□ 기술해설 □

컴퓨터 범죄와 그 법적 대응책

인하대학교 장영민*

● 목 차 ●

1. 서 언

'정보화 사회'의 단계를 지나 '정보사회'에 진입했다는 평가가 나올 정도로, 오늘날 우리 사회는 컴퓨터 보급의 급속한 확대를 통해서 많은 정보들이 전산화되어 정보이용의 효율성이 극대화되고 있다. '초고속 정보통신망의 구축'이 속속 이루어져 대량의 정보들이 보다 신속히 접근, 활용되어 '정보의 유토피아'가 구현될 것으로 기대되고 있다.

그러나 이러한 정보사회가 갖는 순기능의 이면에는 무시할 수 없는 역기능이 존재한다. 이러한 정보의 불법적 이용 가능성이 도사리고 있기 때문이다. 그 대표적인 것이 컴퓨터 범죄이다. 컴퓨터 범죄는 컴퓨터의 오, 남용을 통해서 범죄를 저지르는 것으로서 종래의 범죄와 유사하지만 정확히 일치하지 않아서 처벌하기에 난관이 있었던 범죄를 말한다. 이에 대응하기 위하여 기존의 법을 적용하는 데에는 한계가 있어서 새로운 입법이 필요한 경우가 많았다. 그리고 컴퓨터 범죄이외에도 전통적인 범죄가 컴퓨터와 관련하여 다양한 형태로 나타나고 있다. 예컨대 종래에는 편지 등의 형태로 존재하던 개인의 비밀이 이제는 컴퓨터 파일 등으로 다양하게 존재하게 되어, 개인의 비밀의 범위가 크게 확대되고 그 침해가능성이 매우 다양해 졌다. 따라서 이에 대한 법적 보호의 필요성이 크다.

다행히 국회에 상정되어 있던 형법개정안의 일부가 수정 발의되어 1995년 12월 1일 국회에서 통과되었다. 컴퓨터 범죄에 관한 규정이 대부분을 차지하는 이 개정형법은 1996년 7월 1일부터 시행된다. 그동안 논의되던 컴퓨터범죄를 망라하여 규정한 이번의 개정형법으로 컴퓨터 범죄의 법적 대응책은 일단 정비되었다고 할 수 있다. 따라서 본 고에서는 이를 집중적으로 살펴보고자 한다. 아울러 개정형법에는 규정되지 않았지만, 다른 특별법에 규정되어 있는 관련 범죄들도 간략히 살펴 보기로 한다.

2. 컴퓨터 범죄에 대한 대응[1]

2.1 컴퓨터 범죄의 유형

컴퓨터 범죄의 유형을 분류하는 방법에는 여러가지가 있지만[2], 이 글에서는 이를 컴퓨터 조작범죄, 컴퓨터 파괴범죄, 컴퓨터 스파이 범

*비 회 원

1) 보다 상세한 것은 졸저, 컴퓨터 범죄에 관한 연구, 한국형사정책연구원, 1993를 참조 바람.

2) 컴퓨터 관련 법익침해행위를 분류하는 관점은 다양하다. 이를 행위의 '객체'를 기준으로 하여 분류하는 입장(일본 경시청

죄, 컴퓨터의 부정사용 그리고 현금자동지급기의 남용범죄로 분류하기로 한다.

2.1.1 컴퓨터操作

컴퓨터操作이란 行爲者가 컴퓨터의 작업과정에 개입하여 컴퓨터의 정당한 자료처리를 방해함으로써 부정한 情報나 資料를 작출하게 하는 행위를 의미한다. 이 犯罪類型은 컴퓨터범죄의 가장 핵심적인 부분이다. 컴퓨터 조작은 컴퓨터의 기능과 관련하여 여러 경로를 통해 이루어 진다. 이에는 첫째 입력자료의 조작, 둘째 잘못된 프로그램의 注入, 셋째 콘솔 조작, 네째 출력조작 등이 있다.

① 入力操作

허위의 자료, 변조된 자료 등을 컴퓨터에 제공함으로써 행위자가 원하는 부정한 처리를 야기하는 犯罪로서, 가장 기본적인 컴퓨터범죄의 형태라고 할 수 있다. 입력조작은 입력자료에 變更을 가하거나, 입력장치를 이용하여 컴퓨터에 허위의 정보를 제공함으로써 이루어지는데, 현재까지 우리나라에서 적발된 컴퓨터범죄 가운데는 이 입력조작에 의한 범죄가 가장 많다.

② 프로그램操作

프로그램이란 컴퓨터를 작동시키거나 일정한 결과를 얻기 위하여 컴퓨터에 부여하는 일련의 命令群이다. 즉 일정한 결과를 얻기 위하여 컴퓨터 등 情報處理裝置 內에서 직접 또는 간접으로 사용되는 一連의 指示, 命令 등의 群이라 할 수 있다. 프로그램 조작이란 이 프로그램에 조작을 가하여 기존 프로그램의 처리과정을 변경시키거나 별개의 프로그램을 만듬으로써 의도하는 부당한 처리를 하게 하는 행위를 말한다.

③ 콘솔操作

콘솔조작이란 컴퓨터의 始動, 停止, 作動狀態, 監視, 情報處理 內容과 方法의 變更, 修正의 경우에 사용되는 콘솔을 조작하여 컴퓨터의 資料處理過程에서 프로그램의 指示나 처리될 記憶情報를 變更시키는 것을 의미한다. 이러한 콘솔造作은 입력장치에 의하여 컴퓨터에 공급되는 자료를 조작하거나, 컴퓨터의 내부 혹은 외부의 記憶裝置에 기억된 자료를 變更시킴으로써도 가능하다. 구체적으로는 프로그램 進行過程中의 命令을 妨害하거나 이를 反復하거나 누락시키는 형태로 나타난다.

④ 出力操作

출력操作은 컴퓨터에 의해 적정하게 처리된 자료를 사후에 變造하는 행위이다. 즉 자료가 정당하게 入力되어 정당한 프로그램에 의해서 처리된 후 出力된 것을 사후에 不法的으로 變更하는 행위를 의미한다. 이와 같은 出力操作은 그 행위가 컴퓨터 내부에 입력된 자료에 의해서가 아니라, 外部에서 이루어진다는 점에서 다른 操作行爲와 구별된다. 출력조작은 시간적으로는 컴퓨터에 있는 자료의 처리가 종료된 후에 비로소 이루어지는 것이므로 컴퓨터에 관한 특별한 전문지식이 없이도 가능하다.

2.1.2 컴퓨터破壞

넓은 의미의 컴퓨터破壞란 컴퓨터 자체, 컴퓨터프로그램, 컴퓨터 내부나 외부의 기억장치에 기억되어 있는 자료를 파괴하는 행위를 의미한다. 컴퓨터하드웨어의 파괴는 손괴죄에 해당하기 때문에 특별히 컴퓨터범죄로 분류하여 논할 필요는 없다. 컴퓨터破壞에서 주로 문제가 되는 것은 자기테이프에 자석 등을 사용하여 데이타나 프로그램을 멸실하는 행위인데, 이를 통해서 기업경영이나 국가행정이 마비되거나 데이타가 가지는 증거가치가 침해되는 결과가 빚어진다. 이 때 멸실되는 것은 유체물이 아니라 데이타나 프로그램이며, 데이타의 내용은 사회, 경제적 가치가 큰 경우가 많다.

