필요가 있기 때문이다.

셋째, 전송중인 데이터를 보호할 필요가 있다. 일반 국민의 대부분은 이메일이나 홈페이지를 통해 데이터 및 정보의 전송을 대화 및 정보교환의 필요성에서 많이 활용하고 있다. 이러한 데이터 및 정보의 컴퓨터파일이 큰 경우 전송에 걸리는 시간이 의외로 많이 걸리고 이러한 전송중인 데이터는 현행 형법의 규정으로는 보호가 전혀 되어있지 않다. 이는 특히 공·사전자기록 위·변작죄, 컴퓨터손괴등으로인한 업무방해죄에서 요구된다고 할 것이다.[31]

---

31) 이러한 전송중인 데이터에 대한 보호가 형사특별법에는 마련되어 있다. '화물유통촉진법 제54조의 2 제1항과 제2항'에서 전송중인 전자문서의 위·변작행위와 이러한 문서의 행사 그리고 그 미수범을 처벌하는 규정을 마련하고 있다.

넷째, 국가적 법익을 보호하는 구성요건을 신설하여 국가소유의 공공 컴퓨터의 법익을 침해하는 자를 국가적 법익을 침해하는 범죄행위로서 처벌하는 법규를 마련할 필요가 있다. 국가소유의 컴퓨터가 행하는 업무는 개인이 행하는 업무와는 달리 국가 혹은 공공기관과 관련된 문서를 다루고 정보처리를 행하는 공적이고 중요한 업무이다. 즉 이는 '보호된 컴퓨터'로서 특별한 보호를 받아야 할 위치에 있다고 생각된다. 그러나 현행 우리형법은 공공기관의 컴퓨터에 불법적으로 접근하는 행위와 공공기관의 컴퓨터의 무권한 사용행위를 비롯한 컴퓨터손괴로 인한 업무방해죄등에서 특별하게 공무와 관련된 범죄행위를 가중처벌하고 있지 않다. 또한 현행 주거침입죄 이외에 국가의 컴퓨터에 접근하는 불법적인 접근행위를 처벌하는 법규를 마련해놓고 있지도 않다. 신속한 보완이 요구되는 항목이다.

마지막으로 컴퓨터의 불법사용죄를 신설할 필요가 있다. 형법은 제331조의 2에서 '자동차등의 불법사용죄'는 처벌규정을 마련해 놓고 있으나 컴퓨터의 불법사용죄에 대해서는 처벌규정을 마련해 놓고 있지 않다. 컴퓨터의 정보의 중요성 및 정보가 가지는 재산적 가치를 고려해 보았을 때 권리자의 동의없이 불법으로 타인의 컴퓨터를 무권한으로 사용하여 정보를 획득한 자를 처벌하는 규정은 반드시 마련해야 할 것이다.[32]

2. 刑事特別法

컴퓨터범죄를 처벌하기 위한 형사특별법은 새로운 범죄행위의 유형에 대처하기 위하여 급하게 입법되어 왔다. 즉 형법의 적용범위 밖에서 일어나는 컴퓨터범죄행위에 급하게 대처하기 위하여 제정되었다. 따라서 그 대부분의 내용은 형법으로 처벌할 수 없는 부분을 보완하는 내용을 주된 내용으로 하고 있다. 이는 '정보통신망이용촉진및정보보호등에관한법률'도 마찬가지이다. 그러나 이러한 형사특별법의 규정들은 이를 일반형법에 편입시킴으로서 굳이 형사특별법의 규정을 존속시키지 않고서라도 해결이 가능하다. '정보통신망이용촉진및정보보호등에관한법률'을 예로 들어 구체적으로 개정방향을 제시해보면 다음과 같다.

① 정보통신망이용촉진및정보보호등에관한법률(이하는 정보통신망법이라고 함) 제

32) 컴퓨터에 대한 절도행위가 없었고 물리적인 정보를 절도해 간 것도 아니므로 이 경우를 절도죄로 처벌할 수는 없다.

