향후 신종범죄 추세전망 및 대응방안에 관한 연구

≪研 究 陣≫

연 구 위 원 :	강 동 범 (서울시립대 교수)
	천 종 철 (서 원 대 교수)
연구지도위원 :	이 형 국 (연세대 법대교수)
연 구 실 장 :	임 영 규 (총 경)
연 구 관 :	이 돈 일 (경 감)

목 차

표 목 차

Ⅰ. 머리말

신종범죄가 무엇이며 어떠한 행위유형이 여기에 해당하는가에 대하여 견해가 일치되어 있지 않다. 이는 신종범죄가 체계적으로 연구되어 학문적으로 규명된 형법학상의 개념이 아니라 다분히 현상적(現象的)인 집합용어라는 점에서 기인한다고 생각된다. 여기서는 연구의 편의상 신종범죄라고 볼 수 있는 위법행위를 두 개의 범주로 구분하여 수법과 특징을 살펴보고, 향후 그 발생추세를 전망함으로써, 이들 범죄에 대하여 적절한 대응방안을 강구하고자 한다. 신종범죄의 첫 번째의 범주로는, 전통적인 범죄행위와 동등한 불법내용을 갖고 있으나 사회환경과 과학기술의 발달에 따라 과거에는 전혀 생각할 수 없었던 새로운 형태의 사회유해적 행위를 들 수 있다. 이것이 고유한 의미의 신종범죄에 해당하는 것으로 신종범죄라는 용어로 표현되는 대상 중 범위가 가장 좁기 때문에 협의의 신종범죄라고 부를 수 있는데, 여기에는 컴퓨터범죄, 신용카드범죄, 홈(폰)뱅킹범죄, 소위 정보통신악용범죄 등이 해당된다. 두 번째의 범주는 전통적인 범죄에 포함되지만 과학기술의 발달 등 사회환경의 변화에 따라 수법이 새로워진 범죄행위이다. 이는 새로운 수법의 범죄(신종수법범죄)로서 광의의 신종범죄라고 부를 수 있을 것이다. 이에는 복사기의 발달·보급에 따른 통화·유가증권의 위조·변조, 첨단장비를 이용한 몰래 카메라 촬영이나 도청, 전화방을 통한 윤락행위의 알선, 위장교통사고 야기후 보험금편취, 의학의 발달에 따라 장기이식수술이 가능해진 점을 악용하여 장기매매를 빙자한 사기, 무인경비시스템의 허점을 이용한 절도 등을 포함시킬 수 있다. 물론 신종범죄와 신종수법범죄의 구별이 반드시 명확한 것은 아니지만 전자는 과거에는 행하여지지 않았던 불법유형임에 반하여 후자는 이미 행하여졌던 불법유형이지만 수법만이 새로워진 것을 의미하는 것으로 구분하기로 한다.

이하에서는 신종범죄를 신종범죄와 신종수법범죄의 둘로 나누어 각각에 대하여 추세를 전망하고 이들 범죄에 효과적으로 대처하기 위한 법적 그리고 제도적 대응방안을 제시하여 보기로 한다. 대응방안과 관련하여서는 먼저 현행법의 어떠한 규정이 이들 신종범죄에 적용될 수 있으며(적용법조의 문제) 처벌의 흠결은 없는가를 규명하여, 새로운 처벌규정의 신설 필요성을 검토한다. 다음으로 제도적 대응방안으로 이러한 신종범죄의 방지와 효과적인 수사를 위한 경찰조직(인력과 장비)의 대응수단과 행정적 대응

수단을 검토한다.

Ⅱ. 신종범죄의 추세전망과 대응방안

1. 컴퓨터범죄

가. 의의와 유형

컴퓨터와 정보통신기술의 결합에 의하여 사회경제생활의 거의 모든 영역에서 획기적인 변화가 초래됨에 따라, 예컨대 은행의 컴퓨터시스템을 악용한 은행원 등에 의한 허위예금자료의 입력, 타인의 현금카드나 전화카드의 磁氣띠부분의 부정작성, 해커에 의한 정보의 부정입수나 컴퓨터파괴행위에 의한 업무방해, 컴퓨터통신망을 통한 음란물 등 불건전정보의 대량유통, 전자우편시스템을 이용하여 수많은 전자우편을 전송하여 전자우편체증을 유발시켜 송신장애를 야기하는 메일폭탄 등 부정행위가 적지 않게 발생하고 있다. 이러한 부정행위는 컴퓨터와 정보통신기술의 발전과 이에 대한 사회의 의존도가 높아짐에 따라 급격하게 증가할 것이다. 이러한 새로운 사회유해적 행위인 컴퓨터범죄의 개념에 관하여는 견해가 일치되어 있지 않으나[1] "컴퓨터의 자료처리과정과 관련되는 위법행위"로 파악하고자 한다.[2]

컴퓨터범죄의 유형은 보는 관점에 따라 다양하게 분류될 수 있으나 지배적인 견해는 컴퓨터의 기능과 행위유형을 기준으로 자료의 부정조작(Computermanipulation), 컴퓨터파괴(Computersabotage), 컴퓨터스파이(Computerspionage), 컴퓨터의 권한없는 사용(unbefugte Computernutzung)으로 분류한다.[3] 이 외에 CD(Cash Dispenser)범죄를 제5

1) 이에 관하여는 강동범, 컴퓨터犯罪와 개정형법, 법조 1997.8, 107면 이하; 장영민/조영관, 컴퓨터범죄에 관한 연구, 한국형사정책연구원, 1993, 24면 이하 참조.

2) 장영민/조영관, 위의 책, 27면. 이철, 법무부의 정책과제와 입법적 대응 - 컴퓨터범죄를 중심으로 -, 정보화사회의 전개와 입법적 대응, 한국법제연구원, 1992, 111면은 광의설을 입장에서 '범행수법에 컴퓨터기술에 관한 지식이 필수적으로 수반된 것으로 한정' 하여 정의하고 있다.

3) K. Tiedemann, Wirtschaftsstrafrecht und Wirtschaftskriminalit t Bd. 2, 1976, 150면 이하; U. Sieber, Computerkriminalit t und Strafrecht 2.Aufl., 1980, 39면 이하; L. Rohner, Computerkriminalit t, 1976, 4면; 장영민/조영관, 앞의 책, 32면 이하.

의 유형으로 분류하는 견해도 있으나 CD범죄는 권한없는 자가 현금자동인출기에 타인의 비밀번호 등을 입력하여 현금을 인출하거나 이체시키는 것이므로 자료의 부정조작의 특별한 형태로 파악될 수 있어 이를 독자적인 컴퓨터범죄의 유형으로 구별할 필요는 없을 것이다. 컴퓨터범죄를 이와 같이 분류할 때 실제로 발생하는 컴퓨터범죄가 위의 어느 한 유형에만 해당하는 것은 아니고, 경우에 따라서는 여러 유형이 결합된 컴퓨터범죄도 많을 것이다. 예컨대 컴퓨터파괴의 경우 파괴대상이 된 전산시스템에 접속하기 위한 비밀번호나 ID 등을 해킹을 통하여 알아낸 후(컴퓨터스파이) 이를 이용하여 전산시스템에 접속하여 프로그램이나 자료를 파괴하게 될 것이다(컴퓨터파괴). 즉 위에 제시된 컴퓨터범죄의 유형은 현실적으로 발생하는 컴퓨터범죄가 위의 4가지중 어느 하나에만 속한다는 의미는 결코 아니다.

나. 수법과 특징

1) 자료의 부정조작

① 수법

자료의 부정조작이란 행위자가 컴퓨터의 처리결과를 변경시키거나 이로 인하여 타인의 손해하에 자신이나 제3자의 재산적 이익을 얻을 의도로 컴퓨터의 자료처리과정에 간섭을 행하는 것을 의미하는 것으로 컴퓨터조작 또는 자료변경이라고도 한다. 이러한 자료의 부정조작은 행위자가 자신의 목적을 달성하기 위하여 컴퓨터흐름의 어느 단계에서 부정조작을 하는가에 따라 세분될 수 있다. 첫 번째의 가능성은 입력단계, 즉 컴퓨터에 자료를 입력시키는 상황에서 존재한다. 두 번째의 가능성은 자료의 처리단계, 즉 컴퓨터의 프로그램에 따른 처리결과를 변경시키거나 거짓의 콘솔조작에 의하여 발생할 수 있다. 세 번째는 출력단계, 즉 컴퓨터에 의해 올바르게 출력된 후 그 출력결과를 변경하는 것이다. 이들을 각각 입력조작, 프로그램조작, 콘솔조작 그리고 출력조작이라고 할 수 있다.

자료를 부정조작하는 수법은 조작이 행하여지는 장소나 목적에 따라 상이하다. 자료의 부정조작이 가장 빈번하게 행하여지는 곳이 금융기관인바, 그곳에서 이루어지는 조작수법은 다음과 같은 것이 있다. 첫째의 방법은 실제로는 입금하지 아니하였음에도 불구하고 단말기취급자가 예금이 된 것처럼 가장하여 허위의 예금자료를 입력한 후 인출하는 방법으로 이러한 수법이 가장 많이 사용되고 있다. 실제로 제일은행 관악지점의 대리 강모씨(34)는 전산조작으로 국민·신한은행 봉천지점 등 주변 5개 은행의 자기

계좌로 계좌당 5천만원씩 위장 온라인 입금시킨 뒤 점심시간에 모두 인출해 달아난 바 있으며(중앙일보 1996.5.30), J은행 구로동지점 대리인 신모씨는 아내 양모씨(32)와 짜고 자신이 근무하는 은행의 단말기에 접근하여 자신의 계좌에 3억9천1백만원을 입금한 것처럼 조작하고, 아내 양씨가 6곳의 은행지점을 돌아다니며 3억6천만원을 인출하고, 남편 신씨는 해외로 달아난 바 있다(동아일보 1998.3.17).

둘째는 대출을 가장하여 컴퓨터단말기를 조작한 후 인출하는 방법이다. 실제로 인천지검 부천지청에 따르면, 외환은행 부천중동지점 대출담당 직원 김모씨(28)는 자신의 친척 김모씨 명의로 2천만원을 대출하는 것처럼 컴퓨터단말기를 조작해 불법인출하는 등 1년간 16차례에 걸쳐 같은 방법으로 고객돈 4억5천1백만원을 빼내 가로챈 행위로 절도혐의로 구속된 바 있다(동아일보 1996.8.14).

셋째는 아직 결제가 되지 않은 당좌수표나 어음을 자기앞수표로 결제하는 방법으로 바꿔치기하여 입력한 후 인출하는 방법이다. 실제로 제주은행 영업부 당좌담당대리 김모(34), 당좌담당 한모(32·여), 수납담당 김모(26·여), 어음교환담당 강모(23·여)씨 등은 한모씨의 오빠가 경영하는 여행사가 경영악화로 부도직전에 이르자 이를 도와주기 위하여 오빠가 제시한 2억5천만원짜리 당좌수표를 자기앞수표로 입금된 것처럼 입금전표를 위조, 온라인단말기의 입금내용을 조작하는 수법으로 약 8개월여 동안 2백80차례에 걸쳐 1백4억7천4백여만원을 부정인출한 바 있으며(경향신문 1992.9.20), 강원은행 옥천동지점에 근무하던 여행원 김모씨(24)는 약 3개월에 걸쳐 당좌수표와 어음을 자기앞수표로 결제하는 등의 방법으로 전산망을 조작하여 수억여원을 횡령한 바 있다(동아일보 1997.6.2).

넷째의 방법은 소위 휴면계좌를 이용하여 일정한도액의 카드론(일명 마이너스통장)이 가능하도록 조작한 후 이를 인출하는 것이다. 실제로 축협안양지점 대부계장인 정모씨(38)는 1996년 9월경부터 10월말까지 자신이 근무하는 지점의 거래자 명단 중 장기간 거래가 없는 고객 25명의 성명, 주민등록번호, 주소를 알아내서 은행 컴퓨터 단말기를 조작하여 최고 5천만원까지 인출되는 일명 마이너스 통장 25개를 개설한 후 알고 지내던 이모씨(34)와 정모씨(29)를 통하여 CCTV가 설치되지 않은 서울, 경남북, 전남북 등의 축협지점을 찾아다니며 93회에 걸쳐 1회에 1천만원씩 9억3천만원을 인출토록 하여 그중 33%인 2억8천만원을 이모씨와 정모씨에게 지급하였다.

다섯째로는 단말기 취급자 아닌 경우에 취급자가 자리를 비운 사이를 이용하여 단말기에 접근하거나 컴퓨터 입력키 열쇠를 훔쳐 내서 단말기를 조작하는 수법이다. 실제로

서울 서대문구 충정로 3가 조흥은행 충정로지점에서 이 은행 계산담당직원 김모씨(25)가 외환계 김모 대리 책상서랍에서 컴퓨터 입력기 열쇠를 훔쳐내 예금입력장치를 조작, 오전에 미리 가명으로 개설해 둔 본점 영업부와 명동지점 계좌에 각각 1억5천만원씩 총 3억원을 입금한 뒤 다음날 오전 10시30분께 두 지점에서 각각 1억2천만원씩을 빼내 달아난 사건(한겨레신문 1989.8.26), H은행 일산지점에 근무하는 행원 김모씨(28)는 근무시간 중 단말기취급자 김모양이 잠시 자리를 비운 사이 단말기를 조작하여 자신의 계좌에 3억2천6백만원이 입금된 것처럼 꾸며 범행을 공모한 황모씨(27) 등으로 하여금 같은 은행 마포지점에서 인출하게 한 사건이 있었다(경향신문 1991.10.14).

그밖에도 금융기관의 대출내역에 관한 컴퓨터자료를 소거하여 마치 대출이 없거나 일부 대출금액이 변제된 것처럼 조작하는 방법도 있을 수 있다. 이들 수법은 이미 수차에 걸쳐 행하여졌는데 비교적 초보적인 수준에 지나지 않아 내부통제 시스템에서 조금만 감독·통제를 하면 쉽게 적발할 수 있다. 그러나 아주 전문적인 부정조작, 예컨대 금융기관의 이자계산 프로그램을 변경시켜 이자액의 일정비율에 해당하는 금액이나 원단위 이하의 극히 적은 금액을 자신이 개설해 놓은 계좌로 입금되도록 조작하는 경우에는 그것의 발견이 매우 어려울 것이다. 이러한 전문적인 수법은 아직 우리나라에서 적발된 것은 없으나 장차 행하여질 가능성이 있는 방법으로서 이에 대한 대책이 마련되어야 할 것이다. 외국의 사례를 보면, 미국의 한 소프트웨어 회사에서 프로그래머로 일하면서 모 은행의 컴퓨터작동을 책임지고 있던 자가 경제적인 어려움에 처하게 되어 약 300달러의 초과대출이 필요하게 되자 그 은행에 있는 자신의 계좌에 대하여는 초과지출이 이루어지더라도 3일동안만 검색되지 않도록 할 의도로 은행의 검색프로그램에 추가적인 프로그램을 만들어 넣었는데 4개월 후에도 이 프로그램이 여전히 남아있어 그의 계좌에서는 이미 1,350달러가 초과대출되고 있었던 사건이 있었다[4] 또한 은행의 프로그래머가 10달러 이하의 현금써비스에는 10센트가, 10달러 이상의 현금써비스에는 1달러가 더해지도록 프로그램을 만든 후 여분의 금액은 자신이 개설한 가명계좌에 입금되도록 조작하였는데 은행이 새로운 판매전략을 세워 고객들에게 감사의 마음을 표시하려고 고객명단을 검색하다가 그 가명의 인물이 존재하지 않음을 발견할 때까지 매월 수백달러를 인출할 수 있었던 사건도 있었다.[5]

---

4) Ulrich Sieber, 위의 책, 55-56면.

5) Brandt Allen, Embezzler's guide to the computer, Harvard Business Review, July-August, 1975, 87면.

자료의 부정조작은 금융기관이 아닌 곳에서도 행하여질 수 있다. 지금까지 발생한 사례를 보면 대학에서의 입시업무가 전산으로 처리되는 점을 악용하여 특정한 수험생의 점수를 상향조정하여 합격시키거나, 자동차면허시험에 떨어진 자에 대한 낙방기록을 면허증을 분실한 것처럼 바꾸어 분실한 면허증을 재발급해주는 것과 같이 처리하여 운전면허증을 부정발급해 준 사건이 있었다. 부동산등기부나 자동차등록원부 등과 같이 공정증서원본으로 기능하게 될 전자기록의 내용을 변경하거나, 주민등록원부나 각종의 공문서를 전자기록의 형태로 기록·보관하게 됨으로써 공문서의 부정조작도 발생하게 될 것으로 생각된다.

또한 컴퓨터담당자나 단말기에 접근할 수 있는 내부인이 아니더라도 컴퓨터통신망을 통하여 타인의 인터넷 홈페이지에 접속할 수 있게 됨으로써 이들 홈페이지의 수록내용을 무단으로 변경하는 행위, 예컨대 타인의 인터넷 홈페이지에 포르노 웹싸이트를 작성하는 수법도 자료의 부정조작에 해당한다. 경찰청에 따르면, 네덜란드 또는 미국인으로 추정되는 해커가 인천교육대, 광주교육대, 대구교육대, 공주교육대, 동양공업전문대의 인터넷 홈페이지에 잇따라 침입, 포르노 웹싸이트를 개설한 사실이 드러나 인터폴에 수사협조를 의뢰키로 하였다고 한다.(동아일보 1998.2.28) 이는 해커가 한 것으로 추정되지만 일반인의 열람이 허용된 타인의 인터넷 홈페이지를 열람하는 것은 해킹이라고 볼 수 없으며, 이 사건에서 문제가 된 것은 포르노 웹싸이트를 개설한 것(즉 포르노를 실어놓은 것)이므로 이는 자료의 부정조작으로 보아야 할 것이다.

② 특징

자료의 부정조작행위는 다음과 같은 특징을 갖고 있다. 첫째 행위자의 거의 전부가 당해 관련자료를 입력하는 컴퓨터담당자 또는 내부인이라는 점이다. 즉 컴퓨터와 연결되어 업무처리에 이용되는 단말기를 취급하는 자이거나 적어도 당해 단말기에의 접근이 용이한 내부인이 자료를 조작하게 된다. 이는 금융기관 등의 주 컴퓨터와 개개의 단말기만이 Network화되어 있기 때문에 당연한 일이다. 따라서 통상적으로는 외부인은 내부자와 공모하여서만 자료의 부정조작을 범할 수 있을 뿐이다. 다만 인터넷과 같이 컴퓨터통신망을 통하여 누구나 접근할 수 있는 전자기록에 대하여는 해커 등 제3자에 의한 조작이 가능하게 될 것이다.

둘째 지금까지는 자료의 부정조작의 대부분이 은행 등 금융기관에서 행하여지고 있으며 재산범죄의 성격을 갖고 있다는 점이다. 그것은 자료의 부정조작은 그 자체가 목적이 아니라 재산획득이라는 목적을 달성하기 위한 수단으로 이용된다는 점에서 기인

하는 것으로 생각된다. 면허시험기록 조작사건의 경우에도 결국은 돈을 받기 위하여 행한 것이었다. 이러한 상황은 앞으로도 계속될 것이지만 장차 문서를 대신하여 증명기능을 하는 각종의 전자기록이 보편화된다면 금융기관은 물론이고 일반기업이나 병원 그리고 공무소에서도 자료의 부정조작이 점차 발생할 것으로 예상된다.

셋째 피해금액이 매우 크다는 점이다. 즉 금융기관에서 발생한 부정조작에 의한 피해액을 보면 적게는 수억원에서부터 많게는 수백억원에 이르고 있다. 이는 범죄발생장소가 금융기관이라는 점과 더불어 단말기의 간단한 조작으로 범행이 가능하고 일단 한번 행하여지면 프로그램의 지시대로 반복적으로 이루어진다는 점 때문으로 생각된다. 이와 같이 피해액이 전통적인 재산범죄에 비하여 대단히 많고, 그것이 금융기관에서 이루어진다는 점을 고려하면, 자료의 부정조작은 금융기관의 부실화를 초래하게 되고 금융기관에 대한 일반인의 신뢰를 떨어뜨릴 위험성이 많다. 이는 결국 금융기관의 적정한 기능을 해치게 되는 파급효과를 가져올 수 있는 중대한 범죄이다.

넷째 부정조작행위 자체는 물론 그 행위자의 발견이 매우 어렵다는 점이다. 그리하여 자료의 부정조작행위를 찾아낸다는 것은 수 십권의 백과사전 속에서 틀리게 한 설명을 찾아내는 것과 같은 것이며[6] 이것을 발견하는 것은 요행이라고까지 할 수 있다. 즉 아주 우연히 발각되든가 아니면 다른 사실로 인하여 발각되는 것이 보통이다. 또한 컴퓨터도 인간과 마찬가지로 실수를 할 수 있기 때문에 컴퓨터를 절대적으로 믿을 수 없다는 점도 자료의 부정조작을 유혹하는 원인이 된다.

2) 컴퓨터파괴

① 수법

컴퓨터의 정상적인 기능을 곤란 또는 불가능하게 만드는 컴퓨터파괴행위는 주로 해커에 의하여 범하여지는데, 지금까지 우리나라에서 발생한 수법을 정리하면 대략 다음과 같다. 첫째의 수법은 컴퓨터에 수록된 자료나 정보를 삭제하거나 변경하는 것인데, 이러한 자료(정보)의 삭제나 변경은 컴퓨터의 작동은 가능하지만 자료의 이용을 방해하게 된다. 실제로 1백만대의 컴퓨터가 가입돼 있는 국제적인 전산망인 '인터네트'를 지방국립대학 등 국내대학 연구실과 연결시켜 주는 교환기 역할을 하는 서울대의 교육전산망용 컴퓨터시스템에 정체불명의 해커가 온라인망을 통해 침입해 6대의 워크스테

6) 大西靖臣, コンピュ - タ社會の憂鬱, 1980, 146면.

이션에 수록돼 있던 정보를 모조리 파괴해 전산망의 가동을 10여 시간 동안 마비시킨 사건(한겨레신문 1992.8.4), 국제적인 통신망인 '인터네트'와 연결돼 있는 서강대 전자계산소의 퍼블릭 시스템에 해커가 침투하여 이 컴퓨터에 기억돼 있던 세계의 대학과 연구소의 공개 자료 목록 등 총 5기가 바이트의 자료가 없어졌으나, 그의 신원을 파악할 수 있는 방법이 없었던 사건(동아일보 1994.12.23), 한남대 부설 전자계산소의 통신망에 해커가 침입하여 48분 동안 전자게시판(BBS)에 수록된 1백여개의 각종 자료 및 통신망사용자의 신상명세서, 전자편지 등의 데이터를 파괴하거나 빼내가는 등 해커 침입으로 한남대 통신망은 약 10시간 동안 완전 마비시킨 사건(동아일보 1994.12.23) 등이 있었다. 이와 같이 현재까지 알려진 컴퓨터파괴의 대상은 대부분 대학의 전산망이었다.

둘째의 컴퓨터파괴수법은 프로그램을 삭제하거나 변경하는 것이다. 이는 자료(정보)의 삭제(변경)와 유사하지만 단순히 자료에 대한 접근이나 그 이용만을 어렵게 하는 것이 아니라 컴퓨터 시스템의 작동 자체를 불가능하게 하는 점에서 그 파급효과가 훨씬 심각하다고 할 수 있다. 예컨대 1994년 12월 24일 주식시장 개장 직후인 오전 9시30분경 갑자기 (주)증권전산의 증권정보조회용 단말기인 「V2단말기」화면에 증권정보 대신 신년인사가 나오면서 캐럴이 흘러나오고 주식시세확인 등 증권정보조회는 한동안 중단된 사건,[7] 부산·경남지역 인터넷동호회 부책임자 김모군(19·대학생)이 1996년 12월27일 집에서 개인용 컴퓨터를 이용해 나우콤의 전산망에 접속한 뒤 해킹프로그램을 사용, 새도파일을 훔치고 이어 인터넷 작동에 필요한 나우콤의 작동 프로그램을 일부 파손, 같은 날 자정부터 다음 날 오전 6시까지 나우콤 인터넷서비스 가입자들이 접속을 못하도록 방해한 사건(중앙일보 1997.5.10), 대학생(22)이 대학 컴퓨터공학과에 입학하면서 해킹연구 동아리를 만들어 전산망 해킹방법을 습득하던 중 습득한 해킹수법을 이용하여 1998.1.26. 인터넷 홈페이지 제작 대행업체인 『디킴스기획』의 전산망에 불법침투, 시스템을 파괴하여 정상적인 영업활동을 방해하고, 1998.2.1. 컴퓨터 통신을 이용한 유료 게임서비스 업체인 『불루넷』의 전산망을 파괴하여 약 9,000여명의 회원들이 게임서비스를 이용하지 못하도록 함으로써 정상적인 영업활동을 방해하는 등 1996년 10월경부터 1998년 4월까지 18개 전산망을 해킹한 사건 등이 있었다.

7) 그러나 이 크리스마스 바이러스가 일부 증권정보조회용 단말기에만 침투했기 때문에 주식거래가 중단되는 피해는 없었다.(동아일보 1994.12.25)

컴퓨터파괴의 세번째 수법으로 이용되는 것으로 주 컴퓨터의 비밀번호를 바꾸는 것이다. 이것을 자료의 부정조작으로 분류할 수도 있으나 컴퓨터에의 접근이나 그 이용을 방해한다는 점에서 컴퓨터파괴행위에 해당하는 것으로 보아야 할 것이다. 검찰에 따르면, 한국과학기술원생 노모씨(20), 김모씨(24), 정모군(19)은 한국과학기술원 전산학과 해킹방지 동아리실에 있는 전산시스템을 통해 포항공대 물리학과 등 이 대학 7개 전산시스템과 이화여대 전산시스템에 침투한 뒤 본체의 비밀번호를 바꾸고 전산자료 일체를 삭제하는 등 전산망을 마비시킨 사건이 있었다(동아일보 1996.5.8).

네 번째로 들 수 있는 컴퓨터파괴의 수법은 컴퓨터에 바이러스를 감염시키는 것이다. 이것이 빈번하게 행하여질 수 있는 컴퓨터파괴행위의 수법이 될 것인바, 우리나라에서도 상당히 많이 발생하고 있는 것 같다. 이와 유사한 수법이 바이러스를 통신망을 통해 불특정 다수인에게 유포하는 행위이다. 이는 통상 바이러스를 만들어낸 자들이 바이러스가 아닌 것처럼 가장하여 컴퓨터통신망에 올려 놓아 이를 알지 못하는 통신망이용자들로 하여금 다운받게 함으로써 컴퓨터를 감염시켜 그 작동을 불가능하게 하는 것이다. 경찰청 컴퓨터범죄수사대의 자료에 의하면, 최모군(13 · 중2)은 1997.7.4.경 주거지에서 컴퓨터시스템 작동을 정지시키는 기능을 가진 율곡바이러스 등 총 7종의 바이러스를 제작하여 스마트라인 통신망을 통해 김종운(29) 등 불특정 다수인에게 유포, 컴퓨터를 감염시켜 피해를 입힌 사건, 오모군(19 · 대학생)이 1997.6.2.경 주거지에서 FCL바이러스를 스마트라인 통신망을 통해 문현일(17) 등 불특정 다수인에게 유포, 컴퓨터를 감염시켜 피해를 입힌 사건, 문모군(18 · 고3)이 1997.8.9.경 주거지에서 고래바이러스를 스마트라인 통신망에 올려 불특정 다수인에게 유포한 사건, 김모군(15 · 중3)이 1997.10.10.경 주거지에서 PS-MPC 522바이러스 등을 스마트라인 통신망을 통해 윤종규(20) 등 불특정 다수인에게 유포, 컴퓨터를 감염시켜 피해를 입힌 사건 등이 있었다.

다섯번째로 컴퓨터의 정상적인 작동을 어렵게 하는 컴퓨터파괴행위의 수법으로 스팸메일(spam mail)에 의하여 통신서비스를 마비시키는 행위가 있다. 스팸메일은 메일폭탄이라고도 하는데 전자우편시스템에 다량의 전자우편(메일)을 발송하여 전자우편관리시스템이 제대로 기능하지 못함으로써 정당한 이용자들의 메일송수신을 불가능하게 하거나 지연시키게 된다. 우리나라에서는 1997년에 하이텔이 운영하는 인터넷 전자우편시스템에서, 신원미상의 한 해커가 인터넷을 통해 10만여통의 전자우편을 무차별로 발송하여 '메일 송수신 프로토콜'이 수차례 가동을 멈추면서 이용자들이 보낸 전자우편이 하루가 지난 다음에야 배달되는 등 심각한 체증현상이 일어난 사건이 있었다.

끝으로 외국에서는 강력한 자기력(磁氣力)을 이용하여 자료나 프로그램을 교란시키는 수법도 발생하고 있다. 예컨대 미국 클리브랜드에 있는 제조업체의 컴퓨터센터에서 불평불만을 가진 종업원이 자석을 사용하여 자기테이프에 수록되어 있던 매우 중요한 프로그램과 자료를 파괴한 사건이 발생한 바 있는데, 그 회사는 이들 프로그램과 자료를 재생시키기 위하여 많은 시간과 비용을 소비하게 되었다. 또한 반전론자들이 미시건주의 미들랜드에 있는 한 화학회사의 자료조사 컴퓨터센터에 침입하여 자석을 이용하여 약 1천여개의 마그네틱 테이프를 해체하거나 못쓰게 만들었는데, 회사에서 이들 테이프의 수록내용에 대한 기초자료의 복사본을 따로 만들어 두었지만 파괴된 테이프를 복구하는데 10만달러의 비용이 소요된 바 있었다.

② 특징

컴퓨터파괴행위의 첫 번째 특징은 행위자의 대부분이 컴퓨터취급자 등 내부인이 아니라 외부인으로서 컴퓨터광(狂)인 해커이며, 주로 해킹을 통해서 이루어진다는 점이다. 해커는 나름대로 컴퓨터와 정보통신기술에 상당한 실력을 가지고 있기 때문에 이들 행위자를 찾아내기가 매우 어렵고 그만큼 수사하는데 많은 노력과 시일을 요하게 된다. 또한 해커들은 자신들의 컴퓨터 관련실력을 과시하려는 의도에서 컴퓨터파괴행위를 하기 때문에 죄의식이 거의 없고 오히려 대단한 성공으로 생각하는 경향이 있다.

둘째 행위자들 중에는 욕구불만이나 복수심을 가진 자도 많다는 점이다. 예컨대 과격파라든지 해고당한 자 등이 컴퓨터파괴행위를 행하는 경향이 많다. 반전론자들이 미시간주의 화학회사 컴퓨터센터의 마그네틱 테이프를 자석을 이용하여 못쓰게 한 사건, 뉴욕에서 컴퓨터 프로그래머로 근무하면서 해고될듯한 예감이 든 자가 회사의 인사관리 프로그램에 조작을 가하여 자신의 이름이 해고자 리스트에 나타나면 자기가 만들어놓은 비밀프로그램이 작동하도록 하였는데 이윽고 그가 해고되자 비밀프로그램이 컴퓨터 기억장치의 내용을 전부 지워버린 사건이 발생한 바 있다. 최근에는 자신의 목적을 달성하기 위하여 컴퓨터를 파괴하겠다고 위협하는, 이른바 핵티비스트(Hacktivist)까지 등장하고 있다.

셋째 행위자들의 연령이 10대 내지 20대 초반으로서 주로 학생들이라는 점도 컴퓨터파괴행위의 특징이라고 할 수 있다. 즉 우리나라의 사례를 보면 행위자들이 중고등학생이거나 대학의 컴퓨터 관련학과에 재학중인 학생들이었다.

넷째 컴퓨터파괴행위의 대상은 자료의 부정조작과는 달리 대학의 통신망이나 컴퓨터통신회사 등과 같이 외부인이 접속하여 이용할 수 있도록 개방되어 있는 컴퓨터통신망

이다. 이들 컴퓨터통신망은 외부인의 자유로운 접근이 비교적 용이한 만큼 해킹에 의한 파괴의 위험에 노출되어 있으므로 컴퓨터보안의 문제가 중요한 관건이 될 것이다. 아직 우리나라에서는 은행 등 금융기관에서 컴퓨터파괴사건이 발생하였다는 보도는 없으나 업무자동화의 대표적인 부문이 금융전산화이므로 장차 금융기관의 컴퓨터에 대한 파괴행위에 대하여도 대비를 하여야 할 것이다. 이미 1994년말에 (주)증권전산의 증권정보조회용 단말기에 크리스머스 바이러스가 침투하여 증권정보조회가 한동안 중단된 바 있었다.

다섯째 컴퓨터파괴행위는 단순히 컴퓨터의 프로그램이나 자료 또는 정보만을 못쓰게 만드는 것이 아니라 당해 컴퓨터를 이용하여 이루어지는 업무에 지장를 초래하여 피해범위가 매우 넓어진다는 특징을 갖고 있다. 즉 컴퓨터파괴는 자동화된 업무처리에 필수불가결하게 기능하는 컴퓨터의 정상적인 작동을 불가능하게 만들기 때문에 컴퓨터파괴행위가 행하여지면 당해 컴퓨터를 이용하여 이루어지는 모든 업무가 마비되게 된다. 예컨대 은행의 컴퓨터가 파괴되면 은행을 통한 금융거래가 불가능해지며, 대학의 전산당이 파괴되면 대학업무가 마비되고, 증권전산의 컴퓨터가 파괴되면 주식거래가 중단되어 엄청난 혼란을 야기할 것이며, 병원의 진단·수술에 이용되는 컴퓨터를 파괴하면 환자의 건강과 생명에 치명적인 위험을 가져올 것이다.

3) 컴퓨터스파이

① 수법

타인의 컴퓨터망에 침입하여 프로그램, 자료 또는 정보를 탐지하는 컴퓨터스파이행위는 주로 해커에 의하여 행하여진다. 첫째의 수법은 해커가 자신의 컴퓨터기술을 활용하여 국가기관이나 타인의 컴퓨터에 접속하여 자료나 정보를 획득하는 것이다. 이것이 컴퓨터스파이의 가장 일반적인 수법이다. 워싱턴 타임즈지에 따르면, 한 컴퓨터해커(16·영국소년)가 美 공군기지의 컴퓨터를 비롯하여 1백여 컴퓨터장치에 침범하였는데 그 피해대상은 한국원자력연구소, 미국항공우주국(NASA), 가더드우주비행센터, 캘리포니아 제트연구소 등이었고, 특히 한국원자력연구소의 모든 자료들을 빼내 이 데이터들을 뉴욕주 소재 롬항공개발센터로 이동하는 등의 장난을 한 것으로 나타났으나 한국원자력연구소측은 주미 한국대사관 과학관의 보고로 이 사실을 처음 알고 이날 오후까지 검색하였지만 어떤 자료가 해커에 의해 이전됐는지 확인하지 못하였던 사건(동아일보 1994.11.5), 경찰청에 따르면 한국의 해커가 데이콤통신망을 통해 유럽 암연구센터 전산

망에 접속, 암에 관한 임상연구보고자료 3만자를 복사해간 사실을 발견한 벨기에 경찰이 인터폴을 통해 경찰청에 수사협조를 요청해 온 사건(동아일보 1994.11.13) 등이 있었다.

둘째의 수법은 컴퓨터통신망에 접속, 비밀번호 해독프로그램 등과 같은 특수프로그램을 설치하여 회원의 비밀번호를 알아낸 후 이를 이용하여 수시로 컴퓨터에 수록된 자료를 열람하거나 복사하는 것이다. 추모씨(24·무직)는 1995년 7월 나우콤 전산망을 통해 서울대 전산원에서 운영하는 「서울대 정보광장」 등 4곳의 전산시스템에 접속, 비밀번호 해독프로그램(일명 트로이목마 프로그램)으로 2백5십여명의 서울대 교수와 학생들의 비밀번호를 알아내 서울대 전산시스템을 마음대로 드나들며 이들의 전자우편을 열람한 사건이 있었다(동아일보 1996.4.17).

셋째의 수법은 컴퓨터망을 사용하는 국가권력기관의 비밀번호를 알아낸 뒤 이 기관을 사칭하여 산하 관련기관에게 자신이 필요로하는 정보를 제공하도록 하는 수법이다. 언론보도에 의하면, 김모씨(23)는 (주)데이콤의 컴퓨터통신망인 '천리안'을 통해 재무부 국세심판소에서 사용중인 사용자이름(ID)과 비밀번호를 알아낸 뒤 청와대가 국세심판소를 이용해 팩시밀리를 보내는 것처럼 속여 데이콤에 청와대비서실이 사용중인 5개 사용자번호의 비밀번호를 모두 'BH0303'으로 바꿔줄 것을 요청하였는데, 데이콤쪽이 이 요청을 받아들여 비밀번호를 모두 바꿔주자 이 번호를 사용해 천리안의 팩스서비스를 통해 청와대 경제수석비서관실 명의로 조흥은행, 농협 등 12개 금융기관 및 정보통신기관에 전산망운영 현황과 구조 등 정보통신관련 기밀자료를 요구하였고, 이에 따라 이들 기관들은 자료제출을 위한 작업을 벌였으나 자료요청을 수상히 여긴 농협이 청와대비서실에 확인한 결과 청와대의 비밀번호가 도용된 것을 안 청와대경호실과 데이콤의 통보로 자료는 유출되지 않았던 사건이 있었다(한겨레신문 1993.2.18).

네 번째의 수법은 전산망에 접속하여 전산시스템 전체의 삭제 또는 내용변경을 마음대로 할 수 있는 「시스템 최고관리자 권능」(이른바 루트권능)을 획득한 후 자료를 무단 열람하는 방법이다. 경찰에 따르면, 자동차 정비공인 김모씨(24)는 3·1절을 기념해 인터넷을 이용, 일본전신전화(NTT)를 통해 일본 외무성 주전산망에 접속, 전산시스템 전체의 삭제 또는 내용변경을 마음대로 할 수 있는 「시스템 최고관리자 권능」(이른바 루트권능)을 획득한 후 일본 외무성의 인터넷 홈페이지에 「독도는 우리땅」이라는 글을 남기려다 외교문제화되는 것을 우려해 실행에 옮기지는 않았다고 하며, 또한 김씨는 1995년 9월부터 지난주까지 일본 5개소, 미국의 대학 및 기업체 27개소, 영국 1개소, 캐

나다 1개소 등 4개국 34개소와 국내 대학 41개소 및 기업체와 연구소 17개소 등 총 92개소의 전산망에 침투, 루트권능을 획득한 다음 자료를 무단 열람하여 왔다고 한다(동아일보 1996.4.19).

② 특징

타인의 컴퓨터에 무단 접속하여 그곳에 수록되어 있는 프로그램이나 자료 또는 정보를 획득·이용하는 컴퓨터스파이는 행위자의 측면에서 보면 컴퓨터파괴와 유사한 특징을 보여주고 있다. 즉 첫째의 특징은 컴퓨터스파이도 대부분 해커에 의하여 범하여지므로 범인의 발견과 처벌이 매우 어렵고, 행위자는 별다른 죄의식 없이 오히려 자신의 실력을 과시하려는 의도에서 행위한다는 점이다.

두 번째의 특징은 피해자가 자신의 컴퓨터가 스파이를 당하였다는 사실을 발견하기가 쉽지 않다는 점이다. 컴퓨터파괴의 경우에는 자신의 컴퓨터가 제대로 기능을 하지 못하기 때문에 피해사실을 인식하기가 용이하지만, 컴퓨터스파이의 경우에는 행위자가 별다른 흔적을 남기지 않고 컴퓨터에 접속하여 필요한 자료나 정보를 빼내가기 때문에 자신의 컴퓨터가 해커에 의하여 스파이행위의 대상이 되었다는 사실을 인식하는 것이 매우 어렵다.

세 번째의 특징으로는 컴퓨터스파이가 행하여지는 대상이 중요한 자료나 정보를 처리·보관하고 있는 기관이라는 점이다. 예컨대 원자력연구소, 항공우주센터와 같은 특수연구기관이나 대학, 기업체(특히 금융기관이나 정보통신관련기관) 등이 컴퓨터스파이 행위의 목표물이 되고 있다. 앞으로 정보화가 더욱 진행되면서 개인정보는 물론 국가나 기업의 중요한 자료가 예외없이 컴퓨터에 의해 처리·전송·보존될 것이라는 점을 생각한다면 컴퓨터스파이행위로부터 어떻게 자료를 보호할 것인가가 심각한 문제로 대두될 것이다. 즉 앞으로의 세계에서는 간첩이나 산업스파이의 주된 활동내용이 컴퓨터스파이가 될 것이다.

컴퓨터스파이의 네 번째 특징으로는 시간적·장소적 제약없이, 특히 국가간의 경계를 초월하여 이루어진다는 점이다. 이는 컴퓨터스파이에 효과적으로 대처하기 위해서는 국가 사이의 협조체제가 필수불가결하다는 것을 보여준다.

다섯째로 컴퓨터스파이에 의하여 컴퓨터망이 해킹을 당하였다는 사실을 알았더라도 피해자가 과연 어떠한 자료가 어느 정도로 유출되었는지를 알 수 없다는 점이다.

4) 컴퓨터의 권한없는 사용

① 수법

컴퓨터의 권한없는 사용이란 타인의 컴퓨터를 사용할 권한이 없는 자가 무단으로 이를 사용하여 일정한 일을 처리하는 것으로, 시간절도(Zeitdiebstahl)라고도 한다. 오늘날 개인용컴퓨터(PC)의 가격은 많이 낮아졌지만 아직도 고가이며, 더구나 기업의 컴퓨터와 같은 대규모의 자료를 처리·저장하는 초고속 대용량의 컴퓨터는 가격이 매우 비싸다. 또한 새로운 종류의 컴퓨터가 매우 빠른 속도로 개발되고 있으며 보수관리라든가 애프터 서비스 등의 문제가 있기 때문에 컴퓨터를 구입하는 대신 임차하여 사용하는 경우가 많다. 이러한 컴퓨터를 권한없이 일정시간 이용함으로써 임차인에게 경제적인 부담을 지우고 권한없는 사용자는 사용대금을 지불하지 않음으로써 불법적인 이익을 얻게 되는 것이다. 컴퓨터의 권한 없는 사용의 수법은 내부인에 의한 경우와 외부인에 의한 경우로 나누어 살펴볼 수 있다. 내부인의 권한 없는 사용은 기업의 업무처리 등 정해진 일정한 목적을 위하여 컴퓨터를 사용할 권한이 있는 자가 그러한 목적을 벗어나서 사적인 일을 처리하기 위하여 컴퓨터를 이용하는 수법이다. 그리고 외부인에 의한 행위는 타인의 ID나 패스워드를 알아내서 그것을 이용하여 컴퓨터가 제공하는 서비스를 제공받는 수법이다. 경찰청 컴퓨터범죄수사대에 따르면, 이모군(21·대학생)은 대학 건축공학과 전산시스템을 관리해 오면서 인터넷을 통해 얻은 해킹프로그램을 이용하여 타인의 ID와 비밀번호를 알아낸 뒤 1998.1.26. 한국통신에서 운영하는 인터넷 서비스인 『코넷』 사용자인 이호석의 ID(shade)와 비밀번호를 도용하여 접속하는 등 1998.4.까지 모두 10여명의 ID를 불법 도용하였다고 한다.

