사이버범죄의 주요동향과 형사정책적 과제

정 완*

국문요약

전 세계의 인터넷사용인구는 현재 10억을 돌파한 것으로 보이며, 국내에서도 지난 2006년말 현재 3천4백만 명을 넘어섰다. 이렇게 많은 사람들이 이용하는 인터넷공간은 전자상거래의 발달 등 유익한 발전을 가져왔지만, 사이버음란물, 사이버폭력, 인터넷사기, 사이버도박 등 사이버범죄의 증가를 초래하였다.

사이버범죄의 규제가 어려운 이유는 첫째, 소프트웨어 개발, P2P 서비스 등장 등 인터넷 기술의 급속한 발전은 누구에게나 쉽게 불법·유해사이트 개설을 가능하게 하고 있고, 둘째, 음란 스팸메일이나 상시접근이 가능한 해외 한글음란사이트에 대한 차단대책을 찾기가 쉽지 않으며, 셋째, 불건전사이트의 규제는 '표현의 자유' 문제로 인해 일률적 제한이나 통제에 어려움이 있다는 점 등이다.

이러한 한계를 의식하고 보다 효율적인 사이버공간 규제를 위해서는 각종의 가능한 정책적 개선과 함께, 무엇보다도 '자율규제의 활성화'가 가장 중요하다고 하겠다.

본문에서는 사이버범죄의 심각성에 대하여 논의해 보고 그 형사정책적 과제에 관하여 고찰하고자 하는바, 사이버범죄의 실태, 사이버범죄의 주요동향, 사이버범죄의 발생경로 등에 대하여 차례로 살펴보고, 사이버범죄의 피해방지책을 검토한 후, 형사정책적 과제를 제시하는 것으로 결론에 갈음하고자 한다.

* 경희대학교 법과대학 교수, 국제법무대학원 인터넷법무학과 주임교수, 법학박사

Ⅰ. 서 언

전 세계의 인터넷사용인구는 현재 10억을 돌파한 것으로 보이며,[1] 국내에서도 지난 2006년말 현재 3천4백만 명을 넘어섰다.[2]

이렇게 많은 사람들이 이용하는 인터넷공간은 순기능으로서 사이버쇼핑몰[3] 등 전자상거래의 발달을 포함한 많은 유익한 발전을 가져왔지만, 그 역기능으로서 사이버음란물의 범람, 사이버폭력의 확산, 인터넷사기의 증가, 사이버도박의 증가 등 다양한 사이버범죄를 초래하여 형사정책분야에서의 과제의 영역을 현실공간에서 사이버공간으로 크게 넓혀 놓았다.

사이버범죄의 개념은 아직 학문적으로 정립된 것은 아니지만 일반적으로 '사이버공간에서의 범죄현상'을 의미한다고 할 수 있다. 과거 컴퓨터범죄, 정보통신범죄, 하이테크범죄 등의 용어가 사용되었으나 현재는 사이버범죄라는 용어가 널리 사용되고 있다.

컴퓨터와 정보통신기술의 결합으로 등장한 인터넷이라는 새로운 생활공간을 일반적으로 '사이버공간'이라고 부르는데, 그러한 새로운 생활공간에서 행하여지는 범죄적 현상에 대하여 형사법적 검토를 함에 있어서는 이론적 관점보다는 현상적 맥락에서 파악하는 용어가 타당할 것이므로 사이버공간에서의 범죄현상을 아우를 수 있는 용어로 '사이버범죄'라는 용어는 매우 적절하다. 결국, 사이버범죄란 "컴퓨터범죄를 포함하여 사이버공간에서 행하여지는 모든 범죄적 현상"을 의미한다고 하겠다.[4]

이하에서는 사이버범죄의 심각성에 대하여 논의해보고 그 형사정책적 과제에 관하여 고찰하고자 하는바, 먼저 사이버범죄의 실태, 사이버범죄의 주요동향, 사이버범죄의 유통경로 등을 차례로 살펴보고, 사이버범죄의 피해방지를 위한 예방책을 고찰한 후, 사이버범죄분야의 형사정책적 과제로

---

1) 2005년말 현재 전 세계의 인터넷이용자수는 980,387,000명이고, 당시 한국의 인터넷이용자수는 33,010,000명으로 미국, 중국, 일본, 인도, 독일에 이어 제6위의 순위를 보였다. 한국인터넷진흥원 인터넷이용자통계 http://isis.nida.or.kr 참조

2) 우리나라 전체 인터넷이용자수는 2006년 12월 현재 34,120,000명이고 전체 인구대비 이용률은 74.8%에 달한다. 한국인터넷진흥원 인터넷이용자통계 http://isis.nida.or.kr 참조.

3) 2006년도 사이버쇼핑몰 거래규모는 13조4,596억원에 달하였다. 한국인터넷진흥원 인터넷통계뉴스 http://isis.nida.or.kr 참조.

4) 강동범, "사이버범죄와 형사법적 대책" 형사정책연구 2000년 제42호 참조.

서 정책적 대응방안을 제시함으로써 결론에 갈음하고자 한다.

Ⅱ. 사이버범죄의 실태

1. 경찰청 사이버테러대응센터 통계자료

가. 사이버범죄의 발생건수

사이버범죄의 발생건수는 2001년도 3만4천여건, 2002년도 6만여건, 2003년도 6만8천여건, 2004년도 7만7천여건, 2005년도 8만8천여건, 그리고 지난해인 2006년도에는 8만2천여건으로 꾸준한 증가추세를 보이고 있다.[5]

아래 표에서 '사이버테러형범죄'란 "정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해장비를 이용한 컴퓨터시스템과 정보통신망 공격하는 행위"를 말하고, '일반사이버범죄'란 "사이버 공간을 이용한 일반적인 불법행위로서 사이버 도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보유출 등의 행위"를 말한다.[6]

(단위 : 건)

구 분	계	사이버테러형 범죄	일반사이버범죄
2006	82,186	20,186	62,000
2005	88,731	21,389	67,342
2004	77,099	15,390	61,709
2003	68,445	14,241	54,204
2002	60,068	14,159	45,909
2001	33,289	10,638	22,651

5) 사이버범죄는 도표에서 보는 바와 같이 매년 증가추세를 보이고 있는데, 유독 2006년도에 전년도보다 약간 감소한 현상을 두고, 경찰청에서는 특별한 의미를 부여하고 있는 것 같다. 하지만 몇 년 더 발생건수 통계를 지켜보고 판단해야 할 것으로 보인다.

6) 사이버테러대응센터 홈페이지 http://www.ctrc.go.kr 참조.

나. 사이버범죄 검거인원

사이버범죄의 발생에 따른 검거인원 또한 2001년도 2만4천여명, 2002년도에 4만7천여명, 2003년도 5만6천여명, 2004년도 7만여명, 2005년도에 8만여명, 2006년도에 9만여명 등으로 꾸준한 증가추세를 보이고 있다.

(단위 : 건(명))

구 분	계	사이버테러형 범죄	일반사이버범죄
2006	70,545(89,248)	15,979(17,498)	54,566(71,750)
2005	72,421(81,338)	15,874(17,371)	56,547(63,967)
2004	63,384(70,143)	10,993(11,892)	52,391(58,251)
2003	51,722(56,724)	8,891(10,047)	42,831(46,677)
2002	41,900(47,252)	9,707(10,762)	32,193(36,490)
2001	22,693(24,455)	7,595(8,099)	15,098(16,356)

2. 대검찰청 첨단범죄수사부 인터넷범죄수사센터 통계자료

경찰청과는 별도로 검찰청에서 처리하고 있는 사이버범죄 단속실태는 인터넷범죄수사센터가 공개한 컴퓨터범죄의 유형별 처리현황에 제시되어 있다.

1997년부터 2005년까지의 기간 동안 제시된 사이버범죄의 단속건수를 보면 공용전자기록손상등, 전자문서관련죄, 전산업무방해죄, 전자기록비밀침해죄, 컴퓨터사용사기죄, 전자기록손괴죄, 정보통신망법위반죄, 개인정보보호법 위반죄, 기타 특별법 위반죄 등으로 유형을 분류하여 통계가 제시되어 있는데, 1997년도에 132건 232(71)명, 1998년도에 195건 354(82)명, 1999년도에 326건 500(64)명, 2000년도에 802건 1,074(122)명, 2001년도에 2,353건 3,143(331)명, 2002년도에 5,722건 7,198(990)명, 2003년도에 12,501건 15,575(1,745)명, 2004년도에 11,685건 15,814(1,104)명, 2005년도에 12,672건 19,234(1,766)명 등으로 꾸준한 증가추세를 보이고 있으며, 9년간 총 46,388건에 63,124명 입건, 6,275명 구속으로 나타나고 있다.

특히 사이버범죄의 중심법이라고 할 수 있는 정보통신망 이용촉진 및

정보보호에 관한 법률 위반사범의 숫자는 크게 높아 9년간 총 25,568건에 32,601명 입건, 1,422명 구속으로 나타났다.