2.1.3 컴퓨터스파이

컴퓨터스파이란 컴퓨터 데이타를 權限없이 획득하거나 이를 누설하는 행위를 말한다. 컴

(편), 경찰백서, 1983, 7면 이하)에서는, 컴퓨터범죄를 컴퓨터 하드 웨어, 소프트웨어, 데이타에 대한 침해로 구분하고, 이를 다시 컴퓨터파괴, 컴퓨터의 부정이용, 컴퓨터프로그램·데이타의 부정입수, 프로그램의 변조, 데이타의 손괴등으로 구분한다. 범죄의 수법에 따라 컴퓨터범죄를 분류하는 입장(Parker, Computer Abuse Assessment, SRI 12, 1975, 29면 이하)에서는 파괴에 의한 침해, 정보나 재산의 사취 또는 절취에 의한 침해, 컴퓨터의 무권한사용으로 구분하고 있다. 그러나 컴퓨터가 데이타를 저장, 처리하는 기계라는 점에 착안하여 보면, 컴퓨터범죄를 데이타의 조작, 데이타의 부정입수-누설, 데이타의 파괴, 그리고 컴퓨터의 무권한사용으로 나눠 볼 수 있다(Sieber, Computerkriminalit t und Strafrecht. 39면 이하).

퓨터의 데이타는 큰 가치의 秘密을 내포하고 있는 경우가 많다. 이러한 秘密은 商業的인 분야(즉 簿記, 決算, 고객등록부 등)나 技術분야(즉 開發이나 硏究資料 등) 혹은 기술의 Know-How 등과 밀접한 관련을 갖고 있어서 이의 누설은 해당 기업이나 국가에 막대한 손해를 초래하게 된다.

컴퓨터스파이 행위의 경우 그 대상이 되는 자료가 컴퓨터에 壓縮된 形態로 존재하여 자료 전체에 대한 스파이 행위가 용이하기 때문에 그 危險性은 전통적인 스파이 행위에 비하여 훨씬 크다고 할 수 있다. 특히 통신망이 구축되어 각 단말기에 의해 자료에 대한 접근, 원격조정이 가능할 경우 위험성은 매우 크다.

2.1.4 컴퓨터의 不正使用

컴퓨터의 부정사용 즉 權限없는 컴퓨터의 사용이란 行爲者가 타인의 컴퓨터를 권한없이 作動시키는 것을 의미한다. 즉 컴퓨터를 利用할 權限이 없는 자가 자신의 일을 처리하기 위하여 컴퓨터를 利用함으로써 컴퓨터의 所有者나 賃借人에게 損害를 가하는 행위를 말한다.

자기회사의 컴퓨터를 時間外에 이용한다든가, 이용하는 施設의 規模가 크지 않은 경우는 被害額이 크지 않을 수 있지만 컴퓨터를 임차하여 사용하는 경우이거나, 컴퓨터의 시설이 클 경우에는 그 賃借料와 使用料로 인해 피해자는 막대한 損失을 입게 된다

이러한 경우 컴퓨터의 使用時間은 財産價値를 가지며, 시간의 盜用은 귀중한 財産價値의 竊盜라는 의미에서 소위 '時間의 竊盜'(Zeitdiebstahl)라는 용어가 사용되고 있다. 우리나라의 경우 이에 관한 사례가 많지 않지만 미국, 서독, 일본 등지에서는 이러한 사례가 빈번하게 발생하여 컴퓨터범죄의 하나의 類型으로 주목받고 있다. 본 범죄는 온 라인 네트워크에 퍼스날 컴퓨터를 접속시켜 遠距離에서도 사용할 수도 있으므로 앞으로 더욱 많이 발생할 것으로 展望된다. 물론 이 경우는 일상적인 컴퓨터 사용시 범죄의식이 없이 일상적으로 발생할 수 있는 것이기 때문에 이를 모두 범죄로 볼 수는 없다. 따라서 이 경우 컴퓨터에 물리적으로나 기술적으로 통제장치를 했음에도 불구하고 이를 해제하고 사용하는 경우에 국한하여 금지되는 행위로 보아야 할 것이다.

2.1.5 銀行現金自動支給機의 濫用

현금자동지급기(Cash Dispenser; 보통 CD機라 약칭함)란 銀行의 顧客이 은행출납창구 이외의 곳에서 현금을 引出할 수 있도록 便宜를 제공하는 機械裝置이다. 현금자동지급기를 이용하기 위해서 고객은 먼저 은행과 契約을 締結하고 본인의 預金狀況과 有效期間 등의 정보를 기계가 읽을 수 있도록 자기스트라이프가 索引된 現金引出카드를 발급받아야 한다. 현금자동지급기의 남용이란 이러한 시스템을 이용하는 과정에서 나타나는 각종 不法的 행위를 말한다.

우리나라도 이제는 현금자동지급기의 設置가 一般化되었다. 그래서 이 유형은 앞으로 급증할 것으로 전망되는 범죄로서 앞으로 주목하여 대처해야 할 것이다.

2.2 컴퓨터 범죄에 대한 현행법의 대응

그간 컴퓨터와 관련한 법익침해행위를 컴퓨터범죄라 칭하면서, 이를 범죄화하여야 한다는 논의가 많이 제기되었는데[3] 이번 형법개정을 통해서 이러한 주장과 요구가 실현되었다. 이러한 행위들을 범죄화하여야 하는 이유는 컴퓨터 관련 법익침해 행위의 당벌성과 처벌의 필요성이 인정되었음에도 불구하고 기존의 구성요건으로는 포섭할 수 없는 특성을 가지고 있었다는 데 있다.

2.2.1 신설된 컴퓨터 관련 범죄 개관

개정형법에는 현재 알려져 있는 컴퓨터 관련 범죄의 양상 가운데 다음과 같은 유형을 범죄로 규정하였다.

우선 ①컴퓨터조작범죄의 범주에 속하는 것으로서, 電磁記錄僞作變作罪(公電磁記錄僞作變作(제227조의2), 公正證書原本不實記載(제228조), 僞造公文書等行使(제229조), 私電磁

3) 대표적인 문헌으로는 김종원 외, 컴퓨터범죄와 이에 대한 현행형법의 대응에 관한 연구, 1987가 있다. 졸저. 앞의 책도 참조.

記錄僞作, 變作(제232조의2), 僞造私文書等行使(제234조), 컴퓨터등使用詐欺(제347조의2))가 규정되었고,

②컴퓨터파괴범죄의 범주에 속하는 것으로서는 컴퓨터業務妨害罪(제314조 제2항), 컴퓨터데이타파괴죄(제366조)가 규정되었고,

③데이타의 스파이(부정입수-누설)범죄의 범주에 속하는 것으로서 컴퓨터데이타探知죄(제316조 제2항)가 규정되었다.

그리고 이들 범주에 속한다고 보기 어려운 범죄의 유형으로서 權利行使妨害罪(제323조)가 있는 바, 이는 電磁記錄의 재물성을 인정하기 어렵기 때문에 규정된 것인데 성격상으로는 제한물권을 보호하는 규정으로서 컴퓨터범죄라고 하기는 어렵다.

이하에서는 신설된 컴퓨터 범죄의 내용을 간략하게 살펴 보고자 한다.

2.2.2 신설된 컴퓨터 관련 범죄

2.2.2.1. 컴퓨터조작범죄

가. 電磁記錄僞造 등 罪

컴퓨터에 저장된 데이타가 법적 거래에 있어서 증명기능을 갖게 되어 이의 보호가 절실한 과제로 등장하였다. 그런데 電磁的[4] 方式으로 컴퓨터 기타 특수매체에 기록된 데이타를 종래의 문서의 개념에 포섭되는 것으로 보는데에는 무리가 있다는 것이 일반적인 견해였기 때문에[5] 이를 보호하기 위하여는 입법적 대책이 요구되고 있었다.

개정형법은 구형법이 문서를 공문서와 사문서로 나누고 이의 위조, 변조 및 행사를 처벌하던 입법태도에 대응하여, 電磁的 記錄을 公電磁記錄과 私電磁記錄으로 나누고 이의 僞作, 變作, 行使를 처벌하고 있다. 그리고 개정형법은 공정증서원본부실기재죄에 대응하여 공정증서원본의 기능을 하는 電磁記錄 등 특수매체기록에 부실의 사실을 기재하게 한 행위도 처벌하고 있다.

