스파이웨어의 법적 문제와 규제 입법의 방향

연구원 이 민 영*

최근 컴퓨터 이용자의 개인정보와 인터넷 사용행태 및 프로필을 유출하는 것으로 알려진 스파이웨어에 대한 관심이 증대되고 있다. 여기서는 스파이웨어 프로그램이 지니고 있는 법률문제의 논의와 미국에서의 스파이웨어 규제에 관한 입법동향을 살펴보고 시사점을 도출함으로써 스파이웨어에 대한 정책적 대응방안을 모색하고자 한다.

목 차

Ⅰ. 머리말
Ⅱ. 스파이웨어의 의의
1. 개념의 정의
2. 논란의 추이
3. 논의의 확장
Ⅲ. 스파이웨어의 규제
1. 법해석적 검토
2. 법실증적 분석
3. 법정책적 제언
Ⅳ. 맺음말

Ⅰ. 머리말

현대사회가 지식정보화라는 순탄치만은 않은 여정을 걸어오는 동안 안겨준 순기능의 이면에는, 기술디스토피아(technology dystopia)가 상존하고 있음은 주지하는 바와 같다. 인터넷의 단일화된 네트워크시설과 이용자에 대한 신원확인기술의 결합에 의하여 개인의 사생활과 익명성의 가치가 위협받는, 이른바 '철창 없는 감옥'의 시대에 우리가 살아가고 있는 것이다. 이는 Michel Foucault가 권력유지의 기술로 제시한 바 있는 Panopticon의 정보적 재구성에 다름 아니다.

Panopticon은 일찍이 18세기에 Jeremy Bentham이 고안한 건축의 형태로서, 그 원리는 다음과 같다.[1)]

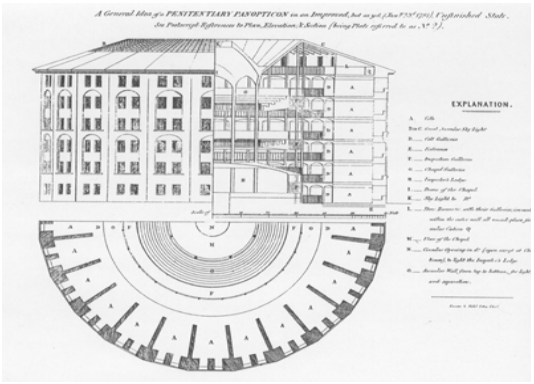
연락처: * 미래한국연구실 (02) 570-4083, mylee@kisdi.re.kr

1) 미셸 푸코 著・오생근 譯,『감시와 처벌: 감옥의 탄생』, 나남출판, 1994, 295쪽: Panopoticon은

"주위에 원형의 건물이 에워싸여 있고, 그 중심에 탑이 하나 있다. 탑에는 원형건물의 안쪽으로 향해 있는 여러 개의 큰 창문들이 뚫려 있다. 주위의 건물은 독방들로 나뉘어져 있고, 독방 하나하나는 건물의 앞면에서부터 뒷면까지 내부의 공간을 모두 차지한다. 독방에는 두 개의 창문이 있는데, 하나는 안쪽을 향하여 탑의 창문에 대응하는 위치에 나 있고, 다른 하나는 바깥쪽에 면해 있어서 이를 통하여 빛이 독방을 구석구석 스며들어 갈 수 있다. 따라서 중앙의 탑 속에는 감시인을 한 명 배치하고, 각 독방 안에는 광인이나 병자·죄수·노동자·학생 등 누구든지 한 사람씩 감금할 수 있게 되어 있다. 역광선의 효과를 이용하여 주위 건물의 독방 안에 감금된 사람의 윤곽이 정확하게 빛 속에 떠오르는 모습을 탑에서 파악할 수 있는 것이다. 그것은 바로 완전히 개체화되고, 항상 밖의 시선에 노출되어 있는 한 사람의 배우가 연기하고 있는 수많은 작은 무대들이자 수많은 감방이다. 일망원형감시의 이 장치는 끊임없이 대상을 바라볼 수 있고 즉각적으로 판별할 수 있는, 그러한 공간적 단위들을 구획 정리한다.…가시성의 상태가 바로 함정인 것이다."

전통적인 감옥에서는 죄수들을 한 곳에 몰아넣는 반면, 일망감시시설(一望監視施設)로서 Panopticon은 감시자가 중앙탑에 있고 죄수들은 주위의 독방에 격리수용되도록 구조화된 원형감옥(圓形監獄)이다. 그리하여 죄수들간의 의사소통이나 집단의식의 위험성을 차단시키는 효과를 내며, 죄수들로 하여금 끊임없이 감시받는다는 의식을 갖게 만든다. 그리고 중앙탑의 감시자는 상징적인 모습으로 언제나 존재하지만 자신의 모습은 노출되지 않고 있는데, 이는 보이지 않는 권력의 존재가 보이는 권력의 존재보다 훨씬 강한 지배력을 지님을 말하고 있다.

〔그림 1〕 Bentham이 설계한 Panopticon의 구조

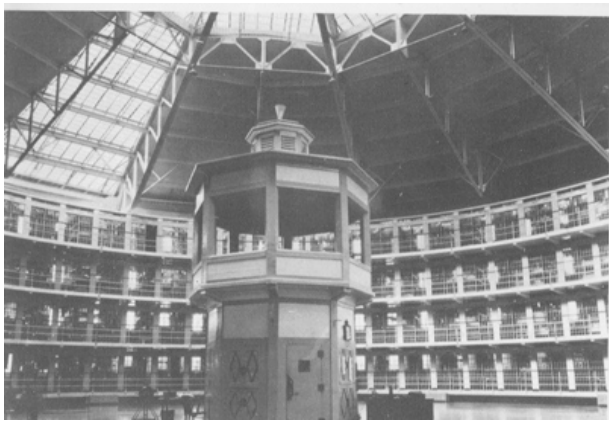


이처럼 감시자를 중심으로 건축된 바퀴모양의 감옥인 Bentham의 Panopticon은 감시자가

당시 망원경과 비슷한 광학기구를 지칭하는 용어로 사용되던 말이었는데, 그 어원은 '다 본다(all seeing)'는 의미를 나타내는 그리스어에서 유래한다.

언제든지 죄수를 그 관찰 아래 놓을 수 있어 감시에 관한 사고의 전형으로 파악되며,[2] 여기에서 일상생활에서의 감시를 낳고 있는 현대사회의 어두운 측면을 Foucault는 간파한 것이다. '봄- 보임'의 관계를 분리시키는 원형감옥의 현대적 재해석인 것이다.

〔그림 2〕 Panopticon 구조의 미국 Stateville 교도소



Foucault는 '과거에는 권력구조의 상위층으로 올라갈수록 개인화가 이루어졌는데 현대에서는 권력이 점점 익명성을 띠게 되고 권력의 지배를 받는 사람들은 더욱더 개체화 혹은 개인화되며, 과거에 위험한 범죄자를 단순히 격리시키는 데 불과했던 감금은 수감자에 대한 권력의 감시로 확산되고 이러한 권력의 전략으로 인간은 개체화되어 왔다'면서 '일망감시시설 구조와 같은 감시체제로 현대의 인간은 권력에 예속되어가고 있다'고 주장한다. 모든 지식은 정치적 권력과의 관계 속에서 생성·존재한다고 말하는 Foucault에 따르면, 현대사회야말로 감금사회·관리사회·처벌사회·감시사회로 이해되어진다.

Panopticon과 같은 21세기형 원형감옥의 탄생은, 감시주체가 비단 국가나 공공기관에만 국한된 것이 아니라 기업이나 개인도 될 수 있음을 암시한다. 우리가 알아차리지 못한 진보된 기술과 놀라운 방법으로 사생활을 추적·감시하는 사회체제가 형성되고 있는 것이다. 감시를 통한 사생활침해요인은 우리 사회를 원형감옥으로 형성하는 기술적 배경으로 작용하며, 인터넷을 위시한 네트워크는 중앙탑의 역할을 하고 있다. 이러한 가운데 스파이웨어가 존재한다. 후술(後述)하는 바와 같이, 스파이웨어는 개인정보를 유출하고 인터넷 사용행태를 송출하는

2) James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. Cin. L. Rev. 177, 186(1997).

기능을 보유하는 까닭에 개인의 사생활과 익명성의 가치를 위협하고 일상적 감시를 조장하는 것으로 파악되기 때문이다. 이에 대한 위기의식을 바탕으로 스파이웨어를 원형감옥으로 상징되는 감시사회의 한 단면으로 평가하는 관점에서, 본고에서는 그 의의와 규제에 관한 동향을 살펴보고 시사점을 도출함으로써 역감시(逆監視)를 통한 투명성 제고를 꾀하려 한다.