② 특징

현재로는 컴퓨터의 권한없는 사용이 빈번한 것은 아니며 그로 인한 손해가 처벌할만큼 큰 경우는 별로 알려지지 않아 이러한 행위를 범죄로서 처벌하여야 할 것인가에 대하여는 견해가 일치되지 않고 있으며 아직 처벌규정을 둔 나라도 없다. 컴퓨터의 권한없는 사용의 특징은 첫째 행위자가 주로 컴퓨터를 사용할 권한이 있는 자라는 점이다. 즉 사용권한 있는 자가 사용권한을 부여받은 목적이 아닌 다른 사적인 목적으로 컴퓨터를 이용하는 것이다.

둘째의 특징은 외부인의 경우 타인의 ID나 패스워드를 알아낼 수 있는 해커나 피해자의 친구 등 주변인물이라는 점이다. 셋째 이들 행위자는 —내부인이든 외부인이든— 이러한 행위가 범죄가 될 수 있다는 인식이 거의 없다는 점도 하나의 특징이다. 즉 자신의 행위에 대한 죄의식이나 피해자의 피해에 대한 별다른 의식 없이 이러한 행위를

한다. 끝으로 다른 컴퓨터범죄의 경우와 마찬가지로 피해자가 자신이 피해를 당하였다는 사실을 인식하기가 대단히 어렵다. 왜냐하면 일반적으로 컴퓨터를 사용하는 사람들은 컴퓨터의 이용시간에 대하여 특별한 관심을 기울이지 않기 때문이다.

다. 추세전망

개인용컴퓨터(PC)를 포함하여 컴퓨터가 널리 보급되고 비약적으로 발전하는 정보통신기술(Information Technology)과 결합하여 컴퓨터통신시대 내지 정보화시대가 도래하면서 세계 각국에서는 날로 증가하는 컴퓨터범죄가 새로운 도전으로 다가오고 있다.

우리나라에서는 1973.10. 과학기술처 중앙전자계산소 프로그래머가 AID차관 아파트의 입주자추첨과 관련하여 프로그램을 조작한 사건이 최초로 발생한 컴퓨터범죄이다. 그후 1985년까지 12년동안 20건[8] 또는 1990년 4월까지 17년동안 41건[9] 에 불과하였으나, 1992년 12월부터 1994년 12월까지 약 2년동안에만 118건[10]이 발생하였다. 또한 한국정보보호센터의 자료에 의하면 1995년에는 183건, 1996년에는 9월까지만 213건(전년대비 116% 증가)이 발생하는 등 최근 몇 년 사이에 급격하게 증가하는 상황에 있다(〈표 1〉 참조). 이를 유형별로 살펴보면, 컴퓨터파괴에 해당하는 컴퓨터바이러스가 가장 많고(68.8%, 78.9%), 컴퓨터스파이에 해당하는 해킹과 자료유출 및 절취(17%, 10.8%), 자료의 부정조작(8.8%, 6.6%), 기타의 순이다(〈표1〉 참조). 이러한 유형별 비율은 수사기관이 파악한 것과는 현저한 차이를 보여주고 있는 바(〈표 1〉과 〈표 3〉을 비교해 보라), 이는 컴퓨터범죄를 각자의 관점에서 유형화함으로써 유형분류가 통일성을 결하고 있다는 점과 양 기관의 성격이나 자료수집 과정이 다르다는 점에 주된 이유가 있다고 보여진다. 이러한 문제는 컴퓨터범죄에 대하여 효과적으로 대처할 수 있는 수단을 강구하는데에 어려움을 야기하므로 향후 발생상황을 정확하게 파악할 수 있는 방안을 마련하여야 할 것이다.

---

8) 김문일, 컴퓨터犯罪論, 법영사, 1989, 158면.

9) 조규정, 컴퓨터操作犯罪, 세미나자료 90년대의 범죄와 형사정책, 한국형사정책연구원, 1990.4, 91면.

10) 동아일보 1995.3.27.

〈표 1〉 1995년부터 1996년 9월 사이의 컴퓨터범죄발생건수[11]

사례 \ 연도	1995	1996.9까지	합계
내부자료 변조 및 파괴	14(7.7%)	13(6.1%)	27
부정정보 처리	2(1.1%)	1(0.5%)	3
컴퓨터바이러스	126(68.8%)	168(78.9%)	294
해킹(통신망무단접속)	17(9.3%)	10(4.7%)	27
자료유출 및 절취	14(7.7%)	13(6.1%)	27
기타	10(5.5%)	8(3.8%)	18
합계	183(100%)	213(100%)	396

컴퓨터범죄의 급격한 증가경향은 대검찰청의 정보범죄관련통계에 비추어 보아도 쉽게 알 수 있다(〈표2〉, 〈표3〉 참조). 그러나 수사기관에 의하여 처리된 건수는 1995년에 21건으로 11.5%(21건/183건), 1996년에 72건으로 33.8%(72건/213건)에 불과한 것으로 나타나 있다(〈표2〉 참조).

〈표 2〉 정보범죄사범 연도별 수사실적(기간:'95. 4. 10. ~ '97. 6. 30.)[12]

연도	건수	명(구속)
1995(4~12)	21	45(12)
1996	72	146(24)
1997(1~6)	33	57(30)
계	126	248(66)

이러한 상황이 초래되는 이유로는 다음의 두가지를 들 수 있을 것이다. 첫째의 이유는 발생한 컴퓨터범죄가 수사기관에 알려지지 않아 수사기관이 개입하지 않고 내부적으로 처리된 경우가 많기 때문으로 보인다. 예컨대 금융기관이나 컴퓨터통신회사 등의 피해자들이 자신들에 대한 고객들의 신뢰하락을 우려하여 피해금액이나 피해범위가 크지 않은 경우에는 피해사실이 공개되는 것을 원치 않아 형사소추가 이루어지지 않을

11) 정보보호총서, 한국정보보호센터, 1996.12, 28~38면.

12) 대검찰청 중앙수사부 정보범죄대책본부(http://www.dci.sppo.go.kr/dci.htm).

수 있다. 물론 친고죄가 아닌 범죄의 경우 피해자의 처벌의사가 형사소추에 조건이 되지는 않지만, 컴퓨터범죄의 성질상 피해자가 신고하지 않으면 수사기관이 범죄발생을 알기가 쉽지 않고 또한 피해자가 굳이 처벌을 원치 않는 경우에 수사기관으로서도 적극성을 보이지 않을 가능성이 많다는 점은 부인할 수 없을 것이다.

〈표 3〉 정보범죄사범 유형별 수사실적 (기간:'95. 4. 10. ~ '97. 6. 30.)[13]

유 형	처 리	
	건	명(구속)
사전자기록등 위·변작	2	4(2)
단말기부정사용 사기	5	14(9)
컴퓨터·전자기록손괴 등 업무방해	4	15(12)
전산망보호조치침해(해킹)	8	13(5)
전산망처리정보훼손 등	3	5
공공기관의 개인정보 부정사용	3	10(6)
ID 부정발급·사용 사기	6	51(5)
홈뱅킹 사기	3	4(3)
상용통신망 사기	5	5
신용카드 사기	4	5(2)
음란CD등 제작·판매	8	8(5)
기 타	75	114(17)
계	126	248(66)

두 번째의 이유로는 범인을 찾아내지 못하였기 때문에 수사와 형사소추가 이루어지지 않았을 것이라는 점이다. 컴퓨터범죄, 특히 주로 해커에 의하여 범하여지는 컴퓨터파괴나 컴퓨터스파이는 범인의 발견이 매우 어렵기 때문에 피해는 입었는데 범인을 알 수 없는 경우가 상당히 많아 수사와 형사소추가 불가능한 사건들이 많을 것으로 생각된다.

컴퓨터가 보다 더 많이 보급되고 정보통신기술의 발달로 국가와 기업 그리고 개인의 정보화가 촉진되면 될 수록 컴퓨터의 자료(정보)처리과정에 불법적으로 개입하는 컴퓨터범죄는 급격하게 증가할 것으로 판단된다. 통계작성기관의 분류방식이 적절하지 않아

13) 대검찰청 중앙수사부 정보범죄대책본부(http://www.dci.sppo.go.kr/dci.htm).

컴퓨터범죄의 유형별 발생추이를 예측하기는 어렵지만, 컴퓨터범죄의 온상이 될 정보사회의 환경을 그려본다면 다음과 같이 발생추세를 전망할 수 있을 것이다. 우선 자동화된 업무의 증가로 인하여 컴퓨터바이러스의 제작·유포 또는 컴퓨터프로그램의 삭제·변경을 수단으로 한 업무방해를 목적으로 하는 컴퓨터파괴범죄가 증가할 것으로 예상된다. 이러한 행위는 종래의 한정된 지역에서의 업무를 방해하는 경우와는 달리 당해 컴퓨터와 연결된 모든 업무를 장소적 제약없이 방해하게 되므로 앞으로 중대한 피해를 야기하는 범죄가 될 것이다. 이러한 컴퓨터파괴에 의한 업무방해는 개인의 업무에 대하여는 물론이고 국가 등 공무에 대하여도 나타나게 될 것이다.

새로운 범죄환경은 자료 내지 정보가 기존의 유형물을 대체하여 자본의 원천으로서 중시되고 경제적·정치적 힘의 원천으로서의 자본의 자리를 계승하게 되는, 소위 정보지배사회(cyberocracy)[14]의 도래로부터도 제공된다. 즉 과거 산업사회에서는 소득의 결정요인이 생산도구의 소유 여부이었지만 정보사회에서의 소득결정요인은 정보의 보유 여부가 될 것이다. 따라서 정보를 생산하여 보호하려는 측과 이를 수집·파괴하려는 측과의 치열한 싸움이 나타날 것이다. 이러한 점을 고려한다면 컴퓨터스파이행위도 증가하게 될 것으로 판단된다. 또한 컴퓨터와 정보통신기술의 발달에 따라 의사나 자료(정보)의 전달이 컴퓨터통신망에 의존하게 되어 통신서비스가 확대될 것이다. 이에 대비하여 컴퓨터에 의하여 처리·보존·전송되는 자료(정보)를 외부의 무단침입으로부터 안전하게 지켜 줄 보안장치의 개발이 중대한 관심사가 될 것이다. 이에 따라 보호조치를 무력하게 만드는 행위, 즉 보호조치를 훼손함으로써 무단접속의 길을 열어 놓는 행위도 중요한 컴퓨터파괴범죄로 등장하게 될 것이다.

컴퓨터범죄의 발생현황과 추세를 예측하기 위하여는 신뢰성이 있는 통계자료의 작성이 필수불가결하다고 할 것이다. 그러나 현재의 통계를 보면 그것의 체계성과 신빙성에 대단히 의문이 많다. 이는 물론 컴퓨터범죄의 유형에 대하여 통일된 견해가 없다는 점에 기인하는 바가 크지만 관련기관 사이의 유기적인 협조를 통하여 공신력있는 통계자료를 작성할 수 있도록 노력하여야 할 것으로 판단된다.

라. 대응방안

1) 형사법적 대응방안

14) 데이비드 론펠트 지음/홍석기 옮김, 정보지배사회가 오고 있다, 자작나무, 1997, 46면.

① 현행 형벌법규에 의한 대응

i) 자료의 부정조작행위에 대하여

ⓐ 적용가능한 구성요건

자료의 부정조작에 적용될 수 있는 구성요건은 공전자기록위작·변작죄(형법 제227조의2),[15] 사전자기록위작·변작죄(형법 제232조의2),[16] 컴퓨터사용사기죄(형법 제347조의2)[17] 그리고 전산망보급확장과이용촉진에관한법률(이하 "전산망법"이라 한다.)상의 전자문서[18] 위작·변작죄(제29조 1항, 제25조 2항)[19] 이다.

ⓑ 전자기록위작·변작죄

자료의 부정조작행위는 그 결과로서 컴퓨터의 하드디스크에 수록된 내용을 변경시키게 되므로 필연적으로 (공·사)전자기록범죄의 구성 여부가 문제된다. 전자기록(電磁記錄)이란 일정한 매체에 전자방식(電子方式)이나 자기방식(磁氣方式)으로 저장된 기록을 의미한다. 따라서 정보를 보존하는 매체(일정한 정보를 기록하는 디스켓 자체) 또는 그것에 기록된 정보 자체가 아니라[20] 정보가 매체에 기록된 상태, 즉 매체와 정보의 불가분적 결합상태를 의미한다. 전자방식은 대전(帶電)시키는 방식으로 이에는 반도체기억집적회로(IC)에 의한 것이 있고, 자기방식이란 자화(磁化)시키는 방식으로 이에는 자기디스크나 자기테이프에 의한 것이 있다. 전자방식에 의한 것이 컴퓨터내의 ROM, RAM 등의 기록이고, 자기방식에 의한 것이 현금카드, 전화카드, 전철표 등의 자기띠

15) 사무처리를 그르치게 할 목적으로 공무원 또는 공무소의 전자기록등 특수매체기록을 위작 또는 변작한 자는 10년이하의 징역에 처한다.

16) 사무처리를 그르치게 할 목적으로 권리 의무 또는 사실증명에 관한 타인의 전자기록등 특수매체기록을 위작 또는 변작한 자는 5년이하의 징역 또는 1천만원이하의 벌금에 처한다.

17) 컴퓨터등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년이하의 징역 또는 2천만원이하의 벌금에 처한다.

18) "전자문서"라 함은 국가기관, 지방자치단체 및 법령의 규정에 의하여 그 위탁을 받은 자가 전산망을 이용하여 전송·처리 또는 보관하는 문서형식의 자료로서 표준화된 것을 말한다(전산망보급확장과이용촉진에관한법률 제2조 3호).

19) 전자문서를 위작·변작하거나 그 사정을 알면서 위작·변작된 전자문서를 행사한 자는 10년이하의 징역 또는 1억원이하의 벌금에 처한다. 이 죄의 미수범은 처벌한다(전산망보급확장과이용촉진에관한법률 제29조 2항).

20) 장영민, 개정형법의 컴퓨터범죄, 고시계 1996.2, 46면; 米澤慶治, 刑法等一部改正法の概要, ジュリスト No. 889, 66면.

부분으로 이것이 현재 가장 널리 사용되고 있다.

'공전자기록'(공무원 또는 공무소의 전자기록)이란 공무원 또는 공무소의 직무집행으로서 작성되는 것을 말한다. 예컨대, 주민등록표화일, 자동차등록파일, 지적화일 등이 이에 해당한다. '사전자기록'(권리 의무 또는 사실증명에 관한 전자기록)의 경우 권리·의무에 관한 사전자기록이란 권리의무의 발생 변경 소멸의 요건으로 되거나 그 원인이 되는 사실에 대하여 증명력을 가지는 것으로 예컨대, 온라인化된 은행예금원장파일 등 문서의 형태로는 계약서등에 상당하는 전자기록(VAN시스템에 있어서의 受注파일 등)을 말하며, 사실증명에 관한 사전자기록이란 사회생활상 중요한 사항을 증명할 수 있는 정보를 기록한 것으로, 예컨대 상품대장파일, 신용카드 직불카드 선불카드[21] 현금카드, 장차 등장할 전자주민카드 등 문서의 형태로는 장부나 증명서에 상당하는 전자기록을 말한다. 따라서 금융기관 등의 예금원장파일은 전자기록범죄의 객체에 해당하지만, 컴퓨터의 정보처리에 관한 명령인 프로그램을 기록한 전자기록은 동죄의 객체에 해당하지 않는다.[22] 즉 프로그램을 조작하여 예금원장파일에 잘못된 내용(예컨대 허위입금)이 기록되는 경우 예금원장파일에 대하여만 (공·사)전자기록범죄를 구성할 수 있을 뿐 프로그램을 변경한 행위 자체는 (공·사)전자기록범죄를 구성하지는 않는다. 이러한 행위는 사전자기록위작죄와 컴퓨터사용사기죄의 상상적 경합범이 될 것이다.

전자기록위작·변작죄의 경우 문서범죄의 행위태양인 '위조 변조 허위작성 변개' 대신 '위작 변작'이라고 한 것은 전자기록등은 문서와는 달리 가독성 가시성이 없을 뿐만 아니라 기록과정에 다수인의 의사나 행위가 관여할 수 있으므로 작성명의를 생각하기 어렵다는 점을 고려한 것이다. 그리하여 개정형법은 문서범죄의 경우와는 다르게 전자기록범죄의 경우에는 공 사전자기록 모두 '위작 변작'만을 행위태양으로 하였다.

전자기록등위작·변작죄의 위작·변작의 의미에 대하여, 위작이란 권한없이 전자기록등을 작성하는 경우와 내용허위의 전자기록을 만드는 것이며 변작이란 권한없이 또는 허위내용으로 기록을 변경하는 것이라는 견해,[23] 위작은 권한없이 전자기록을 만들어

21) 다만 信用카드 直拂카드 先拂카드는 별도로 여신전문금융업법의 적용을 받으므로 권한없이 타인의 신용카드 直拂카드 先拂카드를 만들거나(위조), 신용카드 直拂카드 先拂카드의 磁氣띠부분의 내용을 변경시키는 행위(변조)는 동법에 의하여 처벌된다(동법 제70조 1항).

22) 이재상, 형법각론, 박영사, 1996, 530면.

23) 배종대, 형법각론, 홍문사, 1996, 501면; 법무부, 형법개정법률안 제안이유서(이하 '이유서'라 함), 1992, 230면.

내는 것을 의미하고 변작은 이미 만들어진 전자기록의 내용을 권한없이 변경하는 것을 의미한다는 견해,[24] 사전자기록의 위작·변작은 사문서의 위조·변조에 대응하여 유형위조만을 의미하지만 공전자기록의 위작·변작은 유형위조와 무형위조를 포함하는 것이라는 견해[25]가 대립한다. 생각건대 전자기록이 문서보다 중하게 보호받아야 할 이유가 있는지 의문이며 또한 컴퓨터범죄에 대한 개정형법의 기본적 태도는 컴퓨터시스템을 특권화하여 보호하려는 것이 아니라 컴퓨터시스템을 이용함으로써 실현되는 개개의 이익 내지 가치를 종래의 법익과 평행하게 보호법익으로 하려는 것이고,[26] 본죄의 보호법익은 정보처리의 정확성이 아니라 전자기록의 증명작용에 대한 공공의 안전과 신용[27]이라는 점을 고려할 때 문서범죄에 대하여 형식주의를 원칙으로 하고 예외적으로 공둔서와 의사의 진단서 등에 대하여 실질주의를 취하고 있는 형법의 입장은 전자기록범죄에도 관철되어야 할 것이다. 즉 작성명의를 생각하기 어려운 전자기록의 특질을 고려하되 기본적으로는 문서범죄와 평행하게 해석하여야 하므로, 위작은 권한없이 전자기록을 만들어 내는 것을 의미하고 변작은 이미 만들어진 전자기록의 내용을 권한없이 변경하는 것을 의미한다고 해석하여야 한다.

어느 견해에 의하거나 자료를 조작할 권한이 없는 자가 컴퓨터통신이나 단말기 등을 이용하여 자료를 부정조작하는 경우에는 전자기록위작·변작죄에 의해 처벌될 것이다. 그러나 권한이 있는 자가 단말기 등을 이용하여 허위입금을 하는 등의 방법으로 자료를 부정조작하는 경우에는 위의 어느 견해를 취하느냐에 따라 전자기록범죄의 구성 여부가 달라지게 될 것이다. 이에 관하여 아직 대법원의 태도가 나와 있지는 않지만 어느 견해에 의하더라도 문서범죄와의 처벌 불균형이 초래된다는 문제점이 있다.

그리고 전산망법에 규정된 전자문서에 해당하는 전자기록을 위작·변작한 경우에는 형법과 전산망법이 함께 적용될 수 있다. 즉 국가기관, 지방자치단체 및 법령의 규정에 의하여 그 위탁을 받은 자가 전산망을 이용하여 전송·처리 또는 보관하는 문서형식의 자료로서 표준화된 전자기록(전산망법 제2조 3호 참조)을 위작·변작하는 행위는 형법상의 전자기록범죄와 전산망법상의 전자문서위작·변작죄의 구성요건에 해당하게 된다.

---

24) 이재상, 앞의 책, 530면.

25) 박상기, 형법각론, 박영사, 1996, 528-530면 및 539면.

26) 컴퓨터손괴등 업무방해죄나 컴퓨터 사용사기죄의 형이 업무방해죄나 사기죄의 형과 동일하고, 전자기록등을 문서와 동일하게 취급하고 있음(제366조, 제141조 1항)이 그 근거이다.

27) 이재상, 앞의 책, 530면.

법의 취지와 처벌규정의 소재에 주목한다면 전산망법의 처벌규정이 형법의 특별법에 해당하므로 통상 전산망법에 의해 처벌되겠지만, 공전자기록의 성격을 갖는 전자문서인 경우에는 공전자기록위작·변작죄의 법정형(10년이하의 징역)이 전자문서위작·변작죄의 법정형(10년이하의 징역 또는 1억원이하의 벌금) 보다 중하기 때문에 이러한 행위는 형법에 의하여 처벌되어야 할 것이다.

ⓒ 컴퓨터사용사기죄

컴퓨터통신이나 단말기 등을 이용하여 은행의 예금원장파일에 기록된 내역을 변경시켜 자신이나 제3자의 예금계좌에 허위로 입금되게 하는 행위가 컴퓨터사용사기죄를 구성할 것인가가 문제된다. 이러한 행위는 컴퓨터 등 정보처리장치에 허위의 정보를 입력하여 정보처리를 하게 함으로써 재산상 이익을 취득하거나 제3자로 하여금 취득하게 한 것이므로 컴퓨터사용사기죄에 의하여 처벌될 것이다.

컴퓨터사용사기죄와 관련하여서는 진실한 정보의 권한없는 사용, 예컨대 습득한 타인의 현금카드를 현금자동인출기에 투입하는 행위 그리고 그에 의하여 현금을 인출하거나 계좌이체하는 행위가 컴퓨터사용사기죄에 해당하느냐가 문제되는 바, 이는 두 개의 관점에서 검토하여야 할 것이다. 먼저 진실한 정보의 권한없는 사용이 컴퓨터사용사기죄의 행위태양인 '부정한 명령의 입력'에 해당하느냐이다. '자료의 권한없는 사용'을 행위태양의 하나로 규정하고 있는 독일형법에서는 이러한 행위는 당연히 컴퓨터사기죄로 처벌된다. 개정형법과 동일한 내용을 포함하고 있는 일본형법 제246조의2[28] 前段의 해석과 관련하여, 다수의 견해는 타인의 현금카드의 부정사용이 동조에 해당한다고 보고 있는데 구체적으로는 허위의 정보의 입력에 해당한다는 견해[29]와 부정한 지령의 입력에 해당한다는 견해[30]가 대립한다. 개정형법의 해석에 있어서도 타인의 현금카드의 부정사용이 부정한 명령의 입력에 해당한다는 견해[31]와 해당하지 않는다는 견해[32]가 대

28) 일본형법 제246조의2: 前條外에 사람의 사무처리에 사용하는 電子計算機에 虛僞의 情報 또는 不正한 指令을 주어 財産權의 得喪 變更에 관한 不實의 電磁的 記錄을 作出하거나 財産權의 得喪 變更에 관한 虛僞의 電磁的 記錄을 사람의 사무처리의 用에 供하여 財産上 不法한 利益을 얻거나 타인으로 하여금 이를 얻게 한 자는 10년이하의 징역에 처한다.

29) 西田典之, コンピュ-タの不正操作と財産犯, ジュリスト No.885, 17면: 大谷實, 前揭論文(下), 判例タイムズ No.651, 32면.

30) 神山敏雄, コンピュ-タ犯罪立法の批判的考察, 法律時報 60卷 1號, 82면.

31) 김일수, 형법각론, 박영사, 1996, 302면: 박상기, 앞의 책, 330면: 배종대, 앞의 책, 344면.

32) 이재상, 앞의 책, 315면: 장영민, 앞의 논문, 49면: 이철, 앞의 논문(한국법제연구원), 131면.

립하고 있는데, 부정설에 의하면 —현금인출행위이든 계좌이체행위이든— 컴퓨터사용사기죄는 성립하지 않을 것이다. 생각건대 '명령'을 프로그램에 한정하여 컴퓨터에 대한 작업지시만이 명령에 해당한다고 해석함으로써 부정한 명령의 입력을 프로그램 자체를 조작하는 것에 한정[33] 한다면 진실한 자료의 권한없는 사용은 프로그램 자체를 조작하는 것이 아니므로 부정설이 타당할 것이다. 그러나 자료와 명령이 엄격히 구별되는 것은 아니며 명령이 반드시 프로그램만을 의미한다고 볼 수 없고 경우에 따라서는 프로그램도 자료가 될 수 있다. 그러므로 부정한 명령의 입력이란 프로그램 자체는 조작함이 없이 명령·자료를 입력(사용)할 권한없는 자가 명령·자료를 입력하는 것도 포함한다고 해석하여야 할 것이므로 진실한 자료의 권한없는 사용도 부정한 명령의 입력에 해당한다고 본다.[34] 또한 위작한 현금카드를 현금자동인출기에 투입·사용하는 것도 부정한 명령의 입력에 해당한다.[35]

진실한 정보의 권한없는 사용이 컴퓨터사용사기죄의 행위태양인 '부정한 명령'에 해당한다는 견해에 의하면 계좌이체행위는 컴퓨터사용사기죄를 구성한다는 점에 의문이 없으나 현금인출행위는 다툼이 있다. 왜냐하면 컴퓨터사용사기죄의 객체가 종래의 사기죄와는 달리 재물을 포함시키지 않고 재산상 이익에 한정되어 있기 때문이다. 생각건대 형법은 재산죄의 객체를 재물과 재산상 이익으로 구별하여 규정하고 있고, 현금은 유체물로서 재물이지 재산상의 이익에 속하는 것이 아니므로, 예컨대 습득한 타인의 현금카드를 현금자동인출기에 투입하여 현금을 인출하는 행위는 컴퓨터사용사기죄가 아니라 절도죄에 의하여 처벌할 수 있을 뿐이다.

ii) 컴퓨터파괴행위에 대하여

ⓐ 적용가능한 구성요건

컴퓨터파괴에 적용가능한 규정은 전자기록손괴죄(형법 제366조 1항),[36] 공용전자기록

33) 이에 따르면 타인의 현금카드를 위작하여 타인계좌에서 자기계좌로 이체하는 것도 "프로그램"을 조작하는 것이 아니므로 부정한 명령에 해당하지 않고 또한 비밀번호와 계좌번호는 위작된 것이기는 하지만 '허위'는 아니므로 허위의 정보에도 해당하지 않게 되어 결국 본죄는 성립하지 않는다고 해석하여야 할 것이다.

34) 법무부, 이유서, 182면.

35) 大谷實, コンピュ-タ關聯犯罪と刑法の一部改正(下), 判例タイムズ No.646, 33면; 神山敏雄, コンピュ-タ犯罪立法の批判的考察, 法律時報 60卷1號, 82면.

36) 타인의 재물, 문서 또는 전자기록등 특수매체기록을 손괴 또는 은닉 기타 방법으로 그 효용을 해한 자는 3년이하의 징역 또는 700만원이하의 벌금에 처한다. 제371조에 의하여 제366

무효죄(형법 제141조 1항),[37] 컴퓨터손괴업무방해죄(형법 제314조 2항),[38] 전산망[39] 보호조치침해죄(전산망법 제30조의2, 제22조 2항)[40] 그리고 전산망정보훼손죄(전산망법 제30조, 제25조 1항)[41]이다.

ⓑ 전자기록손괴죄와 공용전자기록무효죄

이 가운데 컴퓨터파괴를 규율하는 일반적인 규정이 전자기록손괴죄와 컴퓨터손괴등 업무방해죄이다. 즉 타인의 컴퓨터에 수록되어 있는 프로그램·자료·정보는 전자기록손괴죄의 행위객체인 전자기록에 해당되고 이러한 것들을 삭제하거나 변경하는 행위는 그 효용을 해하는 것이므로 전자기록손괴죄의 손괴에 해당되어 결국 컴퓨터파괴행위는 전자기록손괴죄로 처벌된다. 만약 이러한 전자기록이 공무소에서 사용되는 것이라면 공용전자기록무효죄에 의하여 처벌될 것이다.

ⓒ 컴퓨터손괴등 업무방해죄

나아가 이러한 것들을 손괴하여 사람의 업무에 사용되는 컴퓨터가 제대로 작동할 수 없게 한다면, 이는 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 것이 되므로 컴퓨터손괴등 업무방해죄를 구성하게 된다.

이와 관련하여 공무에 사용되는 컴퓨터나 전자기록에 대하여 파괴행위(프로그램이나 자료 등 기록내용의 삭제·교란행위)를 함으로써 공무수행에 장애를 초래한 경우에 어

조의 미수범도 처벌된다.

37) 공무소에서 사용하는 서류 기타 물건 또는 전자기록등 특수매체기록을 손상 또는 은닉하거나 기타 방법으로 그 효용을 해한 자는 7년이하의 징역 또는 1천만원이하의 벌금에 처한다. 제143조에 의하여 제141조의 미수범도 처벌된다.

38) 컴퓨터등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형(5년이하의 징역 또는 1천5백만원이하의 벌금)과 같다.

39) "전산망"이라 함은 전기통신설비와 전자계산조직 및 전자계산조직의 이용기술을 활용하여 정보를 처리·보관하거나 전송하는 정보통신체제를 말한다(전산망보급확장과이용촉진에관한법률 제2조 1호).

40) 전산망을 이용하여 정보를 처리·보관·전송하는 사업을 영위하는 자가 전산망의 안정성 및 정보의 신뢰성을 확보하기 위하여 강구한 전산망의 보호조치를 침해 또는 훼손한 자는 3년이하의 징역 또는 3천만원이하의 벌금에 처한다(전산망보급확장과이용촉진에관한법률 제30조의2, 제22조 2항).

41) 전산망에 의하여 처리·보관·전송되는 타인의 정보를 훼손하거나 비밀을 침해·도용 또는 누설한 자는 5년이하의 징역 또는 5천만원이하의 벌금에 처한다.

떤 구성요건을 적용할 것인가의 문제가 있다. 공무집행방해죄(형법 제136조)나 위계공무집행방해죄(형법 제137조)는 폭행·협박·위계를 행위태양으로 하는데, 이들 행위는 사람에 대하여만 행하여질 수 있는 것이므로 공무에 사람이 개입되지 않고 컴퓨터에 의하여 자동적으로 처리되는 경우에는 이들 구성요건을 적용할 수 없게 된다.

기존의 업무방해죄(형법 제314조)도 허위사실유포·위계·위력을 행위태양으로 하고 있기 때문에 컴퓨터에 의해 자동화된 업무를 컴퓨터파괴행위에 의하여 방해하는 경우에는 적용할 수 없어 처벌의 공백이 있기 때문에 이를 메우기 위하여 컴퓨터손괴등 업무방해죄를 신설하였던 것이다. 그런데 공무방해에 관한 죄에는 컴퓨터손괴등 업무방해죄에 상응하는 규정을 신설하지 않아 문제가 된다.

위계·위력에 의한 업무방해죄와 마찬가지로 공무가 컴퓨터등 손괴죄의 업무에 포함되느냐에 관하여 견해가 대립하고 있으며, 특히 위계·위력에 의한 업무방해죄의 업무에는 공무가 포함되지 않지만 본죄의 업무에는 공무가 포함된다는 견해[42]도 있다. 이 견해는 개정형법이 공무집행방해죄의 경우에는 컴퓨터파괴에 의한 공무방해를 규정하지 아니하였으므로 본죄의 업무에서 공무를 제외하여야 할 이유가 없고, 개정형법이 참고하였던 독일형법 제303조b가 기업의 업무 뿐만 아니라 관청의 업무도 규율대상으로 하고 있다는 점을 근거로 하고 있다. 그러나 우리 형법상 공무집행방해죄와 업무방해죄는 보호법익을 달리 하는 별개의 범죄이며, 독일형법은 공무방해죄만을 처벌하고 있는데(제316조b) 제303조b는 공무 여부를 묻지 않고 '컴퓨터에 의해 처리되는 업무'를 특히 보호하기 위한 규정이므로 독일형법의 규정내용을 이유로 공무를 컴퓨터손괴등 업무방해죄의 업무에 포함시킬 수는 없다. 또한 만약 컴퓨터손괴등 업무방해죄의 업무에 공무가 포함된다고 해석하게 되면, 공무를 방해한 것이 폭행·협박·위계에 의한 경우이면 '5년이하의 징역 또는 1천만원이하의 벌금'(제136조, 제137조)임에 반하여 컴퓨터파괴에 의한 경우이면 '5년이하의 징역 또는 1천500만원이하의 벌금'으로서 상이하게 된다. 따라서 일반업무방해죄의 업무와는 달리 본죄의 업무에 공무를 포함하는 견해는 타당하지 않고 일반업무방해죄와 동일하게 본죄의 업무에 공무는 포함되지 않는다고 해석하여야 한다.

결국 정보화의 진진에 따라 사람의 개입없이 이루어지는 자동화된 공무에 사용되는

42) 전지연, 컴퓨터파괴에 대한 형법적 검토, 형사정책 제8호(1996), 273면; 박상기, 앞의 책, 215 및 219면.

컴퓨터나 전자기록을 파괴하여 당해 공무의 수행에 장애를 초래한 경우에는 처벌의 공백이 나타나게 된다.

ⓓ 전산망정보훼손죄(전산망법)

형법상의 전자기록손괴죄의 객체인 "전자기록"은 기록으로서의 성질상 계속성이 있어야 하므로 컴퓨터통신을 이용하여 전송중이거나 컴퓨터에 의하여 처리중인 자료는 이에 해당하지 않는다. 이러한 정보를 훼손하는 행위는 전산망정보훼손죄에 의하여 처벌될 것이다. 다만 전산망정보훼손죄의 객체에는 "전산망에 의하여 처리·전송되는 타인의 정보"는 물론이고 "보관"되는 타인의 정보도 포함되므로 컴퓨터에 수록되어 있는 타인의 정보를 컴퓨터파괴행위에 의하여 못쓰게 하였다면 형법상 전자기록손괴죄의 특별규정인 전산망법상의 전산망정보훼손죄를 적용하여 처벌하여야 할 것이다.

그리고 해커가, 전산망사업을 영위하는 자가 자신의 전산망에 대한 무단침입으로부터 전산망의 안정성과 정보의 신뢰성을 확보하기 위하여 마련해놓은 보호조치를 파괴(무력화)하였다면 전산망법에 규정된 전산망보호조치침해죄에 의하여 처벌된다. 다만 동죄는 '전산망사업자가 강구해 놓은 전산망의 보호조치'를 침해 또는 훼손하는 행위만을 처벌대상으로 하므로, 전산망사업자 아닌 프로그램개발자가 강구해 놓은 보호장치(복제방지장치 등)를 파괴하는 행위는 처벌할 수 없다는 한계를 갖고 있다.

iii) 컴퓨터스파이행위에 대하여

ⓐ 적용가능한 구성요건

컴퓨터스파이행위에 대한 처벌법규는 스파이의 대상인 탐지내용이 무엇이냐에 의하여 나누어 검토하여야 한다. 먼저 국가나 공무소의 비밀을 탐지한 경우에는 형법상의 간첩죄(제98조 1항)나 기술적 수단에 의한 공무상비밀침해죄(제140조 3항)[43]에 의하여 처벌될 것이다. 다음으로 개인비밀침해행위에 대하여는 기술적 수단에 의한 비밀침해죄(형법 제316조 2항),[44] 전기통신감청죄(통신비밀보호법 제16조 1호)[45] 그리고 전산망비

43) 공무원이 그 직무에 관하여 봉함 기타 비밀장치한 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형(5년이하의 징역 또는 700만원이하의 벌금)과 같다.

44) 봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형(3년이하의 징역이나 금고 또는 500만원이하의 벌금)과 같다. 이 죄는 고소가 있어야 공소를 제기할 수 있다(형법 제318조).

45) 우편물의 검열, 전기통신의 감청 또는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하

밀침해죄(전산망법 제30조, 제25조 1항)[46]의 적용이 고려될 수 있다.

ⓑ 비밀침해죄와 공무상비밀침해죄

형법상의 비밀침해죄와 공무상비밀침해죄는 '봉함 기타 비밀장치'와 같이 특수한 보호조치를 취한 개인이나 공무상의 비밀을 보호하는 규정이므로, 암호조치를 해 놓은 컴퓨터상의 전자기록에 접근하여 그 내용을 알아낸 경우에는 본죄에 해당하지만 별도의 보안대책을 강구하지 않은 데이터베이스에 대한 무단접근행위에는 적용될 수 없다. 또한 그 내용이 '비밀성'을 갖고 있어야 하므로, 주체가 비밀로 하려는 의사가 있고 객관적으로 비밀로 할만한 이익이 있어야 한다. 나아가 그 내용이 전자'기록'의 형태로 저장된 것이어야 하는데 전송중인 자료나 정보는 계속성이 없어 이에 해당하지 않으므로, 컴퓨터통신을 이용하여 교환되는 비밀을 해킹에 의해 알아내는 행위는 형법상의 비밀침해죄나 공무상비밀침해죄에 의하여는 처벌할 수 없다.

ⓒ 전기통신감청죄(통신비밀보호법)와 전산망비밀침해죄(전산망법)

통신비밀보호법은 통신비밀을 보호하고 통신의 자유를 신장하기 위하여 통신 및 대화비밀을 침해하는 행위를 처벌하는 규정을 두고 있다. 이 법상의 "전기통신"이라 함은 유선·무선·광선 및 기타의 전자적(電磁的) 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말하므로(동법 제2조 3호) 컴퓨터통신에 의한 자료나 정보의 전송도 이에 해당할 것이다. 그리고 "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치(電子裝置)·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다(동법 제2조 7호). 따라서 컴퓨터통신을 이용하여 전송되는 타인의 자료나 정보를 해킹하여 그 내용을 알아내거나 기록한 경우에는 통신비밀보호법에 의해 처벌될 것이다. 이 경우에는 전송되는 자료나 정보는 비밀성을 요하지 않으며, 특별히 보안대책을 강구한 것이어야 할 필요도 없다.

컴퓨터통신은 전산망법에서 말하는 전산망에 해당하기 때문에 컴퓨터통신을 이용하여 전송되는 타인의 자료나 정보를 해킹하여 그 내용을 알아낸 행위는 동법상의 전산

거나 그 취득한 통신 또는 대화의 내용을 공개하거나 누설한 자는 7년이하의 징역에 처한다. 미수범을 처벌한다(통신비밀보호법 제18조).

46) 전산망에 의하여 처리·보관·전송되는 타인의 정보를 훼손하거나 비밀을 침해·도용 또는 누설한 자는 5년이하의 징역 또는 5천만원이하의 벌금에 처한다.

망비밀침해죄의 구성요건에도 해당된다(동법 제30조, 제25조 1항). 동죄의 대상은 비밀이어야 하지만, 특별히 보안대책을 강구한 것이어야 할 필요는 없으며 전산망에 의하여 처리·보관·전송되는 비밀이면 족하다.

결국 컴퓨터통신망에 의하여 전송되는 타인의 비밀을 해킹에 의하여 알아내는 행위는 통신비밀보호법 위반죄(전기통신감청죄)와 전산망법 위반죄(전산망비밀침해죄)의 상상적 경합이 되어 법정형이 무거운 전기통신감청죄로 처벌될 것이다.

ⓓ 영업비밀누설죄(부정경쟁방지법)

기업의 비밀을 컴퓨터스파이행위에 의하여 탐지·누설하는 산업스파이행위에 대하여는 영업비밀누설죄(부정경쟁방지법 제18조 1항 3호),[47] 기술적 수단에 의한 비밀침해죄(형법 제316조 2항) 그리고 전산망비밀침해죄(전산망법 제30조, 제25조 1항)가 적용될 수 있다.

산업스파이행위를 직접적으로 처벌하기 위한 규정은 부정경쟁방지법상의 영업비밀누설죄이다. 동죄는 일정한 지위에 있는 자가 특정의 목적을 갖고 기업의 생산기술에 관한 영업비밀을 누설한 경우에 처벌하므로, 신분범이며 목적범에 해당한다. 부정경쟁방지법상의 영업비밀이라 함은 공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 상당한 노력에 의하여 비밀로 유지된 생산방법·판매방법 기타 영업활동에 유용한 기술상 또는 영업상의 정보를 말한다(동법 제2조 2호). 영업비밀에 관한 부정경쟁방지법상의 규정은 과거에 법률이 직접적으로 규율하지 않았던 노하우(Know-How)[48] 를 직접적으로 법적 규제하에 두기 위하여 부정경쟁방지법[49]을 개정하여 신설한 것이다. 동법은 영업비밀을 보호하기 위한 규정(제10조 - 제12조)을 신설하면서, 처벌대상이 되는 행위를 "기업의 임원 또는 직원"(내부자)이 "부정한 이익을 얻거나 그 기업에 손해를 가할 목적"(주관적인 목적)으로 그 "기업에 특유한 생산기술에 관한 영

47) 기업의 임원 또는 직원으로서 부정한 이익을 얻거나 그 기업에 손해를 가할 목적으로 그 기업에 특유한 생산기술에 관한 영업비밀을 제3자에게 누설한 자는 3년이하의 징역 또는 3천만원이하의 벌금에 처한다. 이 죄에 대한 공소는 피해자의 고소가 있어야 한다(동조 2항).

48) 송영식·이상정·황종환, 지적 소유권법, 1991, 168면. 일반적으로 노하우(Know-How)라 함은 특허적격이 있는 것을 포함하여 특허를 부여받지 않은 발명, 기술, 제조방법, 판매방법, 경영방법과 비밀로 하려는 정보를 말하며, 기술적 노하우와 영업적 노하우로 구분된다. 통상 노하우라고 할 때에는 기술적 노하우를 말한다(송영식·이상정·황종환, 위의 책, 167면).

49) 1991.12.31. 법률 제4478호.

업비밀"(소위 기술적 노하우)를 누설한 경우로 한정하고 있다.[50] 즉 영업비밀 일반에 대한 스파이행위가 아니라 기술적 노하우에 대한 스파이행위만을 처벌대상으로 하고 있다. 부정경쟁방지법상의 영업비밀탐지·누설행위에 대하여는 고소가 있어야 논할 수 있다(부정경쟁방지법 제18조 제2항).

