時策

인터넷 명예훼손범죄의 특성과 수사상 대응전략

■ 백 창 현*

Ⅰ. 들어가며

인터넷 환경과 활용 등의 면에서 우리나라는 이제 거의 세계 최고 수준이 되었다고 할 수 있을 것이다. 총 인구의 약 60%에 달하는 2,600만명 이상이 인터넷을 이용하고 있고 초고속인터넷 가입자 수는 이미 1,000만명을 돌파하여 초고속인터넷 부문에서는 가히 타의 추종을 불허할 정도이다(정보통신부, 2003a).

그러나 이에 따른 인터넷범죄 역시 폭발적으로 증가하여 인터넷을 이용한 해킹과 컴퓨터바이러스 유포, 인터넷 사기, 사이버성폭력, 음란·범죄 사이트 운영 및 음란물 배포, 인터넷 채팅을 이용한 청소년성매매, 인터넷 명예훼손 등은 매년 급증하는 추세이다.

이러한 범죄들은 그 어느 것 하나도 심각하지 않은 것이 없겠으나 그 중에서도 특히 인터넷 명예훼손은 이미 그 심각성이 도를 넘어선 것으로 보인다. 인터넷을 검색해보면 불특정 또는 다수인이 익명으로 자유로운 내용의 글을 올릴 수 있는 인터넷 자유게시판을 중심으로 하여 명예훼손성·모욕성 게시물들이 끊이지 않고 있음을 알 수 있다. 그것은 웹사이트의 종류를 불문한다. 인터넷 공간에서의 개인이나 단체에 대한 비방, 욕설, 감정 싸움 등은 사실상 이제 일상화가 되어 버렸다고 말할 수 있을 정도 이다. 특히 연예인 등에 대한 사이버테러와 명예훼손은 이미 사회문제화된 실정이다.

인터넷 명예훼손범죄가 피해자에게 미치는 영향은 상당하다. 인터넷 게시판에 올라온 익명의 비방성 게시물들을 보고 고민하던 한 초등학교 교장이 스스로 목숨을 끊은 사례(강홍준, 2003), 자신이 에이즈 보균자라는 사실이 인터넷 게시판에 폭로되자 게시한 사람을 찾아가 살해한 사례(이율,

* 성균관대학교 법과대학 법학과 / 계명대학교 대학원 경찰행정학과

2002) 등은 그것이 개인에게 얼마나 치명적이고 큰 상처를 줄 수 있는지를 단적으로 말해주는 예라 할 수 있다.

예로부터 지금까지 타인의 명예를 훼손하는 방법에는 여러 가지가 있었다. 소문을 퍼뜨리거나 공공 장소에 벽보를 붙이는 등의 원시적인 방법에서부터 신문 · 잡지 · 라디오 · TV · 영화 등의 매스 미디어(mass media)를 이용하는 현대적인 방법까지 그 종류는 실로 다양하다고 할 수 있다. 그러나 인터넷의 혁명적 등장은 자연스레 이러한 기존의 명예훼손 수단에 대한 획기적 변화를 가져오게 된다. 즉 이제는 개인이 누구라도 마음만 먹으면 방안에 가만히 앉아서 컴퓨터로 인터넷 에 접속하여 매우 손쉽게 타인의 명예를 훼손할 수 있게 된 것이다.

또한 인터넷을 이용한 명예훼손은 실행의 용이성에 비해 전파력 · 파급력의 면에서 매스미디어에 버금가는 엄청난 효과를 가지고 있기에 아주 효율적이다. 또한 강한 익명성을 가짐으로써 행위자에 대한 경찰의 수사와 검거 역시도 쉽지가 않다. 따라서 명예훼손범죄의 실행방법으로 인터넷은 다른 그 어떤 방법을 생각할 수 없을 정도로 가히 최상의 조건을 갖추고 있는 것이다. 어찌 보면 현재와 같은 인터넷 명예훼손의 확산은 이러한 인터넷의 수단적 특성에 기인한 당연한 귀결일지도 모른다. 그러므로 이에 대한 대책은 시급하다 할 것이다. 하지만 의외로 이 부분에 대한 연구는 그리 많지 않은 것으로 보인다.

여기서는 인터넷 명예훼손범죄의 특성을 분석해보고 그에 대한 수사방법과 문제점을 살펴본 후 효율적인 수사상 대응방안을 제시해보기로 한다.

II. 인터넷 명예훼손범죄의 특성

1. 익명성

인터넷 명예훼손범죄의 가장 큰 특성 중의 하나는 강한 익명성이다. 이것은 인터넷의 특성에 기인한 결과라 할 수 있다. 따라서 범죄자의 신원이 직접 드러나지 않기 때문에 그에 대한 경찰의 수사와 범인 검거에는 상당한 애로가 뒤따른다.

인터넷 공간에서 익명성(anonymity) 은 상대방의 정체가 잘 드러나지 않는 상태를 지칭한다. 익명성은 개인의 실제 정체를 드러내지 않음으로써 사회적 차별이나 정치적 보복에 대한 두려움 없이 진실한 목소리를 낼 수 있다는 긍정적인 측면에도 불구하고 많은 논란이 되고 있다. 익명성은 개인을 보복으로부터 보호해 주기도 하지만 말과 행위에 대한 책임성을 약화시켜 많은 부작용을 낳게 하기도 하는 것이다(조동기 · 김병준 · 조희경, 2001: 110).

일반적으로 인터넷상에서의 익명성이 가지는 폐해로 ① 법집행의 곤란성 ② 일탈성향의 조성 ③ 정보에 대한 신뢰성 감소 등을 들고 있다. 이런 점들 때문에 전반적으로 인터넷 공간의 신뢰성은 약화될 수 있다(한상희, 2003: 16).

