[제1주제]

사이버범죄의 과거, 현재 그리고 미래

전 지 연*

차 례

Ⅰ. 서 론

형사법학회가 창립한지 50년이 되는 데 이 50년이라는 기간 동안 과학기술 그중에서 IT기술의 발전은 상상을 초월한다. 특히 최근 20년 동안의 IT기술의 발전은 가히 폭발적이라고 말할 수 있다. 컴퓨터로 대표되는 정보처리장치는 수많은 자료를 전자적 방식으로 보관하도록 만들었고, 이러한 전자적 저장을 통하여 자료의 방대함에도 불구하고 필요한 자료들을 효과적으로 탐색하거나 전송하는 것이 가능하였다.[1] 또한 정보처리장치의 발전이 개인용 컴퓨터의 광범위한 보급과 정보통신기술의 발전이라는 요인들과 어울려 인터넷의 대중화가 이루어졌으며 현실세계와는 또 다른 세계인 사이버공간을 만들었다.[2] 우리나라의 경우 1994년에 인터넷이 상용화된 이후 2007년 3월 현재 인터넷이용자수가 3,400만 명에 이르는 것으로 보고되며, 이는 전 세계 인터넷이용자수의 3.1%에 해당하며, 인터넷이용자수에 있어서 미국, 중국, 일본, 독일, 인도, 영국에 이어 7위에 해당하는 숫자이며, 국민의 66.5%가 인터넷을 사용한다는 점에서 국민의 인터넷이용비율은 거의 정상급에 해당한다.[3]

사이버공간에서 인터넷이라고 부르는 컴퓨터통신망을 통해 개인은 자신의 개성이나 욕구를 표출하고 있으며, 기업이나 교육기관은 새로운 시장의 개척수단이나 정보전달의 장으로 인터넷을 이용하게 되었다. 그리고 국가는 이것들이 가능할 수 있도록 인프라를 구축하는 일에 사활을 걸고 있다.[4] 그러나 다른 한편으로는 자료들을

* 연세대학교 법과대학 교수, 법학박사

1) Annette Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 1면.
2) Tobias Liebau, Cyber-Crime, jura 2006, 520면.
3) http://www.internetworldstats.com/top20.htm(2007년 6월 27일 방문)

전자적으로 저장하기 때문에 개인적 사생활에 속하는 정보나 기업의 업무상 비밀 등 중요한 정보들이 대량으로 유출될 위험성 역시 상대적으로 커졌다. 또한 큰 노력을 기울이지 않고 단순한 기술적 조작을 통하여 무분별하게 스팸메일을 전송하거나, 해킹과 바이러스 유포 등을 통해 업무를 방해 하거나 재산상의 이익을 취득하거나, 음란물이나 명예훼손적 내용의 게시와 같은 불법한 내용의 콘텐츠를 인터넷을 통해 유포하는 등의 일탈행위가 발생하였다.

그러나 이러한 사이버공간의 일탈행위는 기존의 법적 규제로는 해결할 수 없는 문제를 야기하였다. 종래의 형사법규정이 사이버공간에서의 유해행위들로부터 개인이나 기업의 정보나 재산을 효과적으로 보호할 수 있는 가는 이미 1990년대 초반부터 의문시 되었다.[5] 따라서 이를 해결하기 위하여 입법적 필요성이 제기되었고, 1995년 '형법중개정법률'이 국회를 통과하여 1996년부터 시행됨으로써 컴퓨터범죄에 대한 형법적 처벌이 이루어졌다. 그러나 정보통신망과 같은 통신기술이 급속히 발달, 보급되고 범죄유형도 점점 더 다양화되면서, 그 이후의 범죄는 단순한 컴퓨터범죄가 아니고 컴퓨터와 정보통신망이 결합하는 범죄로 확대되어, 다시금 이에 대한 신속한 대응이 필요하다는 이유로 특별법들을 통하여 형사법적인 처벌이 이루어지게 되었다.

본고는 사이버범죄에 대한 형사법적 처벌에 대한 변화과정을 살펴보고 장래의 범죄출현모습을 살펴보는 기회로 삼고자 한다. 이를 위해 우선 다양한 용어로 사용되는 사이버범죄의 개념을 명확히 하여 그 한계를 정하고, 현재 우리나라에서의 사이버범죄에 대한 현황을 통계적으로 살펴본다(Ⅱ). 그리고 사이버범죄의 변천과정을 시기별로 나누어 살펴보며, 시기의 구분은 1995년 형법개정을 기점으로 하여 컴퓨터형법시기 이전과 이후로, 그 후 형사특별법인 정보통신망이용촉진및정보보호등에관한법률(이하에서는 정보통신망법이라고 칭함)의 제정 이후의 사이버형법시기로 구분하여 살펴보며(Ⅲ), 장래의 사이버범죄의 출현형태를 유비쿼터스형법시기로 명하고 유비쿼터스형법의 특징과 형사법적인 문제점, 그리고 유비쿼터스형법에서 출현할 신종범죄의 모습을 살펴보고 형법과 특별법의 통합을 위한 제안을 한다(Ⅳ). 끝으로 이상의 논의를 요약하여 본고의 결론을 맺고자 한다(Ⅴ).

---

4) 현대사회를 정보화사회라고 하며, 정보사회로의 발전을 '제2의 산업혁명'이라고 부르기도 한다(Sieber, Informationstechnologie und Strafrechtsreform, 1985, 12면). 정보화사회에서는 각종 정보가 홍수를 이루고 그 가운데 자신이 필요로 하는 정보를 얼마나 효과적으로 획득할 수 있는가 또는 정보의 홍수를 얼마나 효율적으로 체계화하여 이를 이용할 수 있는가에 의하여 개인이나 사회의 성패가 직접적으로 영향을 받는다.

5) 이 당시의 문제제기에 대해서는 특히 김문일, 컴퓨터범죄론, 법영사, 1992; 김종원(외), 컴퓨터범죄와 이에 대한 형행 형법의 대응에 관한 연구, 1987; 김종원(외), 컴퓨터범죄에 관한 비교법적·입법론적 연구, 1988; 신규철, 컴퓨터와 법률문제, 법영사, 1993; 이철, 컴퓨터범죄와 소프트웨어보호, 박영사, 1995; 장영민/조영관, 컴퓨터범죄에 관한 연구, 한국형사정책연구원, 1993 참조.

Ⅱ. 사이버범죄의 개념과 현황

1. 사이버범죄의 개념

사이버공간에서 발생하는 범죄행위에 대하여 「사이버범죄」라는 용어 이외에도「컴퓨터범죄」, 「인터넷범죄」, 「하이테크범죄」, 「정보범죄」, 「정보통신범죄」 등 다양한 용어가 사용되고 있으나, 해당 용어의 의미와 범위에는 다소 차이가 있는 것으로 보인다. 즉 어떤 용어를 사용하는 가는 해당 범죄의 어떤 측면을 강조한 것인가에 따라 다소간 달라질 수 있을 것으로 보인다.

컴퓨터범죄의 개념을 부정하는 견해도 있으나, 일반적으로는 컴퓨터범죄의 개념을 긍정한다. 그리고 그 범위에 대하여 좁은 의미로 이해하는 견해도 있으나, 컴퓨터범죄는 컴퓨터를 행위의 수단으로 하거나 목적으로 하여 형사처벌 되거나 형사처벌 할 가치가 있는 모든 행위로 파악된다.[6] 정보범죄의 개념도 컴퓨터범죄와 크게 다르지 않다고 본다. 하이테크범죄는 고도의 과학기술 혹은 첨단과학기술과 관련이 있는 모든 신종범죄라고 말할 수 있으나, 주로 컴퓨터기술과 정보통신기술로 형성되는 사이버공간과 직접 관련이 있는 범죄유형만을 따로 지칭하는 경우도 있다. 따라서 좁은 의미의 하이테크범죄는 사이버범죄와 일치할 수 있으나, 하이테크라는 일반적 용어의 의미상 사이버범죄보다 넓은 개념으로 파악된다.[7] 인터넷범죄는 인터넷이라는 정보통신망으로 연결된 컴퓨터시스템이나 이들을 매개로 한 사이버공간에서 인터넷을 악용하여 행하는 범죄를 나타내는 말이다. 그리고 정보통신범죄는 '정보를 주고받을 수 있는 가상공간을 매개로 하여 발생하는 행위' 또는 '정보교환의 매개수단이 되는 정보통신망 자체에 해를 입히는 행위'로 정의하고 있다.[8] 이러한 의미에서 정보통신범죄는 인터넷범죄의 개념과 일치하는 것으로 보이며, 사이버범죄의 개념과도 상당부분 일치하는 것으로 보인다. 다만 정보통신망을 매개로 한다는 점에서 정보통신망을 매개로 하지 않는 컴퓨터범죄와는 부분적으로 일치하지 아니한다.

이와 같이 다양한 범죄개념들이 모두 명확히 정의된 것은 아니다. 해당 용어들은 컴퓨터와 인터넷의 등장으로 새롭게 나타나고 있는 신종범죄를 지칭하기 위한 용어들로서, 범행도구나 범행수법 등을 중심으로 범죄현상을 파악하려는 시도에서 출발하였다. 그러나 개념정립의 기초가 되는 컴퓨터, 하이테크, 인터넷 또는 사이버라는

6) 전지연, 컴퓨터범죄에 대한 형법적 대응방안, 한림법학FORUM, 제5권(1996), 130-133면 참조.
7) 강동범, 사이버범죄 처벌규정의 문제점과 대책, 한국형사정책학회 2007춘계학술회의자료집, 38면.
8) 홍승희, 정보통신범죄의 전망, 형사정책, 제19권 제1호(2007), 11면.

용어 자체가 명확하게 정의하기 어려운 개념들이어서, 그에 대한 범죄개념 역시 명확한 정의가 곤란하다.[9] 그럼에도 사이버공간에서 발생하는 범죄현상들에 대한 적절한 대응을 위해서는 이들을 지칭할 적당한 용어들이 필요하다. 전통적인 범죄와는 수사방법이나 증거수집 및 조사 등에서 달리 취급해야 할 필요성과 이들을 둘러싼 환경이 급속히 변화되기 때문에 법적 안정성을 중시하는 사법제도의 경직성과의 괴리를 막기 위해서라도 새롭게 등장하는 범죄현상을 신속하게 포착하여 개념화시키는 작업은 필요하다고 본다.

따라서 어떤 방식으로든 사이버범죄의 개념을 정의할 필요가 있을 것으로 보인다. 사이버 범죄를 인터넷과 같은 정보통신망으로 연결된 컴퓨터시스템이나 이를 매개로 형성되는 사이버공간을 중심으로 발생하는 범죄행위라고 정의하거나,[10] 컴퓨터 범죄를 포함한 사이버공간에서 행해지는 모든 범죄적 현상으로 정의하거나,[11] 인터넷 사이트나 이를 서로 연계시키는 컴퓨터 네트워크를 수단으로 하거나 대상으로 하는 범죄라고 파악할 수도 있다. 이에 대해 필자는 사이버범죄를 사이버공간에서 발생하는 범죄행위의 총체로 파악하고자 한다. 여기서 사이버공간은 컴퓨터의 네트워크화로 컴퓨터 내에서 번져 나가는 정보세계를 말하며, 물질적인 실체와 떨어진 가상공간을 말한다. 이와 같은 가상공간인 사이버공간에서 발생하는 범죄는 전통적인 의미의 컴퓨터범죄와 컴퓨터의 네트워크를 통한 연결성을 이용하여 행해지는 범죄를 포괄하는 개념으로 보아야 할 것이다. 따라서 사이버범죄는 전통적 컴퓨터범죄와 정보통신망을 이용한 범죄를 포섭하는 범죄로 이해하여야 한다.

2. 사이버범죄의 현황

사이버범죄행위에 대한 단속은 경찰청과 검찰청에서 이원적으로 실시되고 있다. 실무에서는 사이버범죄를 주로 사이버테러형 범죄와 일반사이버범죄로 구분하는 데, 여기서 사이버테러형범죄는 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용한 컴퓨터시스템과 정보통신망을 공격하는 행위를 말한다. 이에 반해 일반사이버범죄는 사이버공간을 이용한 일반적인 불법행위로서 사이버도박, 사이버스토킹, 사이버성폭력, 사이버명예훼손과 협박, 전자상거래사기, 개인정보유출 등의 행위를 말한다.