그리고 형법상의 비밀침해죄는 일정한 보호조치를 강구하여 놓은 사람의 비밀을 침해하는 행위를 처벌하는 일반적인 규정이고, 전산망법의 규정은 전산망에 침입하여 비밀을 침해·도용 또는 누설하는 행위를 처벌한다. 따라서 형법이나 전산망법도 산업스파이행위를 처벌할 수 있는 규정에 해당한다.

iv) 컴퓨터의 권한없는 사용행위에 대하여

ⓐ 적용가능한 구성요건

현행법상 컴퓨터의 권한없는 사용행위를 직접적으로 처벌하는 규정은 없다. 그 이유는 그러한 행위는 일종의 사용절도에 해당되는 것으로 현재로는 빈번한 것이 아니며 그로 인한 손해가 처벌할만큼 큰 경우도 별로 없다는 점에 있을 것이다. 다만 개정형법에 신설된 편의시설부정이용죄(제348조의2)[51] 와 컴퓨터손괴등 업무방해죄(제314조 2항)가 컴퓨터의 권한없는 사용에 고려될 수 있다.

ⓑ 편의시설부정이용죄와 컴퓨터손괴등 업무방해죄

편의시설부정이용죄는 부정한 방법으로 대가를 지급하지 아니하고 유료자동설비를 이용하여야 성립한다. 동죄의 "유료"자동설비란 비용이 투입되어야 재물이나 용역을 제공하는 설비를 말하는 바, 타인의 컴퓨터가 반드시 이에 해당하지는 않으므로 제348조의2가 컴퓨터의 권한없는 사용에 적용될 수 없다. 또한 컴퓨터손괴등 업무방해죄는 컴퓨터등에의 가해행위에 의해 현실로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해함으로써 성립하는 바, 타인의 컴퓨터를 권한없이 사용하는 행위가 정보처리에 장애를 발생시키지 않는 한 동죄에 해당하지 않는다. 그러나 컴퓨터를 권한없이 사용하여 컴퓨터의 처리능력을 초과하게 함으로써 정보처리에 장애를 일으킨 경우에는 본죄에

50) 부정경쟁방지법 제18조 1항 3호. 부정경쟁방지법은 영업비밀 일반에 대한 스파이행위가 아니라 기술적 노하우에 대한 스파이행위만을 처벌대상으로 하고 있으며 동법상의 영업비밀탐지·누설행위에 대하여는 고소가 있어야 논할 수 있는 친고죄이다(동법 제18조 2항).

51) 부정한 방법으로 대가(對價)를 지급하지 아니하고 자동판매기, 공중전화 기타 유료자동설비를 이용하여 재물 또는 재산상의 이익을 취득한 자는 3년이하의 징역, 500만원 이하의 벌금, 구류 또는 과료에 처한다.

해당하므로 개정형법은 제한된 범위에서 컴퓨터의 권한없는 사용을 처벌할 수는 있다. 즉 형법 제314조 2항은 특별한 경우에 제한적으로 컴퓨터의 권한없는 사용을 처벌할 수 있음에 불과하다.

② 처벌법규의 신설 내지 보완

ⅰ) 자료의 부정조작행위에 대하여

ⓐ 전자기록위작·변작죄

전자기록은 의사표시의 방법과 표현매체, 표시된 의사의 인식방법, 작성명의인 등 문서와는 여러 면에서 구별되지만 전자기록을 문서와 유사하게 행위객체로 하는 새로운 규정을 신설한 것은 전자기록이 문서와 동일한 기능을 하기 때문에 이를 보호하기 위한 것이다. 즉 새로운 표현매체의 등장으로 인하여 그 형식은 다르지만 사회적 증명기능은 동일하다는 판단에서 전자기록을 "문서에 관한 죄"의 일부로 규정한 것이므로 전자기록범죄의 보호법익은 '전자기록의 진정(眞正)에 대한 공공의 안전과 신뢰'라고 보아야 한다. 기록매체와 기록방법의 상이함을 고려한다고 하더라도 전자기록범죄의 경우에 문서범죄와 다르게 행위태양을 규정하여 기록매체가 전자기록인가 문서인가에 따라 실질적으로 동일한 법익침해행위에 대하여 그 처벌이 달라지는 것은 타당하지 않다. 또한 전자기록(형법상의 용어)과 전자문서(전산망법 등 주로 정보통신과 관련된 법률상의 용어), 위작·변작(형법이나 전산망법상의 표현)과 위조·변조(여신전문금융업법상의 신용카드에 대한 표현)가 과연 왜 달라야 하고 어떻게 다른가의 문제가 있다. 사견으로는 형법상 전자기록범죄의 행위태양인 위작·변작은 생소한 용어로서 어떻게 해석하더라도 문서범죄와의 현저한 불균형을 초래하므로 "위조·변조"로 하든가 아니면 "권한없이 작성하거나 변경"하는 것으로 개정하여야 한다고 본다. 그에 따라 허위공문서작성죄(제227조)에 대응하여 공전자기록에 대하여는 허위로 작성하거나 변경하는 행위를 처벌하는 규정을 신설하여야 할 것이다.

ⓑ 컴퓨터사용사기죄

컴퓨터사용사기죄의 경우 동죄의 객체를 사기죄와는 달리 재산상 이익에 한정한 결과 컴퓨터에 허위의 정보나 부정한 명령을 입력하여 정보처리를 하게 함으로써 재물을 취득하거나 제3자로 하여금 취득하게 한 때에는 컴퓨터사용사기죄가 아니라 절도죄로 처벌할 수밖에 없을 것이다. 그러나 완전히 동일한 행위임에도 불구하고 취득한 재산이 재물인가 재산상 이익인가에 따라 성립되는 범죄가 다르며, 더욱이 그 처벌에 있어서도 재물취득인 경우에는 절도죄로서 6년이하의 징역 또는 1천만원이하의 벌금이고 재산상

이익취득인 경우에는 컴퓨터사용사기죄로서 10년이하의 징역 또는 2천만원이하의 벌금인 점에서 대단히 문제가 많다. 따라서 컴퓨터사용사기죄의 객체에 재물을 추가하여야 할 것이다.

그리고 진실한 정보를 권한없이 사용하여 재물이나 재산상 이익을 취득한 경우에 컴퓨터사용사기죄가 성립하느냐에 대하여는 앞서 살펴본 바와같이 견해가 대립하고 있다. 사견으로는 이러한 행위도 컴퓨터사용사기죄의 '부정한 명령의 입력'에 해당한다고 해석하는 것이 타당하다고 생각하지만, 해석의 다툼을 없애기 위하여 독일형법과 같이 "진실한 정보를 부정하게 사용"하는 행위도 구성요건에 추가하는 것이 바람직하다고 본다.

ii) 컴퓨터파괴행위에 대하여

컴퓨터파괴행위, 즉 컴퓨터 자체의 손괴나 전자기록의 손괴·교란에 의하여 정보처리에 장애를 발생하게 하여 사람의 업무를 방해하면 손괴죄 외에 업무방해죄도 성립하게 된다. 이러한 상황은 개인이나 기업의 업무에 대하여는 물론이고 국가와 지방자치단체의 사무에 대하여도 초래될 것인 바, 이번 형법개정에서 "공무방해에 관한 죄"에는 이러한 행위를 처벌하는 규정을 신설하지 않았다. 물론 위에서 살펴본 바와같이 컴퓨터손괴등 업무방해죄(제314조 2항)의 업무에는 공무가 포함된다고 해석하는 견해가 있지만 이러한 해석이 타당하지 않다는 점은 이미 언급하였다.

결국 컴퓨터파괴에 의한 공무방해행위를 규정하지 아니한 것은 중대한 입법의 흠결로서 향후 컴퓨터범죄에 적절하게 대처하는데 많은 어려움을 가져올 것이므로 컴퓨터손괴등 업무방해죄와 유사한 내용으로 컴퓨터손괴등 공무방해죄를 신설하여야 할 것이다.

iii) 컴퓨터스파이행위에 대하여

컴퓨터스파이행위와 관련하여서는 동일한 행위에 대하여 여러 법률이 중첩적으로 적용되는 점을 정비할 필요가 있다. 예컨대 보호조치를 해 놓은 컴퓨터에 기록되어 있는 비밀을 알아낸 경우에는 형법상의 비밀침해죄와 전산망법위반죄(제30조, 제25조 1항)에 해당하며, 컴퓨터통신망을 이용하여 전송되는 타인의 비밀을 취득하거나 그 내용을 공개 또는 누설하는 경우에는 통신비밀보호법(제16조 1호)과 전산망법이 중첩적으로 적용되는 문제가 있다. 또한 특별히 보호조치를 해놓은 비밀에 대한 침해행위(형법상의 비밀침해죄)의 법정형과 특수한 통신수단에 의해 전달되는 자료나 정보에 대한 침해행위(통신비밀보호법등 특별법)의 법정형과의 비교·검토도 필요하다고 본다.

산업스파이행위를 직접적으로 처벌하기 위한 규정인 부정경쟁방지법 제18조 제1항은 주체를 '기업의 임원 또는 직원'으로, 객체를 '기업에 특유한 생산기술에 관한 영업비밀'(소위 기술적 노하우)로 제한하고 있으며, 초과주관적 요소로서 '기업에 손해를 가할 목적'을 요구하고 있다. 따라서 기업외부자의 탐지·누설행위나, 내부자라도 부정한 이익의 취득이나 가해의 목적이 없는 경우(예컨대 군사적인 목적에서 탐지·누설한 경우) 또는 생산기술이 아닌 영업비밀(예컨대 고객정보 등)을 탐지·누설한 경우에는 여전히 적절하게 처벌할 수 없다. 다만 그러한 행위가 형법상의 다른 구성요건을 충족하는 경우(예컨대 절도죄, 사기죄, 횡령죄, 배임죄, 장물죄 등)에는 그 한도에서 간접적으로 보호받을 수는 있겠지만 그러한 방법은 사안의 본질과는 부합하지 않는다. 예컨대 외부자가 생산기술이 아닌 노하우가 들어 있는 문서나 컴퓨터디스켓 등을 절취하는 경우에는 주거침입죄나 절도죄로 처벌할 수밖에 없을 것이다.[52]

그러나 오늘날의 산업스파이행위는 내부인은 물론 외부인에 의하여, 특히 컴퓨터통신을 악용하여 기업의 전산망에 침입하는 자들에 의하여 침해될 위험성이 매우 높으며, 생산기술이 아닌 고객정보 등 기업정보도 대단히 중요시됨에 비추어 부정경쟁방지법의 처벌규정은 산업스파이행위에 대하여 별로 효과를 발휘할 수 없을 것이다. 또한 형법상의 비밀침해죄와 전산망법은 산업스파이행위를 직접적으로 규율할 목적으로 제정된 것은 아니다. 나아가 제한된 범위에서 처벌되는 부정경쟁방지법상의 산업스파이행위(3년이하의 징역 또는 3천만원이하의 벌금)가 그 행위의 불법정도 및 손해 그리고 파급효과에 비추어 볼 때 일반적인 비밀침해행위(3년이하의 징역 또는 5백만원이하의 벌금)와 비슷한 형으로 처벌되는 점도 검토해 보아야 할 것이다.

iv) 컴퓨터의 권한없는 사용행위에 대하여

컴퓨터의 권한 없는 사용행위에 대하여는 과연 형사적인 제재가 필요할 것인가에 관하여 지속적인 연구검토가 필요할 것이다. 이를 위하여 과연 그러한 행위가 얼마나 발생하고 있는가, 그리고 그로 인한 피해는 어느 정도인가에 관하여 자료를 수집하고 분석하여야 한다.

2) 경찰제도적 대응방안

52) 국내기업에 이사대우로 근무하면서 해외시장판로 및 납품가격 등이 수록된 컴퓨터디스켓을 훔쳐 경쟁회사에 넘겨 준 호주인산업스파이가 고작 절도혐의로 구속되었을 뿐이다(동아일보 1993.1.25.).

① 전문수사조직의 설치·운영

컴퓨터관련기술의 비약적인 발전과 컴퓨터의 보급활용이 일상생활과 경제거래의 모습을 획기적으로 변화시키면서 범죄자들도 하루가 다르게 새로운 범죄대상과 범행수법을 찾아내고 있다. 컴퓨터가 생활필수품의 하나가 되면서 아마 앞으로는 전자적 정보처리시스템(EDPS)이 범죄행위의 중요한 대상이나 수단이 될 것이다. 지금까지는 통상 범죄자들이 유형적 방법을 사용하여 피해자와의 대면적(對面的) 상황에서 범죄를 범하였으나, 앞으로는 컴퓨터조작 등 전문적인 기술을 사용하여 피해자에게 모습을 드러내지 않는 익명적(匿名的) 상황에서 수많은 범죄를 범할 수 있게 되었다. 따라서 기존의 전통적인 범죄를 염두에 둔 수사기관의 대응만으로는 날로 과학화·지능화·전문화되어 가는 컴퓨터범죄자들을 효과적으로 찾아내고 증거를 발견·수집하여 처벌하기가 거의 불가능하다고 하여도 지나친 말이 아닐 것이다.

이를 그대로 방치한다면 컴퓨터범죄는 날로 기승을 부릴 것이고 그에 따라 정보화사회는 중대한 도전에 직면하리라는 것은 명약관화한 일이다. 즉 정보화사회가 범죄의 광활한 천국(범죄의 유토피아)이 아니라 구성원의 생활의 질을 획기적으로 향상시켜 삶의 유토피아로 정착되려면 컴퓨터범죄에 대한 효과적인 수사와 처벌이 가능하도록 대비하여야 한다. 이를 위하여는 컴퓨터의 하드웨어와 소프트웨어에 풍부한 지식을 갖춘 전문적인 수사관으로 구성되는 조직이 필수적이라고 할 것이다. 즉 컴퓨터범죄에 대한 수사를 담당하고 그에 관련된 정보를 수집하며 수사기법을 연구·개발할 수 있는 시스템을 경찰조직내에 갖추고 있어야 한다. 이러한 권한과 기능--수사, 정보수집, 수사기법의 연구와 개발-- 중 경찰의 본래적 임무인 범죄수사와 그에 관련된 정보수집을 담당하는 조직은 경찰청 자체에 두어야 하겠지만, 수사기법의 연구와 개발은 경찰청 산하에 있는 치안연구소나 교육기관에 맡겨야 할 것이다. 그리고 컴퓨터범죄를 수사하는 조직은 각 경찰청 단위로 우선 1개씩 설치·운영하여 그 장단점을 분석·보완한 후 범죄의 증가 등에 따라 증설 여부를 검토하는 것이 바람직하다고 본다. 이러한 컴퓨터범죄수사대에는 법률이나 범죄수사의 전문가는 물론 컴퓨터전문가가 반드시 포함되어야 할 것이다.

② 수사관에 대한 교육의 강화

컴퓨터와 관련된 기술은 날로 발전하고 있으며 그에 따라 컴퓨터를 이용하는 범죄양상도 변화되어 갈 것이다. 따라서 수사요원에 대하여 새로운 컴퓨터기술과 변화하는 범죄양상을 지속적으로 교육함으로써 새로운 수법의 컴퓨터범죄를 수사할 수 있는 충분

한 역량을 갖추도록 교육체계를 확립하여야 한다. 현재의 7년인 수사경찰에 대한 교육주기는 너무 길어 새롭게 등장하는 신종범죄에 적절하게 대처할 수 없으므로 이들에게 새로운 범죄환경에 대한 교육기회가 충분하게 제공되도록 5년 정도의 주기로 재교육을 실시하여야 한다. 예컨대 수사연수소 등 경찰교육기관에 컴퓨터범죄에 관련된 교과목을 설치하여 컴퓨터기술과 컴퓨터범죄에 대하여 재교육을 받을 수 있도록 프로그램을 수립·시행할 필요가 있을 것이다. 또한 각종의 경찰관련 교육기관에서도 컴퓨터범죄에 관한 기본적인 내용을 교육하여야 한다. 물론 이러한 교과목의 내용에는 컴퓨터의 하드웨어와 소프트웨어에 관련된 기술, 컴퓨터범죄의 수법 그리고 이들 컴퓨터범죄에 적용가능한 법률의 해석론 등이 포함되어야 할 것이다.

③ 피해자의 요청시 비밀수사

컴퓨터범죄의 암수율이 정확하게 조사되어 있지는 않지만 범죄의 특성상 숨은 범죄가 상당히 많을 것으로 생각된다. 즉 전문적인 지식과 기술을 갖춘 자에 의하여 은밀하게 이루어지고 있어 피해자가 피해사실을 인식하기가 쉽지 않고, 컴퓨터범죄의 피해를 입는 기관의 상당수가 자신들의 신뢰도 등 이미지를 생각하여 범죄피해사실을 숨기려는 경향이 있기 때문이다. 이러한 상황은 범죄자들이 안심하고(?) 범죄를 범할 수 있는 동기를 부여하게 되고 이는 결국 범죄에 대한 효과적인 대응을 어렵게 만든다. 이점을 고려하여 피해자의 요청이 있을 경우에는 범죄피해사실을 비밀에 부치고 수사를 할 필요가 있다고 본다.

이와 같이 범죄피해사실을 공개하지 않고 수사를 진행하는 것(비밀수사의 필요성)은 범죄피해신고율을 향상시켜 범죄예방 및 범인검거실적을 높일 뿐만 아니라 수사기관으로 하여금 범죄건수와 범죄수법을 파악할 수 있도록 함으로써 장래의 수사활동에도 많은 도움을 줄 것이다.

3) 사회적 대응방안

① 내부통제장치의 강화

컴퓨터범죄 중 자료의 부정조작은 대부분 전산망취급자나 기타 내부인에 의하여 범하여지므로 이들에 대한 관리감독체계와 보안체계를 강화할 필요가 있다고 본다. 또한 이러한 범죄의 현황을 제대로 파악하여야 효과적인 예방책을 강구할 수 있으므로 범죄발생시 내부적으로 처리하도록 방치하기 보다는 감독기관 등에 반드시 신고하도록 하는 범죄발생신고의무제를 시행하는 방안도 검토해 보아야 할 것이다.

② 언론의 범죄수법 공개보도 자제

범죄자들은 스스로 범죄수법을 체득하기도 하지만 상당수는 타인의 수법으로부터 배우거나 그것을 나름대로 발전시킨다. 타인의 수법을 학습·발전시켜 범행에 사용한다는 것은 교도소에서 일정기간 수형생활을 한 후 다시 범죄를 하는 자들을 통해서 이미 알려진 것이며, 그밖에도 각종의 추리소설이나 언론보도에 나타난 수법을 사용하기도 한다. 이러한 점을 고려할 때 언론기관에서 범죄사실을 보도할 경우에는 범죄자가 사용한 수법을 구체적으로 상세하게 언급하는 것을 자제할 필요가 있을 것이다. 아울러 범죄사실이나 범인을 발견·체포하게 된 단서에 대한 보도 역시 신중하게 취급하여야 할 것이다. 왜냐하면 또다른 범죄자는 그러한 실수(?)를 하지 않으려고 노력할 것이고 이는 결국 수사기관의 수사활동에 많은 부담을 줄 뿐만 아니라 범죄를 예방하여 국민의 법익을 효과적으로 보호하는 데에도 별로 도움을 주지 않을 것이기 때문이다.

이를 위하여 경찰청 등 수사기관이나 컴퓨터보안 관련단체 등 연구기관들이 언론기관에 그 취지를 충분히 설명하여 납득시키는 노력을 하여야 한다. 물론 이러한 보도자제는 국민의 알권리라는 기본권과의 관계에서 문제가 제기될 소지가 있지만 범죄사실이나 체포사실 자체의 보도를 자제하는 것이 아니라 범죄수법이나 체포단서에 대한 구체적이고 상세한 보도를 자제하는 것은 알권리와 모순되지는 않는다고 본다.

③ 컴퓨터관련기관 사이의 연계협력

컴퓨터범죄는 컴퓨터의 기능을 악용하여 행하여지기 때문에 범행후에 수사기관의 활동에 의하여 범인을 발견·체포하여 처벌하는 것도 중요하지만, 보안장치의 개발 등 사전에 컴퓨터범죄를 억제할 수 있는 기술적인 노력을 통하여 컴퓨터범죄가 행하여질 수 있는 틈새를 봉쇄하는 것이 더욱더 중요하다.

이를 위하여는 컴퓨터 생산자, 프로그램 개발자 그리고 대학 등 연구기관 사이의 정보공유와 협력을 통하여 컴퓨터보안체계의 문제점이나 컴퓨터범죄의 발생가능성에 대하여 정보를 교환하고 그에 대한 예방책을 함께 강구하는 노력이 요구된다(소위 산학협동체제의 구축). 여기에는 수사기관이 참여하여 각종의 컴퓨터범죄에 대한 자료를 제공하여야 할 필요가 있음은 물론이다. 또한 수사기관에서는 별도로 컴퓨터범죄의 유형과 수법에 대한 체계적인 분류체계를 연구검토하여 컴퓨터범죄의 발생추세와 향후 대응전략을 마련하는데 도움이 될 수 있도록 제시할 필요가 있다고 생각한다.

④ 컴퓨터범죄에 대한 인식의 확산

컴퓨터파괴행위나 컴퓨터스파이행위는 주로 연령이 낮은 컴퓨터광들이 별다른 죄의

식 없이 자기과시욕의 발로에서 행하는 경우가 많으므로 이러한 행위가 중대한 범죄행위로서 처벌대상이 된다는 점을 컴퓨터에 대한 교육과정에서 널리 인식시켜 나가야 할 것이다. 컴퓨터의 권한 없는 사용행위의 경우 아직은 범죄로서 다루어야 할 필요가 없다고 하더라도 이러한 행위는 분명히 정보사회의 진전에 장애가 된다는 점을 널리 인식시킬 필요가 있다고 본다.

2. 홈(폰)뱅킹범죄

가. 의의와 유형

전화의 발전과 보급 그리고 은행업무의 컴퓨터화, 정보통신기술(IT)의 발전과 컴퓨터의 보급은 금융업무가 사람의 개입 없이 이루어질 수 있는 가능성을 열어 놓았다. 그리하여 전화를 이용하여, 또는 PC통신을 이용하여 자신이 거래하는 은행지점에 직접 갈 필요 없이 그리고 은행의 영업시간 이외의 시간에도 금융거래가 가능하게 되었다. 즉 오늘날 발전된 정보통신기술을 잘 활용한다면 장소적·시간적 제약 없이 금융거래를 할 수 있게 된 것이다.

홈뱅킹(home banking)이란 금융기관의 컴퓨터와 가정의 단말기를 통신회선으로 연결하여 잔액조회, 계좌이체 등의 금융서비스를 제공하는 것을 말하며, 이를 이용하면 송금수수료가 감액되는 등 개인의 금융부대비용이 절약되는 장점이 있다. 펌뱅킹(firm banking)이란 금융기관의 컴퓨터와 기업의 단말기를 통신회선으로 연결하여 일괄송금, 자금이체 등의 금융서비스를 제공하는 것을 말하며, 이를 이용하면 기업의 사무비용이 절약되고 은행의 입장에서도 고객확보차원에서 적극 추진하고 있다고 한다. 홈뱅킹이나 펌뱅킹은 거래은행의 창구에서 홈(펌)뱅킹번호와 비밀번호, 계좌번호를 등록하고 약정서를 작성, 신청한 뒤 컴퓨터통신망을 통하여 미리 등록한 비밀번호 등의 확인을 거쳐 원하는 금융거래를 하게 된다. 그리하여 홈(펌)뱅킹사기는 타인의 비밀번호 등을 알게 된 자가 컴퓨터통신망을 이용하여 홈(펌)뱅킹고객의 계좌로부터 자신이나 제3자의 계좌로 이체시킨 후 이를 인출하는 형태로 이루어진다.

폰뱅킹(phone banking)이란 가정의 전화를 이용하여 금융서비스를 제공받는 것을 말한다. 이것 역시 송금수수료가 절약되는 등의 장점이 있다. 홈(펌)뱅킹이 컴퓨터통신망을 이용하는 것과는 달리 폰뱅킹은 전화선을 이용하여 자동응답시스템(ARS)의 지시에

따라 비밀번호 등을 입력함으로써 원하는 금융거래를 하게 된다. 폰뱅킹사기도 타인의 비밀번호 등을 알게 된 자가 폰뱅킹고객의 계좌로부터 자신 또는 제3자의 예금계좌로 이체시킨 후 이를 인출하는 방법으로 행하여진다.

나. 수법과 특징

1) 수법

① 홈(펌)뱅킹사기수법

홈뱅킹이나 펌뱅킹과 같은 PC뱅킹을 악용하는 사기의 첫 번째 수법은 금융기관이나 컴퓨터회사의 내부인이 홈(펌)뱅킹을 이용하는 고객의 인적사항과 비밀번호 등을 알아내서 자기 또는 제3자의 예금계좌로 이체시킨 후 이를 인출하는 방법이다. 경찰청에 따르면, C은행 모 지점 당좌계장인 김모씨(34)는 골프상 최모씨 등과 공모하여 자신이 관리하던 A회사 당좌계좌의 번호와 홈뱅킹 비밀번호를 알게된 것을 기화로 이를 이용하여 임의로 A회사의 홈뱅킹 계좌를 개설하고 홈뱅킹을 이용하여 A회사의 당좌계좌에 입금된 50억중 44억을 S은행 등 다른 은행 16개 계좌에 이체한 후 이중 9억4천만원을 인출하여 도주하였다고 한다.

두 번째의 홈(펌)뱅킹사기수법은 컴퓨터망에 특수프로그램을 설치해 PC통신을 통하여 홈뱅킹을 이용하는 은행고객의 계좌번호와 비밀번호, 이용자번호를 알아낸 뒤 이들 은행고객의 예금계좌에서 자신이나 제3자 등의 예금계좌로 이체하는 방법이다. 이러한 방법은 해커와 같은 외부인에 의하여 이루어지게 된다. 서울지검 특수2부에 따르면, 모 대학원생 최모씨(20)는 모 통신회사의 인터넷 서비스망에 특수프로그램(TELNET)을 설치해 PC통신을 통해 홈뱅킹을 이용하는 은행고객 13명의 계좌번호와 비밀번호, 이용자번호(ID) 등을 알아낸 뒤 A은행에 개설된 이모씨의 예금계좌에서 5백92만원을 컴퓨터판매업자의 계좌로 자동이체시켜 자신이 구입한 노트북 2대값을 지불하였고, 이에 앞서 최모씨는 홈뱅킹사기를 시험하기 위해 B은행 박모씨의 계좌에 있던 2백75만원을 C은행 서모씨의 계좌로 이체하는 등 3개은행에 개설된 3명의 계좌를 마음대로 순회이체한 바가 있다고 한다(동아일보 1996.9.25).

② 폰뱅킹사기수법

폰뱅킹의 수법도 홈(펌)뱅킹의 수법과 유사하다. 첫 번째의 폰뱅킹사기수법은 금융기관의 내부인이 고객의 계좌번호와 비밀번호를 알아낸 뒤 이를 이용하여 자신이 가짜로 개설해 놓은 예금통장으로 폰뱅킹을 통해 이체시킨 후 인출하는 방법이다. 보도에 따르

면 K은행 모지점 대리(41세)가 신용카드 할인업자(26세)와 짜고 고객 2명의 예금계좌를 조회하고 이들 명의의 가짜계좌를 K은행의 다른 지점에 개설한 후, 이들 고객 2명의 실제계좌가 개설되어 있던 각 지점에 전화를 걸어 자신들이 개설한 가짜계좌로 각각 9천만원과 2억4천9백4십만원을 이체하도록 한 뒤 이를 찾아간 사건이 있었다(동아일보 1996.4.18, 4.19, 4.23).

두 번째의 수법은 금융기관의 자동응답장치에 도청송신기를 설치하여 도청수신기와 자동판독기를 이용하여 폰뱅킹을 이용하는 고객들의 계좌번호와 비밀번호 등을 알아낸 뒤 이들 고객의 예금계좌에서 자기 또는 제3자의 계좌로 폰뱅킹을 통해 예금을 이체하는 것이다. 이것은 ARS, 극초단파 도청기, 자동판독기를 활용한 범죄로서 첨단범죄의 극치라고 할 수 있는 것으로 이미 우리 나라에서 이 방법을 사용하여 3억1천여만원을 인출한 사건이 발생한 바 있다. 경찰청에 따르면, 은행원 출신 권모씨(34)와 컴퓨터전문가 김모씨(27)는 A은행 폰뱅킹센터 전산실에 자동응답장치(ARS) 교환기 수리업체 직원을 가장해 들어가 손가락 크기의 극초단파 도청송신기를 설치하고 이 은행 건물 옆에 승용차를 세워놓고 도청수신기와 자동판독기를 이용, 폰뱅킹을 이용하는 고객들의 계좌번호와 비밀번호 등을 알아낸 후 위조한 주민등록증으로 A은행에 85개의 계좌를 개설하고 도청을 통해 알아낸 은행고객 박모씨의 계좌에서 폰뱅킹을 통해 자신들이 만든 계좌로 3천2백만원을 이체하는 등 72명의 계좌에서 3억1천여만원을 이체하여 중국 교포를 시켜 현금자동인출기에서 돈을 인출하였다고 한다(동아일보 1998.4.22).

2) 특징

홈(펌)뱅킹사기나 폰뱅킹사기는 고객의 계좌번호와 비밀번호 등을 쉽게 알 수 있는 금융기관의 직원에 의한 범행일 가능성이 높다는 점이 하나의 특징이라고 할 수 있다. 또다른 특징은 컴퓨터통신망에 무단으로 접속하여 자료를 획득할 수 있는 기술을 습득하고 있는 해커 등 제3자가 범죄를 범할 수도 있다는 점이다. 그리고 이러한 홈(펌)뱅킹사기나 폰뱅킹사기 역시 피해자의 신고가 없으면 그 발견이 매우 어렵다는 점도 특징의 하나라고 할 수 있다.

다. 추세전망

홈(펌)뱅킹사기나 폰뱅킹사기사건은 지금까지의 발생건수가 많지는 않은 것같다. 대검찰청 정보범죄대책본부의 통계에 의하면, 1995년 4월부터 1997년 6월 사이에 홈뱅킹

사기사건이 3건 발생한 것으로 나타나 있을 뿐이다. 그러나 홈(펌)뱅킹이나 폰뱅킹의 편리함과 비용절감의 장점에 비추어 이를 이용하는 고객이 급속하게 증가할 것이며[53] 이에 따라 홈(펌)뱅킹사기나 폰뱅킹사기의 사례도 많이 증가할 것으로 판단된다.

라. 대응방안

1) 형사법적 대응방안

① 현행 형벌법규에 의한 대응

i) 적용가능한 구성요건

홈(펌)뱅킹사기나 폰뱅킹사기에 대하여 적용될 수 있는 구성요건은 사전자기록위작·변작죄(형법 제232조의2), 절도죄(형법 제329조) 그리고 컴퓨터사용사기죄(형법 제347조의2)이다.

ii) 사전자기록위작·변작죄

홈뱅킹사기 또는 폰뱅킹사기에 의한 계좌이체나 현금인출은 피해자의 비밀번호 등을 알아내어 이를 악용하는 것인데, 당해 예금계좌에 대하여 비밀번호 등을 입력·사용할 권한이 없는 자가 홈뱅킹사기 또는 폰뱅킹사기를 위하여 이를 입력·사용함으로써 은행의 예금원장파일에 권한없이 변경을 가한 것이므로 이는 사전자기록의 변작행위에 해당하게 된다.

iii) 절도죄와 컴퓨터사용사기죄

홈뱅킹 또는 폰뱅킹은 통상 계좌이체를 하는 것으로서 현금 자체에 대한 사실상의 물적 지배를 획득하는 것은 아니므로 홈뱅킹사기 또는 폰뱅킹사기에 의한 계좌이체만으로는 절도죄의 절취에 해당하지 않는다고 생각된다. 이에 반하여 컴퓨터사용사기죄가 성립하느냐에 대하여는 동죄의 '허위의 정보 또는 부정한 명령의 입력'을 어떻게 해석하느냐에 따라 견해가 대립할 수 있다.

타인 예금계좌의 비밀번호를 알아내서 홈뱅킹사기 또는 폰뱅킹사기를 위해 사용하는 경우 이러한 비밀번호 등은 부정하게 입수한 것일 뿐 허위의 자료는 아니므로 "허위정보의 입력에 의한 재산상 이익의 취득"에는 해당하지 않는다. 그러면 '부정한 명령'인가. 앞서 살펴본 바와 같이 '부정한 명령'을 프로그램의 변경에 한정하거나, 진실한 정

53) 은행감독원에 따르면, 1996년 3월말 현재 1백48만6천명으로 1995년 6월말의 46만6천명 보다 219%가 증가했다고 한다(동아일보 1996.6.14).

보의 권한없는 사용을 '부정한 명령'에 해당하지 않는다고 해석하는 견해에 의하면, 타인 예금계좌의 비밀번호 등을 부정하게 알아낸 행위만이 문제될 뿐 획득한 비밀번호를 사용하여 홈뱅킹 또는 폰뱅킹에 의해 계좌이체한 행위는 컴퓨터사용사기죄의 구성요건 해당성이 부인될 것이다. 그러나 사견으로는 진실한 정보의 권한없는 사용도 컴퓨터사용사기죄의 '부정한 명령의 입력'에 해당한다고 보기 때문에 홈뱅킹사기 또는 폰뱅킹사기는 동죄를 구성한다고 본다.

그리고 홈뱅킹사기 또는 폰뱅킹사기에 의하여 피해자의 계좌로부터 자신이나 제3자의 계좌로 이체한 단계에서 발각되어 현금을 인출하지 못하였다고 하더라도 컴퓨터사용사기죄는 기수에 이른 것이다. 왜냐하면 피해자의 계좌로부터 일정한 금액을 자신이나 제3자의 계좌로 이체함으로써 당해 금액을 인출하여 사실상 처분할 수 있는 지위를 얻은 것이므로 이는 이미 재산상의 이익을 취득하였다고 보아야 하기 때문이다. 홈뱅킹사기 또는 폰뱅킹사기에 의한 계좌이체후 현금을 인출한 경우에 절도죄의 성부가 문제될 수 있으나 계좌이체후의 현금인출은 절도죄의 절취에 해당할 수 없다고 생각하지만 설령 절도죄의 구성요건해당성을 긍정한다고 하여도 계좌이체에 의하여 성립한 컴퓨터사용사기죄의 불가벌적 사후행위라고 보아야 할 것이다.

iv) 비밀침해죄와 전산망비밀침해죄

나아가 홈뱅킹사기의 경우 행위자가 컴퓨터통신망을 통하여 이용고객의 계좌번호와 비밀번호 등을 알아냈다면, 추가적으로 기술적 수단에 의한 비밀침해죄(형법 제316조 2항)와 전산망비밀침해죄(전산망법 제30조, 제25조 1항)가 성립하게 될 것이다. 이에 반하여 폰뱅킹사기의 경우 행위자가 도청장치와 자동판독기 등을 활용하여 계좌번호와 비밀번호 등을 알아냈다면 이는 기술적 수단에 의한 비밀침해죄는 성립할 수 있어도 전산망비밀침해죄는 성립할 수 없다고 본다.

② 처벌법규의 신설 내지 보완

전자기록위작·변작죄와 컴퓨터사용사기죄에 대하여는 해석의 다툼을 없애기 위하여 컴퓨터범죄에서 살펴본 바와 같이 보완하여야 할 것이다. 즉 사전자기록위작변작죄의 '위작·변작'을 "권한없이 작성하거나 변경하는" 행위로 변경하고, 컴퓨터사용사기죄의 행위객체에 "재물"을 추가하고 행위태양으로 "진실한 정보를 권한없이 사용하는" 것도 추가하여야 한다.

2) 경찰제도적 대응방안

① 전문수사조직의 설치·운영

홈(펌)뱅킹사기나 폰뱅킹사기도 컴퓨터통신이나 유선전화통신 등의 정보통신기술을 악용하여 범하는 전문적인 수법의 범죄라는 점에서 컴퓨터범죄와 유사하다. 따라서 이러한 범죄를 효과적으로 발견하고 수사함으로써 이에 적절하게 대처하려면 정보통신기술에 정통한 수사관으로 구성된 조직이 필요하게 될 것이다. 즉 컴퓨터범죄수사대와 마찬가지로 이들 범죄만을 전담하여 수사하는 기능과 능력을 가진 전문화된 수사조직을 설치·운영하여야 한다.

② 피해자의 요청시 비밀수사

홈(펌)뱅킹이나 폰뱅킹은 이미 새로운 금융제도로서 정착되어 있으며 이 제도를 운영하는 금융기관은 물론 이를 이용하는 기업이나 개인도 많은 편리함과 경제적 이익을 얻고 있다. 그리하여 각 금융기관은 보다 많은 고객을 확보하기 위하여 이 제도를 안전하게 운영하려고 많은 노력을 기울이고 있으며, 이 제도의 성패는 바로 안전성에 달려있다. 따라서 제도운영자인 금융기관들은 홈(펌)뱅킹이나 폰뱅킹의 안전성에 결정적으로 의문이 제기될 수 있는 홈(펌)뱅킹사기나 폰뱅킹사기의 사실이 알려지는 것을 극도로 꺼리고 있다. 즉 이용자들인 고객에 대하여 피해자의 이미지실추를 염려하여 범죄피해신고를 기피하려는 경향이 있다. 이 점을 고려하여 피해자의 요청이 있으면 피해사실을 비밀로 하고 수사하는 방안도 수립하여 시행할 필요가 있다고 본다.

3) 사회적 대응방안

① 범죄피해 신고의무의 부과

새로운 형태의 범죄에 대하여 효과적으로 대처하려면 그것의 실상—범행방법과 발생현황—에 대한 정확한 이해가 전제되어야 하므로 이를 위하여 범죄사실의 신고의무를 부과하는 방안을 생각할 수 있다. 물론 홈뱅킹사기나 폰뱅킹사기의 대상이 된 금융기관들은 고객에 대한 신뢰문제를 이유로 피해사실을 은폐하려는 경향이 있으나 이는 또다른 범죄를 유발할 수 있다는 점을 명심하여 적어도 금융감독원 등 감독기관에 신고할 의무를 부과하여야 할 것이다.

② 내부통제장치와 기술적 보안대책의 강구

홈뱅킹사기나 폰뱅킹사기는 금융기관 내부인이나 해커 등 외부인에 의하여 범하여지므로 이들의 범행을 방지할 수 있는 제도적·기술적 노력이 있어야 할 것이다. 예컨대 내부인에 의한 범행을 예방하기 위하여는 비밀번호 등이 기재된 예금원장에 대하여는

반드시 2인 이상이 함께 열람하도록 하는 등 고객의 비밀번호에 대한 관리를 엄격하게 하고 이에 대한 감독체계를 강화하여야 할 것이다. 나아가 해커 등 외부인에 의한 범행을 예방하려면 컴퓨터통신이나 유선전화의 보안체계를 확고하게 하여 외부로부터의 무단접속을 봉쇄할 수 있는 기술적 장치를 마련하려는 노력을 계속하여야 할 것이다.

3. 신용카드범죄

가. 의의와 유형

오늘날 거래방법의 다양화와 함께 신용거래의 한 수단으로 등장한 것이 신용카드제도이다.[54] 1980년대부터 은행의 부수업무형태로 출발한 우리나라의 신용카드산업은 짧은 기간에도 불구하고 급성장을 거듭하고 있고 거래에 있어서 각종 편의를 제공하는 등 여러가지 순기능을 하고 있다. 한국신용카드업협회의 발표에 따르면 1996년말 협회 소속 8개 신용카드회사의 카드발급건수는 모두 4천 25만 7천개로 한 해전보다 23.7% 증가하였고, 이용실적도 61조 3천 1백 97억원으로서 국내이용실적이 60조 1백 86억원, 해외이용실적이 1조 3천 11억원에 달하였다고 한다.[55] 또한 1997년에는 총매출액이 73조 1천 7백 80억원으로 전년보다 16.1%, 신규카드 발급건수는 11.4% 각각 증가하여[56] 이른바 '국민 1인당 1카드시대'를 열고 있다.

그러나 이러한 신용카드산업의 양적 성장에 못지 않게 카드업계의 무리한 경쟁에 따른 미성년자나 무자격자에 대한 카드발급으로 매년 카드대금의 연체액수도 늘고 있고[57] 또한 신용카드제도를 악용한 여러 형태의 범죄들도 발생하고 있는데, 예를 들면 신용카드를 부정발급받은 후 부정사용하는 경우라든지, 도난·분실된 타인명의의 신용카드의 부정사용, 신용카드 및 매출전표의 위조·변조, 통신판매를 이용한 사기행위 등 종래에

54) 신용카드란 여신전문금융업법에서 정의한 바에 의하면, 「이를 제시함으로써 반복하여 신용카드가맹점에서 물품의 구입 또는 용역의 제공을 받을 수 있는 증표로서 동법 제3조 제1항의 규정에 의하여 신용카드업의 허가를 받은 자가 발행한 것」을 말한다(여신전문금융업법 제2조 3호).

55) 한겨레신문 1997년 5월 6일자 참조.

56) 서울신문 1998년 2월 21일자 참조.

57) 1997년 한 해동안 우리나라의 신용카드회사들이 떠안고 있는 연체액은 무려 6천 6백억원에 달한다고 한다(서울신문 1998년 2월 21일자 참조)

는 생각하지 못했던 새로운 형태의 범죄들도 빈발하고 있다. 이들 범죄들은 모두 신용카드를 행위의 수단 또는 목적으로 하는 범죄로서 사기, 사문서 위·변조 등 일반 형사법에 따른 범죄로도 볼 수 있지만, 새로운 범죄현상에 대한 적극적인 대응책을 마련한다는 의미에서 일반적으로 이를 포괄하여 신용카드범죄라고 한다. 즉 신용카드범죄란 일률적으로 정의할 수는 없지만 일반적으로 신용카드를 수단으로 하거나 신용카드제도를 악용하여 범하는 모든 범죄적 현상이라고 정의할 수 있다.[58] 신용카드범죄는 신용카드시스템을 악용하는 전문적이고 지능적인 범죄로서 컴퓨터범죄와 함께 앞으로도 계속 확대될 전망인 신용사회와 정보화사회의 큰 장애요인이 되리라고 보여지므로 이에 대한 적극적인 대책마련이 요구된다.

신용카드범죄의 유형을 분류하는 방법은 관점에 따라 매우 다양하여서, 현행 여신전문금융업법 제70조에 의하여 처벌되는 행위를 중심으로 분류할 수도 있고, 범죄행위자를 기준으로 분류할 수도 있다. 여기서는 신용카드범죄에 대한 형사법적 대응필요성을 모색한다는 의미에서 신용카드의 부정취득, 신용카드의 부정사용, 신용카드의 부정처분, 가맹점에 의한 범죄로 분류하기로 한다.[59]

나. 수법과 특징

1) 수법

① 신용카드의 부정취득

신용카드의 부정취득은 보통 신용카드의 부정사용을 위한 수단으로 행하여지는 것으로 여기에는 진정한 신용카드를 부정취득한 경우와 신용카드를 위조한 경우를 들 수 있다. 그리고 진정한 신용카드를 부정취득한 경우는 자기명의의 카드를 부정취득한 경우와 타인명의의 카드를 부정취득한 경우로 분류할 수 있다.