그리고 이러한 익명성은 탈금제 (脫禁制, disinhibition)의 토대가 된다. 탈금제란 대면적 상황에서는 함부로 말할 수 없는 내용을 인터넷 공간에서의 익명성에 힘입어 자신의 생각과 의견을 쉽게 표현하고 구속감을 적게 느끼고 보다 개방적인 태도를 취하게 되는 현상을 말한다. 그러나 이러한 탈금제는 개인들이 행위의 결과에 대한 책임의식 없이 함부로 행동하게 하는 경향을 낳아 이용자들이 바람직하지 못한 욕구나 감정을 추구하도록 만들기도 한다. 이에 따라 거친 말, 절제되지 않은 비판, 분노, 혐오, 두려움이 무차별적으로 표현되기도 하고 현실공간에서는 쉽게 접근할 수 없는 음란물이나 폭력물과 같은 지하세계가 드러나기도 하는 것이다(조동기 · 김병준 · 조희경, 2001: 110-112).

결국 인터넷 공간에서의 이러한 익명성과 탈금제의 경향이 지금과 같은 인터넷 명예훼손의 만연을 가져오게 된 것이라 할 수 있다. 그 곳에서는 지금도 익명 내지 가명을 이용한 상호간의 거친 의사표현과 모욕, 명예의 훼손이 장소와 시간을 불문하여 벌어지고 있다.

2. 용이성과 효율성

또 다른 특성으로는 범죄 실행의 용이성과 효율성을 들 수 있다. 인터넷을 이용한 명예훼손은 그 실행이 매우 용이하다. 인터넷이 연결되어 있는 컴퓨터만 있다면 누구든 방안에 가만히 앉아 마우스 클릭 몇 번으로 짧은 시간 내에 아주 쉽게 타인의 명예를 훼손할 수 있다(용이성). 그리고 실행의 용이성에 비해 그 효과가 매우 크다고 할 수 있는데(효율성) 이것은 인터넷의 막강한 전파력과 파급력에 기인한 결과이다.

한편 인터넷을 이용한 명예훼손은 실행도 용이하지만 그에 비례해 인멸도 매우 용이하다는 것을 알 수 있다. 작성한 게시물은 언제든 본인이 비밀번호 등의 입력만으로 간단히 삭제할 수 있기 때문이다. 그래서 피해자의 고소나 경찰의 명예훼손 수사에 있어서는 게시물이 행위자 등에 의해 삭제되기 전에 일단 그것을 저장하거나 인쇄하여 증거부터 확보해 놓는 것이 우선된다. 즉 인터넷 명예훼손범죄의 경우에는 그 행위의 자취나 흔적 자체도 무형적이기 때문에 그것을 손쉽게 변환 · 삭제할 수 있다는 특징을 지닌다. 증거의 은닉도 현실 공간의 그것에 비하여 훨씬 용이하므로 적발의 가능성도 낮아지게 되는 것이다(한상희, 2003: 16).

3. 범의 유발성

앞서 기술한 익명성 · 용이성 · 효율성 등의 특징은 범의를 갖고 있는 사람으로 하여금 인터넷 명예훼손범죄를 직접 실행으로 옮기는 데에 큰 유인으로 작용할 수 있다. 즉

범의의 형성과 범죄의 실행을 촉진하는 방향으로 작용할 수 있는 것이다.

특히 익명성은 추적의 가능성을 축소하여 범죄의 유혹을 받는 사람이 손쉽게 범죄로 나아갈 수 있는 여지를 마련해 준다. 인터넷에서는 이러한 익명의 가능성과 비용이 현실공간에 비하여 현저하게 적다는 점에서 이러한 점은 더욱 설득력을 얻는다(한상희, 2001: 27). 즉 익명성으로 인한 적발가능성의 축소 현상은 범죄의 비용을 감소시키고 그 범죄로 인한 기대이익을 상대적으로 증가시킨다는 점에서 범죄를 촉발할 가능성을 야기하는 것이다(한상희, 2003: 16).

사실 행위자가 명예훼손의 방법으로 인터넷을 선택하는 가장 큰 이유 중 하나는 바로 이러한 익명성 때문이라 할 수 있다. 행위자는 이 점을 인식하여 행위시에 자신은 검거되지도 않고 처벌되지도 않을 것이라는 기대감을 갖는다.

4. 범죄의식 결여

인터넷의 익명성 등은 사이버 공간의 문화양태들을 주류의 사회문화로부터 일탈시키거나 혹은 주변적인 것으로 하락시키는 효과를 야기한다. 즉 주류의 문화공간에서는 감히 공개되지 못하던 담론들이 사이버 공간에서는 보다 손쉽고도 공개된 형태로 상호소통되는 현상이 나타나게 되는 것이다. 예컨대 성행위, 엽기, 자살, 범죄공모, 징집거부, 동성애 등에 관한 사이트는 이의 대표적인 예라 할 수 있다. 익명의 공간을 통하여 사람들은 사회적 규범이나 구속으로 부터 해방감을 느끼고 이를 바탕으로 범죄 또는 비행을 아무런 범죄의식이나 일탈의식 없이 저지르게 되고 이를 사이버 공간에서의 보편적인 행위로 일반화하는 것이다(한상희, 2001: 27-28). 개방적이고 공개적인 인터넷 공간의 문제는 일탈적이거나 반사회적인 개인이나 집단에 의한 오염이라 할 수 있다. 다양한 사람들이 쉽게 참여할 수 있는 인터넷 공간에서는 익명성 등의 경향으로 인해 일탈적이거나 반사회적인 행위가 빈번하게 발생하고 있다(조동기 · 김병준 · 조희경, 2001: 114).