경찰청 사이버테러대응센터에서 집계한 최근 6년 동안의 사이버범죄의 발생현황은 <표-1>에서 보는 바와 같이 2001년 33,289건에서 2006년 82,186건으로 급속히 증가

9) Annette Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 1-2면.
10) 김종섭, 사이버범죄 현황과 대책, 형사정책, 제12권 제1호(2000), 234면.
11) 강동범, 전게논문, 39면.

하였다.

<표-1> 사이버 범죄 발생 현황

(단위 : 건)

구 분	계	증 감	사이버테러형범죄	일반사이버범죄
2001년	33,289		10,638	22,651
2002년	60,068	△26,779	14,159	45,909
2003년	68,445	△8,337	14,241	54,204
2004년	77,099	△8,654	15,390	61,709
2005년	88,731	△11,632	21,389	67,342
2006년	82,186	△6,545	20,186	62,000

* 출처: 경찰청 사이버테러대응센터

사이버범죄의 발생에 대한 검거현황에 대해서는 <표-2>와 같으며, 2001년에는 전체 사이버범죄발생건수의 약 65% 내외를 검거하였으나, 2006년 현재에는 전제 사이버범죄의 약 85%를 검거하여 검거율이 상당한 정도로 상승하였다. 그리고 전체 사이버범죄의 약 70% 정도를 20대와 30대가 범하는 것으로 나타났으며, 이는 컴퓨터에 익숙하여 이를 가장 많이 사용하는 젊은 세대에 의해 사이버범죄가 저질러지고 있음을 보여준다(<표-3> 참조).

<표-2> 사이버 범죄 검거현황

(단위 : 명)

구분	총 계			사이버테러형 범죄			일반사이버 범죄		
	발생	검 거		발생	검 거		발생	검 거	
		건수	인원		건수	인원		건수	인원
2001	33,289	22,693	24,455	10,638	7,595	8,099	22,651	15,098	16,356
2002	60,068	41,900	47,252	14,159	9,707	10,762	45,909	32,193	36,490
2003	68,445	51,722	56,724	14,241	8,891	10,047	54,204	42,831	46,677
2004	77,099	63,384	70,143	15,390	10,993	11,892	61,709	52,391	58,251
2005	88,731	72,421	81,338	21,389	15,874	17,371	67,342	56,547	63,967
2006	82,186	70,545	89,248	20,186	15,979	17,498	62,000	54,566	71,750

*출처: 경찰청 사이버테러대응센터

<표-3> 연령별 사이버 범죄 현황

(단위 : 명)

구 분	계	10대	20대	30대	40대	50대	기타
2001년 (%)	5,052 (100.00)	2,193 (43.41)	1,661 (32.88)	777 (15.38)	242 (4.79)	87 (1.72)	92 (1.82)
2002년 (%)	21,817 (100.00)	8,205 (37.61)	6,876 (31.52)	3,743 (17.16)	1,881 (8.62)	563 (2.58)	549 (2.52)
2003년 (%)	30,150 (100.00)	10,187 (33.79)	11,185 (37.1)	5,437 (18.03)	2,277 (7.55)	725 (2.4)	339 (1.12)
2004년 (%)	36,148 (100.00)	9,391 (25.98)	13,296 (36.78)	8,176 (22.62)	3,337 (9.23)	1,289 (3.57)	659 (1.82)
2005년 (%)	37,828 (100.00)	8,630 (22.81)	13,982 (36.96)	9,026 (23.86)	4,135 (10.93)	1,461 (3.86)	594 (1.57)
2006년 (%)	45,877 (100.00)	6,158 (13.42)	15,400 (33.56)	13,543 (29.52)	7,967 (17.36)	2,149 (4.68)	660 (1.43)

*출처: 경찰청 사이버테러대응센터

Ⅲ. 사이버범죄의 과거와 현재

1. 컴퓨터형법 이전 시기(1995년 형법개정 이전)

1) 이 시기의 특징

이 시기는 형법이 제정된 1953년부터 컴퓨터관련범죄에 대하여 형법이 개정되기 이전까지의 기간을 말한다. 우리나라 컴퓨터범죄의 효시는 1973년 10월 과학기술처 중앙전산실의 프로그래머가 반포 AID차관아파트의 입주추첨과 관련하여 프로그램을 조작한 사건으로 알려져 있다.[12] 그 동안 사회적, 경제적 여건이 변화되고 컴퓨터 기술의 발달과 보급으로 그에 따른 심각한 부작용이 문제되었음에도, 형법은 1953년에 제정된 이후 큰 개정 없이 이 때 까지 이르고 있었다. 오히려 정부에서는 컴퓨터 범죄에 대처하기 위한 방안으로 형법개정 보다는 형법이론이나 형사정책적 고려에 대한 충분한 고민 없이 진압위주적인 강경적 법정책의 기조위에[13] 각 부처별로 상황에 따라 필요할 때마다 특별법을 제정하는 방법을 선택하였으며, 이러한 정부의 대

12) 장영민/조영관, 컴퓨터범죄에 관한 연구, 1993, 65면 이하 참조.
13) 서보학, 인터넷상의 정보유포와 형사책임, 형사정책연구, 제12권 제3호(2001 가을), 10면.

처방법은 다수의 유사한 규정을 여러 법률에 산재시킴으로써 법률간 형벌의 불균형, 법체계상의 문제점 등을 야기하였다.

이 시기의 사이버범죄와 관련한 형사법적 입장을 요약하여 살펴보면, 첫째 이 시기는 컴퓨터관련범죄들이 처음으로 출현하기 시작한 시기로 전통적인 형사법으로는 이를 처벌하는 데에 한계가 있어 이를 특별법을 통해 규율하려고 시도하기 시작하였으며, 둘째 컴퓨터의 보급은 되었으나 아직 정보통신기술이 충분히 발달하지 못한 관계로 인터넷범죄나 정보통신범죄보다는 컴퓨터범죄들에 대한 형사법적용이 주를 이루고 있는 시기였다.

2) 이 시기의 컴퓨터관련범죄의 내용과 문제점

컴퓨터범죄의 유형은 범죄객체에 의한 분류, 범죄수법에 의한 분류 등 학자에 따라 다양한 방법으로 분류하고 있으나 일반적으로 컴퓨터데이타의 처리,보존기능과의 관련을 기준으로 하여 ① 컴퓨터부정조작, ② 컴퓨터파괴, ③ 컴퓨터데이타의 부정입수 및 누설(컴퓨터스파이), ④ 컴퓨터의 무권한사용의 네 가지로 분류할 수 있으며,[14] 그에 대한 처벌가능성을 당시의 형법에 따라 검토하면 다음과 같다.

① 컴퓨터를 부정조작하여 재산상 이익을 취득한 경우, 예컨대 컴퓨터를 조작하여 입금자료를 변경시켜 자기구좌에 허위의 입금을 시킨다든가 임금계산에 있어 자기의 임금이 수차에 걸쳐 지급되게 프로그램을 조작하는 경우에 해당 행위를 재산범죄로 처벌할 수 있는 가에 대하여 논란이 되었다. 당시의 형법에 의하면 절도죄의 경우에는 재물의 취득이 없다는 점에서, 사기죄의 경우에는 사람에 대한 기망과 그에 따른 처분행위가 없다는 점에서, 횡령죄에서는 신뢰관계가 없다는 점에서 각각의 죄책을 인정하기 어렵다. 다만 피해자에 대하여 재산상의 사무처리를 하도록 신뢰의무를 가지고 있는 기업내의 일부 사무원에게만 배임죄를 적용할 수 있었다. 또한 컴퓨터에 사용되는 전자기록을 조작한 경우 전자기록이 증명적 기능을 가지고 있다고 할지라도, 전자기록은 표시된 내용을 시각적 방법에 의하여 인식할 수 있는 기재의 가시성과 영속성이 결여되기 때문에 문서의 개념에 포함될 수 없었다.[15]

② 컴퓨터파괴의 경우는 첫째, 컴퓨터나 저장장치라는 하드웨어는 재물에 포함되므로 이를 파괴하는 행위는 재물손괴죄로 처벌된다. 둘째, 하드웨어가 업무에 사용되는 관계로 컴퓨터를 파괴하면 업무방해죄를 구성할 수 있는가에 대하여 업무방해죄의 행위방식은 위계 또는 위력에 의한 업무방해만을 인정하고 있으며, 여기서의 위계 또는 위력은 사람에 대하여 행해져야만 한다. 따라서 컴퓨터와 업무방해 사이에

14) Sieber, Computerkriminalität und Strafrecht, 39면 이하.

15) 같은 취지로 김종원, 컴퓨터범죄와 이에 대한 현행형법의 대응에 관한 연구, 1987, 24면 이하; Sieber, Computerkriminalität und Strafrecht, 277면; Aachenwach, NJW 1986, 1867.

사람이 개입되어 있는 경우에는 컴퓨터의 파괴행위에 의한 업무방해죄가 성립할 수 있으나, 중간에 사람이 개입되지 않은 경우에는 업무방해죄가 성립하지 않는다. 셋째, 본래의 기억매체와는 별도로 기록매체가 기록목적에 이용되어 자료가 저장되어 있는 경우에 그 자료의 내용을 삭제하거나 변경하는 것은 해당 기록이 삭제되는 경우에도 여전히 해당 기록매체는 사용가능하기 때문에 기록매체의 효용을 해한 것으로 볼 수도 없으므로 재물손괴죄에 해당하지 않는다.[16] 넷째, 자료파괴의 경우에 업무방해죄를 인정하는 것은 경우에 따라서는 자료파괴라는 행위 자체만으로 재물손괴죄에서 더 나아가 항상 업무방해죄로 처벌될 가능성이 존재한다.

③ 컴퓨터스파이의 경우는 자료가 기록되어 있는 자기디스크 등의 기록매체 자체를 부정하게 입수하는 방법과 컴퓨터의 자료를 인쇄하거나 복사하여 정보를 입수하는 방법의 두 가지로 나눌 수 있다. 이 두 가지 유형은 다시 침해되는 법익의 종류와 관련하여 재산범죄와 비밀침해범죄로 나누어 살펴볼 수 있다. 첫째, 재산범죄와 관련하여 살펴보면 전자의 방법은 문제되지 않고, 후자의 방법에 의한 경우에 기록된 매체를 복사하여 정보를 절취하더라도 본래의 소지자는 범행이전의 정보를 그대로 보유하기 때문에 절도죄나 횡령죄로 처벌 할 수 없다.[17] 둘째, 컴퓨터스파이의 경우에 당시 형법에 의하면 비밀침해죄의 객체는 신서, 문서, 도화로 제한되어 있고, 전자기록이나 전자기록매체는 여기에 해당하지 않는다.

④ 컴퓨터의 무권한사용은 행위자가 타인의 컴퓨터를 일정한 시간 동안 자신을 위하여 작동시키는 것을 말하며, 이는 처벌의 대상이 아니다. 이에 대한 처벌규정을 둔다고 할지라도 그 실효성에 문제가 있으며, 일반적으로 사용절도를 처벌하지 않는 상황에서 컴퓨터의 무권한 사용만을 처벌하는 것도 법익보호의 형평성에 어긋날 수 있다.

2. 컴퓨터형법시기(1995년 형법개정부터 정보통신망법 제정까지)

1) 이 시기의 특징

컴퓨터범죄에 대처하기 위해 한편으로는 형법이 일부개정 되었으며, 다른 한편으

16) 더 나아가 전송중인 자료나 아직 기록매체에 기록되지 않고 있는 상태(RAM상태)에 있는 자료를 소거하거나 변경하는 경우에는 해당 자료의 물체성을 인정할 수 없기 때문에 이를 삭제하는 것 역시 재물손괴죄에 해당하지 않는다.

