韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-3-3

컴퓨터범죄의 국가간 대응방안에 관한 연구
- 경찰 수사절차를 중심으로 -

오 태 곤*

A Study on the Countermeasures against International Computer Crimes
- Focusing on The Police Investigation Procedure -

Tae-Kon Oh*

요 약

본 논문에서는 국가간 컴퓨터범죄의 대응방안에 대해 연구하였다. 오늘날 컴퓨터 관련 범죄는 기술 발전의 속도만큼이나 훨씬 더 지능화, 다양화, 첨단화 되고 있는 현실이다. 특히 기술발달과 이에 따른 대량생산체제로 인한 컴퓨터 장비의 저가화 경향은 누구나 고도의 컴퓨터 장비를 소유할 수 있게 되었고, 최첨단 네트워크 환경과의 결합을 통해 컴퓨터범죄가 자행되고 있으며, 그 피해상황은 어마어마하다. 또한 최근의 컴퓨터범죄는 나날이 발전해가는 양태를 보이고 있어 예방은 고사하고, 사후대응조차 힘든 지경인 것이다. 특히 국가간 발생하는 컴퓨터범죄의 경우에는 개별국가들의 상이한 법체계로 말미암아 해결이 더욱 힘들다. 본 논문에서는 이러한 문제인식을 기초로 컴퓨터 범죄에 대해 그 구체적인 유형을 살펴보고, 컴퓨터범죄의 해결을 위한 국가간 컴퓨터범죄의 대응방안에 관해 경찰 수사절차를 중심으로 살펴보고자 한다.

Abstract

A Study on the Countermeasures against International Computer Crime focusing on the Police Investigation Procedure. These days, much more intelligent, varied and advanced techniques for computer crimes have been used than for development of technology. In particular, it has been reported that the damages are enormous. Damages of some computer crimes can not be accurately reported. This study is to speculate specific types of computer crimes and obtain its prevention and countermeasures centering on the Police Investigation Procedure. In particular, it is to speculate international cooperation under the condition that global damages occur frequently due to preparation of advanced network environment.

▸ Keyword : 컴퓨터범죄(Computer Crime), 지능화(Intelligent techniques), 첨단화(Advanced techniques), 수사절차(Investigation Procedure), 네트워크 환경(Network Environment)

• 제1저자 : 오태곤
• 접수일 : 2005.05.25, 심사완료일 : 2005.07.10
* 전남도립남도대학 경찰행정경호과

Ⅰ. 서 론

우리나라의 컴퓨터 보급률은 인구수로 비례하면 미국보다 훨씬 앞서고 있으며, 1가구 1PC 시대에 돌입하면서 2003년 말 현재 인구 100명당 초고속인터넷 가입자 수는 17.16명으로 세계 1위이며, 2위인 캐나다 8.4명보다 무려 2배 이상 앞서있고 또한 세계1위의 휴대폰 생산국이기도 하다.[1] 이러한 정보인프라 환경과 특히 기술개발에 따른 컴퓨터의 저가화 경향으로 인하여 지금 우리의 컴퓨팅 환경은 이른바 유비쿼터스의 세계를 향해가고 있으며,[2] 향후 이와 같은 추세 속에서 더욱더 편리한 생활을 영위하게 될 것이다. 그러나 이와 같은 순기능 못지않게 많은 역기능을 안고 있으니, 이것이 이른바 '컴퓨터범죄'이다.

일례로 2004년 9월 23일자로 시행된 '성매매알선등행위의처벌에관한법률'로 인하여 오프라인 상에서의 성매매가 어렵게 되자, 인터넷 챗팅방을 통한 온라인에서의 성매매 알선행위가 횡횡하였음을 각종 언론매체 등을 통하여 심심치 않게 접하고 있는 것이다.[3] 이러한 온라인 상의 성매매 알선행위는 음성화·지능화로 특정 장소에 근거를 두지 않으며, 사이버 공간에서 범행이 기수되어 제3의 장소에서 범행이 완료되며, 또한 사이버 공간의 익명성 등의 특성으로 성매매 관련자를 특정하거나 구체적인 犯罪 입증을 어렵게 하고 있다. 비단 이와 같은 경우뿐만 아니라 인터넷을 통한 음란물 유포와 명예훼손, 해킹을 통한 비밀침해, 중요정보의 침해 및 파괴, 전자우편을 통해 바이러스를 통한 컴퓨터의 파괴 등 헤아릴 수 없는 양태와 피해가 발생하고 있다.

특히 오늘날 초고속 네트워크망을 통해 세계가 하나의 네트워크 안에 포섭되고 있는 현실에서 컴퓨터범죄는 국제화 되는 경향을 보이고 있으며, 이에 대한 대응방안의 마련은 컴퓨터 관련 기술의 발전만큼이나 중요하다 할 것이다. 이러한 문제인식을 기초로 본고에서는 기존의 컴퓨터범죄에 대한 일반적인 이론을 검토하고, 특히 컴퓨터범죄에 대한 국가간 대응방안에 대하여 경찰작용을 중심으로 검토해 보고자 한다.

Ⅱ. 이론적 배경

2.1 컴퓨터범죄의 개념

컴퓨터(Computer)란 본래 계산기라는 의미로 한정되어 사용하였으나, 기술이 혁신적으로 발달한 현대에는 단순히 계산의 도구로서의 차원을 넘어 EDPS(Electric Data Processing System)라 불리는 것처럼 '전자적 자료처리장치'라고 보고 있다. 이는 전자의 원리를 이용하여 지시된 명령에 따라 자료를 처리하며 필요한 정보를 만들어내는 기계, 기술 및 시스템을 말한다. 그러나 이러한 컴퓨터의 정의는 어디까지나 자연과학적 개념에 불과하며, 법체계 안에서 규정되어지는 컴퓨터범죄에 있어서 컴퓨터의 개념은 그 용어의 정의를 필요로 하지 않는다.[4] 특히 법적 규제의 경우에는 그 보호법익의 필요성에 의해 그 개념이 각기 개별적으로 한정되어져야 하는데, 이는 범죄유형에 따라 그 대상이 되는 컴퓨터의 범위가 다를 수 도 있기 때문이다. 미국의 경우만을 보더라도 컴퓨터의 개념에 대해 '논리적, 수학적 연산이나 데이터저장, 검색, 통신, 제어기능 등을 수행할 수 있는 컴퓨터프로그램과 데이터를 포함한 장치'라고 규정하기도 하고,[5] '논리, 계산 또는 보존의 기능을 하는 전기적, 자기적, 광학적, 전기화학적 또는 기타의 고속의 데이터처리장치를 의미한다'고 서로 다르게 규정하고 있다.[6]