특히 자신과 의사소통하게 되는 상대방의 인격 역시 현실적 인격과는 상이하거나 또는 상이한 것으로 인식되는 상황에서는 자기 행위의 결과가 어떠한 현실을 만들어내게 되는지 인식하기 힘들게 되며, 상대방이나 의사소통공간의 물리적 변화에 대한 인식이 결여되게 됨으로써 결과발생으로 인한 죄의식이나 가책감을 느끼기 힘들게 된다. 뿐만 아니라 현실범죄와는 달리 순간적으로 행위가 이루어지면서 동시에 그 행위 과정이 순식간에 지워져 버린다는 점에서 행위자가 자신의 행위를 되돌아보고 반성할 수 있는 중요한 모티브조차도 소멸시키게 된다. 결국 인터넷 명예훼손범죄는 여타 일반적인 인터넷 공간에서의 의사소통행위와 마찬가지로 손쉽게 저질러지고 손쉽게 잊혀지는 비일탈적 · 일상적 행위로 인식되기까지 하는 것이다(한상희, 2003: 16). 또한 군중심리와 집단의식 등은 더욱 더 그러한 범죄의식 · 일탈의식을 낮아지게 할 것이다. 인터넷은 개인을 익명의 군중 속에 쉽게 참여 · 몰입할 수 있게 한다. 그리하여 그러한 범죄를 더욱더 별다른 죄의식 없이 저지르게 되는 것이다.

명예훼손성 · 모욕성 게시물들은 사실 범죄에 해당함에도 불구하고 이제는 너무나 일상화되어 있어서 행위자, 피해자, 제3자를 가릴 것 없이 범죄의식, 일탈의식, 심지어 피해의식조차도 상당히 약화된 상태라 생각된다. 이것은 행위자에게는 더욱 쉽게 명예훼손범죄로 나아가게 하고, 피해자에게는 그것을 어쩔 수 없이 감내하게 하고, 제3자에게는 그것을 재미있는 구경거리 정도로 인식하게 하는 태도로 연결되고 있다.

5. 높은 숨은범죄

인터넷 명예훼손범죄의 또 다른 중요한 특성은 숨은범죄(hidden crime)가 매우 많다는 점이다. 사실상 인터넷 명예훼손범죄의 거의 대부분은 사법적 처벌의 대상이 되지 않고 있다. 그 이유는 형사법적으로 명예훼손 관련 범죄는 반의사불벌죄 또는 친고죄이므로 경찰 등에서도 피해자의 명시적인 고소가 있기 전까지는 수사에 착수하지 않으며 피해자 역시도 고소를 잘 하지 않는 경향이 있기 때문인 것으로 추측된다. 그나마 피해자의 명시적인 고소로 사법기관에 인지된 사건들도 대부분이 다시 가해자와 피해자간 합의 등으로 종결되는 것으로 보인다.

6. 유형의 다양성과 부수 범죄 유발성

인터넷을 이용한 명예훼손은 일반적인 명예훼손에 비해 그 유형이 매우 다양하다고 할 수 있다. 인터넷이 등장하기 전의 명예훼손 범죄는 그 유형이 어느 정도 한정되어 있었다. 그러나 최첨단 문명의 이기인 인터넷을 이용한 명예훼손은 그것을 이용하는 과정에서 또 다른 최첨단 수단들을 사용하게 되고 결국 이것은 온갖 다양한 유형의 명예훼손범죄로 나타나게 되는 것이다. 인터넷 명예훼손범죄는 주로 전자게시판을 통하여 발생하게 된다. 전자 게시판의 경우 보통은 사실을 적시하는 글(문자 등으로 작성된 것)로 이루어지는 경우가 많으나 음성 · 사진 · 동영상 파일 등을 주로 또는 부수적으로 이용하는 사례 또한 많다.[1)]

1) 음성 파일을 이용한 경우의 대표적인 사례가 바로 모 여자가수의 사례이다. 누군가가 그녀의 목소리를 교묘히 위 · 변조하여 마치 팬과의 전화통화에서 팬에게 욕을 하는 것 같은 내용의 음성 파일을 만들어 그것을 게시판에 올린 사건이다. 게시물은 삽시간에 사람들에 의해 이 게시판에서 저 게시판으로 전파되었고 당사자는 상당한 피해를 입었다. 사진 파일을 이용한 경우로는 모 여자탤런트의 사례를 들 수 있다. 지방의 한 교도소에서 경비교도 대원으로 복무 중이던 한 군인이 재소자 검색 프로그램을 이용해 다운 받은 그녀의 수의 차림 사진(그녀가 마약복용 혐의로 구속되어 서울구치소에 수감될 당시 촬영된 실제 사진임)을 인터넷에 게재한 사건이다. 동영상 파일을 이용한 경우의 대표적인 사례로는 한때 사회적으로 큰 파문을 일으켰던 모 여자가수의 사례를 들 수 있다. 그녀가 가수로 데뷔하기 전에 촬영한 실제 정사장면이 인터넷에 유포된 사건이다.

그리고 전자우편(e-mail)을 이용하는 경우도 있는데, 이 때에는 한번에 많은 수의 사람들에게 메일을 동시 발송하는 방법을 사용하게 될 것이다.

그러나 이 방법은 수신자들의 메일 주소를 알아내어 그것을 수신자 목록에 일일이 입력하는 등의 불편함이 따르기 때문에 실행의 용이성 측면에서 본다면 인터넷 게시판을 이용하는 것에 비해 그리 효율적인 방법은 아니라 할 수 있다.

다만 특정인들 에게만 그것을 보여주어 명예를 훼손하고자 할 때에는 이 방법을 사용하게 될 것이다. 이에 관한 사례는 조금 드물기는 하나 종종 보고되고 있다.[2)]

그 외 웹페이지(html 문서)를 이용하는 경우도 있을 수 있는데, 이 때에는 자신이 직접 사이트를 개설하여 특정 웹페이지에 명예훼손성 내용을 작성하는 등의 방법을 사용하게 될 것이다.