17) 절도죄나 횡령죄가 부정되는 이유는 첫째, 절도죄나 횡령죄의 객체는 재물로서 전자기록이나 프로그램은 재물에 해당하지 않으며, 둘째 전자기록의 재물성을 인정한다고 할지라도 양 범죄는 점유의 이전이나 횡령행위를 요구하고 있으나 전자기록의 복사행위는 본래의 소지자도 범행전의 정보를 그대로 보유하기 때문에 점유에 대한 침해를 인정할 수 없기 때문이다(전지연, 전게논문, 146-147면).

로는 다양한 특별법의 제정과 개정을 통하여 컴퓨터범죄 이외에 새로이 대두하기 시작한 인터넷범죄들이 규제되기 시작하였다.

정부는 1992년 6월 형법개정안을 국회에 제출하였다. 이 개정안은 1985년 6월 형사법개정특별심의위원회가 발족한 이후 수차례의 토론과 의견수렴을 거치며 확정된 법률안으로, 그 안에 컴퓨터범죄의 처벌규정이 신설되어 있었다.[18] 그러나 이 개정안은 국회의 논의과정에서 너무 많은 시일이 걸렸고, 해당 회기내에 통과되지 못하면 1996년 초의 새로운 국회구성으로 인하여 폐기될 위기에 놓여 있었다. 이와 같은 급박한 상황에서 국회는 개정안 전체에 대한 심의는 보류하고 신속히 개정되어야 할 부분만 발췌하여 '형법중개정법률'로 1995년 12월에 이를 통과시켰다. 이때 통과된 개정 법률에 컴퓨터범죄에 해당하는 내용들이 기존의 조문에 부가적인 방식 등으로 삽입되었고, 이는 1996년 7월 1일부터 시행되었다. 이에 반해 특별법의 규정들은 다양한 법률에 산재하여 있었고, 그 규율의 내용에서도 중복과 흠결이 있어, 2001년에 정보통신망법과 정보통신기반보호법의 제정에 의하여 정보통신망을 통한 컴퓨터범죄의 유형들이 거의 망라적으로 동법률에 의하여 규율되는 모습을 지니게 되었다.

따라서 이 시기는 컴퓨터범죄관련 규정들에 대한 형법개정이 행해진 시점에서 정보통신망법이 제정되기 이전의 시기를 의미한다. 그리고 이 시기를 컴퓨터형법시기로 표현한 이유는 이 시기에 적용된 개정형법의 내용이 주로 정보통신관련 보다는 전통적인 컴퓨터관련 범죄의 내용을 그 대상으로 하기 때문이다.[19]

2) 개정형법의 컴퓨터범죄

개정형법은 컴퓨터범죄를 컴퓨터기능을 기준으로 구성요건화한 것이 아니라 기존의 구성요건에 부가하는 방식으로 이를 규정하고 있다. 개정형법의 구체적인 내용에 대하여는 다수의 논문과 연구결과가 발표되었으므로[20] 상세한 설명은 약하고, 다만

18) 이 개정안은 형법을 대폭 개정하여, 사실상 형법의 전면 개정에 해당하는 법률안으로, 총칙의 대부분의 규정들을 수정, 보완하였고, 각칙의 체제를 전면적으로 개편하여 개인적 법익을 침해하는 범죄, 사회적 법익을 침해하는 범죄, 국가적 법익을 침해하는 범죄의 순으로 배치하였으며, 컴퓨터범죄나 환경에 관한 범죄를 신설하고, 기존의 구성요건들을 수정하거나 보완하고, 그에 대한 법정형을 정비하였다(상세한 내용에 대하여는 법무부, 형법개정법률안 제안이유서, 형사법개정자료(XIV), 1992.10. 참조). 이 개정안의 밑거름이 되었던 당시 형사법개정특별심의위원회의 회의자료 등이 이번 형사법학회 50주년 기념 CD로 제작되어 형사법연구자들에게 배포된 것은 매우 의미있는 일이었다.

19) 경찰청에서는 신종범죄인 컴퓨터관련범죄에 대처하기 위해서 경찰청내에 1995년에 해커수사대라는 명칭으로 업무를 시작해서, 이를 1997년에는 컴퓨터범죄수사대로 개편하였으며, 이를 다시 1999년에는 사이버범죄수사대로 개편하였고, 2000년 7월부터는 사이버테러대응센터를 창설하여 운영하고 있으며, 각 지방경찰청에는 사이버범죄수사대를 운영하고 있다. 이와 같은 수사대의 명칭변화의 과정 역시 여기서의 시기변화의 과정과 비슷한 맥락에서 이해될 수 있을 것이다.

개정형법에 포섭된 컴퓨터범죄의 종류들을 살펴보면 전자기록등손괴죄, 전자기록등위작, 변작죄(공전자기록, 사전자기록), 컴퓨터업무방해죄, 컴퓨터등사용사기죄, 비밀침해죄 등이 여기에 해당한다.

3. 사이버형법시기(정보통신망법 제정시 - 현재)

1) 이 시기의 특징

정보통신망의 발달은 단순한 형태의 컴퓨터범죄를 네트워크화된 범죄형태로 발전시켰다. 개인이나 기업의 컴퓨터는 정보통신망에 의하여 연결되고, 사람들은 컴퓨터 앞에서 언제든지 다른 사람들의 자료나 정보에 접근할 수 있으며, 이러한 사이버공간은 시공을 초월하여 무한으로 확대되었다. 이러한 상황에서 이 시기의 범죄는 단순히 컴퓨터에 대한 침해나 컴퓨터내의 자료에 대한 침해의 형태에서 벗어나 정보가 정보통신망을 통해 대량으로 유통된다는 점으로부터 이전과는 다른 형사법적인 대응이 필요하게 되었다. 이와 같이 외관상 단순한 컴퓨터의 범죄를 벗어나 네트워크화된 인터넷공간에서 범죄가 발생한다는 점과 이러한 종류의 범죄들이 주를 이루고 있다는 점에서 이 시기를 사이버형법시기라고 부르고자 한다.

2) 사이버형법시기에 형사법의 대응

현재에 해당하는 사이버형법시기의 사이버범죄에 대한 형사법적 대응을 유형별로 나누어 살펴보면 <표-4>와 같다.

<표-4> 사이버 범죄의 유형과 적용법조

사이버범죄의 형태	구체적 유형	적용법조
해킹	정보통신망 무단침입[21]	정보통신망법 제48조, 제63조
비밀침해	컴퓨터 비밀침해(공무상 비밀침해)	형법 제316조 제2항, 140조 제3항
	정보통신망 비밀침해	정보통신망법 제49조, 제62조
	서비스제공자의 개인정보 무단이용행위	정보통신망법 제24조, 제62조
	공공기관의 개인정보 불법변경행위	공공기관의개인정보보호에관한법률 제23조 제1항
	영업비밀의 침해행위[22]	부정경쟁방지및영업비밀보호에관한법률 제18조

20) 개정형법의 내용에 대해서는 강동범, 법정고시, 1996/6, 101면 이하; 김성천, 인터넷법률, 제9호(2001/11), 35면 이하; 장영민, 고시계, 1996/2, 45면 이하; 전지연, 전게논문, 139면 이하 참조.

	주요정보통신기반시설 저장자료의 유출	정보통신기반보호법 제12조, 제28조
	속이는 행위에 의한 개인정보수집[23]	정보통신망법 제49조의2, 제62조
전자기록의 삭제 등	전자기록 손괴	형법 제366조
	전자기록위작·변작	형법 제227조의2, 제232조의2
	정보통신망 정보훼손	정보통신망법 제49조,제62조
	주요정보통신기반시설의 저장자료 파괴	정보통신기반보호법 제12조, 제28조
업무방해	컴퓨터 등에 의한 업무방해	형법 제314조 제2항
	대량데이터 업무방해	정보통신망법 제48조, 제62조
바이러스	악성프로그램 전달·유포행위[24]	정보통신망법 제48조, 제62조
	주요정보통신기반시설에 바이러스 투입	정보통신기반보호법 제12조, 제28조
인터넷사기	해킹 등을 통한 재산취득	형법 제329조, 제347조, 제347조의2, 여신전문금융업법 제70조 제1항 제3호
사이버 음란물	정보통신망이용 음란영상 배포 등[25]	정보통신망법 제65조 제1항 제2호
	청소년이용음란물의 판매 등의 행위	청소년의성보호에관한법률 제8조 제2항
	통신매체이용 음란행위	성폭력범죄의처벌및피해자보호등에관한법률 제14조
사이버 명예훼손	정보통신망이용 명예훼손행위	정보통신망법 제61조
사이버 스토킹	정보통신망이용 공포심조성	정보통신망법 제65조 제1항 제3호
저작권침해	컴퓨터프로그램무단복제행위	컴퓨터프로그램보호법 제29조 제1항, 제46조 제1항
	저작권침해행위	저작권법 제98조
인터넷도박	도박과 도박장개장	형법 제246조, 제247조
스팸메일	대량 데이터전송에 의한 업무방해	정보통신망법 제48조, 제62조
	소량의 광고성 스팸메일 전송행위	정보통신망법 제50조, 제67조 제1항 제15호

21) 미수범의 경우도 처벌한다.
22) 미수 및 예비, 음모도 처벌한다.
23) 피싱(Phishing)의 경우에 대한 처벌규정을 나타낸다.
24) 바이러스 제조행위는 처벌하지 아니한다.
25) 동일한 내용으로 구 전기통신기본법 제48조의2 규정이 있었으나 동 규정은 삭제되었다.

Ⅳ. 포스트 사이버 형법 - 유비쿼터스 형법

1. 포스트 사이버형법의 특징으로서 유비쿼터스형법

사이버범죄가 장래에 어떤 모습으로 변화할지를 예측하는 것은 쉬운 일이 아니다. 사이버범죄의 수단이 되는 컴퓨터기술이나 정보통신기술의 발전은 상상을 초월할 정도로 빠른 속도로 진행되고 있다. 따라서 현재의 시점에서 해당 과학기술들이 장래에 어느 정도까지 발전될 지를 판단하기 어려우며, 또한 기존의 IT기술이 아닌 아주 새로운 형태의 IT기술이 개발되고 이를 통하여 완전히 새로운 사이버범죄의 출현도 가능할 것이기 때문이다.

그럼에도 불구하고 IT기술의 발전방향에 비추어 가까운 장래의 사이버범죄를 예측하면 한편으로는 기존의 IT기술에 바탕을 두면서 신종의 사이버범죄가 출현하고, 다른 한편으로는 인터넷과 새로운 기술과의 결합 등에 의한 전혀 새로운 사이버범죄가 나타날 수도 있을 것으로 보인다. 어쨌든 이러한 신종범죄는 기존의 사이버범죄가 컴퓨터 앞에서 범해지는 특성을 가지나 장래의 범죄는 이러한 장애를 넘어 언제, 어디서나 사이버범죄를 범할 수 있는 형태로 진화할 것으로 보이며, 필자는 이러한 범죄에 대응하는 형법을 유비쿼터스형법으로 부르고자 한다.

유비쿼터스란 용어는 사전적 의미로는 물이나 공기처럼 시간과 공간을 초월해 "언제 어디서나 존재한다" 는 뜻의 라틴어로,[26] 언제든지, 어느 곳에서, 어떤 장치로, 어떤 통신망을 통해, 어떤 서비스도 제공 받을 수 있는 것이 유비쿼터스이다. 그래서 유비쿼터스를 5 Any(Any Time, Any Where, Any Device, Any Network, Any Service)라고 정의하기도 한다.