1) 신설된 조문

- 제227조의2(公電磁記錄의 위작, 변작) 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 電磁記錄 등 특수매체기록을 위작 또는 변작한 자는 10년 이하의 징역에 처한다.

- 제228조(公正證書原本等의 不實記載) 공무원에 대하여 허위신고를 하여 공정증서원본 또는 이와 동일한 電磁記錄 등 특수매체기록에 불실의 사실을 기재 또는 기록하게 한 자는 5년 이하의 징역 또는 1000만원 이하의 벌금에 처한다.

- 제229조(위조등 공문서의 행사) 제225조 내지 제228조의 죄에 의하여 만들어진(위조, 변조, 작성, 변작, 위작, 변작 또는 불실기재, 기록된 제303조 내지 제307조에 규정된) 문서, 도서, 전자기록 등 특수매체기록, 공정증서원본, 면허증, 허가증, 등록증… 을 행사한 자는… 각조에 정한 형에 처한다.

- 제232조의2(私電磁記錄의 위작, 변작) 사무처리를 그르치게 할 목적으로 권리, 의무 또는 사실증명에 관한 타인의 電磁記錄 등 특수매체기록을 위작 또는 변작한 자는 5년이하의 징역 또는 1000만원 이하의 벌금에 처한다.

- 제234조(僞造私文書등의 行使) 제231조 내지 제232조의 죄에 의하여 만들어진 문서, 도서 또는 電磁記錄 등 특수매체기록을 행사한 자는 각 죄에 정한 형에 처한다.

2) 성립요건

전자적 기록을 종래의 문서의 개념에 포섭되는 것으로 보아 보호하기 어려웠던 이유는, 문서는 계속성, 증명성, 보장성을 그 개념요소로 하는데[6], 전자적 기록 자체는 계속성의 내용인 '시각적 지각가능성'이 없고, 또 전자적 기록은 다수인에 의하여 만들어지는 경우가 많으므로 명의가 없거나 분명하지 않은 경우가 있어서 보장성을 결하는 경우가 많기 때문이다.

문서위조죄의 保護法益을 '문서에 대한 공공의 신용'이라고 한다면, 본죄의 보호법익은 '전자적

4) 이는 일반적으로 사용되는 표현은 아니나, 電氣(또는 電子)와 磁氣를 총칭하는 용어로 사용되었다. 일본형법의 영향인 것으로 보인다.

5) 김종원, 앞의 글, 24면 이하; 이재상, 컴퓨터범죄에 대한 형법적 대응의 연구, 경희법학, 제25권 제1호, 1990, 59면 이하; Sieber, Computerkriminalit t und Strafrecht, 1977, 277면.

6) 이재상, 형법각론, 527면; 정성근, 형법각론, 660면; 진계호, 형법각론, 566면 이하; SK-Samson, 267, Rdn 2; Sch nke-Schr der-Cramer, 267 Rdn 2 등 참조.

기록에 대한 공공의 신용"[7] 이라 할 수 있다.

본죄의 客體는 '電磁的 記錄 等 特殊媒體記錄'이다. 電磁的 記錄이란 일정한 매체에 電氣(電子)적, 磁氣적 방식으로 저장된 기록을 말한다. 일정한 매체란 집적회로, 자기디스크, 자기테이프 등을 말하여, 전자적 기록이 아닌 예컨대 음반(LP)에 기록된 음성신호는 이에 해당하지 않는다. 전자적 기록이외에 특수매체기록으로 인정되는 것으로는 레이저를 이용한 광디스크가 있다.

개정형법은 '전자적 기록등 특수매체기록'에 대하여 입법적 정의는 하지 않고 있다. 이에 비하여 일본의 개정형법은 '전자적 기록'을 입법적으로 정의하여, "電磁的 記錄이란 電子적 방식, 磁氣적 방식, 기타 사람의 지각으로써 인식할 수 없는 방식에 의하여 만들어지는 기록이며, 전자계산기에 의한 정보처리에 사용되는 것"(同法 제17조의 2)이라고 정의하고 있다.

'기록'은 데이타 또는 매체 그 자체를 의미하는 것은 아니며, 따라서 통신중의 데이타나 처리중의 데이타는 여기에 포함되지 않는다.[8] 반도체 기억집적회로, 자기테이프, 자기디스크, 광디스크 등에 수록된 데이타는 여기에 속한다. 또 기록은 계속성을 가져야 하므로 모니터에 화상의 형태로만 존재하는 데이터는 기록에 해당하지 않는다.

개정형법은 본죄의 행위의 태양을 "사무처리를 그르칠 목적으로… 타인의 電磁記錄 등 특수매체기록을 위작, 변작"하는 것으로 규정하고 있다. 행위의 태양을 기술하는 용어로서 '위조, 변조'라는 용어를 사용하지 않고 '위작, 변작' 등의 용어를 사용한 것은, 전자적 기록이 문서와는 달리 가시성, 가독성이 없을 뿐만 아니라, 작출과정도 문서와는 다르기 때문이다. 따라서 개정형법의 '위작'이라 함은 "처음부터 허위의 기록을 만들어내어 저장·기억시키는 행위"를 의미하고, '변작'이라 함은 "기존의 기록을 부분적으로 고치거나 말소하는 행위"를 의미한다.

본죄는 주관적 구성요건으로 '사무처리를 그르치게 할 목적'을 요구하고 있다. '사무처리를 그르치게 한다'함은 부정작출된 전자적 기록을 사무처리장치에 사용함으로써 사무처리를 잘못되게 함을 뜻한다.[9] 동일한 데이타인 경우에는 부정하게 작출된 것이라 하더라도 증명작용에 대한 실해가 발생하지 않는다는 점에서 처벌의 대상을 '증명작용에 실해를 발생시킬 것'을 목적으로 하는 경우에 한정하자는 취지이다.[10] 따라서 이와 같은 목적이 없는 경우에는 비록 데이타의 위작, 변작이 있다 하더라도 본 죄는 성립하지 않는다. 예컨대 데이타를 기존의 방식과 다른 방식으로 저장한 경우에는 본죄는 성립하지 않는다.

'행사'라 함은 위작 또는 변작된 기록을 정보처리할 수 있는 상태에 두는 것을 말한다.[11]

나. 컴퓨터使用詐欺罪

컴퓨터가 사람을 대신하여 각종 사무, 특히 재산권의 득실변경의 사무를 처리하는 기술이 도입됨에 따라, 이를 악용하여 재산상의 불법한 이득을 얻는 행위가 발생하고 있다. 이러한 행위 가운데는 기존의 재산범에 관한 규정으로는 대처하기 어려운 경우가 있다.[12] 따라서 이와 같은 불법이득 행위에 대하여는 별도의 구성요건을 마련하여 처벌하는 것이 세계적인 입법의 경향이다.[13] 개정형법도 이러한 추세에 따라 일본이나 독일의 경우 처럼 사기죄와 병행하여 제347조의2에 컴퓨터사용사기죄를 신설하였다.

1) 신설된 조문

— 제347조의 2(컴퓨터 등 사용사기죄) 컴

7) Dreher/Tr ndle 269 Rdn 2; SK-Samson 269 Rdn 1; 형사법개정특별심의위원회, 일본형법개정작업경과와 내용, 1989, 558면.

8) 이에 관하여는 〈전산망보급확장과 이용촉진에 관한 법률〉 제25조가 규정하고 있는데, 이의 침해행위에 대하여는 3년 이하의 징역 또는 1000만원 이하의 벌금에 처하도록 하고 있다(동법 제30조 제1항).

9) 형사법개정특별심의위원회, 일본형법개정작업경과와 내용, 1989, 559면.

10) 앞의 책, 560면.

11) 이재상, 앞의 글, 같은 면.

12) 김종원 외, 앞의 글, 43면; 이재상, 앞의 글, 60면; Rohner, Computer kriminalit t, 109면; Lenckner, Computerkriminalit t und Verm gensdelikte, 25면 이하; M hrenschlager, wistra, 1982, 202면.