해당 웹페이지의 접속자 수가 많다면 오히려 전자게시판을 이용하는 경우 보다 전파력과 파급력의 면에서는 훨씬 더 효과적일 수 있는 방법이다.

그러나 아직까지는 우리나라에서 이와 관련된 실제 사례가 특별히 보고되고 있지는 않다. 역시 전자게시판을 이용 하는 것에 비해 실행이 훨씬 어려우며 추적의 가능성이 크다는 등의 이유 때문인 것으로 생각된다. 다만 앞으로는 특정 웹페이지를 해킹하여 거기에 명예훼손성 글이나 그림 등을 올려놓는 사례가 빈발할 것으로 예상된다. 외국의 경우에는 웹페이지의 해킹을 통한 명예훼손 사례가 자주 보고되고 있다.[3)]

특히 우려할 만한 것은 이 때 나타나는 부수 범죄들이라 할 수 있다. 컴퓨터로 위·변조한 음성·그림 파일을 이용한 명예훼손의 경우에는 위·변조 등의 부수 범죄가 발생하게 되고, 음란 사진이나 음란 동영상물을 이용한 명예훼손의 경우에는 음란물 제작·반포나 기타 성관련 범죄 등의 부수 범죄가 발생하게 되고, 웹페이지나 e-mail의 해킹을 통한 명예훼손의 경우에는 해킹 등의 부수 범죄가 발생하게 된다.

2) 이에 관한 사례로는 IOC 위원들에게 대한체육회장을 비방하는 내용의 영문 e-mail을 발송한 사례 (이학준, 2001), 여자친구가 헤어지자고 하자 여자친구의 e-mail 계정을 해킹한 뒤 남자친구와 성관계로 산부인과를 출입했다는 내용의 메일을 친구들에게 보낸 사례(신창호, 2002) 등을 들 수 있다.

3) 최근의 대표적인 사례로는 미국과 이라크의 전쟁 때 아랍 텔레비전 네트워크인 알자지라 방송의 영어 홈페이지가 미국의 해커 단체에 의해 해킹 당하고 거기에 미국 성조기와 이라크를 비방하는 내용의 메시지가 게재된 사건을 들 수 있다.

Ⅲ. 인터넷 명예훼손범죄에 대한 수사와 문제점

1. 수사기관

인터넷 명예훼손 등의 사이버범죄에 대응하기 위한 국내의 경찰 수사기관 으로는 사이버테러대응센터(CTRC)를 대표적으로 들 수 있다. 사이버테러대응 센터의 장은 총경으로 보하며 (경찰청과그소속기관등 직제시행규칙 제9조 제2항), ① 사이버테러의 탐지·추적수사 및 경보 등 조치 ② 사이버 테러관련 수사기법의 연구·개발 및 국제 경찰기구 등과의 협력 ③ 사이버범죄의 수사 및 지도의 사항을 분장한다(경찰청과그소속 기관등 직제시행규칙 제9조 제9항). 현재 수사 인원은 약 70여명이며 4개팀으로 운영되고 있는데, ① 협력운영팀(기획, 서무, 신고민원 처리·상담, 관계법령·제도 연구, 대외협력) ② 수사1팀(사이버테러 관련대책수립 및 주요 사범수사, 국제공조수사) ③ 수사2팀(사이버 수사기획·지도, 위법·유해사이트 검색) ④ 기법개발팀(사이버테러 예방전략 및 수사기법 연구개발, 일선 사이버수사 기술지원)으로 이루어져 있다(사이버 테러대응센터, 2003).

한편 각 지방경찰청 수사과에는 사이버범죄수사대를 두고 있다.

2. 수사방법

현재 익명의 인터넷 명예훼손범죄에 대한 경찰의 수사방법은 사실상 IP주소를 추적하고 로그인 기록을 분석하는 것이 전부라고 해도 과언이 아니다. 그나마 이러한 IP주소의 추적을 통하여 글이 발송된 컴퓨터를 찾아낸다고 하더라도 범인은 찾아내지 못하는 경우가 많다고 할 수 있다. 이것은 역시 앞서 기술한 바와 같은 익명성의 특징 때문이라 할 수 있다. 수사의 방법기는 전자게시판의 경우와 전자우편의 경우로 나누어서 볼 수 있으나 전자게시판에 대한 수사기법은 보안성 문제가 있기때문에 전자우편에 대해서만 간단히 소개하고자 한다.

명예훼손 등의 내용이 담긴 e-mail이 발송된 경우에는 헤더(header)[4)]에 나타난 발신 IP주소와 시각을 확인한다. 그 이후의 IP 주소를 추적한다.

웹 메일[5)]의 경우 헤더를 보려면 메일 확인 웹페이지에 접속하여 메일을 확인한 후 상단의 '메일헤더보기' 라는 버튼을 클릭하면 된다. 계정 메일의 경우에는 메일 프로그램(Outlook Express 등)을 이용하여 메일을 확인한 후 메뉴상의 '보기-옵션-메시지머리글' 을 차례로 클릭하면 된다.

한편 전기통신사업법 제54조에서는 전기통신 사업자는 법원, 검사 또는 수사

4) 그 e-mail이 어디로부터 어디로 전달되는 것인지의 내용이 상세히 담긴 부분이다.

5) 웹 메일은 별도의 메일 프로그램(Outlook Express 등)이 필요없이 메일 서비스를 제공하는 웹사이트에 접속하여 메일을 송·수신하는 방식의 메일이다. 반대로 계정 메일은 별도의 메일 프로그램(Outlook Express 등)을 이용하여 해당 컴퓨터에서 메일을 송·수신하는 방식의 메일이다. 각기 장·단점이 있지만, 우리나라의 경우 거의 대부분의 사람들이 웹 메일을 쓰고 있다.