Ⅱ. 스파이웨어의 의의

1. 개념의 정의

가. 명칭과 의미

스파이웨어(spyware)는 무료 또는 유료로 배포되는 공개 프로그램에 들어있는 일종의 정보 수집 모듈을 통칭하는 것으로, 광고효과 모니터링을 위하여 프로그램 이용자에 대한 개인정보를 미리 설정된 특정 서버로 보냄으로써 외부에서 인터넷을 통해 특정 이용자의 개인정보를 확인할 수 있도록 해주는 소프트웨어를 의미한다. 인터넷이나 PC통신에서 무료 유틸리티 프로그램을 다운로드 받을 때, 자동으로 컴퓨터 본체에 탑재돼 불법으로 개인정보를 상대방에게 보내는 개인정보 유출프로그램인 것이다.[3)]

인터넷을 통해 급속 확산되고 있는 스파이웨어는 개인정보를 유출하고 무차별적으로 광고사이트를 띄우지만, 바이러스 백신 프로그램으로도 치료되지 않고 스팸메일 업체에 개인정보를 유출시키고 있어 새로운 인터넷 공해로 떠오르고 있다.[4)] 개인정보를 빼내 광고업체 등에 판매하기 위한 목적으로 설치되어 인터넷 이용자 정보와 이메일의 내용까지 소프트웨어 제작업체로 유출하기도 하므로 이용자의 주의가 필요하다.[5)]

원래 이름이 애드웨어(adware)인 이 족속(族屬)은 미국의 어느 인터넷 광고전문회사에서 개인 이용자의 취향을 파악하기 위해 고안된 것으로, 광고(advertisement) 효과를 높이기 위한 소프트웨어라는 의미로 애드웨어라 불리었다. 그러나 표적광고의 수단으로 이용되기 시작하면서 필요한 정보만을 추출한다는 개발 의도와 달리 최근에는 이용자 이름은 물론 IP 주소·즐겨 찾는 URL·개인 ID·패스워드까지 알아낼 수 있게 발전되었고, 마치 기업의 비밀을 탐지하는 첩자(spy)와 같은 소프트웨어로 인식되는 탓에 스파이웨어라 불리고 있다.

---

3) 김철완·이민영 外, 『건전한 정보통신 윤리확립과 개인정보 보호대책 방안 연구』, 연구보고 01-03, 정보통신정책연구원, 2001, 127쪽.
4) 문화일보 2003년 8월 14일자 27면 기사.
5) 국민일보 2003년 9월 2일자 27면 기사.

나. 기능과 성격

스파이웨어는 악성 소프트웨어[6]처럼 시스템을 손상시키지는 않지만, 당해 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑할 때 이용자의 개인정보나 온라인활동에 관한 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전송하는 것을 주된 기능으로 한다. 이렇듯 스파이웨어는 단지 개인정보를 유출할 뿐이므로 백오리피스 등의 해킹 툴과는 구별된다.

이와 같은 스파이웨어를 통하여 ① 시스템 레지스트리에 있는 이용자 이름, ② 이용자의 IP 주소, ③ 이용자의 컴퓨터에 깔린 소프트웨어 목록, ④ 이용자가 찾아간 URL 목록, ⑤ 마우스로 누른 배너 광고, ⑥ 여러 사이트에서 내려 받은 파일 정보, ⑦ 브라우저를 이용할 때에 나타나는 동작 정보 등을 알아낼 수 있다.

스파이웨어는 대개의 경우 유용한 유틸리티 안에 함께 적재되어 있다가 유틸리티 장착 시에 동시에 설치되어 지속적으로 동작하는 형태를 취한다. 이 경우 스파이웨어는 일종의 트로이 목마로 분류된다. 그러나 스파이웨어가 전파되는 과정이 관련된 유틸리티의 내려 받기와 실행만을 통해서 이루어지는 것이 아니라, 특정 사이트를 방문하는 것만으로도 설치하여 운영되는 경우도 볼 수 있어서 홈페이지 서버에 설치되어 이 서버를 방문하는 사용자의 웹브라우저가 실행되는 동안 내내 사용자의 인터넷 사용 실태 정보를 보내준다. 이러한 경우 스파이웨어는 혼합형 웜의 성격을 띄게 되어 이번에는 웜으로 분류될 수 있다.

2. 논란의 추이

가. 국내에서의 논란

스파이웨어의 존재는 2000년 6월 2일 한국통신 ADSL 이용자 동호회의 한 회원이 동호회 홈페이지[7]에 주의를 촉구하는 글을 올리면서 네티즌 사이에 회자되기 시작하였다. 이러한 스파이웨어는 정품의 무료배포재원을 마련하기 위하여 소프트웨어업체가 마케팅정보회사와 계약을 맺고 설치하는 경우가 대부분인데, 네티즌이 많이 사용하는 공개 프로그램에 '인터넷 스

6) 그 위험성이 일반인들에게도 이미 체험적으로 잘 알려져 있는 악성 소프트웨어(maliware; malicious software)는 이용자의 동의 없이 설치되거나 실행되어 시스템에 이상을 일으키거나 사용자의 제반 정보를 유출하기도 하고 어떤 경우는 손상시킨다. 컴퓨터 바이러스로 대표되는 악성 소프트웨어는 크게 바이러스(virus), 웜(worm), 트로이 목마(Trojan horse) 그리고 불법 서버(illicit server)로 구분되어지며, 기술적으로나 법적으로 많은 문제점을 낳는 나쁜 소프트웨어인 탓에 '악성(惡性)' 소프트웨어로 불리고 있다; 김명주, 「스파이웨어, 합법적인 악성 소프트웨어인가?」, 『인터넷법률 제9호』, 법무부, 2001, 75~78쪽 참조.

7) http://sig.kornet.net/adsl

파이웨어'라는 개인정보유출 프로그램을 포함시켜 네티즌의 시스템 정보 및 인터넷 사용 상황을 미국 Radiate사로 보고하고 있다는 주장이 제기되었다.

이에 대해 국내 백신업계의 견해는 대립되고 있다. 즉 스파이웨어가 이용자 정보를 유출한다는 점에서 위험성이 있으며 악의적 해커에 의해 금융권과의 사이버거래에 사용되는 ID나 패스워드 등이 유출될 가능성을 배제할 수 없다는 측면에서 그 위험성을 경고하고 있는 입장과 소프트웨어 설치조건에 스파이웨어를 함께 설치한다는 항목이 명시돼 있어 법적으로도 하자가 없으므로 백신 프로그램에 스파이웨어 제거기능을 추가하지 않겠다는 입장이 그것이다.

나. 해외에서의 논란

지난 2000년 2월에는 프랑스 국방성 산하 전략문제대표단의 한 고위관료가 전세계 소프트웨어시장의 90%를 차지하는 Microsoft사의 소프트웨어에 컴퓨터 내의 모든 정보를 미국의 국가안보국(NSA)으로 자동 전송하는 비밀프로그램이 설치되어 있다는 주장을 제기한 바 있다.

미국에서는 2001년 초, 특정 소프트웨어를 설치하면 이용자의 온라인 행동에 대한 정보가 인터넷서비스제공자에게 지속적으로 흘러들어 감으로써 이용자 본인도 모르게 개인정보가 유출된다는 내용의 언론보도가 있었다.[8] 뉴스위크에 실린 이 기사는 NBC 방송이 운영하는 NBCi라는 인터넷방송을 통해서 무료로 배포되던 유용한 소프트웨어인 QuickClick에 대해 제기된 스파이웨어 기능의 의혹에 대해 보도하면서, 개인정보 유출의 심각성과 위험성을 경고함과 동시에 인터넷서비스제공자가 인터넷 이용자의 개인정보를 상업적으로 이용하고 있음에 대해 제기된 논란을 싣고 있다. 해당 소프트웨어의 소스코드를 분석한 미국 사생활보호협회 기술간사의 판단을 근거자료로 싣고 있는 이 기사에 대해 NBCi측에서는 분석결과가 사실임을 인정한 바 있어 온라인을 통한 개인정보의 수집이 기술적으로 실시되어 왔음이 확인되었으나, NBCi에서는 개인정보가 입수되는 즉시 폐기된다고 주장하였다고 전해진다.

한편 Time지의 첨단기술 수석기자인 Adam Cohen은 '인터넷의 위헌성'이라는 기사를 쓰기 위해서 인터넷상에서 VNC(Virtual Network Computing)이라는 무료 스파이웨어 프로그램을 다운받아 압축을 풀고서 같은 회사 동료의 컴퓨터에 설치하고 그 동료의 ID를 절도한 바 있다. 이렇게 하여 동료의 컴퓨터에서 이루어지는 모든 작업이 그의 모니터에 그대로 나타났으며, 그의 동료가 인터넷상에서 어느 웹사이트를 방문하는지를 알 수 있었고 동료가 읽은 e-mail에 대해 답장을 쓰는 것조차 지켜볼 수 있었다고 한다.[9] 이 사례를 보도한 2001년 6월

8) Steven Levy, *Is It Software? Or Spyware*, Newsweek Vol. 137, 2001. 2. 19.