13) Sieber, The International Handbook on Computer Crime, 42면 이하 참조.

퓨터 등 情報處理裝置에 허위의 情報 또는 부정한 命令을 入力하여 정보처리를 하게 함으로써 財産上의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2000만원 이하의 罰金에 처한다.

개정형법은 문언상, 자동적으로 처리되는 재산권의 득실, 변경의 사무에 대하여 허위의 정보 또는 부정한 명령을 입력함으로써 불법하게 이득을 취하는 행위만을 처벌하고, 진실한 정보를 입력하여 불법하게 이득을 취하는 행위는 명시하지 아니하고 있어 문제가 된다. 이에 반해 독일 형법은 위의 모든 경우를 포괄하는 입법형식을 취하고 있다[동법 제 263조의a(컴퓨터사기죄)].

2) 성립요건

개정형법의 컴퓨터사용사기죄의 보호법익은 사기죄와 마찬가지로 재산권이지만[14], 사기죄와는 달리 '인간의 의사결정과정'에 대한 직접적인 기망을 가하는 것이 아니라 '재산적으로 중요한 정보처리과정'에 대한 침해를 통해 기망을 가하는 범죄이다.[15,16]

본죄는 행위자에 제한이 없다. 프로그래머, 오퍼레이터 또는 컴퓨터정보처리 담당자들은 물론, 그밖에 정보처리전산망에 연결되어있는 외부인도 본죄의 행위자가 될 수 있다.

본죄의 행위는 '컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 하는 것'이다. '컴퓨터 등 정보처리장치'라 함은 주컴퓨터 뿐만 아니라 네트워크 시스템에서의 단말장치를 포함하는 의미이다. 은행의 현금지급기도 여기에 포함된다. '허위의 정보를 입력한다' 함은 예컨대 허위의 입금데이타를 입력하는 것과 같이 사실관계와 일치하지 않는 자료를 입력함을 말하며, '부정한 명령을 입력한다' 함은 프로그램을 구성하는 개개의 명령을 부정하게 변경, 삭제, 추가하거나 프로그램 전체를 변경하는 등 프로그램을 조작하는 경우를 말한다.[17] '정보처리를 하게 한다'는 것은 (허위의) 데이타를 입력하여 계산처리과정을 실행하게 하여 진실에 반하는) 기록을 만드는 것을 말한다.

여기서 타인의 CD카드를 가지고 현금지급기로부터 예금을 인출하는 행위가 본죄에 해당하는가가 문제된다. CD카드를 습득하고 그 비밀번호를 알아내어 이를 통하여 은행에서 예금을 인출하는 경우, 이를 '허위'의 정보를 입력하는 것으로 볼 수 있는가에는 의문이 있다. 왜냐하면 이는 '허위'가 아니라 진정한 정보를 권한없이 사용하는 것이기 때문이다. 따라서 이를 '허위의 정보를 입력'하는 행위에 해당한다고 보는 것은 타당하다고 하기 어렵다.

독일 형법은 개정형법과는 달리 컴퓨터사기죄(제263a조)에서 '진정한 데이타의 무권한 사용'을 처벌하고 있다.[18] 이를 독자적인 범주로 처벌하는 취지는 단순히 정보를 습득하여 컴퓨터를 기망하여 이를 이용하는 행위까지도 처벌하자는데 있다.[19] 급증하는 CD범죄 및 그 밖의 지불거래수단 남용행위 중 '진정한 데이터의 무권한 사용'이 큰 비중을 차지하고 있으며, 이에 대한 규정이 없을 경우 처벌은 앞서 살핀 바와 같이 무리가 있다. 이에 관하여는 종래 절도죄로 처벌하여 왔으나 우리나라도 '진정한 데이타의 무권한 사용'을 처벌할 수 있는 입법적인 근거를 명백히 하는 것이 타당하다고 생각된다.

2.2.2.2 컴퓨터파괴범죄

가. 컴퓨터業務妨害罪

1) 신설된 조문

— 제314조 제2항 : 컴퓨터등 정보처리장치

14) Dreher/Tr ndle, 263 a Rdn. 2.

15) SK-Samson, 263 a, Rdn. 1.

16) 개정 형법 제348조의2는 편의시설부정이용죄라는 제목하에 "부정한 방법으로 대가를 지급하지 아니하고 자동판매기, 공중전화 기타 유료 자동설비를 이용하여 재물 또는 재산상의 이익을 취득한 자는 3년 이하의 징역, 500만원 이하의 벌금, 구류, 과료에 처한다"는 규정을 두었다. 이는 종래에 절도죄로 의율하여 왔지만, 문제가 없지 아니하였던 사안에 관하여 명확히 한 것이다. 따라서 이러한 행위들은 컴퓨터사기죄와 무관한 것으로 해석할 수있게 되었다.

17) 이재상, 이유서, 제16장 제211조 참조.

18) SK-Samson, 263a Rdn 6.

19) 이재상, 형법개정이유서, 제 14 장 신용, 업무와 경매에 관한 죄 참조.

또는 電磁記錄등 特殊媒體記錄을 손괴하거나 정보처리장치에 허위의 情報 또는 부정한 命令을 入力하거나 기타 방법으로 情報處理에 障碍를 발생하게 하여 사람의 業務를 방해한 자도 제1항의 형과 같다(5년 이하의 징역 또는 1500만원 이하의 벌금).

컴퓨터 등 정보처리장치와 電磁記錄 등 특수매체 기록을 사용하여 이루어지는 업무는 종래의 수작업을 중심으로 행해지던 업무에 비할 수 없을 만큼 대량의 업무를 신속, 정확하게 처리할 수 있게 되었다. 따라서 형법적으로도 이를 보호해야 할 필요성은 매우 크다. 그리고 이와 같은 유형의 업무방해행위는 과거의 업무방해와 같은 제한된 범위에 국한되는 것이 아니라, 기업 전체나 전국적인 범위의 업무에 장애를 야기할 정도로 침해법익의 범위가 광범위할 수 있다는 점에서 더욱 문제시 된다.

개정형법은 컴퓨터 정보처리장치를 손괴하거나 정보처리에 장애를 발생하게 함으로서 업무를 방해하는 행위를 기존의 업무방해죄와 병행하여 처벌하는 구성요건을 두었다.

2) 성립요건

개정형법의 컴퓨터업무방해죄(제314조 제2항)의 보호법익은 '업무'이다. 경제적 업무 뿐 아니라 사회활동으로서의 업무를 포함한다. 컴퓨터 업무방해죄의 행위의 객체는 '컴퓨터 등 정보처리 장치와 電磁記錄 등 특수매체기록'을 통해서 이루어지는 사람의 업무이다. 컴퓨터 등 정보처리장치란 컴퓨터시스템을 의미하며, 특수매체기록에는 앞서 언급한 바와 같이 電磁記錄 이외에 전기적 기록, 자기적 기록, 광기술을 이용한 기록을 포함한다.[20] 본 죄는 컴퓨터 등 정보처리장치에 대한 침해를 그 행위수단으로 하기 때문에, 행위의 객체인 컴퓨터는 그 자체 자동적으로 정보처리를 행하는 기계로서 일정한 독립성을 갖고 업무에 사용되는 것에 한정된다. 따라서 정보처리를 행하지 않는 기계(예컨대 자동판매기)의 구성부분을 이루고 있는 마이크로 프로세서 등은 이에 해당하지 않는다.[21]