컴퓨터범죄 유형별 처리현황(1997년～2005년)

유 형	처 리		
	연 도	건	명(구속)
공용전자기록손상등	'97~'02	.	.
	'03	2	4(0)
	'04	1	2(0)
	'05	2	4(1)
	계	5	10(1)
전자문서관련죄	'97	10	28(5)
	'98	9	19(5)
	'99	12	15(3)
	'00	15	17(3)
	'01	76	108(35)
	'02	241	285(62)
	'03	535	694(177)
	'04	890	1,442(282)
	'05	2,406	5,752(1,133)
	계	4,194	8,360(1,705)
전산업무방해	'97	9	16(12)
	'98	5	9(0)
	'99	7	7(1)
	'00	35	41(8)
	'01	43	55(3)
	'02	30	45(1)
	'03	26	43(2)
	'04	33	39(8)
	'05	27	35(0)
	계	215	290(35)

전자기록비밀침해	'97	2	4(3)
	'98	2	3(0)
	'99	4	10(0)
	'00	4	4(0)
	'01	5	9(0)
	'02	8	8(0)
	'03	10	16(0)
	'04	7	10(0)
	'05	3	3(1)
	계	45	67(4)
컴퓨터사용사기	'97	62	88(27)
	'98	131	206(67)
	'99	194	253(49)
	'00	247	325(66)
	'01	428	588(146)
	'02	1,346	1,603(680)
	'03	2,403	2,777(846)
	'04	1,634	2,040(323)
	'05	1,208	1,465(203)
	계	7,653	9,345(2,407)
전자기록손괴	'97	.	.
	'98	3	5(0)
	'99	3	6(0)
	'00	9	9(1)
	'01	8	10(2)
	'02	16	20(1)
	'03	8	9(0)
	'04	12	18(0)
	'05	12	12(1)
	계	71	89(5)

정보통신망법	'97	21	31(5)
	'98	21	27(2)
	'99	54	96(7)
	'00	447	607(37)
	'01	1,695	2,174(138)
	'02	4,024	5,152(244)
	'03	5,531	7,030(345)
	'04	6,222	7,775(310)
	'05	7,553	9,709(334)
	계	25,568	32,601(1,422)
개인정보보호법	'97	28	65(19)
	'98	24	85(8)
	'99	52	113(4)
	'00	45	71(7)
	'01	98	199(7)
	'02	57	85(2)
	'03	72	114(2)
	'04	75	131(5)
	'05	112	215(10)
	계	563	1,078(64)
기타 특별법	'03	3,914	4,888(373)
	'04	2,811	4,357(176)
	'05	1,349	2,039(83)
	계	8,074	11,284(632)

컴퓨터범죄의 유형별 처리현황 종합통계 (1997년～2005년)

범죄유형	처 리		
	기 간	건 수	인원수(구속자수)
공용전자기록손상등	1997~2005	5	10(1)
전자문서관련죄	1997~2005	4,194	8,360(1,705)
전산업무방해	1997~2005	215	290(35)
전자기록비밀침해	1997~2005	45	67(4)
컴퓨터사용사기	1997~2005	7,653	9,345(2,407)
전자기록손괴	1997~2005	71	89(5)
정보통신망법	1997~2005	25,568	32,601(1,422)
개인정보보호법	1997~2005	563	1,078(64)
기타 특별법	2003~2005	8,074	11,284(632)
연도별 컴퓨터범죄 발생현황	1997	132	232(71)
	1998	195	354(82)
	1999	326	500(64)
	2000	802	1,074(122)
	2001	2,353	3,143(331)
	2002	5,722	7,198(990)
	2003	12,501	15,575(1,745)
	2004	11,685	15,814(1,104)
	2005	12,672	19,234(1,766)
	계	46,388	63,124(6,275)

Ⅲ. 사이버범죄의 주요동향

1. 사이버음란물 유통

요즘 인터넷에는 유명연예인들의 성관계장면이 녹화된 동영상이나 국내외에서 제작된 몰래카메라 동영상을 비롯한 수많은 음란 화상 및 동영상들로 가득 차 있고 이를 손에 넣기 위하여 많은 청소년 및 성인들이 시간을 헛되이 보내는 등 중독증세를 보이고 있어 우리 사회가 크게 병들고 있음을 짐작케 한다.[7]

또한 청소년들 사이에서 많이 이용되고 있는 화상채팅에 있어서도 음란화상과 동영상을 주고받는 행태가 계속 늘어나고 있으며, 또한 이메일의 역기능으로 크게 사회문제가 되고 있는 스팸메일의 증가에 있어서도 음란메일이 크게 한 몫을 하고 있는 점들을 언급하지 않을 수 없는 상황이다.

최근에는 UCC[8]의 범람추세와 함께 대형 포탈사이트에마저 음란동영상이 장시간 게재되는 사건이 잇따라 발생되어[9] 정부, 포털사이트 사업자, UCC 사업자 등이 대책회의를 통하여 사이버음란물 차단대책을 발표하기에 이르렀다.[10]

이와 같이 사이버공간에 넘쳐나는 음란물에 대한 보다 효과적인 대응책이 매우 절실한 상황이지만, 최근에 미국 연방대법원이 인터넷포르노금지법에 대하여 표현의 자유를 규정한 헌법을 위반하였다는 판결을 내림으로써

---

7) 사이버음란물의 유통과 규제에 관한 깊이 있는 내용에 대하여는 정 완, "사이버음란물의 유통과 규제" 형사정책연구 2000년 제41호 참조.

8) User Created Contents의 약자로 인터넷이용자들이 새롭게 창작한 콘텐츠이다. 대부분 동아리나 동호회 등에서 직접 제작되어 저작권 침해문제가 거의 없다는 장점이 부각되어 이용자들에게 계속 확산중인 동영상 콘텐츠이다. 그러나 내용상 음란물에 해당하는 것들이 자주 노출되는 문제가 발생한다.

9) 경향신문 "유명 포털에 포르노동영상 6시간 노출, 물의" http://news.khan.co.kr 2007.3.19자 기사 및 머니투데이 "네이버, 다음에서도 음란물 노출사고" http://www.moneytoday.co.kr 2007.3.21자 기사 등 참조.

10) 첫째, 정부와 민간업체의 모니터링 및 대응 체계 강화, 둘째, 해외사이트에 대한 기술적 차단 강화, 관리 소홀 사업자에 법적 제재 강화, 넷째, 이용자·사업자의 자율적 책임의식 강화, 다섯째, 대국민 캠페인 등 인터넷 윤리의식 확산 등이 그것이다. 정보통신부 2007.3.26자 보도자료 "정부, 민간인터넷업체와 함께 음란물 차단에 적극 나서기로" 내용 참조.

사이버공간상의 음란물에 대한 정부차원의 대응을 매우 힘들게 하고 있다.[11]

2. 소프트웨어 불법복제

BSA(Business Software Alliance, 사무용소프트웨어연합회) 2006년 보고서에 따르면 전 세계의 2005년 소프트웨어 불법복제율은 35%이고 매년 감소 경향을 보이고는 있지만 여전히 세계 소프트웨어산업을 어렵게 만드는 가장 큰 원인이 되고 있다. 지역적으로 서유럽, 북미, 중동 · 아프리카, 라틴아메리카지역은 모두 불법복제율이 감소하고 있는 추세이나 동유럽의 불법복제율은 상당히 높은 편이며, 아시아 · 태평양의 불법복제율은 1996년 이래 최고 수준인데 이는 중국의 높은 불법복제율이 그 원인이다.[12]

※ BSA의 전세계 SW불법복제율 변화추이('96~'05)

구분	'96	'97	'98	'99	'00	'01	'02	'03	'04	'05
미국	27%	27%	25%	25%	24%	25%	23%	22%	21%	21%
영국	34%	31%	29%	26%	26%	25%	26%	29%	27%	27%
일본	41%	32%	31%	31%	37%	37%	35%	29%	28%	28%
한국	71%	67%	64%	50%	56%	48%	50%	48%	46%	46%
중국	96%	96%	95%	91%	94%	92%	92%	92%	90%	86%
세계평균	43%	40%	38%	36%	37%	40%	39%	36%	35%	35%

한국의 2005년도 불법복제율은 46%로 1996년도의 71%에서 꾸준히 감소해오고 있다. 이는 미국(21%), 영국(27%), 일본(28%) 등 선진국과는 상당한 격차가 있는 반면, 같은 아시아지역 내의 중국(86%)보다는 월씬 낮은 수치이다.

---

11) 미국 연방대법원은 2007년 3월 미성년자의 사이버음란물 접근을 허용한 음란사이트 운영자를 처벌하는 내용의 아동온라인보호법(Child Online Protection Act, 1998)이 헌법상 표현의 자유를 침해한다고 판결하였다. 뉴시스, "미법원, 아동온라인법에 위헌판결" http://www.newsis.com 2007.3.23자 기사 및 한국일보, "포르노규제보다는 표현의 자유가 우선" http://www.hankooki.com 2007.3.23자 기사 등 참조.

12) 컴퓨터프로그램보호위원회 홈페이지 http://www.socop.or.kr 참조.

국내에서 조사한 통계를 보면 국내의 불법복제율은 50%보다 약간 더 높게 나타나고 있으며 이는 기업과 기관의 불법복제율만을 계산하였을 때의 수치이고, 개인의 불법복제율(75%)을 반영하면 전체 불법복제율은 60%에 이르는 것으로 나타났다. 개인의 경우 4명중 3명은 불법복제 소프트웨어를 이용하고 있다는 뜻이 된다.

이처럼 많이 이용되고 있는 불법복제소프트웨어는 친구나 동료로부터 얻는 경우가 50%를 넘고, 컴퓨터를 구입할 때 미리 설치하는 경우가 20%, 인터넷을 이용하여 얻는 경우가 10% 정도로 나타나고 있지만, 최근에는 접근이 손쉬운 인터넷을 통한 불법복제(다운로드)가 급격히 늘고 있는 추세여서 그 심각성을 더해가고 있다. 인터넷을 통한 불법복제경로는 이른바 와레즈(Warez) 사이트에서 다운로드하는 경우(30%)와 소리바다 등 P2P 방식의 다운로드(30%)가 중심을 이루고 있고, 기타 팝폴더, 웹하드, PD박스 등 개인정보 저장공간을 이용하거나 FTP에 의한 전송 등에 의해서도 불법복제가 많이 행해지고 있다.[13]

3. 사이버폭력

최근 인터넷을 통한 정보전달 등 유통이 매우 활발해지고 있어 인터넷의 발달전망을 밝게 하고 있지만, 이와 함께 각종 뉴스에 등장하는 개별 사건마다 인터넷이용자들의 활발한 개인적 의견이 댓글 등의 형태로 제시됨에 따라 욕설이나 모함 등 근거 없는 각종의 모욕 또는 명예훼손행위가 크게 늘고 있어 크게 사회문제화하고 있다.[14]

야당 당수나 대통령 등 유명정치인을 대상으로 한 사진합성물에 의한 명예훼손 행위가 우리를 놀라게 하였을 뿐 아니라 연예인 X파일 공개 및 유포에 의한 명예훼손사건, 간호사들의 신생아 학대사진 유통사건, 개똥녀 사건, 된장녀 사건, 군삼녀 사건 등 하루가 멀다 하고 우리의 관심을 끄는 사이버폭력 사례가 인터넷 등 사이버공간을 장식하고 있는 상황이다.

---

13) 소프트웨어 불법복제에 대한 실태와 문제점 및 대응방안에 대한 상세한 내용은 정 완, 소프트웨어 불법복제실태와 법제도적 개선방안, 한국형사정책연구원 보고서 2003 참조.