관서의 장(군 수사기관의 장을 포함), 정보수사기관의 장으로부터 재판, 수사, 형의 집행 또는 국가 안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디 (컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호를 말한다), 가입 또는 해지일자에 관한 자료(통신자료)의 열람이나 제출을 요청 받은 때에 이에 응할 수 있으며(동조 제3항), 통신자료제공의 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(자료제공요청서) 으로 하여야 함(동조 제4항)을 규정하고 있다. 그러므로 수사기관 등은 자료제공요청서 만으로도 영장 없이 전기통신사업자로부터 가입자에 대한 인적 자료 등을 제공받을 수 있다.

Ⅳ. 인터넷 명예훼손범죄에 대한 수사상 대응방안

1. PC방 사용자 기록 보관의 법제화

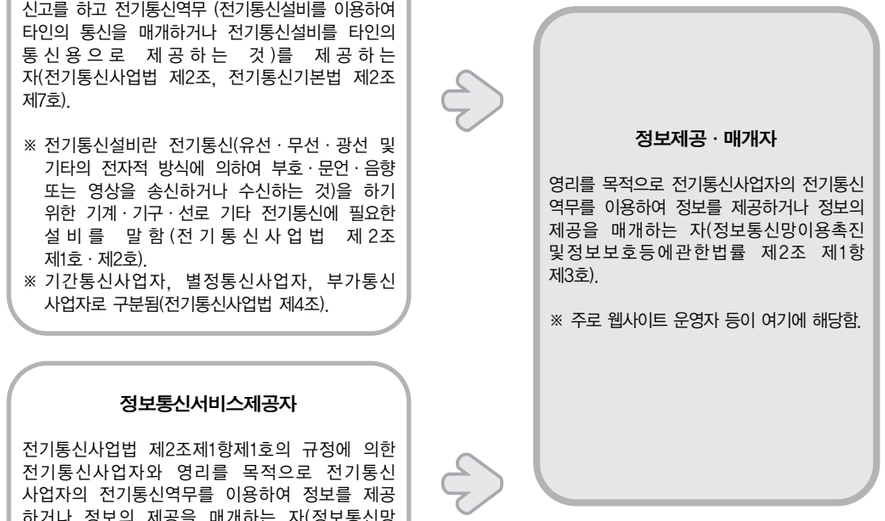
사실상 전체 사이버 범죄의 60-70%는 PC방에서 이루어진다. 사이버 범죄자들은 자신의 접속 위치를 추적 당하지 않으려는 생각에서 익명성이 쉽게 보장되고 언제든 자리를 떠날 수 있는 PC방을 자주 이용하고 있는 것이다(경찰청, 2002).

인터넷을 이용한 범죄를 행할 때 PC방을 이용하는 것은 마치 전화를 이용한 범죄(협박 · 음란 · 장난전화 등)를 행할 때 공중전화를 이용하는 것과 유사하다. 즉 위치를 추적 당하더라도 즉시 그 자리를 떠나기만 하면 검거되지 않는 곳을 이용하는 것이다. 현재 전국적으로 PC방은 약 2만 - 2만5천개에 달하는 것으로 추산되는데 우리나라는 세계에서 가장 많은 PC방을 보유하고 있다.

앞서 기술한 바와 같이 인터넷 명예훼손 사건을 수사함에 있어 범인이 PC방을 이용한 경우에는 해당 PC방과 사용 컴퓨터를 추적해서 찾아내더라도 정작 해당 사용자는 찾아내지 못하는 경우가 대부분이다. 사용자의 인적 사항 등이 PC방 측에 기록되어 있거나 하지는 않기 때문이다. 그래서 PC방의 경우는 직접 해당 PC방을 방문하여 문제의 IP주소를 사용한 컴퓨터를 확인하고 주인과 손님 등을 상대로 문제의 시간에 사용한 사람을 탐문하여 찾아내는 식의 어려운 수사가 이루어질 수밖에 없는 것이다.

그러므로 PC방 업주에게 고객의 간단한 신상정보와 사용내역(사용시간, 사용컴퓨터 등)에 대한 기록을 보관해 두도록 법률적으로 의무화시키는 방안을 생각해 볼 수 있다. 이 때 신상정보는 주민등록번호에만 국한하도록 하는 것이 좋을 것으로 생각된다. 경찰 수사에서는 그것만으로도 다른 모든 인적 사항의 조회가 가능하며 그 이상의 정보는 개인정보 유출 등의 우려가 있기 때문이다. 단, 주민등록번호의 유출이 이루어지지 않도록 개인정보를 보호할 수 있는 기술적인 조치가 반드시 뒤따라야 할 것이다. 이것을 위한 구체적 방안으로 각 사용자가 PC방 컴퓨터 사용시 초기화면에서 주민등록번호를 입력하고 인터넷에 접속하도록 하는 방법을 들 수 있다. 이러한 것은 PC방 관리프로그램[6]의 기술적 수정만으로 쉽게 가능할 것으로 보인다.

이러한 방안은 사후 범인 추적과 검거뿐만 아니라 인터넷 명예훼손 행위를 사전에 억제하는 효과가 상당히 클 것이다. 그리고 이것은 인터넷 명예훼손뿐만 아니라 인터넷을 이용한 모든 범죄에 적용될 수 있으므로 매우 효율적인 대처방안이 될 수 있을 것으로 생각된다.



【그림 1】 전기통신사업자와 정보통신서비스제공자의 개념도

6) 보통 회원관리, 요금산정, 사용자의 PC사용 시작 · 종료 알림, PC의 위치확인 및 제어, PC사용현황관리 등의 기능을 제공한다.

2. 통신자료제공요청권 객체의 확대

전기통신사업법 제54조 제3항에서는 수사기관 등의 전기통신사업자에 대한 통신 자료 제공요청권을 규정하고 있음은 앞서 기술한 바와 같다. 즉 자료제공 요청서만으로도 영장 없이 전기통신 사업자의 동의를 얻어 통신자료(이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입·해지 일자 등의 인적 사항)를 제공받을 수 있는 것이다.