ⅰ) 자기명의의 카드를 부정취득하는 경우

이는 신용카드입회 자격기준에 미달하는 자가 입회신청서에 허위사실을 기입하거나 다른 회사의 재직증명서를 위조하는 등 허위정보를 제공하여 신용카드회사로부터 부정하게 신용카드를 발급받음으로써 입회시 카드사용대금을 지불할 의사와 능력이 있는

58) 강동범, 신용카드범죄의 실태와 형법적 대응, 형사정책연구, 1995 여름, 117면; 오경식, 신용카드범죄의 실태와 법적 문제점, 한국형사정책연구원보고서, 1995. 3, 37면 참조.

59) 이에 관하여는 강동범, 전게논문, 118면 참조.

것처럼 가장하여 신용카드회사를 기망한 경우이다.[60] 예전에는 개인이 첨부서류를 위조하여 부정발급받는 경우가 많았으나 최근에는 카드부정발급 전문대행업체들을 통하여 조직적으로 부정발급을 받는 사례가 급증하고 있다. 특히 IMF경제체제로 실직자와 신용불량자들이 대량으로 양산되어 신용카드의 신규발급이 어려워지자 이들 유령 대행업체들을 통하여 신용카드를 부정발급받는 사례가 급증하고 있는데, 이들 대행업체들은 주로 지역생활정보지를 통하여 '카드발급'이라는 광고를 게재한 뒤 이를 보고 찾아 온 신용불량자 및 카드발급부적격자들에게 첨부서류 및 재직확인서 등을 허위로 작성하여 카드를 부정발급받는 것으로 알려지고 있다.[61]

이 이외에도 자기명의의 카드를 부정취득하는 경우에 포함시킬 수 있는 것은 신용카드약관에 따라 분실·도난신고 접수시점으로부터 15일전 이후에 발생한 제3자의 카드 부정사용금액에 대하여는 카드회사가 그 손실을 부담한다는 점을 이용하여 허위로 카드분실신고를 하고 카드를 재발급받는 경우를 생각할 수 있다.

ii) 타인명의의 카드를 부정취득하는 경우

여기에는 여러 유형이 있을 수 있는데 그 수법을 보면 대체로 다음과 같다. 첫째는 타인명의의 신용카드를 부정발급받아 사용하는 수법이다. 이는 타인의 주민등록증 등을 위조하여 신용카드입회신청서를 허위로 작성, 제출하고 타인명의의 신용카드를 발급받아 사용하는 경우이다. 즉 신용카드가맹점을 신청하면 서류검토만으로 허가가 난다는 점을 악용하여 유령회사를 설립한 후 신용카드회사로부터 가맹점허가를 얻고 타인을 회사의 직원인 양 위장하여 신용카드회사로부터 타인명의로 신용카드를 부정발급받아 매출전표를 허위작성하고 해당은행에 접수시키는 방법으로 현금을 편취하는 경우가 여기에 해당한다.

둘째는 타인명의의 신용카드를 절취하거나 분실된 타인명의의 신용카드를 습득하여 사용하는 수법이다. 신용카드를 절취함에 있어서는 카드회원이 장기간 카드도난사실을 알지 못하게 하기 위하여 정상적인 카드를 빼내고 거래정지된 카드로 바꿔치기 하는

60) 이 경우 범인은 재직확인을 할 것에 대비하여 범인이 직접 개설한 전화로 재직확인에 응하고 외출시에는 수화기를 내려 놓아 통화 중 상태로 만들어 놓음으로써 통화량이 많은 회사인 것처럼 위장하는 수법을 사용하기도 한다.

61) 카드업계에 따르면 부정발급으로 분류되거나 사전적발된 건수는 1998년 상반기에만 무려 1천 5백 여건에 달해 1997년에 비해 2배 이상 늘어난 것으로 나타났다(문화일보 1998년 9월 17일자 참조).

수법도 발생하고 있다. 한편 타인의 우편함에 배달된 신규카드를 절취하거나 잘못 배달된 타인의 신규카드를 습득하여 회원서명란에 서명한 후 부정사용하는 경우는 미완성의 카드를 완성하여 사용하는 것이므로 후술하는 신용카드를 위조하여 취득한 경우로 보아야 할 것이다.

셋째는 타인명의의 카드를 강취, 사취, 갈취, 횡령하여 부정사용하는 수법이다. 이것은 여신전문금융업법 제70조 제1항 제3호가 '분실 또는 도난된' 타인명의의 신용카드 부정사용행위만을 처벌하고 있기 때문에 강취, 사취, 갈취, 횡령 등의 수법으로 타인명의의 카드를 부정취득하여 사용한 경우에는 동법의 적용에 있어서 해석상의 문제가 발생한다는 점에서 위의 두 번째 수법과 분리해 본 것이다. 즉 여신전문금융업법 제70조 제1항 제3호의 '도난'이라는 개념을 '절취'만을 의미하는 것으로 제한해석해야 할 것인지 아니면 '강취'한 경우도 포함하는 것으로 해석해야 할 것인지에 대하여 의문이 있을 수 있고[62], 그 이외의 '사취, 갈취, 횡령'의 경우에는 동법의 적용이 어렵다는 점에서 입법론을 고려하여 분리해서 논할 필요가 있다고 하겠다. 사취의 방법으로는 은행직원 및 카드회사직원을 사칭한 범인들이 회원을 방문하여 새로 발급된 카드로 교체해 주겠다거나 카드뒷면의 자기테이프가 잘못되어 비밀번호에 오류가 생겨 새 카드로 교체해 주겠다면서 비밀번호를 파악하고 카드를 회수한 후 부정사용하거나, 카드모집인을 사칭하여 이미 신용카드를 소지하고 있는 회원에게 특별카드로 등급변경을 해주겠다고 속인 후 카드를 반납받아 부정사용하는 수법을 들 수 있다. 또한 최근에는 신용카드사의 전화자동응답시스템을 이용하여 다른 사람의 명의로 신용카드 분실신고를 한 뒤 카드를 재발급받아 부정사용하는 수법도 발생하고 있다.[63]

iii) 신용카드를 위조하여 취득한 경우

신용카드위조범죄는 현재 우리나라에 있어서 다른 신용카드범죄수법에 비해 많이 발생하는 편은 아니나 점차 위조기술이 진보하고 있고 그 피해규모가 매우 크다는 점에서 주목해야 할 범죄이다. 신용카드위조의 수법으로는 신용카드 뒷면의 자기테이프속에

62) 이에 대하여 장용석, 신용카드 이용범죄의 유형과 처리, 법조, 1992. 4, 85면; 임양운, 신용카드범죄의 실무상 문제, 저스티스 제29권 제3호, 1996. 12, 184면은 '도난'개념의 문리해석상 '절도'뿐만 아니라 '강취'까지도 포함하는 것으로 해석하는 것이 타당하다고 한다. 한편 판례도 '강취'한 타인의 카드를 부정사용한 경우에 여신전문금융업법상의 부정사용죄를 적용하고 있다(대판 1997. 1. 21, 96 도 2715; 대판 1998. 2. 27, 97 도 2974).

63) 서울신문 1998년 5월 25일자 참조.

다른 사람의 정보를 입력시켜 사용하는 수법, 타인의 개인정보를 습득한 뒤 공카드를 이용하여 진짜와 똑같은 신용카드를 교묘하게 위조하는 수법 등이 있다. 전자의 경우는 신용카드가맹점에서 신용카드조회단말기(CAT)로 카드를 조회할 때 신용카드의 앞 면에 인쇄되어 있는 카드번호를 보고 입력하여 확인해 보면 자기테이프판독에 의하여 정상적으로 발급받은 카드로 아무 이상이 없는 것으로 나타나지만, 신용카드 뒷면의 자기테이프속에 입력된 타인의 카드번호, 비밀번호, 유효기간 등의 정보는 단말기에 자동으로 입력되어 카드뒷면의 자기테이프상의 회원에게 대금결제가 청구되는 것을 이용한 수법이다. 이 외에도 우송 중에 분실된 타인의 신규 내지 갱신카드를 습득하여 회원서명란에 서명한 후 사용하거나, 유효기간이 경과하여 버려진 타인의 신용카드를 습득하여 그 유효기간을 연장·개작하여 사용하는 행위도 여기에 해당한다.

지금까지 우리나라에서 발생한 신용카드의 위조는 신용카드 뒷면의 자기테이프속에 다른 사람의 정보를 입력시켜 사용하는 수법에 불과했으나, 최근에는 개인정보를 통째로 빼내 외국의 범죄조직과 결탁하여 복제하는 사례도 발생하고 있다. 예를 들면 신용카드업체 및 신용카드배송업체에 위장취업해 배달과정에서 신용카드를 빼돌려 개인정보를 알아낸 뒤 이 중 비자나 마스터카드 등 외국에서 사용가능한 카드를 복제하여 해외에서 현금인출한 사례라든지, 신용카드조회업체 직원을 매수해 고객의 신용정보를 한꺼번에 입수한 뒤 이를 일본으로 가져가 위조신용카드를 대량으로 만들어 사용한 사례[64] 그리고 카드대출사무소를 차려 놓고 대출을 받으러 온 사람의 카드비밀번호 등을 암호해독기를 통해 알아낸 뒤 이를 외국(홍콩)의 위조조직에 보내 현지에서 카드를 복제하여 해외한도까지 현금을 인출한 사례들이 최근에 자주 발생하고 있다. 신용카드는 해외에서 사용할 경우 카드 1개로 2만달러까지 현금서비스를 받을 수 있을 뿐만 아니라 물건구매까지 가능하므로 그 피해규모가 매우 크다고 할 수 있다. 따라서 신용카드회원의 개인정보에 대한 보안의 문제가 신용카드위조의 방지를 위하여 중요한 문제로 대두되게 되었다. 이제 멀지 않아 직접 국내에서 카드를 대량 복제하여 부정사용하는 사례도 빈발할 것으로 보여지므로 시급히 이에 대한 대책을 마련할 것이 요청된다.

② 신용카드의 부정사용

신용카드의 부정사용과 관련된 범죄는 신용카드범죄의 대부분을 차지하는 것으로서 신용카드의 부정취득도 궁극적으로는 신용카드의 부정사용을 위하여 행해지는 것이라

64) 경향신문 1997년 10월 24일자 참조.

고 할 수 있다. 따라서 두 행위는 보통 연결된 형태로 나타난다. 부정사용의 형태는 카드가맹점에서 물품을 구입하거나 용역을 제공받는 경우뿐만 아니라 현금자동지급기나 현금자동입출금기에서 예금을 인출하거나 현금서비스를 받는 경우를 모두 포함한다. 이러한 신용카드의 부정사용은 자기카드의 부정사용과 타인카드의 부정사용으로 나누어 볼 수 있다.

자기카드의 부정사용은 유효하게 신용카드를 발급받은 회원이 대금을 지급할 의사나 능력이 없음에도 불구하고 있는 것처럼 가장하고 신용카드를 사용하여 물품을 구입하는 경우이며, 타인카드의 부정사용은 위조, 변조, 도난, 분실된 타인의 카드를 마치 자신이 카드의 명의인인 양 가장하고 카드를 사용하는 경우이다. 도난·분실된 카드를 사용함에 있어서 범인은 도난·분실신고로 거래정지된 카드를 회원의 주민등록증을 위·변조한 다음 거래정지해제후에 부정사용하는 행위도 간혹 발생하기도 한다.

한편 통신판매의 경우 신용카드의 제시없이 전화상으로 신용카드번호만 제시하면 물품의 구매 등 신용거래가 가능하다는 점을 악용하여 타인의 신용카드번호를 몰래 알아내어 제시함으로써 타인명의의 카드로 결제가 이루어지도록 하는 행위들도 발생하고 있는데, 이러한 행위도 비록 신용카드를 사용하지 않지만 신용카드의 부정사용의 유형에 포함시킬 수 있을 것이다.[65]

③ 신용카드의 부정처분

신용카드의 소유권은 신용카드발행회사에 있고 카드회원은 그 대여를 받아 사용할 권한을 갖고 있음에 불과하다. 따라서 신용카드회원은 선량한 관리자의 주의로 관리하여야 하며 카드를 양도하거나 질권설정 등 불법처분을 하여서는 안된다. 여신전문금융업법 제15조는 신용카드의 양도, 양수 및 질권설정행위를 금지하고 있고, 이에 위반한 경우 동법 제70조 제3항에 의하여 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하고 있다. 그러나 이러한 유형의 범죄는 실제 많이 발생하고 있지는 않은 것으로 보인다.

④ 가맹점에 의한 범죄

65) 특히 인터넷을 통한 전자상거래가 확산되면서 인터넷을 통해 물건을 구매한 고객들의 신용카드번호와 비밀번호가 전문해커들에게 노출되어 피해사례가 빈발하고 있다. 현재 국내 대부분의 카드회사는 그 피해를 개인에게 부담시키고 있어 전자상거래를 할 경우 해킹위험은 전적으로 개인이 부담해야 하는 상황이다.

가맹점에 의한 신용카드범죄는 주로 매출전표와 관련된 범죄가 주종을 이루는데 그 유형을 보면 대체로 다음과 같다.

ⅰ) 신용카드이용 현금대출행위

이는 사채업자가 불량가맹점을 개설하거나 다른 가맹점의 명의를 대여받은 뒤 급전이 필요한 고객의 신용카드를 이용, 물품을 판매한 것처럼 가장하여 허위매출전표를 작성하고 높은 선이자(16-18%)를 공제한 후 자금을 융통하여 주거나 이를 중개, 알선하는 행위이다. 최근에는 사채업자가 국내 이용한도를 초과하였거나 연체 중인 카드를 대납한 후 신용카드와 비밀번호를 넘겨받고 해외로 출국하여 해외의 ATM기에서 현금서비스를 받거나, 해외가맹점과 짜고 물품을 구매한 것처럼 허위매출전표를 작성하는 형태의 불법대출이 나타나고 있다. 한편 이 과정에서 신용카드회원 몰래 매출전표를 추가로 작성하여 돈을 인출한 뒤 도주하거나, 회원의 비밀번호 등을 알아낸 뒤 카드를 위조하여 시중에 유통시키기도 한다. 이와 같은 위장거래에 의한 현금대출은 실제 많이 발생하고 있는 범죄행위임에도 불구하고 대출업자들이 점조직으로 구성되어 쉽게 노출되고 있지 않으며, 가맹점에 대한 관리도 미비한 실정이어서 적발되는 숫자가 많지 않은 편이다.

ⅱ) 매출전표의 할인 및 유통행위

이는 자격요건 미달업소가 본인명의 또는 타인명의를 이용하여 가맹점가입신청서를 허위로 작성하거나 사업자등록증 등을 위조하여 허위 가맹점을 개설한 후 다른 가맹점에 매출전표를 교부해 주었다가 다시 할인매입하거나 또는 다른 가맹점에서 작성된 매출전표를 할인해주고 고율의 선이자를 받아 부당이득을 취하는 수법을 말한다. 이와 같은 수법은 무허가 주류판매업소나 유흥업소들 중 매출규모를 축소하여 세금납부를 회피하거나 신속한 자금회전을 위해 신용카드 매출전표를 할인하려는 업소들이 많은 점을 이용하여 범행이 이루어지고 있다.

ⅲ) 위조매출전표작성행위

이는 가맹점 보관용 매출전표를 구입하여 동 전표를 견본으로 플라스틱 등을 이용 카드 양각부분을 엠보싱기로 위조하여 행사할 목적으로 위조 매출전표를 작성한 후 신용카드회사에 대금을 청구하거나 매출전표 유통업자에게 유통시켜 할인하는 수법이다. 이러한 수법은 매출전표의 교부 및 가맹점 보관용 매출전표의 관리가 허술할 뿐만 아니라 신용카드의 양각부분의 위조가 용이하다는 점을 악용한 것이다. 최근에는 카드가 없는 상태에서 카드번호와 유효기간의 숫자만으로 신용카드의 비밀암호체계를 해독한

뒤 허위로 매출전표를 작성, 은행에서 거액을 빼낸 신종카드사기단이 적발되기도 하였다.[66]

iv) 이중매출전표작성 내지 매출전표 금액변조행위

이는 유흥업소 종업원들이 취중의 회원이 카드를 사용할 때 매출전표를 추가작성한 후 서명을 임의로 기재하여 매출전표를 위조하거나 매출전표의 금액을 변조하여 유통시키는 수법이다.

v) 가맹점수수료의 회원전가행위

여신전문금융업법 제70조 제3항 제2호에 의하면 신용카드 가맹점이 물품을 판매한 후 카드회사에 지불하는 가맹점수수료를 신용카드회원에게 부담케 하는 행위를 처벌하고 있으므로 가맹점의 수수료 전가행위도 가맹점에 의한 범죄의 한 유형에 해당한다. 이러한 유형의 범죄는 판매금액에 수수료율을 포함하여 판매하는 행위로서 주로 고객이 신분노출을 꺼리는 업소에서 성행하고 있다.

2) 특징

신용카드범죄는 첫째 범행이 단기간에 집중적으로 반복하여 발생된다는 특징을 가지고 있다. 즉 1992년 10월부터 전거래 사전승인제도의 실시로 모든 신용카드거래는 금액과 상관없이 신용카드회사의 사전승인을 받도록 되어 있기 때문에 일단 신고만 접수되면 부정사용은 불가능하다. 따라서 타인명의의 신용카드를 부정취득한 자가 부정사용하는 경우 신용카드회원이 신용카드회사에 사고통지를 하거나 신용카드회사로부터 가맹점에 통보하기 전의 짧은 기간을 이용하여 범행을 집중 반복하며, 최장 57일간의 지불유예기간을 이용하려고 하기 때문에 동일한 신용카드를 이용한 경우에는 범행이 단기간에 집중적으로 발생하고 있다. 더구나 자기명의의 신용카드를 부정사용하는 경우에는 누구의 의심도 받는 일없이 범행을 반복하여 행할 수 있을 것이다.

둘째 신용카드범죄는 신용카드의 전문적인 지식을 악용하여 범해지는 지능적이고 전

66) 예를 들면 윤모씨(35)는 장은신용카드를 소유하고 있는 김모씨(41)의 신용카드번호와 유효기간을 알아낸 뒤 이들 숫자로 조합된 카드뒷면 마그네틱부분의 암호체계를 해독해 냈다. 이어 윤씨는 승인조회기(이지체크기)를 조작, 김씨가 부산의류점에서 68만원 상당의 의류 1점을 구입한 것처럼 가짜 매출전표를 작성해 박모씨(27)에게 일당 15만원씩 주고 외환은행 부산 남천동지점에서 구매대금을 받아내게 하였다. 경찰조사결과 이들은 유령 카드 가맹점을 만들어 국내 10여개 카드회사 고객 71명의 명의로 매출전표를 허위로 작성해 은행에서 4천5백만원을 빼낸 것으로 드러났다.(경향신문 1995년 8월 20일자 참조)

문적인 범죄로서 조직적으로 범행이 이루어지는 특징을 보이고 있다. 특히 신용카드 위조의 경우 고도의 컴퓨터조작능력과 모조기술이 필요하며, 단독으로 범행을 하기 보다는 역할을 분담한 다수의 사람들이 집단적으로 범행에 관여하고 있다. 또한 카드회사직원과 공모하여 범행을 하는 경우도 발생하고 있어서 더욱 범죄가 교묘화되고 있으며, 최근 신용카드범죄에서 파생되는 막대한 금전적 이익을 노리고 국내외의 조직범죄집단이 이에 개입하고 있는 것으로 밝혀져 더욱 심각한 문제로 되고 있다. 그리고 신용카드 현금대출범죄의 경우에도 현금대출업자들이 점조직으로 구성되어 있어서 쉽게 노출되지 않고 있어 적발이 쉽지 않은 실정이다.

셋째 현재 발생하고 있는 신용카드범죄의 경향을 보면 범행이 전국적으로 광범위하게 행하여지는 특징을 가지고 있는데, 이는 범행의 방법이 비교적 간단하여 기동성을 가지고 있다는데 기인하는 것으로 보인다. 그러나 범행지역이 광범위하다고는 하지만 대체로 서울, 경기 등 수도권지역에서의 범죄가 대부분이고, 사고가맹점도 유흥음식점이 반수를 차지하는 특징도 보이고 있다. 또한 대부분의 신용카드가 비자카드 또는 마스터카드 등 외국의 카드회사들과 제휴되어 외국에서의 사용이 자유로워짐에 따라 신용카드범죄가 국경을 초월하여 국제화되고 있는 실정이다.

다. 추세전망

신용카드의 보급이 확대되면서 카드의 위·변조, 부정발급, 도난카드사용 등 관련범죄가 매년 증가하고 있다. 경찰청에 따르면 신용카드 관련범죄는 지난 94년에 1천 1백 87건에서 95년에 1천 4백 27건, 96년에 1천 8백 24건, 97년에 2천 38건으로 매년 12-28%씩 증가하고 있어서 최근 4년 사이 72%나 증가한 것으로 나타났다.[67] 이같은 증가율은 매년 10% 미만인 전체 범죄증가율을 훨씬 넘는 것으로 신용카드범죄는 이제 더 이상 방치해서는 안될 중요한 범죄유형으로 자리잡고 있다고 할 수 있다. 그러나 우리나라에서는 수법별 범죄상황에 대한 공식적인 통계가 아직 없어서 정확한 범죄추이를 파악하기는 어려운 실정이다. 따라서 1994년의 일본에서 검거된 신용카드범죄의 유형별 상황을 살펴 봄으로써 어느 정도 그 발생추이를 가늠해보고자 한다.

위 표에서 보듯이 일본의 경우 1994년에 검거한 신용카드범죄의 유형 중 절취카드사용이 33.4%로 가장 많고, 다음으로 습득카드사용이 30.0%, 타인명의카드 부정취득사용

67) 세계일보 1998년 4월 13일자 참조

이 13.1%, 자기명의카드사용이 8.2%, 편취카드사용이 1.6%, 갈취카드사용이 1.0%, 위조카드사용이 0.3%의 순으로 나타나 있다. 따라서 일본의 경우 도난, 분실된 타인명의 카드를 취득하여 부정사용하는 경우가 반수 이상을 차지하고 있고 위조카드사용은 0.3%에 불과한 것으로 나타나 있는데 우리나라의 경우에도 상황이 비슷하리라고 보여진다. 그러나 최근 외국과의 왕래가 빈번해지면서 외국의 범죄조직과 결탁해 카드를 위조하는 사례들이 발생하고 있고 멀지않아 위조기술이 국내에 유입될 가능성도 있는 등 그 수법에 있어서 과거 남의 카드를 훔치거나 주워 사용하는 단순한 범죄에서 신분증을 위조해 카드를 발급받거나 카드암호해독용 기계와 프로그램 등을 활용한 카드의 위·변조행위 등 지능형 범죄로 발전하고 있다는 점에서 조금 더 적극적인 대응책을 마련할 필요가 있다고 하겠다.

〈표 4〉 일본에 있어서 신용카드범죄의 유형별 상황(1994년)[68]

범 죄 유 형	검 거 건 수	비 율(%)
자기명의 카드사용	572	8.2
절 취 카 드 사 용	2,335	33.4
습 득 카 드 사 용	2,102	30.0
갈 취 카 드 사 용	70	1.0
타인명의카드 부정취득사용	914	13.1
편 취 카 드 사 용	115	1.6
위 조 카 드 사 용	21	0.3
기 타	869	12.4
합 계	6,998	(100)

라. 대응방안

1) 형사법적 대응방안

① 현행 형벌법규에 의한 대응

i) 신용카드의 부정취득과 관련된 범죄

먼저 자기명의의 신용카드를 부정취득한 경우로서 신용카드발급신청자가 신용카드대금을 지불할 의사나 능력이 없으면서도 있는 것처럼 가장하여 자기명의의 신용카드를

68) 警察白書(平成 7년판), 동경 : 대장성인쇄국, 1995

신용카드회사로부터 발급받는 행위가 사기죄를 구성하는가가 문제된다. 즉 실제에 있어서는 신용카드의 사용단계에서의 사기죄의 성립 여부가 문제되겠지만, 신용카드를 사용하기 이전인 취득단계에서 과연 사기죄의 성립을 인정할 수 있을 것인가이다. 이에 대하여는 긍정설[69]과 부정설[70]이 존재한다. 긍정설은 신용카드 자체가 이미 형법상의 재물에 해당하므로[71] 대금결제의 능력과 의사가 없음에도 불구하고 그것이 있는 것처럼 신용카드회사를 기망하여 신용카드를 발급받은 경우에는 신용카드라는 재물 자체를 취득한 것임과 동시에 신용카드회사에 대하여 재산상의 손해발생의 위험을 발생시키는 것으로서 사기죄가 성립한다고 본다. 이에 반해 부정설은 신용카드회사가 신용을 제공받을만한 재산상태나 거래실적을 갖추고 있지 못한 사람들에게까지 신용카드를 무분별하게 발급하고 있는 현실을 고려할 때 신용불량회원의 카드부정사용으로 인한 재산상의 손해는 카드회사의 위험부담으로 돌릴 필요가 있다는 전제에서 사기죄의 성립을 부정한다. 즉 신용카드 그 자체는 단지 미미한 경제적 가치를 지닌 물질에 불과하기 때문에 신용카드를 취득하는 행위만으로는 형사처벌이 필요한 불법 내지 범죄유형성을 갖지 못한다고 본다. 또한 신용카드를 아직 사용하지 않은 단계에서는 신용카드회사의 전체 재산에 대하여 직접적인 손해가 발생한 것도 아니고 손해발생의 구체적 위험도 있다고 할 수 없으며 그러한 위험은 단지 추상적인 위험에 불과하다고 보아 카드의 취득 자체만으로는 재산상의 손해의 요건을 충족하지 못하므로 사기죄의 죄책을 지우는 것은 무리라고 본다. 한편 판례는 변제의사와 능력이 없음에도 불구하고 결제할 것처럼 가장하여 신용카드를 발급받은 행위 자체를 사기죄로 보고, 그 이후에 그 신용카드로 물품을 구입하거나 현금자동지급기에서 현금을 인출하는 행위 모두 카드회사의 기망당한 의사표시에 따른 카드발급에 터잡아 이루어지는 사기의 포괄일죄로 보고 있다.[72] 생각건대 신용카드는 단순히 플라스틱조각인 것을 넘어 소지인이 신용카드회원임을 증명하는 기능을 함과 동시에 이를 이용하여 여러 가지 유용한 서비스를 받을 수 있도록 하고 있어 현금 이상의 경제적 효용을 가지고 있다는 점을 고려할 때 단지 미미한 경제적 가

69) 강동범, 자기신용카드의 부정사용행위에 대한 형사책임, 고시계, 1997.12, 46면; 박상기, 형법각론, 박영사, 1997, 340면; 배종대, 형법각론, 홍문사, 1996, 335면; 장영민, 자기명의의 신용카드남용행위의 죄책, 법학논집 제2권 제1호, 이화여자대학교 법학연구소, 1997, 83면.

70) 오경식, 전게논문, 72면; 이상돈, 자기신용카드의 부정발급사용, 고시계, 1998. 11, 111-112면.

71) 형법상 재물이란 반드시 객관적으로 경제적, 금전적 교환가치가 있는 것만이 재물이 되는 것이 아니라 주관적 가치가 있는 것도 소유권의 목적이 될 수 있는 한 재물에 포함된다.

치를 지닌 물질에 불과한 것으로 보기는 어려울 것으로 보인다. 이는 진정하게 발행된 타인의 신용카드를 절취, 강취, 사취, 갈취한 경우 각각 절도죄, 강도죄, 사기죄, 공갈죄의 성립을 인정하고 있는 것을 보아도 알 수 있다. 따라서 재직증명서를 위조하는 등 적극적으로 카드회사를 기망하여 부정하게 신용카드를 발급받은 경우 사기죄의 성립을 인정해야 할 것으로 본다.

다음으로 타인명의의 신용카드를 부정취득한 경우로서 먼저 제3자의 이름을 도용하여 입회신청서를 작성하고 타인명의의 신용카드를 발급받으면 발급신청서 등의 작성과 관련하여 사문서위조 및 동행사죄가 성립하고 신용카드의 발급과 관련하여 사기죄가 성립한다. 한편 앞에서 기술했듯이 타인의 신용카드를 절취, 강취, 사취, 갈취, 횡령한 경우에는 각각 절도죄, 강도죄, 사기죄, 공갈죄, 횡령죄가 성립함은 물론이다. 또한 분실되었거나 잘못 배달된 타인의 신용카드를 영득하면 점유이탈물횡령죄가 성립한다.

신용카드를 위조·변조한 경우는 일단 자기띠 이외의 부분을 위조·변조한 경우와 자기띠부분을 위작·변작한 경우로 나누어 볼 수 있다.[73] 자기띠 이외의 부분을 위조·

72) 대판 1996. 4. 9, 95 도 2466 (신용카드의 거래는 신용카드회사로부터 카드를 발급받는 사람이 위 카드를 사용하여 카드가맹점으로부터 물품을 구입하면 그 카드를 소지하여 사용하는 사람이 카드회사로부터 카드를 발급받은 정당한 소지인인 한 카드회사가 그 대금을 가맹점에 결제하고, 카드회사는 카드사용자에 대하여 물품구입대금을 대출해 준 금전채권을 가지는 것이고, 또 카드사용자가 현금자동지급기를 통해서 현금서비스를 받아 가면 현금대출관계가 성립되는 것인 바, 이와 같은 카드사용으로 인한 카드회사의 금전채권을 발생케 하는 카드사용행위는 카드회사로부터 일정한 한도내에서 신용공여가 이루어지고, 그 신용공여의 범위 내에서는 정당한 소지인에 의한 카드사용에 의한 금전대출이 카드발급시에 미리 포괄적으로 허용되는 것인 바, 현금자동지급기를 통한 현금대출도 결국 카드회사로부터 그 지급이 미리 허용된 것이고, 단순히 그 지급방법만이 사람이 아닌 기계에 의해서 이루어지는 것에 불과하다. 그렇다면 피고인이 카드사용으로 인한 대금결제의 의사와 능력이 없으면서도 있는 것 같이 가장하여 카드회사를 기망하고, 카드회사는 이에 착오를 일으켜 일정한도 내에서 카드사용을 허용해 줌으로써 피고인은 기망당한 카드회사의 신용공여라는 하자있는 의사표시에 편승하여 자동지급기를 통한 현금대출도 받고, 가맹점을 통한 물품구입대금 대출도 받아 카드발급회사로 하여금 같은 액수 상당의 피해를 입게 함으로써, 카드사용으로 인한 일련의 편취행위가 포괄적으로 이루어지는 것이다. 따라서 카드사용으로 인한 카드회사의 손해는 그것이 자동지급기에 의한 인출행위이든 가맹점을 통한 물품구입행위이든 불문하고 모두가 피해자인 카드회사의 기망당한 의사표시에 따른 카드발급에 터잡아 이루어지는 사기의 포괄일죄이다).

73) 강동범, 전게논문, 166면은 신용카드의 자기띠부분은 독자적인 의미를 갖는 것이 아니고 그 밖의 부분과 불가분적으로 결합하여 하나의 신용카드를 구성하고 있을 뿐이므로 나누어서 고찰할 필요는 없다고 한다.

변조하는 것은 예컨대 카드를 부정취득하여 회원서명란에 자기이름을 써 넣는다든지 카드의 유효기간을 연장하는 등의 방법을 말한다. 이 경우 신용카드는 사실증명에 관한 사문서에 해당하므로 사문서위조·변조죄에 해당하지만 여신전문금융업법 제70조 제1항 제1호[74]에 별도의 처벌규정을 두고 있으므로 여신전문금융업법위반죄에 해당한다. 한편 자기띠부분에 대한 위작·변작행위는 개정형법에서 신설한 사전자기록 위작·변작죄(제232조의 2)[75]에 해당한다는 점에는 문제가 없다. 다만 신용카드의 위조·변조행위를 처벌하고 있는 여신전문금융업법 제70조 제1항 제1호가 자기띠부분의 위작·변작행위에도 적용된다고 볼 것인가에 대하여 문제가 될 수 있으나 이를 긍정해야 할 것이다. 왜냐하면 자기띠부분에는 회원번호, 회원성명, 비밀번호 등이 기록되어 있어 이의 위작·변작행위는 자기띠 이외의 부분의 위조·변조행위와 구별할 이유가 없기 때문이다. 따라서 사전자기록 위작·변작죄와 여신전문금융업법은 법조경합관계에 있으므로 자기띠부분의 위작·변작행위도 여신전문금융업법만이 적용될 것이다.

ii) 신용카드의 부정사용과 관련된 범죄

먼저 자기명의의 유효한 신용카드의 부정사용행위에 대해서는 카드사용대금을 결제할 의사와 능력없이 자신의 카드를 이용하여 신용카드 가맹점에서 물품이나 용역을 제공받은 경우와 변제할 의사없이 자기명의의 신용카드를 이용하여 현금서비스를 받은 경우로 나누어 볼 수 있다. 전자의 경우에 형법상의 사기죄가 성립하는가 여부가 문제되는데 이에 관하여는 견해의 대립이 있다. 대체로 학설의 다수[76] 와 판례[77]는 사기죄의 성립을 인정하고 있는데, 다만 피기망자와 피해자를 누구로 볼 것인가에 관하여 가맹점이 피기망자 및 피해자라는 견해(제1설), 가맹점이 피기망자이고 카드회사가 피해자라

74) 다음 각호의 1에 해당하는 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. 신용카드 등을 위조 또는 변조한 자
2. 위조 또는 변조된 신용카드 등을 판매하거나 사용한 자
3. 분실 또는 도난된 신용카드 또는 직불카드를 판매하거나 사용한 자

75) 사무처리를 그르치게 할 목적으로 권리·의무 또는 사실증명에 관한 타인의 전자기록 등 특수매체기록을 위작 또는 변작한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

76) 강구진, 형법강의(각론 I), 박영사, 1983, 324면; 강동범, 자기신용카드의 부정사용행위에 대한 형사책임, 51면 이하; 김일수, 한국형법(Ⅵ), 박영사, 1994, 235면; 이재상, 형법각론, 박영사, 1995, 322면; 김우진, 신용카드의 부정사용죄의 기수시기, 형사판례연구(3), 287면; 장영민, 전게논문, 85면 이하 등.

77) 대판 1996. 4. 9, 95 도 2466

는 견해(제2설), 카드회사가 피기망자이고 피해자라는 견해(제3설)로 나뉜다.[78] 이에 반하여 소수설[79] 은 신용카드의 단순한 제시행위는 그 제시자와 카드에 기재된 자가 동일인물이라는 표시행위에 불과하기 때문에 가맹점에 대하여 카드소지자의 지불의사와 능력에 대하여 착오를 일으키게 할 만한 기망행위라고 보기는 어려우며, 또한 카드가맹점도 신용카드 자체의 적법성, 인물과 서명의 동일성 그리고 이지체크에 의한 거래정지 여부의 형식적 심사만을 하고 이상이 없으면 신용판매를 거절하지 못하도록 되어 있기 때문에 카드제시자의 대금지불의사와 능력에 대하여는 아무런 관념이 없으므로 착오를 인정하기도 곤란하다고 한다. 따라서 현행 형법의 해석상 자기명의의 유효한 신용카드의 부정사용의 경우 사기죄의 성립을 인정하는 것은 어렵다고 한다. 생각건대 자기의 신용카드를 가맹점에 제시하여 사용하는 자는 단순히 카드가 자기의 것이고 그것이 유효하다는 점만을 나타내는 것이 아니라 대금결제일에 카드대금을 결제하겠다는 의사를 표시한 것으로 보아야 할 것이다. 왜냐하면 신용카드회원은 카드회사로부터 카드를 발급받을 때 앞으로 카드사용으로 인하여 발생하는 대금을 결제하겠다는 의사를 표명한 것이며, 따라서 신용카드거래는 바로 미래의 대금결제를 전제로 성립하는 것이므로 신용카드제시행위는 결제일에 대금을 결제하겠다는 것을 나타내는 행위로 볼 수 있기 때문이다. 그러므로 결제할 의사없이 가맹점에서 물품이나 용역을 제공받기 위하여 자기의 신용카드를 제시하고 매출전표에 서명하는 행위는 묵시적 기망행위로 보아야 하며, 이러한 기망행위에 의하여 착오에 빠진 가맹점의 처분행위가 존재하게 되는 것이다. 사기죄를 인정할 경우 고소를 할 수 있는 피해자가 누구인가도 문제가 되는데, 가맹점은 특별한 사정이 없는 한 카드회원이 작성한 매출전표에 기하여 카드회사로부터 대금을 지급받게 되므로 재산상의 손해가 발생하지 않는다. 따라서 피해자는 카드회사가 되며 결국 이러한 거래는 피기망자 내지 처분행위자와 피해자가 일치하지 않는 이른바 '삼각사기'의 한 형태라고 볼 수 있다. 피기망자와 피해자가 일치하지 않는 경우 통설, 판례에 따라 피기망자인 처분행위자에게는 피해자의 재산을 처분할 지위에 있어야 하는데 ,처분자인 가맹점은 카드대금이라는 채권을 발생시킨 것으로서 카드회사와의 가맹점 계약에 따라 카드회사의 재산을 처분할 수 있는 지위에 있는 것으로 볼 수 있다. 이렇

78) 그 자세한 내용에 관하여는 장영민, 전게논문, 84면-85면 참조.

79) 김영환, 신용카드부정사용에 관한 형법해석론의 난점, 형사판례연구[3], 310면; 배종대, 전게서, 336면; 오경식, 전게논문, 109면; 이상돈, 전게논문, 115면 이하.

게 본다면 매출표를 작성하여 가맹점으로부터 물품이나 용역을 제공받은 때에 사기죄는 기수에 도달한 것으로 볼 수 있다. 한편 자기명의의 신용카드로 변제할 의사없이 현금자동지급기로부터 현금서비스를 받은 경우의 죄책에 대하여는 사기죄설, 절도죄설, 무죄설이 대립하고 있다.[80] 판례는 이에 대하여도 사기죄를 인정하고 있으나[81] 기계에 대한 기망이나 기계의 착오를 인정할 수 없다는 점에서 사기죄를 인정하기는 어렵다고 본다. 또한 개정형법상의 컴퓨터사용사기죄(제347조의 2)의 적용을 생각해 볼 수 있으나 본죄가 성립하려면 '허위의 정보 또는 부정한 명령'을 입력하여야 하는데, 자기의 진정한 신용카드를 투입한 행위는 여기에 해당하지 않으며, 컴퓨터사용사기죄는 사기죄와는 달리 재산상의 이익만을 그 객체로 하는데 신용카드를 현금자동지급기에 투입, 조작하여 인출한 현금은 재물이므로 본죄를 적용할 수는 없다. 그리고 은행은 신용카드와 비밀번호를 소지한 정당한 권리자에 대하여 현금서비스를 내주도록 기계조작을 함으로써 은행의 동의하에 지급이 이루어진다는 점에서 절도죄를 인정하기도 어렵다. 여신전문금융업법도 도난, 분실된 카드의 부정사용행위만을 처벌하고 있기 때문에 동법을 적용하기도 어렵다. 결국 변제할 의사없이 자기명의의 신용카드로 현금서비스를 받은 경우에 현행법상으로는 처벌하지 못하는 입법상의 흠결이 발생한다. 따라서 이러한 행위는 결제할 의사없이 가맹점으로부터 물품이나 용역을 제공받는 행위와 그 당벌성에 있어서 차이가 없으므로 이를 처벌하기 위한 입법적인 조치가 필요할 것으로 보인다. 한편 타인명의카드의 부정사용에 대하여는 먼저 신용카드를 절취, 강취, 사취한 후 이를 부정사용한 경우에 신용카드의 부정사용행위는 새로운 법익의 침해로 보아야 하고 이와 같은 부정사용행위가 절도죄, 강도죄, 사기죄의 불가분적 사후행위가 되는 것은 아니다.[81] 따라서 타인명의카드의 부정사용행위에 대하여는 먼저 여신전문금융업법이 제70조 제1항 제2호, 제3호에서 별도의 처벌규정을 두고 있으므로 당해규정이 적용될 것이다. 여신전문금융업법 제70조 제1항 제3호의 '도난되거나 분실된 신용카드 또는 직불카드'라 함은 타인이 절취 혹은 습득한 신용카드뿐만 아니라 자기가 직접 절취 혹은 습득한 카드를 사용한 경우도 포함한다.[83] 그리고 여기서 '신용카드의 사용'이라 함은

80) 그 자세한 내용에 관하여는 장영민, 전게논문, 89면 이하 참조.
81) 대판 1996. 4. 9, 95 도 2466; 대판 1996. 5. 28, 96 도 908.
82) 대판 1996. 7. 12, 96 도 1181.
83) 대법원도 절취한 본범도 포함된다고 본다(대판 1996. 4. 9, 95 도 2466).

신용카드의 소지인이 본래 용도인 대금결제를 위하여 가맹점에 신용카드를 제시하고 매출전표에 서명하여 교부하는 일련의 행위를 가리킨다.[84] 따라서 단순히 신용카드를 제시하는 행위는 신용카드부정사용죄와 사기죄의 실행에 착수한 것이라고 할 수는 있을지언정 신용카드사용행위를 완성한 것으로 볼 수 없다. 그런데 여신전문금융업법 제70조 제5항은 제1항 제1호와 제2호, 즉 신용카드의 위조·변조와 위조·변조된 신용카드의 부정사용에 대해서만 미수범을 처벌하고 있기 때문에 분실 또는 도난된 신용카드를 단지 제시한 것에 불과한 경우에는 여신전문금융업법으로는 처벌할 수 없고 사기죄의 미수범으로 처벌해야 할 것이다.

한편 타인의 신용카드를 부정사용하는 경우 그 과정에서 있게 되는 매출전표에의 서명 및 매출전표의 교부는 전형적인 수반행위로서 사문서위조 및 동행사죄의 구성요건을 충족한다고 하여도 이 사문서위조 및 동행사죄는 신용카드부정사용죄에 흡수되어 별도로 성립하지 아니한다.[85]

그리고 여신전문금융업법이 부정사용의 객체를 '위조·변조·도난·분실'된 카드에 한정하고 있으므로 그 이외의 방법으로 취득한 신용카드의 경우에는 여신전문금융업법이 적용되기 어렵고 형법에 의하여 규율할 수밖에 없을 것으로 본다. 여기서 '도난'의 개념에 '절취'뿐만 아니라 '강취'도 포함되는가가 문제될 수 있는데, 판례는 '강취한 신용카드를 온라인 현금자동지급기에 주입하고 비밀번호 등을 조작하여 피해자의 예금을 인출한 행위는 신용카드의 현금카드기능을 사용한 것으로 이와 같은 일련의 행위도 신용카드 본래의 용도에 따라 사용하는 것으로 보아야 하므로 부정사용의 개념에 포함된다'[86]고 하여 '강취'한 타인의 신용카드를 부정사용한 경우에 여신전문금융업법상의 부정사용죄를 적용하고 있다. 그러나 그 이외의 경우에는 여신전문금융업법이 적용될 수 없고 형법에 의하여 규율하여야 할 것이다. 즉 '사취, 갈취, 횡령'한 타인의 카드를 물품구입을 위하여 자기카드인 것처럼 가맹점에 제시한 행위는 형법상의 사문서부정행사죄에 해당할 뿐만 아니라 사기죄의 실행에 착수한 것며, 나아가 매출전표에 서명하여

84) 대판 1993. 11. 23, 93 도 604.