14) 사이버폭력의 실태와 법제도적 문제점에 대한 상세한 내용은 정 완, 사이버폭력에 대한 법제도적 대응방안 연구(정보통신윤리위원회, 2005) 참조.

최근의 게시물 및 댓글 등에 의한 피해사례를 도표로 정리하면 다음과 같다.[15)]

<게시물, 댓글 등에 의한 최근 피해사례>

사건명	일 시	내 용
군삼녀 사건	2007	남성들의 군복무기간에 관한 한 여학생의 인터뷰 내용이 실명과 동영상으로 알려지면서 이 여학생에 대한 무차별적 폭언이 댓글로 행해져 이 여학생의 정신적 피해가 큰 것으로 보도됨.
된장녀 사건	2006	사치스런 생활을 하는 여성들에 대한 비난성 댓글에 의한 사이버폭력이 도를 지나치고 있음
MBC 음악캠프 나체 시위 장면	2005.8	MBC 음악캠프라는 프로그램에서 출연가수 일부가 나체로 시위를 한 내용의 비디오물이 인터넷을 통하여 확산되고 있어 추가 피해가 우려되고 있음
개똥녀 사건	2005.6	지하철에서 애완견의 배설물을 치우지 않은 여성 사진 및 동영상 유포
체벌여교사 자살 사건	2005.4	체벌 혐의를 받은 여교사가 자살하자 체벌 사실을 알렸던 학생들이 가출한 사건
신생아 학대사건	2005.4	간호사들이 자신의 홈페이지에 올린 신생아 학대사진이 유포되어 문제됨
트위스트김 사건	2005.4	연예인 트위스트킴이 음란사이트의 운영자로 몰려 피해
연예인 X파일 사건	2005.1	유명연예인 99명의 신상정보를 담은 미확인 사실이 유포됨
왕따 동영상 사건	2004.2	왕따동영상이 촬영된 중학교의 교장이 자살

'사이버폭력'이란 아직 확정된 개념은 아니며 다의적이고 논쟁적인 개념이다. 대체로 사이버공간에서 행해지는 온갖 형태의 폭력적 표현행위를 포함하는 개념이라 하겠다.

사이버폭력의 일반적 사례로는 특정인에 대하여 모욕적인 언사나 욕설 등을 게시판에 올리거나 메모 또는 채팅 상에서 행하는 '사이버모욕', 특정인에 대한 허위의 글이나 명예에 관한 사실을 인터넷게시판 등에 올려

15) 박종현, "사이버폭력 피해구제제도 현황 및 문제점" 2005.7.21 정보통신윤리위원회 세미나 발표자료에 일부 첨삭함.

불특정 다수인에게 공개하는 '사이버명예훼손', 인터넷상에서 음란한 대화를 강요하거나 성적 수치심을 주는 대화로 상대방에게 정신적 피해를 주는 '사이버성희롱', E-mail로 특정인 또는 불특정 다수인에게 음란·폭력적인 내용의 글 또는 영상물을 발송하는 '음란스팸메일', 인터넷 또는 PC통신상의 대화방, E-mail 등 정보통신망을 이용하여 특정인에게 원하지 않는 접근을 지속적으로 시도하거나 성적 괴롭힘을 행사하는 '사이버스토킹', 인터넷이나 PC통신망의 대화방을 이용하여 원조교제를 유도하거나 알선·중개하여 10대 매매춘을 확산시키는 '사이버성매매', 유명연예인의 몰래카메라 등 현실세계에서 만들어진 내용을 유통시키는 '사이버음란물' 등을 들 수 있다.

사이버공간은 빠른 전파력이 특징인데다 익명성이 상당 부분 보장돼 정치인이나 연예인 등 유명인뿐 아니라 누구나 폭력의 희생양이 될 수 있다는 점에서 이와 같은 사이버폭력에 관한 문제 심각성이 더해지고 있다.

정보통신윤리위원회 통계자료에 따르면 사이버폭력 피해상담 건수가 해마다 늘고 있고 그 주요내용은 명예훼손 또는 모욕에 관한 것으로 나타나고 있다.[16]

■ 사이버 폭력 피해 상담내용 분석(2001 - 2007. 3)

(단위 : 건)

구 분	계	피 해 내 용			
		명예훼손(모욕)	성폭력	스토킹	기타
2001	1,054	278(33)	204	22	550
2002	3,616	1,248(115)	224	53	2,091
2003	4,217	1,916(894)	557	95	1,649
2004	3,913	2,285(979)	322	81	1,225
2005	8,406	5,735(1,802)	889	193	1,589
2006	7,050	4,751(1,641)	968	184	1,147
2007. 3	1,361	923(422)	125	36	277
합계	29,617	17,136(5,886)	3,289	664	8,528

16) 정보통신윤리위원회 홈페이지 http://www.kiscom.or.kr 통계자료 참조.

4. 인터넷사기

"저희 은행의 인터넷뱅킹 보안 시스템을 강화하였습니다. 고객님께서는 저희 은행 홈페이지에 접속하신 후 개인정보를 확인해 주시기 바랍니다."

이것은 피싱메일의 전형적인 내용이다. 또한 개인정보를 갱신하라는 메일 통보와 함께 보안에 취약한 사이트를 해킹해 해당 사이트처럼 위장한다. 대부분의 피싱은 일반인이 거래하는 은행이나 인터넷사이트 등의 이름을 도용해 메일을 보내고 위장된 사이트로 접속을 유도해 은행 계좌번호, 금융거래용 비밀번호, 기타 개인정보 등을 입력하게 한 후 이를 이용해 불법으로 타인의 예금을 이체하거나 물품구매 사기 등에 악용한다.[17]

아직까지 국내에서 피싱 기법에 의한 예금 인출 등 금융사고 피해사례가 보고되지는 않고 있다. 이는 우리나라의 경우 전자 금융거래에 공인인증서를 사용하고 있고, 공인인증서 비밀번호와 보안카드 번호 등 여러 장치가 돼 있어 미국 등 여타 국가보다 상대적으로 안전하기 때문이다. 그러나 우리나라 역시 확률이 낮을 뿐 피싱의 안전지대는 아니다. 인터넷을 이용한 뱅킹, 쇼핑몰, 게임 등 전자거래가 활발한 국내의 인터넷 환경에서 피싱 사고 발생 가능성은 항시 존재하기 때문에 각별한 주의가 요구된다. 또 공인인증서는 통상 PC의 하드디스크에 보관되는데, 해킹을 당한 PC 내의 공인인증서는 해커가 절취할 수도 있다.

2004년 KISA에 접수된 국내 위장 홈페이지 신고 건수는 총 220건으로, 월평균 18건의 보안 취약 사이트가 해외 피싱사고의 경유지로 악용된 것으로 나타났다. 2005년 1월에는 61건이 신고돼 지난해에 비해 급증하는 추세를 보였으며, 6월에는 100건을 넘어섰다. 이러한 신고 건수의 증가는 보안이 취약한 일부 국내 웹서버들이 해킹을 당해 외국 금융기관, 쇼핑몰 등의 위장 홈페이지로 악용되는 사례가 증가했음을 의미한다. 실제로 안티피싱 워킹그룹(APWG)에 따르면 우리나라는 2005년 4월 기준 경유지로 악용된 서버를 보유한 국가 순위에서 3위를 차지했다.[18]

한편, 2004년부터 전 세계를 들끓게 했던 인터넷 사기방식인 '피싱

17) 인터넷사기의 실태와 법제도적 대응방안에 대하여는 정 완, "인터넷사기의 신종유형과 법제도적 대응방안" 경희법학 2005년 제40권 제1호 참조.

18) 전자신문 2005.7.26자 "[열린마당] 피싱으로부터 안전하십니까" 기사참조.

(Phishing)'에 이어 이번에는 '파밍(Pharming)'이 최근 신종 인터넷 사기 수법으로 부상하고 있다. 파밍은 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인네임시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도, 개인정보를 훔치는 새로운 수법으로, 기존의 피싱 공격방식보다 사용자들을 쉽게 속일 수 있어 이에 대한 대책 마련이 필요하다.

기존의 피싱 공격이 사회공학적 기법을 가미해 금융기관 등의 웹사이트에서 보낸 이메일로 위장, 링크를 유도해 개인의 인증번호나 신용카드 번호, 계좌정보 등을 빼내는 반면, 파밍은 아예 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 중간에서 탈취한다. 사용자들은 늘 이용하는 사이트로 알고 의심 없이 탈취된 해당 사이트를 이용해 개인ID, 패스워드, 계좌정보 등을 쉽게 노출시키는 것이 특징이다.

이 같은 파밍은 보통 인터넷 하이재킹(hijacking) 수법을 이용해 도메인마다 등록 만기와 등록기관 이전 등 복잡한 등록유지 절차가 있음을 악용, 특정 도메인을 강탈하는 방식을 사용한다. 파밍은 사용자가 익숙하게 이용해온 인터넷 주소 자체를 강탈해 사용하기 때문에 사용자들이 아무리 도메인 주소나 URL 주소를 유의해 본다 해도 쉽게 속을 수밖에 없어 대규모의 피해가 예상된다.[19]

Ⅳ. 사이버범죄의 발생경로

1. 인터넷카페 등 사이버커뮤니티

사이버커뮤니티는 대략 5가지 유형으로 나누어 볼 수 있다. 첫째 일반 채팅, 화상 채팅, 아바타 채팅 등 채팅을 중심으로 한 채팅사이트의 커뮤니티이고, 둘째는 카페, 동호회 클럽, 와레즈 등의 포털 사이트 내의 커뮤니티이며, 셋째는 메신저와 P2P를 이용한 커뮤니티이고, 넷째는 게시판, 방명록, 웹메일을 통한 커뮤니티, 다섯째는 온라인 게임 등을 포함한 기타

19) 디지털타임스 2005.3.18자 관련기사 참조..

커뮤니티 등이 그것이다. 인터넷 이용자수, 이용률의 증가와 더불어 주요 포탈사이트의 사이버 커뮤니티 증가 등으로 사이버공간은 이제 일상공간으로 정착되고 있음을 알 수 있다. 이러한 커뮤니티의 급속한 증가와 더불어 커뮤니티 내의 불법・청소년유해정보 유통 및 사기사건 등 사이버 커뮤니티의 역기능 문제가 제기되고 있다.