그러나 여기에는 한 가지 문제점이 있는 것으로 보인다. 즉 통신자료제공 요청권의 객체를 '정보통신서비스 제공자'로 하지 않고 '전기통신사업자'로 규정함으로써 실제적인 수사효율성 확보가 제대로 이루어지지 못할 우려가 있는 것이다. 그것을 논하기 위해서는 먼저 '전기통신사업자'와 '정보통신 서비스 제공자'의 개념을 명확히 구분할 필요가 있다〈그림 1〉에서 보듯 '정보통신서비스제공자'는 '전기통신사업자'와 '정보제공·매개자'를 모두 포함하는 넓은 개념이다. 즉 '정보통신서비스제공자 = 전기통신 사업자 + 정보제공·매개자'라는 등식이 성립 된다.

전기통신사업법 제54조에서는 전기통신사업자에 대해서만 수사기관 등의 통신자료 제공요청권을 인정하고 있으므로 '전기통신사업자가 아닌 정보통신서비스제공자', 즉 '정보제공·매개자'의 경우에는 수사기관이 통신자료의 제공을 요청할 수 없다는 결론이 된다. 전기통신사업법 제54조의 통신자료 제공에 관한 규정은 엄격해석의 원칙이 적용되어야 하기 때문에 전기통신사업자가 아닌 경우에는 이를 적용할 수 없다고 하여야 한다. 그러므로 '전기통신사업자가 아닌 정보통신서비스 제공자(정보제공·매개자)'에게는 영장에 의하여 통신자료의 제출을 요구하여야만 하는 것이다(황승흠, 2001 : 9 - 10).

'전기통신사업자가 아닌 정보통신 서비스 제공자(정보제공·매개자)'는 주로 웹사이트의 운영자 등이 해당되는데, 실제 인터넷 명예훼손 관련 사건의 수사에서는 회원 등의 통신자료를 전기통신사업자에게 요청하는 경우도 있겠지만 웹사이트 운영자 등에게 통신자료를 요청하여야 할 경우가 많을 것이다. 왜냐하면 성명, 주민등록번호, 주소, 전화번호 등의 개인정보 입력을 통한 회원가입절차를 거치고 아이디, 비밀번호를 입력하여 로그인을 하여야만 정보를 이용할 수 있는 웹사이트가 매우 많기 때문이다. 이러한 사이트에서 어떤 회원이 직접 자신의 아이디를 통해 로그인한 후 게시판에 명예훼손성 게시물을 올린 경우 에는 해당 웹사이트의 운영자 등이 보관하고 있는 로그인 기록을 통해 해당 회원의 통신 자료를 제공받아 더욱 신속·정확 하게 범인을 검거할 수 있게 될 것이다. 그럼에도 불구하고 현행법의 해석상 이들에게는 영장을 법원으로 부터 발부 받아 통신자료의 제출을 요구할 수밖에 없게 되는데, 이것은 수사의 신속성과 효율성 확보 등의 입법취지로 마련된 전기통신 사업법 제54조가 그 실효성을 제대로 거두지 못할 가능성이 있음을 말해주는 것이라 할 수 있다.

그러므로 관련법 개정 등을 통해 통신자료제공요청권의 객체를 '전기통신 사업자'에서 '정보통신서비스제공자'로 확대하여 규정할 필요가 있을 것이다. 이는 곧 중·대형 웹사이트의 관리자로부터 수사기관 등이 그의 동의를 얻어 해당 웹사이트 회원의 통신자료를 즉시 제공받을 수 있게 됨을 의미한다.

물론 영장주의의 예외라 할 수 있는 이러한 규정의 적용 확대는 바람직하지 못하다는 반론이 제기될 수도 있겠지만 ① '전기통신사업자는 ... 이에 응할 수 있다'라고 규정하여 통신자료제공을 전기통신사업자의 의무사항이 아닌 선택사항으로 둔 점 ② 그 대상이 비교적 간단한 정보(성명, 주민등록번호, 주소, 전화번호, 아이디, 가입·해지 일자)에 한정된 점 ③ 반드시 서면(자료제공요청서)으로 하도록 하고 있는 점 등에서 애초에 위헌 등의 소지는 적은 것으로 생각되는 규정이므로 수사의 신속성·효율성 확보, 폭증하는 인터넷 명예훼손범죄의 척결 등의 차원에서 통신자료제공요청권 객체의 확대 필요성은 크다고 생각된다.

2002년도에 전기통신사업자들이 수사기관에 협조한 가입자 인적 자료 제공건수는 127,787건으로 2001년의 113,422건에 비해 12.7%가 증가하였다. 이 중 15,285건(전체의 12.0%)은 인터넷 관련 사업자들이 제공한 것인데, 이것은 2001년의 5,209건에 비해 193.4%가 증가한 수치이다. 인터넷 관련 사업자들의 제공 건수가 급증한 것은 인터넷 이용사기, 개인정보유출사범, 인터넷 명예훼손 등 사이버 범죄가 증가함에 따라 이를 수사하기 위한 인적 정보의 요청이 증가한 때문인 것으로 분석된다(정보 통신부, 2003b).

3. 로그인 기록 요청 및 보관의 법제화

수사기관이 정보통신서비스제공자 등으로부터 로그인 기록을 쉽게 요청할 수 있도록 관련법 개정을 통해 이를 명확히 법제화하는 방안도 요청된다. 전기통신사업법 제54조 제3항에서는 제공받을 수 있는 통신자료를 이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 또는 해지 일자에만 한정하여 규정하고 있기 때문이다.