국가간통신과 컨버젼스 기술이 보편화된 오늘날 유비쿼터스가 세상을 바꾸는 미래의 핵심기술이 된다는 것에 그 누구도 반론을 제기하지 않는다. 따라서 모든 방면에서의 유비쿼터스를 실현하기 위하여 방송, 신문 등 미디어 매체를 통하여 u_헬스, u_시티, u_공항, u_물류, u_국방, u_군수, u_교육, u_정보, 등 모든 단어에 유비쿼터스를 의미하는 소문자 "u"자를 붙이는 것이 유행처럼 되고 있다.[27] 이와 같은

---

26) 이 용어를 정보통신 업체에 처음 소개한 사람은 마크 와이저(Mark Weiser)로, 그는 제록스(Xerox)의 팰로 알토 연구소(PARC: Palo Alto Research Center)의 소장으로, 사이언티픽 아메리칸(Scientific American) 1991년 9월호의 논문에서 "미래의 컴퓨터는 우리가 그 존재를 의식하지 않는 형태로 생활속에 점점 파고 들어 확산될 것이다. 한개의 방에 수백개의 컴퓨터가 있고, 그것들이 케이블과 무선 양쪽의 네트워크로 상호 접속되어 있을 것이다"라고 하였다(김도현/진희채/정지선, 유비쿼터스 서비스의 단계적 진화모델, 정보화정책, 제13권 제2호(2006 여름), 28면).

유선과 무선을 통합한 유비쿼터스 컴퓨팅의 시대에서는 많은 정보기술이 서로 융합되고 컨버전스(Convergence)하게 된다. 이러한 사용환경에서 각 개인은 각 단계마다 ID와 비밀번호, 인증을 필요로 하게 될 것이다. 현재도 주민등록증을 도용하여 은행통장개설과 타인명의 핸드폰구입, 타인명의 전자상거래사용 등을 하고 있어 문제가 되고 있는데, 유비쿼터스 컴퓨팅환경에서는 유선과 무선에서 개인활동이 증가함에 따라 개인정보노출이 심해지고, 개인정보 불법취득도 많아지며, 개인은 시간과 장소 그리고 필요한 범행도구에 구애됨이 없이 원하는 범행을 수행할 수 있다.

2. 유비쿼터스형법에서의 문제점

1) 적용범위의 문제

사이버범죄의 경우 범죄행위가 시간적 제약과 국가적 경계를 넘어 발생하며, 유비쿼터스형법시기 또한 이와 다르지 아니하므로 해당 행위들에 대한 형법적 적용의 문제가 발생한다.[28] 형법은 그 적용범위에 대하여 속지주의, 속인주의, 보호주의의 입장을 보이고 있다. 사이버공간에서의 범죄에 형법을 적용할 수 있는가의 문제는 주로 속지주의에서 범죄지 확정에 달려 있다. 결과범의 경우에는 실행행위지 뿐만 아니라 중간현상 발생지를 포함한 결과발생지가 범죄지로 인정된다. 그러나 사이버공간의 대부분 범죄는 추상적 위험범에 해당하고,[29] 추상적 위험범에서는 결과발생을 필요로 하지 않기 때문에 실행행위지만이 범죄지의 기준이 된다. 또한 여기서 실행행위지는 행위 당시에 행위자가 소재하고 있던 곳(소재지)을 의미한다.[30] 따라서 외국에서 upload나 전송된 내용이 불법인 경우 서버나 사이트의 소재지가 국내외인가에 관계없이 형법을 적용할 수 없다는 불합리한 결론에 이른다. 결국 사이버상에서 발생하는 범죄에 대하여 범죄지의 확정이 기존의 전통적인 실행행위지에 따라 결정되면 형법적용상의 불합리하거나 처벌의 흠결이 나타나게 되어, 이에 대한 새로운 수정, 제한의 필요성이 대두하게 되었다.

---

27) 예를 들면 홈오토메이션을 이용하여 가스를 잠그지 않고, 외출한 주부가 밖에서 전화로 가스 밸브를 잠그도록 할 수 있다. 유비쿼터스 개념은 이보다 더 나아가 보다 진화한 인공지능을 가지고 있어, 실내조명을 위해 커튼을 연다든가, 실내온도 조절을 위해 관련정보(데이타베이스) 컴퓨터에 현재의 최적 온도를 물어 스스로 온도를 조절한다. 여기서 중요한 것은 사람이 모르게 스스로 판단하여 사람에게 최적의 모든 환경을 제공한다는 것이다.

28) 이러한 문제는 이미 2000년에 하태훈, 인터넷과 형법의 변화, 인터넷법률, 창간호(2000), 95면 이하에서(Sieber, NJW 1999, 2065를 인용하여) 지적되었다.

29) 사이버상의 행해지는 범죄 가운데 다수에 해당하는 음란물유포나 명예훼손의 경우 해당 범죄들은 보통 추상적 위험범에 해당한다.

30) Schönke/Schröder/Eser, §9 Rn.4; Tröndle/Fischer, §9 Rn.3; 전지연, 사이버공간에서 형법적 적용범위의 수정・제한, 법조, 2003/11, 78면.

이를 수정하는 방법으로서는 크게 실행행위지의 개념을 확대하는 입장과 결과발생지를 확대하는 입장이 있다.[31] 첫째, 실행행위지를 확대하는 입장은 실행행위지를 행위 당시 행위자가 소재하고 있던 장소뿐만 아니라 "행위자가 의도적으로 그리고 자신의 통제 하에 자료를 저장하는 서버의 소재지"도 실행행위지로 인정하여 범죄지로 보는 입장[32]이다. 그러나 범행 장소에서는 범죄를 구성하지 않으나, 우리나라에 사이트가 있다는 이유로 우리 법률을 적용하게 된다는 비판을 받는다. 둘째, 결과발생지를 확대하는 입장은 추상적 위험범의 경우에도 구체적 위험범과 같이 추상적 위험이 실현될 가능성이 있는 장소도 결과발생지로 해석하는 입장이다. 다만 이러한 제한을 인정하는 입장에서와 같이 위험의 결과 가능성이 있는 장소를 범죄지의 기준으로 사용하는 경우에도 과도한 형벌권의 확장을 피하기 위해 제한하는 시도가 행해지고 있다. 예컨대 ① 자국의 형법을 적용하면서 불법내용의 사이트 운영자나 자료게시자가 목표지향적인 직접 고의(소위 제1급고의)를 가지고 인터넷을 통하여 자국에서 영향을 끼치려는 의도를 가지고 있는 경우에만 자국의 형법을 적용한다는"주관적 측면에 의한 제한"과 ② 실행행위지에서 불가벌인 행위는 자국 형법의 적용을 배제하려는 "행위지의 가벌성에 의한 제한", ③ 자국과의 특별한 관련점이 존재하는 경우에만 적용하려는 "자국 관련성에 의한 제한", ④ 자국 형법의 적용은 추상적 위험범 중 일정한 법익을 침해한 경우로만 제한하려는 "세계원칙에 의한 제한"으로 보는 견해 등 다양한 견해가 있다.

사이버공간에서 자국형법을 무차별적으로 적용하여, 각 국가들이 '사이버공간의 지배자', '전산망의 보안관' 또는 '인터넷의 파수꾼'으로 뛰어 오르려고 하는 것은 바람직하지 않다. 따라서 형법의 적용범위는 기존의 단순한 속지주의의 입장을 사이버공간에 그대로 적용하는 것은 타당하지 않다. 오히려 사이버공간에서의 표현물 규제는 자국의 영토 내에서 위험이 발생할 가능성이 있고, 해당 위험이 세계주의에 의하여 보호되는 정도의 일정한 법익에 대한 위험인 경우에만 자국형법을 적용하는 것이 타당하다고 본다.[33]

2) OSP(ISP)의 책임문제

사이버범죄에 대한 이제까지의 처벌은 주로 사이버공간에서 불법한 내용물을 게재한 자를 중심으로 논의되어 왔다. 그러나 정보통신망이 일반인들의 보편적 사용수단이 되고 이에 의한 불법내용들의 게시나 유통이 확대되는 관계로 이를 가능케 하

31) Heinrich, GA 1999,80; Hilgendorf, NJW 1997,1877; Schönke/Schröder/Eser, §9 Rn.46 ff. 참조; 김정환, 인터넷상에서 국제형법, 인터넷법률, 제37호(2007), 157면 이하.
32) 김성천, 인터넷상의 범죄와 형법의 적용, 인터넷법률 제9호, 35면.
33) 전지연, 법조, 2003/11, 78-110면.

는 정보통신망의 운영자에 대한 처벌가능성에 주목하게 되었다.[34]

현행법상 정보통신서비스제공자에 대한 일반적 개념규정은 없고, 각각의 법률에 따라 다양하게 개념규정하고 있다. 정보통신관련 서비스제공자에 대한 정의규정에 대해 예를 들면 '전기통신사업자', '정보통신서비스제공자', '온라인서비스제공자' 등 각각의 특별법의 취지나 내용에 따라 조금씩 다른 방식으로 해당 정보통신망의 제공자로 나뉘고 있다.

아직까지 ISP의 형사책임에 관한 일반원칙을 직접적·명시적으로 규정한 법률은 없고,[35] 다만 정보통신망법이 ISP의 '개인정보보호의무'(제27조 제1항 및 제28조)나 '정보통신망안정성확보의무'(제45조 제1항)를 부여하고 있다. 그러나 이 규정들 역시 ISP에 대한 일정한 책임의 존재만 확인하고 있을 뿐 정보통신서비스제공자의 책임을 묻기 위한 구체적 요건이 입법된 것이라고는 볼 수 없다.[36] 따라서 이용자 등에 의한 불법한 내용의 콘텐츠 게시 등과 같은 사이버범죄에 대하여 ISP의 형사책임은 형법이론에 기초하여 해당 사이버범죄의 부작위범 또는 방조범의 성립가능성을 검토한다.[37] 그러나 이러한 결과가 논증합치적인가에 대하여는 다소 의문이 있으며, 이에 대한 보다 세밀한 검토가 필요할 것으로 보인다.

---

34) 민사법적인 책임과 관련하여서는 최근에 인터넷게시판에 올라온 사진을 삭제해 달라는 요구에 적극적으로 대응하지 않은 사이트 운영업체에 대하여 법원은 손해배상책임이 있다고 판결하였다. 해당 사건에서 피해자는 "사진 삭제요구를 들어주지 않아 초상권 침해를 당했다"며 온라인사진동호회 사이트를 운영하는 기업을 상대로 위자료청구소송을 제기하여 승소하였다. 재판부는 피해자의 삭제요구에 사이트 운영회사는 사진을 게시한 게시자의 개인 홈페이지 방명록에 삭제요청 글을 남겼을 뿐 게시자에게 직접 연락할 노력을 기울이지 않았고, 비공개 게시물로 처리하는 방법이 있었음에도 한 달 가량 사진을 방치하는 등 사이트 운영자로서 주의의무를 다하지 못한 과실이 있다고 밝혔다. 또한 법원은 사이트 운영회사가 해당 사이트를 회원들의 자발적인 사진게시 공간으로 제공할 뿐 선별이나 분류에 관여하지 않는다 해도 회원들이 올리는 초상권 또는 저작권 침해, 명예훼손 게시물을 관리할 책임이 없는 것은 아니라고 판단하였다(서울서부지방법원 2007.4.19, 2006나8560 판결).

35) 이와 같은 입장에서 최근에 정통부는 인터넷포털에 대한 규제법안을 추진하기로 하였다. 즉 포털의 영향력이 커지는 가운데 그에 합당한 사회적 책임을 물을 법적인 근거를 갖추겠다고 하고 있다. 여기에는 포털이 명예훼손 게시물이나 음란물을 방치할 경우 법적인 책임을 지도록 하고, 언론사에 제공한 콘텐츠를 다룰 때 자의적으로 편집·가공할 수 없도록 하는 등의 내용이 포함된 포털규제법을 올 하반기 정기국회에 제출하겠다고 설명했다(한겨레신문 2007-05-24 오전 01:54:45).

36) 황태정, 정보통신서비스제공자의 책임에 관한 비교법적 고찰, 인터넷법률, 제28호(2005/3), 22면 이하.

37) 대법원은 구체적으로 논증하고 있지는 않으나 ISP에게 조리상의 의무에 기초하여 방조범의 죄책을 인정하고 있다(음란물의 경우는 대판 2000.03.23, 2000도326; 2006.4.28, 2003도4128; 2006.4.28, 2003도80). 명예훼손의 경우 ISP의 책임에 대한 상세한 검토는 박광민, 인터넷상의 명예훼손에 관한 형사법적 규제, 형사법연구, 제24호(2005 겨울), 107면 이하 참조.