인터넷상에서 커뮤니티가 다양화되어 신유형서비스를 제공함에 따라 단순한 동호회 활동을 넘어서 정보매매를 목적으로 하는 상업성 커뮤니티까지 등장하고 있다.[20]

커뮤니티사이트에 게시된 비정상적 성행위, 잔인하게 죽은 시체 사진, 시체놀이 등 혐오감을 주는 사진도 청소년 정서에 심각한 악영향을 줄 수 있다. 이 밖에 커뮤니티사이트에 포르노 교환사이트가 존재하거나 어린이 성행위 장면 등이 게시돼 있고 게시판 등이 성인사이트로 링크되는 등의 문제점도 대두됐다. 사업자들은 음란성이 심한 일부 카페는 자체 폐쇄시키지만, 운영자가 다른 이름으로 카페를 재개설해 운영, 실질적인 제재 조치는 힘든 상황이다.

정보통신윤리위원회의 “2003 인터넷민간자율규제활동 지원사업”의 일환으로 실시된 한국여성단체협의회의 커뮤니티 사이트 실태조사에서 불건전 커뮤니티의 현황을 조사한 결과 불건전 커뮤니티는 전체 62%(4,730개), 건전 커뮤니티는 38%(2,951개)로 나타났다. 불건전 커뮤니티 4,730개는 다시 성인음란물 3,564개, 불법프로그램 863개, 사기물 127개로 콘텐츠의 절반 가까운 47%가 성인음란물임을 알 수 있다.[21]

3. 미니홈피・블로그

인터넷홈페이지가 일반화되면서 홈페이지를 제작할 줄 모르거나 제작

---

20) 이러한 커뮤니티는 연령제한 없이 무료 가입돼 청소년들의 운영, 가입이 급증하고 있으며, 특히 음란・불법자료가 많을수록 이용도가 높다. 김기봉, “인터넷상에서의 청소년보호정책의 방향과 과제” 제32회 형사정책세미나 자료, 107쪽 참조.

21) 또한 단어 필터링(검색차단)이 되는 커뮤니티 사이트도 적용 단어가 한정되어 있고 금칙어도 특수기호나 숫자 등과 조합하면 기능이 안 돼 유명무실했으며, 커뮤니티 운영자의 개인정보도 대부분 비공개와 익명이어서 청소년 여부를 확인하기 어려운 것으로 나타났다. 청소년보호위원회, 청소년 인터넷 유해환경 실태 모니터링 보고서(2003.7) 참조.

에 어려움이 있는 인터넷사용자들을 대상으로 이른바 미니홈페이지 또는 블로그를 제공하는 인터넷 포탈사업체들이 늘고 있다.

미니홈페이지나 블로그는 정해진 유형의 포맷을 가지고 이용자가 콘텐츠만 채우면 되는 방식의 홈페이지이기 때문에 그 사용자는 급속도로 늘고 있는 상황이다. 이에 따라 미니 홈피나 블로그에도 불법적인 정보를 유통시키는 사례가 크게 늘고 있는 것으로 파악되고 있다.

최근 정보통신윤리위원회는 미니홈피나 블로그를 통한 음란물 유통이 심각하다고 보고 이에 대한 집중단속을 실시하여 음란정보를 유통하고 있는 이용자에 대해 경고, 이용해지 등 시정을 요구하는 조치를 취하였다. 이 조사 결과, 일부 미니홈피와 블로그 상에서 성행위를 노골적으로 묘사한 정보, 청소년의 알몸 및 성기가 노출된 정보, 연예인의 이미지를 조작한 누드 등 다양한 형태의 음란정보가 유통되고 있는 것으로 확인됐다. 미니홈피, 블로그 상의 음란정보 중에는 아동 또는 청소년을 성적 유희의 대상으로 구체적으로 묘사하거나 집단성행위·수간 등 변태적인 성행위, 근친상간을 주제로 하는 만화정보 등 음란의 정도가 위험 수위를 넘어선 정보가 다수 유통되고 있어 청소년들의 건전한 정서함양에 심각한 악영향을 끼칠 우려가 있는 것으로 나타났다.

특히, 일부 미니홈피에서는 방문자나 댓글이 많을 경우 포인트 획득을 통해 홈피를 꾸미는데 필요한 아이템을 제공하는 등 다양한 혜택을 주는데, 이를 위해 운영자 스스로 방문자 수를 늘리기 위해 선정적인 정보를 게시하는 등의 부작용이 있었다. 또한, 타인이 운영하는 홈피·블로그의 정보를 쉽게 옮겨 올 수 있는 '퍼오기' 기능을 통해 음란물이 빠른 속도로 폭넓게 확산되고 있는 것으로 나타났다.

정보통신윤리위원회는 향후에도 지속적인 조사를 통해 인터넷상에서 유통되고 있는 음란정보에 대해 강력히 대응해 나갈 것이며, 무엇보다도 인터넷 이용자의 자율적인 정화 노력이 중요한 만큼 사업자들과의 협력을 통해 자율규제를 강화해 나가고 대국민 홍보 활동을 활발히 전개해 나갈 것이라고 밝혔다.[22]

---

22) 인터넷 상의 불법·청소년유해정보에 대한 신고는 '불법·청소년유해정보신고센터'(www.internet119. or.kr)로 하면 된다. 정보통신윤리위원회 투데이뉴스 2005.3.21자 기사 참조.

4. P2P 서비스

현재 인터넷을 통하여 유통되고 있는 각종 불법유해정보의 상당부분은 P2P 서비스에 의하여 행해지고 있다. P2P는 'peer to peer'의 약자로서 말 그대로 중앙 서버에 담겨져 있는 파일을 주고받는 것이 아니라 클라이언트 컴퓨터, 즉 각 개인이 사용하는 PC에 들어 있는 파일을 검색하고 이러한 PC 상호간의 파일교환이 이루어지는 형태를 말한다.[23]

이러한 P2P 서비스의 방식도 중앙서버가 필요했던 과거의 방식에서 중앙서버가 필요하지 않은 순수한 P2P 서비스 방식으로 변화되었다가 최근에는 분산다중방식의 P2P 서비스가 이용되기 시작하였다고 한다.[24]

중앙서버에 의하여 관리되던 초기방식의 P2P 서비스로 유명했던 회사가 미국의 냅스터(Napster)와 한국의 소리바다였다. 이러한 방식에서는 각 PC에 저장되어 있는 음악파일의 목록관리 등 중앙서버가 일정한 역할을 담당하는 것으로 대부분의 작업이 중앙서버에 의하여 이루어지게 된다.

그 후 중앙서버의 역할이 제외되고 순수하게 클라이언트 PC들 간의 자료공유가 이루어지게 된 P2P 서비스로 유명한 것이 우리가 가끔 사용해 본 적이 있는 누텔라(Gnutella), 구루구루(Guruguru) 등이다. 그리고 소리바다가 검찰에 의하여 기소된 후 저작권 문제점을 해결하였다고 주장하며 새로이 채택한 시스템이 바로 이 순수한 P2P 방식에 의한 소리바다2 였던 것이다.

최근에는 1대1 방식의 네트워크가 아닌 1대 다중 방식의 P2P 서비스가 등장하였는데 그 예로는 e동키(당나귀), 고부기(GoBoogy) 등을 들 수 있다. 이 서비스는 중앙서버를 거치지 않고 사용자끼리 직접 파일을 주고받으며 특정파일을 다운로드하면서 또다른 접속자에게 업로드가 동시에 가능하여 파일공유의 호환성이 매우 높은 장점이 있다.

5. UCC의 확산

2006년 6월 호주의 한 여대생은 UCC사이트인 유튜브에 '에멀리나

23) P2P 서비스의 개념에 대한 상세는 박익환, "P2P 서비스와 저작권문제", 한국디지털재산법학회 학술세미나 자료집, 2001.11.23 2쪽 이하 참조.
24) 구태언, "P2P 서비스의 현황과 형사책임", 정보법학 제7권 제2호, 124쪽 참조.

(Emmalina)'라는 필명으로 애완동물・운동・취미 등 자신의 일상을 공개하는 동영상을 연재했고, 이 동영상은 조회수 30만을 기록하는 폭발적인 인기를 끌며 인터넷 백과사전 위키피디아에 등재되기도 했다. 그러나 이 여대생은 이어지는 개인정보 해킹 및 악용, 음해성 동영상・악플 등에 시달리다 2개월만에 자신의 프로필과 동영상 콘텐츠를 모두 삭제했고, 유명해지는 것이 꼭 좋은 것만은 아니라는 취지의 글을 남기고 떠났다.[25] 타임지는 지난해 '올해의 발명품'으로 UCC사이트인 유튜브를 꼽았다. 현재 유튜브에 동영상을 올리는 회원은 7,200만 명에 달하며, 미국 최고의 인터넷회사인 구글은 이런 폭발력을 감안해 최대의 UCC 유통회사인 유튜브 닷컴을 한화 1조 7,000억원에 사들였다.

UCC 열풍은 이용자들의 삶에 획기적인 변화를 가져다주고 있다. UCC를 통해 누구나 스타가 될 수 있고 가공할 미디어의 힘을 발휘할 수 있는 기자나 PD가 될 수 있다. 평범한 학생, 회사원, 주부 등이 자신의 취미생활이나 일상을 담은 동영상으로 UCC 스타가 되기도 한다.

UCC는 선거결과에도 영향을 미쳤다. 2006년 미국 중간선거에서 공화당 조지 앨런 상원의원이 인도계 청년을 향해 '원숭이'라고 말하는 동영상이 퍼지자, 승리가 예상됐던 그는 낙선했다. 이처럼 UCC를 통하여 누구나 새로운 경제적 부를 창출하는 것은 물론 한 순간에 스타가 되거나 몰락하기도 한다.

UCC가 가져다주는 역기능은 프라이버시 침해, 유해정보, 저작권・초상권 침해, 명예훼손 등이다. 개인정보화 도구를 갖춘 영상세대는 소위 '뜨기 위해' 어지간한 개인정보노출은 가볍게 여긴다. 흥미를 위해 타인의 사생활 등을 쉽게 노출하고 드러내거나 무작위로 사이버 '펌질'도 마다하지 않는다.