본죄는 행위의 태양을 ①컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하는 행위 ②정보처리장치에 허위의 정보 또는 부정한 명령을 입력하는 행위 ③기타의 방법으로 정보처리장치에 장애를 발생하게 하는 행위로 나누고 있다. 따라서 컴퓨터 업무방해는 우선 '컴퓨터파괴'와 '컴퓨터부정조작'으로 인한 업무방해가 수단이 된다.[22] 손괴란 물리적인 파괴나 멸실뿐만 아니라 電磁記錄의 소거를 포함하며, 허위의 정보 또는 부정한 명령을 입력하는 것은 진실에 반하는 자료를 입력하거나 사무처리과정상 주어서는 아니되는 프로그램을 입력하는 것을 말한다. 따라서 이는 컴퓨터사용사기죄의 행위태양과 동일하다(컴퓨터사용사기죄는 이득죄인 점에서 차이가 있다). '기타의 방법'이란 컴퓨터에 대한 가해로 인하여 그 사용목적에 부합하는 동작을 하지 못하게 하거나 사용목적에 어긋나는 동작을 하게 하는 일체의 행위를 말한다. 앞서의 행위태양으로 열거되지 아니한 것으로서 데이터의 무권한사용도 업무방해에 해당될 수 있으며 그외에 전원의 절단이나, 低壓의 배전, 온도, 습도의 조작등 작동환경의 파괴, 통신회선의 절단 등이 여기에 해당한다.[23]

나. 컴퓨터데이타破壞罪

컴퓨터 하드웨어에 대한 손괴는 재물손괴죄(제366조)에 해당한다. 이에 비하여 '컴퓨터범죄'로서의 컴퓨터파괴에서 문제가 되는 것은 컴퓨터에 저장되어 있는 각종 데이타의 손괴행위이다. 컴퓨터 등 특수기억매체에 기록된 데이타 그 자체를 재물로 볼 수 있다면, 이의 손괴행위에 대하여 손괴죄의 적용이 가능할 것이다.[24] 그러나 우리나라에서는 이에 대하여 재물성을 부정하는 것이 다수의 견해였으며[25] 타

20) 이재상, 형법개정이유서, 제 14 장 신용, 업무와 경매에 관한 죄 참조.

21) 大谷實, 앞의 책, 128면.

22) 따라서 컴퓨터데이타손괴 등을 통하여 업무를 방해한 경우에는 제366조의 컴퓨터데이타파괴죄는 법조경합으로서 본죄에 흡수된다.

23) 이재상, 앞의 글, 제14장 참조.

24) 예컨대 Sieber, Computerkriminalit t und Strafrecht, 192면 이하; Krey, Strafrecht, BT, Bd. 4, 88면; Lackner, 303 Rdn 2; Sch nke-Schr der Cramer, 303 Rdn 3등 독일의 통설은 이를 재물손괴죄에 해당한다고 보고 있다. 즉 이를 쌍극자

당하다. 따라서 이를 손괴죄로 처벌하기 위해서는 손괴죄의 행위의 객체를 확장하는 것이 필요하게 된다.

1) 신설된 조문

제366조(재물손괴 등) 타인의 재물, 문서 또는 電磁記錄등 특수매체기록을 손괴, 은닉하거나 기타 방법으로 그 효용을 해한 자는 3년 이하의 징역 또는 700만원이하의 벌금에 처한다.

개정형법은 형법 제366조(재물 또는 문서의 손괴)의 행위 객체에서 '電磁記錄 등 특수매체기록'을 추가하였다.

행위의 객체로서 電磁記錄 등 특수매체기록을 추가한 것은 앞서 본 바와 같이 컴퓨터 데이타등의 소거 또는 변경도 손괴죄로 처벌할 수 있게 하기 위한 것이다.[26] 개정형법은 기존의 문서손괴죄의 행위객체에 전자적 기록을 추가한 일본의 개정 형법의 입법형식을 따른 것으로 보인다. 일본개정형법이 우리나라의 기존 형법 및 형법개정형법과 다른 점은 문서손괴를 단순한 재물손괴와 구분하여 규정하고 있으며, 문서와 컴퓨터데이타가 갖는 사회적, 경제적 효용가치를 인정하여 이들을 재물손괴죄보다 무거운 형을 부과하고 있다는 점이다.

2) 성립요건

개정형법의 電磁記錄損壞罪의 보호법익은 '정보(데이타)이용권'이라고 할 수 있다. 재물손괴죄의 보호법익이 민법상의 소유권임을 감안하여 정보 이용의 측면에서 본 소유권(정보소유권)이라고 말할 수 있을 것이다.[27] 보호의 객체는 전자기록 등 특수매체기록이다.

개정형법은 세가지의 행위유형을 규정하고 있다. 첫째는 '電磁記錄의 손괴행위'이다. 이는 데이타의 내용을 변경시키거나 그 효용을 감소 또는 멸실케하는 행위를 의미한다. 데이타기록장치나 전송매체를 파괴한다든가, 자기테이프에 기록된 종전의 기록위에 새로운 데이타를 덮어 씌운다든가 하는 것이 그 예라 할 수 있다. 둘째는 '電磁記錄의 은닉행위'이다. 이는 데이타를 권한있는 자의 이용가능영역으로 부터 이탈시킴으로써 데이타의 사용을 불가능하게 하는 것을 의미한다. 셋째는 '기타의 방법으로 효용을 해하는 행위'이다. 이는 데이타의 사용능력에 손상을 가함으로써 그 본래의 목적을 충족시킬 수 없게 하여 그 기능을 손상하게 하는 행위를 의미한다.

본죄는 데이타에 관하여 일본 형법 처럼 공전자기록과 사전자기록을 구별하지 않고 있으며, 사회적으로 중요한 의미를 갖는 정보인가의 여부에 따른 구별도 하지 않고 있다.

2.2.2.3. 컴퓨터스파이범죄

가. 컴퓨터데이타探知罪

컴퓨터데이타 탐지의 전형적인 행위유형으로서는 컴퓨터프로그램의 탐지와 컴퓨터 데이타의 탐지를 들 수 있다. 컴퓨터 프로그램의 탐지에 관하여는 현재 〈컴퓨터프로그램보호법〉(1986년 12월 31일 법률 제 3920호)이 제정되어 프로그램 저작자의 권리를 보호하고 있다. 이에 비하여 컴퓨터에 기록된 데이타 역시 보호의 필요성은 크지만 실효적인 보호를 하기가 어려웠다. 왜냐하면 컴퓨터데이타를 탐지하는 행위('컴퓨터스파이행위'라고도 한다)는 점유를 침해하지 않는 특징(이른바 데이타의 '비이전성')을 가지고 있어 재산죄의 구성요건이 적용되기 어려웠기 때문이다. 또 기존의 비밀침해죄(제316조)에 있어서는 '행위의 객체'가, 업무상비밀침해죄(제318조)에 있어서는 '행위의 주체'가 너무 제한적이어서 데이타를 부정입수하고 누설하는 행위를 처벌하기가 어려웠다. 개정형법은 이를 고려하여 '컴퓨터데이타탐지죄'를 비밀침해의 죄에 추가하여 처벌하도록 하였다.

1) 신설된 조문

— 제140조 제3항(공무상비밀표시무효) 전2항 기재의 문서, 도서 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다(5년이하의 징

라하고 하는 다수의 미세한 유체물의 변경으로 보기 때문이다.

25) 이재상, 형법개정안이유서, 제19장 손괴의 죄 참조.

26) 이재상, 앞의 글, 같은 항.

27) SK-Samson, 303 a Rdn 7,8.

역 또는 700만원이하의 벌금).

제316조 제2항(비밀침해) : 封緘 기타 秘密裝置한 사람의 便紙, 文書, 圖書 또는 電磁記錄 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아 낸 자도 제1항의 형과 같다(3년 이하의 징역이나 500만원 이하의 벌금).

구형법은 봉함 등을 개봉[28]하지 않고 기술적으로 그 내용을 지득하는 행위를 처벌할 수 없었기 때문에 이를 입법적으로 해결하였다. 나아가 행위객체에 '電磁記錄 등 특수매체기록'을 추가하였다. 기술적 수단으로 편지 등과 전자적 기록 등의 비밀을 알아낸 자를 처벌할 것을 규정하고 있는 독일 형법 제202조(신서의 누설) 및 제202a조(데이타탐지죄)와 오스트리아 형법 제118조 제2항 제2호를 계수한 것으로 보인다.