85) 대판 1992. 6. 9, 92 도 77; 대판 1993. 11. 23, 93 도 604 판결도 신용카드부정사용죄에 있어서 '사용'의 개념에 관하여 '···신용카드의 사용이라 함은 신용카드의 소지인이 본래 용도인 대금결제를 위하여 가맹점에 신용카드를 제시하고 매출전표에 서명하여 이를 교부하는 일련의 행위를 가리키므로···'라고 판시하고 있다.

86) 대판 1998. 2. 27, 97 도 2974.

교부하면 추가로 사문서위조죄 및 동행사죄가 성립할 것이다.

한편 타인의 카드를 부정사용하여 가맹점에서 물품을 구입한 경우 신용카드부정사용죄와는 별도로 사기죄가 성립하는데 타인의 카드를 부정사용하는 행위로 기망행위를 한 것이므로 양죄는 상상적 경합관계로 보아야 할 것이다.[87] 그러나 판례는 신용카드부정사용죄와 사기죄는 그 보호법익이나 행위의 태양이 전혀 달라 실체적 경합관계에 있다고 한다.[88]

다음으로 부정취득한 타인의 신용카드를 사용하여 현금자동지급기에서 현금을 인출하는 행위(소위 현금서비스)에 대해서는 현금자동지급기가 기계라는 점을 들어 사기죄가 아니라 점유를 배제하는 절도죄에 해당한다는 절도죄설[89]과 컴퓨터사용사기죄설[90] 이 있다. 먼저 컴퓨터 등 사용사기죄의 성립 여부에 대하여, 부정한 명령을 입력한다는 본죄의 구성요건은 프로그램 자체를 조작하는 경우에 국한하여 타인의 비밀번호를 알아내어 사용하는 것과 같이 정당한 정보를 부정하게 사용하는 경우에는 적용할 수 없다는 견해[91]도 있으나, 명령이 반드시 프로그램만을 의미한다고는 볼 수 없고 경우에 따라서는 프로그램도 자료의 일종이므로 프로그램 자체는 조작함이 없이 명령·자료를 입력할 권한이 없는 자가 명령·자료를 입력하는 경우, 즉 진실한 자료의 권한없는 사용도 입법취지에 맞게 부정한 명령에 해당한다고 보아야 할 것이다. 그렇지만 이러한 해석에도 불구하고 재물과 재산상의 이익을 구별하고 있는 형법하에서 컴퓨터 등 사용사기죄의 행위객체는 재산상의 이익이므로 타인의 신용카드를 사용하여 현금지급기에서 현금을 지급받은 경우에는 본죄가 성립하지 아니한다. 따라서 절도죄로 보아야 할 것이나 부정취득한 타인의 신용카드로 현금자동지급기에서 현금서비스를 받는 행위는 신용카드부정사용에 해당되므로 여신전문금융업법이 적용될 것이다.

한편 타인의 신용카드를 사용하여 현금자동지급기에서 현금서비스를 받는 것이 아니

87) 강동범, 전게논문, 128면.

88) 대판 1996. 7. 12, 96 도 1181.

89) 대판 1986. 3. 25, 85 도 1572; 1995. 7. 28, 95 도 997; 정영진, 신용카드범죄의 유형과 제재, 재판자료 제64집, 250면

90) 김일수, 302면; 손동권, 고시연구, 1996. 5, 174면은 진실한 자료를 부정하게 사용하는 것은 제347조의 2의 구성요건에 포함시킬 수 없으므로 동죄의 성립을 부인한다. 그러면서도 만일 진실한 자료의 부정사용을 포함시킨다면 컴퓨터 등 사용사기죄가 성립하고 절도죄의 성립은 배제된다고 본다.

91) 손동권, 전게논문, 174면; 장영민, 개정형법의 컴퓨터범죄, 고시계, 1996. 2, 49면

라 타인의 구좌의 예금을 인출한 경우 여신전문금융업법상의 신용카드부정사용죄에 해당할 것인가가 문제된다. 판례는 '신용카드를 사용하여 예금을 인출할 수 있는 현금카드기능은 구 신용카드업법 제6조 제2항, 구 신용카드업법시행령 제5조 제3호, 제6조의 규정 등에 따라 · · · 구 신용카드업법의 목적을 달성하기 위하여 허가한 부대업무로 볼 수 있으므로 ' 강취한 타인의 신용카드를 현금자동지급기에 주입하고 비밀번호 등을 조작하여 피해자의 예금을 인출한 행위는 신용카드의 현금기능을 사용한 것으로 이와 같은 일련의 행위도 신용카드 본래 용도에 따라 사용하는 것으로 보아 신용카드부정사용죄를 인정하고 있다.[92] 그러나 부정취득한 타인의 현금카드의 부정사용행위에 대하여는 여신전문금융업법이 적용되지 않는 점을 고려할 때 신용카드를 단지 현금카드기능에 한정하여 사용하는 경우에 이와 달리 처벌하는 점에 있어서는 문제가 있지 않을까 생각된다. 참고로 갈취한 타인의 현금카드로 여러번 현금을 인출한 행위에 대하여 현금카드 갈취행위와 분리하여 절도죄의 성립을 인정할 것이 아니라 공갈죄의 포괄일죄를 인정한 판례[93] 가 있다. 판례에 의하면 예금주인 현금카드 소유자를 협박하여 피해자로부터 예금인출의 승낙을 받고 현금카드를 교부받아 현금자동지급기에서 예금을 여러번 인출한 행위에 대하여, 하자있는 의사표시이기는 하지만 피해자의 승낙에 의하여 현금카드를 사용할 권한을 부여받아 이를 이용하여 현금을 인출한 이상, 피해자가 그 승낙의 의사표시를 취소하기까지는 현금카드를 적법, 유효하게 사용할 수 있고, 은행의 경우에도 피해자의 지급정지신청이 없는 한 피해자의 의사에 따라 그의 계산으로 적법하게 예금을 지급할 수밖에 없는 것이어서 현금지급기에서 피해자의 예금을 취득한 행위는 현금지급기 관리자의 반하여 그가 점유하고 있는 현금을 절취한 것으로 볼 수 없고 피해자의 예금을 갈취하고자 하는 피고인의 단일하고 계속된 범의 아래에서 이루어진 일련의 행위로서 포괄하여 하나의 공갈죄를 구성한다고 한다.

iii) 신용카드의 부정처분과 관련된 범죄

신용카드의 소유권은 신용카드발행회사에게 있고 카드회원은 이를 사용할 권한을 갖고 있을뿐이므로 카드회원은 타인의 재물인 신용카드를 보관하는 자에 불과하다. 따라서 카드회원이 신용카드를 불법처분하면 횡령죄를 구성하겠지만, 여신전문금융업법 제70조 제3항 제1호[94] 는 별도로 신용카드의 양도 · 양수와 질권설정행위를 처벌하고 있으

92) 대판 1998. 2. 27, 97 도 2974.

93) 대판 1996. 9. 20, 95 도 1728.

므로 이들 행위는 횡령죄가 아닌 여신전문금융업법위반죄가 된다.

iv) 가맹점에 의한 범죄

가맹점에 의한 범죄에 있어서 이중매출전표작성행위나 매출전표의 위·변조행위는 사문서위조와 변조죄에 해당하고 이것을 이용하여 카드회사로부터 대금을 지급받는 행위는 위·변조사문서행사죄와 사기죄의 상상적 경합이 되어 사문서위·변조죄와 실체적 경합범이 된다. 물품의 판매 또는 용역의 제공을 가장하거나 실제 매출금액을 초과하여 신용카드 매출전표를 작성하고 자금을 융통하여 준 행위 또는 이를 중개, 알선한 행위는 여신전문금융업법 제70조 제2항 제3호[95]에 의하여 처벌된다. 또 다른 가맹점명의로 매출전표를 작성하여 매출채권을 행사한 경우 당해 매출전표를 작성하거나 이를 작성하도록 가맹점명의를 대여하는 행위는 여신전문금융업법 제70조 제3항 제4호[96]에 의하여 처벌된다. 그리고 매출전표를 양도하는 행위 및 이를 양수하는 행위는 여신전문금융업법 제70조 제3항 제5호[97]에 의하여 처벌된다. 그런데 여신전문금융업법 제70조 제2항 제3호와 제70조 제3항 제5호 소정의 '매출전표'는 당해 신용카드가 카드회원 본인에 의하여 정당하게 사용됨으로써 진정하게 성립된 매출전표를 말한다. 따라서 위조·변조 또는 도난·분실된 신용카드 등의 사용에 의하거나 신용카드의 제시도 없이 카드회원의 서명이 위조되어 작성된 매출전표는 여기에 해당하지 아니한다.[98] 그리고 가맹점수수료를 신용카드회원에게 전가하는 행위는 여신전문금융업법 제70조 제3항 제2호[99]에 의하여 처벌된다.

② 처벌법규의 신설 내지 보완

---

94) 다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1'천만원 이하의 벌금에 처한다.
1. 제15조의 규정(신용카드의 양도 등의 금지)에 위반하여 신용카드를 양도·양수하거 나 질권설정을 한 자

95) 다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.
3. 물품의 판매 또는 용역의 제공을 가장하거나 실제 매출금액을 초과하여 신용카드 매출전표를 작성하고 자금을 융통하여 준 자 또는 이를 중개·알선한 자

96) 다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
4. 제19조 제4항 제4호의 규정에 위반하여 신용카드가맹점의 명의를 타인에게 대여한 자

97) 제20조 제1항의 규정에 위반하여 매출전표를 양도한 자 및 이를 양수한 자

98) 대판 1996. 5. 31, 96 도 449.

99) 제19조 제3항의 규정에 위반하여 가맹점수수료를 신용카드회원 등으로 하여금 부담하게 한 자

현행 여신전문금융업법 제70조에는 신용카드범죄라고 볼 수 있는 행위에 대한 벌칙조항을 규정하고 있다. 그러나 단 한 개의 조문만을 규정하고 있기 때문에 현재 증가일로에 있고, 다양화·교묘화되고 있는 각종 신용카드범죄를 처벌하는 데 있어서 적지 않은 문제점을 안고 있다고 할 수 있다. 그러한 문제점 중의 하나는 앞에서 보았듯이 변제할 의사 또는 능력없이 자신의 카드를 이용하여 현금자동지급기에서 현금서비스를 받는 경우 처벌의 흠결이 발생한다는 점이다. 이러한 행위는 자기의 신용카드로 결제할 의사나 능력없이 가맹점에서 물품을 구입하거나 용역을 제공받는 행위와 그 당벌성에 있어서 차이가 없다고 생각되므로 이러한 자기신용카드의 남용행위에 대한 처벌규정을 마련할 필요가 있다고 하겠다.

또한 부정사용행위의 경우 여신전문금융업법과는 별도로 형법상의 사기죄가 성립하게 되는데, 판례는 양죄의 관계를 실체적 경합관계로 보고 있으나 타인의 카드를 부정사용하는 행위로 기망행위를 한 것이므로 양죄는 상상적 경합관계에 있다고 보아야 할 것이다. 그러나 문제는 사기죄의 법정형이 10년 이하의 징역인 것에 반하여 신용카드부정사용죄의 경우 법정형이 7년 이하의 징역이어서 상상적 경합관계로 볼 경우 법정형이 중한 형법상의 사기죄의 규정이 언제나 적용되기 때문에 여신전문금융업법 제70조 제1항이 사문화될 우려가 있다. 따라서 여신전문금융업법 제70조 제1항의 법정형을 조정할 필요가 있다.

또한 여신전문금융업법 제70조가 도난, 분실된 신용카드 등의 부정사용만을 규정하고 있으나 강취, 갈취, 사취, 횡령 등 기타의 방법으로 불법영득한 신용카드를 사용한 경우까지 추가하여 규정하는 것이 바람직하며, 동법 제70조 제2항 제3호의 매출전표 허위기재행위의 경우에는 그 법정형이 3년 이하의 징역으로 되어 있는데, 법정형이 5년 이하의 징역인 사문서위조,변조죄와 비교하여 볼 때 5년 이하의 징역으로 상향조정함이 바람직하다.

2) 제도적 대응방안

① 카드발급시 가입신청회원의 자격에 대한 철저한 조사

신용카드에서 발생하는 막대한 이윤 때문에 신용카드회사들이 신용카드의 양적 확대를 위하여 카드회원에 관한 자격요건에 관한 심사를 소홀히 하고 신용카드의 발급을 남발함으로써 연체료의 규모가 매년 증가하고 있을 뿐만 아니라 범죄를 유인하는 것으로 보인다. 따라서 신용카드발급시 가입신청회원의 자격에 대한 조사를 철저히 하여 불

량회원에 대한 카드발급을 사전에 예방하고, 그 후에도 회원의 거래상황을 파악하여 회원을 적절하게 관리할 수 있도록 하여야 할 것이다. 신용카드발급의 남발을 막기 위하여 관계당국이 연체비율이 높은 카드회사에 대하여 신규발급을 중단시키는 조치도 고려해 볼 수 있을 것이다.

② 신용카드의 송부방법의 대책

신용카드가 배달과정 중에 본인에게 전달되지 않고 사용권한이 없는 제3자에게 전달되어 부정사용되는 경우가 있다는 점을 고려하여 카드우송시 개별봉인하여 회원 이외에 타인이 개봉하지 못하도록 하고 카드교부시 반드시 수령증을 청구하도록 하여야 할 것이다.

③ 가맹점 및 매출전표의 관리철저

신용카드가맹점 허가시에도 직접 회사를 방문하는 등 철저한 심사를 통하여 허위가맹점이 생기지 않도록 하여야 하며, 위조매출전표의 경우 단기간에 대량으로 접수된다는 점을 고려하여 건당 매출금액이 고액이고 다량의 매출전표가 접수될 때에는 진위여부를 확인하는 등 심사를 강화하고, 가맹점 보관용 매출전표의 관리를 철저히 함은 물론 위조가 불가능한 비표를 개발하여 매출전표제도에 대한 개선방안을 검토하여야 할 것이다. 또한 사채영업을 하는 변칙 가맹점을 색출하기 위해 국세청과의 협조체제를 강화해야 할 것이다.

④ 신용카드 사후관리업무의 강화

분실, 도난신고 접수시 지체없이 카드가맹점에 통보해야 하며 매월 카드사용한도액을 초과하여 부당사용한 회원에 대하여는 신용카드거래정지 등 제재조치를 강화하여야 한다. 또한 각 가맹점에 신용조회단말기의 보급을 확대함은 물론 중앙전산조직과 온라인망을 연결하는 등 전산조직의 정비도 강화해야 할 것이다. 또한 모든 금융기관에 현금자동지급기에 대한 디지털 CCTV를 설치하여 범인의 추적에 활용하여야 할 것이다.

⑤ 신용카드보안기능의 강화

분실, 도난당한 신용카드의 부정이용을 방지하기 위하여 회원의 사진이 부착된 소위 Photo 서명카드의 발급을 확대하고, 위조·변조 등을 방지하기 위하여 I.C칩이 내장된 스마트카드나 레이져 등을 이용한 카드를 발급하도록 하여야 할 것이다. 그리고 카드가맹점도 카드거래시 카드상의 서명과 매출전표상의 서명을 철저히 대조하고 주민등록증을 통하여 신원확인을 하는 풍토가 조성되어야 할 것이다.[100] 그리고 신용카드 뒷면의 자기테이프를 변조하는 것을 예방하기 위하여 특수한 방법의 카드확인장치(CVC)[101]를

적극적으로 가동하여야 한다. 또한 최근 카드고객의 정보가 유출되어 해외에서 대량으로 카드를 복제하여 사용하거나 국내로 카드복제기를 들여와 카드를 쉽게 위조하는 사례들이 발생하고 있다는 점을 고려하여 신용카드회원의 고객정보에 대한 관리도 철저히 함으로써 고객정보가 유출되어 쉽게 카드가 위조되는 것을 방지하여야 할 것이다.

⑥ 수사기술의 개발 및 수사기구의 집중화

신용카드범죄에 대한 수사는 그 특성상 종래의 전통적인 범죄에 대한 수사와는 다를 수밖에 없다. 따라서 종래의 수사기술에만 의존하지 말고 새로운 수사기법을 개발해야 하며, 이를 전담하는 수사기구를 설치할 필요가 있다. 현재 경찰청은 홈뱅킹사기, 컴퓨터해킹, 신용카드위조 등 전문범죄에 대처하기 위하여 경찰청 형사국에 지능과를 설치하여 운영하고 있는데, 이를 지방경찰청에 까지 확대할 것이 요망되며 장기적으로는 신용카드범죄를 전담하는 전담수사기관을 설치할 필요가 있다고 하겠다. 또한 신용카드범죄의 효율적인 처리와 국제적인 카드범죄에 대처하기 위하여는 검찰, 국세청, 신용카드회사 등 관련기관과의 유기적인 공조체제의 구축도 아울러 요구된다.

⑦ 신용카드범죄에 관한 공식적인 통계작성과 연구

신용카드범죄는 신용카드회사가 범죄통계를 자체적으로 집계하고 있어도 신용실추를 우려하여 이를 공개하고 있지 않기 때문에 정확한 실태와 심각성을 파악하지 못하고 있다. 따라서 경찰 자체만이라도 신용카드범죄에 관한 공식통계를 집계하고 그 수법 등을 분석, 연구하여 이를 토대로 수사기법의 개발에 활용하여야 한다.

⑧ 신용카드회사 등에 대한 사전협조관계의 유지와 신고체제의 확립

신용카드범죄에 대한 수사에 있어 큰 애로점 중의 하나는 신용카드회사나 신용카드업협회가 자체 조사를 하다 충분한 증거확보를 하지 못한 상태에서 고소, 고발 또는 진정을 해온다는 점이다. 신용카드회사의 입장에서는 범인의 적발과 증거의 확보가 곤란

100) 금융결제원은 최근 신용카드가 부정사용되는 것을 방지하기 위하여 신용카드 사용자의 본인여부를 확인하는 검증서비스를 시작했다고 한다. 검증서비스란 영업중인 카드가맹점에서 고객이 물품을 구입하거나 유료서비스 가입을 신청할 때 고객이 제시한 카드번호와 함께 주민등록번호 또는 비밀번호를 입력해 본인 여부를 사전조회하는 시스템을 말한다. 금융결제원은 검증서비스를 통하여 통신판매나 홈쇼핑, 전자상거래 등에서 타인의 카드번호만으로 부정사용되는 것도 막을 수 있을 것이라고 한다(한겨레신문 1998년 9월 18일자 참조).

101) CVC는 신용카드 뒷면의 자기테이프에 카드확인코드를 입력하여 이 코드로 카드의 위. 변조 여부를 식별할 수 있는 장치이다. 그러나 최근 이 장치도 완벽하지는 못한 것으로 드러나 다른 보안장치의 개발도 서둘러야 할 실정이다.

하여 수사의뢰를 하는 것이겠지만, 사전에 이들 기관에 고소장 또는 고발장의 기재사항 및 기재요령 등에 관한 협의와 수사상의 애로점 등을 홍보하여 사전협조관계를 유지하여야 한다. 또한 신속한 신고체제를 확립하여 범인의 증거인멸이나 도주의 가능성을 차단하여야 한다.

4. 정보통신범죄

가. 의의와 유형

오늘날 소위 '정보의 바다'라고 일컫는 인터넷의 급격한 보급확산과 정보통신망의 구축으로 인하여 모든 종류의 다양한 정보들이 시간과 국경을 넘어 자유자재로 유통될 수 있게 되었다. 그러나 이러한 정보에는 유익한 정보뿐만 아니라 사회적으로 유해하거나 위험한 정보들도 많이 유통되고 있고, 인터넷이나 정보통신망을 종래의 전통적인 범죄에 악용하는 행위들도 발생하고 있어서 많은 사회적 문제를 야기시키고 있다. 즉 익명성·다양성·국제성·시공초월성 등을 특징으로 하는 인터넷은 종래의 PC통신망과는 차원을 달리하는 소위 '사이버스페이스'라는 가상공간을 형성하고 있어서 이 공간에서 펼쳐지고 있는 이들 범죄에 대하여는 종래의 법률이나 수사체제 및 기법으로는 적절히 대처하기 어려운 많은 문제점을 야기시키고 있는 것이다.

따라서 인터넷이나 정보통신망을 이용한 이들 범죄에 대한 통일적이고 효율적인 대응책을 마련하기 위하여 아직 학문적으로나 법률적으로 확립된 개념은 아니지만 이들 범죄를 정보통신범죄로 분류하여 논할 필요가 있다고 하겠다.

인터넷이나 정보통신망을 악용하는 정보통신범죄의 유형은 컴퓨터해킹을 통한 각종 전산자료의 누출과 개인의 비밀침해행위, 컴퓨터통신 상대방에 대한 무절제하고 비윤리적인 언어의 폭력과 인격모독적이거나 명예를 훼손시키는 통신행위, 각종 불법복제된 상용 소프트웨어의 배포·판매행위, 컴퓨터통신이용 사기 및 각종 음란물의 전파·판매행위, 전자도박장에서의 도박행위, 다른 컴퓨터시스템에 침입하여 시스템을 파괴하는 행위, 컴퓨터통신망을 마약거래나 자금세탁의 장소로 이용하는 행위 등 매우 다양하다. 그러나 앞서 고찰한 컴퓨터범죄와 중복되지 않는 범위내에서 사이버테러, 인터넷상의 음란정보나 위험정보의 유통, 인터넷사기, 컴퓨터통신을 통한 다른 사람에 대한 명예훼손이나 모욕 등과 같은 대표적인 몇가지 유형을 살펴 보기로 한다.

나. 수법 및 특징

1) 사이버테러

사이버테러란 정보처리장치나 정보통신망을 이용하여 다른 사람의 생명, 신체, 재산에 해악을 가할 것을 고지하거나 이러한 행위를 수단으로 금품이나 경제적 이득을 꾀하는 행위를 말한다.

사이버테러의 전형적인 수법은 '13일의 금요일' 등 일정한 조건을 만족시키면 특수 프로그램이 저절로 작동되어 컴퓨터시스템을 공격, 귀중한 정보를 무차별 파괴하는 「논리폭탄」(Logic Bomb)이 대표적인 것이지만, 최근 상품광고 등 수만 통의 전자우편을 한꺼번에 송신하여 다른 사람의 정보처리장치의 기억매체가 과부하에 이르러 작동하지 못하게 하는 「전자우편폭탄」(Email Bomb 또는 Spam mail), 뉴스그룹을 통해 역정보를 흘리는 「플레임」(flame)[102], 전자기파를 발사해 컴퓨터의 자기기록 정보를 파괴하는 「고출력 전자총」(Herf Gun)[103] 등 새로운 유형의 수법들이 등장하고 있다.

이미 사이버테러는 국제적으로 여러차례 시도되었는데, 국제테러리스트들은 세계 유명금융기관이나 전자상거래업체들의 컴퓨터시스템, 그리고 유명인사의 인터넷 홈페이지까지 무차별적으로 테러를 감행하여 왔다. 우리나라에서도 1997년 8월 특정인에게 10만통의 전자우편을 한꺼번에 전송하여 '하이텔'의 인터넷 전자우편기능을 마비시킨 사례[104]와 450메가의 대규모 파일을 동시에 전송하여 '나우누리'의 인터넷 접속망을 마비시킨 사례[105]가 발생한 바 있는데, 만약 북한이 국제범죄조직과 연계하여 국가기간전산망에 침입, 전산망을 마비시킬 경우 그 피해는 막대할 것으로 보여져 앞으로 사이버테러는 정보화사회를 구축하는데 있어서 뿐만 아니라 국가안보에 있어서도 심각한 위협요

---

102) 네티즌들이 공통의 관심사를 논의하기 위해 개설된 토론방인 뉴스그룹에 고의로 기업·개인 등에 관한 악성루머를 유포하여 곤경에 빠뜨리는 기법을 말한다.

103) 컴퓨터는 전자회로로 구성돼 고출력 전자기파를 받으면 오작동하거나 정지된다는 점을 이용한 것으로 특히 기업들의 핵심정보가 수록된 하드디스크는 허프건에 가장 취약한 것으로 알려지고 있다.

104) 중앙일보 1998년 2월 3일자 참조

105) 이는 1998년 2월 26일 오후 5시 10분께 내국인으로 추정되는 해커가 PC통신 나우누리의 통신망에 침입해 소위 폭탄메일을 수천명의 가입자에게 동시에 보내는 바람에 전자메일을 담당하는 하드디스크에 이상이 생겨 다음날 오전 2시 응급복구가 완료될 때까지 무려 9시간동안 전자메일 기능이 완전히 마비된 사례이다.(한국일보 1998년 2월 27일자 참조)

소가 될 것으로 보인다.

2) 인터넷상의 음란정보나 위험정보의 유통

최근 불법복제기술의 발달, 디스켓·CD-ROM 등 다양한 저장매체의 보급과 함께 인터넷이 대중화되면서 이를 이용한 음란물의 청소년사회로의 확산이 심각한 사회문제로 되고 있다[106] 음란정보를 저장한 인터넷의 뉴스그룹이나 음란사이트가 접속에 아무런 제한이 없는 상태에서 광범위하게 개설되고 있으며, 청소년의 호기심을 상업적으로 이용하려는 섹스샵마저 범람하고 있다. 현재 인터넷 성인사이트는 1만개 정도인 것으로 알려지고 있고, 주로 월단위로 이용료를 받는 회원제이며 신용카드결제를 통해 연간 120억달러 정도의 매출을 올리고 있어 이제 하나의 산업으로 부상하고 있을 정도이다.

그런데 최근에 새롭게 나타난 경향은 해외의 포르노 웹사이트를 모방한 한국형 음란사이트의 등장이라고 할 수 있다. 지금까지 인터넷이용자들은 해외의 음란·도색성 웹사이트에 접속해 왔으나 올해초부터 20 여개의 한글 음란사이트가 생겨나 영어를 모르는 청소년들까지도 쉽게 접속하는 것이 가능하게 되었다.[107]

한편 PC통신을 이용하여 음란CD나 인터넷의 유료성인용 홈페이지를 볼 수 있는 비밀암호를 사고 파는 온라인 음란물거래도 매우 성행하고 있다. 통신망을 통하여 이루어지는 음란물의 배포실태를 보면 동화상으로 되어있는 음란소프트웨어의 경우는 대체로 파일의 크기가 대용량이기 때문에 파일 자체의 전송보다는 음란소프트웨어가 수록되어 있는 음란CD나 디스켓을 통신망을 통하여 판매하는 행위로 이루어지고 있고, 파일의 크기가 비교적 작은 정지화상으로 된 음란성소프트웨어나 음란한 내용의 텍스트파일은 통신망상으로 그대로 전송하는 방식도 많이 사용하고 있는 것으로 보인다. 인터넷상으

106) 정보통신윤리위원회가 지난 7월 13일부터 18일까지 서울과 부산, 대전 등 18개 중·고교생 2400명을 대상으로 'PC통신과 인터넷상의 불건전정보유통 및 윤리의식실태조사'를 벌인 결과 응답자 중 38.6%가 음란물과 폭력정보에 접촉한 경험이 있는 것으로 나타났다. 그 중 68.2%는 초등학교때부터 접촉한 것으로 나타났고, 음란물을 접촉하게 된 동기로는 50.5%가 친구들의 권유라고 응답하였다(한국일보 1998. 11. 20).

107) 국산음란사이트들은 특히 지난해 청소년들이 직접 제작해 물의를 빚었던 '빨간 마후라'의 동영상화면, 여배우·탤런트 등 인기연예인들의 얼굴과 나체사진을 합성한 사진, 여관방·비디오방과 모 여자대학 화장실에 '몰래카메라'를 설치해두고 촬영한 화면, 성행위장면 등을 난삽하게 묘사한 이른바 '야설' 등으로 해외도색사이트들과 차별화해 청소년들의 호기심을 자극하고 있다(중앙일보 1998. 5. 14일자 참조).

로 주로 전파되는 음란성파일의 대부분도 음란한 내용의 정지화상을 보여주는 소프트웨어들과 음란한 내용의 전자우편들이다.

그런데 최근에는 인터넷이나 PC통신을 이용한 음란사이트의 운영 또는 음란·불법복제물의 판매가 무직자와 실직자의 가담으로 점점 기업화되고 수법도 교묘해지는 추세를 보이고 있다.[108] 즉 음란물판매계층이 IMF체제이후 청소년컴퓨터매니아에서 돈벌이가 목적인 20-30대 실직자나 무직자로 옮겨져 기업형판매업자까지 등장하고 있는 것이다. 그리고 그 수법도 외국의 인터넷서비스업체들이 고객확보차원에서 인적사항에 대한 확인없이 신청절차만 거치면 무료로 홈페이지 및 게시판, 전자메일주소를 개설해 주는 것을 이용하여 가명으로 가입해 음란사이트개설이나 음란물판매를 해외에서 외국인이 하는 것처럼 위장한다든지 수시로 주소를 바꿈으로써 단속을 피하고 있고, 위조 또는 도난된 주민등록증을 이용하여 은행계좌를 개설한 뒤 공급, 판매책을 나누어 점조직으로 비디오, CD 등을 다량으로 밀매하기도 하고 심야에 잠깐 광고를 내고 사라지는 등 지능적인 수법이 사용되고 있다. 특히 최근 CD제작기(CD-Recorder)가 비교적 저렴한 가격에 공급되고 있어 음란성 CD가 쉽게 복제되어 국내에 널리 배포되고 있다. 이와 같이 컴퓨터통신망을 이용한 전자상거래가 음란물의 판매방법으로 악용되면서 정보화사회를 이루는 최첨단기술들이 청소년의 정서를 극도로 해치고 성문화의 퇴폐화를

108) 서울지검 특수 2부는 인터넷에 음란홈페이지를 개설하거나 PC통신을 통해 음란비디오 및 CD를 판매해온 부산 K초등학교 교사 한모(30)씨 등 15명을 전기통신기본법 또는 음반 및 비디오물에 관한 법률위반 혐의로 구속기소했다. 검찰은 고교생 이모군(17), 박모군(17)등 2명을 같은 혐의로 불구속 기소하는 한편 PC통신망을 이용, 윤락알선 광고를 내 회비명목으로 3백만원을 챙긴 민모(26)씨를 통신사기및 윤락행위 방지법위반등 혐의로 지명수배했다. 검찰에 따르면 교사 한씨는 '나우누리'에 홈페이지를 개설, '핫스토리'란 제목으로 근친간 또는 사제간 성행위나 미성년자의 성행위를 묘사한 음란소설(속칭 야설) 1백여편을 게재하고 외국 음란사이트에 접속토록 한 혐의다. 검찰이 개인의 홈페이지에 외국의 성인사이트를 접속케 한 이른바 '링크' 개설행위에 대해 전기통신기본법 위반 혐의를 적용해 처벌하기는 처음이다. 수배된 민씨는 지난 3월말 컴퓨터 통신망에 '화려한 외출'이란 제목아래 "윤락상대를 공급해 주겠다"고 광고를 내 3명으로 부터 1백만원씩 3백만원을 차명계좌를 통해 입금받은 것으로 밝혀졌다. 검찰조사결과 대학생 5명과 이군 등 고교생 2명, 실직자 6명이 포함된 음란홈페이지 개설자들은 인터넷망의 무료서비스를 이용, 자신의 인적사항을 가명으로 등록하거나 외국의 서버를 차용해 신분을 위장해 왔으며 입금계좌를 도난된 주민등록증을 이용해 개설한 뒤 공급·판매책을 나눠 점조직으로 비디오, CD 등을 다량 밀매한 것으로 드러났다.(한겨레신문 1998. 5. 13)

부추기는 수단으로 전락하고 있다. 즉 음란물에 노출된 청소년들에게는 음란물모방과 중독현상이 나타나 건전한 성장을 방해하고 비행을 저지르게 할 우려가 있는 것이다.

그런데 최근에는 컴퓨터통신망을 통해 회원을 모집하여 윤락행위를 알선하는 사례도 발생하고 있고, 컴퓨터통신망을 통해 '부부교환코너'를 마련하는 사례가 나타나는 등 인터넷과 컴퓨터통신망은 소위 '사이버 홍등가'로 전락하고 있다. 하지만 이러한 성인정보를 검색하고 감독해야 할 컴퓨터통신회사들은 정보조회율이 높을수록 이들 업체와 나눠갖는 수입이 늘어나는데다 뚜렷한 규제기준이 없다는 이유로 사실상 방치하고 있는 실정이다. 또한 사이버상의 음란물을 전파하는 사람들이 수시로 주소를 바꾸고 있어서 정확한 실태파악조차 쉽지 않을 뿐만 아니라 인터넷 자체가 공개된 시스템이어서 단속도 어려운 실정이다. 앞으로 통신시장이 개방되어 컴퓨터통신사업에 자유롭게 참여하게 될 경우 상업적인 음란정보제공자는 더욱 늘어날 전망이다.

한편 인터넷을 통하여 폭발물제조법과 그 사용법, 폭발물 및 화약구입 방법, 마약제조법 등이 상세히 기술되어 있는 자료들이 보급되고 있어 인터넷을 통한 범죄유포의 가능성이 나타나고 있다는 점도 심각한 문제가 될 것으로 보인다. 실제 미국에서는 청소년들이 인터넷을 통해 마약제조법이 담긴 문서를 구한 뒤 마약을 제조하거나 폭탄제조법을 보고 폭탄을 제조한 사례가 발생하여 충격을 주고 있다.

그리고 컴퓨터통신에서 본인의 확인이나 행위자에 대한 추적이 쉽지 않은 점을 이용한 이적표현물의 게시, 반국가단체 또는 이적단체에 대한 고무, 찬양 나아가 동 구성원간이나 적국과의 통신 등 이적행위와 간첩행위도 점차 증가할 것으로 보여 이에 대한 규제가 필요할 것으로 보인다.

3) 인터넷사기

인터넷을 이용한 전자상거래가 증가하면서 이를 악용한 범죄들도 발생하고 있는데, 회원의 확장이나 회원인도시 수수료지급 등을 미끼로 한 피라미드식 물품판매가 횡행하고 있고, 인터넷에 복권중개방을 개설한 다음 외국복권을 비싸게 팔아 부당이득을 보거나, 물품판매를 가장한 사기행위도 발생하고 있다. 즉 타인의 컴퓨터통신 ID 및 비밀번호를 도용하여 PC통신망 게시판에 상품염가판매 광고를 낸 뒤 이를 보고 연락해 온 이용자들에게 물건은 보내주지 않고 물품대금만 가로채는 신종통신사기범이 등장하고 있으며[109], 가공인물명의의 ID를 부정발급받아 이를 돈을 받고 판매하는 사례도 발생하고 있다. 또한 웹사이트를 디자인해 준다고 해놓고 돈만 받고 사라지는 인터넷서비스

관련사건에서부터 PC통신망을 이용 윤락알선광고를 낸 뒤 회비명목으로 금전을 가로채는 사례라든지, PC통신 게시판을 이용하여 '숙식제공, 기본급 120만원 수당 지급' 등 광고를 내 일을 시킨 뒤 임금을 지급하지 않는 등의 수법으로 사기를 치는가 하면, 대화방을 통해 알게 된 여성들의 인적사항을 이용 물품을 구입하고 대금을 전가시키는 사례[110] 등 사기사건의 유형도 다양하다. 최근 IMF경제체제 이후 실업자가 증가하자 재택근무채용사기 등 엉터리 사업기회를 선전하여 돈을 챙기고 약속을 지키지 않는 사기행위도 발생하고 있다.

전자상거래가 확산될 경우 이를 이용한 사기 및 불법행위도 확산될 것으로 보이는데 미국 등 선진국에서는 전자상거래와 관련된 사기 및 불법거래가 중요한 사회문제로 등장하고 있다.

4) PC통신을 통한 명예훼손과 모욕

PC통신에 설치된 전자게시판은 회원들이 자유롭게 의견을 제시하고 교환하여 토론문화의 향상과 여론형성에 도움을 주어 정보민주주의를 이룩한다는 긍정적인 측면도 있으나, 한편으로는 특정인을 상대로 한 인신공격성 허위사실의 유포, 폭언 등 명예훼손과 모욕적인 내용들이 게재되어 사회문제를 야기하고 있다.

이는 행위자가 누구인지 쉽게 확인할 수 없고, 타인의 ID를 도용할 수도 있으며, 범행의 흔적을 없애기 쉬운 컴퓨터통신의 특성을 이용한 것으로 보이는데, 타인에 대한 명예훼손이나 모욕도 컴퓨터통신의 대중화와 더불어 차츰 증가하는 추세이다. 특히 컴퓨터통신망에서 소위 컴섹을 강요하거나 언어폭력으로 상대방 여성에게 정신적 피해를 가하는 온라인성폭력도 빈발하여 1992년 한 여중생이 이를 비관하여 자살하는 사건도 발생하였다.

---

109) 조선일보 1997년 5월 14일자 참조.

110) 경찰청 컴퓨터범죄수사대는 PC통신을 통해 알게 된 여성들의 신상정보를 알아내 고가의 컴퓨터 프로그램을 전송받아 대금을 전가시킨 안모씨(22)를 사기등 혐의로 구속했다. 경찰에 따르면 안씨는 PC통신 대화방에서 알게된 이모씨(22)의 비밀번호를 이용, 일본어 번역 프로그램인 '오경박사' 등 7점의 프로그램을 전송받아 이씨에게 3백만원을 대신 물게 하는 등 15명의 여성들에게 1천2백여만원의 컴퓨터 프로그램 전송대금을 전가시킨 혐의다. 조사결과 안씨는 PC통신 대화방에서 "친하게 지내자"며 여성들의 전화번호 등 신상 정보를 파악하고 야간에 PC통신회사의 고객상담실에 전화를 걸어 요금납부 등을 구실로 내세워 피해 여성들의 납입자 번호, 비밀번호 등을 알아낸 것으로 드러났다.(한국일보 1998. 4. 2)

그리고 지방의회선거나 국회의원선거를 앞두고 특정후보를 비방하는 메시지를 PC통신에 게재하는 사례도 발생하고 있다. 앞으로 PC통신을 이용한 조직적인 불법선거운동이 빈발할 것으로 보이는데 헌법상 보장된 표현의 자유와 국민의 알 권리를 침해하지 않는 범위내에서 PC통신에 대한 지속적인 모니터링을 실시하여 이를 단속할 필요가 있다고 하겠다.

다. 추세전망

지금까지 정보통신범죄로 분류된 이들 범죄유형의 발생건수에 대한 정확한 통계는 아직 집계되지 않고 있어 그 현황을 알기는 어려우나, 대검찰청 정보범죄대책본부의 통계[111]에 의하면 1995년 4월부터 1997년 6월 사이에 처리된 정보범죄사범 중 전산망처리 정보훼손사건이 3건, ID 부정발급·사용 사기사건이 6건, 상용통신망 사기사건이 5건, 음란CD 등 제작·판매사건이 8건인 것으로 나타나 있다. 그러나 실제 발생한 정보통신범죄는 이 보다 훨씬 많을 것으로 추산된다.

최근 정보통신부가 국회에 제출한 국감자료를 보면 전화, PC통신, 인터넷을 통해 유통되는 불건전 음란정보가 1996년 85건에서 불과 3년만에 1998년 7월말까지 3,933건으로 무려 46배 가량 폭증한 것으로 나타나 있고, 1996년부터 3년간 유통된 음란정보는 7536건에 내용이 삭제된 건수는 2750건, 이용정지 1052건, 이용해지 46건에 이른 것으로 집계되어 있다.[112]

한편 정보통신망의 구축과 전자상거래의 확산으로 인터넷사기사건도 앞으로 폭발적인 증가를 할 것으로 예상된다. 이는 지난 9월 10일 미국 소비자연맹(The National Consumers League)이 1997년의 인터넷 사기사건은 1996년에 비해 300퍼센트나 증가했다고 밝힌 사실에서도 알 수 있다.

특히 그 유형도 1996년까지의 사기사건들이 실생활에서 아이디어를 얻은 사기수법을 단순히 온라인으로 옮긴 것에 불과했다면 1997년에 와서는 인터넷에서만 발생할 수 있는 독특한 온라인형 사기수법으로 바뀌고 있다고 한다. 그리고 사기규모의 경우는 실생활에서의 사기와 다르게 소액형태가 많은데 10달러에서 크게는 1만달러가 가장 많다고

111) 대검찰청 중앙수사부 정보대책본부(http://www.dci.sppo.go.kr/dci.htm) 정보범죄사범 유형별 수사실적('95. 4. 10-'97. 6. 30) 참조

112) 한국일보 1998. 10. 23일자 참조

하며, 이런 사기들은 대부분 안전한 전자상거래 시스템을 갖추지 않은 서비스를 이용한 이용자들에게 집중적으로 가해진다고 한다. 또한 사기사건의 지불형태를 살펴 보면 60퍼센트가 현찰이나 수표 등을 직접 입금하는 형태로 이루어졌으며, 19퍼센트만이 신용카드에서 발생했다고 한다.

인터넷에서 발생하는 사기사건들을 경고하기 위해 운영되고 있는 인터넷사기감시단이 발표한 사기유형 톱10을 살펴보면 다음과 같다.

〈표 5〉 인터넷 사기감시단이 발표한 사기유형 톱 10[113]

1996		1997(1-6월)	
1	피라미드/다단계 판매	1	인터넷 서비스 판매
2	사업설명	2	온라인 쇼핑(일반상품 판매)
3	컴퓨터 및 소프트웨어 판매	3	경매
4	인터넷 서비스 판매	4	피라미드/다단계 판매
5	재택근무	5	사업설명
6	회원제 서비스	6	재택근무
7	잡지구독	7	경품 및 복권
8	투자홍보	8	신용카드 제공
9	회원제 학습	9	서적판매
10	경품 및 복권	10	잡지구독

앞으로 각국에서 활발히 추진하고 있는 초고속 정보통신망 구축 프로젝트가 완성되면 지구상의 거의 모든 컴퓨터가 네트워크로 연결된다. 따라서 고도정보통신사회의 진전, 즉 개인용 컴퓨터의 광범위한 보급과 인터넷의 상용화 및 대중화 그리고 정보통신망의 급격한 확장과 함께 정보통신범죄유형에 해당하는 범죄들은 양적으로 폭발적인 증가를 할 것으로 예상되며, 질적으로도 인터넷을 통한 마약거래와 자금세탁 등 더욱 다양하고 교묘한 수법의 범죄들이 발생하리라고 생각된다.