3) 과잉범죄화와 과잉형벌화의 문제

(1) 과잉범죄화와 과잉형벌화의 원인

사이버범죄에 대한 형사법적 규제는 형법뿐만 아니라 다양한 특별법에 의하여 이루어지고 있다. 사이버범죄를 특별법 중심으로 규제하게 된 이유는 사이버공간에서 나타나는 일탈행위에 신속하게 대응할 필요성이 있어서 그때그때 마다 입법이 필요하다고 판단하여 이를 특별법으로 포섭하였다. 그리고 또한 사이버공간에서 발생하는 일탈행위와 관련하여 직접적으로 이해관계가 있다고 보여지는 정보통신망업체, 컴퓨터관련기관 그리고 이를 담당하는 정부기관들의 시각에 의하여 처벌의 유형과 대상 그리고 법정형들이 정해지고 이것이 형사규제로 입법화되었다. 그 결과 사이버범죄의 처벌과 관련하여 형법의 일반원리와 당벌성 그리고 다른 범죄들과의 형평성 등의 내용들이 구체적으로 고려되기 보다는 신속한 형사법적 대응이 필요하다는 점과 발생하는 법익침해가 막대하다는 점만이 전면에 등장하였다. 이에 근거하여 사이버공간의 일탈행위에 대한 거의 전방위적 처벌과 또한 그 처벌도 엄격한 처벌을 통하여 사이버범죄를 예방하려는 시도는 도처에 중첩적인 처벌규정들과 엄격한 규정들을 생산하여, 결국 사이버범죄에 대한 형사법적 규제는 과잉범죄화와 과잉형벌화의 문제를 지니게 되었다.

(2) 과잉범죄화

사이버범죄에서 과잉범죄화가 문제되는 유형은 두 가지 형태로 존재한다. 하나는 동일한 구성요건행위가 다양한 법률에 중복 또는 중첩적으로 규정되어 있는 결과 중복적으로 적용되기 때문에 과잉이 되는 유형과 해당 구성요건 자체가 범죄로 존속하여야 할 필요가 있는가가 문제되는 유형의 두 가지 유형이 있다.

첫째, 중복으로 인한 구성요건이 과잉되는 경우는 예컨대 사이버 자료손괴를 들 수 있다.[38] 형법의 재물손괴죄의 규정에서 '전자기록 등 특수매체기록'에 대한 효용을 해하는 경우를 처벌하고 있으며, 정보통신망법에서는 정보통신망에 의하여 보관되는 정보를 훼손하는 경우를 처벌하며, 나아가 정보통신망에 의하여 처리 또는 전송되는 정보를 훼손한 경우를 처벌한다. 또한 해당 정보가 공공기관에서 처리하고 있는 개인정보의 경우에 이를 공공기관의 개인정보 처리업무를 방해할 목적으로 개인정보를 말소한 경우에는 공공기관의개인정보보호에관한법률에 의해 처벌되며, 물류전산망에 의하여 처리·보관 또는 전송되는 물류정보를 훼손한 경우에는 화물유통

38) 자료삭제 이외에도 자료조작이나 자료변경의 경우 그리고 전자적 자료나 정보를 누설하는 경우에도 자료삭제의 경우와 동일하게 다수의 구성요건이 중첩하는 일이 존재한다.

촉진법에 의해, 신용정보전산시스템의 정보를 삭제 기타 이용불능케 하는 행위는 신용정보의이용및보호에관한법률에 의해 처벌된다. 이와 같이 해당 자료가 어떤 종류의 자료인가에 따라 다양한 법률에 중첩적으로 규정되어 있다. 이러한 경우에는 각각의 해당 행위들이 가지는 처벌필요성과 다른 범죄와의 형평성 및 다른 법률들과의 관련성 등을 검토하여 통합하는 등의 작업이 필요하다.

둘째, 구성요건의 존속필요성이 의문스러운 범죄는 예컨대 단순 해킹이라고 불리는 정보통신망의 무단침입죄를 들 수 있다. 해킹은 그 자체만으로는 아직 구체적으로 정보통신망이나 컴퓨터시스템 파괴 등에 의하여 다른 사람의 업무를 방해하였다거나, 저장된 전자적 자료나 문서들을 삭제, 위작 또는 변작하였다거나, 재산상 이익을 취득한 것이라고 할 수 없으므로 과연 이러한 행위 자체만을 처벌할 수 있을 것인가가 논란이 되었다.[39]

일부에서는 이러한 침입행위는 업무방해나 비밀침해 등의 예비행위에 불과하므로 우리 형법상 각각의 유사한 해당조문에 예비행위에 대한 처벌규정이 없는 한 이에 상응하게 불처벌하는 것이 타당하다고 주장하였다. 이에 반하여 권한이 없는 사람이 시스템관리자의 의사에 반하여 시스템에 침입하는 행위자체는 그것이 자료의 부정조작이나 컴퓨터 등 손괴에 의한 업무방해행위 비밀침해 등 다른 범죄행위로 나아가기 위한 선절차로서의 의미를 가지는 경우는 물론이려니와, 그와 같이 다른 범죄행위로 나아갈 의사 없이 단순한 호기심이나 영웅심 등에 기인하여 이루어진 경우라 할지라도 이러한 유형의 해킹행위가 폭증하고 있고, 그 위험성 또한 적지 아니하다는 점에서 이를 처벌할 필요성이 있다고 주장하였다.

입법자는 해킹의 처벌필요성을 인정하여 구 정보통신망이용촉진등에관한법률 제29조에 정보통신망의 보호조치를 침해하거나 훼손한 자는 3년 이하의 징역 혹은 3천만 원 이하의 벌금에 처하는 것으로 규정하고 있었다(정보통신망보호조치침해죄). 그러나 본 법을 개정하여 2001년 7월 1일부터 시행된 정보통신망법에서는 이러한 보호조치 침해 규정 대신 제63조에 정보통신망 침입행위 금지 규정을 마련하였다.[40] 즉 정보통신망법에 의하면 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입하여서는 안되며(정보통신망법 제48조), 이 규정을 위반하여 정보통신망에 침입한 자는 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처하도록 하였으며(정보통신망법 제63조 제1항 제1호), 최근에는 그에 대한 미수범도 처벌하

39) 해킹의 처벌여부에 대한 논란은 유인모, 정보형법의 과제와 전망, 형사정책, 제12권 제1호(2000), 71-73면 참조.

40) 이것은 해킹의 기술적 발전에 따라 보호조치를 침해하지 않고 보호조치를 우회하는 등의 방법으로 정보통신망에 침입할 수 있는 수단이 확보되면서 처벌의 흠결이 발생할 것을 의식해 취해진 조치이다.

도록 하였다(정보통신망법 제63조 제2항<신설 2004.1.29>).

그러나 해킹에 대한 무차별적인 처벌과 미수범에게까지 그 처벌범위를 확대한 것에는 문제가 있다. 특정범죄를 범할 생각이나 기회로 정보통신망에 침입하여 해당 범죄의 결과를 실현하거나 실현하려고 하였던 경우에는 해당 범죄로 처벌가능하다. 그러나 범죄목적을 포함하여 단순히 정보통신망에 침입한 것만 가지고는 아직 결과실현과 직접적인 연결이 있다고 보기 곤란하고, 그럼에도 불구하고 이를 처벌하려는 시도는 장래에 발생할 법익침해의 위험을 미리 방지하는 임무를 부담하는 셈이 된다.[41] 이는 형법의 일반적 임무가 아니라 경찰법의 과제에 속한다고 볼 것이다.[42] 또한 정보통신망법상의 무단침입은 해당 통신망이나 시스템에 보호조치가 있는 것을 전제로 하지 아니하며, 판례에서도 인정하는 바와 같이 서비스제공자로부터 권한을 부여받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단하여야 한다.[43] 따라서 보호조치가 되어있지 않은 상태에서 단순히 "일반인은 접속하지 마십시오"라는 지시가 되어있는 정보통신망에 접속하는 것도 권한 없는 접속에 해당하며,[44] 아이디와 비밀번호를 입력하는 등의 보호조치가 되어있는 정보통신망의 경우에도 이용권자의 동의하에 그의 아이디와 비밀번호로 해당 통신망에 접속하는 것도 모두 무단침입에 해당한다. 왜냐하면 대부분의 정보통신서비스제공업체는 이용자와 맺고 있는 회원계약의 약관[45]에 회원의 아이디와 비밀번호를 타인이 이용하지 못하도록 규정하고 있기 때문이다. 더 나아가 미수범의 경우도 처벌하므로 접속을 시도하거나 접속하기

---

41) 위험사회에서 위험형법으로의 변화에 대해서는 하태훈, 전게논문, 105면 이하 참조.

42) 이상돈, 해킹의 형법적 규율방안, 법조, 2002/3(통권 546권), 112면.

43) 대판 2005.11.25, 2005도870.

44) 본래 해킹이라 함은 그 용어자체에서 '특별한 기술적인 방법에 의한다'는 것을 전제로 하고 있다. 따라서 기술적인 방법이 아닌 단순히 지시에 반하여 접속하거나, 우연히 알게 된 아이디와 비밀번호로 접속하는 것은 해킹에 해당하지 않으나, 우리 법률은 해킹이라는 용어를 사용하지 않고 접근권한 없이 '침입'이라는 용어를 사용하여 이러한 문제가 발생하리라고 본다.

45) *Daum 서비스약관 제10조(이용자의 ID 및 비밀번호에 대한 의무) ① "Daum"이 관계법령, "개인정보보호정책"에 의해서 그 책임을 지는 경우를 제외하고, 자신의 ID와 비밀번호에 관한 관리책임은 각 이용자에게 있습니다. ② 이용자는 자신의 ID 및 비밀번호를 제3자에게 이용하게 해서는 안됩니다.
*NAVER 이용약관 제11조(회원의 의무) (5) 회원은 회사의 명시적 동의가 없는 한 서비스의 이용권한, 기타 이용계약상의 지위를 타인에게 양도, 증여할 수 없으며 이를 담보로 제공할 수 없습니다.
*천리안 이용약관 제11조(이용자의 ID 및 비밀번호에 대한 의무) ① 회사는 관계법령, 개인정보보호정책에 의해서 그 책임을 지는 경우를 제외하고, 자신의 ID와 비밀번호에 관한 관리책임은 각 이용자에게 있습니다. ② 이용자는 자신의 ID 및 비밀번호를 제3자에게 이용하게 해서는 안됩니다.

위하여 아이디나 비밀번호를 입력해보는 행위 역시 처벌의 대상이 된다는 결론에 이른다. 따라서 무단침입의 경우 미수범의 처벌규정은 삭제되어야 하고, 무단침입의 경우는 보호조치의 여부라는 제한이나 특정범죄를 범할 목적이라는 주관적 요소에 의한 제한이나 어떤 방식으로든지 제한이 필요하다고 보여진다.[46]

⑶ 과잉형벌화

동일한 내용의 불법행위가 사이버공간과 오프라인에서 발생한 경우 그에 대한 처벌규정이 각기 존재하는 경우 사이버공간에서의 범죄에 대한 법정형이 일반범죄에 대한 법정형과 비슷하거나 다소 높은 것이 보통이다. 예를 들면 사기죄와 컴퓨터등사용사기죄, 업무방해죄와 컴퓨터등업무방해죄의 법정형은 동일하다. 그러나 대량데이터의 전송을 통하여 정보통신망에 장애를 일으킨 경우(정보통신망법 제62조 제5호)에는 업무방해죄보다 벌금의 액수만 다소 높다.[47] 이와 같은 법정형의 차이는 사이버공간에서의 범죄는 일반범죄에 부가하여 정보통신망에 대한 신뢰성과 안정성을 위태롭게 한다거나, 범죄의 피해범위나 정도가 클 수 있다는 점에서 정당화되어 질 수 있다.