UCC사이트를 이용하는 네티즌들은 내 개인정보와 마찬가지로 타인의 개인정보를 보호해야 한다. 그렇지 않을 경우 발생하는 인격모독이나 마녀사냥 등으로 인한 피해는 확산될 것이다. 개인들에게 팽배한 개인정보 보호 무의식증과 노출증의 확산은 결국 UCC 세상을 위협하게 될 것이다. UCC사이트 운영 기업들의 보안에 대한 시급한 대책도 필요하다.

---

25) 디지털타임스 2007년 2월 7일자 "제2의 에멀리나를 막기 위해서는" 기사 참조.

전문가들은 수십억 개의 사용자 검색, e메일 정보가 저장된 데이터베이스를 보유한 구글 같은 인터넷회사 등에서 UCC사이트를 오픈하고 있어 UCC를 통해 웜바이러스가 전파될 위험성이 대폭 증가할 수 있다고 우려하고 있다. 또 거대한 양의 데이터베이스 유출이나 해킹도 우려하고 있다.[26]

이와 같은 UCC가 음란물 제작·유통, 지적재산권 침해, 선거법 위반 등의 문제를 야기하거나 가능성이 커짐에 따라 정보통신윤리위원회, 저작권심의조정위원회, 중앙선거관리위원회 등 관련부처에서 이에 대한 단속대책을 마련하고 있다.[27]

Ⅴ. 사이버공간 규제와 표현의 자유

1. 사이버범죄의 특수성

사이버공간을 통하여 발생하는 각종 사이버범죄는 현실공간에서 행해지는 범죄행위와는 여러 가지 면에서 그 차별성이 인정된다.

예컨대 현실공간에서의 모욕이나 명예훼손은 한정된 공간에서 행해지고 그 피해의 확산도 그다지 심각하지 않다고 할 수 있고, 따라서 가해자와 피해자간의 해결에 의하여 사건이 마무리되는 것이 보통이다.

그러나, 사이버공간에서 행해지는 각종 유형의 사이버범죄는 그것이 일단 발생하면 순식간에 인터넷을 이용하는 모든 사람들에게 무제한적으로 퍼지게 되어 피해자가 입은 인격적 침해나 명예훼손의 피해는 이루 말할 수 없이 크고 회복불가능한 상태에 빠지게 된다.

또한 사이버공간의 특성인 익명성에 의하여 사이버범죄는 실명으로 나타나지 않기 때문에 사이버범죄자가 누구인지 특정하기가 매우 어렵고 퍼나르기에 의한 무수한 공범자들이 존재하므로 범죄피해에 대한 신고나 고소, 고발이 매우 어려운 특징을 가지고 있다.

---

26) 디지털타임스 2007년 2월 7일자 "제2의 에멀리나를 막기 위해서는" 기사 참조.

27) 각 부처의 대응책마련에 관한 상세한 내용은 전자신문 2007.2.13자 "건전하지 못한 UCC 꼼짝마" 기사 참조.

아울러 이러한 사건들을 지켜보는 수많은 네티즌들은 보고 싶지 않고 알고 싶지도 않는 사건들에 대하여 수많은 사람들이 피해자를 공격하는 폭력적 언사를 두 눈 뜨고 지켜볼 수밖에 없으며 관련 사진이나 각종 증거물이 인터넷을 뒤덮어 인터넷은 그야말로 쓰레기 공간으로 변해버리기 일쑤인 것이다.

이러한 사이버공간 및 사이버범죄의 특수성은 형법상의 종래의 범죄구성요건으로는 처벌하기 어려운 '특별하고 새로운 범죄'임을 보여주고 있으나 우리의 법적 규제 현실은 이를 따라가고 있지 못하며 막연한 '표현의 자유' 침해가 우려된다는 주장에 막혀 건전한 사이버문화 조성에 어려움을 겪고 있는 것이 현실이다.

2. 사이버공간상 표현의 자유의 한계

인터넷은 뚜렷한 중심이 없고 누구나 참여와 이용이 가능하며 외부의 통제나 규제가 어렵고 시간과 공간의 제약으로부터도 자유롭다는 특성을 가진다. 또한 익명성이 보장되어 상호간에 사회적 지위나 성별, 연령, 인종 등의 선행조건을 전제하지 않은 상태에서 대화와 토론이 가능한 수평적 커뮤니케이션이 가능하다. 이러한 자신의 신원을 드러내지 않는 익명성이라는 특성 때문에 실생활에서 적용되는 법규라든가 윤리·도덕과 같은 일련의 사회적 구속으로부터 벗어난 일탈행위들이 자행되는 결과를 초래하기 쉽다.

인터넷의 등장으로 인하여 포르노와 같은 음란물이 만연하고 청소년유해물에 대한 청소년의 접근이 더욱 용이해졌으며, 보이지 않는 자에 의한 통제가 가능해져 종전보다 개인정보 등 프라이버시가 침해될 위험성이 높아졌을 뿐 아니라, 사회적 연대보다는 개인의 고립화를 초래하고 있다는 비판이 있다. 또한 전자우편이라는 편리한 통신수단이 스팸메일의 형태로 악용됨으로써 개인이 정신적·물질적 피해를 입게 되는 역기능이 발생하고 있다. 또한 기존 매체와 달리 무한복제가 가능하고 신속한 전파가 그 특징인 인터넷은 저작권침해라거나 개인의 사생활침해 또는 명예훼손 행위 등이 더욱 빈번해지고 있고 사이버공간을 통하여 순식간에 확산되는 개인의 피해는 상상하기 힘들만큼 매우 심각한 상황이다.

사이버공간상 표현의 자유는 어느 정도의 수준에서 인정되고 보호되어야 할 것인가 ?

헌법재판소는 “오늘날 가장 거대하고 주요한 표현매체의 하나로 자리를 굳힌 인터넷상의 표현에 대하여 질서위주의 사고만으로 규제하려고 할 경우 표현의 자유 발전에 큰 장애를 초래할 수 있다. 표현매체에 관한 기술의 발달은 표현의 자유의 장을 넓히고 질적 변화를 야기하고 있으므로 계속 변화하는 이 분야에서 규제의 수단 또한 헌법의 틀 내에서 다채롭고 새롭게 강구되어야 할 것”이라고 하였다.[28]

그러나 어떠한 표현을 사용하든 인터넷상의 표현의 자유도 헌법 제23조 제4항의 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해해서는 안 된다는 한계를 분명히 가지고 있는 것이다. 한편, 헌법 제13조는 “모든 국민은 법률에 의하지 아니하고는 언론, 출판, 집회, 결사의 자유를 제한받지 아니한다”고 규정하고 있으므로, 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하는 행위에 대한 사이버공간의 규제는 ‘입법’을 통해서 가능한 것이라고 하겠다.

3. 사이버공간 규제와 표현의 자유의 조화

사이버범죄의 규제는 개인의 법익보호를 위하여 반드시 필요하지만 그러나 사이버공간에 대한 지나친 규제는 자칫 ‘표현의 자유’를 침해하는 결과로 이어지기 쉽다.

반대로 사이버공간에 대한 규제의 완화는 곧 자유로운 의사소통의 가능을 의미하며 이는 표현의 자유의 확장을 의미하는 것이다.[29] 그러나 만일 사이버공간의 규제가 적절히 행해지지 않는다면 사이버범죄의 피해가 발생할 경우 합리적으로 대응할 수 없게 되므로 개인의 중요한 보호법익을 지켜주지 못하는 결과를 초래할 수 있고 또한 무책임한 유언비어의 남발이나 명예훼손성 표현으로 인해 큰 사회적 혼란을 야기할 수도 있는 것이다. 결국 사이버공간 규제에 관한 논의는 이 두 가지 중요한 법익, 즉

---

28) 권영성, 헌법학원론, 498쪽 이하 참조.

29) 인터넷상 표현의 자유에 대하여는 鈴木秀美, “インタネットと表現の自由-ドイツ·マルチメディア法制の現狀と課題-” ジュリスト1153, 1999.4.1 참조.

인격권으로서의 명예와 자유권으로서의 표현의 자유를 어떻게 효과적으로 조화시킬 수 있을 것인가의 문제로 발전되어 온 것이라 하겠다.

사이버공간은 자유로운 의사표현을 위한 무한한 가능성을 지닌 공간이라는 점에서 '표현의 자유'를 가장 중요시하지 않을 수 없다. 이와 관련하여 헌법재판소는 사이버공간에서의 표현의 자유에 대하여 인터넷을 '가장 참여적인 시장, 표현촉진적인 매체'라고 하면서 "인터넷상의 표현에 대하여 질서위주의 사고만으로 규제하려고 할 경우 표현의 자유 발전에 큰 장애를 초래할 수 있다"고 하여 사이버공간에서의 표현의 자유의 중요성을 명시적으로 선언한 바 있다.[30]

사이버공간의 규제에 있어서는 이와 같은 표현의 자유를 침해하지 않도록 그 합리성과 적절성이 보장되는 전제하에 개인의 법익침해행위에 대한 보호적 차원의 규제가 될 수 있도록 조화가 이루어져야 할 것이다.

Ⅵ. 사이버범죄의 예방대책

1. 사이버윤리교육 강화

먼저, 사이버공간에 대한 올바른 이해와 활용방안에 대한 청소년, 교사, 학부모, 사업자 등 대상별 정보윤리교육의 확대실시가 매우 중요하다. 이에 따라 각종 학교와 정보통신서비스사업체에서의 사이버윤리교육 확대, 온라인 원격교육 실시, 다양한 사이버윤리교재의 개발 및 보급이 행해져야 한다.

아울러 학부모와 청소년이 동시에 참여하는 사이버윤리교육 방안도 모색해야 한다. 일회성 이벤트 행사로 끝날 것이 아니라 학부모와 청소년 등 다양한 계층이 동시에 참여할 수 있는 지속적인 교육과정의 개설이 중요하다.

---

30) 헌법재판소의 구 전기통신사업법 제53조의 위헌결정문에 표현된 구절이다. 헌법재판소 2002.6.27 결정 참조.

2. 유관기관 간 협력체제의 구축

불법・유해정보와 관련하여 유관기관 간 신고처리지연, 공조체계 미흡 등 문제점이 발생하고 있다. 정보통신윤리위원회, 검찰, 경찰 등 관련기관 간 적극적 협력이 무엇보다 중요하다. 이러한 협력방안으로 인터넷 이용자, 인터넷 사업자, 검찰・경찰, 정부유관기관을 포함하는 실무자급 협의체 구성 및 사이버범죄 신고사항 처리기관별 분류・이관 및 처리결과 안내 등에 관한 종합시스템 구축 등도 검토되어야 할 것이다. 또한 불법・유해정보의 생산・유통자 및 불법스팸발송자에 대한 신속하고 종합적인 대응을 위한 민・관 핫라인 구성・운영의 활성화도 필요하다.