이러한 컴퓨터범죄에 대해서 관련된 독자적인 범죄현상들은 인정은 하나 '컴퓨터범죄'라는 용어의 사용을 부정하여 기존의 범죄 체계 내에서 포섭하려고 하는 부정설과 독립적인 개념 자체를 인정해야 한다는 긍정설의 대립이 있다.

2.2 컴퓨터범죄의 인정여부

먼저 부정하는 견해를 살펴보면, 인간이 컴퓨터를 발명하여 활용하기 시작한 이래 1970년대 초반까지, 컴퓨터 관련 범죄의 법익침해와 그 사회·경제적 영향이 그리 크지 않았던 시기에 주로 주장되었던 견해로, 이에 의하면 컴퓨터 자체가 범죄적인 것이 아니며 컴퓨터라는 개념 자체를 명확히 정의 내릴 수 없을 뿐만 아니라 컴퓨터범죄라고 칭해지는 범죄들이 대부분 컴퓨터의 기술적 특수성이 개입되지 않은 것으로 기존의 범죄유형과 다를 것이 없으므로 이를 처벌하

기 위한 별도의 구성요건을 필요로 하지 않는다고 한다.[7] 결국 컴퓨터범죄란 "컴퓨터와 관련된 불명확한 사건의 행위들의 집합체에 불과하므로 컴퓨터범죄와 연관되는 '보호법익의 설정' 자체가 필요 없다는 것이다. 또한 동 견해에서는 컴퓨터 자체가 범죄를 저지를 수는 없는 것이므로 컴퓨터의 오용은 인정하되, 컴퓨터범죄라는 용어 자체는 인정하지 않고 대신 컴퓨터남용(Computer Misuse)이라는 용어를 사용하면서, 컴퓨터남용을 컴퓨터 망과 관련을 갖는 모든 종류의 위법적이고 사회적으로 비난 가능한 행위라고 정의하고 있다.[8]

다음으로 긍정하는 견해는 1970년대 중반을 지나가며 점차 정치·경제·사회적으로 컴퓨터에 대한 의존도와 그 비중이 증대됨에 따라 오늘날 다수의 견해는 컴퓨터 안전에 대한 경고적, 예방적 견지에서, 컴퓨터관련 사회침해적 행위의 처벌가능성, 그리고 컴퓨터의 특성상 전통적 범죄와 질적인 면에서 많은 차이가 있다는 점 등에서 컴퓨터범죄(Computer Crime)를 새로운 범죄유형으로 인정해야 된다는 것이다. 이러한 긍정의 견해는 '컴퓨터범죄'라는 개념 속에 어떤 범죄들을 포섭시킬 것인가와 관련하여 최협의설과 협의설, 광의설로 그 견해가 나누어 대립되어오고 있다. 이와 같이 대립되어지는 이유는 컴퓨터범죄라는 개념 자체가 컴퓨터 시스템을 이용하거나 컴퓨터 시스템과 관련하여 발생하는 수많은 범죄들을 포함하는 개념이기 때문이다. 먼저, 최협의설은 협의의 컴퓨터범죄의 범위 내에서 현금지급기에 사용하는 현금인출카드와 각종 신용카드를 이용한 범죄는 따로 분리시키고, 나머지 부분을 컴퓨터범죄로 보는 견해로 현금인출카드를 주워서 현금을 인출하는 것과 같은 행위는 전문적인 기술을 요하는 것이 아니고 마치 길에서 아파트 열쇠를 주워서 그 아파트 문을 열고 들어가 물건을 절취하는 것과 같은 단순한 범죄이므로 전문지식을 요하는 컴퓨터범죄와 분리시키는 것이 당연하다는 주장이다.[9] 협의설은 컴퓨터에 특수한 범죄의 총체를 규정하기 위한 전제로, 협의설에 의하면 컴퓨터범죄란 컴퓨터가 행위의 수단 또는 목적인 고의의 재산적 침해행위만을 의미한다고 한다.[10] 다음으로, 광의설은 컴퓨터범죄에는 현재 형사처벌법규에만 당벌적(Strafwürdig)이라고 여겨지는 모든 행위가 포함되며,[11] 독일의 다수설이 이와 같은 개념정의에 동의하고 있다. 즉, 행위의 수단과 목적인 컴퓨터에 적극적으로 개입(Einwirkung)하는 것뿐만 아니라 의무위반적인 불개입(Pflichwidrige nicht Einwirkung)까지도 컴퓨터범죄에 포함시키고 있으며, '컴퓨터와 관련하여 시도되는 모든 종류의 위법하고, 사회침해적인 행위'를 컴퓨터범죄라 칭한다.[12]

컴퓨터범죄를 정의함에 있어서 이러한 광의설과 협의설의 차이는 컴퓨터가 행위의 수단 또는 목적으로 사용되는 범죄를 컴퓨터범죄라 정의하는 점에서 크게 차이는 없으나, 그 개념에 재산적 침해행위와는 별도로 개인의 사생활에 대한 비밀의 침해나 국가적·정치적 비밀에 대한 침해를 포함시키느냐의 차이가 있다. 그러나 개인의 인격권과 사생활의 비밀과 같은 비재산적인 법익들도 충분히 보호할 필요가 있으며, 또한 현실적으로 사이버공간 상에서의 명예훼손, 개인의 신상정보 등 비밀누설행위, 음란정보의 유통과 같은 비재산적 법익에 대한 침해들이 급격히 늘어가고 있는 현실을 고려하면, 컴퓨터 시스템과 관련하여 발생되는 처벌가능하고 처벌할 가치 있는 모든 행위를 광범위하게 포섭하는 광의설의 입장이 타당하다고 생각하며, 다만 이 경우에도 광의설의 단점으로 지적되는 컴퓨터 하드웨어나 빈 디스켓의 절취와 같은 '컴퓨터에 특별하지 않은' 태양들은 당연히 제외되어야 하며, 컴퓨터범죄의 행위형태를 '컴퓨터기술의 발달이 없었더라면 유사한 형태라도 나타나지 않았을 행위의 태양', 즉 '컴퓨터에 특별한' 행위의 태양으로 제한하여야 할 것이다.[13]