2) 성립요건

개정형법 제140조 제3항의 보호법익은 '공무상의 비밀'이며, 제316조 제2항의 보호법익은 '개인의 비밀'이다. 오늘날 비밀은 종래와 같이 문서의 형태로서 보존될 뿐 아니라, 컴퓨터 등 특수매체기록의 형태로 보존되는 경우가 많아졌기 때문에 이의 보호의 필요성은 크다고 할 수 있다. 구형법으로서는 이와 같은 형태의 비밀을 보호할 수 없었기 때문에 형법 제140조 제3항과 동법 제316조(비밀침해죄)에 행위의 객체와 행위의 수단을 추가하였다.

먼저 개정형법은 행위의 객체를 종래의 편지, 문서, 도서 등 유형적 기록물 이외에 '電磁記錄 등 특수매체기록'으로 확장하고 있다. 전자기록이란 컴퓨터 디스크에 수록된 데이타 뿐 아니라, 전기적 혹은 전자적으로 녹음테이프, 녹화테이프, 광디스크 등에 기록된 데이타가 포함된다. 독일 형법 제202조 a의 (2)항은 이를 "전기적, 전자적 기타 직접적으로 지각할 수 없는 상태로 입력되어 있거나, 전송중인 데이타"라고 넓게 정의함으로써, 전송중인 데이타도 행위객체에 포함시키고 있다.[29] 이에 비하여 개정형법은 행위의 객체를 '전자적 기록 등 특수매체기록'이라고 규정함으로써 전송중인 데이타가 포함되는가에 대해 논란이 있을 수 있다. 문언상으로는 전송중인 데이타는 '기록'이라고 할 수는 없으므로 포함되지 않는다고 보아야 할 것이다. 이의 침해행위는 앞서 살핀 바와 같이 〈전산망보급확장과 이용에 관한 법률〉에 따라 처벌된다.[30]

개정형법은 행위의 태양으로 '개봉'하는 이외에 '기술적 수단을 이용하여 행위객체의 내용을 알아낸 행위'를 추가하고 있다. 이와 같은 기술적 수단을 이용하는 방법으로는 편지, 문서의 내용을 투시장치를 통해 지득한다든가, 데이타의 내용을 기술적 방법으로 탐지하는 경우 등을 생각할 수있다.

본죄는 기술적 수단을 이용하여 전자적 기록의 내용을 '지득함'으로써 성립한다. 지득한다 함은 봉함 또는 비밀장치한 객체의 내용을 알게 되는 상태를 의미하는데, 반드시 내용을 알아야 하는 것은 아니고 지득'할 수 있는' 단계에서도 본죄는 성립한다고 보아야 할 것이다. 따라서 편지, 문서, 도서의 경우 비밀장치를 개봉하였으나 내용을 지득하지는 않은 경우에도 본죄가 성립하는 것은 물론, 전자적 기록 탐지행위의 경우 기술적으로 데이타의 내용을 지득하지 않고 탐지하여 복사·전달하는 경우에도 본죄는 성립한다고 보아야 한다. 컴퓨터의 특성상 행위자가 그 데이타의 내용을 알지 못하고서도 데이타를 유출시킴으로써 개인의 비밀을 침해할 수 있는 가능성은 크며, 이러한 행위도 본죄에 해당한다.

한편 오늘날 크게 문제가 되고 있는 기업비밀의 누설, 탐지행위에 관하여는 개정형법에는 규정되지 않았다. 이는 1991년 12월 31일 개정된 부정경쟁방지법 제 18조(제1항 3호)에서 기업의 생산기술에 관한 영업비밀을 누설하는 행위를 처벌하는 규정을 둔 점을 고려한 결과이다.[31]

28) 개정 형법에서는 종래의 '開披'라는 문구를 쓰지 않고 開封이라는 문구를 사용하고 있다.

29) 이재상, 형법개정이유서, 제 12장 비밀침해의 죄 참조.

30) 전산망에 의하여 관리되는 경우가 아닌 경우에는 〈통신비밀보호법〉 제2조 제2호("유선, 무선, 광선, 기타 전자적 방식에 의하여 모든 종류의 음향, 문언, 부호 또는 영상을 송신하거나 수신"하는 경우), 제3조("감청하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취"한 자는), 제16조 제1항에 의하여 7년 이하의 징역으로 처벌할 수있다.

31) 부정경쟁방지법 제18조 제1항 제3호 참조.

2.2.2.4 權限없는 컴퓨터의 利用

권한없이 컴퓨터를 이용한다 함은 권한없이 타인의 컴퓨터 시스템을 이용하거나 권한은 있으나 그 범위를 넘어서 이용하는 것을 말한다. 예컨대 기업의 종업원이 그 기업의 컴퓨터 시스템을 사적 목적을 위해 이용하는 경우나, 종업원 아닌 외부인이 자신의 목적을 위해 이를 이용하는 경우가 여기에 해당한다.

이와 같은 부정이용행위는 형법의 적용과 관련하여 컴퓨터의 사용절도 및 전기에 대한 절도죄, 사기죄 그리고 배임죄 등이 문제된다. 그러나 배임죄에 있어서는 행위주체가 신뢰관계에 있는 자에게 한정되므로 그 범위가 너무 좁고, 전기절도에 있어서는 동 행위의 목표가 전기사용이 아니라 기계의 이용을 통한 재산적 이익의 취득이라는 점으로 미루어 절도죄의 적용에는 무리가 있다. 결국 신뢰관계를 기초로 하지 않는 내부인이나 외부인에 의한 '시간절도'는 컴퓨터의 사용절도 이외에 달리 해석하기 어렵다.

이와 같은 컴퓨터의 무권한 이용에 대한 입법태도는 나라마다 다르다. 미국의 연방과 주법은 시간절도를 서비스절도라는 이름으로 처벌하고 있고, 캐나다의 개정형법(1985년)도 '권한없이 컴퓨터서비스를 취득하는 행위'를 처벌하고 있다. 독일은 1985년 의회의 형법개정안에서 컴퓨터 무권한사용을 처벌하는 규정을 두었으나 제2차 경제범죄방지법에서는 이 규정을 삭제하였다. 스위스, 오스트리아, 프랑스형법개정안 등에서도 동 행위를 처벌하는 규정을 두고 있다.

컴퓨터무권한사용에 대하여 각국이 전면적으로 처벌하고 있지 않은 이유는 범죄화원칙의 문제와 규제의 실효성에 문제가 있는 것이 아닌가 생각된다. 즉 컴퓨터 무권한사용의 실제 발생 빈도, 적발가능성, 민사적 구제가능성 등의 면에서 이에 대한 형법적 대응에 큰 실효성이 없는 것이 아닌가 생각된다. 또 무권한 사용되는 컴퓨터의 범위와 정보의 범위를 어디까지 인정할 것인가를 정하는 것도 쉽지 않은 문제이다.

개정형법은 제331조의 2에서 '자동차 등 불법사용'이라는 제목하에 "권리자의 동의없이 타인의 자동차, 선박, 항공기 또는 원동기 장치자전거를 일시 사용한 자는 3년 이하의 징역, 500만원 이하의 벌금, 구류, 과료에 처한다"고 규정하였다. 이로써 우리나라에서도 일정한 재물에 대하여 사용절도를 인정하는 태도를 취하고 있으나 컴퓨터무권한사용에 관하여는 입법자는 침묵하고 있다. 따라서 현단계에서는 이는 민사문제로 처리하는 것이 타당하다고 생각된다.

2.2.2.5. 기 타

가. 권리행사방해죄

1) 신설된 조문

- 제323조(권리행사방해) 타인의 점유 또는 권리의 목적이 된 자기의 물건 또는 전자기록 등 특수매체기록을 취거, 은닉, 또는 손괴하여 타인의 권리행사를 방해한 자는 5년 이하의 징역 또는 700만원 이하의 벌금에 처한다.