그러나 유사한 범죄행위가 오프라인에서 행해졌느냐 정보통신망 등을 통하여 수행되었는가에 따라 법정형에서 상당한 차이를 나타내면 그에 대해서는 형평성의 견지나 과잉금지의 원칙에 비추어 처벌이 조정되어야 할 것이다. 전자기록이나 특수매체기록을 기술적 수단을 이용하여 알아낸 컴퓨터 등에 의한 비밀침해의 경우 '3년 이하의 징역이나 금고 또는 500만 원 이하의 벌금'에 해당하나(형법 제316조 제2항), 패킷 스니퍼링 기법으로 정보통신망에 의하여 전송되는 타인의 비밀을 알아낸 경우에는 '5년 이하의 징역 또는 5천만 원 이하의 벌금'에 해당한다(정보통신망법 제62조 제6호). 그리고 또한 이와 유사하게 타인간의 전기통신을 무단으로 감청한 경우에는 '10년 이하의 징역과 5년 이하의 자격정지'에 해당한다. 이러한 법정형의 현격한 차이는 특별법의 과잉을 보여준다.[48] 따라서 오프라인의 범죄와 사이버공간의 범죄의 형량을 비교 검토하여 과잉형벌에 대한 문제를 해소하여야 한다.[49]

---

46) 무단침입의 미수를 비범죄화하여야 한다는 주장에 동의하는 것은 류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구 제6권 제2호, 202면; 이상돈, 전게논문, 116면 이하 참조(더 나아가 바이러스의 유포의 경우도 비범죄화 하여야 한다고 주장함).

47) 출판물에 의한 명예훼손죄와 사이버명예훼손죄의 경우에도 사정은 비슷하다.

48) 동일한 취지로 이상돈, 전게논문, 121면.

49) 기타 사이버스토킹과 바이러스전달·유포죄의 경우에도 과잉형벌의 문제가 제기된다(강동범, 전게논문, 51면, 53면 참조).

4) 개별적 유형에서의 문제점

기타 각론적인 관점에서 제기될 수 있는 내용을 열거적으로 살펴보면 게임아이템이나 사이버머니의 거래와 재산범죄가능성,[50] 피싱(Phishing)[51]과 같은 방법에 의한 개인정보의 무단수집과 이에 의한 인터넷사기, 스팸메일의 해결방안,[52] 컴퓨터등 사용사기죄의 객체에 '재산상의 이익'외에 '재물'을 추가한 개정안에 대한 검토[53] 등이 필요할 것이다.

3. 유비쿼터스 형법에서의 새로운 범죄유형

유비쿼터스 컴퓨팅의 시대에 어떤 새로운 범죄가 출현할 것인가를 구체적으로 예측하는 것은 곤란하다. 그러나 IT기술의 발전으로 인한 자유로운 네트워크에의 접근과 새로운 통신매체나 정보전달매체의 상호 융합이 새로운 범죄형태로 출현할 것이라고 보인다. 이와 같은 통합형 범죄형태로는 현재에도 나타나기 시작한 모바일범죄와 웹 리얼리티와 같은 가상 사이트에서의 범죄이다.

첫째, 새로운 범죄형태로서의 모바일범죄는 IT환경이 무선인터넷 중심으로 변화하

---

50) 게임아이템의 재물이나 재산성에 관한 문제에 대하여는 김혜경, 온라인 게임 아이템의 재산범죄 성립가능성, 연세대 법학연구, 제14권 제2호(2004), 232면 이하; 변종필, 인터넷게임 아이템과 재산범죄, 인터넷법률, 제19호(2003/09), 47면; 윤해성, 인터넷게임 아이템거래에 관한 형사법적 검토, 인터넷법률, 제34호(2006/09), 94면; 탁희성, 재산죄의 객체로 전자정보의 포섭가능성 및 그 한계, 형사정책연구, 제16권 제2호(2005 여름), 141면; 홍승희, 정보재산권의 형법적 보호, 형사정책연구, 제16권 제3호(2005 가을), 105면 참조.
또한 최근에 법률개정을 통해 게임물의 이용을 통하여 획득한 유·무형의 결과물(점수, 경품, 게임 내에서 사용되는 가상의 화폐로서 대통령령이 정하는 게임머니 및 대통령령이 정하는 이와 유사한 것을 말한다)을 환전 또는 환전 알선하거나 재매입을 업으로 하는 행위를 금지하며, 이를 위반한 경우에는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처하도록 규정하고 있다(게임산업진흥에관한법률 제32조). 따라서 이러한 규정의 취지에 따르면 법률은 명시적으로 아이템에 대한 재산성을 부정한 것으로 해석할 수 있다. 그러나 다른 한편 국세청은 2007년 7월 1일부터 온라인 게임아이템거래에 대하여 세금을 부과하기로 하였지만 이것은 아이템거래의 합법화와 전혀 무관하다는 것이 문화관광부와 국세청의 일치된 해석이라고 한다. 이와 같은 게임아이템의 과세문제에 대하여는 윤현석, 온라인게임 아이템거래의 과세문제, 인터넷법률, 제37호(2007), 101면.

51) 이 용어는 보통 password와 fishing 또는 private data와 fishing이 결합되어 만들어진 것으로 알려져 있다(Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 80면 참조). 피싱 이외에 인터넷상에서 개인정보를 알아내는 기술적인 방법에 대해서는 전지연, 개인정보 관련법제의 형사정책적 검토, 형사정책연구, 제16권 제3호(2006 가을), 45-48면 참조.

52) 스팸메일의 규제방식을 Opt-out방식에서 Opt-in방식으로 바꿔야 한다고 주장한다.

53) 컴퓨터사용사기죄에 대한 개정안에는 재산상 이익뿐만 재물도 포함하도록 규정하고 있으므로 판례에서 일관되게 인정된 절도죄와 컴퓨터사용사기죄의 관계를 어떻게 이해할 것인가가 문제된다.

고 모바일에 이러한 인터넷기능이 더하여져 모바일범죄가 빠르게 진행되고 있다. 최근에는 국내 이동전화의 가입자 수가 4천만 명을 넘어서, 1인 1이동전화시대가 되었다. 광 네트워크와 모바일 풀 브라우저의 보급확산은 PC뿐만 아니라 이동전화를 통해서도 정보검색을 쉽게 할 수 있는 환경을 제공하였다. 그 결과 최근 SK텔레콤과 KTF가 풀 브라우징 서비스[54] 도입으로 인해 국내의 모바일 검색시장이 가열되고 있다.[55]

정보통신망을 통하여 정보처리장치나 PC 등에 행해진 다양한 불법유형들이 이제는 모바일에서 발생하기 시작하고 있다. 예컨대 모바일을 통하여 스팸전화 외에 스팸문자를 이용한 광고, 협박, 욕설, 스토킹, 성적 수치심을 야기하는 문자나 화상의 배포,[56] 특정인에 대한 허위사실의 유포 등 이른바 모바일기기를 이용한 사이버폭력이 발생하고 있다. 또한 SK텔레콤과 KTF에서 서비스되고 있는 모바일 게임 '삼국지 무한대전'의 관련 커뮤니티 80여개에서 수시로 게임아이템에 대해 현금거래가 이루어지고 있다고 한다.[57] 음란한 화상이나 동영상 역시 모바일을 통하여 유포됨으로써 음란물시장을 모바일이 담당하는 것처럼 보여지는 상황이다.

인터넷뱅킹을 사용하는 것과 마찬가지로 앞으로는 모바일뱅킹의 사용도 상당수에 이를 것으로 보인다.[58] 이와 같은 상황 속에서 IT 보안전문가들은 2007년에 모바일 뱅킹에 대한 사이버공격이 기승을 부릴 것이라고 전망했으며, 현재 200개 이상의 모바일 바이러스가 발견되었고 이 수치는 거의 6개월에 2배씩 증가한다고 한다. 이러한 의미에서 장래의 사이버범죄는 모바일범죄로 변화될 것으로 보인다.

---

54) 휴대폰을 통해 다양한 유선 웹사이트에 접근할 수 있는 개념으로, 사용자는 휴대폰을 통해서도 PC로 보는 웹사이트와 동일한 형태로 볼 수 있으며, 이동통신사 무선포털이 제공하는 콘텐츠 범위를 넘어 URL 입력을 통해 유선 웹 포털로 직접 접속이 가능하다.

55) 박현주, 모바일 인터넷 시장 동향, 정보통신정책, 제19권 제7호(2007/4), 22-23면 참조.

56) 미용학원에서 강사로 일하는 이OO씨는 "나 어때?"란 제목의 문자메시지를 받았다. 무심코 메시지를 열어본 이씨는 너무 놀라 휴대전화를 떨어뜨릴 뻔 했다. 메시지를 열자 남자의 은밀한 부위를 확대해 찍은 사진이 휴대전화 화면에 가득 떠올랐기 때문이다. 이씨는 " 처음엔 너무 놀라서 말이 안 나왔고 그리고는 누군지 너무 궁금하고 찾아서 쫓아가 죽이고 싶었다"며 당시 상황을 설명하였다(http://kr.news.yahoo.com/service/news/shellview.htm?linkid=12&articleid=20070517094747632 70&newssetid=82).

57) 게임 아이템 거래 사이트 '아이템베이'(www.itembay.com)에서 이뤄진 거래내역을 확인한 바에 따르면, 엔텔리전트의 '삼국지 무한대전'시리즈와 게임빌의 '삼국쟁패 패왕전기'의 아이템들이 꾸준히 현금을 통해 거래되고 있는 것으로 드러났다. 온라인 게임에서나 이뤄지던 아이템의 현금 거래와 불법복제가 일부 모바일 게임에서도 이뤄지고 있고 점차 그 빈도가 늘어나고 있는 것으로 나타나 우려를 사고 있다.

58) 미국의 경우에는 모바일 뱅킹이 2010년까지 온라인뱅킹 서비스 이용 가구의 35%를 차지하며 핵심적인 금융 서비스 수단이 될 전망이라고 한다. 금융분야 시장조사기관 Celent는 미국 시장에서 모바일 뱅킹이 정착되면서 다른 온라인뱅킹 수단에 비해 급성장할 것이라고 내다봤다.

둘째, 웹 리얼리티에서의 범죄에 대한 평가와 대응의 문제이다. 최근에 가상세계의 하나인 Second Life라는 web reality 사이트의 이용자수가 미국을 중심으로 급증하고 있다. Second Life는 간단하게 말하면 이용자가 아바타(Avatar)를 통해 3D 환경을 돌아다닐 수 있는 가상세계로 이용자는 이 가상세계에서 채팅이나 각종 버추얼 게임을 하거나 옷이나 무기 등의 아이템을 판매해 실제로 돈을 벌수도 있다.

현실세계와는 다른 가상공간이기 때문에 일부 마니아들만 이용할 거라는 이미지가 강하지만 사실 이용하는 사람들의 대부분은 보통의 평범한 어른들로, 평균 연령은 32세이며 이용자의 43%가 여성이라고 한다. 이용자의 분포를 국가별로 보면 50%가 북미, 28%가 유럽, 11%가 아시아, 6%가 남미로 나타났으며, 지난 30일 이내에 로그인한 이용자 수는 553,000명으로 그 기간에만 1,000만 개의 이상의 상품이 만들어지고 총 90만 건의 판매가 이루어졌다고 한다.[59] 올해부터 본격적으로 일본에서도 서비스가 시작되었으며, 우리나라에도 곧 들어올 전망이다.

이와 같은 온라인 공간에서의 제2인생이 확대되면서 현실세계와 충돌할 가능성도 커지고, 통제가 어려운 범죄가 증가할 것으로 보인다.[60] 예컨대 이 가상세계 속에서 사생활침해, 명예훼손, 해킹을 통한 사이버피해, 카지노 등에서 불법도박 행위나 성매매 등 형사법적으로 검토하여야 할 내용들이 산재해있다.

3. 통합의 제안

1) 형법의 개정

사이버범죄에 형사법적 제재는 정보통신망을 매개로 하지 않는 대부분의 컴퓨터 범죄는 형법에 의하여 규율되며, 정보통신망에 의하여 매개되는 사이버범죄는 대부분 정보통신망법을 포함하여 다양한 특별법에 의하여 규율되고 있다. 결국 사이버범죄는 형법과 특별법의 이분화된 방법에 의해 처벌되고, 그 가운데 특별법은 너무 많은 법률들에 산재하여 있어 이를 정비할 필요성이 있다.