2.3 컴퓨터범죄의 특징

컴퓨터범죄는 인간이 죄를 규정하여 처벌하기 시작한 이래, 종래 전통적 개념의 범죄와는 매우 다른 양상을 보이고 있다. 첫째, 컴퓨터범죄는 전문성을 띄며 범행의 동기 및 행태에서 기존의 범죄와는 매우 다른 형태를 띤다. 이는 컴퓨터를 다룰 수 있는 정도의 지식인이면 대부분 고학력자들이고 두뇌도 명석한 편에 속하며, 기본적 범행도구의 준비적 측면에서 일정수준 이상의 경제력도 필요로 하기 때문이다.[14] 이러한 연유로 생계형 범죄 보다는 개인적 호기심 충족과 향락의 추구 또는 영웅심의 발로, 기술능력에의 과신과 우월감, 완전범죄를 꿈꾸는 범죄심리에서 비롯되는 범행이 많다. 또한, 최근 냉전체제의 종식 이후에는 국가간 경제전쟁의 심화로 각종산업정보와 기술정보를 부정으로 빼내거나 중요자료를 지워버리는 행위를 국가지원 형태의 범죄형태도 늘고 있다.[15] 둘째, 광범위성과 쌍방향성을 띈다. 특히 사이버범죄는 전세계적으로 구축된 초고속 네트워크망과 다수 컴퓨터의 실시간 데이터처리를 통하여, 광범위한 지역에 걸쳐 측정 불가능한 피해를 나타나게 된다.[16] 또한 상호대화식 쌍방향 서비스로 인하여 인터넷 사용자들은 일반적으로 정보를 제공받는 것 뿐만 아니라 정보를 제공하기도 하고 대화할 수도 있게 되었으며, 이러한 특성은 음란물사이트 혹은 위험사이트의 개설을 가능하게 하고, 채팅을

통한 매춘을 가능하게 하기도 한다. 셋째, 여타범죄에 비하여 비교적 용이한 실행성을 가진다. 사이버공간은 단지 한 번의 클릭만으로 상대방과의 의사소통을 가능하게 하므로 이용자는 별다른 고려 없이 즉흥적으로 특정 또는 불특정의 상대방에게 직접 정보를 발송할 수 있게 되었고, 이는 사이버공간의 구성원이 현실세계보다 용이하게 상대방과 접촉할 수 있으며, 메시지 전달의 공적 성격이 상대적으로 약하다는 것을 의미하며, 이러한 특성으로 인해 사이버공간에서의 범죄행위가 현실세계에서보다 더욱 쉽게 발생할 수 있다. 넷째, 프로그램에 부정한 데이터를 한번 삽입하면 결과를 원할 때는 항시 자동적으로 의도한 부정한 결과를 얻을 수 있으므로 매번 동일한 프로그램 조작행위를 할 필요가 없는 등의 자동성을 띤다. 즉 어떤 행위를 1회 행위를 명령하고 나면 그것을 다시 정지시키지 않은 한 그 행위는 자동적이며 영속적으로 전개된다는 것이다. 이는 일반범죄가 어떤 행위를 1회 실행하면 1회로 끝나는 일회성인데 반해 컴퓨터 범죄는 1회 명령 또는 작동을 하여 두면 자동으로 행위가 이루어지며 또한 경우에 따라서는 그 작업이나 명령을 중지시키거나 지워버리지 않은 한 영구히 계속되는 것이 특징이다.[17] 마지막으로, 적발과 증명이 대단히 곤란하다는 것이다. 컴퓨터조작은 거의 무한한 양의 관련 데이터를 순식간에 처리하게 되고 디스크, 마그네틱테이프 등 좁은 공간에 축소·저장시키고, 저장된 자료는 폐쇄성, 은닉성, 불가시성을 갖기 때문에 그 적발과 증명이 곤란하다.[18]

III. 컴퓨터범죄의 유형

3.1 컴퓨터의 부정조작

컴퓨터부정조작이란 불법적인 목적을 추구하는 컴퓨터에 있어서의 입력매체의 내용의 변경, 프로그램의 변경 혹은 자료처리과정에 대한 간섭을 의미하기도 하고, 자료변경(Datenveränderung)을 행위자가 컴퓨터의 처리결과 혹은 인쇄출력을 변경시켜 이로 인하여 자신의 재산적 이익을 얻기 위한 의도를 가지고 전자자료 처리의 영역에 있어서 부분적인 자료변경을 시도하는 것이라 한다. 그러나, 일반적으로는 "행위자가 컴퓨터의 처리결과 혹은 출력인쇄를 변경시키거나 이로 인하여 자신이나 제3자의 재산적 이익 등을 얻을 의도를 가지고 컴퓨터시스템 자료처리의 영역에 있어서 간섭을 행하는 것"이라 할 수 있다.[19]

따라서 컴퓨터부정조작은 컴퓨터흐름의 어떠한 단계에서 행하여지는 가에 의하여 일반적으로 입력조작, 프로그램조작, 콘솔조작, 출력조작 등으로 분류할 수 있다. 우리 형법은 부정조작에 대하여 전자기록위작·변작죄(제227조의2, 제232조의2)와 컴퓨터등사용사기죄(제347조의2)를 규정하고 있다.