9) http://www.CNN.com/showcase

27일자 CNN 방송의 인터뷰기사에서, 스파이웨어를 찾을 수 있는 검사프로그램을 실행한다 해도 특정 소프트웨어가 모든 스파이웨어를 잡아내지 못할 뿐만 아니라 스파이웨어를 찾아낸다고 주장하는 소프트웨어가 실제로는 제대로 기능하지 못하기 때문에 정보의 유출 여부조차 알아낼 수 없다는 데에 그 심각성이 있다고 Cohen은 말했다.

다. 정보유출의 논의

스파이웨어는 이용자의 개인정보나 인터넷 사용 형태에 관한 정보를 지속적으로 유출하는 것을 주된 목적으로 한다. 이처럼 유출한 정보는 나중에 사용자에게 보다 효율적인 서비스를 제공하는 데 활용되기도 하지만, 그것은 어디까지나 표면적인 이유이지 언제나 믿을 수 있는 성질의 것은 아니다.

개인정보를 빼낼 수 있는 모듈을 무료 소프트웨어에 첨부해 이를 다운로드할 때 자동으로 보내는 방법으로 유포되고 있는 스파이웨어는 엄연히 개인정보를 외부로 알려주고 있는 것이 사실이며, 자기도 모르는 사이에 사생활이 노출될 수 있고 해커나 악의적인 업체에 의해 피해를 볼 수도 있으며 귀찮은 스팸메일에 시달리게 될 수도 있다. 또한 스파이웨어를 포함하고 있는 소프트웨어를 설치할 때 사용허가약정(使用許可約定: License Agreement)에 개인정보를 외부로 유출한다는 사실을 표시하는 경우도 있지만, 거의 모든 이용자들은 약정을 읽지 않아 내용도 모른 채 함께 설치하는 경우가 많다.

더군다나 본 프로그램을 삭제할지라도 첨부되어 있던 스파이웨어는 삭제되지 않으며 본 프로그램을 실행하지 않아도 몰래 작동을 한다. 게다가 프로그램을 제작한 회사가 정보송출모듈을 임의로 업그레이드할 경우, 이용자의 키보드 사용명세까지 알아낼 수 있는 고성능 소프트웨어 설치가 가능하기 때문에 전자상거래나 사이버 뱅킹을 할 때 신용카드번호나 패스워드가 유출될 가능성은 매우 크다.[10] 이용자들이 본인도 모르는 사이에 자신의 컴퓨터나 웹브라우저에 스파이웨어의 설치와 활동을 이미 승인해 준 경우가 대부분이기 때문에 문제의 심각성이 존재한다. 그렇기 때문에 어느 특정한 소프트웨어를 설치하는 데 동의하여 그 수락의 의사로 마우스의 클릭이라는 표시행위를 하였으나 본의 아니게 스파이웨어를 함께 내려 받게 되고 그것이 개인정보를 유출·도용하는 일반적 관행에 적절한 규제가 요구되는 것이다.

10) 김연수, 『개인정보보호』, 사이버출판사, 2001, 481~482쪽.

3. 논의의 확장

가. 유형의 분류

스파이웨어가 설치된 소프트웨어들은 기술적인 측면으로 볼 때 어떤 스파이웨어 컴포넌트를 사용했느냐에 따라 다음과 같이 크게 구분해 볼 수 있다.[11)]

1) Radiate사의 Aureate

광고전문회사로 1996년에 세워진 Radiate사는 많은 소프트웨어 제품에 스파이웨어 컴포넌트의 원조인 Aureate 컴포넌트를 이식함으로써 해당 소프트웨어 사용자에 대한 광고주 활동을 극대화시켜 주었다. 현재로서는 가장 많은 소프트웨어들이 이 스파이웨어 컴포넌트를 사용하고 있기 때문에 스파이웨어를 발견하고 제거하고자 하는 안티- 스파이웨어(anti-spyware) 제품들이 우선적으로 Radiate사의 Aureate 컴포넌트를 취급함으로써 많은 스파이웨어를 처리할 수 있다. Aureate가 적재된 대표적인 소프트웨어 목록은 다음과 같다.

– CuteFTp	– DownloadAgent	– GetRight
– Go!Zilla	– JPEG Optimizer	– MP3 Album Finder
– MP3 Player 2000	– Netbus Pro	– NetScan 2000
– ProxyChecker	– Total Whois	– WebCamVCR
– WebCam Viewer	– WinEdit 2000	– Zip Express 2000

2) Conducent사의 Timesink

이는 사용자의 컴퓨터에 설치된 소프트웨어에 특정 컨텐츠를 동적으로 전달해주는 기술을 바탕으로 활동하는 컴포넌트로서, 사용자에게 노출된 컨텐츠상의 광고정보 그리고 사용자가 자료를 선택한 정보 등이 보고자료로서 매일 Conducent사에 되돌려 보내진다.

3) Web3000사의 Web3000

특정 웹페이지를 방문한 사람들의 숫자와 그곳에서 머문 시간 등을 분석하여 정보를 송부하는 이 스파이웨어 컴포넌트는, 웹브라우저의 배너 광고상에 직접 적재되어 있다가 사용자가 어느 사이트를 방문하든지 함께 따라다니며 활동한다.

4) 기타 스파이웨어 컴포넌트

그밖에 Gator 컴포넌트, Comet Cursor 컴포넌트, BeeLine 컴포넌트, GoHip 컴포넌트 등이 두각을 나타내고 있으며, 이들 이외에도 새로운 컴포넌트들이 지속적으로 나타나고 있다.

11) 이하 김명주, 같은 글(註 6), 79~81쪽 참조.

나. 발견과 제거

여기서는 컴퓨터 이용자가 개별적으로 스파이웨어에 대응하는 방법에 대해 알아본다.[12]

이용자들이 잠재적 위험성을 느끼는 스파이웨어에 대해 가장 최신의 정보를 제공받으려면, SISL 사이트로 불리는 Info-Force 홈페이지[13]를 방문하면 된다. 스파이웨어를 한 마디로 '비열한 행위(a despicable action)'로 정의하는 Gilles Lalonde에 의해 운영되는 SISL 사이트는, Spyware Infested Software List의 약칭이다. SISL 사이트는 스파이웨어 관련 소프트웨어 목록을 제공하는 서비스 이외에도, 스파이웨어 출현에 따른 일종의 소프트웨어 건전성 확인 프로그램이라 할 수 있는 '스파이웨어 없는 소프트웨어 인증 프로그램(Spyware Free Software Certification Program)'도 운영한다.

1) 컴퓨터 백신 프로그램

현재 스파이웨어의 특성상 나타나는 다음과 같은 심각한 문제점에 부딪혀 스파이웨어를 발견하고 제거하는 기술의 적용은 거의 고려 대상에서 제외된 상황이다. 그것은 첫째로 컴퓨터 바이러스와 같이 불법적인 악성 코드만을 골라내어 통보해주고 제거하는 백신 소프트웨어의 원래 기능 측면에서 볼 때, 아직까지 명백한 증거를 드러내지 않은 스파이웨어를 잠재된 위험 가능성 때문에 제거한다는 것은 기술적 월권이라는 시각이 존재한다. 둘째로 스파이웨어를 포함하여 함께 설치하는 유틸리티의 대부분이 해당 스파이웨어를 발견하여 제거하는 순간부터 원래의 기능마저 중단하거나 오류를 내도록 작성되었다는 점이 그것이다. 국내 백신개발업체에서도 같은 입장을 취하고 있는 예가 있다.[14]

2) Ad-aware

이러한 논란으로 인해 사용자가 스파이웨어를 적극적으로 발견하고 제거하기 위해서는 이를 전문으로 담당하는 소프트웨어를 사용하는 것이 효과적이다. 지금까지 스파이웨어를 발견하고 제거하는 데 가장 효과적인 것으로 알려진 소프트웨어는 Ad-aware이다.

2003년 현재 6.0버전이 출시되어 있는 Ad-aware는 Lavasoft사에서 만든 것으로, 다운로드받기 위해서는 해당 홈페이지[15]를 방문하면 된다. Ad-aware를 설치하여 실행하면, 이용자 컴퓨터의 메모리・레지스트리・하드디스크를 검색하여 이미 알려진 바 있는 스파이웨어 컴포넌트의 존재 여부를 검사하고 제거할 수 있다.

---

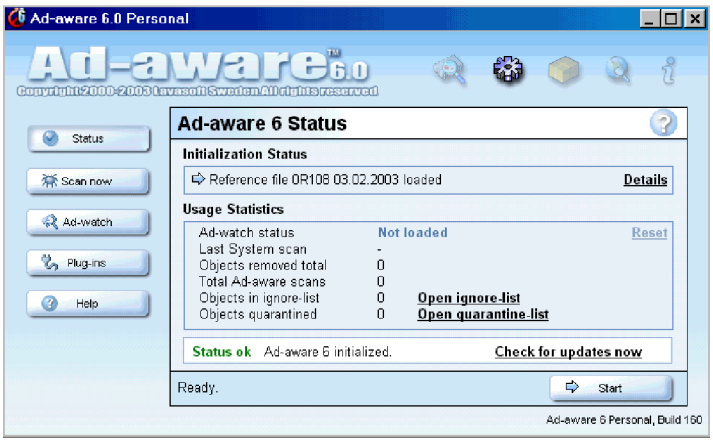
12) 이하 김명주, 같은 글(註 6), 82~84쪽 참조.