61조는 형법 제309조 '출판물등에 의한 명예훼손죄'에서 처벌할 수 없는 유형인 정보통신망을 통한 행위를 처벌하고 있다. 다만 정보통신망법 제61조가 양형에 있어서 더 높게 책정되어 있다. 이는 형법 제309조 제1항의 행위수단에 '정보통신망(인터넷포함)'을 새롭게 구성요건에 편입시킴으로서 해결이 가능하다.[33]

② 정보통신망법 제62조 제1호 내지 제3호와 제63조 제2호는 형법 제317조 '업무상 비밀누설죄'에서 처벌할 수 없는 주체의 처벌 즉 컴퓨터범죄와 관련된 업무에 종사하는 자 또는 종사하였던 자를 주체에 포함시켜 업무상 비밀누설죄에 해당하는 행위를 행한 자를 처벌할 수 있는 근거를 마련하였다는 데에 의의가 있다. 이는 형법 제317조의 주체에 '정보통신서비스제공자 또는 정보통신서비스제공업무를 행하였었던 자'를 범죄의 주체에 편입시킴으로서 해결이 가능하다.

③ 정보통신망법 제62조 제6호는 형법 제316조 제2항의 '비밀침해죄'와 형법 제366조의 '재물손괴등죄'를 보완하여 형법으로는 처벌할 수 없는 전송중인 데이터를 범죄의 객체로 하는 행위와 내용을 알아내지 않고 행하는 정보의 훼손 및 침해·도용·누설행위를 처벌하기 위한 규정이다. 이는 형법 제316조 제2항과 제366조의 객체에 '정보통신망에 의하여 전송중인 또는 전송된 전자기록등특수메체기록'을 편입시킴으로서 역시 해결이 가능하다.

④ 스팸메일 발송을 규제하기 위한 정보통신망법 제65조의 2 제3호는 형법 제329조 절도죄의 객체에 '정보통신망을 통한 타인의 정보'를 편입시키면 해결이 가능하다. 이는 또한 자연스럽게 형법 제362조의 장물의 범위에 들어오므로 이러한 타인의 전자우편주소를 수집·판매·유통 또는 정보전송에 이용하는 행위도 형법 제362조의 장물죄로 처벌할 수 있다.

⑤ 정보통신망법 제62조 제4호와 제5호 그리고 정보통신기반보호법 제12조와 제28조는 형법 제314조 제2항의 업무방해죄및 제366조의 손괴죄로 처벌할 수 없는 미수행위 즉 업무방해의 결과를 발생시키지 않았거나 손괴죄의 결과를 발생시키지 않은 행위(장애·교란·마비 및 악성프로그램의 전달·유포)를 단지 컴퓨터범죄의 위험성만으로 처벌이 가능하다는 데에 그 의의를 찾을 수 있다. 그러나 손괴죄는 미수범처벌규정이 있으므로(형법 제371조) 정보통신망법 제62조 제4호와 제5호는 형법상 손괴죄의 미수로 규제가 가능하다 할 것이다. 다만 업무방해죄의 미수범처벌규정이 없으므로 신설이 요구된다고 할 것이나 양형에서 업무방해죄가 손괴죄보다 형벌이 무겁다는 점은 고려되어야 할 것이다.

---

33) 이는 굳이 위의 행위를 형법 제307조의 명예훼손죄로 처벌할 필요성이 없음을 의미한다.

⑥ 그 외에도 정보통신망법 제63조 제1항 제1호와 제2항은 형법 제319조 제1항의 주거침입죄의 보완조항이다. 이는 형법 제319조 제1항의 행위의 객체에 '정보통신망'을 편입시킴으로서 해결이 가능하다. 그리고 제65조 제1항 제2호는 형법 제243조 음화유포등의 죄의 보완조항이다. 이는 형법 제243조의 구성요건상의 행위수단 및 행위유형에 '정보통신만을 통하여'라는 수단과 '부호·문언·음향·화상 또는 영상'이라는 행위유형을 편입시킴으로서 해결이 가능하다. 또한 정보통신망법 제65조 제1항 제3호와 제2항은 형법 제283조 협박죄로 처벌할 수 없는 컴퓨터범죄를 처벌하는 보완규정이다. 따라서 형법 제283조 제1항의 행위유형에 '정보통신망을 통하여 공포심이나 불안감을 유발하는 말·음향·글·화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자'를 편입시킴으로서 해결이 가능하다.