3. 인터넷사업자, 민간단체 등의 자율규제 강화

해외 한글불법사이트에 대한 인터넷 사업자의 모니터링과 국제관문에서의 자율차단 확대실시뿐만 아니라 포털사업자, 인터넷정보센터(KRNIC), 인터넷서비스제공자(ISP) 등 사업자가 상시협력체제를 구축하여 스팸발송자 유동IP 차단 등에 대한 효과적 대책이 마련되어야 한다.

또한 성인정보에 대한 청소년 접근을 방지하기 위해 포털사이트 검색서비스에 성인인증제도의 철저한 시행을 유도하고 포털업체의 성인사이트 등록기준 마련 및 관리 강화가 필요하다. 또한 최근 대형화되고 있는 커뮤니티 및 채팅사이트 등에 대하여 개설자의 실명확인 및 운영자와 회원 준수 사항에 대한 사업자 공동 가이드라인 제정 및 해당 사이트 신고센터 간 핫라인 운영을 통한 불량회원 관리 강화를 위한 사업자의 자율규제를 적극 지원해야 할 것이다.

한편, 청소년유해환경감시단, 안전한 온라인을 위한 민간네트워크, 한국사이버감시단, 한국여성단체협의회, 한국 ISP협회, 한국인터넷콘텐츠산업협회, 게임비디오물 민간 합동자율지도위원회, 이메일환경개선협의체 등 수많은 민간단체와의 협조도 효율적인 규제를 위하여 필수적이다.

그러나 이러한 자율규제가 사이버범죄의 범람을 적절히 차단하기에는 여전히 역부족인 상황이며, 앞으로 무선인터넷이 활성화될 경우에는 문제

가 더욱 확대될 것으로 예상된다. 민간단체에 의한 자율규제가 효과를 발휘하려면 첫째, 기업이나 민간단체가 정부와 효율적인 협조체제를 구축하고, 둘째, 자율규제를 법제도와 연계되도록 방안을 강구해야 할 것이다.

4. 인터넷이용기관의 자체 지침서 마련 강화

학교, 직장 등 인터넷 이용기관에서도 자체적인 대책 마련을 강구할 필요가 있다. 많은 기업체와 회사에서 인터넷의 이용을 생활화하고 있는데, 소속 직장인들은 직장 내에서 발생하는 불만을 직장 홈페이지 게시판이나 직원의 이메일을 이용하여 제기하고 있다. 학교에서도 홈페이지 게시판이 교사나 동료 학생을 비방하거나 조롱하는 곳으로 이용되는 일이 증가하고 있다.

그러므로 학교, 직장 등에서는 인터넷 이용에 관한 지침을 마련하고 문제발생시 이를 신속히 해결할 수 있도록 하여야 할 것이다. 예컨대 직장 내에서 사이버 성폭력, 음란물 전송 등과 같은 행위를 할 경우 징계할 수 있는 근거규정을 만들고 아울러 사이버 성폭력 방지를 위한 교육이나 캠페인을 실시하여야 한다. 그리고 학교 홈페이지 운영자는 학생들에게 학교 홈페이지 이용에 대한 안내서를 제공한다. 안내서의 내용은 주로 인터넷상에서 자기 표현하는 기술 가르치기, 불량행위에 대한 제재조항 설명, 경고성 메일을 받은 횟수에 따라 게시판의 이용금지 그리고 실생활에 가해지는 제재조치 등을 포함할 수 있을 것이다.

Ⅶ. 사이버범죄분야의 형사정책적 과제

1. 수사기관의 단속·처벌 활동 강화

모든 범죄에 대하여 마찬가지이지만, 사이버범죄에 대하여도 사법기관을 통한 사건해결은 가장 강력하고 최종적인 피해해결방안이다. 경찰청 사이버테러대응센터나 검찰청 첨단범죄수사부 등이 사이버범죄에 적절한 대응을 하려고 노력하고 있지만, 아직 사이버범죄에 대하여 '적극적인' 대

처를 하고 있다고 보기 어렵다.

사이버범죄의 피해자들은 경찰의 적극적 수사를 기대하고 있지만, 사안이 경미하여 수사인력을 투입하기 어려운 경우가 적지 않고, 피해자가 충분한 증거자료를 확보하고 있지 못한 경우가 많다. 또한 경찰이 사이버범죄를 조사하는데 필요한 컴퓨터 기술이 부족하고, 범죄자 ID의 진정한 사용자를 제대로 파악하기가 어려우며, 사이버사건의 수사에는 장기간의 수사기간을 요하고, 사이버범죄자를 수사할만한 수사력이 충분히 확보되어 있지 않은 등의 이유로 사이버범죄 수사는 현실적으로 많이 미흡한 상황이다.

이 결과 사이버범죄에 대해 수사기관에 신고한 피해자는 곧 좌절하게 되며 경찰의 대응이 소극적인 것으로 여겨지게 된다. 따라서 경찰 등 수사기관은 사이버범죄에 대한 전문 수사인력과 수사역량을 확보하여 다수의 인터넷 이용자들의 범죄피해에 보다 적극적으로 대응하여야 할 것이다.

2. 스팸메일 대응책으로 옵트인 방식의 도입

불법스팸메일 발송자에 대한 형사처벌 강화와 과태료 부과에 대한 금액 상향 추진과 옵트인(Opt-in)제도 도입을 적극 검토해야 한다.

스팸메일 규제방식에 대하여 현행 정보통신망법에서는 “수신자의 명시적인 수신거부의사에 반하는 영리목적의 광고성 정보전송을 금지하고 그 위반시 과태료를 부과”하는 이른바 ‘Opt-out 방식’을 채택하고 있으나, 보다 효율적이고 적극적인 규제를 위해서는 ‘Opt-in’ 방식으로 전환할 필요가 있다. 각국에서도 대체로는 Opt-out 방식을 채택하고 있지만 전송매체 및 정보의 내용에 따라 부분적으로 ′Opt-in 방식′을 채택하고 있다. 예컨대, 전자우편에 대하여는 Opt-out 방식을 채택하되, 수신거부연락처 및 “광고” 등의 표시로 문제점을 보완하고, 수신자에게 직접적으로 경제적 피해를 주는 전화, 팩스 등에 의한 광고성 정보 전송은 Opt-in 방식을 채택하며, 청소년유해정보의 미성년자에 대한 전송은 금지하는 등이 그것이다.[31]

31) 불법스팸대응센터 정책자료 “스펨매일 규제방식에 대한 검토” 참조.

3. 인터넷실명제의 확대실시

인터넷게시판, 자료실, 인터넷카페 등 인터넷커뮤니티에 인터넷실명제 도입을 적극 검토하여 건전한 사이버문화를 조성할 수 있도록 노력해야 한다.

인터넷실명제 실시는 사이버공간이 가지고 있는 최대의 특징인 익명성을 제한하는 조치이다. 익명성은 자신의 이름과 얼굴을 감추고 사이버공간을 이용할 수 있다는 특징을 말하는 것인데, 사이버공간에 불법유해정보가 만연하게 된 원인을 이 익명성에서 찾는 견해가 많다. 이에 따라 이러한 익명성을 제한하고 실명제를 실시한다면 불법유해정보를 취급하는 인터넷 이용자는 대부분 사라지게 될 것이라는 것이 인터넷실명제 실시에 찬성하는 의견의 근거이다. 그러나 인터넷의 발전은 익명성에 의하여 달성된 것이고 앞으로도 익명성을 근거로 그 이용이 활발해질 것이므로 이러한 익명성을 제한하고 인터넷실명제를 실시하는 것은 인터넷발전을 저해할 뿐 아니라 표현의 자유를 침해하는 결과가 될 것이라는 반대론도 강하다.

사이버범죄를 막기 위한 방안으로 '인터넷 실명제'를 실시해야 한다는 여론은 점차 높아지고 있는 상황이다.[32] 주요 포털사이트가 네티즌을 상대로 인터넷 실명제 도입에 대한 여론조사를 실시한 결과 찬성 쪽이 훨씬 많은 것으로 나타났다.[33] 이는 인터넷의 주요 이용자인 네티즌조차도 인터넷 실명제가 필요하다는 쪽으로 생각이 바뀌고 있음을 의미하는 것이다.[34]

세계 최고수준의 초고속정보망 인프라를 바탕으로 한 우리의 인터넷 문화는 선진국조차 부러워할 정도로 만개된 상태다. 그러나 칼의 양날과도 같이 긍정적인 면 못지않게 해악을 주는 악영향도 심각하다. 인권권 침해와 명예훼손, 욕설 등과 같은 인신공격이 가장 문제다. 인터넷에 의한 개인의 인격권 침해는 본인에게는 회복불능의 치명적 타격이 된다. 네티즌과 메카시즘의 합성어인 '네카시즘'이란 말이 생겨날 정도로 현대판 마녀사냥이 사이버 공간에서 공공연하게 자행되고 있는 것이 현실이다. 최근 논란이 된 '군삼녀'사건, '된장녀'사건, '연예인 X파일'사건, '개똥녀'사건, '트위

32) 연합뉴스 2005-07-04자 기사 참조.
33) 중앙일보 2005-07-04자 기사 '인터넷 실명제' 찬성 확산' 참조.
34) 그 배경에는 최근 도를 넘어선 인터넷의 부작용과 무관치 않다고 본다. 연합뉴스 2005-07-04자 기사 참조.

스트김'사건 등은 사이버폭력범죄의 심각성을 잘 보여준 사례들이다.

우리 헌법은 언론출판의 자유를 보장하면서도 그 제21조 4항에서 "언론 출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니 된다"고 규정하고 있어, 언론출판의 자유가 민주국가에서의 불가결한 제도이지만 그것이 남용될 경우 다른 헌법적 가치들이 침해될 수 있고, 특히 타인의 명예는 한번 침해되면 회복하기 어려운 상황에 직면하게 되므로 이를 막기 위한 법제도의 보완은 충분히 타당한 것이다.