13) http://www.infoforce.qc.ca/spyware

14) 안철수바이러스연구소가 이 경우에 해당한다. 반면 하우리는 스파이웨어의 위험성을 경고하면서 스파이웨어를 검색・삭제할 수 있는 패치파일을 자사의 백신소프트웨어에 추가한 바 있다.

15) http://www.lavasoftusa.com

〔그림 3〕 Lavasoft 사이트에서 제공되는 Ad-aware 6.0



3) OptOut

Steve Gibson이라는 프로그래머가 발표한 프로그램인 OptOut은 본격적으로 스파이웨어에 대항한 전문 소프트웨어이다. 이 소프트웨어를 작성한 Gibson이 다른 영역으로 연구방향을 옮기면서 OptOut은 이제 공급이 중단된 상태이지만, 스파이웨어의 심각성을 알리고 이에 대한 기술적 대처를 한 공로는 지금도 인정받고 있다. 해당 기술이나 관련 정보를 제공하는 웹사이트[16]는 아직도 열려 있다.

Ⅲ. 스파이웨어의 규제

1. 법해석적 검토

가. 흠 있는 의사표시

법률행위의 필수적 요건으로서 권리주체의 의지에 의하여 권리의 발생·변경·소멸이라는 일정한 법률효과를 가져오는 행위를 의사표시(意思表示)라고 하는 바,[17] 이러한 의사표시는 어떠한 행위를 한다는 의식이 있어야 하고, 그 행위가 특정의 법률효과를 얻기 위한 의도에서 행해져야 하며, 말이나 글 혹은 행동 등의 방법을 통해 표현되어져야 한다. 그런데 의사표시

16) http://grc.com/optout.htm

17) 의사표시는 자연인의 일상적 행위 가운데 일정한 법적 의사를 가지고 하는 행위를 법률적으로 분리해내기 위한 강학상(講學上)의 개념이다: 현암사 編, 『법률용어사전』, 현암사, 2002, 422쪽.

에 있어 내심의 의사와 표시의 행위가 서로 일치하지 않거나 의사형성과정에 결함이 있다면, 바꾸어 말해서 의사표시에 흠결(欠缺) 또는 하자(瑕疵)가 있으면 그 흠(欠)의 정도에 따라 무효(無效)가 되거나 혹은 취소(取消)되어질 수 있다.

그렇다면 인터넷상에서 무료 유틸리티[freeware] 혹은 공유 소프트웨어[shareware] 등을 내려 받는 동안[downloading] 무의식중에 스파이웨어의 설치를 수락하게 되는 경우 컴퓨터 이용자는 스파이웨어의 설치를 동의(同意)한 것인가? 이는 분명 표의자(表意者)의 효과의사(效果意思)는 특정 소프트웨어의 다운로드인데, 내밀하게 은폐된 '스파이웨어 설치의 동의'에 마우스를 클릭하는 표시(表示)로 의사표시가 이루어짐으로써 논란의 여지를 남기는 사안(事案)으로 보인다. 다시 말해 표의자가 지니는 '동의'의 의사는 특정 소프트웨어의 설치에 있으나 표시되는 '동의'는 스파이웨어의 다운로드로 귀속되므로, 여기에 과연 의사표시의 흠이 존재하지 않는 것인지 의문이다. 아래에서 살펴본다.

우선 컴퓨터 이용자가 의식적으로 자신의 포괄적 효과의사와 다른 전자적 의사를 선택하여 입력행위를 함으로써, 그 입력행위대로 컴퓨터가 효과의사와는 다른 표시를 한 경우에 있어 의사표시의 효력이 문제된다. 이러한 전자적 의사표시가 특정한 내용의 의사표시를 하고자 하는 표의자의 생각을 말하는 진의(眞意) 아닐 때에는, 우리 민법 제107조[18]를 적용하면 원칙적으로 유효하며 동조(同條) 단서에 따라 상대방이 전자적 의사표시가 표의자의 진의 아님을 알았거나 알 수 있었을 경우에는 무효라고 할 것이다. 하지만 이 때 비진의의사표시(非眞意意思表示)에서는 표시와 진의의 불일치에 대하여 표의자가 알고 있어야 한다. 이렇듯 비진의의사표시가 표의자의 심리적 의사와 입력되는 프로그램 등으로 전자화된 의사간에 불일치가 있음을 표의자가 스스로 인식하는 경우에만 제한적으로 적용된다면, 표의자가 대부분 그 사실을 모르는 것이 일반적인 본 사안에서는 비진의의사표시를 구성하지 않는다고 봄이 일응 타당한 것으로 보인다.

다음으로 착오(錯誤)의 문제를 검토할 필요가 있다. 컴퓨터 이용자인 표의자가 다운로딩 과정에서 스파이웨어를 내려 받을 수 있음을 인식하지 못하고 특정 소프트웨어의 설치만을 의도하여 마우스를 클릭하였다면 컴퓨터 프로그램이라는 설비의 이용에 잘못이 있는 경우로 볼 수 있다는 측면에서 그러하다. 달리 표현하자면 컴퓨터 이용자의 포괄적 효과의사와 컴퓨터의 표시가 일치하지 않는 것으로, 표시의 내용과 내심의 의사가 일치하지 않는 것을 표의자

18) 民法 第107條 (眞意 아닌 意思表示) ① 意思表示는 表意者가 眞意 아님을 알고 한 것이라도 그 效力이 있다. 그러나 相對方이 表意者의 眞意 아님을 알았거나 이를 알 수 있었을 경우에는 無效로 한다.
② 前項의 意思表示의 無效는 善意의 第三者에게 對抗하지 못한다.

자신이 알지 못하는 사안이다. 앞서 살펴본 비진의의사표시의 경우 그 성립요건에서 '표의자의 인식'이 요구됨에도 불구하고 스파이웨어와 관련해서는 일반적으로 이용자의 인식이 결여되는 경우가 상례적인 바, 이와 같이 의사와 표시의 불일치를 알지 못하는 표의자를 보호하려는 취지에서 일정한 요건에 따라 착오에 기한 의사표시를 소급적(遡及的)으로 무효화시킬 수 있는 착오론이 적용될 수 있을 것으로 보여진다. 그 가운데에서도 본 사안은 동기의 착오를 다루어져야 하리라 본다. 동기(動機)의 착오란 의사표시를 함에 있어서 그 의사표시의 동기에 착오가 생긴 것으로, 의사형성과정에서 그러한 의사를 품게 된 동기가 어떤 사실에 대한 착오에 의해 이루어진 경우를 의미한다. 여기서 그 동기가 외부로 표시된 경우에 한하여 그 의사표시를 취소할 수 있다고 판단하더라도, 특정 소프트웨어의 설치에 동의하고 그 다운로드를 하려는 데 표의자의 진의와 효과의사가 있음 - 역으로 표의자는 스파이웨어의 설치와 개인정보의 유출을 꺼린다는 사실- 을 상대방이 알 수 있는 경우이다. 그러기에 표의자의 중과실이 확인되지 않는 한, 당해 사안은 법률행위의 내용의 중요부분에 착오가 있는 때에 해당하므로 우리 민법 제109조[19]에 의해서 취소 가능한 의사표시로 풀이될 수 있다.

마지막으로 본 사안에 있어 의사표시의 상대방이 표의자를 기망(欺罔)하고 있지는 않는가 하는 점이다. 살피건대 특정 소프트웨어의 설치 동의서에 숨겨진 스파이웨어 수인약정(受引約定)은 고지의무(告知義務)를 해태(邂怠)하고 있으며, 스파이웨어의 설치를 통해 개인정보의 유출과 상업적 활용을 전제로 하고 있다. 그리고 마우스를 클릭하면 스파이웨어가 설치되면서 개인정보가 유출된다는 진실이 차단된 가운데, 사실상 단순히 특정 소프트웨어의 설치를 의도한 표의자는 그릇된 의사형성에 의해 의사표시로서의 동의를 표하게 된다. 이와 같은 경우 표의자인 인터넷 이용자에게는 통상의 '과실(過失)'만이 존재하는 반면에 스파이웨어를 운용하는 자는 부당하게 스파이웨어 프로그램을 설치하려는 '고의(故意)'와 함께 개인정보를 수집·유포하려는 '악의(惡意)'를 보유한다는 점을 염두에 둔다면, 여기서의 동의를 진정한 의사로 받아들이기는 어렵다고 여겨진다. 더군다나 스파이웨어의 설치를 은닉하면서 개인정보의 유출 및 부정사용을 의도하고 있는 데에는 합법적이지 못한 범의(犯意)가 존재하고 있다는 점에서 상대방이 획책하고 있는 기망행위의 위법성을 확인할 수 있다. 그러므로 우리 민법 제110조[20]를 좇아 본 사안을 사기(詐欺)에 의한 의사표시로 보아 취소할 수 있는 행위로

19) 民法 第109條 (錯誤로 인한 意思表示) ① 意思表示는 法律行爲의 內容의 重要部分에 錯誤가 있는 때에는 取消할 수 있다. 그러나 그 錯誤가 表意者의 重大한 過失로 인한 때에는 取消하지 못한다.
② 前項의 意思表示의 取消는 善意의 第三者에게 對抗하지 못한다.