2) 구성요건

개정형법은 권리행사방해죄의 객체에 '電磁記錄 등 특수매체기록을' 추가하였다. 앞서 언급한 바와 같이 電磁記錄 등 특수매체기록은 직접 재물로 보기 어려우므로 재물에 국한되는 권리행사방해죄의 행위의 객체를 확대하기 위하여 별도의 문구를 삽입한 것이다.

여기서 손괴라 함은 디스크나 테이프 자체의 손괴와 같이 재물손괴의 범주에 포함되는 것은 제외되며, 기록의 전부 또는 일부의 소거행위가 이에 해당한다. 프로그램이나 데이터를 소거, 멸실시키지 않고 단지 이용불가능하게 하는 행위는 은닉이라고 할 수 있다.

3. 개인정보의 보호

정보사회가 도래함에 따라 개인의 신상에 관한 여러 측면의 정보가 수집, 관리되게 되었다. 그런데 이러한 정보가 간단한 조작에 의하여 종합, 정리되어 알려지게 되면 개인은 문자 그대로 알몸과 같은 '유리처럼 들여다 볼 수 있는' 지위에 놓이게 된다. 이는 오늘날 헌법적으로 보호되는 개인의 프라이버시 권을 침해하게 되는 결과가 된다.

1995년 1월 부터 발효한 〈공공기관의개인정

보보호에관한법률)은 이러한 문제에 대응하여 마련된 법이다. 이에 의하면 공공기관(이에는 국가, 지방자치단체뿐 아니라 교육법 등 법률에 의하여 설치된 각급학교, 정부투자기관, 특별법에 의하여 설립된 특수법인 등이 포함된다)은 컴퓨터로 처리되는 개인정보를 보호하여야 하며, 이를 누설(무권한 처리, 타인의 이용에의 제공) 한 경우에는 3년이하의 징역 또는 1천만원 이하의 벌금에 처하여 지게 된다(동법 제 23조 2항). 또 개인정보의 변경, 말소행위에 대하여는 더욱 중하게 처벌하여 10년 이하의 징역에 처하게 하고 있다(동법 제23조 제1항). 詐僞, 기타 不正한 방법으로 공공기관으로 부터 처리정보를 열람 또는 제공받은 자는 2년 이하의 징역 또는 700만원 이하의 벌금에 처한다(동법 제23조 3항).

또 1995년 7월 부터 누구나 공공기관이 보유 관리하는 자신에 대한 개인정보를 열람할 수 있게 되었으며, 잘못 입력된 개인정보에 대하여 정정을 요구하면 공공기관은 이를 정정하도록 하였다.

4. 국가기밀의 보호

초고속 정보통신망이 구축 운용되는 경우 국가적 차원에서 고려해야 할 사항으로서 중요한 것은 '국가기밀의 누설'일 것이다. 우리나라의 국가보안법은 '국가안전에 대한 중대한 불이익을 회피하기 위하여 한정된 사람에게만 지득이 허용되고 적국 또는 반국가단체에 비밀로 하여야 할 사실, 물건, 지식'을 '탐지, 수집, 누설, 전달, 중개한 행위'에 대하여는 사형, 무기징역이라는 중형을 과하고, 위의 사항 이외의 군사상 기밀 또는 국가기밀에 대하여 앞의 행위를 한 자에 대하여는 사형, 무기 또는 7년 이상의 징역을 과하고 있다.

판례는 간첩의 정의로서 '간첩이란 단순한 군사기밀뿐만 아니라 정치, 경제, 사회, 문화, 사상 등 각 방면에 걸쳐서 우리나라의 국방상 적국에 알리지 아니하거나 확인되지 아니함이 우리나라의 이익이 되는 모든 기밀사항을 탐지, 수집함을 말하고, 국내에서 신문, 잡지, 라디오 등에 보도되어 알려진 사항이라 하더라도 적국에 유리한 자료가 될 경우에는 기밀에 포함된다'고 하여 간첩행위의 범위를 폭넓게 인정하고 있다.

이렇게 볼 때 국가기밀의 보호에 관하여는 법제상의 미비는 없는 것으로 생각된다. 왜냐하면 전자기록 등 국가기밀의 존재형태에 대한 제한이 법규상으로나 해석상으로나 존재하지 않기 때문이다. 따라서 전통적인 정보의 탐지, 수집, 누설, 전달, 중개행위에 대한 규정이 전자기록이나 전송중의 신호상태에 있는 경우에 대하여도 적용될 수있다. 그리하여 행위주체와 행위양상에 따라 형법상의 간첩죄, 일반이적죄, 외교상의 기밀누설죄 등과 국가보안법, 군사기밀보호법, 군형법 등이 적용가능하다.

다만 문제는 오늘날 민주주의의 확대를 통해서 알 권리의 일환으로 국가 정보의 공개를 요구할 권리가 인정되어 가고 있다는 점이다. 따라서 종래 국가기밀의 내용과 범위가 이와 관련하여 조정되어야 할 필요성이 대두되고 있다. 외국의 예를 보면 기밀을 우리나라처럼 포괄적으로 정의하지 않고 실질적으로 정의하여, "공공의 토론이나 국민적 감시에 친하지 않는 사항, 공개되는 경우 행정의 목적이 상실되는 사항, 공공의 토론이나 국민적 감시에 우선하여 공무수행을 할 필요가 있는 사항"으로 실질화함으로써 광범위하게 알권리를 인정하는 방향으로 나아가고 있으며, 다만 법령에 의한 비밀, 범죄수사정보, 공개될 경우 원활하고 공정한 행정에 지장이 있는 정보, 의사형성과정에 있는 정보등은 예외적으로 공개를 거부할 수 있도록 하고 있다.

따라서 사실상 보안과잉이었다고 말할 수 있을 정도였던 우리나라의 사정에서 이에 관한 보다 실질적인 기준을 정하여 국민의 알권리를 보장하는 한편 국가의 핵심 기밀도 보호하는 노력이 있어야 할 것으로 생각된다.

5. 해커의 침입으로부터의 보호

해커의 침투행위를 처벌할 수 있는 처벌규정으로는 1986년에 제정되고 1992년에 개정된 〈전산망보급확장과이용촉진에관한법률〉 제22조 제2항과 동법 제25조의 규정이 있다. 제22

조 제1항은 전산망사업자에게 전산망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 강구할 의무를 부과하고, 동조 제2항은 "누구든지 불법 또는 부당한 방법으로 제1항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다"고 규정하였다. 이에 대한 벌칙은 3년이하의 징역 또는 1천만원 이하의 벌금에 처한다(동법 제29조).

제25조는 "누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하여서는 아니된다"고 규정하고 이에 대한 벌칙으로서, "제25조의 규정에 위반하여 타인의 비밀을 침해 또는 누설한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다"(동법 제30조 제1항)고 규정하고, 동조 제 2항은 "전산망사업에 종사하는 자가 제 1항의 죄를 범한 때에는 5년 이하의 징역 또는 2천만원 이하의 벌금에 처한다"고 규정하였다. 따라서 해커를 처벌할 수 있는 규정은 마련되어 있다고 할 수 있지만, 이를 위하여는 형사소송을 거쳐야 하고 이에는 증거가 필요하기 때문에, 흔적을 남기지 않는 침투는 처벌하기가 사실상 곤란하다는 점에 유의하여야 한다. 이에 대한 대비가 요망된다.

또 외국에서 외국인이 이러한 행위를 하는 경우 어떻게 처벌할 수 있는가. 우선 이 법에는 형법총칙이 적용되므로 형법 제6조의 보호주의 규정이 적용되어 이 법은 외국인에게도 적용될 수 있다.