인터넷실명제는 헌법상 금지되어 있는 검열에 해당한다는 주장이 있다. 그러나 검열은 사상이나 의견이 발표되기 이전에 국가행정기관이 내용을 심사, 선별하여 일정한 사상이나 의견의 표현을 사전에 억제하는 제도를 말한다.[35] 우리 헌법재판소도 "검열은 행정권이 주체가 되어 사상이나 의견이 발표되기 이전에 예방적 조치로서 그 내용을 심사, 선별하여 발표를 사전에 억제하는, 즉 허가받지 아니한 것의 발표를 금지하는 제도를 뜻한다"고 판시하였다.[36] 따라서 인터넷실명제는 사전적 내용심사에 속하지 않으므로 검열이라고 볼 수 없는 것이다.

또한 인터넷실명제는 범죄수사의 편의를 위한 편의적 발상이고 표현의 자유를 제한하며 과잉금지의 원칙에도 위배된다는 견해가 있다. 그러나 실명을 걸고 행하는 의사의 표현은 절대적으로 보장되며 합법적인 한도 내에서 어떠한 내용의 표현도 제한하는 것이 아니다. 타인에 대한 욕설이나 명예훼손행위는 이미 형법상 중요한 범죄행위의 일종이므로 그러한 표현을 규제하는 것을 표현의 자유 제한으로 연결시켜서는 안 될 것으로 생각된다. 그리고 실명을 사용하게 하는 약간의 개인적 불편함에 비하여 그로부터 보호되는 타인의 명예권과 인격권이라는 공익이 훨씬 크기 때문에 법익의 균형성 심사도 무난히 통과될 수 있다고 판단되며 따라서 헌법상 과잉금지의 원칙 또는 비례의 원칙에도 위배되지 않는다고 생각된다.

이와 같이 인터넷실명제는 위헌적인 제도라기보다는 사이버공간을 건전하고 보호받을 수 있는 영역으로 만들기 위한 실천적이고 합리적인 제도인 것이다. 설사 인터넷실명제가 어떠한 문제점을 안고 있다고 하더라도 사이버폭력 등 사이버범죄가 난무하는 오늘날의 심각한 현실을 고려할

35) 권영성, 헌법학개론 480쪽 이하 참조.
36) 헌법재판소 1998.12.24 96헌가23 참조.

때, 우선은 그 실시의 당위성이 인정된다고 하겠다.

인터넷실명제는 우리 헌법이 보호하고 있는 문화국가의 실현을 위한 제도이다. 그 동안 인터넷을 통한 국어훼손은 그야말로 커다란 충격이었다. 욕설 등 무례한 언어사용뿐만 아니라 표준어를 파괴하고 의사소통에 있어 다른 상대방의 의견을 무시하는 발언 등은 문화국가 실현에 중대한 걸림돌이 된다고 생각한다. 토론문화의 올바른 형성과 국어보호를 위해 인터넷실명제는 긍정적 기능을 한다고 볼 수 있다.[37] 하물며 댓글욕설에 의한 인격침해나 사진합성물 등을 통한 타인의 명예훼손행위의 현격한 감소에도 매우 현저한 기능을 할 것으로 여겨진다.

그 동안 우리는 새로이 등장한 효율적 매체인 사이버공간의 특성과 문제점을 제대로 파악하지 못하고 이에 대응하는 방법을 갖지 못한 것도 사실이다. 이제는 헌법 제21조 제4항이 요구하는 역기능에 대한 대책을 세우고 강력하게 실천해 나가려는 노력이 필요한 때인 것이다. 인터넷 게시판을 이용함에 있어서 실명을 사용하게 하는 것이 국민의 기본권을 제한하는 것인지에 대하여는 의견이 갈리고 있지만, 어느 쪽 의견을 택하건 적절한 규제를 위해서는 적정한 입법에 의한 제도의 실천이 요구되는 바이다.

인터넷실명제는 일찍이 공직선거법에 도입되었으나 실명확인방법과 관련하여 후속조치의 미비로 제대로 실시되지 못하였고, 최근 정보통신망법 개정법에 도입되어 '제한적 본인확인제'라는 이름으로 실시에 들어갔으나 이 역시 많은 사람들이 이용하는 대형 사이트에만 적용될뿐더러 실명을 기재하지 않아도 되는 등 미비한 제도로 되어 있어 그 실효를 거둘 것인지는 의문이다. 아무튼 제도의 실시결과에 주목하여 보다 효율적이고 실질적인 인터넷실명제가 될 수 있도록 지속적으로 보완하여, 확대 실시해 나가야 할 것이다.

4. 인터넷서비스제공자(ISP)의 책임 강화

최근 인터넷 포털사이트나 대형 ISP 게시판, 각종 경매사이트를 이용한 사이버범죄가 증가하고 있으나, 업체들의 무관심으로 사이버범죄행위가 무방비 상태로 방치되고 있는 실정이다. 이러한 사이트에 접근하여 보면, 다

37) 명재진, "공공기관의 인터넷게시판 실명제실시에 관한 소고" 정보통신부 자료실 토론회자료 참조.

양한 유형의 사이버범죄가 행해지고 있음을 알 수 있다(예컨대 각종 음란물 판매광고나 성매매를 부추기는 내용 등). 업체 관계자들은 이러한 불법 게시물에 대해 인력부족 등의 이유를 들어 삭제가 불가능하다고 변명하고 있으나, 이는 변명에 불과하고 도덕적 불감증과 상업적 이기주의에 의해 이러한 불법 게시물을 방치하는 것으로 보인다. 따라서 이들 업체에 대하여 보다 강화된 법적 책임을 물을 수 있도록 하여야 할 것이다.

타인이 제공한 정보에 대하여도 정보통신서비스제공자는 책임을 면하기 어렵다. 다만 정보통신서비스 제공자가 구체적으로 어떠한 형태의 책임을 져야 하는지는 매우 어려운 문제이다. 예컨대 인터넷 경매 사이트에서 이용자가 음란물을 판매한 경우 또는 누구나 이용할 수 있는 인터넷게시판에서 타인을 비방하는 명예훼손성 글을 게재한 경우 사이트 운영자를 형법상의 방조범으로 처벌할 수 있는지는 용이한 문제가 아니기 때문이다.

따라서 법・제도의 개선을 통하여 불법・유해정보 유통 관련 사업자 책임규정 명문화를 할 수 있는 방안을 적극 고려해야 한다. 당해 정보가 불법정보임을 알 수 있었거나 불법정보 제공 또는 유통을 방지하는 것이 기술적으로 가능할 경우 이에 대한 정보통신서비스제공사업자의 책임규정 명문화는 반드시 필요하다.

사이버공간상의 불법정보에 대하여 ISP의 형사책임을 인정할 수 있는가에 대하여는 논란이 있다. 관련법령의 직접위반자와 함께 게시판관리자 또는 온라인서비스제공자에게도 최소한 방조범으로서의 형사책임을 물을 수 있어야만 그 자율규제를 초래하여 사이버공간의 건전한 문화를 조성할 수 있다는 필요성은 제기되고 있으나 민사책임과 달리 형사책임의 경우에는 직접 위반의 고의를 전제로 하기 때문에 이론적으로 그 적용이 쉽지 않은 상황이다.[38]

---

38) 불법유해정보의 유통과 관련하여 ISP의 형사책임은 불법정보에의 접속을 차단하지 않았다는 측면에서 부작위에 의한 방조의 책임으로 다루어질 수 있다. 그 형사책임을 긍정하기 위해서는 우선 ISP에게 보증인의 지위와 보증인의 의무가 인정되어야 하는데, 이 보증인의 의무는 불법정보에 대한 관리의무라는 형태로 등장할 수 있다. 그러한 점에서 일단 다른 서버에 저장된 불법정보를 매개해 주는 ISP의 서비스에 대해서는 그 정보에 대한 통제가능성의 결여로 인하여 보증인의 의무를 갖지 않는다고 해야 한다. ISP의 보증인의 의무는 ISP가 자신의 서버에 불법정보를 저장하여 관리하고 있는 경우에 그리고 그 불법정보의 존재를 인식한 경우에 문제될 수 있다. 그러나 그러한 보증인의 의무가 인정되더라도 실제 ISP가 인터넷상의 불법정보의 유포결과와 관련하여

최근에 음란사이트를 링크한 인터넷서비스제공자에 대하여 그 형사책임을 인정한 대법원의 판결이 주목되고 있다.[39] 그러나 이 판결에 대하여 학자들은 방조범으로서의 책임이라면 몰라도 정범으로서의 책임은 인정하기 곤란하다는 의견을 제시하거나,[40] 입법을 통하지 않은 이러한 해석은 지나치고 무리한 해석이므로 반드시 입법을 통하여 해결해야 한다는 의견을 제시하고 있다.[41]

이와 같이 ISP의 형사책임 인정에 비판적인 견해도 보이지만, 현재의 상황은 어떠한 형태로든 그 책임을 인정하는 추세로 가고 있음을 확인할 수 있다고 하겠다.

가장 효과적인 사이버공간 규제는 당해 사이버공간을 관리하고 있는 ISP들이라고 할 수 있으므로 ISP에 대하여 해당 관리공간에 대한 사이버 게시물에의 감시의무를 부여하고 그러한 의무를 게을리할 경우 행정벌 또는 형사벌에 처할 수 있도록 입법함으로써 보다 적극적인 사이버공간 정화에 나설 수 있을 것이다.

독일의 경우 TDG(통신서비스법)이 그 제8조(자기의 정보에 대한 책임), 제9조(타인정보의 중개에 대한 책임), 제10조(타인정보의 caching, 즉 중간저장에 대한 책임), 제11조(타인정보의 저장에 대한 책임) 등에서 엄격한 요건 하에 ISP에 대하여 민·형사책임을 포괄하는 광범위한 책임을 묻고 있는 것으로 해석된다.[42]

우리도 정보통신망법에 ISP의 행정적 또는 형사적 책임을 물을 수 있

부작위범의 성립이 인정되는 경우는 매우 한정적일 수밖에 없다. 즉, ISP가 최종적으로 불법정보의 유통에 대한 형사책임을 지게 되는 경우는 ISP가 불법정보에 대한 기술적 차단가능성을 가지고 있고 또 법공동체로부터 그러한 정보차단이 합리적으로 기대될 수 있어야 한다는 요건을 충족시킬 때뿐인데, 대부분의 ISP는 이러한 요건을 충족시키지 못하기 때문이다. ISP의 형사책임에 관한 상세한 내용은 이호중, "위험정보의 유통과 ISP에 대한 형법적 규제" 비교형사법학회 2003년도 하계국제학술대회 발표문(2003.8.21) 참조.