20) 民法 第110條 (詐欺, 强拍에 의한 意思表示) ① 詐欺나 强拍에 依한 意思表示는 取消할 수 있다.

구성할 수도 있을 것이다.

종합해보면 '표의자의 인식'이라는 조건이 충족되지 못함에 대한 과실과 확연한 상대방의 고의를 비교형량(比較衡量)하고 상대방인 표시수령자(表示受領者)에게 '표의자의 인식'을 가로막은 데 대한 응분의 책임을 묻는 것이 필요할 것이므로, 결국 은밀히 스파이웨어의 설치를 설정한 표시수령자가 악의(惡意) 없음을 입증하지 못하면 당해 의사표시는 하자가 있는 것으로 보아 취소될 수 있다고 새겨야 한다. 왜냐 하면 사용자의 효과의사는 스파이웨어의 설치나 개인정보의 유출에 있지 않고, 특정 소프트웨어를 다운로드하려는 데 있기 때문이다. 개인정보의 유출 가능성이 잠식된 상황에서 이루어진 스파이웨어의 설치에 관한 동의의 의사표시는 진의가 함몰된 것이고, 따라서 흠 있는 의사표시로 다루어진 것이 신의칙(信義則)에도 부합하리라 본다. 위 법리(法理)에 비추어 보면 본 사안에서의 의사표시는 그 하자로 인해 취소할 수 있는 것이 된다. 이러한 판단의 근저에는 특정한 모듈의 설치로 인해 개인정보가 유출될 수 있음이 명확히 고지되지 않는다면 클릭이라는 행위가 동의의 의사표시로 인정되고 동의의 절차 준수로 해석되는 데는 무리가 있다는 생각과 당사자간의 형평(衡平)을 고려하여 법이론을 적용하자는 취지가 담겨 있다.

그렇지만 이렇게 법리구성이 이루어진다고 할지라도, 이미 설치된 스파이웨어에 따른 개인정보의 유출의 피해에 대해 설치 동의 의사표시의 취소가 보전해줄 수 있는 것은 없다. 취소가능한 의사표시라 할지라도 이미 수집・획득된 개인정보의 환원이 보호가치의 실익(實益)을 가져다줄 수 있을 것인지에 대하여는 부정적일 수 밖에 없기 때문이다. 이러한 연유에서 스파이웨어에 대한 적절한 규제가 요망된다. 한편으로는 현행법규에서 명백히 위법인 개인정보유출을 감행하고 있다는 점에서 그러한 불법 조장에 대한 규제는 입법정책적으로 긴요하다고 판단된다. 개인정보침해에 대해 불법행위로 인한 손해배상책임이 부담지워질 수 있음은 별론으로 하더라도, 사후구제수단(事後救濟手段)과 양립하는 사전억제(事前抑制) 및 방지(防止)로서의 적정규제방안(適正規制方案)의 설정은 개인정보보호제도의 핵심요소인 탓이다.

요컨대, 더욱이 개인정보수집에의 '동의'는 몰각한 채 [I Agree]에의 클릭이라는 '동의' 자체만을 부각시켜 스파이웨어의 유포를 합법적으로 보는 시각은, 현대 정보사회에서 인격의 존엄을 보호하기 위해 절대적으로 필요한 최소한의 헌법적 보장장치인 정보자기결정권(情報自己決定權)[21]에 대한 불합리한 제한을 정당화하여 인터넷이용환경을 오염시킨다는 측면에

② 相對方 있는 意思表示에 관하여 第三者가 詐欺나 强拍을 行한 경우에는 相對方이 그 事實을 알았거나 알 수 있었을 경우에 限하여 그 意思表示를 取消할 수 있다.

③ 前二項의 意思表示의 取消는 善意의 第三者에게 對抗하지 못한다.

21) 독일의 연방헌법재판소가 1984년에 결정한 인구조사판결(BVerfGE 65, 1)에서 처음으로 인정

서 법제도적 보완이 시급하다. 더욱이 스파이웨어를 찾을 수 있는 검사 프로그램을 실행하거나 빼낸 개인정보가 불법으로 악용되기 전에는 개인정보 유출 여부를 알 수가 없어 정확한 실태 파악조차 힘든 형세임과 안티- 스파이웨어 프로그램 역시 새로운 스파이웨어의 활동을 억지(抑止)하지 못하는 것이 현실임을 감안한다면, 조속한 규제 입법의 마련은 더욱 요청된다.

나. 관련 판례의 개관

1) 사실관계와 판시사항

이하에서 살펴볼 판례는 AOL(America OnLine)의 자회사인 넷스케이프사의 스마트다운로드(SmartDownload) 기능이 불법적으로 exe 파일과 zip 파일의 다운로드를 감시하고 자체 네트워크를 통해 소프트웨어를 다운로드하는 소비자들의 행태를 도청한다는 주장을 기초로 기소한 Specht 사건이다.[22]

집단소송의 형태를 취하고 있는 이번 소송에서 원고측 대표로 나선 Christopher Specht는 피고의 위 소프트웨어가 인터넷을 통해 부당하게 원고의 파일전송행위에 관한 사적인 정보를 피고회사로 전송함을 이유로 제소하면서 손해배상청구를 제기하였고, 넷스케이프사는 사용허가약정 및 이용조건에 규정되어 있는 대로 중재조항에 원고가 구속됨을 주장하면서 버지니아주에서 중재를 받기로 하고 이송을 신청하였다. 뉴욕주 연방법원은 이러한 유형의 계약체결 방식은 [동의함]에 클릭할 필요 없이 당해 웹사이트에 접속하는 것만으로 계약이 성립하는 browse-wrap이라고 빗대면서 무릇 계약의 성립은 양 당사자간의 합의가 존재하여야 하는 바, 원고는 문제의 사용허가약정에 대한 인식을 전혀 하지 않고서도 소프트웨어를 다운받

된 정보자기결정권(Recht auf informationelle Selbstbestimmung)은 미국에서는 정보프라이버시(informational privacy)라 부르는 개인정보보호의 핵심요소로, 자신에 대한 정보가 언제・어떻게・어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 자율적으로 결정할 수 있는 권리를 의미한다. 이는 미국과 독일에서는 일반적 기본권으로서 프라이버시 및 일반적 인격권으로부터 도출되는 것으로 헌법이론상 인정되고 있으며, 우리나라의 경우 헌법 제17조에서 규정하고 있는 사생활의 자유에서 근원을 찾을 수 있는 자신의 정보에 대한 접근권이다.

22) *Specht v. Netscape Communications Corp. 150 F. Supp. 2d 585* (S.D.N.Y : 2001. 7. 5) : 스마트다운로드는 1998년에 11월 넷스케이프를 인수할 당시 AOL이 획득한 소프트웨어로 넷스케이프 브라우저를 다운로드하는 사람들이 일반적으로 설치하는 프로그램으로, 설치 후 사용자가 웹에서 파일을 다운로드할 때마다 자동적으로 실행된다. 이 소송에서 주장하는 바는 해당 웹사이트(http://wp.netscape.com/download/smartdownload.html)를 방문해 소프트웨어를 다운로드할 때, 스마트다운로드가 고유하게 식별할 수 있는 정보를 포착해 다시 넷스케이프로 전송한다는 것이었다. 소장(訴狀)에는 "피고들은 집단소송 원고들에게 알리지 않고 그들의 허가도 없는 상태에서 인터넷 활동을 염탐해 왔다"고 기록돼 있었으며, 이런 행위가 넷스케이프가 소비자의 다운로드 프로필을 작성할 수 있도록 허용한다고 원고측은 주장하였다.