3.2 데이터의 부정입수

이는 비교적 최근에 등장한 범죄 유형으로, 컴퓨터스파이라고도 하는데 컴퓨터시스템의 자료를 권한 없이 획득하거나 이용·누설하여 타인에게 재산적 손해를 야기시키는 행위를 말한다.[20] 컴퓨터 부정입수에 있어서 컴퓨터 자료의 불법취득행위로 인한 재산 침해행위와 더불어 비밀침해행위가 문제되는데, 개인의 비밀을 침해하는 경우,[21] 국가의 비밀을 침해하는 경우로[22] 나눠 볼 수 있다. 부정입수에 대한 형법 규정으로는 비밀침해죄(제140조3항, 제16조2항)가 있다.

3.3 컴퓨터의 파괴

이는 하드웨어로서의 컴퓨터 전부 또는 일부를 파괴하거나 작동되지 않도록 하는 행위와 데이터나 프로그램을 저장하고 있는 매체, 즉 자기테이프·자기디스크·자기드럼 등을 파괴하는 행위, 컴퓨터에 의존하고 있는 업무를 방해하는 것을 말한다.[23] 이와 같은 파괴의 행위는 물리적 방법에 한정하지 않고, Computer Virus, Trojan Horse, Logic Bomb 등 프로그램의 파괴와 자료접근을 방해하는 등 다양한 형태로 나타나고 있다. 물리적 방법으로 인한 컴퓨터 파괴 행위는, 그 방법에 따라 손괴죄, 방화죄 등이 적용될 수 있고, 기타의 경우는 그 피해의 행태에 따라 형법 적용에의 논란의 여지가 있다. 컴퓨터파괴에 대한 형법 규정으로는 컴퓨터손괴등업무방해죄(제314조2항), 전자기록손괴죄(제366조1항)등이 있다.

3.4 컴퓨터의 무권한사용

컴퓨터 무권한사용(또는 부정사용)이란 정당한 사용권한을 갖지 않은 행위자가 개인의 컴퓨터를 자신을 위하여 일정한 시간동안 작동시키는 행위를 말한다.[24] 이러한 무단사용은 컴퓨터조작, 사기, 스파이 등의 목적으로 행하여질 뿐만 아니라 해커들이 장난삼아 하는 경우도 있다. 현재로서는 컴퓨터의 권한 없는 사용이 빈번한 것은 아니며 그로

인한 손해가 처벌할 만큼 큰 경우는 별로 없었으므로 개정 형법은 이를 처벌하려는 규정을 신설하지는 않았으나, 개정 형법에 신설된 제348조의2(편의시설부정이용죄)와 제314조2항(컴퓨터손괴등업무방해죄)이 컴퓨터의 권한 없는 사용에 고려될 수는 있으나, 타인의 컴퓨터가 언제나 "유료"자동설비인 것은 아니므로 제348조의2가 컴퓨터의 권한 없는 사용에 관한 규정이라고 할 수는 없다. 또한 제314조2항도 특별한 경우에 한하여 컴퓨터의 권한 없는 사용을 처벌할 수 있음에 불과하다.

3.5 사이버범죄

오늘날 컴퓨터범죄의 유형에 있어서 가장 문제가 되고 있는 것 중의 하나가 바로 '사이버범죄(Cyber Crime) 혹은 인터넷관련범죄(Internet related Crime; 이하 아래에서는 사이버범죄로 일칭)'이다. 최근 월례 행사처럼 벌어지고 있는 Virus에 의한 전세계적인 피해 상황들을 굳이 언급하지 않더라도, 범죄 역시 새로이 형성된 사이버공간을 기반으로 신종범죄들이 속속 등장하고 있다. 이러한 범죄들은 기존 컴퓨터범죄의 성질과 함께 사이버공간 특유의 네트워크에 의한 전세계적 연결이라는 특성에 의해 이미 상당한 사회적 문제가 되고 있으며 이러한 경향은 앞으로 더욱더 심화될 것으로 여겨진다.[25] 이러한 사이버범죄는 기존의 컴퓨터범죄의 특성 외에 가상공간에서 불특정다수를 상대로 하는 비대면성을 갖는다. 이는 가상공간에서의 익명성이 담보되기 때문에 가능한 것이다. 또한 컴퓨터의 특수한 기술적 특성들을 이용하는 기존의 컴퓨터범죄들이 인터넷과 같은 네트워크와의 결합으로 하루하루 새로운 형태로 변모되어 가고 있는 탓에 기술의 발달에 따른 유동성과 자기 발전성을 가지며, 현실사회의 전통적 범죄들이 가상공간의 특유한 특성과 결합하여 어떠한 양상으로 일어나게 될는지 그 예측과 대응이 쉽지 않다는 특성이 있다.

유형별로는 과거 현실세계의 범죄가 단지 컴퓨터시스템을 이용하여 범해지는 형태의 '일반사이버범죄'와 '특수사이버범죄'로 나눌 수 있다. 전자는 과거 현실세계의 범죄가 단지 컴퓨터시스템을 이용하여 행해지는 범죄로서 통신사기, 사이버 도박, 음란사이트운영, 개인정보 침해, 명예훼손 및 모욕, 사이버 성폭력 등을 들 수 있다. 다음으로 후자는 사이버테러, 해킹, 컴퓨터바이러스 등을 들 수 있는데, 사이버테러는 실무적으로 해킹, 바이러스 제작·유포 등 대규모 피해를 야기 시키는 사이버공간에서의 범죄를 말하며, 해킹은 컴퓨터시스템의 취약점을 이용하여 불법적으로 접근한 후 자료의 유출, 위·변조 및 삭제, 시스템 장애 및 마비를 유발시키는 장애행위를 말하며, 서비스거부(Denial of Service), 전자우편 폭탄(E-mail Bomb), 논리폭탄(Logic Bomb), 트로이 목마(Trojan Horse), 인터넷 웜(Internet Worm), 등의 형태로 나타나게 된다. 마지막으로, 컴퓨터 바이러스는 자기 복제를 하여 전파되면서 시스템에 오동작을 일으키거나 파일을 손상시키는 프로그램을 말한다.