Ⅴ. 結 論

형법은 일정한 범죄행위에 대해 일정한 형벌과 보안처분을 과할 것을 예고하고 그 범죄에 대한 국가의 규범적 평가를 명백히 하는 것을 사명으로 하고 있다. 또한 범죄로 인하여 침해되거나 위협을 받게 될 가치를 보호하고 사회질서를 유지하며 국가의 형벌권남용으로부터 국민의 자유와 권리를 보장하는 일반법이며 기본법이다.

형사특별법은 형법과는 성격이 다르다. 물론 그것이 단지 제정되었다는 이유 하나만으로 법익체계에 부적합하다고 단언할 수는 없다. 새로운 행위태양에 급하게 대처하기 위하여 그리고 기본법이라서 손대기가 부담스러운 형법을 개정하기보다 임시방편적인 형사특별법을 입법하는 것은 입법자의 재량일 수 도 있다. 그러나 앞에서 살펴보았듯이 현재 형사특별법으로 제정되어있는 대부분의 컴퓨터범죄처벌법규는 형법의 확장으로 규제가 가능하다. 또한 지금은 컴퓨터범죄가 일정한 컴퓨터전문가집단에서만 문제되는 범죄가 아니라 모든 일반국민이 필수적으로 컴퓨터를 사용하고 있다는 데에 주목해야할 필요가 있다. 이러한 상황에서 형사특별법에 의한 규제는 컴퓨터범죄에 대한 형법의 보장적 기능에 있어서 형법의 체계를 왜곡하고 기본법으로서의 위치를 흔들리게 할 가능성이 있다. 이를 바로 잡아주기 위해서라도 컴퓨터범죄의 처벌에 대한 법적 규제는 대부분 형법에 의하는 것이 바람직하다.

이러한 목적을 달성하기 위하여 위에서 검토한 방안들이 완벽하게 컴퓨터범죄에 관한 처벌법규로서 형법에서 기능을 발휘할 수 있으리라고는 생각하지 않는다. 컴퓨터 및 인터넷의 사용은 하루가 멀다하고 변하기 때문이다. 다만 시급한 실천을 위한

구체적 노력의 일환으로서 기존 형법규정에 대하여 컴퓨터범죄에 관한 과실범처벌규정의 신설, 형법총칙규정에서 컴퓨터범죄와 관련한 위법성조각사유의 제한완화규정보완, 전송중인 데이터보호규정의 입법화, 국가소유의 컴퓨터를 보호하기 위한 국가적법익보호규정의 마련, 컴퓨터의 불법사용죄 처벌규정 마련, 기존의 정보통신망이용촉진및정보보호등에관한법률의 벌칙규정의 형법에의 편입이 신속하게 요구된다 할 것이다.

임석원

컴퓨터범죄(Computer crimes), 컴퓨터의 불법사용(illegal use of computer)

전송중인 데이터의 보호규정(Protective article for data in transmission)

컴퓨터 관련 과실범(Computer – related criminal negligence)

국가소유컴퓨터의 보호규정(Protective article for state control computers)

[abstract]

A Review on The Laws about Computer - related Crimes

Lim, Seok Won*

The rapid emergence of computer technologies and the Internet's exponential expansion have spawned a variety of new criminal behaviors. As a result, the government revised the criminal law in 1995 to work out this problem and enacted many special laws as countermeasure of the computer crimes. But these special laws that exist have not been in accordance with the criminal law revision in 1995. Besides the criminal law revision in 1995 cannot protect the computer crimes which are being changed.

Now the computer crimes are not the crimes which are made a target of specific people. On the contrary, they are taking aim at the general public. Therefore, there is some distorted possibility of the criminal law from regulation of criminal special laws that exist. For that reason, it is desirable that the criminal law should have restriction for computer - related crimes.

It is my thought that solution to be shown before cannot solve perfectly Computer - related Crimes. But as a part of concrete endeavor, it should be demanded swiftly to include penal regulations of information and communication law into the criminal law, to prepare penal article of illegal use of computer and protective article for state control computers, to legislate protective article for data in transmission, to make up for restriction-relaxing articles in illegality-remission-reason connected with computer - related crimes of general provisions of the criminal law, to establish penal article of computer - related criminal negligence.

* Ph. D. in Law, A senior researcher of the Institute for comparative Legal Studies of Sungkyunkwan-University.