을 수 있었고 이런 상황에서는 원고의 사용허가에 대한 동의는 찾아 볼 수 없다고 결론지었다. 그리고 다운로딩 행위의 목적은 소프트웨어를 원고의 컴퓨터로 이전시키는 것이지 그것이 계약에의 동의를 내포한다고 볼 수 없다고 판시했다. 게다가 위 소프트웨어는 무료소프트웨어여서 사용자들의 어떠한 주의를 환기시키는 내용도 웹페이지상 없었음을 들었다. 계약에의 동의를 의미하려면 '사용자가 [동의함] 버튼을 클릭하는 것과 같이 소프트웨어의 사용 이전에 분명히 동의를 나타내는 적극적인 행동을 하여야만 한다'고 못박았다. 따라서 소프트웨어의 설치 및 사용은 사용자가 사용허가계약에 구속되는 것에 대한 동의의사로 본다는 구절이 사용허가약정에 있음에도 불구하고 사용허가문구는 물론 그 안의 중재합의조항 역시 계약에 편입되어지지 않는다고 하였다. 결국 법원은 '수령 버튼을 클릭하거나 넷스케이프 스마트 다운로드 소프트웨어를 설치하고 이용함으로써 이 제품의 이용을 허락 받은 개인이나 기업은 이 계약의 당사자로서 그에 구속되는 것에 동의하는 것으로 본다'는 조항의 효력을 부정한 것이다. 왜냐하면 사용허가약정으로의 [링크]가 [다운로드] 밑에 기재되어 있어 계약조건을 확인하는 것은 내려 받기 위한 전제조건이 아니라고 보았고, 이러한 사정 하에서 캘리포니아주법에 따라 이용자의 동의 없는 계약은 집행할 수 없다고 해석하였기 때문이다. 법원은 "다운로드하는 것의 주된 목적은 계약조건에 동의하는 것이 아니라 소프트웨어를 취득하는 것인데, [동의함]이라는 버튼을 주의하지 않고 만든 잘못이 있었다"고 지적하였다.

2) 판결 의의 및 시사점

이용조건에 링크는 되어 있지만 웹사이트에 계약조건을 보여주는 것만으로는 이용자와 계약을 맺었다고 보기에는 불충분하다는 결론을 내리고 있는 Specht 판결은, 위 소프트웨어가 스파이웨어는 아닐지라도 이용자의 명시적인 동의가 없는 것에 대하여 계약의 성립을 부정하는 법원의 입장을 확인하는 것이어서 시사하는 바가 크다. 스파이웨어의 경우에 있어서도 암묵적인 동의로의 링크를 특정 소프트웨어의 취득에 대한 동의 이외에 다른 계약을 성립하는 것으로 볼 수 없음을 원용할 수 있게 하기 때문이다. 이는 전술(前述)한 바와 같이 스파이웨어의 설치와 개인정보유출에의 동의는 의사표시에 흠이 있으므로 취소할 수 있는 것으로 해석하려는 필자의 견해와 결론을 같이 한다.

다만 사건의 주요쟁점 가운데 하나인 해당 소프트웨어의 부당한 개인정보전송에 대하여 법원이 증거불충분으로 인용하지 않았음에는 아쉬움이 남는다. 스파이웨어에 있어서는 개인정보유출에 대한 명확한 입증을 담보하기 더욱 어렵다는 측면에서, 뉴욕주 연방법원이 보다 적극적인 심리를 보이지 않았음에는 미온적 평가만이 허락되어질 뿐이다. 본 판결내용에 추록된 청구취지를 통해 원고측이 피고가 전자통신프라이버시법(Electronic Communications Privacy Act)을 위반하였다고 주장하였음을 알 수 있으나, 법의 해석 이전에 재판부의 충분

한 사실관계 파악이 미치지 못하였음을 느낀다. 개인정보침해사실이 확인되지 않았지만 스마트다운로드는 스파이웨어의 기능을 내재하고 있으므로, 관련법의 적용을 배제하고 중재계약에 관한 법리만을 검토한 이 사건 판결은 문제의 소지가 있다는 관점에서는 더욱 그러하다. 그러기에 이하에서 고찰하고자 하는 내용에서처럼, 스파이웨어를 보다 효율적으로 통제하려는 입법자의 의도를 정책적 고려에 담아내는 것이 이 문제를 해결하는 데 단초가 될 것이다.

2. 법실증적 분석

가. 스파이웨어규제 입법 동향

1) 제107차 의회에 제출된 규제법률안

스파이웨어에 법적으로 대응하기 위하여 미국에서는 2001년 1월 29일 John Edwards 상원의원이 이른바 '스파이웨어 통제 및 프라이버시보호법(Spyware Control and Privacy Protection Act of 2001: 이하 SCPP법안으로 약칭함)'을 상원에 제출한 바 있으며, 이는 바로 직전 의회에도 제출했다가 회기 연도와 관련하여 처리되지 못했기에 다시 제출한 것이었다. 제107차 의회에서 법안번호 S.197로 발의된 SCPP법안의 공식제명은 'A bill to provide for the disclosure of the collection of information through computer software, and other purposes'이다.

SCPP법안에서는 스파이웨어를 기능적인 측면에서 정의하여, 인터넷 사용자가 가지는 구매 습관과 기타 관심사에 대해 은밀한 추적을 담당하는 프로그램으로 보고 있다. 존 에드워드 의원은 사생활을 좀먹는 놀라운 사례들 중의 하나로 스파이웨어를 지목한다.

SCPP법안에 따르면, 소프트웨어 공급자가 인터넷 사용자를 추적하려는 프로그램 코드를 사용할 경우, 사용자가 구입하거나 내려 받기를 할 당시에 분명한 언어로 이러한 사실을 명시하도록 요구하고 있다. 다시 말해 사용자의 동의를 얻지 않고서는 인터넷상에서의 그 어떠한 행동 정보도 수집될 수 없게 하자는 의도이다. 아울러 이처럼 수집된 자료들을 기업 활동에 이용하고자 할 경우, 사용자들에게 구체적으로 어떤 정보가 선별되어 결합되는지 고지해야 하며, 이들 정보에 오류가 발생할 때의 교정하는 방법이나 해커 등으로부터의 비합법적 접근으로부터 정보를 보호하는 방법 등도 기반구조로 의무 제공해야 할 것을 요구한다.

2회독 후 통상과학운송위원회(Committee on Commerce, Science, and Transportation)에 회부된 SCPP법안에 대하여는 그 이후 별다른 후속조치가 취해지지 않은 상태이어서, 성안되지 못한 채 현재 여전히 위원회에 계류되어 있다.

2) 제108차 의회에 제출된 규제법률안

스파이웨어로부터 개인의 사생활을 보호할 수 있도록 의회에 제출된 SCPP법안이 성안되지 못한 데는 나름대로의 이유가 있겠지만, 광고회사를 포함한 업계의 반발과 회유가 작용하였을 것이라는 추측이 가능하다. 그러나 바이러스와 같이 사용자의 동의 없이 실행되는 악성 소프트웨어와는 구별된다고 하지만, 인터넷 활용 상황을 감시할 수 있게 할 뿐 아니라 개인식별정보의 수집을 가능하게 하는 스파이웨어에 대하여 법적 규제의 도입을 역설하는 주장은 저간 제기되어 오고 있다. 같은 맥락에서 미국의 입법적 조치가 현실화되고 있는 바, 스파이웨어를 통하여 개인정보가 수집되는 것으로부터 인터넷 이용자를 보호하려는 취지에서 제안된 프라이버시침해대응법(Safeguard Against Privacy Invasions Act: 이하 SPI법안으로 약칭함)이 지난 7월 25일 법률안으로 발의되었다. Mary Bono 하원의원에 의해 입안된 이 법안은 제108차 의회에서 법안번호 H.R.2929로 제출되었으며, 공식제명은 'A bill to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes'이다. SPI법안과 관련하여 법안의 제안자인 Bono 의원은 "소비자들이 그 사실을 인지하지 못한 채 때로는 패스워드에서부터 신용카드번호까지의 모든 것들이 스파이웨어를 이용하는 기업체들에 의해서 관찰되고 있다. SPI법안의 제정으로 그러한 프라이버시침해를 예방할 수 있을 것이다. 이 법안을 통해 이용자들은 스파이웨어의 설치 및 작동 조건에 명시적으로 동의할 수 있게 될 것이다"고 밝혔다.[23] SPI법안은 법안발의당일 의회 에너지 및 통상위원회(House Committee on Energy and Commerce)에 회부되었고, 지난 8월 8일부로 통상무역소비자보호분과위원회(Subcommittee on Commerce, Trade and Consumer Protection)에 넘겨진 상태이다.

표제·스파이웨어 프로그램의 전송 규제권·법 집행·정의·시행령 등의 총 5개 조항으로 구성된 SPI법안은, 스파이웨어가 사용자의 컴퓨터에 장착되기 전에 이러한 응용기술과 정보수집의 사실을 인식할 수 있도록 운용자가 조처하게끔 하고 있다. 또한 그러한 기술을 이용하는 기업체에게 스파이웨어 탑재의 의사를 이용자에게 알리도록 함과 아울러 설치 이전에 승인을 얻도록 요구하고 있다. 더불어 이용자에게 스파이웨어의 존재와 그 의도된 작용을 뚜렷하게 알려주는 사용허가약정을 제공하도록 하고 있는데, 여기에는 업체의 상호명 및 주소 그리고 유효한 회신용 전자우편주소 등을 밝히도록 하고 있다. 그리고 SPI법안에서는 스파이웨어 프로그램을 전송하는 것에 대하여 컴퓨터 이용자가 적극적인 요구나 명확하고 확실한 응답을 통해 명시적으로 동의하지 않는다면 인터넷에 의한 스파이웨어 프로그램의 전송을 금지

23) CNET News, *Lawmaker wants limits to spyware*, 2003. 7. 29.