이렇게 기존의 컴퓨터범죄와는 다른 특징을 갖는 사이버범죄에 대해 일부 학자들은 구별을 시도하지만,[26] 이는 이미 컴퓨터라는 개념 자체에서 네트워크라는 의미가 빠질 수 없는 요소로 등장하게 되었고 이러한 네트워크 기능이 컴퓨터의 주요한 기능과 역할로 인식되고 있는 현 시점에서 논의의 실익이 없다고 생각한다. 이보다는 컴퓨터범죄라는 하나의 용어 안에 각기 나타나는, 혹은 나타나게 될 범죄 태양들에 따른 개념적 성질들을 밝히는 것이 필요하며, 무엇보다도 시급한 문제라 하겠다.

Ⅳ. 국가간 컴퓨터범죄의 수사

4.1 컴퓨터범죄의 국가간 대응

오늘날 인터넷을 이용한 컴퓨터범죄가 자행됨에 따라 이제 컴퓨터범죄에 대한 수사 및 재판은 국내에 그치는 문제가 아니게 되었다. 예컨대 독일 연방체신청이 운영했던 전신우편함 시스템(Telebox-System)은 네덜란드의 MEMOCOM, 영국의 TELECOM GOLD, 미국의 Dialcom, 오스트레일리아의 MINERVA, 캐나다의 CNOP E.O.S 등 외국의 통신망과 연결되어 있다.[27] 그리고 인터넷은 전세계적으로 가동되는 것이므로 그 통신망을 이용하는 자는 마음먹기에 따라서는 특정국가의 법적용 대상에서 얼마든지 벗어날 수도 있다.[28] 우리의 경우도, 2004년 5월 인터넷 음란 사이트에서 '딸기'라는 이름으로 큰 인기를 누려온 포르노자키(PJ)가 경찰에 구속된 사건이 있었다. 동 사건에서는 국내의 단속을 피해 포르노 제작자가 캐나다에서 음란물을 제작한 다음 인터넷을 통하여 국내 유저들을 상대로 부당이득을 취한 것이다.[29] 위와 같이 컴퓨터 시스템이 세계적으로 연결됨에 따라 여러 나라에 걸친 컴퓨터 범죄에 대처하기 위해 통일된 대응체계가 요구되고 있다. 이를 위해서는 국내법 제정을 위한 표준화된 규정을 마련하고 국제적인 사법

공조체제를 갖추기 위해 국제협약을 체결하거나, 컴퓨터 소프트웨어의 불법복제를 방지하기 위해 민간단체를 결성하는 등으로 대처할 필요가 있다고 하겠다.[30]

이하에서는 이러한 문제인식에 근거하여 컴퓨터범죄에 대응하기 위한 국가간 수사절차에 대해 살펴보고자 한다.

4.2 컴퓨터범죄의 국가간 수사절차

컴퓨터범죄의 국가간 수사절차에 관해서는 먼저, 국외범의 국외수사가 문제된다. 이는 우선 내국인이든 외국인이든 묻지 않고 국외의 컴퓨터 범죄인에 대해 국내 수사관이 국외나 국제정보통신망을 이용하여 국내에서 수사할 수 있는 권한이 있는가 하는 문제이다. 현행 형사소송법이 형법과 달리 그 장소적 적용범위에 관한 규정을 두고 있지 않기 때문에 발생할 수 있는 문제로, 우리와 입법사정이 비슷하고 활발히 논의가 전개되고 있는 일본의 경우를 예로 들어 살펴보고자 한다. 일본의 경우는 크게 다음과 같은 세가지의 견해 대립이 있다. 첫째 견해는, 형사소송법은 원칙적으로 자국영토 내에서만 적용되는 것이고 예외적으로 타국의 승인을 얻으면, 그 타국의 주권을 침해하지 않고 자국 내에서와 같은 권능을 행사하는 것은 국제법상 허용된다고 해야 하며, 따라서 예컨대 검사는 미국의 승인을 받아 자국의 형사소송법을 준거로 하여 임의수사로 미국 내에 있는 사람을 조사하고, 그 진술을 녹취할 수 있다는 견해이다. 둘째 견해는 이에 대하여 형사소송법은 자국의 주권이 미치는 범위뿐만 아니라 전세계에 걸쳐 적용될 수 있는 것이고 다만, 그것이 외국의 주권과 충돌하는 경우에만 국제법상 그 적용이 제한되는 것에 불과하다고 해야 하므로 상대국가의 승인이 있으면 자국의 주권이 현존화하여 수사권한의 행사 등이 가능하게 된다고 하여 첫 번째 견해가 법령적용의 범위와 국가주권의 문제를 혼동하였다고 비판한다. 세 번째 견해는 형사소송법 규정 중 증인소환 등 상대방에게 직접, 간접적으로 의무를 피하는 규정과 같이 주권의 지배 작용에 관계된 규정은 자국 영역 내에서만 적용되는 것이고 영역 외에서는 적용되지 않는다고 해야 하는 반면, 국가기관의 권한분배나 상대방에게 의무를 과하지 않는 기관의 활동에 관한 규정은 영역의 국가기관의 활동에 대해서도 적용된다고 한다.[31] 이와 같은 일본의 논의 상황을 검토해보면, 자국의 수사기관이 외국에 체재하는 범죄인을 체포해도 그 효력을 부인할 필요는 없다는 점에서 두 번째 견해가 타당하다고 생각된다.[32] 즉 국외에서 강제처분도 외국정부의 승인이 있으면 가능하다고 보아야 한다. 따라서 외국정부의 승인을 얻어 외국 수사기관의 협력에 의해 국가간 컴퓨터 정보통신망을 탐색하는 수사활동은 국내법은 통신 비밀보호법 등에 정한 요건을 충족하여 법관이 발부한 영장에 기해 행해지는 한 적법한 수사활동이며, 그에 기해 획득한 증거는 증거능력이 있다고 보아야 한다. 미국의 경우는, 외국인이 미국 외에서 범한 범죄에 대해서도 내국질서에 대해 직접적이고 실질적으로 예견가능한 영향(direct. substantial and foreseeable effect)을 미칠 수 있는 행위이면 그에 대해 미국내법을 적용한다는 입장을 취하고 있다.[33] 그리고 국외범인 컴퓨터 범죄인에 대해 국내 수사관이 국외나 국제정보통신망을 이용하여 국내에서 수사를 진행하여 획득한 증거에 대해 그 수집절차의 위법성을 논할 필요는 없다고 본다. 왜냐하면 그 수사를 행한 지역은 국내이기 때문이다. 이밖에 외국주재 대한민국 공무원이 작성한 공문서나 공전자기록의 내용에 전문진술이 포함되어 있으면 원진술자를 소환, 신문하여 그 진정성립 및 진술의 임의성이 인정되거나 전문법칙의 예외규정에 의해 증거능력이 인정되어야 위 공문서나 공전자기록을 유죄인정의 자료로 사용할 수 있겠다.[34]