라. 대응방안

1) 형사법적 대응방안

① 사이버테러

113) http://www.fraud.org/internet/instat.htm

먼저 사이버테러행위에 대하여는 현행 형법상 전자기록손괴죄(형법 제366조)[114], 공용전자기록무효죄(형법 제141조 1항)[115] 그리고 컴퓨터관련업무방해죄(형법 제314조 2항)[116]가 적용될 수 있을 것이다. 여기서 '허위의 정보나 부정한 명령을 입력한다'는 것은 진실에 반하는 정보나 예상하지 않은 프로그램을 입력하는 것을 말하는데 컴퓨터 바이러스가 그 대표적 예다. 또한 전산망의 보호조치를 침해하거나 훼손한 경우에는 전산망보급확장과 이용촉진에 관한 법률위반죄(동법 제22조 제2항[117], 제30조의 2[118])가 적용된다. 그러나 사이버테러행위를 사전에 방지하기 위해서는 인터넷 서비스업체로 하여금 반드시 전자우편중계용 컴퓨터에 스팸방지용 시스템을 의무적으로 설치하게 하는 등 소위 '사이버테러방지법'을 제정할 필요가 있다. 아울러 인터넷사용자들에게 불쾌감을 주거나 업무를 방해하는 스팸전자메일을 방지하기 위한 법적 조치가 필요하다고 생각되는데, 최근 미국 의회에 제출된 스팸관련법안은 좋은 참고가 될 것으로 본다. 미국 의회에서는 하원 및 상원에 다음과 같은 3건의 스팸관련법안을 제출하여 전자우편의 오남용에 대비하고 있다.[119] 하나는 "네티즌 보호법안(Netizens Protection Act of 1997)"으로서 Cristopher Smith에 의해 하원에 제출되었으며, 광고성 FAX를 금지한 법안인 통신법(Communication Act of 1934)에 전자우편을 추가하여 수신자가 원하지 않는 전자우편의 발송을 금지하고 있다. 특히 이를 위반하여 전자우편을 보낼 경우 수신자에게 돈을 지불해야 하는 등 발신자 측에 부담을 전가하고 있다. 또 하나는 "미요청 상업전자메일 선택법안(Unsolicited Commercial Electronic Mail Choice Act of 1997)"으로서 Murkowski에 의해 상원에 제출되었으며, 광고성 전자우편의 경우 제목에

114) 타인의 재물, 문서 또는 전자기록 등 특수매체기록을 손괴 또는 은익 기타 방법으로 그 효용을 해한 자는 3년 이하의 징역 또는 700만원 이하의 벌금에 처한다.

115) 공무소에서 사용하는 서류 기타 물건 또는 전자기록 등 특수매체기록을 손상 또는 은익하거나 기타 방법으로 그 효용을 해한 자는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

116) 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리장치에 장애를 발생하게 하여 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천 500만원 이하의 벌금에 처한다.

117) 누구든지 불법 또는 부당한 방법으로 제1항의 규정에 의한 보호조치를 침해하거나 훼손하여서는 아니된다.

118) 제22조 제2항의 규정에 위반하여 전산망의 보호조치를 침해 또는 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

119) http://www.jmls.edu/cyber/statutes/email/

"광고"라는 단어를 의무적으로 삽입하도록 규정하는 한편 ISP가 가입자를 위해 필터링 기능을 제공하도록 하고 있다. 한편 "전자우편 보호법안(Electronic Mailbox Protection Act of 1997)"은 Torricelli에 의해 상원에 제출되었으며 전자우편의 발신자 위조, 타인의 전자우편 서비스도용, 수신자가 원하지 않는 광고성 전자우편의 발송을 금지하는 내용을 가지고 있다.

② 인터넷상의 음란정보나 위험정보의 유통

최근 미국은 인터넷상의 음란물의 범람으로부터 청소년을 보호하기 위하여 온라인상에 외설폭력물을 올린 사람에게 25만달러의 벌금 또는 2년 이하의 징역에 처하도록 규정한 연방통신품위법(the Communication Decency Act, 보통 줄여서 CDA라 부른다)을 마련하였으나, 97년 6월 연방대법원에 의하여 이 법률이 언론의 자유를 침해한 것으로서 위헌이라는 판결을 받았다. 통신품위법 제223조(a)항 (1)(B)를 간추려보면, "통신수단을 통해 고의로 18세 미만의 미성년자에게 음란하거나(obscene), 저속한(indecent) 성적 내용물을 만들거나 전송하는 행위"를 규제하고 있고, 제223조 (d)항 (1)에는 "우리 시대의 사회기준에 의할 때 공공연히 해로운(patently offensive) 성적행위·기관을 묘사하는 내용물을 18세 미만의 미성년자 또는 특정인에게 보내거나 18세 미만자가 접근할 수 있는 방법으로 보여주는 인터랙티브 컴퓨터 서비스를 사용한 자는 형벌에 처한다"고 규정하고 있었다. 이것은 인터넷상의 음란물을 통제할 법적 근거를 갖춘다는 것을 의미하였으나, 인터넷의 검열을 반대하는 미국시민자유연대(the American Civil Liberties Union, 이것을 줄여서 ACLU라고 부른다)와 같은 자유주의자들의 법적 투쟁에 부닥쳐 결국 좌절되고 말았다. 이들은 통신품위법에 규정된 '저속한(indecent)'과 '공공연히 해로운(patently offensive)'이란 표현이 지나치게 일반적이고 추상적이어서 이를 위반했는지 여부를 가려낼 수 없으므로 표현의 자유를 보장한 수정헌법 제1조에 위배된다고 주장하면서 펜실베니아 제3순회 항소법원에 제소했고, 법원은 '저속한'이라는 문언과 '공공연히 해로운'을 규정하고 있는 제223조 (d)항 (1)이 위헌이라고 판결하였다. 이에 미정부는 즉각 연방대법원에 상고하였으나 미연방대법원은 1997년 6월에 위헌판결[Reno v. ACLU]을 내렸다. 그 후 미정부는 다시 컴퓨터온라인에 '미성년자에게 해로운' 자료를 제공하는 기업들은 사전에 성인 여부를 확인하도록 의무화하고 이를 어길 때에는 5만달러 이하의 벌금이나 6개월 이하의 징역에 처한다는 내용의 '어린이 온라인보호법'(COP)을 마련하였고, 현재 언론자유에 대한 침해라는 논란속에 미 하원을 통과한 상태에 있다.

한편 우리나라에서는 인터넷상의 음란정보를 규제할 수 있는 법적규정들이 마련되어 있다. 예를 들면 전산망보급확장과 이용촉진에 관한 법률, 전기통신사업법, 전기통신기본법, 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률, 음반 및 비디오물에 관한 법률 등이 그것이다. 먼저 전산망보급확장과 이용촉진에 관한 법률 제23조는 전산망사업자·전산망관리자 및 그 종사자와 전산망이용자로 하여금 공공의 안녕질서 및 미풍양속을 해치는 행위를 못하도록 하고 있다. 또한 전기통신사업법 제53조는 전기통신이용자에게 공공의 안녕질서 또는 미풍양속을 해치는 컴퓨터통신 및 음성정보서비스(소위 700서비스)와 같은 불온통신[120]을 금지하고 있고, 정보통신부장관은 불온통신에 대하여 전기통신사업자로 하여금 그 취급을 거부, 정지 또는 제한하도록 명할 수 있도록 하고 있으며, 이 시정명령을 이행하지 않을 경우 동법 제71조에 의하여 2년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 하는 등 불온통신의 단속에 관한 근거규정을 두고 있다. 그리고 제53조의 2에 민간기구인 '정보통신윤리위원회'를 설치하여 불온통신 등을 심사·규제할 수 있는 법적 근거를 마련하고 있다. 정보통신윤리위원회는 최소규제의 원칙, 공정성 및 객관성의 원칙, 비밀보호의 원칙에 따라 음성 뿐만 아니라 전기통신회선을 통하여 공개를 목적으로 유통되는 데이터 베이스, 사설 BBS, 게시판, 공개자료실, 대화방 등을 모니터링해 사후심의하도록 하고 있다.[121] 한편 음란정보제공자는 전기통신기본법 제48조의 2[122]에 의하여 처벌할 수 있고, 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률 제14조(통신매체이용음란죄)[123]에 의한 처벌도 가능하다. 여기서 음란정보제공자에 대하여 형법 제243조 음화반포 등 죄가 적용될 수 있을 것인가가 문제

120) 전기통신사업법 시행령 제16조는 불온통신의 내용으로 범죄행위를 목적으로 하거나 범죄행위를 교사하는 내용의 전기통신, 반국가적 행위의 수행을 목적으로 하는 내용의 전기통신, 선량한 풍속 기타 사회질서를 해하는 내용의 전기통신을 열거하고 있다

121) 위 규정에 따라 나우누리에 '섹스강국론', '무장공비 사건 조작 가능성 높다' 등의 글을 올린 김모씨에 대해 1년간 이용금지조치를 나우컴에 요청, 나우컴에서는 문제가 된 글을 모두 삭제한 바 있다. 또한 인터넷상의 북한사이트접속을 차단했으며, 인터넷의 Erotica사이트를 폐쇄했다.

122) 전기통신역무를 이용하여 음란한 부호·문언·음향 또는 영상을 반포·판매 또는 임대하거나 공연히 전시한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다

123) 자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화·우편·컴퓨터 기타 통신매체를 통하여 성적수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건을 상대방에게 도달하게 한 자는 1년 이하의 징역이나 300만원 이하의 벌금에 처한다.

될 수 있는데 대법원은 '형법 제243조는 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자에 대한 처벌규정으로서 컴퓨터 프로그램파일은 위 규정에서 규정하고 있는 문서, 도화, 필름 기타 물건에 해당한다고 할 수 없으므로 · · · 전기통신기본법 제48조의 2의 규정을 적용할 수 있음은 별론으로 하고 형법 제243조를 적용할 수는 없다'고 판시하여 이를 부정하고 있다.[124] 이는 개정형법이 컴퓨터범죄에 관한 규정들을 신설하면서 전자기록의 형태로 존재하는 음란물에 대한 처벌규정을 미처 마련하지 못하였기 때문에 나타난 결과로 보이는데 앞으로 법개정시 이를 반영하여야 할 것으로 보인다. 또한 개인의 홈페이지에 외국의 성인사이트를 접속케 하는 '링크'개설행위에 대해서도 전기통신기본법 등 현행법으로 처벌할 수 있을 것인가 여부에 관해서 논란의 여지가 있을 수 있는데, 논란의 여지를 막기 위하여는 이를 명확히 규정해 놓을 필요가 있을 것으로 보인다. 한편 PC통신을 통해 음란비디오 및 CD를 판매하는 경우 음반 및 비디오물에 관한 법률제25조 제1항[125]에 의하여도 처벌할 수 있을 것이다. 그러나 이처럼 개별적인 단행법률에 의해 규제하는 것은 급변하는 새로운 사회환경의 변화에 신속히 대응하지 못할 것이고 또한 각 법률에 따라 형의 균형이 맞지 아니할 가능성이 높기 때문에 관할대상에 통괄적으로 적용되는 특별법의 제정을 적극적으로 검토할 필요가 있다.[126]

한편 인터넷상의 홈페이지에 북한을 찬양하는 자료를 올린 경우에는 국가보안법이

124) 대판 1999. 2. 24, 98 도 3140 참조.

125) 다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 1. 제4조 제1항의 규정에 의하여 등록을 하지 아니하고 판매·배포·대여 또는 시청제공 등의 목적으로 음반 또는 비디오물을 제작한 자
2. 제15조 제1항 또는 제2항의 규정에 의한 추천을 받지 아니하고 외국음반 또는 외국비디오 물을 수입 또는 제조한 자
3. 제17조 제3항(누구든지 제1항의 규정에 의하여 심의를 받지 아니하거나 심의결과와 다른 내용의 비디오물을 판매·배포·대여 또는 시청제공하거나 판매·배포·대여 또는 시청제 공할 목적으로 진열 또는 보관하거나 불특정 다수인이 출입하는 장소에서 상영하여서는 아 니되며, 제 18조 제2항의 규정에 의한 시청등급을 위반하여 연소자에게 판매·배포·대여 또는 시청하게 하여서는 아니된다)의 규정에 위반한 자
4. 제조에 대한 정당한 권리를 가지지 아니하고 판매·배포·대여 또는 시청제공 등의 목적으 로 타인의 음반 또는 비디오물을 제조한 자

126) 한봉조, "통신망을 통한 음란물배포의 문제점과 대책", 「인터넷 불건전정보 방지세미나」발표논문(정보통신윤리위원회 주최), 1995. 9. 29

적용될 수 있을 것이다.[127] 그러나 인터넷은 전세계적으로 가동되는 것이고 망과 망이 유기적으로 연결되어 있어 물리적으로 차단하더라도 얼마든지 우회하여 정보를 습득할 수 있기 때문에 이러한 법적 규제나 기술적인 규제방법이 횡행하고 있는 인터넷상의 음란물접속을 차단하는데 과연 실효가 있을 것인가는 의문이다.

③ 컴퓨터통신이용사기

PC통신을 이용한 사기행위의 경우 형법상의 사기죄가 적용될 것이다. 또한 타인의 컴퓨터통신 ID 및 비밀번호를 도용하여 통신망에 음란CD 등의 판매광고를 낸 뒤 돈을 받아 가로채는 경우 사기 및 전산망법 위반에 해당한다.

④ 컴퓨터통신을 통한 명예훼손과 모욕

한편 PC통신에 설치된 전자게시판에 특정인을 상대로 한 허위사실의 유포나 폭언 등 명예훼손 및 모욕적인 내용들을 게재한 경우 형법상의 명예훼손죄 및 모욕죄에 해당한다. 사이버공간에 타인의 명예를 훼손하는 사실을 적시하는 것은 불특정 또는 다수인이 지실할 수 있는 상태에 두는 것이므로 공연성을 인정할 수 있기 때문이다. 한편 컴퓨터통신토론방에서 국회의원선거에 출마예정인 특정입후보자에 대하여 낙선시킬 목적을 갖고 구체적인 사실을 적시하여 비방한 경우 명예훼손죄가 성립하는 것은 물론 공직선거 및 선거부정방지법 제251조[128]에 의하여 처벌될 것이다.

정보통신범죄는 앞으로 더욱 다양하게 발생할 것으로 예상되므로 발생한 범죄의 단속만 할 것이 아니라 암호기술의 부정이용방지, 부정접속의 금지 등 정보통신과 관련된 범죄의 발생 자체를 방지하기 위한 제반조치와 범죄발생시 나타날 수 있는 절차법적인 문제의 해결을 망라한 소위 '정보통신범죄방지법'과 같은 통일적인 입법의 제정이 필요할 것으로 보인다.

2) 제도적 대응방안

정보통신범죄는 정보통신기술에 관한 최첨단 지식이 사용되며, 사이버스페이스의 시

127) 실제 지난 8월에는 서울 경찰청이 나우누리의 한총련 CUG(Closed User Group)를 국가보안 법 위반혐의로 폐쇄한 바 있다.

128) 당선되거나 되게 하거나 되지 못하게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 공연히 사실을 적시하여 후보자(후보자가 되고자 하는 자를 포함한다), 그의 배우자 또는 직계존·비속이나 형제자매를 비방한 자는 3년 이하의 징역 또는 500만원 이하의 벌금에 처한다. 다만, 진실한 사실로서 공공의 이익에 관한 때에는 처벌하지 아니한다.

간적, 지리적 무제약성이라는 특징 등으로 인하여 일반범죄와는 크게 다른 특성을 보이고 있다. 따라서 그 대응방법도 전통적인 범죄에 대한 대응방법과는 달리해야 할 것으로 보인다.

① 기술적 보안대책의 강구와 컴퓨터통신실명제의 도입

먼저 국내기업들은 사이버테러 등 정보통신범죄에 대처하기 위하여 인터넷 보안시설을 갖추거나 기업내 보안전담팀을 운영하는 등 자구노력을 기울여야 할 것이다. 또한 익명성을 이용하여 상대를 비방한다든지, 유언비어유포, 신종사기, 음란물유포 등의 행위를 막기 위하여 PC통신 가입자들의 신원확인과 등록ID를 실명으로 발급하는 등 '컴퓨터통신실명제'의 도입을 적극 검토할 필요가 있다.

② 민간 사이버경찰제도 내지 소비자모니터제도의 도입

사전검열은 언론의 자유와의 상충문제가 있으므로 자체적으로 불건전통신을 규제하는 등의 노력을 기울일 필요가 있으나[129] 컴퓨터통신회사의 모니터요원이 불과 100명 정도에 불과하여서 제대로 된 통제가 불가능하다는 점을 고려하여 민간단체가 소위 '사이버경찰'을 조직하여 온라인상의 불법행위를 감시, 고발토록 하는 제도도 생각해 볼 수 있다. 또한 인터넷상의 사기행위를 방지하기 위하여는 감시적발체제를 구축할 필요가 있는데 예를 들면 소비자모니터제도의 도입이 그 한 예가 될 것이다. 그리고 제보용인터넷주소를 만들어 인터넷으로 제보를 받는 방안을 고려해야 할 것이다.

③ 음란물 차단프로그램의 개발

인터넷상의 음란정보를 차단하기 위한 방안의 하나로 음란물차단프로그램을 개발하여 청소년의 음란물접속을 차단하는 것도 생각해 볼 수 있다. 현재 개발되어 있는 음란물 차단프로그램으로는 'NCA 패트롤(NCA patrol)'[130], '예스체커'[131] 등이 있으나 이

129) 정보통신윤리위원회는 IP(Imformation Provider)가 PC통신에 성인정보를 게재할 때 이를 사전심의하는 기능을 최근 폐지하고 기존심의규정내 심의세칙에 '음란성에 관한 기준' 항목을 추가하여 IP가 이를 참고로 음란성 여부를 자체 판단해 성인정보를 제공할 수 있도록 했다. 그러나 PC통신에 게재된 성인정보를 수시로 감시하는 사후심의기능은 더욱 강화하기로 하였다.(전자신문 1998. 10. 24)

130) 한국전산원이 개발하여 무료로 배포하고 있는 음란물차단프로그램으로서 음란물 등 불건전정보를 제공하는 인터넷사이트의 주소와 단어목록을 PC에 저장해 놓으면 이용자가 접속을 시도할 경우 자동으로 접속을 차단하는 기능을 한다. 또한 컴퓨터에 익숙한 자녀가 음란물을 보기 위해 임의로 이 프로그램을 삭제하면 자동으로 인터넷 이용기능을 정지시키는 보안기능도 갖추고 있다.

들은 모두 음란물을 찾아내는 도구로 활용될 가능성이 있고 새로 생기는 음란물홈페이지는 바로 차단하지 못하는 문제점을 안고 있다. 효과적인 음란물차단프로그램의 개발이 시급한 실정이다.

④ 사용자 신상정보유출의 방지

인터넷 내지 컴퓨터통신 이용사기에 대한 대책으로서 먼저 기망적 표시광고를 규제하는 등 법적 규제장치를 정비할 필요가 있고, PC통신을 통해 알게 된 사람들의 신상정보를 이용한 사기행위를 막기 위하여 사용자 신상정보유출을 막기 위한 제도적인 보완책이 마련될 필요가 있다 하겠다.

⑤ 연구조직과 전문수사조직의 설치 및 운영

점점 지능화·전문화되어 가는 정보통신분야의 첨단신종범죄에 효과적으로 대처할 수 있기 위하여는 첨단신종범죄에 대한 자료를 수집·분석하여 이에 대한 수사기법을 연구·개발하는 연구조직이 필요할 뿐만 아니라, 경찰청 및 지방청에 인터넷 및 컴퓨터 전문가들로 구성된 첨단신종범죄 전담수사팀을 설치·운영할 필요가 있다. 연구조직으로는 기존의 치안연구소를 활용하는 것이 바람직 하며 장기적인 계획하에 지속적인 연구를 하는 것이 필요하다. 또한 수사조직으로는 경찰청 및 각 지방청에 수사요원 중 컴퓨터관련지식을 갖추고 있는 자와 외부의 컴퓨터전문가로 구성된 첨단신종범죄 전담수사팀을 확대·설치하여 장래의 고도의 지능적인 수법의 첨단범죄를 독자적으로 수사할 수 있는 역량을 강화해야 할 것이다.

⑥ 전문수사관의 양성

정보통신범죄는 그 수사에 있어서 컴퓨터에 관한 전문적인 지식을 필요로 하므로 전문수사요원의 확보가 중요한 문제로 대두된다. 전문수사요원을 확보하기 위한 방안으로는 어느 정도 컴퓨터에 관한 지식을 갖춘 수사요원을 선발하여 교육하는 방법과 정보처리기사자격증 소지자 또는 컴퓨터관련분야 종사자를 채용하여 수사지식에 대한 교육을 하는 방법을 생각해 볼 수 있다. 그러나 자체 교육을 통한 수사인력의 양성에는 한계가 있다는 점을 고려하여 이들 분야의 전문적인 지식을 갖춘 사람들을 선발 또는 특채하여 전문수사관으로 양성하는 것이 장기적으로 보아 더 바람직할 것으로 생각된다.

---

131) 한국컴퓨터생활연구소가 개발보급에 나선 음란물차단프로그램으로서 인터넷상의 음란물접속을 막아주는게 아니라 하드디스크에 저장돼 있는 음란이미지를 체크 차단하는 소프트웨어이다.

⑦ 컴퓨터관련업계 및 컴퓨터전문가와의 긴밀한 협력체제의 구축

전문적인 지식을 갖춘 수사관을 양성하기 전까지는 고도의 전문기술을 가진 범죄자들의 지식수준을 따라잡기 어려운 것이 현실이며, 전문수사관이 양성되어도 모든 유형의 정보통신범죄에 적절하게 대처한다는 것도 어려운 일이다. 정보통신범죄의 예방과 진압 및 수사를 위해서 관련분야의 전문가들로 구성된 자문조직을 구축하여 두는 것은 물론 업계 등과의 긴밀한 협력체제를 구축해 나가도록 하여야 한다.

⑧ 국제적인 수사협력체제의 구축

마지막으로 정보통신범죄가 국경을 초월하여 발생하고 있다는 점을 고려하여 인터넷과 신기술을 이용한 범죄행위에 각국의 수사기관들이 수사 및 사법공조, 도주범죄인 인도 등 공동협력하는 방안을 모색해야 할 것이며, 나아가서는 수사체제를 국제범죄에 효과적으로 대응할 수 있도록 개편, 보완해야 하지 않을까 생각한다.

Ⅲ. 신종수법범죄의 추세전망과 대응방안

1. 신종수법범죄의 유형과 특징

가. 스캐너 등을 이용한 화폐·유가증권의 위조

1) 수법과 특징

① 수법

최근 복사기, 스캐너 및 프린터의 제작기술이 발전함에 따라 최첨단 칼라복사기, 스캐너 및 칼라프린터가 널리 보급되면서 이들을 이용하여 지폐와 유가증권을 위조하는 행위가 발생하고 있다. 종전의 통화·유가증권 위조행위는 인쇄방식에 의한 것으로 육안으로 위조 여부를 비교적 용이하게 판단할 수 있었으나 칼라복사기나 스캐너 및 칼라프린터를 이용하여 위조하는 경우에는 육안으로는 물론이고 전문가도 위조 여부를 식별하기가 대단히 어렵게 된다. 이러한 최신 위조수법의 하나는 컬러복사기를 이용하여 진본과 동일하게 복사하는 방법이다. 1995년에 일제 컬러복사기를 이용하여 10만원권 수표와 1만원권 지폐를 다량으로 위조한 사건이 발생한 바 있다.

또 하나의 수법은 수표를 컴퓨터 스캐너로 스캔닝한 후 이를 컬러프린터를 이용하여 위조하는 방법이다. 이러한 방법으로 10만원권 수표를 위조하여 사용한 대학생이 구속

된 바 있다.

② 특징

컬러복사기나 컴퓨터스캐너·컬러프린터를 사용하여 위조하는 행위의 특징은 대략 다음과 같다.

첫째는 위조된 화폐나 유가증권이 원본과 거의 동일하여 일반인은 물론이고 전문가도 위조 여부를 쉽게 인식하지 못하기 때문에 범죄를 발견하기가 대단히 어렵다는 점이다. 특히 컴퓨터스캐너와 칼라레이저 프린터를 이용하는 경우에는 더더욱 그렇다.

둘째의 특징은 위조화폐나 유가증권을 발견하였다고 하더라도 복사기나 스캐너·칼라프린터에 관하여 전문적인 지식을 갖춘 수사인력이 부족하여 수사하는데 어려움이 대단히 많다는 점이다. 1993년에 서울의 용산과 답십리에서 컬러복사기를 이용하여 위조한 10만원권 수표가 다량으로 발견되었으나 수사기관에서는 위조에 사용된 복사기의 기종만을 추정할 뿐 2년여가 지나서까지도 사건해결의 아무런 단서도 찾지 못하고 있으며, 1995년에 일제칼라복사기를 이용하여 10만원권 수표를 복사위조한 범인도 범행에 가담한 자 중의 1인이 친구들에게 위조수표를 보여주면서 "감쪽같지 않느냐"고 자랑한 것이 입에서 입으로 전해져 경찰관에게 알려짐으로써 검거되었다고 한다.

셋째의 특징은 이러한 첨단의 과학기술장비를 이용하여 위조하는 경우에는 아주 간단한 조작으로 손쉽게 다량으로 위조할 수 있다는 점이다. 그리하여 통화와 유가증권의 진정에 대한 일반사회의 신뢰를 크게 손상시켜 건전한 경제거래질서를 위태롭게 만들어 신용사회의 기반을 무너뜨릴 수 있다. 1995년에 일제 컬러복사기를 이용한 위조범일당은 수사결과 10만원권 수표 600여장과 1만원권 지폐 373장을 위조하였다고 한다.[132]

2) 적용법조

컬러복사기나 컴퓨터 스캐너와 컬러프린터를 이용하여 화폐나 유가증권을 위조하는 행위에 대하여는 형법상의 통화에 관한 죄[133] 와 유가증권에 관한 죄로 처벌할 수 있기 때문에 이러한 행위에 대하여 처벌의 공백은 없다. 그리고 위조한 지폐나 유가증권을 사용하는 행위는 행사죄에 의하여 처벌되는 바, 이와 관련하여 사람에게 사용하지 않고 현금자동입출금기(Automatic Teller's Machine)를 사용하여 입금하는 경우에 문제될

132) 문화일보 1995년 1월 16일자.

133) 특히 형법 제207조에 규정된 죄(통화위조·변조·행사·수입·수출)를 범한 경우에는 특정범죄가중처벌등에관한법률 제10조에 의하여 중하게 처벌된다.

수 있다.

위조화폐행사죄나 위조유가증권행사죄의 구성요건적 행위인 "행사"란 화폐나 유가증권을 거래상의 유통에 놓는 것으로서 반드시 사람에 대하여 사용할 것을 의미하지는 않으므로 위조된 화폐나 유가증권을 현금자동입출금기를 통하여 입금한 경우에도 행사죄에 의하여 처벌될 것이다. 따라서 이러한 위조행위와 관련하여 발생하는 형사법상의 문제점은 수사의 어려움이다.

3) 대응방안

① 수사전문가의 양성과 수사장비의 확보

칼라복사기나 컴퓨터 스캐너 및 칼라프린터와 같은 첨단과학기술장비를 이용하는 화폐·유가증권의 위조범죄에 효과적으로 대처하려면 수사기관의 노력은 물론 행정기관이나 첨단장비를 개발생산하는 기업의 노력이 종합적·체계적으로 결합되어야 할 것이다. 수사기관의 입장에서는 먼저 컬러복사기나 컴퓨터 스캐너·칼라프린터에 관하여 전문지식을 갖춘 수사전문가를 양성하여야 한다. 즉 위조에 사용된 장비가 복사기인지 프린터인지, 어떠한 기종의 장비를 사용하였는지를 식별하는 능력을 갖춘 수사요원의 확보가 필수적이다. 이를 위하여 수사연수소 등 수사요원 교육기관에서 위조수법에 대한 강의는 물론 복사기나 컴퓨터 스캐너·프린터의 원리 등 기술적인 내용의 강의를 개설할 필요가 있을 것이다.

나아가 위조에 사용된 기종을 식별할 수 있는 장비나 위폐감식기 등 첨단수사장비를 갖추어야 할 것이다. 이러한 방법으로 수사요원과 장비를 구비하지 않으면 민간전문가나 민간장비를 이용할 수밖에 없는데 이는 수사의 기동성과 신뢰성에 치명적인 결함을 낳게 될 것이기 때문이다.

② 칼라복사기 등에 대한 관리감독의 철저

전문적인 능력을 가진 수사요원의 양성과 첨단수사장비의 확보와 함께 위조행위에 사용될 수 있는 칼라복사기 등 첨단과학기술장비를 등록하도록 하고 이러한 장비가 위조범행에 사용되는지의 여부를 확인할 수 있도록 수시로 점검하는 행정적 조치를 강구하여야 할 것이다. 오늘날 복사기나 프린터 등이 널리 보급되어 개인까지도 이를 소유하고 있는 현실에 비추어 어떠한 종류의 칼라복사기 등을 등록·점검하여야 할 것인가는 칼라복사기 제조업체와 수사기관의 상호 협조하에 결정하여야 할 것이다.

③ 기술적 보안대책의 강구

아울러 화폐나 유가증권의 위조에 사용될 수 있는 컬러복사기 등을 개발·생산하는 기업들이 위조범행을 방지할 수 있는 기술적 조치도 함께 개발하려는 노력이 요구된다. 예컨대 이러한 기업들이 자신들의 제품에 화폐나 유가증권의 위조를 방지할 수 있는 프로그램을 개발·장착한다거나, 복사시에 복사기의 고유번호가 육안으로 식별되지는 않지만 위조화폐나 위조수표위에 찍히도록 하는 기술(일제 캐논복사기의 경우처럼)을 개발하여야 한다.

나아가 오늘날 현금입출금기(ATM)나 현금자동지급기(CD)가 널리 보급되면서 위조된 화폐나 유가증권이 이들 기계를 통하여 유통될 수 있으므로 이들 기계에 위조 여부를 인식할 수 있는 프로그램을 장착하여 입출금시 위조 여부를 검증할 수 있도록 하여야 한다. 실제로 1997년에 컴퓨터 그래픽을 활용하여 컬러프린터로 위조지폐를 만든 후 현금입출금기에 위조지폐를 입금하고 진정한 화폐로 바꾸어 인출한 사건이 발생한 바 있는데, 현금자동인출기나 현금자동입출금기가 더욱 많이 설치될 것을 생각한다면 장차 지폐의 위조행위를 조장할 위험이 매우 크다고 할 것이다.

나. 몰래 카메라에 의한 시청·촬영

1) 수법과 특징

① 수법

과학기술의 발전에 따라 초소형의 카메라가 개발·보급되면서 피촬영자가 전혀 알수 없는 아주 조그만 틈새에 이를 설치하여 폐쇄회로 TV를 통하여 관람하거나 촬영하는 행위가 발생하고 있다. 이는 개인의 사생활의 자유를 침해할 뿐만 아니라 타인에게 노출되기를 꺼리는 신체의 은밀한 부분을 노출시켜 수치심을 야기함으로써 행동의 자유를 크게 제약하는 결과를 가져온다. 특히 이러한 방법으로 은밀한 신체부위를 촬영한 테이프가 유통되기도 하여 건전한 성문화를 위태롭게 하고 있으며, 촬영자가 이러한 테이프를 무기로 피촬영자를 협박하여 재산상 이익을 취득하는 등 다른 범죄의 수단이 되기도 한다. 모 백화점이 비록 절도범행을 적발하여 백화점의 재산을 지키려는 목적을 가졌다고는 하지만 화장실에 감시용카메라를 설치하여 폐쇄회로 TV를 통하여 화장실 이용자들을 지켜 보았던 사건은 많은 사람을 경악하게 하였다. 또한 중견화가가 호텔 여자화장실 벽 아래 틈새로 초소형 카메라렌즈를 밀어넣거나 손가방에 카메라를 감춘 채 짧은 치마를 입은 여성들의 은밀한 부위를 촬영한 후 이를 판매하려다가 적발된 바 있으며, 독서실 주인이 여자화장실에 몰래 카메라를 설치한 사건도 있었다.

몰래 카메라의 수법은 초소형의 카메라를 촬영대상자가 출입하는 장소의 틈새에 설치하는 방법이다. 이를 장소부착형의 몰래 카메라라고 할 수 있을 것이며, 주로 폐쇄회로 TV를 통하여 관람하려는 자에 의하여 행하여진다.

또다른 수법은 몰래 카메라를 휴대하면서 짧거나 노출이 많은 의복을 악용하여 신체의 은밀한 부분을 촬영하는 방법이다. 이를 휴대형의 몰래 카메라라고 할 수 있다.

② 특징

몰래 카메라에 의한 관람·촬영행위의 특징은 다음의 세가지로 요약할 수 있을 것이다. 첫째의 특징은 이러한 행위는 주로 남성에 의해 이루어진다는 점이다. 이는 여성을 성상품화하는 사회의식과 많은 관련이 있다고 생각한다. 따라서 몰래 카메라의 촬영대상은 주로 여성들이며 설치장소 역시 여성만이 사용할 수 있는 장소라는 점을 또하나의 특징이라고 할 수 있다. 몰래 카메라 사용행위의 세번째의 특징은 대상자가 전혀 인식할 수 없고 그에 따라 이러한 행위를 발견하기가 대단히 어렵다는 점이다.

2) 적용법조

① 카메라등 이용 촬영죄

종래 몰래 카메라를 설치하여 이를 폐쇄회로 TV로 시청하거나 녹화하는 행위 자체를 처벌하는 규정이 없었다. 그러나 카메라를 몰래 설치하여 여성의 신체 등을 시청하거나 촬영하는 행위가 적발되면서 물의를 일으키자 이러한 행위를 처벌하여야 할 필요성이 제기되고 있었다. 그리하여 1998년 12월 28일 법률 제5593호로 성폭력범죄의처벌및피해자보호등에관한법률(이하 "성폭력특별법"이라 함)을 개정하여 몰래 카메라를 설치·촬영하는 행위를 처벌할 수 있는 규정을 신설하게 되었다. 즉 카메라 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영한 자를 5년이하의 징역 또는 1천만원이하의 벌금에 처하도록 하였다(성폭력특별법 제14조의2).

이 규정에 의하여 앞으로 카메라를 설치하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 몰래 촬영하는 행위는 성폭력특별법상의 카메라등이용촬영죄로 처벌된다. 동죄는 사람의 성적 욕망을 유발하거나 만족시킬 목적을 필요로 하는 범죄(목적범)가 아니며, 촬영대상인 타인의 신체가 성적 욕망이나 수치심을 유발할 수 있는 부분이면 성립한다. 따라서 반드시 성적 욕망을 유발하거나 만족시킬 목적이 아닌 다른 목적, 예컨대 촬영내용을 폭로하겠다고 협박하여 피촬영자를 강요하거나 재산상 이익을

얻을 목적으로 몰래 카메라를 설치하여 촬영한 경우에도 본죄로 처벌할 수 있다. 나아가 방범목적을 위하여 몰래 카메라를 설치·촬영하는 경우라도 화장실 등에 설치하여 드러내기 싫어하는 신체의 은밀한 부위를 촬영하는 행위도 본죄에 의하여 처벌될 수 있을 것이다. 본죄에는 몰래 "카메라" 뿐만 아니라 "기타 이와 유사한 기능을 갖춘 기계장치"를 이용하여 촬영하는 행위도 포함된다.

본죄의 미수범은 처벌되므로(제12조) 카메라 등을 설치한 단계에서 적발된 자도 당연히 처벌된다. 이와 관련하여 본죄의 실행의 착수시기가 문제될 수 있는데, 적어도 카메라를 설치하려고 한 때에 실행에 착수하였다고 할 것이다. 따라서 몰래 카메라를 설치하기 위하여 설치할 장소에 들어간(침입한) 것만으로는 아직 실행에 착수하였다고 할 수 없으므로, 주거침입죄 등의 성립은 별론으로 하고 카메라등이용촬영죄로는 처벌할 수 없을 것이다.

나아가 법인의 대표자, 법인 또는 개인의 대리인·사용인 기타 종업원이 법인 또는 개인의 업무에 관하여 몰래카메라 등을 설치하여 촬영한 경우에는 그 행위자를 처벌하는 외에 그 법인 또는 개인에 대하여도 벌금형을 과하여 처벌할 수 있다(법 제37조). 이는 법인의 대표나 피용인 등의 법위반행위에 대하여 법인이나 사용인에게 형사책임을 물음으로써 선임·감독의무의 철저한 이행을 담보하기 위한 규정이라고 할 것이다.

② 주거침입죄

타인의 주거 등 건조물에 들어가 몰래 카메라를 설치한 경우 주거침입죄의 성부가 문제된다. 물론 주거자의 부재중에 타인의 주거 등에 들어가 몰래 카메라를 설치하였다면 당연히 주거침입죄에 해당한다. 왜냐하면 타인의 주거 등에 몰래 카메라를 설치하여 사람의 은밀한 부분을 엿보려는 것은 헌법이 보장하고 있는 사생활의 자유를 침해하는 불법적인 행위이고 이러한 불법의사를 알았더라면 설치자의 출입을 주거자가 허락하지 않았을 것이기 때문이다.

그리고 강도·절도 등 범죄를 범하려는 불법적인 목적을 숨기고 주거자의 승낙을 얻어 출입한 경우 주거자의 추정적 의사에 반하므로 "침입"에 해당하다고 보는 다수설·판례에 의하면, 타인의 주거 등에 들어가 몰래 카메라를 설치한 행위는 주거침입죄로 처벌된다. 그러나 주거자의 현실적인 승낙이 있었다면 설사 범죄목적으로 출입하였다고 하더라도 승낙은 유효하므로 침입이 될 수 없다는 반대의 견해에 의하면, 몰래 카메라를 설치하려는 의도를 숨기고 주거자의 현실적인 승낙을 얻어 들어갔다면 주거침입죄

의 구성요건해당성이 부인되어 동죄로 처벌할 수 없게 된다.

이에 반하여 자신의 건조물에 몰래 카메라를 설치하여 출입자들을 대상으로 한 경우에는 주거침입죄로 처벌할 수 없다. 왜냐하면 주거침입죄의 객체인 '사람의 주거 등'은 '자기 이외의 타인의 주거 등'을 의미하기 때문이다. 또한 침입은 신체적 침입을 의미하는데 몰래 카메라를 설치하여 폐쇄회로 TV로 시청하거나 이를 촬영하는 행위는 침입에 해당하지도 않는다. 따라서 자기 소유 또는 자기 관리하의 건조물에 몰래 카메라를 설치하는 행위는 주거침입죄로는 처벌할 수 없다.

③ 성풍속에 관한 죄

몰래 카메라를 설치하여 그 내용을 녹화한 경우 그 녹화테이프는 통상 음란한 물건 내지 필름에 해당할 것이기 때문에 형법상의 "성풍속에 관한 죄"에 의하여 처벌할 수 있을 것이다. 즉 몰래 카메라에 의한 녹화테이프를 반포·판매·임대·공연전시·상영한다면 음화반포등죄(형법 제243조)로, 이러한 행위에 공할 목적으로 몰래 카메라에 의하여 녹화하였다면 음화제조죄(형법 제244조)로 처벌될 것이다. 그러나 몰래 카메라로 녹화한 테이프를 촬영자 혼자 시청하였다거나 이를 위하여 녹화하였다면 음화반포죄나 음화제조죄에 의하여 처벌할 수 없게 된다.

3) 대응방안

① 처벌규정의 보완

몰래 카메라를 설치하는 과정에서 타인의 주거 등에 주거자의 의사에 반하여 들어갔다면 주거침입죄로, 몰래 카메라에 의하여 신체의 은밀한 부분을 녹화한 테이프를 반포·판매하거나 일정한 목적(반포·판매 등)을 갖고 몰래 카메라로 이러한 녹화테이프를 만드는 행위를 음화반포죄 또는 음화등제조죄로 처벌할 수 있다. 그러나 이러한 처벌은 우회적인 방법에 불과할 뿐 몰래 카메라에 의한 성적 욕망의 충족이나 수치심의 야기 또는 사생활침해의 본질에 적절하게 대응하지 못할 뿐만 아니라, 자신의 건물 등에 몰래 카메라를 설치하여 이를 시청하거나 자신이 시청하기 위하여 몰래 카메라로 타인의 은밀한 부분을 촬영(녹화)하는 행위는 처벌할 수 없었다.

그러나 오늘날 몰래 카메라에 의하여 사생활이 침해될 수 있는 상황이 증가하고 있고 이에 대하여 일반 국민이 느끼는 위험성이 매우 심각하므로 이러한 처벌의 공백을 방치하여서는 아니된다. 이러한 상황에서 성폭력특별법을 개정하여 몰래카메라나 비디오를 설치하여 은밀하게 촬영하는 행위를 처벌하는 새로운 규정을 둔 것은 적절하다고

본다. 다만 동죄는 카메라 등을 몰래 설치하여 촬영까지 한 행위를 처벌대상으로 하기 때문에, 촬영하지 않고 폐쇄회로 TV를 이용하여 시청하는 행위는 처벌할 수 없다는 문제점이 있다. 촬영이라는 용어가 시청을 포함한다고 해석할 수 없기 때문이다. 이러한 처벌의 공백은 몰래 카메라의 위험성을 인식하고 이를 처벌하기 위하여 신설된 규정을 거의 무의미하게 만들게 될 것이므로 "촬영" 다음에 "시청"을 추가하는 내용으로 시급히 보완하여야 한다.

② 사생활보호에 대한 사회적 인식의 제고

과거와는 달리 오늘날 개인의 사생활은 대단히 중요한 보호영역으로 인식되고 있다. 이것은 사회의 급속한 개인주의화 경향에 따라 사적 영역의 확보욕구가 강하여졌을 뿐만 아니라 과학기술의 발달에 따라 개인의 사생활영역을 피해자 몰래 들여다 볼 수 있는 첨단장비들이 개발·보급되었기 때문이기도 하다.

나아가 정보화사회의 진전에 따라 개인의 모든 정보를 아주 손쉽게 파악할 수 있는 길이 열려져 있다. 이러한 상황을 고려하여 타인의 사생활영역을 보호하는 것이 오늘날 정보화사회의 중요한 과제가 되고 있으며, 그에 따라 몰래 카메라를 설치하여 타인의 은밀한 생활영역을 엿보는 행위는 중대한 법익침해행위가 된다는 인식을 신문·잡지 등 언론매체와 각종의 교육기회를 활용하여 사회에 널리 확산시킬 필요가 있다.