다만 동조 단서에 따라 행위지의 법률에 의하여 범죄를 구성하지 아니하거나 소추 또는 형의 집행을 면제할 경우에는 예외로 하게 되므로 행위지 국가의 법에 의존하게 된다. 그리고 외국인 행위자에게 형법을 적용하는 경우 처벌을 위하여는 범죄인 인도에 의해 신병을 인도받아야 한다. 그런데 현재 우리나라가 범죄인 인도 조약을 체결한 나라는 호주, 스페인, 카나다, 필리핀, 칠레의 5개국에 불과하며(이 가운데 앞의 세나라에 대하여는 발효하였으며, 뒤의 두 나라는 미비준 상태이다. 금년중 미국, 프랑스, 홍콩 등과 범죄인인도조약 체결 추진중이다), 미국, 캐나다, 호주와 형사사법공조조약을 체결하고 있다.

6. 음란물 등으로부터의 보호

형법학상 모든 음란물을 금지하여야 하는가에 관하여는 논란이 있다. 왜냐하면 어느 정도의 성적 표현은 헌법상 보장되는 표현의 자유의 범위에 들어갈 수있기 때문이다. 따라서 외국에서는 음란물을 획일적으로 금하지는 않고 허용하되 '관리의 대상'으로 하는 성표현물과 철저하게 금하는 성표현물로 나누고 있다. 대체로 그 표현의 노골성이 강하거나 폭력적, (유아에 대한) 남용적 성행위를 다루는 표현물을 '경성 성표현물'(hard-core pornography)이라고 하여 금하고, 그렇지 않은 표현물을 '연성 성표현물'(soft-core porno graphy)이라고 하여 관리의 대상으로 하는 것이다. 관리의 대상이라 함은, 이러한 성표현물에 노출되기를 원하지 않는 사람들을 위하여 이를 시야에 직접 들어오게 하지 않고 일정한 지역을 정하여 은폐된 상태에서 상연하게 한다든가 눈에 잘 띄지 않는 코너에 진열하여, 한편으로는 이를 원하는 사람이 접근, 향유할 수 있게 하면서 다른 한편으로는 원하지 않는 사람도 보호하는 정책을 시행하고 있다.

우리나라에는 이에 관하여 대법원은 비교적 보수적인 태도를 취하고 있다. 그리하여 단순한 나체화는 음란물이 아니라고 보면서도(최근의 유0실, 산타 페 누드화집에 대한 판결), 그것이 성적 수치심을 유발하거나 성욕을 자극하거나 성도덕을 침해하는 경우에는 음란물이 된다(즐거운 사라 사건에 대한 판결)고 하고 있다.

그런데 오늘날 전통적으로 서적이나 영화(필름)의 형태로 존재하던 음란물이 직접적으로는 전혀 可視性, 可讀性이 없는 음반, 테이프(비데오, 카세트 테이프 등), CD-ROM, 그리고 전자적 신호전송의 현태로 존재하고 있어 형법적용의 문제가 되고 있으며, 나아가 이들이 대체로는 노출이 금지되어 있는 청소년들에게 무차별하게 노출되는 문제를 야기하고 있다.

이를 처벌하는 근거 규정으로서는 형법의 음란물 관련 규정을 들 수 있다. 그런데 이에 대하여는 경우를 나누어서 보아야 할 것이다. 우선 음란 비디오테이프나 CD-ROM을 판매하는

경우에는 형법상의 음화등 판매죄에 직접 해당한다고 보기는 어렵고, 음반법 기타 특별법상의 처벌규정에 따라 처벌된다. 이에 비하여 음란물을 전기적 신호로 컴퓨터 통신망에 올린 경우 형법 제 243조의 음화 등 반포죄의 규정에 해당할 가능성이 있다. 그것은 이 규정이 음란물의 '공연전시'를 처벌하고 있기 때문이다. 즉 이러한 행위가 공연성을 갖는 경우에는 처벌할 수 있다고 하겠다.

컴퓨터통신망의 '게시판' 등을 이용하여 사기, 협박, 공갈, 명예훼손, 모욕 등을 하는 행위를 어떻게 볼 것인가. 주지하는 바와 같이 컴퓨터 통신망에는 회원들간에 정보교환을 위하여 (전자)게시판을 운영하여 글을 올리고 또 열람할 수 있게 하고 있다. 이를 이용하여 앞에 열거한 범죄행위를 하는 경우, 사기, 협박, 공갈 등의 행위가 성립하는 데에는 별다른 이론이 없다. 왜냐하면 이는 전기적 신호로 바뀐 음성을 통해서 협박등의 행위를 하는 '전화를 통한 협박'이 타인에 대한 '害惡의 告知'로서 인정될 수있는 것과 같기 때문이다.

명예훼손이나 모욕의 경우에는 약간의 문제가 있다. 왜냐하면 이 경우는 앞서의 다른 범죄들과는 달리 그 성립에 '공연성'을 요구하고 있기 때문이다. 공연성을 인정하기 위하여는 판례의 표현에 따르자면 이른바 불특정 다수인에 대한 '傳播可能性'이 있어야 한다. 따라서 컴퓨터 통신망에 올린 표현이 불특정, 다수인에 대한 전파가능성이 있는가의 여부가 관건이 된다.

이는 둘로 나누어서 살펴보는 것이 타당할 것이다. 첫째 불특정 다수인이 접근할 수 있는 게시판에 명예훼손 내지 모욕의 표현을 올린 경우는 불특정 다수인에 대한 전파가능성이 있다고 볼 수 있다. 이는 가능성있으면 성립되는 것이기 때문에 설사 그 당시 우연히 아무도 그 게시판을 참조하지 않았다 하더라도 이 죄는 성립한다고 하겠다. 둘째로 전자메일 등 불특정다수인이 접근할 수는 없는 난을 이용한 경우에는 공연성의 요건을 결하므로 이 죄는 성립할 수 없다. 설사 이 내용을 해커가 침입하여 알아내어 전파시켰다 하더라도 다름이 없다.

7. 결 어

컴퓨터 범죄에 효율적으로 대응하는데 있어서 처벌규정을 두는 것으로서 만족할 수는 없다. 우선 기술적, 행정적 통제방법을 세밀하게 구사할 필요가 있다. 그러나 물론 궁극적으로 형벌을 통한 대응도 고려하지 않을 수 없을 것이다. 이에 관하여는 이번의 형법 개정을 통해서 법제상으로--약간의 문제가 없는 것은 아니지만--일단 대응책이 정비되었다고 할 수 있다.

그러나 이와 같이 법이 정비되는 경우에도 문제로서 남는 것이 있다. 우선 이러한 범죄의 暗數化의 문제이다. 컴퓨터 범죄는 화이트 칼라 범죄의 성격이 강해서 범죄가 발생해도 이를 '범죄'로서 처리하지 않는 경향이 있다. 즉 기업(일반 기업체, 은행 등)자체가 이러한 범죄행위가 외부에 드러나는 것을 꺼려서 사법적 처리로 이행하지 않고 내부에서 징계 등으로 사건을 마무리하는 경우가 많다. 이것이 컴퓨터 범죄를 방임, 조장하는 분위기를 형성시켜서는 안된다. 둘째로 컴퓨터 범죄의 형사소송상의 난점은 앞서도 지적하였다. 증거가 없어서 처벌할 수 없는 상황에 빠지지 않기 위해서는 증거를 남게 하는 기술적인 뒷받침이 중요하다. 끝으로 국제화하는 컴퓨터 범죄에 대응하여 국제적인 수사망의 형성과 효율적인 처벌을 위한 국제형사사법공조 등의 국제적 대비책을 마련하는 것도 중요한 사항이다. 이러한 문제를 해결하기 위하여는 앞으로 많은 노력을 경주하여야 할 것이다.

장 영 민

1976 서울대학교 법과대학
1979 서울대학교 석사
1990 서울대학교 박사
1982~현재 인하대학교 법정대학 법학과 전임강사, 조교수, 부교수, 현재 정교수 한국 형사정책연구원 초빙 연구위원 역임.