다음으로 외국정부가 수집한 컴퓨터범죄의 증거능력이 문제된다. 일본에서는 이른바 록히드 사건에서 수사 중인 검찰관이 일본 형사소송법 제226조[35]에 기해 록히드사 사장에 대한 증인신문을 청구하자, 그 청구를 접수한 법관이 미국 법원에 촉탁하여 미국 법원에서 위 사장에 대한 증인신문을 실시하여 증인신문조서를 작성, 일본 법원에 송부해 왔고, 당해 일본 법원은 이를 검찰에 송부한 사건이 있었다. 이 사안에 대해 피고인측은 사법공조제도와 관련하여 일본 형사소송법은 일본의 국내 법원이 외국법원에 증인신문을 촉탁하는 권한을 인정하지 않고 있다고 다투었다. 즉 일본 민사소송법 제264조 제 1항은 외국에서 행할 증거조사에는 그 국가의 관할관청, 외국영사 등에 촉탁하여 증거조사 할 것을 요한다는 취지로 규정하고 있지만,[36] 일본 형사소송법은 그러한 명문이 규정을 두고 있지 않다는 것이다. 이에 관하여 형사소송법에 그러한 규정을 두고 있지 않는 한 외국법원에 증거조서를 촉탁할 수 없다는 주장도 있으나, 일본 하급심 법원들은 모두 이를 허용하는 것이라고 판시하였다. 즉 법원은 그 소송상의 지위에 기하여 명문의 규정이나 소송의 기본구조에 저촉되지 않는 한 적절한 재량에 의해 공정한 소송지휘권을 행사하고 소송의 합목적적인 진행을 도모해야 할 권한과 책임을 갖고 있으므로 사안의 해명에 필요한 이상 소송지휘의 한 내용으로 외국법원에 증거조사를 촉탁할 수 있으며 일본의 외국재판소의 촉탁에 대한 공조법은 상호보호를 조건으로 외국법원의 증거조사 촉탁에 대해 일본 법원이 응할 것을 규정하고 있는바, 이는

일본 법원이 외국법원에 증거조사를 촉탁할 수 있는 권한이 있음을 전제로 하고 있다는 점 등을 논거로 하여 이를 허용된다고 보고 있는 것이다.[37] 이와 같은 논의를 우리의 경우에 적용해 본다면, 법원의 소송지휘권에 기해 재판장은 외국법원에 증거조사를 촉탁할 수 있다고 보아야하고, 또 그렇게 보는 것이 실체적 진실발견을 위해 타당할 뿐만 아니라, 피고인의 권리를 침해할 염려도 없다고 생각된다. 위와 같이 외국법원에 촉탁하여 작성된 증인 신문조서도 형사소송법 제 314조에 의해 증거능력을 인정할 수 있겠다.[38]

다음으로 외국의 수사기관이나 외국 법원 등에 의해 수집된 증거의 증거능력에 관해서는, 우리 형사소송법 제315조 제1호의 외국공무원의 직무상 증명할 수 있는 사항에 관하여 작성한 문서에 해당하는 것으로 보거나 동 조문 제3호의 '기타 특히 사용할 만한 정황 아래에서 작성된 문서'로 보거나 또는 범죄증명에 필요한 증거인지 여부 및 그 작성에 관한 정황의 요건을 살펴 같은 법 314조의 공판준비 또는 공판기일에 진술을 요할 자가 기타 사유로 인하여 진술할 수 없는 때에 해당하는 것으로 보아 증거능력을 인정할 수 있겠다.[39] 외국수사기관이나 외국법원이 수집, 작성한 서면 기타 증거를 우리나라 수사기관이나 법원이 수집, 작성한 증거와 동일하게 보아 증거능력을 부여하기는 어렵기 때문이다. 따라서 외국수사기관이 컴퓨터 동작을 통해 작성한 실황조사서도 우리나라 수사기관이 작성한 검증조사와 동일하게 보기 어려우므로 위와 같은 규정에 의해 증거능력을 인정해야 할 것이다. 물론 외국의 수사기관이 얻은 정보를 회답하여 온 서류에 대해 형사소송법 제 315조 제 1호에 의해 증거능력을 인정할 수 없다는 것이 학설이고,[40] 판례이기는 하나[41] 그 증거능력을 일률적으로 부정할 수는 없다고 본다. 적어도 위 제315조 제3호나 제314조에 의해 증거능력을 인정할 수는 있다고 해야 한다. 더욱이 위와 같은 학설이나 판례의 태도에 의하더라도 외국의 법원에 의해 수집된 증거의 증거능력을 위 제315조 제1호에 의해 인정할 수 있으며, 다만 증명목적으로 작성되었다고 볼 수 없는 판결서 등은 당해 판결이 있었다는 사실이 아니라, 판결서의 내용에 기재된 사실을 인정하기 위한 증거로는 사용될 수 없기 때문이다.