사이버범죄에 대한 형법적 규정들의 정비방안으로는 사이버범죄특별법과 같이 사이버범죄의 처벌규정을 모두 하나의 특별법 규정으로 포섭하는 방안[61]과 사이버범죄의 처벌을 원칙적으로 형법에 두고 특별히 특별법에 두어야 할 필요성이 있는 경우에 한하여 특별법으로 처벌하는 방안[62]이 제시되고 있다.

---

59) http://blog.daum.net/elekylee/11021692; http://secondlife.com/world/kr/(2007.5.5.)

60) 이정아, 정보사회 현안 분석 [3], 현실과 가상세계의 통합 '웹 리얼리티'진화, 한국정보사회진흥원, 2007.4,

61) 원혜욱, 인터넷범죄의 특징과 범죄유형별 처벌조항, 형사정책연구, 제11권 제2호(2000), 113면.

사이버범죄를 가능한 한 모두 형법전에 규율하는 것이 다음과 같은 몇 가지 이유에서 타당하다고 본다. 첫째 사이버범죄는 이미 사회에서 자주 발생하는 범죄의 유형이기 때문에 사이버범죄에 대한 처벌이 [특별한] 것이 아니라 [일반적]이라는 것을 국민들에게 인식시킬 필요가 있으며, 이를 통해 일반예방적 기능이 더 효과를 나타낼 것이기 때문이다. 둘째 형법전으로의 편입이나 형법에의 제정과 개정을 통하여 해당 행위에 대한 처벌의 정도를 다른 범죄들과 비교・검토함으로써 처벌범위에 대한 정당성을 획득하고 다른 범죄와의 체계와 형평성을 유지할 수 있기 때문이다.[63] 셋째 사이버범죄가 가지는 실무적 중요성에 비추어 장래의 법조인인 법대생이나 시험을 준비하는 학생들에게 사이버범죄에 대한 충분한 교육이 필요할 것이며, 이를 연구하는 연구자에게도 이에 대한 심도있는 연구가 요청된다. 넷째 사이버범죄에 대한 현재의 입법태도도 정보통신망이 매개된 경우에 특별법으로 규율하고 일반 컴퓨터범죄는 형법에서 규율하고 있다는 점에서 어느 정도 체계적으로 정리된 것이라고 볼 수도 있다. 그러나 컴퓨터범죄가 형법에 규정된 것과 같이 정보통신망이 매개여부를 떠나 정보통신망범죄도 그와 비슷한 방식으로 형법에 규정될 수 있는 것이다. 다만 사이버공간에서의 특유한 범죄유형은 기존의 범죄와 다른 유형이므로 유사한 관련규정조차 없다. 그러나 이러한 경우에도 해당 행위로 인한 법익침해가 형법전의 어느 범죄와 유사한 지를 파악하여 그에 포섭하고, 전혀 포섭할 규정이 없는 경우에는 새로운 장이나 절을 마련하여 처리하는 것도 가능하다.

2) 특별법규정의 형법전화

특별법의 내용들을 형법에 포섭하기 위해 어떤 방식으로 어떻게 포섭할 것인가를 모든 특별법 규정들에 대해 살펴보는 것은 이곳에서는 불가능하다. 따라서 형법전에 규정하는 방식을 두 가지 종류로 나누어 기존의 조문에 부가하여 조문화하는 방식으로 특별법의 내용을 포섭하는 범죄(사이버공간에서 발생하나 전통적 범죄와 동일한 행태나 법익이 관련된 경우)의 경우와 기존의 조문들과 완전히 독립적인 방식으로 규정되어야 할 특별법의 범죄의 경우로 나누어 볼 수 있다.

전자에 해당하는 범죄로 사이버상 음화반포죄를 예시하여 보면, 기존의 형법 제243조의 규정과 정보통신망법 제65조 제1항 제2호의 규정[64]을 결합하여 형법전에 다

62) 강동범, 전게논문, 54면; 오영근, 인터넷범죄에 관한 연구, 형사정책연구, 제14권 제2호 (2003), 330면.

63) 비슷한 취지로 강동범, 전게논문, 54면.

64) 정보통신망법 제65조 (벌칙)
① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
2. 제44조의7제1항제1호의 규정을 위반하여 음란한 부호·문언·음향·화상 또는 영상을

음의 <대안-1> 또는 <대안-2>와 같이 규정한다.

<대안-1>

제243조(음화반포등) 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

제243조의2(음화상반포등) 정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

<대안-2>

제243조(음화반포등) ① 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

② 정보통신망을 통하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

그리고 후자에 해당하는 범죄의 예로 정보통신망 무단침입과 기망에 의한 개인정보 수집범죄를 들 수 있으며, 정보통신망법 제63조 제1항과 제2항의 규정[65]을 다음과 같이 형법에 규정한다.

제 ○ 장 정보통신망에 대한 죄<신설>

제OOO조(무단침입) 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

제OOO조(기망에 의한 개인정보수집) 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나, 제공하도록 유인하여 타인의 개인정보를 수집한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

배포·판매·임대하거나 공연히 전시한 자

65) 정보통신망법 제63조(벌칙)

① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.<개정 2005.12.30>

1. 제48조제1항의 규정을 위반하여 정보통신망에 침입한 자
3. 제49조의2 제1항의 규정을 위반하여 타인의 개인정보를 수집한 자

② 제1항 제1호의 미수범은 처벌한다.<신설 2004.1.29>

V. 결 론

형법에서 컴퓨터범죄를 규정한 지 이제 10년이 조금 더 지났고, 정보통신망법에서 사이버범죄를 정리하여 규정한 지 5년 정도가 지났다. 시간적으로 그렇게 많은 시간이 지난 것은 아님에도 불구하고 사이버범죄와 관련하여서는 입법적으로 많은 수정과 보완이 있었으며, 학계에서는 이에 대하여 상당히 많은 연구결과가 발표되었고, 실무에서도 적지 않은 판례가 형성되었다. 이제까지 논의된 자료와 연구논문들의 양과 깊이 그리고 판례의 축적이라면 사이버범죄에 대한 문제들은 어느 정도 해결되어 있어야 할 것으로 보인다. 그러나 아직도 사이버범죄에 대한 논의는 여전히 현재진행형이다. 그리고 이것은 앞으로도 계속하여 진행형의 연구영역이 될 것으로 보인다. 그 이유는 사이버공간에서의 범죄문제는 사이버공간이라는 일정한 범위 내에서 발생하는 범죄와 그에 대한 형사법적인 적용의 문제임에도 불구하고 사이버공간 자체가 현실공간과는 달리 지속적으로 확대되고, 그 안에서 계속하여 새로운 유형의 일탈행위들이 발생하기 때문이다. 새로운 유형의 범죄행위는 사이버공간의 확대 그리고 IT 기술과 통신매체의 급속한 발달과 변화에 따라 변화될 것이다.

그러나 여기서 사이버공간의 모든 범죄행위를 처벌의 대상으로 삼아 사이버공간을 형사법을 통하여 범죄로부터 전방위적으로 보호하려는 유혹에 빠져서는 안된다. 가상공간의 범죄가 현실공간의 범죄보다 덜하다고는 생각하지 않으나, 그렇다고 하여 그 역으로 사이버범죄는 그 침해가 엄청난 결과, 예컨대 인터넷뱅킹의 해킹에 의해 금융시스템이 완전히 마비되거나, 개인의 자료탐지로 모든 국민의 비밀이 침해되었다든가, 자료일부가 삭제 또는 변경되어 국가의 업무가 불능상태에 빠진다거나 하는 결과를 가져오는 것으로 평가해서도 곤란하다. 여전히 사이버범죄도 가상세계에서의 범죄이지만 사회 내의 가상세계이며 우리의 형법원칙은 여전히 유효하다고 볼 것이다. 따라서 형법원칙의 구체적 실현을 위하여 특별법의 내용을 <대안>과 같은 방식으로 형법전에 편입하여 사이버범죄의 과잉범죄화와 과잉형벌화를 방지하였으면 한다.

* 주제어 : 사이버범죄(cybererime), 컴퓨터범죄(computercrime), 인터넷범죄(internetcrime), 정보통신망법, 유비쿼터스형법, Internetdelikt

* 논문접수 : 2007. 7. 30. * 심사개시 : 2007. 9. 15. * 게재확정 : 2007. 9. 15.

<Zusammenfassung>

Vergangenheit, Gegenwart und Zukunft der Cyber-Kriminalität

Jun, Ji-Yun*

Es ist schon 10 Jahren vorbei, zu bestrafen die Computerkriminaltaet in koreanischem Strafrecht und 5 Jahren vorbei, zu bestrafen die Cyberkriminalitaet in dem Gegsetz ueber die Kommunikationsnetz der Information. Durch diese Zeitgaenge sind die verschiedene Regelungen gesetzgeberisch geaendert, reformiert. Um die neuartige Kriminalitaetsform wirkunsvoll bekaempfen zu koennen und die Rechtsguetern entschloss sich der Gesetzgeber schuf spezifische Tatbestaende. So wurde der Straftatbestand des Computerbetrugs, Faelschung der elektronischen Daten, Datenveraenderung, Ausspaechen von Daten, Computerspionage. Durch das besondere Gesetz sind die Internetsdelikten geregelt wie Haecking(einschliesslich die reine Haecking), Cyber Beleidung, Cyber Sexualitaetshandlung, Cyber Stalking, pornografische Verbreiten in Cyberraum usw.

Das Strafrecht muesste sich im Laufe der letzten Jahrenzehnte auf Grund der technologischer Veraenderungen immer wieder neuen Herausfordeungen stellen.

Trotzdem gilt es immer noch die strafrechtliche dogmatische Prinzipien zu entwickeln bei der Cyberkriminalitaet, die Rechtssicherheit schaffen.

* Dr. jur. Professor an der Yonsei Uni.

<토론문>

“사이버범죄의 과거, 현재 그리고 미래”에 대한 토론

박 광 민*

(1) 전지연 교수님의 발표문은 “사이버범죄의 과거, 현재 그리고 미래”라는 제목에서 함축적으로 나타난 바와 같이, 우리나라의 사이버범죄에 대한 현황과 그동안의 대응방법과 문제점 및 향후의 대응전략 등을 형사법적 관점에서 총괄적으로 고찰한 시의적절하면서도 좋은 논문으로, 저에게 많은 공부가 되었습니다. 특히 ‘유비쿼터스 형법’이라는 개념과 ‘유비쿼터스 형법에서의 새로운 범죄유형’ 및 각종의 특별법에 산재해 있는 사이버범죄 관련 규정을 형법전에 편입하기 위한 입법론적 제안은 매우 깊은 인상을 남겼습니다. 이러한 훌륭한 발표문에 대해서 사족을 달기가 매우 쑥스럽지만, 발표문 중에서 저와 다소 견해가 다른 부분과 보완이 필요하다고 생각하는 부분을 중심으로 토론을 전개할까 합니다.

(2) 먼저, 사이버범죄의 개념정의에 관한 부분이다. 발표문에서는 사이버범죄의 개념을 “전통적인 의미의 컴퓨터 범죄와 컴퓨터 네트워크를 통한 연결성을 이용하여 행해지는 범죄를 포괄하는 개념”으로 폭넓게 파악하였다.