그리고 로그인 기록 요청 시에도 정보통신서비스제공자 등이 로그인 기록을 제대로 보관하고 있지 않아 수사에 어려움을 겪는 경우가 많으므로 정보통신서비스제공자 등의 로그인 기록 보관 의무에 대한 법제화 역시 필요할 것으로 보인다.

정보통신서비스제공자에게 접속기록 보관 의무를 부과하는 것은 타인이 제공한 정보에 대한 정보통신서비스제공자의 법적 책임과 연계되어 있는 문제라 할 수 있다. 특히 정보통신망이용촉진및정보 보호등에관한법률 제44조에서는 정보통신망을 이용하여 일반에게 공개를 목적으로 제공된 정보로 인해 법률상 이익이 침해된 자는 해당 정보를 취급한 정보통신서비스제공자에게 당해 정보의 삭제 또는 반박내용의 게재를 요청할 수 있으며, 정보통신서비스제공자는 이에 의하여 당해 정보의 삭제 등의 요청을 받은 때에는 지체없이 필요한 조치를 취하고 이를

즉시 신청인에게 통지하여야 함을 규정하고 있다. 즉 명예훼손성 게시물로 인해 법률상 이익이 침해된 자의 정보통신서비스제공자에 대한 게시물 삭제 및 반론 게재 요청권과 이에 대한 정보통신서비스제공자의 조치 및 통지 의무를 규정하고 있는 것이다.

만약 정보통신 서비스제공자가 이러한 의무를 게을리한 경우 인터넷 명예훼손의 피해자는 이 규정에 근거 하여 가해자뿐만 아니라 정보통신 서비스 제공자에게도 민사상 손해배상을 청구할 수가 있게 될 것이다. 그러므로 만약 정보통신망 이용촉진및정보보호등에관한법률 제44조에 의하여 정보통신서비스제공자의 법적 책임[7]이 인정 된다면 이에 근거하여 접속기록의 보관 의무를 규정할 수 있을 것이다. 영국의 경우 에는 인터넷 사업자의 법적 책임을 근거로 하여 일정 기간의 접속기록 보관 의무를 부과 하고 있다(황승흠, 2001: 14).

한편 현행법상에는 이러한 접속기록 보관 의무와 비슷한 '전자상거래사업자의 거래기록 보존 의무'가 규정되어 있다. 전자상거래 사업자는 전자상거래에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하여야 한다(전자상거래 등에서의 소비자보호에관한법률 제6조 제1항). 공정거래위원회는 이에 위반한 사업자에 대해서 500만원이하의 과태료에 처하고(동법 제45조 제2항 제1호), 시정조치(당해 위반행위의 중지, 법에 규정된 의무의 이행, 시정조치를 받은 사실의 공표, 그밖에 시정을 위하여 필요한 조치)를 명할 수 있다(동법 제32조 제1항·제2항). 이 때 표시·광고에 관한 기록은 6개월, 계약 또는 청약철회 등에 관한 기록은 5년, 대금결제 및 재화 등의 공급에 관한 기록은 5년, 소비자의 불만 또는 분쟁처리에 관한 기록은 3년 동안 보존하여야 한다(전자상거래등에서의 소비자보호에 관한법률시행령 제6조 제1항). 그러므로 로그인 기록의 보관 의무도 이러한 규정에 준하여 규정하면 될 것으로 생각된다.

7) 이러한 정보통신서비스 제공자의 민사상 책임을 보통 'ISP (Internet Service Provider) 책임'이라 부른다.

4. 게시물에 IP주소 현출

로그인 기록 분석을 통하는 이유는 IP주소와 게시물 게재 시각 등을 파악하기 위해서이다. 그러므로 만약 게시물 자체에 IP주소와 게재시각 등이 나타나 있다면 여러 가지로 번거로운 로그인 기록 분석 단계를 거치지 않아도 될 것이다. 또한 수사기관의 정보통신서비스제공자에 대한 로그인 기록 요청, 정보통신서비스 제공자의 로그인 기록 보관 등도 더 이상 필요 없게 된다. 그러므로 이것은 인터넷 명예훼손 사건의 수사효율성을 제고하기 위한 매우 근본적인 대책이 될 수 있는 방안이라 할 수 있다.

게시물 자체에 IP주소와 게재시각 등이 표시되도록 하고 있는 게시판 프로그램은 IP주소의 공개를 위해 이미 일부 사이트에서 사용되고 있다. 그러나 아직까지는 공개되지 않는 프로그램이 많이 사용되고 있는 실정이다. 따라서 게시물에 IP주소와 게재시각 등이 나타나도록 되어 있는 게시판 프로그램의 사용을 적극 권장하거나 이를 법제화할 필요성이 있을 것이다.

이러한 방안은 사후 범인 검거뿐만 아니라 인터넷 명예훼손범죄를 사전에 예방하는 효과도 클 것으로 생각된다. 게시물의 IP주소가 공개되는 경우 행위자는 자신의 위치가 추적 당할 수 있다는 생각으로 범의가 상당히 줄어들게 될 것이다.

5. 수사기관의 위상 제고

사이버테러대응센터 등의 책임자는 컴퓨터와 정보통신에 관한 전문지식 이외에 국내외 각급 기관의 협력을 얻는 데에도 불편이 없는 지위와 계급을 갖춘 사람일 필요가 있을 것으로 보인다. 특히 한국과 같이 상대방의 지위와 서열에 따라 협조 범위가 달라지는 풍토 하에서는 사이버테러대응센터의 책임자를 총경으로 보할 것이 아니라 좀더 높은 계급으로 조정하고 센터의 위상도 수사국 산하의 과에서 좀더 격상시킬 필요가 있다고 생각된다. 즉 관련 법령의 개정을 통하여 경찰청 수사국 산하의 과에 해당하는 사이버테러대응센터를 국단위 부서(가칭 '사이버테러대응본부')로 격상시키고, 최고 책임자의 계급도 치안감 또는 경무관급으로 격상시킬 필요가 있을 것으로 보인다(이황우·조병인·최응렬, 2001: 494-495). 장소와 시간을 초월하여 변화무쌍하게 발생하는 사이버범죄에 대응하기 위해서는 관련 수사기관의 위상을 더욱 제고시켜 줄 필요가 있을 것이다.