할 수 있도록 함과 동시에, 개인식별정보를 수집하려는 데 스파이웨어 프로그램을 사용하려는 것이 고지되어지지 않는다면 이러한 프로그램 사용에도 제재조치를 취할 수 있도록 연방거래위원회(FTC)에 일정한 규제 권한을 부여하고 있다.[24] 또한 SPI법안은 동의 없이 개인식별정보를 수집하거나 고의로 법규를 위반한 자를 형사처벌할 수 있도록 규정하고 있다.

나. 규제 입법의 정책 시사점

스파이웨어를 발견·제거하는 안티- 스파이웨어 제품들이 지금껏 개발되어 왔지만, 프로그램에 들어 있는 파일을 임의로 삭제할 경우 저작권 문제의 소지가 있다. 더욱이 사용자의 개별적 대응이 지니는 한계를 고려할 때, 법정책적 판단을 정리해야 할 필요성을 느낀다. 이러한 시점에서 발의된 SPI법안의 내용은 우리에게 정책적 함의를 제공해준다. 우선 스파이웨어에 대한 규제의 정당성에 있어 시사점을 준다. 즉 정보주체인 이용자의 동의를 함몰시킨 채 개인정보를 유출하는 프로그램을 설치하게 하는 것이 부당하다는 점이다. 이는 앞서 고찰한 바 있는 의사표시의 흠결 내지 하자와도 관련성을 지닌다.

무릇 개인정보보호에 관한 국제적 기준이 되는 원칙 가운데 대표적인 것으로 경제협력개발기구(OECD)이사회가 1980년 9월 23일에 채택한 「사생활보호 및 개인정보의 국경 없는 흐름에 관한 지침(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」을 들 수 있다. 이는 공적·사적 부문을 초월한 정보주체로서의 개인과 관련된 모든 정보를 그 적용대상으로 하면서 프라이버시 보호뿐 아니라 정보의 자유로운 흐름도 막지 않을 목적으로 규정한 권고안(勸告案)이다. 그 주요 내용은 (1) 정보의 수집에 있어, ① 수집제한의 원칙(Collection Limitation Principle: 적법하고 공정한 수단에 의해 정보주체의 인식·동의하에서의 데이터 수집), ② 목적명확화의 원칙(Purpose Specification Principle: 목적 범위 내에서의 데이터 수집과 이용), (2) 정보의 이용에 있어, ③ 정보내용정확성의 원칙(Data Quality Principle: 이용목적에 따라 정확·안전한 최신데이터의 유지), ④ 이용제한의 원칙(Use Limitation Principle: 데이터의 다른 목적으로의 이용 금지), (3) 정보의 관리에 있어, ⑤ 안전보호의 원칙(Security Safeguards Principle: 데이터의 분실·부당한 접근 및 수정·부당한 열람에의 안전조치), ⑥ 공개의 원칙(Openness Principle: 시스템 및 개인정보에 관한 개발·운용·정책 등에 관한 주지), ⑦ 개인참가의 원칙(Individual Participation Principle: 정보주체의 데이터에의 접근·이의신청, 데이터의 소거·수정 등의

24) 이와 관련하여, FTC는 파일교환(P2P) 소프트웨어를 사용할 때 개인정보가 담긴 파일들을 공유하지 않도록 조심할 것과 인터넷 사용습관을 기록하는 스파이웨어 설치에 유의할 것 등의 내용이 담긴 소비자 보호지침을 함께 발표한 바 있다; CNET News, *FTC warns about file trading, spyware*, 2003. 7. 30.

권리), ⑧ 책임의 원칙(Accountability Principle: 상기의 제원칙을 실시하기 위한 데이터관리자의 책임)과 같은 8대 원칙이 거론되고 있다.[25] 이와 같이 개인정보보호에 관한 국제적 기준은 정보의 수집에 있어 적법·공정한 수단에 의한 것과 정보주체의 인식·동의하에 획득할 것을 주요 원칙으로 삼고 있음에도, 스파이웨어 프로그램의 속성은 이를 묵살하고 있다. 또한 스파이웨어 콤포넌트에서는 해당 정보에 대한 정보주체의 접근이나 이의신청 등이 원천적으로 봉쇄되어 있기 때문에 정보주체의 능동적인 정보자기결정권의 행사를 기대할 수 없다는 점에서도 그 위법성을 재확인할 수 있다.

스파이웨어가 내포하는 심각성이 이와 같다면, 그 외연에의 규제는 어떠해야 할 것인가? SPI법안을 기준 삼아 생각건대, 은밀한 합법화를 금지하고 구체적인 적법요건을 법제화하는 동시에 개인정보의 활용에 따른 책임을 확연히 설정함이 바람직할 것으로 판단된다. 현행 정보통신망이용촉진및정보보호등에관한법률이 제50조의5에서 '정보통신서비스제공자는 영리목적의 광고성 정보가 보이도록 하는 프로그램을 이용자의 컴퓨터 그 밖에 대통령령이 정하는 정보처리장치에 설치하고자 할 때에 이용자의 동의를 얻어야 한다. 이 경우 해당 프로그램의 용도와 삭제할 수 있는 방법을 고지하여야 한다'고 규정하고 있으며, 같은 법 제67조 제1항 15의5호에서는 '제50조의5의 규정을 위반하여 이용자의 동의를 얻지 아니하고 프로그램을 설치한 자는 1천만원 이하의 과태료에 처한다'라고 명시하고 있다. 그런데 문리해석상 본조가 스파이웨어를 적용대상으로 한다고는 보이지 않으며, 이를 규율범위에 포섭함에 있어서는 동의 방법과 고지의무 사항을 구체화하고 같은 법 제67조 소정의 행정벌(行政罰)을 적정화하는 수고로움을 감내해야 하리라 사료된다. SPI법안 이전에도 사생활 보호를 위해 스파이웨어를 통제하는 SCPP법안이 상원에 제출된 전례가 있음이, 전자감시사회의 어두운 먹구름이 쉽사리 걷히지는 않을 것임과 나날이 진보되어 가고 있는 기술에 가치중립적인 규범 정립의 노정이 순탄치만은 않을 것임을 예고하는 듯한 까닭에서 이다.

3. 법정책적 제언

이미 지적한 바대로 법제도적으로 스파이웨어의 은밀한 합법화를 금지하고 이용자에게 명백하게 밝히는 구체적 합법요건을 규정해야 할 것이며, 개인정보의 활용에 따른 책임과 제반 보장도 강구해야할 것을 명문화해야 할 것이다. 또한 정보기술개발 측면에서, 스파이웨어에 대한 방제 연구 및 현황 추적에 대한 국내 기술개발의 확충과 정보기술연구팀의 구성 및 적

25) 김철완·이민영, 『인터넷 개인정보보호에 관한 법제도 연구』, 정책연구 00-10, 정보통신정책연구원, 2000, 52~53쪽.

극적인 지원도 국가적으로 요청된다고 본다. 이하에서는 입법정책의 방향만을 다루도록 한다.

가. 규제조항의 신설

법체계를 보면, 우리나라의 경우는 미국과 달리 스파이웨어의 규제에 대하여 개별입법을 제정할 이유는 없다. 특히 스파이웨어 프로그램이 '전기통신기본법 제2조 제2호의 규정에 의한 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제'인 정보통신망을 통해 '전기통신사업법 제2조 제1항 제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자'인 정보통신서비스 제공자에 의하여 유포되는 것이라는 점에서 정보통신망이용촉진및정보보호등에관한법률에 포섭될 수 있다. 따라서 정보통신망이용촉진및정보보호등에관한법률에 관련 규제조항을 신설하고 이에 대한 집행력을 담보할 수 있도록 편제를 강화하는 것이 요구된다.

현실적으로 입법가능한 방법으로는,[26] 현행 정보통신망이용촉진및정보보호등에관한법률에 제50조의6을 신설하면서 제명을 '스파이웨어 프로그램의 설치 제한'으로 하고 "① 정보통신서비스제공자는 개인정보를 무단으로 수집하는 스파이웨어 프로그램을 이용자의 컴퓨터 그 밖에 대통령령이 정하는 정보처리장치에 설치하고자 할 때에는 이용자의 명시적인 동의를 얻어야 한다. 이 경우 개인정보의 유출 가능성 및 해당 프로그램의 용도와 삭제할 수 있는 방법 그리고 기타 대통령령으로 정하는 사항에 대하여 고지하여야 한다"라는 내용을 담을 수 있도록 규정함이 고려되어져야 할 것이다. 그리고 스파이웨어 프로그램에 대한 규제권한을 보유한 기관에 의하여 적절한 감독과 규제가 이루어질 수 있도록 명시화하는 것이 요구되는데,[27] 예컨대 한국정보보호진흥원을 지목한다면 "② 전항의 내용을 위반한 프로그램의 설치에 대하여 이 법 제52조 소정의 한국정보보호진흥원은 규제 및 감독업무에 필요한 조치를 하여야 한다. 다만 규제감독권한의 구체적 내용과 수행업무에 대하여는 대통령령에서 정한다"라고 구성하는 방안이 검토되어질 수 있을 것이다. 신설조항이 위임하고 있는 사항에 대하여 대통령령에서는 스파이웨어의 정의와 설치 원칙 및 규제감독기관의 권한과 업무수행방법 등을 규정하여야 할 것이다. 다만 이러한 법제개편은 규제감독기관의 실효성 있는 권한행사를 전제로 하여 이루어져야 할 것임이 누락되어서는 아니될 것이다.