오늘날 사이버공간에서 발생하는 범죄현상과 관련하여 「사이버범죄」, 「컴퓨터범죄」, 「인터넷범죄」, 「하이테크범죄」 및 「정보통신범죄」 등 다양한 용어가 사용되고 있다. 발표문에서도 적절히 지적하는 바와 같이 이들 개념은 법률적 용어도 아닐 뿐만 아니라, 서로 중첩적으로 사용되기도 하고 서로 내포하는 영역이 다르기도 하므로, 이들을 개념적으로 명확히 구분하는 것은 확실히 어려운 문제에 속한다. 따라서 넓은 의미로 파악하면 이들을 같은 부류로 보아도 무방하다. 그러나 첨단과학기술 특히 IT(Information Technology)기술의 비약적 발전과 더불어 새롭게 등장하는 신종범죄에 대한 신속한 파악과 이에 대한 적절한 대응을 위해서는 각각의 개념이 내포하는 차이점을 면밀히 분석하여 이들을 개념적으로 구분할 필요가 있다고 생각한다. 이러한 관점에서 「컴퓨터범죄」는 범죄의 수단 내지 대상이 되는 독립적인 컴퓨터시스템에 중점을 두어 “컴퓨터에 의한 자료처리과정과 관련되는 위법행위”라고 그 개념을 좁게 파악할 필요가 있으며, 사이버범죄는 “인터넷과 같은 정보통신망으로 연결된 컴퓨터시스템이나 이를 매개로 형성되는 사이버공간을 중심으로 발생하는 범죄행위의 총체”[1]라고 정의하여 전통적인 의미의 컴퓨터범죄를 제외하는 것이 바람직

* 성균관대학교 법과대학 교수

1) 김종섭, 사이버범죄의 현황과 대책, 형사정책 제12권 제1호(2000), 234면.

하다고 본다.

만약 사이버범죄의 개념을 위와 같이 파악한다면, 사이버범죄를 시기별로 구분한 발표문의 내용 중 1995년 형법개정 이전과 2001년 정보통신망법 제정 이전까지의 독립된 컴퓨터시스템을 중심으로 발생하는 범죄에 대한 형사법적 대응은 좁은 의미의 컴퓨터범죄에 대한 고찰이므로 큰 비중을 두지 않아도 좋을 것이다. 다만 이 부분은 사이버범죄 등장의 배경 내지 현재와 미래의 사이버범죄에 대한 합리적 대응을 위해서 형법의 태도 등을 살펴본다는 의미에서는 필요할 것으로 보인다.

(3) 둘째, 사이버범죄의 유형과 관련된 부분이다. 아마도 제한된 지면 때문인 것으로 보이지만, 발표문에서는 사이버범죄의 유형분류에 대한 기준을 생략한 채 사이버범죄의 개별 구체적 유형과 적용법조를 개관하는데 그친 점은 아쉬웠다.

사이버범죄의 유형을 일정한 기준에 따라 몇 개의 카테고리로 구분하는 것은 사이버공간이라는 새로운 공간이 창출됨에 따라 등장된 사이버범죄에 대한 적절한 형사법적 대응방안을 강구하기 위해서 필요불가결하다고 보기 때문이다. 이러한 관점에서 사이버범죄의 유형도 새로운 환경에 대비한 구성요건의 신설 또는 정비를 위한 목적론적 관점에 중심을 두어, 사이버공간에서의 전통적인 범죄유형과 사이버공간에서의 새로운 범죄유형 및 사이버공간에 특유한 불법유형으로 구분하는 견해[2]가 적절하다고 본다. 여기서 ‘사이버공간’이라는 개념은 기본적으로 ‘가상적’이어서 ‘없는 것’이라는 의미보다는 ‘비가시적’이어서 ‘눈에 보이지 않는다’는 의미에 중점을 두어야 할 것이다.

이에 따르면 “사이버공간에서의 전통적 범죄”는 새롭게 창출된 사이버공간을 이용하여 기존의 전통적인 범죄행위를 저지르는 경우로, 예컨대 사이버성폭력, 사이버명예훼손, 사이버협박, 사이버업무방해, 사이버비밀침해, 사이버사기, 사이버자료손괴, 사이버자료조작, 사이버음란물유포 등을 들 수 있다. “사이버공간에서의 새로운 범죄유형”은 사이버공간이라는 새로운 공간이 등장하면서 전통적인 범죄와는 전혀 다른 새로운 불법유형이 나타난 경우로, 사이버공간의 안전을 위협하는 해킹, 바이러스 유포 및 스팸메일 등을 들 수 있다. 그리고 “사이버공간에 특유한 불법유형”은 도메인주소를 훔치거나, 사이버머니나 아이템을 불법적으로 취득하거나 사이버캐릭터에 대한 침해행위 등을 말한다.

(4) 셋째, ‘포스트 사이버형법’ 소위 ‘유비쿼터스 형법’과 관련된 내용이다. 발표문에서는 기존의 사이버범죄가 컴퓨터 앞에서 범해지는 특성을 가지나 장래의 범죄는 이러한 장애를 넘어 언제 어디서나 사이버범죄를 범할 수 있는 형태로 진화할 것으

2) 동지: 강동범, 사이버범죄 처벌규정의 문제점과 대책, 한국형사정책학회 2007 춘계학술회의 자료집, 40면.

로 보이며, 이를 '유비쿼터스 형법'이라고 명명하고 있다.

최첨단 IT기술의 눈부신 발전과 더불어 미래의 사회는 고도화 내지 고속화된 네트워크 인프라를 기반으로 온라인과 오프라인의 구별이 모호해지고 유·무선의 통신망이 통합되는 등 일상생활의 각 부문이 유비쿼터스 컴퓨터 환경으로 재구성되는 유비쿼터스 사회가 도래될 것으로 예측된다. 이로 인하여 장래의 사이버범죄는 인터넷과 새로운 기술과의 결합 등에 의한 전혀 새로운 사이버범죄가 나타날 것으로 예측되며, 이에 대한 형법적 대응을 '유비쿼터스 형법'이라고 명명한 것으로 판단된다.

그러나 형법의 기본적 속성인 최후수단성 내지 보충성을 고려하면 '유비쿼터스 형법'이라는 명칭은 전통적 형법의 적용범위를 뛰어넘는 것이며, 장래에 나타날 것으로 예측되는 범죄는 보호법익과 가벌성이 확정되지 않은 상태이므로 이를 전체형법에 확대 적용하기에는 다소 성급하다는 생각이 든다. 다만, 이를 전체형법이 아니라 유비쿼터스 사회에서의 사이버범죄에 국한하여 "사이버범죄의 유비쿼터스화" 또는 "유비쿼터스 사이버형법" 정도의 명칭은 어떨까 하는 생각이 든다. 그리고 사이버범죄의 유비쿼터스화에 따라 새롭게 발생될 것으로 예측되는 범죄유형에 대한 심도있는 논의를 전개하는 것이 바람직하다고 판단된다. 발표문에서도 이에 대해서는 "유비쿼터스 형법에서의 새로운 범죄유형"이라는 부분에서 모바일범죄와 웹 리얼리티와 같은 가상 사이트에서의 범죄에 대한 평가와 대응 등 자세한 설명을 하고 있다.

(5) 넷째, 유비쿼터스 형법에서의 문제점에 관한 부분이다. 발표문에서는 이를 세분하여 ① 사이버범죄의 적용범위의 문제, ② OSP(ISP)의 책임문제, ③ 과잉범죄화와 과잉형벌화의 문제, ④ 개별적 유형에서의 문제점으로 나누어 매우 심도있는 논의를 전개하고 있다. 발표문에서의 주장내용은 대체로 저의 생각과 비슷하여 특별히 언급할 필요는 없다고 본다. 다만, 개별적 유형에서의 문제점은 지면관계상 대폭적으로 생략한 것으로 보인다. 여기에서는 게임아이템이나 사이버머니의 거래와 관련된 저의 생각을 간략히 기술함으로써 발표자의 생각을 듣는 기회를 얻고자 한다.

게임아이템이나 사이버머니의 거래와 관련하여서는 아이템 매수 후 비용미지급 혹은 비용수령 후 아이템 미지급, 위탁관리 아이템의 횡령·배임, 해킹을 이용한 아이템 갈취, 폭행·협박 등을 통한 아이템 강취 등의 범죄행위가 빈발하고 있으므로 이러한 행위에 대한 재산범죄를 인정할 수 있는가가 문제된다. 이에 관하여 판례는 사기죄(서울지법 2004. 2. 16. 2003고단10839 판결 등), 정보통신망법위반죄(서울지법 2003. 6. 3. 2003고단3578 판결), 컴퓨터사용사기죄(부산지법 2004. 10. 7. 2004고단3425, 4613 판결), 강도죄(서울고등법원 2001. 5. 8. 2000노3478 판결), 공갈죄(서울지법 서부지원 2000. 11. 8. 2000고단1366 판결)를 인정하는 등 유사한 행위에 대해 일관된 입장을 유지하지 않고 있다. 학설상으로도 아이템의 재물성을 부정하는 데에는 거의 의견이 일치되고 있으나, 재산상의 이익으로 인정함에는 의견일치를 보이지 않고 있다.

생각건대, 아이템의 관리는 현실사회의 재물에 대해 적용되는 물리적인 관리가 아니라, 게임사측의 게임서버와 게이머들의 PC에 깔린 고객간의 연속적인 정보나 명령교환에 의해 가능하도록 되어 있는 게임서비스의 한 기능에 불과하다. 따라서 재물의 개념을 유체성설 뿐만 아니라 통설인 관리가능성설을 따른다 하여도, 아이템은 재산죄의 객체로서 재물개념에 포섭되기는 어렵다. 그러나 아이템은 현실사회에서 현금거래의 객체가 되고 있고 온라인 경제시장에 있어서도 그 거래비중이 급속히 확대되고 있으므로, 경제적 재산개념에 입각하여 경제적 가치 있는 재산상의 이익으로 파악하는 것이 타당하다고 본다.[3)]

(6) 마지막으로, 통합의 제안과 관련한 부분이다. 발표문에서는 형법과 정보통신망법을 비롯한 다양한 특별법에 산재되어 있는 사이버범죄를 가능한 한 모두 형법전에 편입시킬 것을 주장하고, 특별법규정의 형법전화를 위한 구체적 방안을 제시하고 있다.

생각건대 방만한 특별법의 제정으로 인한 과잉범죄화와 과잉형벌화의 문제점 뿐만 아니라 형법상의 다른 범죄들 간의 체계성과 형평성 등의 유지를 위해서는 사이버범죄도 원칙적으로 형법전에 통합하는 것이 바람직하다. 이러한 관점에서 보면 앞에서 설명한 사이버범죄의 유형에서 첫째의 “사이버공간에서의 전통적 범죄”는 현실공간에서 처벌되는 범죄가 사이버공간을 통하여 이루어지고 있으므로 그 가벌성에 의문도 없고 전통적인 범죄와의 균형을 위하여 형법전에 쉽게 편입시킬 수 있다. 또한 둘째의 “사이버공간에서의 새로운 범죄유형”경우도 그 가벌성을 쉽게 확정할 수 있고 현실세계의 법익에 직접적으로 영향을 미치고 있으므로 기존의 형벌법규의 보완을 통하여 형법전에 편입시킬 수 있다. 그러나 셋째의 “사이버공간에 특유한 불법유형”의 경우에는 사이버공간에서만 관계된 것으로 기존의 법적 개념과 괴리가 발생할 뿐만 아니라, 그 가벌성의 확정에도 어려움을 발생시키므로 형법전의 편입이 용이하지 아니하다. 또한 사이버범죄의 고유의 특성상 신속하게 변화・발전하는 유비쿼터스 컴퓨터 환경에 적절히 대처하기 위해서도 형법전에 편입시키기 보다는 특별법의 형태가 바람직할 수도 있다. 따라서 사이버범죄의 처벌을 원칙적으로 형법전에 두지만, 특별히 특별법으로 규율할 필요가 있는 경우에는 예외적으로 특별법에 두는 방안이 합리적이라고 본다.[4)] 다만, 사이버범죄에 대한 현행의 형법과 산재해 있는 특별법의 규정은 빠른 시일내에 전면적으로 정비하여 형법상의 다른 범죄들 간의 체계성과 형평성을 유지시키고, 과잉범죄화 과잉형벌화의 문제점을 해소시키는 것이 바람직하다고 본다.

---

3) 동지: 변종필, 인터넷게임 아이템과 재산범죄, 인터넷법률 제19호(2003/09), 47면; 홍승희, 정보재산권의 형법적 보호, 형사정책연구 제16권 제3호(2005 가을), 105면.

4) 동지: 오영근, 인터넷범죄에 관한 연구, 형사정책연구 제14권 제2호(2003), 330면; 강동범, 앞의 논문, 54면.