V. 맺으며

인터넷 명예훼손범죄는 그 독특한 특성으로 인하여 수사도 여타 범죄에 있어서 와는 상당히 다른 방식으로 이루어지고 있다. 그러나 여러 가지 법제도적 · 기술적 한계로 인하여 아직까지는 IP주소의 추적이나 로그인 기록 분석, 탐문 수사 등에 머무르고 있는 실정이라 할 수 있다.

앞서 든 수사상 대응방안들 중 게시물에 IP주소를 현출하도록 하는 것은 근본적이고도 중요한 방안이라 할 수 있다. 이러한 게시판 프로그램의 사용이 보편화되거나 법제화될 경우 로그인 기록 분석 · 요청 · 보관 등의 번거로운 절차가 더 이상 필요 없게 될 것이기 때문이다.

또한 게시물의 IP주소가 공개되는 경우 행위자는 자신의 위치가 추적 당할 수 있다는 생각으로 범의가 상당히 줄어들게 되어 인터넷 명예훼손범죄를 사전에 예방하는 효과도 클 것으로 보인다.

그리고 PC방 사용자 기록 보관의 법제화 역시 상당한 효과를 거둘 수 있는 방안이라 할 수 있다. 이것은 특히 인터넷 명예훼손범죄 뿐만 아니라 인터넷을 이용한 모든 범죄에 적용될 수 있으므로 매우 효과적인 대응방안이 될 수 있을 것으로 생각된다. 우리나라에서 PC방은 사실상 모든 사이버범죄의 주요 발생지라 할 수 있기 때문이다.

인터넷 명예훼손범죄에 대한 수사상 대응전략은 앞서 기술한 바와 같은 인터넷 명예훼손범죄의 독특한 특성에 맞춘 적절한 방법들을 사용하여야 할 것이다. 세계 최고의 인터넷 강국 중 하나이며 그에 따른 인터넷 명예훼손 문제 역시 매우 심각한 수준인 우리나라에서 그에 대한 수사상 대응전략 역시도 세계에서 가장 앞서나가야 함은 당연 하다 할 것이다. 앞으로 이에 대한 부단한 연구를 통해 더욱 효과적이고 효율적인 대응책의 개발이 뒤따라야 할 것으로 생각 된다.

참 고 문 헌

강홍준. (2003). 학교 홈페이지에 익명으로 서교장 공격(중앙일보 2003년 4월 7일자). 2003. 4. 8. 인용: http://news.naver.com/news_read.php?oldid=20030407000 0452144012s=284,692&e=392,800

경찰청. (2002). 2002년 경찰백서: 범죄추세와 경찰활동 - 사이버범죄. 2003. 4. 2. 인용: http://www.police.go.kr/data/police/2002/02_02_04.shtml

네이버. (2003). 네이버백과사전 'IP주소' . 2003. 3. 30. 인용:http://100.naver.com/ search.naver?adflag=1&cid=AD1047879928539&query=&where= 100&command=show&mode=m&id=717691&sec=1

사이버테러대응센터. (2003). 사이버테러대응센터 조직. 2003. 4. 1. 인용: http://www.ctrc. go.kr/intro/intro_02.jsp

신주화. (2001). 인터넷 명예훼손 수사, IP추적부터. 수사연구, 207, 22-27.

신창호. (2002). 인터넷 명예훼손 205명 입건(국민일보 2002년 4월 12일자). 2003. 5. 9. 인용 : http://news.naver.com/news_read.php?oldid=2002041200000107018 &s=6&e=239

이 율. (2002). 에이즈 보균 인터넷 게시하자 흉기 살해(연합뉴스 2002년 12월 11일자). 2003. 4. 8. 인용: http://news.naver.com/news_read.php? oldid= 2002121100000696002&s=0&e=244

이학준. (2001). 김운용씨 비방 체육인 명예훼손 혐의 구속(국민일보 2001년 7월 19일자). 2003. 5. 9. 인용: http://news.naver.com/news_read.php? oldid= 2001071900000200018&s=107&e=339

이황우 · 조병인 · 최응렬. (2001). 경찰학개론. 서울: 한국형사정책연구원.

정보통신부. (2003a). 초고속인터넷의 사회경제적 파급 효과. 2003. 3. 29. 인용 :http:// www. mic.go.kr/jsp/it_10000000/it_10000000_r_2.jsp?code=03

정보통신부. (2003b). 2002년 감청, 통신사실확인자료 및 가입자인적자료제공 통계현황. 서울: 동부. 조동기 · 김병준 · 조희경. (2001). 사이버문화의 특성과 사회적 영향 (연구보고 01-39). 서울: 정보통신정책연구원.

한상희. (2001). 통신실명제 - 그 가능성의 검토. 재단법인 지식문화재단 입법공청회 발표자료 : 사이버명예훼손 어떻게 대처할 것인가 - 정보통신망이용촉진및 정보보호등에관한법률 개정안을 중심으로, 21-51.

한상희. (2003). 사이버공간에서의 익명성과 책임. CLIS Monthly, 2003-5/6호, 14-25.

황승흠. (2001). 사이버명예훼손에 대한 입법과제 - 정보통신망이용촉진및정보보호등에관한법률 제44조의 개정안을 중심으로. 재단법인 지식문화재단 입법공청회 발표자료: 사이버명예훼손 어떻게 대처할 것인가 - 정보통신망이용촉진및정보보호등에관한법률 개정안을 중심으로, 1-18.