다음으로 국가간 형사사법공조에 있어서 적용되는 특정성의 원칙에 관해 살펴보면, 이 '특정성의 원칙' 또는 '특정주의의 원칙'은 범죄인 인도제도에서 확립된 원칙으로 인도된 범죄인은 인도청구의 원인으로 특정된 행위에 한하여 소추·처벌되어야 한다는 원칙이다.[42] 그러므로 피요청국에 의해 행해진 사법공조행위는 청구국이 그러한 협력을 청구한 형사절차에서만 이를 활용할 수 있는 것이 원칙이다. 형사사법공조에 관한 유엔모델조약 제8조는 요청국은 피요청국의 동의 없이 피요청국에 의해 제공된 정보나 증거를 요청서에서 언급된 수사나 소송절차 이외의 다른 절차를 위하여 사용하거나 이전해서는 안 된다고 하여 위 특정성의 원칙을 천명하고 있고, 독일 범죄인인도법 제 54조도 외국정부가 형사사법공조를 허용하면서 사법공조 결과의 사용에 관하여 조건을 붙일 때는 내국절차에서 위 조건을 준수하여야 한다고 규정하고 있다.[42] 그러나 이는 국가간 형사사법공조에서 국가간에 준수해야 할 국제법적인 사항을 정하고 있는 원칙일 뿐이고 위 원칙에 위반하여 당해 사법공조 목적이 된 범죄와 별개의 범죄를 재판하는 국내법원이 우리 형사소송법규정에 의해 외국 수사기관이 수집, 작성한 컴퓨터 기록을 증거로 사용하는 것까지 금지하는 원칙이라고 할 수는 없다고 생각된다.

마지막으로 쌍방가벌성 원칙의 완화에 대해 살펴보면, 형사사건의 수사나 재판은 국가주권행사의 대표적 형태중 하나라고 할 수 있는데 국가간 형사사법공조는 결국 이러한 형사사법에 관한 국가주권이 제한에 해당되며[43] 이는 컴퓨터 관련 범죄와 같이 국제화되기 쉬운 범죄에 특히 의의가 있는 분야라고 할 수 있다. 국가간 형사사법공조에 관해서는 상호주의 원칙(Principle of Reciprocity), 쌍방가벌성 원칙(Principle of Double Criminality) 및 특정성의 원칙(Principle of Speciality)과 같은 기본원칙들이 정립되어 있는데 그중 쌍방가벌성의 원칙이란 형사사법공조의 대상이 되는 범죄는 청구국과 피청구국의 법률에 의하여 모두 처벌이 가능한 범죄이어야 한다는 원칙이다.[44] 그러나 폭력, 테러범죄 등의 조직범죄에 대해 청구국 법률상의 범죄구성요건과 피청구국 법률상의 범죄구성요건 사이에 실제적 유사성(Substantial similarity)만 존재하면 쌍방가벌성 원칙을 충족하는 것으로 보는 것이 현대적인 추세이다. 우리나라가 미국과 체결한 형사사법공조조약 제 3조 제 2항도 쌍방가벌성의 예외를 광범위하게 인정하고 있는데, 동 조약 부속서에서 예시하고 있는 예외범죄에는 컴퓨터 관련 범죄가 포함되어 있다.[45] 위와 같이 쌍방가벌성 원칙이 완화되고 있으므로 국가간 사법공조시도 청구국의 컴퓨터 관련 범죄 처벌규정과 피청구국의 그것 사이에 실질적인 유사성만 인정되면 공조를 해주어야 할 것이다. 그리고 미국과의 사이에 체결된 위 형사사법공조조약에 의하면 한국과 미국 사이에서는 상호 국내법에 의해 처벌되지 않는 컴퓨터 관련범죄에 대해서도 형사사법공조를 요청할 수 있다.

V. 결 어

컴퓨터는 분명히 인류가 불을 발견했을 때와 비교될 만큼 우리 사회에 없어서는 안 될 중요한 산물임에 틀림없다. 또한 우리가 살아가고 있는 21세기는 무선인터넷의 발달로 인하여 노트북, 휴대폰을 통하여 이동 중이거나, 또한 언제 어느 곳에서도 컴퓨터와 인터넷을 사용할 수 있을 만큼 관련 기술이 발전하고 있다. 이러한 기술 발전의 영향으로 우리의 삶은 더욱 윤택해지고 편리해지고 있다. 그러나 이러한 순기능과 더불어 예상치 못했던 많은 역기능들이 발생하고 있는데, 일찍이 1993년 OECD 회의에서도 컴퓨터범죄에 대해 "컴퓨터와 관련된 반사회적 행위 또는 자료의 자동처리 및 전달을 포함한 불법적, 비윤리적, 무권한적 행위"라고 정의된 바 있듯이, 초고속 네트워크망과의 결합을 통하여 국경 없는 범죄의 양태를 보이고 있으며, 이에 대응할 국가간 수사체제의 확립은 시급한 일이라 하겠다.

앞서 살펴본 바와 같이 각국은 컴퓨터범죄에 대해 국내적 측면에서 대응체제를 마련해야 함은 물론이고, 국외범의 국외수사, 외국이 수집한 관련 증거의 증거능력, 죄형법정주의의 명확성, 적정성의 원칙에 맞는 쌍방가벌성의 완화 등에 관하여 국가간 합의점을 도출하여 컴퓨터범죄의 역기능에 대한 대비에 만전을 기해야 할 것이다.

참고문헌

[1] 동아일보, 2004.4.17.

[2] 조영섭 · 조상래 · 유인태 · 진승헌 · 정교일, 유비쿼터스 컴퓨팅과 보안요구사항 분석, 정보보호학회지, Vol.14 No.1,, 2004, 1면.

[3] 세계일보, 2005.3.23. : '인터넷을 통한 성매매는 아예 특별법 무풍지대다.'

[4] 오기두, 형사절차상 컴퓨터 관련증거의 수집 및 이용에 관한 연구, 서울대 박사학위 논문, 2003, 15면.: 장영민, 형법개정안의 컴퓨터범죄, 한국형사정책연구원, 형사정책연구, 1992, 84면.

[5] California Computer Crime Act 1985, sec.502.