39) 대법원 2003.7.8 선고2001도1335 판결 참조.

40) 예컨대 서보학, "유해정보사이트에 링크해 놓은 경우의 형사책임", 법률신문 제3205호 판례평석 참조.

41) 오영근, "인터넷상 음란정보 전시의 개념" 법률신문 제3213호(2003.10.23) 판례평석, 13쪽 참조.

42) 백광훈, 사이버범죄에 대한 ISP의 형사책임에 관한 연구, 한국형사정책연구원 2003, 107쪽 이하 참조.

는 조항을 엄격한 요건 하에 신설한다면 보다 효과적이고 실제적인 사이버공간 정화가 가능하다고 하겠다.

5. 디지털증거의 형사절차법상 사용근거 마련

사이버공간상 디지털증거의 수집과 사용의 중요성은 매우 크다. 디지털 증거는 삭제하더라도 복구가 가능하고 네트워크상의 정보는 당사자의 의사에 관계없이 서버에 존재하므로 증거수집이 유체물증거보다 오히려 용이할 수도 있다. 따라서 디지털 증거가 형사재판에서 증거로 사용되기 위해서는 이미 증거를 수집하고 분석하는 단계에서 원본 증거의 멸실이나 훼손을 막고 증거의 진정성이 훼손되는 것을 방지할 수 있는 적절한 조치를 취할 필요가 있다.

현행 형사소송법에는 디지털 정보나 증거의 압수, 수색과 관련하여 직접적인 근거규정이 없다. 다만 일반 유체물인 증거에 대해서만 증거수집 절차만을 가지고 있을 뿐이다.

따라서 형사소송법에 디지털증거의 수집과 분석, 증거사용에 대한 일반적인 규정을 마련해야 하며, 그러한 후에는 아울러 디지털증거를 수집하고 분석하는 구체적인 표준지침이나 가이드라인 등 디지털포렌식 표준도 마련되어야 한다. 그러한 내용으로는 수사관과 분석가의 이원화, 디지털 증거수집시의 준수사항, 원본증거의 수집, 보관 및 복사 증거의 제작방법, 증거분석 의뢰시 준수사항, 분석의뢰서 접수시 준수사항, 분석의뢰서 접수후 준수사항, 기타 분석의뢰서 및 결과보고서 양식 등을 생각해볼 수 있다.[43]

6. 국제사법공조 강화

아동포르노 심각성, 해외한글 음란사이트 문제 등을 해결하기 위해서는 국제 간 공조체제구축을 위하여 국제기구나 단체에 적극 참여해야 한다.

정보통신윤리위원회는 인터넷상의 아동포르노 등 불법유해정보에 대한 국제적인 공조체제를 구축하기 위하여 2003년 인터넷핫라인협회(INHOP

43) 안경옥, “정보화사회에서의 형법의 중요 문제와 과제”, 인터넷법학회 세미나 자료, 2007.6 151쪽~154쪽 참조.

E)[44]에 가입한 바 있다.

그 동안 불법·유해정보가 한국의 서버로부터 세계 각국으로 유통되어 국가적 이미지를 손상시켜도 각 국의 핫라인 간 협력체제 미흡으로 적절한 조치를 취하기 위한 수단이 적었다. 따라서 불법·청소년유해정보에 대한 신고처리를 신속히 하고 국제적인 이미지와 신뢰도 향상에 기여하기 위해서는 INTERPOL 등 국제기관 및 INHOPE, Cyber Tipline(미국의 민관협력 감시망) 등 해외민간감시기구와의 유기적 공조체제 구축이 적극 요망된다.

한편, 사이버범죄는 국가마다 그 규제방식과 내용이 달라 국제조약으로 법규범화하기에는 어려움이 있고 그 불가능을 주장하는 견해도 있어 왔다. 그러나 이러한 예상과는 달리 유럽에서 최초로 사이버범죄방지조약이 체결되었다.[45] 5개 가입국의 국회인준이라는 요건을 충족한 3개월 후인 2004년 7월 1일 발효한 이 사이버범죄방지조약에는 회원국뿐 아니라 비회원국인 미국, 캐나다, 일본, 남아프리카공화국 등도 가입되어 있고 2007년 6월 현재 미국을 포함하여 20여개 국가가 인준한 상태이므로[46] 추후 세계 사이버범죄방지정책의 흐름을 주도하게 될 것으로 예상된다. 따라서 비회원국에 마련되어 있는 가입절차에 따라 우리나라도 적극적 가입을 검토하여 사이버범죄의 방지를 위한 국제협력에 동참해야 할 것이다.

7. 포털사업자의 윤리척도 평가

최근 사이버공간에서 주로 유통되는 불법유해정보는 상당부분 포털사업자가 운영하는 포털사이트의 게시판이나 뉴스댓글 등을 통하여 주로 발생하고 있다.

위에서 ISP의 법적 책임 강화가 필요하다는 취지의 서술을 하였지만,

---

44) INHOPE는 유럽연합의 지원을 받는 기관으로서 1999년 11월에 설립되었으며 유럽 국가들 가운데 핫라인을 운영하는 사업자들이 주축이 되어 만들어진 단체이다. 주요 목적은 인터넷의 불법 유해정보로부터 이용자를 보호하는 것이고, 아동포르노, 상업사이트, 음란영상, 대화방, 인종차별 사이트 등을 주요 검토 대상으로 활동하고 있다. 현재 한국을 포함하여 16개국 18개 단체가 가입되어 있다. 김기봉, 앞의 글, 129쪽 참조.

45) 유럽의 사이버범죄방지조약에 관한 상세한 내용에 대하여는 정 완 外, 사이버범죄방지조약에 관한 연구, 형사정책연구원 보고서(2001)를 참조 바람.

46) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=6/13/2007&CL=ENG 도표참조.

다수의 네티즌이 이용하는 사이트의 관리자가 불법게시물에 대하여 가장 효율적인 관리를 할 수 있으므로 포털사업자에게 사이버윤리척도 등 평가기준을 마련하여 이를 적용하여 평가를 하고 그 결과에 따라 관련 사업에 대하여 인센티브를 부여하거나 오히려 규제를 하는 등의 방법을 통하여 포털사이트의 합리적인 규제가 가능할 것이다.

따라서 정보통신부나 청소년위원회 등에서 개별적으로 마련하고 있는 사업평가기준이나 사이버윤리척도를 충분히 활용한 사업자평가가 필요하며 이를 통하여 사이버공간의 정화 및 자율규제가 가능하다고 하겠다.

참고문헌

권영성, 헌법학원론(법문사, 2003)
박용상, 표현의 자유(현암사, 2002)
한국전산원, 한국인터넷백서(2005)
정보통신부, 국가정보보호백서(2005)
정보통신윤리위원회, 정보통신윤리백서(2002)
정보통신윤리위원회, 인터넷 정보이용 실태조사(2005.6)
청소년보호위원회, 2004년 인터넷모니터 종합보고서(2005.1)
한국인터넷진흥원, “인터넷이용자수 및 이용행태 조사”(http://isis.nida.or.kr, 2007)

명재진, “공공기관의 인터넷게시판 실명제 실시에 관한 소고”, CLIS Monthly(정보통신정책연구원, 2003)
백광훈, 사이버범죄에 대한 ISP의 형사책임에 관한 연구, 한국형사정책연구원 2003
백윤철, “인터넷상 명예훼손과 ISP의 법적 책임”, 인터넷법연구 제1호 2002
서보학, “인터넷상의 정보유포와 형사책임”, 형사정책연구 제12권 제3호(2001년 가을호)

정완, 사이버공간상 불법유해정보의 합리적 규제방안(한국형사정책연구원, 2005)
정완, 사이버폭력에 대한 법제도적 대응방안 연구(정보통신윤리위원회, 2005)
정완・황태정, 정보통신망상 불법행위의 형사책임에 관한 연구(한국형사정책연구원, 2004)
정완, “인터넷 범죄의 형사법적 과제와 전망”, 인터넷법연구 제2호, 2003.4
정완 外, 사이버범죄에 관한 연구, 한국형사정책연구원 2000
안경옥, “정보화사회에서의 형법의 중요 문제와 과제”, 인터넷법학회 세미나 자료, 2007.6
한상희, “사이버공간에서의 익명성과 책임”, CLIS Monthly, 2003.5/6 정보통신정책연구원
홍순철, “정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정을 위한 공청회”정보통신윤리위원회, 2004.4

Joshua Dressler, Encyclopedia of Crime & Justice(2nd Edition) 1 - 4 (Gale Group, 2002)
John Seely Brown & Paul Duguid, The Social Life of Information(Harvard Business School Press, 2002)
Cees J. Hamelink, The Ethics of Cyberspace(SAGE Publications, 2000)
Jan Samoriski, Issues in Cyberspace - Communication, Technology, Law, and Society on the Internet Frontier(Allyn and Bacon, 2002)
Ferrera etc, Cyber Law(West, 2001)
名和小太郎, 変わりゆく情報基盤 - 走る技術・追う制度(關西大學出版部, 2000)
西村總合法律事務所, IT法大全(日經BP社, 2002)
岡村久道, 新保史生, 電子ネットワークと個人情報保護(經濟産業調査會, 2002)
サイバーロ研究會 編, サイバースペース法(日本評論社, 2000)
銀座第一法律事務所 譯, サイバーロー(中央經濟社, 1999)

Current Situation and Criminal Subject of Cybercrime

Choung, Wan*

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet.

In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself.

However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their

* Professor, Law Department of Kyung Hee University, Ph.D of Law.

identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

I think it is necessary for korean government to enforce some measures to protect a lot of crimes in cyberspace, which are using real name in cyberspace, strengthening internet service provider's liability, promoting international cooperation between countries and establishing laws and regulations against illegal cybercrimes.

주제어 : 사이버공간, 사이버범죄, 주요동향, 형사정책, 사이버폭력, 발생경로, 피해방지
Keywords : Cyberspace, Cybercrime, Criminal Policy, Cyber Violence, Internet Real Name System, ISP Liability