---

26) 정보통신망이용촉진및정보보호등에관한법률을 포함한 현행 개인정보보호법제가 안고 있는 문제점은 별론으로 제외하고, 현행법에서의 스파이웨어 규제를 위한 검토만을 고려하기로 한다.

27) 물론 여기서 개인정보보호에 관한 독립감독기구의 신설을 역설할 여지가 있으나, 본고의 고찰 범위를 넘어선 까닭에 논외(論外)로 한다. 다만 그 필요성에 대해 필자 역시 공감함을 표한다.

나. 제재규정의 도입

스파이웨어의 규제를 위하여 현행 정보통신망이용촉진및정보보호등에관한법률에 제50조의6을 신설한다면, 적절한 규제의 종국적 담보수단으로서 벌금(罰金)과 같은 행정형벌(行政刑罰)과 과태료(過怠料)와 같은 행정질서벌(行政秩序罰)의 도입이 요구되어진다. 이러한 행정벌의 편성으로 의무위반에 대한 제재를 가함과 동시에 심리적 압박에 의해 간접적으로 의무이행을 확보하는 효과를 볼 수 있기 때문이다.

이에 따라 벌칙규정인 정보통신망이용촉진및정보보호등에관한법률 제65조의2에 제4호를 신설하여 '제50조의6의 규정을 위반하여 이용자의 명시적인 동의 없이 스파이웨어 프로그램을 설치하거나 개인정보를 수집하는 자'에 대해 1천만원 이하의 벌금에 처할 수 있도록 하는 것을 상정할 수 있다. 다음으로 과태료부과조항인 정보통신망이용촉진및정보보호등에관한법률 제67조에 15의6호를 신설하여 '제50조의6의 규정을 위반하여 고지의무를 해태하면서 스파이웨어 프로그램을 설치하는 자'에 대하여 1천만원 이하의 과태료에 처할 수 있도록 하는 방안을 모색할 수 있을 것이다. 다만 상술(上述)하였듯이 규제내용의 제재수단으로서 행정벌의 도입에 있어서는 그 강도와 정도의 적정화가 요구되어지는 바, 벌칙에 있어 벌금의 상향조정이라든가 과태료 부과에 있어 이행강제금(履行强制金)을 병과(竝科)할 수 있는 등의 내용에 대하여 충분한 숙려(熟慮)가 선행되어야 함은 물론이다. 무엇보다 이러한 논의의 과정에는 행정제재를 포함한 규제조항의 신설에 있어 공청회를 통한 의견수렴 등 행정절차의 준수로 이루어지는 형식적 타당성과 실질적 정당성의 기반을 확보하는 것이 중요함은 분명하다.

Ⅳ. 맺음말

과거에는 상상도 하지 못했을 영역의 정보에 대한 수집과 분석이 컴퓨터처리의 발전으로 가능해지고 있다. 상이한 데이터베이스로부터 정보를 조합하는 것이 새로운 유형의 감시와 통제를 점진적으로 양산하고 있는 것이다. 자신의 활동이 관찰되어진다는 개인의 인식이 물리적 폭력에 의하지 않고서도 행동통제에 영향을 미치는 데 충분한 감옥으로서 Bentham이 고안한 Panopticon의 악몽을 여기서 발견할 수 있다. Foucault가 구상한 사회적 원형감옥화는 현재의 기술진화로 인해 이제 무서울 정도로 실현가능해졌다.[28] 이것이 다름 아닌 전자감시사회(電子監視社會)의 출현이리라. 스파이웨어가 프로그램 실행파일을 숨기는 기능을 갖고 있어 이용자가 설치 여부를 알 수 없다는 점은 Panopticon에서 이루어지는 감시로부터

28) J. M. Balkin, *What is a postmodern constitutionalism?*, 90 Mich. L. Rev. 1966, 1987(1992).

우리 사회가 직면한 암울한 모습을 상징하고 있는 듯하기에, 전자감시사회의 감시수단으로서 스파이웨어를 받아들이는 데에는 무리가 없을 것이다. 그 논거로 개인정보의 유출로 침해가 발생하면 불법행위가 성립되므로 손해배상을 청구할 수 있지만, 이용자가 인식하지 못하는 사이에 스파이웨어가 설치된다는 점과 빼낸 개인정보가 불법으로 악용되기 전에는 개인정보 유출 여부를 알 수가 없다는 점에서 행위의 존재・손해의 발생・인과관계 등의 입증이 용이하지 못하다는 난점을 안고 있다는 것을 얘기할 수 있다. 더욱이 정보자기결정권이 통제되는 여건에서 부당한 프로그램의 유포와 불법적인 프라이버시 침해가 이루어지는 상황국면에 놓여 있기에, 개인정보의 상업적 거래로 인해 발생할 수 있는 부차적인 사생활 침해는 불법행위로 인한 손해배상청구라는 민사적 구제수단에만 의존할 사안이 아니라 할 것이기 때문이다.

권리로서의 프라이버시는 단순히 소극적인 것이 아니라 정보자기결정권이라는 적극적인 접근권과 통제권을 내용으로 하는 것으로 설시하는 우리 법원의 태도처럼,[29] 오늘날 프라이버시권은 단순히 '혼자 있을 권리'가 아니라 자신의 신상정보를 통제할 수 있는 권리이자 개인의 참여를 보장하고 개인의 체계적 역감시를 요청하는 적극적인 권리로 재해석되고 있다. 하지만 보호되어야 할 사생활의 비밀 가운데 중요한 요소로 개인정보가 자리 잡고 있음에도 불구하고, 기술적 추적으로 정보자기결정권이 침해되고 있는 실정인 것이다. 이와 같은 상황에서는 개인정보처리의 남용을 통해 개인을 감시하고 통제하려는 위험을 차단시키는 역감시의 기능을 제대로 발휘할 수 없게 된다. 이러한 형국에서 정보의 수집과 접근에 대한 제한을 가하는 내용으로 감시와 역감시의 균형을 설정하는 데 역점을 두어야 할 필요성이 대두되며, 그와 같은 역할을 수행하는 기제로 법제도의 정비가 작용한다. 그러므로 감시에 대한 규제와 역감시의 조성을 사회적 합의에 담아내는 그릇으로서 법이 기능할 수 있어야만, 정보자기결정권의 정당한 행사에 의하여 전자감시에 대한 효율적 통제가 가능하다.

자본주의의 정보적 확장이라는 형태로 진행되는 현재의 정보화는 기업으로 하여금 발달된 정보기술을 이용하여 개인에 대한 광범위한 감시를 일상적으로 행하도록 한다. 엿보기와 엿듣기가 대중화되고 있는 전자감시사회에서 개인은 오히려 발달된 정보기술을 통해 역감시의 요청에 실시간으로 참여할 수 있다. 다만 그러한 역감시를 가능하게 하는 데에는 법제도적 토대의 마련이 요구된다. 이러한 관점에서 스파이웨어 프로그램의 전자감시에 대한 역감시는 정합(整合)된 법리에 의한 정치(精緻)된 규제를 통해서만이 정보주체로서의 개인에게 수단적 통제권을 허여(許與)할 수 있으리라 생각하며, 전자감시적 현황이 역감시를 통한 변증법적 합치로 발돋움하여 Panopticon에의 우려가 한낱 기우(杞憂)가 되길 바라면서 본고를 맺는다.

29) 대법원 1998. 7. 24. 선고, 96다42789 판결 [공 1998. 9. 1, (65), 2200] 참조.

참 고 문 헌

[1] 김명주, 스파이웨어, 「합법적인 악성 소프트웨어인가?」, 『인터넷법률』 제9호, 법무부, 2001.

[2] 김연수, 『개인정보보호』, 사이버출판사, 2001.

[3] 김철완・이민영 外, 『건전한 정보통신 윤리확립과 개인정보 보호대책 방안 연구』, 연구보고 01-03, 정보통신정책연구원, 2001.

[4] 미셸 푸코 著・오생근 譯, 『감시와 처벌 : 감옥의 탄생』, 나남출판, 1994.

[5] CNET News, *Lawmaker wants limits to spyware*, 2003. 7. 29.

[6] James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. Cin. L. Rev. 177(1997).

[7] J. M. Balkin, *What is a postmodern constitutionalism?*, 90 Mich. L. Rev. 1966 (1992).

[8] http://www.moleg.go.kr(법제처 종합법령정보)

[9] http://thomas.loc.gov(미국 의회 입법정보검색)