다. 첨단장비를 이용한 도청

1) 수법과 특징

① 수법

도청은 타인간의 대화를 그들의 동의 없이 청취하거나 녹음하는 것으로서 과학기술의 발전에 따라 손쉽게 도청이 가능하게 되었다. 이러한 도청은 개인의 대화비밀을 침해하여 인간의 자유로운 인격의 발전을 위협하는 행위이다. 과거의 도청은 대화하는 사람과의 근접한 장소에서 행하여지거나(대화도청) 전화선에 도청장치를 부착하여 행하여졌고(유선도청) 그런만큼 도청하는 자는 발각당할 위험이 상당하였고 도청당하는 사람은 그러한 사실을 비교적 용이하게 감지할 수 있었다. 그러나 과학기술이 날로 발전함에 따라 초소형의 무선도청기가 개발·보급되어 일반 개인도 마음만 먹으면 별 어려움 없이 원거리에서 타인간의 대화나 전화통화를 도청할 수 있게 되었다. 나아가 정보통신기술이 비약적으로 발전하면서 개인휴대전화 등 새로운 무선통신매체가 널리 활용되고 있으며 이에 대한 도청도 문제되고 있다(무선도청).

유선도청은 송수화기나 전화선에 도청장치를 설치하여 타인간의 대화내용을 알아내거나 녹음하는 수법으로 행하여지며 이러한 방법으로 도청하면 통화의 감이 떨어지거나 이상한 잡음이 나서 통화당사자들이 누군가가 엿듣고 있다는 생각을 하게 된다.

개인휴대전화 등 무선통신매체에 대한 도청도 —기술적으로 유선도청 보다는 어렵지만— 가능하다. 무선도청의 방법에는 두가지가 있다. 하나는 도청대상자의 휴대전화 단말기에 입력된 고유번호(이를 "헥사코드"라고 함)와 동일한 번호를 다른 단말기에 똑같이 입력하여 도청하는 방법이다. 이렇게 하면 도청대상자에게 전화가 걸려올 때마다 신호음이 같이 울리게 되므로 대화내용을 알아낼 수 있게 된다. 이러한 헥사코드이용도청은 도청대상자의 단말기와 같은 기지국 안에 있어야 가능하므로 가까운 거리에서만 도청할 수 있게 된다.

두 번째의 무선도청방법은 올밴드수신기라는 특수한 통신기기를 이용하는 것이다. 올밴드수신기란 무선통신매체의 주파수가 맞으면 동일한 주파수를 사용하는 모든 무선통신기의 대화내용을 모두 수신할 수 있는 장치이다. 따라서 도청대상자의 휴대전화와 주파수를 동일하게 하여 놓으면 그의 대화내용을 엿들을 수 있게 된다. 이러한 올밴드수신기이용도청은 도청대상자의 주파수를 맞추기가 어렵고 아날로그방식에 대하여만 가능하다.

② 특징

도청의 특징의 하나는 통신매체에 대한 전문적인 지식이 필요하다는 점이다. 특히 무선도청의 경우에는 헥사코드를 이용하여 도청하려면 헥사코드라는 것이 있다는 점과 도청대상자의 단말기의 헥사코드를 알아야 한다. 이는 결국 이동통신회사의 직원이나 대리점의 직원으로부터 입수할 수밖에 없으므로 도청하려는 자는 이들과 공모하거나 이들을 속여 몰래 알아내는 것이다. 마찬가지로 올밴드수신기를 이용하여 도청하는 경우에도 주파수를 알아야 하므로 이에 대한 전문적인 지식이 필수적이다.

도청의 또다른 특징은 심부름센타 등과 같은 개인용역업체에 의하여 배우자의 불륜이나 채무자의 소재파악 등에 관한 증거를 잡기 위하여 행하여진다는 점이다. 보도에 의하면,[134] 통신보안전문가가 "전화번호부나 심부름센터의 태반은 도청을 주업무로 한다"고 말한바 있고, 실제로 대여섯 군데의 용역업체에 문의해 본 결과 도청일을 하지 않는다고 한 업체는 한 곳밖에 없었다고 한다. 끝으로 몰래 카메라의 경우와 동일하게

134) 뉴스플러스 제134호(1998/05/21) 29면.

대상자가 전혀 인식할 수 없고 그에 따라 이러한 행위를 발견하기가 대단히 어렵다는 점도 도청의 특징이라고 할 수 있다.

2) 적용법조

통신비밀을 보호하고 통신의 자유를 신장하기 위하여 통신 및 대화비밀을 침해하는 행위를 처벌하기 위하여 통신비밀보호법이 제정되어 시행되고 있다. 이 법은 우편물의 검열, 전기통신의 감청 또는 공개되지 아니한 타인간의 대화를 녹음 또는 청취하거나 그 취득한 통신 또는 대화의 내용을 공개하거나 누설한 자를 처벌하는 규정을 두고 있으며(통신비밀보호법 제16조 1호), 이러한 행위의 미수범도 처벌한다(동법 제18조).

통신비밀보호법상의 "전기통신"이라 함은 유선·무선·광선 및 기타의 電磁的 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말하므로(동법 제2조 3호) 유선전화나 휴대전화도 여기에 해당할 것이다. 그리고 통신비밀보호법상의 "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 電子裝置·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·共讀하여 그 내용을 지득 또는 採錄하거나 전기통신의 송·수신을 방해하는 것을 말하므로(동법 제2조 7호), 도청은 동법상의 감청에 해당된다. 따라서 현행법상 첨단장비를 이용한 도청에 대하여는 처벌의 공백이 없다.

3) 대응방안

① 수사전문인력과 장비의 확보

수사기관의 입장에서는 도청피해에 대한 신고가 있을 때 이의 정확하게 판단할 수 있는 도청탐지장비와 같은 첨단수사장비와 전문인력을 확보하고 있어야 한다. 이를 위하여는 예산을 확보하고 통신관련교육기관에의 위탁교육 및 수사관에 대한 계속교육의 프로그램을 개발하여 시행하는 방안을 강구하여야 할 것이다.

② 도청장비에 대한 관리감독의 철저

첨단장비를 이용하는 도청에 대하여는 기존의 도청과 마찬가지로 통신비밀보호법에 의하여 처벌되므로 발각된 도청에 대하여 처벌할 수 없는 경우는 없다. 오히려 도청에 관련된 형사법적 문제는 이러한 불법적인 도청을 어떻게 효과적으로 억지할 수 있느냐이다. 이를 위하여는 먼저 사전적인 조치로서 도청에 악용될 수 있는 장비에 대한 관리를 철저히 하여 일반인이 이러한 장비를 마음대로 입수하지 못하도록 하여야 한다. 아울러 권한 있는 기관이 보유하고 있는 도청장비에 대하여도 보관사용에 대하여 엄격하

게 통제함으로써 그것이 남용되지 않도록 유의하여야 한다. 이와 함께 난립하고 있는 용역업체에 대한 지도단속을 강화하여 이들이 의뢰인들의 목적(불륜적발, 소재파악 등)을 달성하기 위하여 불법적으로 도청하는 일이 없도록 해야 한다.

③ 도청행위에 대한 사회적 인식의 제고

도청 역시 몰래 카메라와 마찬가지로 심각한 범죄행위라는 점에 대한 인식을 제고시킴으로써 도청에 대한 경각심을 갖도록 할 필요가 있다. 이를 위하여는 신문이나 잡지 등 언론기관과 각종 교육기관에서 지속적인 관심을 갖고 도청의 불법성에 대하여 홍보와 교육을 실시하여야 할 것이다. 그리고 수사기관이나 정보기관 등 국가기관이 통신비밀보호법에 의하지 아니한 불법감청을 하지 않아야 함은 두말할 필요가 없다.

라. 전화방을 통한 윤락알선 및 전화이용매춘

1) 수법과 특징

소위 '전화방'이란 전화회선을 이용하여 불특정한 남녀간에 대화의 기회를 제공하는 영업으로서 일본의 텔레크라(テレクラ)영업을 모방하여 최근에 우리나라에도 등장한 영업형태이다. 그 영업방식으로는 전화방영업소를 설치하고 전화가 가설된 개인용방에 이용객을 입장시킨 후 이용료를 받는 유형과 이용객에게 필요한 전화번호와 비밀번호 등을 주어서 전화를 걸게한 후 설치된 전화연결용 컴퓨터단말기로 전화를 연결시켜 주는 유형 그리고 이용객에게 전용전화로 전화를 걸게 하여 음성축적장치에 등록된 이성의 메시지를 듣게 하는 유형 등이 있다. 일반적으로 남성이용객의 경우에는 이용료를 직접 받거나 은행계좌로 미리 입금받고 회원으로 가입시키는 방식을 취하는 반면, 여성이용객의 경우에는 이용료를 수신자가 부담하는 080서비스를 이용하도록 하게 하여 회원가입절차없이 무료로 폰팅에 참가하게 하는 것이 보통이다. 경우에 따라서는 미리 여성이용객을 가장한 아르바이트여성을 수당을 주고 고용하는 경우도 있다.

그런데 '전화방'영업은 그 동안 남녀간의 건전한 교제를 위한 대화의 도구로 이용되기보다는 오히려 그 익명성으로 인하여 남녀 모두 성적 흥미를 가지고 이용하는 것이 보통이며, 따라서 음란통화 등 불건전한 통신문화를 확산시키는 도구로 악용되어 온 것이 현실이다. 더구나 문제는 전화방에 전화를 거는 여성들이 대부분 가정주부나 10대들인데다가 외설스런 통화로만 끝나지 않고 부업이나 아르바이트의 대상으로서 윤락행위로까지 이어지고 있다는 점에서 그 폐해가 매우 크다고 할 수 있다. 또한 최근에는 윤락녀들이 전화방을 접속수단으로 이용하여 매춘을 하는 신종매춘이 나타나고 있으며[135],

전화방을 통하여 알게된 여성을 성폭행하거나 성관계를 가진 뒤 이 사실을 공개하겠다고 협박하여 금품을 갈취하는 등 범죄의 수단으로 악용되고 있기까지 하여 큰 사회문제로 되고 있다.

이러한 전화방의 폐해가 늘면서 당국이 전기통신사업법을 근거로 전화방에 대한 단속을 강화하자[136], 최근에는 별도의 영업장소가 없이도 시내전화를 통하여 남녀를 직접 연결해주는 소위 '폰팅시스템'이라는 장치를 일본으로부터 들여와 영업하는 등 그 수법이 갈수록 교묘해지고 있다.[137] 폰팅시스템은 가정집에 전화연결용 컴퓨터단말기를 설치하여 남녀간의 전화를 연결해주기 때문에 '주택전화방'이라고도 불리며, 전화방에 가지 않고도 집이나 사무실에 앉아서 상대방과 통화할 수 있다는 이점 때문에 종전의 전화방보다 더욱 성행하고 있는 실정이다. 그리고 이용자의 신분이 노출되지 않다 보니 회사원과 주부뿐만 아니라 중, 고등학생들에게까지 급속히 확산되어 청소년 탈선행위를 더욱 부추기고 있다. 이러한 형태의 전화방의 특징으로는 영업장소없이 불특정한 장소에서 영업을 하기 때문에 광고를 주된 영업수단으로 한다는 점이다. 따라서 이들 전화방업자들은 지역생활정보지에 폰팅광고를 내거나 호객꾼(속칭 삐끼)들을 동원해 회원번호와 비밀번호를 적은 쿠폰, 소위 '폰팅티켓'을 편의방이나 유흥주점에서 파는 수법을 이용한다.[138]

문제는 이들이 주택가로 숨어들어 1-2개의 전화번호만 갖고 영업을 하기 때문에 정확한 숫자도 파악할 수 없는 등 단속에 어려움이 있으며, 적발한다고 하여도 전기통신

135) 최근 청량리나 천호동 등지의 속칭 '텍사스촌' 유흥업소에 대한 검찰과 경찰의 단속이 강화되어 일부 업소가 폐쇄되면서 윤락녀들이 전화방을 이용하여 매춘을 하는 사례가 발생하고 있다.

136) 그 동안 전화방의 설립 및 영업자체를 규제하는 법규가 없어 단속의 어려움이 있었으나, 최근 서울지법은 전화방 업주들이 한국전기통신공사를 상대로 낸 전화서비스이용 방해금지 가처분 신청사건에 대해 전화방영업형태는 전기통신사업법에 위반된다는 취지로 기각하여 한국통신측의 통화정지 조치는 정당하다고 판결함으로써 전화방에 대한 통화를 정지시킬 수 있는 법적 근거를 확보하게 되었다.

137) 폰팅시스템은 97년 4월 첫 도입된 이래 급속히 확산되어 97년 10월까지 전국에 1백 여개가 성업 중인 것으로 파악되고 있다.(문화일보 97. 10. 11)

138) 예를 들면 신림동 일대에서 거래되는 폰팅티켓은 명함 2배의 크기로 겉면에 '텔레폰 미팅 카드'나 'OK카드'라고 적혀 있고 뒷면에는 음성사서함 전화번호와 티켓의 이용방법이 상세히 적혀 있다. 신종 전화티켓은 기존의 전화방이 시간당 1만 여원의 입장료를 받고 남성들을 각 방에 입장시켜 통화하던 것과는 달리, 돈을 내고 티켓을 구입하여 회원번호를 받으면 가정이나 사무실 등 어디서나 상대 여성과 폰팅이 가능하도록 되어 있다.

사업법 제32조의 2[139]에 위반된 행위를 한 전화방업자에 대하여는 500만원 이하의 벌금형(동법 제74조)밖에 선고할 수 없어 단속의 실효를 거두기 어려운 실정이다. 따라서 전화방형태의 영업행위에 대한 법적, 제도적 대응책의 마련이 시급하다고 할 수 있다.

2) 대응방안

① 영업규제를 위한 법적 근거 마련

전화방 등 신종풍속영업에 대하여 탄력적으로 대응하기 위하여는 풍속영업에 전화방을 포함시키거나 풍속영업의 범위를 업종명칭열거방식에서 영업형태나 방법에 대해 포괄적으로 설명하는 방식으로 개정해야 한다는 견해가 있을 수 있다. 그러나 앞에서 보았듯이 전화방영업은 그 영업방식의 특성상 음란통신 등 불건전한 통신문화를 확산시키고 매춘에 이용되는 등 그 폐해가 매우 크다고 할 수 있다. 더구나 여성이용객의 경우 080서비스를 통하여 무료로 폰팅에 참가하고 있기 때문에 청소년의 이용을 막을 길이 없으며, 소위 폰팅시스템을 이용한 전화방의 경우에는 남성이용객에 있어서도 그가 청소년인가의 여부를 확인할 방법이 없어 청소년의 탈선행위를 조장하는 등 청소년에게 유해한 영향을 미치는 영업형태라는 점에서 전화방영업 자체를 규제할 필요가 있다고 하겠다. 그런데 현재 검찰과 경찰은 전기통신사업법을 근거로 이를 단속하고 있으나 법정형이 벌금형밖에 규정되어 있지 않아 효과적인 단속을 못하고 있는 실정이다. 따라서 전화방영업을 효과적으로 규제할 수 있는 법적 근거를 마련할 필요가 있으며 그 법정형도 상향조정할 필요가 있다고 하겠다.[140]

② 전화번호의 역추적을 통한 단속

소위 폰팅시스템을 이용한 전화방의 단속에 있어서는 영업장소없이 불특정한 장소에서 1, 2개의 전화번호만 갖고 영업을 하기 때문에 단속에 어려움이 없지 않겠지만, 전화방업자들이 영업수단으로서 스포츠신문이나 생활정보지 등에 폰팅광고를 내거나 호

139) 누구든지 전기통신사업자가 제공하는 전기통신역무를 이용하여 타인의 통신을 매개하거나 타인의 통신용에 제공하여서는 아니된다.

140) 최근 PC통신에 '부부교환코너'를 설치하는 등 반사회적 행태가 빈발하고 있어 PC통신을 이용한 음란성폰팅을 주선한 사람에 대한 벌칙을 대폭 강화한 전기통신사업법개정안이 국회에 제출되었다(조선일보 1998. 10. 19). 전기통신사업법개정안에 따르면 전기통신부장관의 허가를 받지 않고 전기통신을 이용해 매개행위를 하는 경우 벌금 500만원인 현행벌칙을 '5년 이하의 징역 또는 5천만원 이하의 벌금'으로 대폭 강화하였고, 또 전기통신사업자가 이를 방조하고 있다고 보고 이에 대한 처벌규정도 신설하였다.

객꾼을 동원해 소위 폰팅티켓을 파는 수법을 이용한다는 점을 고려할 때 이들 폰팅광고나 폰팅티켓의 전화번호에 대한 역추적을 통하여 단속을 하여야 할 것이다.

마. 보험사기(특히 교통사고관련 보험사기를 중심으로)

1) 수법과 특징

보험사기란 보험금의 편취를 목적으로 보험계약을 체결한 후 보험사고를 고의적으로 유발·위장하거나 손해액을 과대조작하여 과대한 보험금을 청구하는 등 보험제도를 악용하여 보험금을 의도적·악의적으로 사취하는 일체의 부정행위를 말한다. 이러한 보험사기는 보험사기피해자들의 생명이나 재산에 피해를 줄 뿐만 아니라 보험회사와 다수의 선의의 가입자들에게 그 피해가 돌아가게 된다는 점에서 보험제도의 정착을 저해하는 범죄라고 할 수 있으며, 최근에는 그 수법이 더욱 다양해지고 지능화되고 있다는 점에서 새로운 수법의 범죄유형에 포함시킬 수 있을 것으로 보인다. 특히 IMF경제체제 이후 실직자가 급증하면서 보험금을 노린 살인, 방화, 교통사고 등과 같은 고의적인 보험사기범죄가 급증하고 있다는 점[141]을 고려할 때 이에 대한 효과적인 대응책의 마련이 시급한 실정이라고 할 수 있다.

보험사기는 일반적으로 보험고객이 보험회사를 상대로 사기를 벌인 경우, 즉 '고객범죄'의 일종으로 발생하는 것이 보통이지만, 보험회사직원이나 보험업무 대행기관이 고객이나 보험회사를 상대로 기망행위를 펼치는 경우도 있다.[142] 후자의 경우는 예를 들면 보험회사직원이 이미 다른 보험에 가입하고 있던 보험고객에게 기존에 가입한 보험을 해약하고 조건이 더 좋은 다른 보험에 가입할 것을 권유한 뒤 고객으로부터 보험종류 변경에 필요한 인감 및 인감증명을 교부받는 등 이에 필요한 절차를 전적으로 위임받은 것을 기회로 보험을 해약하고 보험불입액을 편취하거나 보험불입액을 담보로 융자받아 이를 편취하는 경우, 고객에게 일시납으로 가입하면 더 높은 이자를 받을 수 있다

141) 1998년 3월 15일 충남 서천에서는 주부 이모씨가 남편명의로 생명보험에 가입해 놓고 남편을 독살하려다 경찰에 적발됐고, 3월 4일에는 서울 천호동의 강모씨가 부인앞으로 4종류 1억 5천만원의 생명보험에 가입한 뒤 부인을 살해하였다. 지난 1월에는 서울 문정동의 김모씨가 5억원의 보험금을 노려 자신이 경영하는 공장에 불을 질렀고, 지난 3월 의정부에서는 고의로 교통사고를 내 2억 5천만원의 보험금을 타낸 보험사기단이 검거됐다(국민일보 1998. 3. 23).

142) 김준호/차종천/김성언, 「사기범죄의 실태에 관한 연구」, 한국형사정책연구원, 1993, 87-88면 참조.

고 속이고 교부받은 일납보험금 중 일부를 고객 몰래 계약조건을 월납으로 변경한 후 이를 편취하는 경우, 보험에 가입하면 주택을 담보로 대출받도록 해 주겠다고 고객을 속인 후 기탁한 보험선납금을 편취하는 경우, 보증보험가입자를 모집하여 보증보험회사의 지점에 알선하고 그 서류접수를 대행하는 일을 전담하는 보증보험회사의 대리점을 운영하는 자가 전문보험브로커들과 짜고 보증능력이 없는 전문보증인들을 내세워 보증보험계약을 체결하게 한 다음 보험가입자들은 피보험자인 리스회사로부터 리스받은 물건을 편취하는 경우 등을 들 수 있다.

그러나 보험사기는 보험고객이 보험회사를 상대로 행하는 전자의 경우가 그 전형적인 것이라고 할 수 있는데 그 수법을 살펴 보면 대체로 다음과 같다. 가장 대표적인 수법은 보험계약을 체결할 때 보험금을 의도적으로 높게 책정하거나 중복하여 보험에 가입한 다음 이 사실을 은폐한다든지 하여 사기로 보험계약을 체결하고, 보험사고를 고의적으로 유발하거나 발생하지도 않은 보험사고를 발생한 것처럼 위장·날조하는 수법이다. 대부분의 보험사기가 이러한 수법으로 이루어지고 있는 것으로 보이며 가장 문제가 되는 수법이라고 할 수 있다. 이러한 보험사기는 단독으로 행해지는 경우 보다 조직적으로 범행을 하는 경우가 많으며, 이 과정에서 보험회사직원이나 의사, 자동차수리업자 등이 가담하기도 한다. 특히 위장교통사고와 관련된 보험사기는 최근 점점 조직화되는 추세에 있고 그 수법도 날로 지능화되고 있다는 점에서 주목해야 할 것으로 보인다. 위장교통사고 보험사기는 보험금 지급절차가 단순한 보장성 보험의 허점을 노려 조직적으로 교통사고를 조작해 보험금을 편취하는 범죄라고 할 수 있다. 즉 보장성 보험은 소액일 경우 진단서, 입·퇴원확인서 등만 제시하면 바로 보험금을 지급하도록 되어 있는데, 위장교통사고 보험사기단들은 이 점을 이용하여 중앙선침범, 신호위반 차량 등 교통법규위반차량을 골라 고의로 사고를 낸 뒤 상대방의 법규위반사실을 약점으로 잡아 고액의 합의금을 받아내거나 병원에 위장입원해 보험금을 편취하는 수법을 사용한다.[143] 이들은 보험회사들이 같은 보험상품에 중복가입해도 모른다는 사실을 이용하여 여러 개의 운전자보험에 가입한 뒤 고의로 교통사고를 내어 거액의 보험금을 편취하고 있고, 이 과정에서 피해차량에 타고 있지 않은 사람을 탑승자로 신고하거나 피해자를 다른 환자로 바꿔치는 수법을 사용하기도 하며, 심지어 일반인들도 가벼운 디스크징후를 보

143) 일방통행로에서 사고시 무조건 가해차량으로 처리되는 역주행차량과 고의로 충돌사고를 낸 뒤 보험금을 타내는 것도 보험사기범이 즐겨쓰는 수법이다.

이는 경우가 많은 점에 착안, 1차진단기간 만료후 병원측에 정밀재감정을 요구하여 이 같은 증상이 나타나면 한시장애진단서를 끊어 보험액을 불리는 수법도 사용하고 있다. 그런데 최근에는 아예 사고도 내지 않은 채 교통사고 시나리오를 사전에 만들어 놓고 가해자, 피해자, 동승자 등의 역할을 분담시킨 뒤 보험회사에 신고하여 보험금을 타내는 수법까지도 등장하고 있다. 이들은 위장교통사고를 연출한 뒤 교통사고 상습피해자라는 의혹의 눈초리를 피하기 위해 가해자와 피해자 등의 역할을 서로 번갈아 바꾸기도 한다. 이와 같은 보험사기가 가능한 것은 병원이 이에 방조 내지 가담하였기 때문이라고 할 수 있는데, 병원은 치료비 수입을 올릴 수 있어서 환자가 입원하겠다고 버티는 경우 병원도 이익이 되기 때문에 굳이 말리지 않아 이러한 사기행위를 방조하고 있고, 진료비를 챙기고 입원하지도 않은 환자에게 서류상으로만 입원한 것처럼 꾸미거나 가짜환자에게 장기입원에 필요한 장애진단서를 떼주는 등 허위, 과장진단서를 발급해 이러한 범행에 가담하는 경우도 발생하고 있다. 한편 사고경위의 정확한 조사가 어려운 해외 여행보험의 맹점을 이용하여 외국에서 고의로 교통사고를 내고 거액의 보험금을 타내는 사례도 발생하고 있다.

그밖에 교통사고와 관련하여 행해지는 보험사기수법으로는 보험사고가 발생한 이후에 보험에 가입하고 보험사고 발생일시를 보험가입일 이후로 허위신고하거나, 보험에 가입하지 않은 차량의 가해사고를 보험가입차량의 사고로 위장하는 등 보험대상이 아닌 운전자 및 차량을 바꿔치기하는 수법과 허위로 차량도난신고를 한 뒤 보험금을 챙기는 수법이 있다. 전자의 수법에 해당하는 실제 사례로는 교통사고를 낸 차량운전자가 보험료미납으로 보험기간이 만료되었기 때문에 보험금을 탈 수 없게 되자 보험회사에 보험료를 송금한 후 사고날짜를 허위신고하여 보험금을 타내려 한 경우라든지 자신의 공장에서 면허없는 직원이 지게차를 운전하다 동료직원을 친 것을 면허를 가진 다른 직원이 운전한 것처럼 허위신고해 보험금을 타내려 한 경우 및 보험에 들지 않은 차량으로 운전하다 행인을 치는 사고를 내고서는 보험에 가입한 차량으로 사고를 낸 것처럼 위장신고한 경우를 들 수 있다. 이러한 유형의 행위들은 사고로 인한 손해를 보험회사에 떠넘기려는 궁여지책에서 비롯된 것으로 보인다. 한편 후자의 수법에 해당하는 실제 사례로는 고가의 차를 할부구입한 뒤 차량을 분해하여 부품은 팔아넘기고 보험회사에는 허위 차량도난신고를 하여 보험금을 타내려 한 경우, 차량을 담보로 돈을 빌려 주었다가 빚을 갚지 않자 차량을 주차 중 분실했다고 경찰에 허위신고한 뒤 이를 근거로 보험회사에 보험금을 청구하고 차량은 주택가 이면도로에 버리거나 무허가 정비업소에

맡겨 차를 해체한 뒤 부속품을 팔아넘기는 경우 및 폐차처리를 함에 있어서 행정절차를 밟는데 시간과 비용이 드는 것을 피하기 위하여 차량은 버리고 허위로 차량도난신고를 한 뒤 보험금을 타내려 한 경우 등을 들 수 있다. 보험업계에서는 전체 도난차량 신고건수의 약 60%가 남은 차량 폐차처리 등을 위한 허위신고로 추정하지만 수사인력의 부족과 지역공조체제의 미흡 등으로 수사실적이 저조한 실정이라고 한다.[144]

이와 같이 보험사기는 그 지능적인 수법으로 인하여 타 범죄보다 적발하기가 쉽지 않으며, 살인·방화·고의적 사고의 유발·물건과 재산의 손상 등 여러 가지 다른 범죄를 유발한다는 특징을 가지고 있다. 또한 보험사기는 경제상황이 어려운 시기에 많이 발생하며 국민들의 도덕적 책임의식이 저하될수록 증대·확산된다는 특징을 가지고 있다.

2) 대응방안

① 보험업계 공동의 종합정보시스템의 구축

보험사기를 사전에 예방하기 위해서는 먼저 보험회사의 자구노력이 전제되어야 한다. 한꺼번에 여러 보험회사에 중복가입한 사람의 경우에는 위장가입의 가능성이 높으므로 이를 선별해내는 전산시스템의 개발을 서둘러야 하고, 94년 4월부터 가동중인 자동차사고경력 조회시스템(자동차보험 피해자조회시스템)을 활용하여 보험사기 여부를 가려내야 할 것이다.

② 보험범죄 전문 조사·연구기관의 설립

보험사기범죄에 능동적으로 대처하기 위하여는 먼저 보험범죄사례들을 수집·분석하여 유형별 범죄수법 및 현 보험제도의 문제점 등을 조사·연구하는 전문기관의 설립이 필요하다. 현재 보험감독원, 양 보험협회(생명, 손해보험), 보험개발원 등에서 산발적으로 범죄사례를 수집하여 보관하고 있으나 정보검색과 정보처리가 되지 못하고 있고 필요한 정보자료가 보험회사들간에 교환되고 있지 않아 보험범죄 예방과 방지에 제약이 있다. 따라서 먼저 보험회사간에 위장환자의 리스트를 작성하여 서로 공유하는 등 필요한 정보를 상호 교환하는 정보교환제도를 실시할 필요가 있고, 나아가 전문기관에서 수집가능한 보험범죄사례를 사고유형별로 분류, 전산입력하고 사고유형별로 범죄자의 행동의 특성과 범죄수단 및 방법을 분석·조사하여 보험범죄 지표화하여 활용하는 것이

144) 세계일보 1994. 3. 30일자 참조.

바람직하다고 볼 수 있다.

③ 보험회사직원에 대한 관리와 교육강화

최근 보험회사직원들과 공모하여 범하여지는 보험사기가 빈발하고 있음을 고려하여 보험회사직원에 대한 관리를 철저히 하고 또 교육도 강화해야 할 것이다. 즉 보험회사들은 단순히 진단서, 입퇴원확인서만으로 보험금을 지급할 것이 아니라 현장실사를 통하여 보험사기 여부를 가려낼 수 있도록 보상직원에 대한 교육을 강화하여야 한다.

④ 진단전담의사제도의 도입

위장교통사고 야기후 보험금편취범죄에 대하여는 사기단과 병원과의 공생관계를 차단할 대책도 마련하여야 할 것인데 그 한 방안으로서 교통사고피해의 진단만을 전담하는 진단전담의사제도의 도입을 생각해 볼 수 있을 것이다.

⑤ 보험회사와 수사기관간의 유기적인 협조체제의 구축

보험범죄의 발생 여부를 먼저 조사하게 되는 것은 보험회사라고 할 수 있는데 수사권이 없는 보험회사에게 있어서는 이러한 조사와 증거수집에 많은 제약이 있을 것으로 생각된다. 따라서 위장교통사고 보험사기를 비롯한 보험범죄에 대한 적발과 신속한 수사를 위하여는 보험회사와 수사기관간의 유기적인 협조체제가 구축되어 있어야 할 것이다. 최근 손해보험협회는 보험범죄의 방지를 위해 협회산하에 검찰, 경찰, 보험업계관계자들이 참여하는 가칭 보험범죄 방지대책협의회를 설치하기로 하였다고 하는데, 앞으로 조금 더 실효성있는 협조체제를 구축해 나가야 할 것이다.

바. 장기매매 알선사기

1) 수법과 특징

현대 의료과학의 발달로 장기이식수술이 가능해졌으나, 아직 법적으로는 뇌사가 인정되지 않고 있고 장기이식의 제도적인 장치가 마련되어 있지 않아 불법적인 장기매매가 성행하고 있는 것이 현실이다.[145] 특히 신장이식은 증여자의 생명유지에 지장이 없기 때문에 공공연히 신장매매를 알선하고 알선료를 챙기는 신장매매 알선조직이 등장하여 불법적인 장기매매를 부추기고 있다. 즉 이들은 대형병원이나 지하철역 등의 화장실에 신장매매 알선광고를 낸 뒤 급전이 필요하여 이를 보고 찾아 온 사람들의 신장을 알선

145) 보건복지부는 현재 뇌사를 법적으로 인정하고, 일정한 요건하에 뇌사자의 장기적출을 합법화하는 「장기 등 이식에 관한 법률」을 마련해 놓고 있다.

하고 알선료를 챙기는 것이다.

그런데 최근 IMF사태 이후 실업자가 증가하자 자신의 장기를 팔아 생활비를 마련하려는 사람도 증가하고 있고 이를 이용하여 장기매매를 알선한다는 명목으로 소개비나 검사비조로 돈만 가로채는 장기매매 알선사기행위도 발생하고 있다. 장기밀매를 희망했던 사람들은 예전처럼 부랑자나 극빈자뿐만 아니라 빚을 진 회사원, 부도를 낸 중소기업사장이 그 대상이 되고 있고, 이들이 대부분 급전이 필요하다는 점을 악용, 신장연합회에 돈을 주면 좀더 빨리 비싼 가격에 팔 수 있게 해주겠다고 속여 돈을 더 뜯어내는 수법을 사용하고 있다. 또한 이들은 길에서 습득한 타인의 주민등록증에 자신의 사진을 붙여 주민등록증을 위조한 다음 이 주민등록증으로 은행계좌를 개설하고 피해자들로 하여금 이 계좌에 소개비 등을 무통장입금토록 한 뒤 가로채는 수법을 사용하였다.

그 외에도 빚을 받아내기 위해 채무자에게 장기를 팔도록 협박해 매매대금을 가로채는 사례도 발생하고 있다.

2) 대응방안

현재 장기매매를 알선, 교사한 행위에 대하여는 의료법위반죄(의료법 제25조 제3항[146], 제67조)를 적용하고 있는 것으로 보이나, 앞으로 장기 등 이식에 관한 법률이 시행될 경우 동법의 적용을 받게 될 것이다. 장기 등 이식에 관한 법률 제6조[147]는 장기매매행위를 금지하고 있는데 이에 위반하여 장기매매를 할 경우 동법 제40조에 의하여 처벌된다. 즉 타인의 장기 등을 제3자에게 주거나 주기 위하여 받는 경우 또는 주고 받을 것을 약속한 경우, 이를 교사·알선·방조한 경우, 장기매매임을 알면서 장기 등을 적

146) 누구든지 영리를 목적으로 환자를 의료기관 또는 의료인에게 소개·알선 기타 유인하거나 이를 사주하는 행위를 할 수 없다.

147) ① 누구든지 금전 또는 재산상의 이익 기타 반대급부를 주고 받거나 주고받을 것을 약속하고 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.
1. 타인의 장기 등을 제3자에게 주거나 제3자에게 주기 위하여 받는 행위
2. 자신의 장기 등을 타인에게 주거나 타인의 장기 등을 자신에게 이식하기 위하여 받는 행 위
3. 제1호 및 제2호의 행위를 교사·알선·방조하는 행위
② 누구든지 제1항 제1호 및 제2호에 위반되는 행위를 교사·알선·방조하여서는 아니된다.
③ 누구든지 제1항 또는 제2항의 규정에 위반되는 행위가 있음을 안 때에는 그 행위와 관련 되는 장기 등을 적출하거나 이식하여서는 아니된다.

출하거나 이식한 경우에는 2년 이상의 유기징역에 처해지고, 자신의 장기 등을 타인에게 주거나 타인의 장기 등을 자신에게 이식하기 위하여 받는 경우 또는 주고 받을 것을 약속한 경우, 이를 교사·알선·방조한 경우에는 10년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있게 된다. 장기매매 알선사기의 경우 사기죄가 적용되는 것은 물론이다.

앞으로 뇌사자의 장기적출이 합법화된다고 하더라도 장기공급은 그 수요에 비해 한계가 있으므로 불법적인 장기매매알선행위는 여전히 성행할 것으로 보인다. 따라서 앞으로도 이에 대한 단속을 더욱 강화해야 할 것이다. 최근 장기매매알선을 빙자한 사기사건이 빈발하고 있다는 점을 고려할 때 더 더욱 그러하다. 장기매매 알선행위에 대한 단속의 방법으로는 장기매매의 알선이 병원이나 지하철역 등의 화장실에서 스티커광고를 통해 이루어진다는 점을 감안할 때 이에 대한 역추적을 통하여 적발할 수 있을 것으로 보인다. 또한 장기이식수술을 할 수 있는 병원과 의사의 자격을 엄격하게 제한하고 관리한다면 불법적인 장기매매를 어느 정도 방지할 수 있을 것이다.

또한 장기매매 알선사기행위를 방지하기 위해서는 그러한 사례를 방송을 통하여 충분히 홍보하므로써 그러한 범죄에 대한 경각심을 일깨워야 할 것이다.

사. 무인경비시스템의 허점을 이용한 절도

1) 수법과 특징

1976년 '용역경비업법'의 제정과 더불어 본격적인 성장의 단계에 돌입한 국내 안전경비산업(사경비업)은 최근 전반적인 경기불황에도 불구하고 매출액이 연평균 20-30%씩 급증하면서 현재 그 시장규모가 약 1조원에 이르고 있고, 2000년엔 매출액이 2조원이 넘을 것으로 예상될만큼 급성장하고 있다.[148] 안전경비산업은 크게 경비용역을 제공하는 인력경비와 센서 등 기계를 이용하는 시스템경비분야로 나눠지는데, 그 중에서 시스템경비분야는 1984년 이후 은행 등 금융기관에서 전자경비시스템을 도입하고 90년대 들어 은행 365일코너의 확산과 함께 급성장하고 있고, 안전경비시스템의 기능향상과 IMF체체 이후 '생계형 범죄'의 증가로 인한 수요층의 확대로 앞으로도 더욱 급성장할 것으로 보인다.[149]

148) 한국일보 1998년 6월 3일 16면 참조.

149) 시스템경비 분야는 1981년 '에스원' (당시 한국안전시스템)이 일본 세콤(SECOM)과 기

그러나 최근 무인경비시스템의 허점을 이용하여 금융기관이나 금은방 등에 침입, 금품을 절취하는 사건이 발생하여 업계의 긴장을 불러 일으키고 있다. 특히 최근 수년간 현금자동인출기와 현금자동입출금기가 크게 늘어나면서 이것을 노리는 전문절도범이 빈발할 가능성이 높아지고 있다. 지금까지 발생한 범죄의 수법으로는 첫째 무인경비시스템의 전용경보선을 절단하여 경보장치를 마비시킨 뒤 침입한 경우를 들 수 있는데, 이는 일반전화회선이 깔린 맨홀들은 별도의 잠금장치가 되어 있지 않다는 점을 이용하여 보안시스템을 잘아는 사람이 야간을 이용해 맨홀뚜껑을 열고 전용회선을 절단하여 경비시스템을 마비시킨 다음 침입하는 수법이다. 그리고 두 번째 수법으로는 정밀장비를 이용하여 경보장치를 마비시킨 뒤 침입한 경우를 들 수 있는데, 전류를 다른 곳으로 흐르게 하는 점퍼선과 반사판 등 정밀장비를 이용해 범행한 것이 그 예이다. 셋째는 경보음이 울린 뒤 경찰과 경비업체 직원이 현장에 도착하기 까지의 짧은 시간을 이용하여 절취를 종료한 경우를 들 수 있다. 이 수법은 경찰과 경비업체가 경보음이 울린 후 현장에 도착하기까지 걸리는 시간이 보통 2분 내지 2분 30초 정도라는 점을 이용하여 불과 1분 30초 정도의 짧은 시간에 범행을 하고 달아나는 수법이다. 그 밖에도 경비업체가 현관열쇄만 보관하고 금고실열쇄는 금융기관의 보안담당직원이 보관하고 있는 점을 이용, 금고실 천정을 뚫고 침입한 사건도 발생하여 무인경비시스템에 대한 신뢰가 흔들리고 있는 실정이다.

2) 대응방안

무인경비시스템의 허점을 이용하여 금융기관 등에 침입하여 절취하는 사건들은 대체로 전문절도단과 경비시스템을 잘 알고 있는 전문기술자가 공모하여 범행하는 것으로 보이므로 전현직 기술직원에 대한 관리를 철저히 하여야 할 것이다.

또한 경비전문용역업체 직원의 실수로 범인검거에 실패하는 경우도 발생하고 있는데 예를 들면 금고실 천정을 뚫고 침입한 사건이 그것이다. 이 사건은 경비업체가 비상경보음이 울리자 보안담당직원을 현장에 출동시켰으나 출입문 등 은행바깥부분이나 은행내부상태를 대충 둘러본 뒤 이상이 없자 가장 중요한 금고실 내부점검은 생략한 채 돌아가고 만 사건이다. 금고실열쇄는 금융기관의 보안담당직원이 보관하고 있기 때문에

술제휴로 첨단전자장비를 갖춘 시스템경비사업을 국내 최초로 시작한 이래 한국보안공사, 범아종합경비 등 전국규모의 업체와 지방업체 등 대략 30여개에 이른다(경향신문 1997년 7월 28일 9면 참조)

비상연락망을 통하여 은행담당직원을 불러내어 금고실내부상태를 확인했어야 하는데 출동하고도 기본적인 근무수칙을 지키지 않는 바람에 예방가능했던 사건을 막지 못한 것이다. 따라서 경비전문용역업체의 직원에 대한 기본적인 근무수칙의 철저한 교육도 필요할 것으로 보인다.

그리고 국가안보용 회선이 깔린 맨홀들은 1, 2, 3급으로 분류되어 뚜껑을 용접하여 쉽게 열수 없도록 되어 있지만, 일반전화회선이 깔린 맨홀들은 별도의 잠금장치가 없어 무방비상태이기 때문에 보안시스템에 대하여 잘 아는 사람이라면 누구나 쉽게 범행을 할 수 있다는 점을 고려할 때 경비회선을 일반전화회선과는 별도로 보안장치하여 관리할 필요가 있다고 하겠다.

2. 신종수법범죄의 추세전망

가. 발생상황

범죄환경이 변화함에 따라 범행의 방법이 새로워진 신종수법범죄들이 어느 정도 발생하고 있는가에 대하여 정확하게 알 수는 없다. 그것은 현재의 범죄통계가 주로 형법상의 죄명 또는 행위자가 위반한 특별형법명을 기준항목으로 하여 작성되기 때문이다. 다만 보험범죄의 경우에는 최근 대한손해보험협회에서 집계한 유형별 보험범죄 현황에서 어느 정도 그 발생상황을 알 수 있는데, 그 내용을 보면 '96년에 총 3,480건(276억 8천8백만원)이던 보험범죄가 '97년에는 총 5,109건(325억 2천5백만원)으로 전년보다 47%나 증가하고 있다. 그 중 교통사고 악용범죄가 '96년 2,464건에 192억 8천 3백만원으로 69.6%를 차지하고 있고 '97년에도 4,025건에 218억 9백만원으로 67.1%를 차지하여 과반수 이상을 점하고 있으며 그 증가율도 63.4%로 급증하고 있다는 점에서 고의 교통사고와 관련된 보험범죄의 심각성을 알 수 있다고 하겠다.(〈표 5〉 참조))

그러나 그 이외의 신종수법범죄의 발생상황에 관한 통계는 찾기가 어렵고, 특히 실질적 의미의 범죄에 해당하지만 처벌법규가 없어 처벌의 흠결이 있는 행위는 전혀 통계에서 다룰 수 없기 때문에 신종수법범죄의 발생상황을 판단할 수 없다. 예컨대 자기가 관리하는 건조물 안의 여자화장실에 몰래 카메라를 설치하고 폐쇄회로 TV를 통하여 여성의 일거수 일투족을 시청한 자는 성폭력특별법이 개정(1998.12.28.)되기 전까지는 처벌할 수 없었기 때문에 이러한 행위는 범죄통계에서 누락될 수밖에 없는 것이다. 따

라서 이들 신종수법범죄의 발생상황을 공식적인 자료에 근거하여 분석할 수는 없지만 언론 등에 보도되고 있는 내용으로부터 추론하여 보면 상당히 많이 발생하고 있다고 판단할 수 있다. 특히 이러한 신종수법범죄는 과학기술의 발달에 따라 더욱 교묘하게 범하여지기 때문에 쉽게 발각되지 않는다는 점을 고려한다면 암수 범죄도 대단히 많을 것이다.