[6] The Federal Counterfeit Access Device and Computer Fraud and Abuse 1984

[7] Betzl, Computerkriminalität-Dichtung und Waheit, DSWR 1972, S.317, 415.

[8] Lindenman, IBM-Deutschland, auf einem Hearing der Interpalamentarischen Arbeitsgemeinschaft, Bonn, 13, 5, 1974, ders IPA-KEDV-Drucksache, Nr. 65, S. 24f.

[9] Taber, A survey of Computer Crime Studies, Computer & Law Journal, No.2., 1998. 195면.

[10] Sieber, Computerkriminalität und Stafrecht, S. 29.

[11] Mühlen, Computerkriminalität und Abwehrmanagmen, S. 17.: Lampe; Computerkriminaliät, DSWR 1974, S. 242ff.

[12] Tiedmann, Computerkriminalität und Missbrauch von Bankomaten, Wm 1983, S. 1326.

[13] 신각철 · 김문일, 「최신 컴퓨터범죄론」, 법영사, 1997. 12-13면.

[14] 강동범, "사이버범죄와 형사법적 대책", 「형사정책연구」 제11권 2호, 2000. 37면.

[15] 법무부, 컴퓨터범죄, 법무자료 제65집, 2003.

[16] 정진섭, "정보사회와 컴퓨터범죄 동향", 이형국 교수 회갑논문집, 1998, p.522.

[17] 강동범, 전게논문, 48면.

[18] 원혜욱, "컴퓨터관련증거의 증거조사와 증거능력", 「수사연구」, 2000.

[19] 김영옥, "컴퓨터범죄에 관한 형법적 고찰", 호남대학교 논문집, 1997, p.389.

[20] Thomas Fischer, Computerkriminalität, Berm, 1979, S.21f.,: Theoder Lenckner, Computerkriminalität und Vermögensdelikte, C.F.Müller, 1981, S.17.

[21] 현행 형법 중 제316조(비밀침해죄)와 제317조(업무상 비밀누설죄)

[22] 현행 형법 중 제98조(간첩죄)와 제113조 (외교상비밀누설죄)

[23] 門田 涉, "我の國におけるコソヒュータ犯罪の現況", 警察公論, 1985, 22면.

〔24〕 Louis Rehbner, Computerkriminalität, Zurich Schulthess Polygraphischer Verlag, AG, 1976, S.15 ; 門田 涉, 상게논문, 22면.

〔25〕 조병인·정진수·정완·탁희성, 사이버범죄에 관한 연구, 한국형사정책연구원, 2000, 18-21면.

〔26〕 최영호, "정보범죄의 현황과 제도적 대처방안", 한국형사정책연구원, 1998, 20-21면.

〔27〕 Christian K. Bschorr, Computer-kriminalitat, Gefahr u. Abwehr, S 176.

〔28〕 정진섭, "인터넷과 컴퓨터범죄의 신동향 저스티스", 한국법학원, 1996. 9. 44면.

〔29〕 동아일보, 2004.5.13.

〔30〕 Barry J.Hurewitz·Allen M. Lo, Computer-reated crimes, American Criminal law Review Vol 30, 1993. 518면.

〔31〕 角田正紀, "犯罪の國際化と捜査", 松尾浩也·井上正仁 編, 刑事訴訟法の爭點(新版), ジュリスト 增刊, 有斐閣, 1991, 99면.

〔32〕 오기두. 전게논문. 27면.

〔33〕 安富 潔. 刑事手續と コソピュタ 犯罪. 有斐閣, 1998. 247면.

〔34〕 대법원 1986. 10. 14. 선고 86도 1283 판결은 "외국주재 대한민국 총영사관 영사작성의 영사증명서의 내용이, 오사까 다이이찌호텔 종업원 사까구찌에 의하면 1983년 1월경 기다무라라는 사람이 동 호텔에 투숙한 일이 있다라는 것이라면, 이는 피고인 아닌 사까구찌라는 사람의 공판기일외에서의 진술을 내용으로 하는 전문증거에 해당하는 것이어서 형사소송법 제311조 내지 제 316조에 규정된 특단의 사정이 있다고 볼 자료가 없는 한 이를 유죄의 증거로 삼을 수 없다"고 한다.

〔35〕 우리 형사소송법에서도 제221조2에 동일취지의 규정을 하고 있다.

〔36〕 우리 민사소송법 제268조도 동일취지의 규정을 하고 있다.

〔37〕 角田正紀, 前揭論文, 101면.(해당 日本 下級審 判例, 東京地決 昭和 五三, 1978. 9. 21.; 東京高判 昭和 五九, 1984. 4. 27.; 刑制月報 제16권 3, 4호, p.180; 東京高判 昭和 六三, 1988. 7. 29, 判示 1257호. 11면.)

〔38〕 오기두, 전게논문, 38-40면

〔39〕 오기두, 전게논문, 40-42면

〔40〕 백형구·차용석·허형구, 「주석형사소송법(중)」, 한국사법행정학회, 1992, 582면.

〔41〕 대법원 1979. 9. 25. 선고 79도 1852 판결.

〔42〕 정동기, "국제형사사법공조의 기본원칙", 「저스티스」 제29권 제1호, 1996. 8. 60면.

〔43〕 우리 국제형사사법공조법 제22조 제2항은 우리나라가 외국의 요청으로 공조자료를 송부하는 경우 그 자료 등의 사용, 반환 또는 비밀유지 등에 관하여 요청국이 지켜야 할 준수사항을 정하여 그 이행에 대한 보증을 요구할 수 있다고 규정하고 있을 뿐 외국이 요청국이 되었을 때 그 외국이 부과한 조건을 우리가 준수해야 하는지 여부에 관한 규정은 두고 있지 않다.

〔44〕 정동기, 전게논문, 52면.

〔45〕 정동기, 상게논문, 56면.

저 자 소 개

오 태 근

2005년 2월 조선대학교 법학과, 법학박사

2005.~현재 :전남도립남도대학 경찰행정경호과 초빙교수 조선대학교 법과대학 외래교수

〈관심분야〉 컴퓨터범죄, 테러리즘