〈표 6〉 유형별 보험범죄 현황[150] (단위:건, 백만원, %)

구분 / 유형별	'96			'97			증감율	
	건수	금액	구성비	건수	금액	구성비	건수	금액
위장, 가공사고	1,004	6,675	24.1	1,070	8,719	26.8	6.6	30.6
교통사고 악용	2,464	19,283	69.6	4,025	21,809	67.1	63.4	13.1
기타(폭력배)	12	1,730	6.3	14	1,997	6.1	16.7	15.4
합 계	3,480	27,688	100.0	5,109	32,525	100.0	46.8	17.5

나. 추세전망

정보통신기술과 같은 과학기술의 발전과 그에 따른 범죄환경의 변화에 수반하여 범죄의 수법도 바뀔 수밖에 없을 것이다. 왜냐하면 범죄도 사회의 한 단면이므로 범행수법도 사회환경의 변화에 반응할 것이기 때문이다. 그것은 신종수법범죄가 점점 증가할 것임을 예고하는 것이며, 이미 그러한 증가추세가 감지되고 있고 장차 더많이 발생할 것임은 거의 의심할 여지가 없다고 생각된다.

먼저 칼라복사기나 컴퓨터 스캐너·칼라프린터를 사용한 화폐·유가증권의 위조행위의 경우를 보자. 앞으로 더욱더 정교한 기종이 속속 개발되고 그 가격도 점점 낮아져 이러한 장비가 널리 보급될 것임은 분명하며 이에 따라 화폐나 유가증권의 위조행위는 훨씬더 용이하게 되고 누구에게나 강한 유혹이 될 것이며 그것의 적발은 그만큼 어려워질 것이다.

몰래 카메라에 의한 시청이나 촬영도 증가할 가능성이 많다. 지금까지 문제가 되었던 설치장소는 백화점이나 호텔 또는 독서실의 여자화장실이었지만 최근에는 여자대학교의 화장실에서 촬영된 테이프와 노래방에서 사랑하는 남녀 사이의 애정표현을 녹화한

150) 치안연구소 시책자료('98 - 7) '보험범죄의 현황과 효율적 대처방안' 참조

테이프가 유통되고 있다는 소문도 있다. 앞으로는 의류가게나 수영장 등의 여성탈의실도 대상이 될 수 있을 것이며, 나아가서는 개인의 안방이나 침실까지도 몰래 카메라에게 노출되지 않을 것이라는 보장이 없다. 더욱 작아지고 정교한 카메라가 개발·보급된다면 몰래 카메라의 공포는 인간의 공개되지 않는 사생활은 전혀 없게 되는 상황이 도래할런지도 모른다. 도청의 경우도 이와 마찬가지가 될 것이다.

또한 전화방을 통한 윤락행위도 전화방영업 자체에 대한 단속을 철저히 하지 않는 한 최근 경제상황의 어려움과 함께 가정주부나 10대들의 아르바이트의 대상으로 증가할 것으로 보이며 그 수법도 더욱 교묘해질 것으로 예상된다.

보험사기도 〈표 5〉의 대한손해보험협회의 통계에서도 볼 수 있듯이 '97년에는 전년보다 47% 증가한 5,109건이 적발되었고 '98년에 와서는 IMF사태 이후 경제상황이 어려워져 노숙자나 실업자를 대상으로 교통사고의 피해자와 목격자로 위장해 보험금을 편취하는 사례가 느는 등 매년 양적으로 증가하고 있을 뿐만 아니라 그 수법도 날로 조직화·다양화되는 추세에 있다.

한편 불법적인 장기매매 알선행위는 장기 등 이식에 관한 법률에 의해 뇌사자의 장기적출이 합법화된다고 하더라도 여전히 성행할 것으로 보이며 장기매매알선을 빙자한 사기행위도 장기밀매행위가 없어지지 않는 한 앞으로도 계속 발생할 것으로 보인다.

또 경비시스템의 허점을 이용한 절도행위 역시 앞으로 가정경비시스템의 확대와 함께 더욱 증가할 것으로 보이며 그 수법도 더욱 다양해질 것으로 예상된다.

3. 신종수법범죄의 대응방안

가. 형사법적 대응방안

신종수법범죄 가운데 컬러복사기나 컴퓨터 스캐너·컬러프린터를 이용하는 화폐·유가증권의 위조행위에 대하여는 형법이나 특정범죄가중처벌등에관한법률에 규정된 통화위조죄와 형법상의 유가증권위조죄로 처벌이 가능하므로 이에 대하여는 특별히 처벌법규의 신설이나 보완이 문제되지는 않는다.

몰래 카메라에 의한 시청이나 촬영행위에 대하여는 제한적으로 처벌이 가능한 경우가 있으나 그것만으로는 충분하지 못할 뿐만 아니라 행위의 실질에 대응하는 처벌이라고 할 수도 없었다. 그리하여 성폭력특별법을 개정하여 카메라등을 설치하여 촬영하는

행위를 처벌하기 위한 규정을 신설한 것은 적절한 조치였다. 그러나 이는 매우 불충분하게 규정된 것이므로 촬영은 물론 폐쇄회로 TV를 통한 시청도 처벌할 수 있도록 보완하고 미수범처벌규정과 양벌규정을 신설하여야 한다.

첨단장비를 이용한 도청행위에 대하여는 형법의 특별법인 통신비밀보호법에 처벌규정이 마련되어 있어 이에 대하여는 처벌의 흠결이 없으므로 처벌법규의 신설이나 보완이 필요하지는 않다.

결국 신종수법범죄의 경우 화폐·유가증권위조행위와 도청행위에 대하여는 처벌의 공백이 없으나 몰래 카메라에 의한 사생활침해행위에 대하여는 처벌의 미비점이 있고 이를 보완하는 입법이 하루빨리 이루어져야 할 것이다.

한편 전화방영업에 대하여는 이를 효과적으로 규제할 수 있는 법적 근거의 마련이 시급하다고 생각되며, 보험사기·장기매매 알선사기·경비시스템의 허점을 이용한 절도의 경우에는 처벌에 있어서 어려움이 없으므로 처벌법규의 신설이나 보완이 필요하지는 않다.

나. 사회적 대응방안

대부분의 범죄에 대한 대책이 그러하듯이 신종수법범죄도 이를 효과적으로 방지하려면 처벌법규의 신설이나 보완이라는 형사법적 대책과 함께 예방대책을 강구하는 것이 바람직할 것이다.

먼저 생각할 수 있는 방안이 범죄에 필수적인 첨단장비에 대하여 철저한 관리감독을 함으로써 이들 첨단장비가 범죄의 수단으로 악용되는 것을 막는 것이다. 예컨대 최신형 복사기나 몰래 카메라 등의 첨단장비를 취급하는 업소를 등록하도록 하여 이러한 장비에 대한 관리점검을 통하여 이들 장비가 범죄에 사용되는지의 여부를 수시로 확인할 수 있게 하는 것이다. 다음으로 기술적인 노력을 통하여 첨단장비 자체에 범죄를 예방할 수 있는 장치를 마련하는 것이다. 예컨대 복사기를 개발하거나 제조하는 기업으로 하여금 위조를 방지할 수 있는 프로그램을 개발하여 복사기에 장착하도록 하며, 현금자동입출금기나 현금인출기에 위조 여부를 식별할 수 있는 프로그램을 개발·장착하여 위조화폐 등이 이들 기계장치를 통하여 유통되는 것을 막아야 한다. 또한 화폐나 유가증권을 발행하는 기관에서는 위조가 불가능한 재질을 개발하여 사용하려는 노력도 기울여야 할 것이다.

이러한 행정적·기술적 예방대책과 아울러 몰래 카메라의 사용이나 도청이 중대한

범죄라는 의식을 갖도록 교육과 홍보를 지속적으로 실시하여야 한다. 즉 이러한 행위는 단순히 호기심의 차원에서 문제되는 것이 아니라 타인의 사생활과 행동의 자유를 심각하게 위협하는 반사회적 행위라는 점을 인식할 수 있게 하여야 한다.

첨단신종범죄를 다루어야 할 수사기관의 입장에서는 이러한 새로운 유형의 범죄행위에 대하여 전문적인 지식을 갖춘 수사인력과 이들 범죄의 발견과 증거수집에 필요한 장비를 마련하여야 할 것이다. 이를 위하여 수사관을 민간전문기관에 위탁하여 관련교육을 받도록 함과 아울러 경찰의 교육기관에서도 주기적으로 계속교육을 받을 수 있는 프로그램을 개발하여 시행하여야 할 것이다.

또한 첨단범죄에 관하여 지속적인 관심을 갖고 끊임없이 자료를 수집하고 수사기법을 계발하는 연구를 게을리하여서는 안될 것이다. 그리고 첨단범죄와 관련된 증거를 수집하고 분석할 수 있는 장비를 구입할 수 있도록 관계기관과 유기적인 협조를 하여 예산을 확보하여야 할 것이다. 또한 전화방영업이나 보험사기, 장기밀매 알선사기, 경비시스템의 허점을 이용한 절도 등과 같은 신종수법범죄에 대하여 지속적인 관심을 갖고 이를 발본색원할 수 있도록 하여야 할 것이다. 그러한 범죄에 대한 효과적인 수사를 위하여는 먼저 전화방영업이나 장기밀매의 경우 티켓이나 스티커 또는 생활정보지 등의 광고에 나와 있는 전화번호를 역추적하여 지속적으로 단속하여야 할 것이고, 장기밀매 알선사기의 경우 이에 대한 홍보를 통하여 경각심을 일깨워야 할 것이다. 또한 보험사기와 경비시스템의 허점을 이용한 절도범죄의 경우 관련업계와의 긴밀한 협조가 필수적이라는 점을 고려하여 유기적인 협조체제를 구축하여야 할 것이다.

그 외에도 교통사고 보험사기에 대처하기 위하여 진단전담의사제도의 도입이라든지, 장기밀매를 방지하기 위하여 장기이식을 할 수 있는 병원과 의사의 자격을 제한한다든지, 경비시스템의 허점을 이용한 절도를 예방하기 위하여 경비시스템 전용회선에 대한 보안장치를 강구한다든지 하는 등의 제도적 대응책을 마련하여야 할 것이다.

Ⅳ. 기 타

1. 전자화폐범죄

가. 전자화폐의 의의와 기능

정보통신기술의 발전에 따라 상거래에서도 커다란 변화를 맞이 하고 있는데, 가장 대표적인 것이 전자화폐(electronic cash)의 등장이다. 전자화폐는 마이크로칩을 내장한 스마트카드에 일정액수의 금액을 기록해 놓은 것으로 판독기에 카드를 투입하여 조작하면 상품이나 용역대금이 자동으로 지불되기 때문에 전자지갑이라고도 불리워진다. 전자화폐와 유사한 것으로 직불카드(Debit Card)와 선불카드(Prepaid Card)가 있는데, 직불카드란 직불카드회원과 신용카드가맹점간에 전자 또는 자기적 방법에 의하여 금융거래계좌에 이체하는 등의 방법으로 물품 또는 용역의 제공과 그 대가의 지급을 동시에 이행할 수 있도록 신용카드업자가 발행한 증표를 말하며(여신전문금융업법 제2조 6호), 선불카드란 신용카드업자가 대금을 미리 받고 이에 상당하는 금액을 기록(전자 또는 자기적 방법에 의한 기록을 말한다)하여 발행한 증표로서 선불카드소지자의 제시에 따라 신용카드가맹점이 그 기록된 금액의 범위내에서 물품 또는 용역을 제공할 수 있게 한 증표를 말한다(여신전문금융업법 제2조 8호). 직불카드는 신용카드업자가 발행한 것으로서, 그 자체가 일정한 가치를 표창하지 않으며 교환의 수단이 되는 것도 아니므로 전자'화폐'라고는 할 수 없을 것이다. 그리고 선불카드는 일정한 금액이 기록된 것으로서 일정한 가치가 표창된 것이므로 전자화폐와 유사하지만 역시 국가가 아닌 신용카드업자가 발행한 것이므로 '화폐'라고는 할 수 없다. 최근의 보도[151]에 의하면 한국은행이 서울이나 경북 등지의 한 곳을 골라 10월을 전후하여 전자화폐를 시범적으로 운영할 계획이라고 한다. 이러한 전자화폐는 종래의 현금과 마찬가지로 은행의 개입없이 개인 사이의 자금이체를 가능하게 하는 것은 물론이다. 나아가 전자화폐는 컴퓨터와 정보통신기술의 결합에 의하여 현금과는 달리 원격지에 있는 사람과도 즉시 자금을 주고받을 수 있으며, 다량의 현금을 가지고 다니지 않아도 된다는 장점이 있다.

151) 동아일보 1999년 1월 15일자.

나. 전자화폐범죄의 수법과 추세전망

전자화폐가 널리 사용되면 이의 위조가 매력적인 범죄행위로 등장하게 될 것이다. 지폐가 주종을 이루는 현재의 통화에 대한 위조행위는 흔적을 남기지만 전자화폐는 전자기록의 형태에 불과하기 때문에 흔적을 남기지 않아 그 발견·처벌이 대단히 어렵고, 일정한 기술만 습득한다면 별 비용없이 반복적으로 범행을 할 수 있으며, 한번에 다액의 위조가 가능할 것이므로 전자화폐의 위조행위에 의하여 통화에 대한 공공의 안전과 신용이 중대한 위협을 받을 것임은 분명하다. 나아가 은행을 거치지 않고 자금이체가 가능하므로 이제까지와는 비교할 수 없을 정도로 검은 돈이 쉽게 은신할 수 있는 가능성이 높다.

다. 전자화폐범죄에 대한 대응방안

1) 형사법적 대응방안

① 현행 형벌법규에 의한 대응

형법은 통화에 관한 여러 유형의 위법행위를 처벌하는 규정을 두고 있다. 즉 행사할 목적으로 통용하는 대한민국의 화폐·지폐·은행권, 내국에서 유통하는 외국의 화폐·지폐·은행권, 외국에서 통용하는 외국의 화폐·지폐·은행권을 위조 또는 변조하는 행위, 위조·변조한 대한민국통화·내국유통외국통화·외국통화를 행사하거나 행사할 목적으로 수입·수출·취득하는 행위, 이들 통화를 취득한 후 그 정을 알고 행사하는 행위 그리고 판매할 목적으로 내국 또는 외국에서 통용하거나 유통하는 화폐·지폐·은행권에 유사한 물건을 제조·수입 또는 수출하거나 그러한 물건을 판매하는 행위가 처벌된다(형법 제207조~제211조).

신용카드회사들이 시험적으로 운용하려는 전자화폐는 통화에 해당하는 것이 아니므로 전자화폐가 이러한 수준에 머무르는 한 전자화폐범죄가 곧바로 형법상의 통화에 관한 죄에 의하여 규율될 수는 없을 것이다. 그러나 전자화폐가 외국 또는 국내에서 강제통용력을 갖는 통화로서의 자격을 획득하게 되거나 외국 또는 국내에서 사실상 유통[152] 된다면, 이를 둘러싼 위법행위는 형법상의 통화에 관한 죄에 해당할 수 있다. 다만 통화는 화폐·지폐·은행권과 같이 일정한 유형물에 구매력이 표창된 것을 의미하므로

152) 유통은 통용과는 달리 강제통용력을 의미하는 것은 아니다(이재상, 앞의 책, 476면).

전자기록의 형태로 일정한 구매력이 저장된 전자화폐를 기존의 통화에 해당하는 것으로 볼 수 있느냐의 문제는 여전히 남게 될 것이다.

② 처벌법규의 신설 내지 보완

전자화폐가 아직은 실험단계에 있어 널리 사용되지 않으며 그것의 구체적인 모습이 확정되지도 아니하였기 때문에 이와 관련된 위법행위를 처벌하기 위한 규정이 문제될 상황은 아니다. 그러나 컴퓨터의 보급 및 카드기술과 정보통신기술의 발달에 따라 조만간 전자화폐가 시험운용된 후 기존의 화폐와 더불어 또는 그것을 대신하여 사용될 것임은 분명하다고 생각된다. 전자화폐와 유사한 기능과 성질을 갖고 있는 선불카드의 사용이 늘어나고 있음에 비추어 보면 전자화폐의 이용확산을 쉽게 추측할 수 있다. 따라서 전자화폐를 실험적으로 사용하고 있는 외국으로부터 전자화폐와 관련된 위법행위의 전개모습을 수집하고 입법적 대책을 준비하여야 한다.

2) 사회적 대응방안

① 시행을 위한 철저한 준비

전자화폐가 아직 시행되고 있지 않지만 이것이 시행된다면 아마도 여러 가지 문제점이 나타날 것이다. 따라서 전자화폐를 실험적으로 사용하고 있는 외국으로부터 전자화폐의 사용과 관련하여 나타나는 문제점이 무엇이며 이러한 결함을 어떠한 방법으로 극복하였는가에 대한 자료를 수집하고 이를 분석하는 등 그 시행에 앞서 충분한 준비를 하여야 한다. 이러한 준비작업에는 전자화폐를 운영할 주체는 물론 금융기관이나 수사기관 등 관련기관의 전문가들이 모두 참여하여야 할 것이다.

② 보안대책의 강구

전자화폐가 유통되고 이를 이용하는 경제거래가 활성화되어 전자상거래시대가 본격화된다면 범죄조직에게는 또다른 범죄대상으로 등장할 것이다. 이를 막지 못하면 전자화폐는 보다 널리 활용되지 못하게 될 것이므로 전자화폐의 안전성을 담보할 수 있는 기술적·제도적 보안대책이 수립되어야 할 것이다. 이와 관련하여 특히 암호화와 관련된 문제는 지금부터 지속적으로 연구검토하여야 할 분야라고 할 수 있다.

2. 환경범죄

가. 환경범죄의 의의와 특징

오늘날 고도산업화사회를 맞이하여 과거 단순히 행정법규 위반행위정도로만 인식되어 왔던 환경오염 내지 환경파괴의 문제는 이제 전세계적으로 인류의 생존 그 자체와 관련되는 중대한 문제로 인식되게 되었고 환경문제에 대한 관심은 헌법적 차원으로 격상되기에 이르렀다.[153] 이에 따라 환경오염행위에 대한 법적 대응도 환경관련 행정법상의 벌칙규정으로 형사처벌을 부과하던 방식에서 1991년 낙동강 페놀오염사고가 계기가 되어 환경범죄의 처벌에 관한 특별조치법이라는 새로운 차원의 환경형법을 제정하기에 이르렀다. 따라서 환경범죄는 이제 단순한 행정법규 위반행위가 아니라 반사회적, 반윤리적 차원에서의 범죄라고 보아야 할 것이며,[154] 모든 범죄에 대한 예방과 수사에 대한 임무를 지니고 있는 경찰로서도 이제 더 이상 환경범죄에 대하여 방관만 할 수는 없다고 하겠다.

환경범죄란 일반적으로 사람의 건강에 위해를 주거나 환경을 저해하는 환경오염행위 또는 이와 관련된 행위로서 법에 의하여 처벌되는 범죄행위라고 정의할 수 있는데,[155] 현재 환경범죄를 처벌하는 특별형법으로서 환경범죄의 처벌에 관한 특별조치법이 있고, 환경관련 행정법규로는 각 환경오염매체별로 구분된 소음·진동규제법, 수질환경보전법, 대기환경보전법, 토양환경보전법, 자연환경보전법, 유해화학물질관리법, 오수·분뇨 및 축산폐수의 처리에 관한 법률, 해양오염방지법, 폐기물관리법 등이 있다.

이러한 환경범죄의 특징은 첫째 개인의 고소, 고발보다는 주로 환경행정기관, 경찰, 검찰의 단속에 의존하는 범죄라는 점이다. 즉 환경형법이나 환경관련행정법은 대부분 환경오염이 인간의 건강에 가시적으로 피해를 입히기 이전의 단계에서 범죄행위로 규

153) 제5공화국 헌법 제33조에 국민의 환경기본권과 환경기본의무가 명시된 이래 제6공화국 헌법 제35조도 같은 내용을 명시하고 있다.

154) 현재 환경관련 행정법이 대부분 법률의 마지막 장에 벌칙조항을 두어 법규위반을 처벌하는 형식을 취하고 있어서 벌칙조항을 환경법이 규정한 행정의무의 이행을 확보하는 수단으로 이해할 가능성이 있다. 즉 환경범죄를 '행정범(법정범)'으로 이해하여 그 행위 자체는 반사회성이 없지만 행정상의 단속의 필요 때문에 처벌하는 것으로 인식할 우려가 있다. 그러나 환경형법은 환경이라는 매체의 특수성으로 인하여 환경범죄의 불법유형을 정형화하기 어렵기 때문에 환경행정법과 불가피하게 결합될 수밖에 없는 것이다. 그러므로 환경형법은 단순히 행정불복종의 처벌 또는 행정의무이행의 확보수단이 아니고 추상적 위험범의 형태로 입법된 것이라고 볼 수 있다(물론 단순한 행정불복종의 경우도 혼재하고 있는데, 이에 대하여 행정벌이 아니라 형사처벌을 하고 있다는 점에서 문제가 된다고 하겠다).

155) 유명건, 환경범죄의 현황과 대책, 공해대책, 1987. 7, 29면.

정하여 처벌하는 형식(이른바 추상적 위험범의 형식)을 취하고 있기 때문에 그 피해가 가시적이지 않아서 개인이 고소, 고발하는 경우가 드물다. 둘째 환경범죄는 다른 범죄에 비하여 가해의식이나 피해의식이 희박하고 피해자가 다수의 불특정인인 경우가 많은 범죄이다. 그리고 셋째 환경범죄는 경제불황시에 특히 처리시설의 고장을 방치한다든지 중화제 등의 경비를 절감한다든지, 주로 경제적 이익의 확대를 목적으로 행해지는 경우가 많다. 또한 넷째 환경범죄는 수사단계에서 이화학적, 기술적 요소로 인하여 증거수집이 어렵고, 이는 기소나 재판에서 인과관계의 입증, 과실의 입증이 곤란한 범죄로 나타나게 된다. 따라서 이러한 점을 경감시킬 수 있는 입법기술로서 우리 환경형법은 행정법적인 기준에 부과된 벌칙의 형태로 이러한 점에 대처하고 있으나, 문제는 다른 행정법규와 마찬가지로 행정의무의 이행을 담보하는 취지에서 벌칙이 부과되어 환경범죄라고 인정할만한 법규위반과 단순한 행정불복종의 처벌이 혼재하고 있다는 점이다.

나. 환경범죄의 추세전망

환경범죄의 발생추이는 단속기관인 환경행정기관이 얼마나 강력한 단속을 펴느냐에 따라 좌우될 수 있고, 또 환경행정기관의 단속내용과 실제 수사기관에서의 처리내용이 달라질 가능성은 항상 존재하기 때문에 공식적인 통계만으로는 정확한 발생현황을 결정하기는 어렵다. 그러나 점차 고도산업화사회로 진전하면 할수록 그리고 도시화가 확산되면 될수록 환경파괴는 더욱 심각한 문제가 될 것으로 예상되며 또 이에 대한 관심과 단속이 강화되어 환경범죄의 발생량도 더욱 증가하리라고 예상된다. 그리고 새로운 오염물질의 발생도 예상되므로 새로운 오염물질의 발생과 함께 즉각 이에 대처할 수 있도록 법적 보완책의 마련도 적절히 행해져야 할 것이다.

다. 환경범죄에 대한 대응방안

1) 법적 대응방안

현재 환경관련 행정법상의 환경법규 위반행위에 대한 제재체계는 매우 복잡한 형태로 규정되어 있다. 즉 동일한 위반행위에 대해서 형벌과 행정벌을 동시에 부과하는 유형이 있는가 하면 행정제재를 먼저 부과하고 이를 이행하지 않을 경우 형벌을 부과하는 유형도 있고, 형벌이나 행정제재 중 어느 하나만을 부과하는 유형도 혼재하고 있다. 이와 같이 그 제재체계가 매우 복잡하고 명확하지 않아서 그 적용에 있어서 많은 어려

움이 있을 것으로 생각된다. 따라서 먼저 그 제재체계를 일정한 원칙에 따라 명확히 규정할 필요가 있다. 그리하여 사소한 법익침해행위에 대하여는 과감히 비범죄화하여 행정제재로서 대체하고 불법성이 큰 위법행위는 형벌로서 제재하는 2원적 체계를 유지하여야 할 것이다.

또한 현재 환경침해행위에 대하여 최종행위자인 하위직원에 대한 형벌과 법인에 대한 소액의 벌금형만으로 대처하고 있는데 이러한 제재내용으로는 모든 책임을 하위직원에게 전가할 위험이 있고 또한 환경범죄를 효과적으로 근절하기도 어렵다고 생각된다. 따라서 환경관리인 등 하위직원이나 실무자중심의 처벌보다는 사업자중심의 처벌의 형태로 전화되어야 할 필요가 있고 그 제재내용도 벌금형 등 행정질서벌 위주의 처벌만 규정할 것이 아니라 신체형 등 다양한 형벌을 마련하여 효율적으로 대처하여야 할 것이다.

2) 제도적 대응방안

① 환경범죄에 대한 인식의 전환

앞에서도 지적했듯이 지금까지 환경오염행위에 대한 형사처벌은 행정목적을 달성하기 위한 하나의 부속수단으로 생각되어 오는 경향이 강하였다. 이는 환경보호의 중요성은 인식하면서도 이제 환경범죄는 살인, 절도, 방화 등과 같은 전통적이고 전형적인 형사범죄와 동일한 차원에서 논해져야 하며 환경범죄가 내포하고 있는 엄청난 사회적 유해성에 걸맞는 강력한 단속을 하여야 할 것이다.

② 환경형법의 구조 및 체계의 정확한 파악

환경형법은 기존의 어느 범죄보다도 적용법조가 복잡하고 해석이 어려운 점이 내재되어 있으며, 다수의 환경법규에 산재되어 있어 전문가도 그 내용을 상세히 파악하기 어려운 정도로 복잡한 환경벌칙의 유형으로 규정되어 있다. 따라서 환경형법의 구조 및 체계 등을 숙달하여 법령을 정확히 파악하는 것이 중요하다. 특히 배출시설 허가대상의 세부규격에 관한 규정이 변경되는 경우가 있으므로 시행령, 시행규칙 등에 유념하고 있어야 한다.

그래서 국민의 건강을 해할 우려가 있고 일상생활에 직접 피해를 주는 사건, 행정기관의 지도에 반하여 행한 사범에 중점을 두고 죄질과 정황 그리고 피해상황을 고려하여 악질이라고 판단되는 중대한 사범에 우선순위를 두어 단속하여야 한다.

③ 환경행정관청과의 관계정립

환경형법의 특성상 환경범죄의 수사에는 환경담당 행정공무원과의 협조가 필수적이다. 따라서 환경행정관청 관계자와 경찰관계자들이 수시로 회동하여 환경범죄 단속의 중점사항을 서로 논의하고 정보를 교환하여 체계적이고 유기적인 환경보전시책을 강구하여야 할 것이다.

④ 환경전담부서의 설치와 환경전담 수사요원의 확보

환경범죄는 대부분 기업체내에서 기업활동과 관련하여 저질러지는 소위 기업형범죄이고 환경과 관련한 기술적인 전문지식없이는 위법사실의 확인뿐만 아니라 이를 뒷받침할만한 증거의 확보가 어려운 범죄이다. 또한 이미 출현된 위법사실이나 증거들도 순간적으로 소실되고 마는 특성을 지니고 있음에 반하여, 현재 경찰은 인력이나 예산, 장비 등이 뒷받침되지 않고 있어서 이에 대응할만한 수사능력을 갖추고 있지 못하다고 할 수 있다.

따라서 단기적으로는 독자적이고 전면적인 환경범죄수사는 수사능력면에서 다소 어려운 점이 있다고 하겠으나, 장기적으로는 전국적으로 많은 수의 기업과 인원에 의하여 다양한 유형으로 범하여지는 환경범죄에 대하여 경찰이 가지고 있는 조직의 방대함과 월등한 기동력, 강력한 정보수집기능을 활용하는 것이 가장 효과적인 대응방안이라고 할 수 있으므로 환경전담부서를 설치하고 최소한 1명 내지 2명 이상의 환경전담 수사요원을 확보하여 둘 필요가 있다.

우선 최소한 대규모공단이 집중되어 있는 특정한 지역부터 환경범죄 전담부서를 설치하여 환경범죄를 수사할 수 있는 자체역량을 강화하여야 할 것이다.

⑤ 환경범죄에 대한 수사인력의 교육

환경범죄는 적용법조가 복잡하고 해석이 어렵기 때문에 이에 대한 교육이 필요하다. 또한 환경침해를 입증하기 위하여는 범행장소에서 후에 감정의뢰될 표본들을 채취하여야 하는데 이에 대한 교육도 필요하다. 따라서 수사연수소의 교육과정에 환경범죄 수사과정을 두어 이점에 대한 교육을 실시하고, 아울러 관련기관에 위탁교육을 실시하여 환경전문 수사요원의 양성에 역점을 두어야 한다.

⑥ 체계적인 자료관리 및 정보수집기능의 강화

환경범죄 단속에 실효성을 거두기 위하여는 사전에 각 경찰서는 관내 공해배출업소 등에 대한 현황과 수계별, 지역별 수질 및 대기의 오염도 변화 등에 관한 사항 등 환경범죄 수사에 필요한 모든 자료를 체계적으로 관리하고 적극적인 정보수집활동을 하여 단속대상을 정리한 후 오염의 질, 정도에 따라 등급별로 분류해 두는 것이 필요하다.

그렇게 하여야만 환경오염사고가 발생한 경우 이에 대한 범죄성립 여부 및 범죄자 규명에 효율적으로 대처할 수 있기 때문이다. 그리고 이러한 자료를 바탕으로 환경범죄가 발생할 주변적 환경이 존재한다고 판단되면 즉시 수사에 나설 준비를 갖추어야 한다.

⑦ 시민감시활동의 강화와 신고체제의 확립

아무리 전문인력을 확보한다고 하더라도 그것만 가지고는 환경범죄에 효율적으로 대처하기는 곤란하다. 국민 각자가 서로 환경보전을 위한 감시자로서의 역할을 자임할 때 비로소 환경보전은 실현된다. 이러한 관점에서 환경오염행위 및 환경범죄에 대한 범국민적 감시망 확충이 시급히 필요하며 이를 위하여는 환경오염행위를 적발하고 감시하는 민간조직의 활성화가 전제되어야 한다. 현재 몇몇의 단체가 조직되어 활동하고 있으나 앞으로는 보다 전국적인 차원으로 확대되어 여러 단체가 상호 유기적인 관련하에 민간환경감시활동을 전개하여야 할 것이다.

그리고 경찰로서도 이들 민간환경단체들과의 협조 및 신고체제를 확립하여 두어야 한다.

⑧ 국립과학수사연구소에 환경연구실 설치

환경범죄는 특성상 증거수집이 곤란할 뿐만 아니라 증거를 수집한 경우에도 환경침해를 입증하기 위하여 전문기관의 감정을 의뢰하여야 한다. 이러한 전문기관으로는 현재 국립환경연구원이 있으나 경찰이 직접 인지 수사하여 증거를 수집한 경우 국립환경연구원을 통하여 감정결과를 통보받기까지에는 상당한 시일이 소요된다는 점이 문제점으로 지적되고 있다. 그러므로 이러한 점을 해결하기 위하여는 국립과학수사연구소에 가칭 환경연구실을 설치하여 경찰의 감정의뢰에 신속히 응할 수 있도록 하는 것이 필요하다.

⑨ 광범위한 일제단속 및 지속적인 수시단속의 병행실시

일제단속은 광범위한 업소를 대상으로 한다는 점에서 일반예방적인 효과를 거둘 수 있을 뿐만 아니라 수시단속이 가지는 편협성의 약점을 시정할 수 있다. 따라서 체계적으로 관리된 자료를 토대로 단계적으로 계획성있게 실시하면 환경범죄단속이라는 미시적인 효과 이외에 적극적인 환경관리에 장점이 있다.

그러나 일제단속은 대상업소수가 많고 준비기간 및 참여인원이 많이 소요되기 때문에 정보의 사전유출 등 단속실적면에서 효과가 낮을 수 있다. 따라서 이러한 단점을 보강하기 위하여 취약시간대인 야간이나 우기 또는 감시소홀을 틈타 저질러지는 악질적인 오염행위자들에 대한 지속적인 수시단속을 병행해야 할 것이다.

Ⅴ. 맺음말 : 요약 및 결론

이상에서 신종범죄와 신종수법범죄의 수법과 특징, 적용법조 그리고 추세를 전망해 보고 이에 대한 대응방안을 살펴보았다. 물론 신종범죄의 범위는 보는 관점에 따라 다르기 때문에 하나의 통일된 기준으로 유형화하여 고찰하는 것은 불가능하다. 여기서는 신종범죄나 신종수법범죄 모두 경제사회적 환경의 변화에 따라 새롭게 등장하게 된 범죄군으로서 특히 과학기술의 발전에 수반하여 이를 악용하는 형태로 나타나는 것을 주된 고찰대상으로 하였다. 사회경제적 환경변화에 따른 범죄환경의 변화는 범죄자들에게 새로운 에너지를 제공하게 되고 그 결과 향후 이러한 신종범죄는 더욱 더 증가할 것임은 의심의 여지가 없다고 본다. 물론 범죄유형에 따라 증감의 정도에는 차이가 있을 것이지만. 따라서 수사기관에서는 이러한 신종범죄에 대하여 대책을 강구하여야 할 시점에 와 있다. 이를 위하여는 어떠한 신종범죄가 얼마만큼 발생하고 있는가에 대하여 정확한 자료를 수집하고 이에 근거하여 장차 어느정도 증가할 것인가를 예측할 수 있어야 한다. 그러나 아직까지 이에 대하여 공식적인 통계가 없으므로 우선 통계자료를 만드는 작업부터 시작하여야 할 것이다.

신종범죄 가운데 현재의 형벌법규로 처벌가능한 것이 있는 반면에 현행법상 처벌의 흠결이 나타나기 때문에 새로운 규정을 신설하여야 처벌할 수 있는 것도 있고 처벌법규의 해석과 관련하여 불충분하여 보완이 필요한 것도 있다. 컴퓨터범죄의 경우 전자기록위작·변작죄와 컴퓨터사용사기죄는 입법적 보완이 필요하고, 컴퓨터손괴에 의한 공무방해죄를 신설하여야 할 것이다. 컬러복사기 등을 이용한 화폐나 유가증권의 위조와 첨단장비를 이용한 도청, 장기매매 알선사기, 교통사고야기후 보험금편취, 경비시스템의 허점을 이용한 절도 등은 현행법상 처벌이 가능하므로 문제는 없다. 그러나 몰래 카메라에 의한 촬영행위에 대하여는 처벌규정을 신설하였지만 폐쇄회로 TV에 의한 시청과 미수범에 대한 처벌의 공백이 초래되므로 이를 보완하여야 할 것으로 생각된다. 그리고 신용카드범죄에 대해서도 변제할 의사없이 자기카드를 부정사용하여 현금서비스를 받은 경우의 처벌규정의 신설과 여신전문금융업법상의 처벌규정의 법정형의 조정 등 보완이 필요할 것으로 보이며, 소위 정보통신범죄에 대해서는 앞으로 더욱 다양하게 발생할 것으로 예상되므로 절차법적인 문제의 해결을 망라한 소위 '정보통신범죄방지법'과

같은 통일적인 입법의 제정이 필요할 것으로 보인다. 또한 전화방영업에 대한 효과적인 규제를 위해서는 법정형의 상향조정 등 입법적인 보완이 필요하다.

신종범죄에 대하여 처벌규정이 완비된다고 하여 이들 범죄를 효과적으로 방지하고 처벌할 수 있는 것은 아니다. 즉 행하여진 신종범죄를 수사기관이 적발하고 그에 관한 증거를 수집하여야만 처벌이 가능하게 된다. 따라서 수사기관의 입장에서는 신종범죄를 수사할 수 있는 독자적인 능력을 구비하여야 하며, 이를 위하여 전문수사인력과 장비를 갖추어야 한다. 예컨대 컴퓨터에 능통한 컴퓨터전문수사관, 위조한 복사기나 컬러프린터를 판별할 수 있는 위조전문수사관, 도청장비나 몰래 카메라의 기능과 사용법에 대하여 일가견이 있는 수사관을 양성·확보하여야 한다. 그리고 이러한 수사관을 중심으로 신종범죄를 전문적으로 수사할 수 있는 가칭 "전문범죄수사단"과 같은 것을 설치운영하여야 할 것이다. 아울러 신종범죄의 범행수법을 연구하여 이에 대응하는 수사기법을 연구계발하여야 할 것이다.

신종범죄는 정보통신기술 등 과학기술의 발전에 따라 새롭게 문제되는 것들이 대부분이므로 이에 효과적으로 대처하려면 처벌법규의 신설·보완이나 수사기관의 노력만으로는 불충분하다. 즉 첨단시설이나 장비를 연구개발하는 기업과 이를 행정적으로 뒷받침해주는 행정기관의 범죄방지노력이 함께 어우러져야 이러한 신종범죄로부터 사회질서와 개인의 법익을 지킬 수 있다. 따라서 기업의 측면에서는 가능한 모든 노력을 기울여 첨단장비가 범죄에 악용되지 않도록 하는 기술적인 억제수단을 함께 개발하여야 하고, 행정기관에서는 중대한 법익침해행위에 사용될 수 있는 첨단장비에 대하여 지속적인 관리점검이 가능하도록 하는 조치를 마련하여야 할 것이다.

앞으로 우리 사회에서는 첨단과학기술, 특히 정보통신기술을 악용하는 새로운 유형의 법익침해행위가 많이 나타날 뿐만 아니라 전통적인 법익침해행위의 영역에서도 그 수법이 정보통신기술을 이용하는 유형으로 점차 대체되어 갈 것이다. 따라서 이러한 각종의 신종범죄에 대하여 효과적으로 대처하려면 수사기관 등 범죄의 발견과 처벌을 직접적으로 다루는 기관은 물론이고 학계와 기업이 적극적·체계적으로 협조하지 않으면 안될 것이라는 점을 강조하고자 한다.

참 고 문 헌

〈단행본〉

김문일, 컴퓨터범죄론, 법영사, 1989.

장영민/조영관, 컴퓨터범죄에 관한 연구, 한국형사정책연구원, 1993.

이철, 법무부의 정책과제와 입법적 대응 - 컴퓨터범죄를 중심으로 -, 정보화사회의 전개와 입법적 대응, 한국법제연구원, 1992.

이재상, 형법각론, 박영사, 1996.

법무부, 형법개정법률안 제안이유서, 1992.

한국정보보호센터, 정보보호총서, 1996.

데이비드 론펠트 지음/홍석기 옮김, 정보지배사회가 오고 있다, 자작나무, 1997.

한상문, 신용카드법 입문, 정법사, 1993.

박상기, 형법각론, 박영사, 1997.

오경식, 신용카드범죄의 실태와 법적 문제점, 한국형사정책연구원, 1995.

최영호, 정보범죄의 현황과 제도적 대처방안, 한국형사정책연구원, 1998.

김준호/차종천/김성언, 사기범죄의 실태에 관한 연구, 한국형사정책연구원, 1993.

장영민/조영관, 경제범죄의 유형과 대처방안, 형사정책연구원, 1993.

신각철/김문일, 컴퓨터범죄론, 법영사, 1997.

大西靖臣, コンピュ-タ社會の憂鬱, 1980.

藤原宏高, サイバ--スペ-スと法規制, 日本經濟新聞社, 1997. 10

Klaus Tiedemann, Wirtschaftsstrafrecht und Wirtschaftskriminalität Bd. 2, 1976.

Ulrich Sieber, Computerkriminalit t und Strafrecht 2.Aufl., 1980.

Louis Rohner, Computerkriminalität, 1976.

〈논문 기타〉

강동범, 컴퓨터犯罪와 개정형법, 법조 1997.8.

조규정, 컴퓨터조작범죄, 세미나자료 90년대의 범죄와 형사정책, 한국형사정책연구원, 1990.4.

장영민, 개정형법의 컴퓨터범죄, 고시계 1996.2.

최영호, 컴퓨터범죄에 대한 사회제도적 대처방안, 정보사회와 범죄(제18회 형사정책세미나), 한국형사정책연구원, 1996.

강동범, 신용카드범죄의 실태와 형법적 대응, 형사정책연구, 1995 여름.

강동범, 자기신용카드의 부정사용행위에 대한 형사책임, 고시계, 1997. 12.

김우진, 신용카드부정사용죄의 기수시기, 형사판례연구(3), 박영사, 1995.

이상돈, 자기신용카드의 부정발급사용, 고시계, 1998. 11

장영민, 자기명의의 신용카드남용행위의 죄책, 법학논집 제2권 제1호, 이화여자대학교 법학연구소, 1997. 5

하태훈, 현금자동인출기 부정사용에 대한 형법적 평가, 형사판례연구(4), 박영사, 1996.

한봉조, Internet 통신망을 통한 음란물 배포의 문제점과 대책, Internet불건전정보 방지 세미나, 정보통신윤리위원회, 1995. 9. 29.

임양운, 신용카드범죄의 실무상 문제, 저스티스 제29권 제3호, 1996. 12.

대검찰청 중앙수사부 정보범죄대책본부(http://www.dci.sppo.go.kr/dci.htm)

경향신문 1991년 10월 14일자, 1992년 9월 20일자.

동아일보 1994년 11월 5일자, 1994년 11월 13일자, 1994년 12월 23일자, 1994년 12월 25일자, 1995년 3월 27일자, 1996년 4월 17일자, 1996년 4월 19일자, 1996년 5월 8일자, 1996년 8월 14일자, 1997년 6월 2일자, 1998년 2월 28일자, 1998년 3월 17일자, 1999년 1월 15일자.

문화일보 1995년 1월 16일자.

중앙일보 1996년 5월 30일자, 1997년 5월 10일자.

한겨레신문 1989년 8월 26일자, 1992년 8월 4일자, 1993년 2월 18일자.

Brandt Allen, Embezzler's guide to the computer, Harvard Business Review, July-August, 1975.

米澤慶治, 刑法等一部改正法の概要, ジュリスト No. 889.

大谷實, コンピュ-タ關聯犯罪と刑法の一部改正(下), 判例タイムズ No.646.

神山敏雄, コンピュ-タ犯罪立法の批判的考察, 法律時報 60卷 1號.

山口 厚, コンピュ-タネットワ-クと犯罪, ジュリスト No.1117.