MINBYUN-Lawyers for a Democratic Society
민주사회를 위한 변호사 모임

서울 서초구 서초동 1555-3 신정빌딩 5층
전화 02) 522-7284, 팩스 02)522-7285
웹페이지 http://minbyun.jinbo.net
전자우편 m321@chol.com

문서번호 : 10-01-사무-07
수 신 : 국회 법제사법위원회
발 신 : 민주사회를 위한 변호사모임 (담당 : 류제성 변호사)
제 목 : 민변 법률의견서
전송일자 : 2010. 1. 22.(금)
전송매수 : 7 매

“통신비밀보호법 일부개정법률안(의안번호 제6976호)”에 관한 민변 의견서

1. 귀 위원회의 무궁한 발전을 기원합니다.

2. 민변에서는 귀 위원회 소관법률인 “통신비밀보호법 일부개정법률안(의안번호 제6976호)”에 관하여 붙임과 같이 의견서를 제출하니 법안심사에 적극 반영하여 주시기 바랍니다.

3. 감사합니다.

붙임. “통신비밀보호법 일부개정법률안(의안번호 제6976호)”에 관한 민변 의견서

2010년 1월 22일

민주사회를 위한 변호사 모임

회 장 백 승 헌

붙임. “통신비밀보호법 일부개정법률안(의안번호 제6976호)”에 관한 민변 의견서

1. 주요 개정내용

(1) 패킷감청의 허가서 내용 구체화(안 제6조제6항 후단 신설).

인터넷 회선에 대한 감청의 허가서에는 전자우편의 내용, 접속한 인터넷홈페이지의 주소, 인터넷홈페이지의 게시판 또는 대화방 등에서 게시한 의견, 검색한 정보목록 등 대통령령으로 정하는 바에 따라 그 대상과 범위 등을 구체적으로 특정하여 기재하도록 함

(2) 통신제한조치 기간 및 연장횟수 제한(안 제6조제7항 및 제7조제2항).

현행 2개월의 통신제한조치 기간을 1개월로 단축하고 1월의 범위에서 2차례에 한해 연장할 수 있도록 함.

(3) 통신제한조치로 알게 된 내용의 열람 또는 복사(안 제9조의2제7항 신설).

우편물 검열의 경우에는 그 대상자가, 감청의 경우에는 그 대상이 된 전기통신의 가입자가 통신제한조치를 집행한 사실을 알게 된 경우에는 대통령령으로 정하는 바에 따라 검사·사법경찰관 또는 정보수사기관의 장에게 해당 통신제한조치로 알게 된 내용의 열람 또는 복사를 요청할 수 있도록 함

(4) 통신제한조치 허가범위 외의 내용이나 불필요한 내용의 폐기의무(안 제12조제2항·제3항 및 제17조제2항제4호 신설).

검사·사법경찰관 또는 정보수사기관의 장이 통신제한조치의 집행으로 인하여 취득된 우편물 또는 그 내용과 전기통신의 내용 중 통신제한조치허가서 또는 긴급감청서에 기재되지 아니한 내용 등이 포함되어 있거나 범죄수사·소추의 목적 등에 더 이상 필요하지 않게 된 경우에는 지체 없이 이를 폐기하도록 하고 그 경위 및 결과의 요지를 조서로 작성하도록 하며, 이를 위반한 경우 3년 이하의 징역 또는 1천만원 이하의 벌금에 처함

2. 검토의견

(1) 패킷감청의 허가서 내용 구체화(안 제6조제6항 후단 신설).

인터넷을 통한 정보전달은 각각의 파일을 패킷(packet)이라는 단위로 잘게 쪼개어 송신한 뒤 이를 받아보는 컴퓨터가 해당 패킷을 재구성해 화면에 다시 구현하는 형태로 이루어진다. 패킷감청이란 이용자가 인터넷을 이용하는 과정에서 인터넷 회선을 통해 전기신호 형태로 흐르는 패킷을 제3자가 실시간으로 가로챔으로써 같은 내용을 들여다보는 것이다. 따라서 패킷 감청을 이용하면 대상자가 인터넷을 통해 접속한 사이트 주소와 접속시간, 대상자가 입력하는 검색어, 전송하거나 수신한 게시물이나 파일의 내용을 모두 볼 수 있다. 이메일과 메신저의 발송 및 수신내역과 그 내용 등 통신내용 일체도 마찬가지로 볼 수 있다.

패킷의 내용을 검사하는 기술은 인터넷 초창기서부터 발달해왔다. 전통적인 패킷 검사들은 패킷 라우팅을 최적화하거나, 네트워크 남용을 탐지하거나, 통계 분석을 하는 등의 이유에서 이루어져 왔다. 이러한 패킷 검사들은 검사자에게 인터넷 트래픽에 대한 기초적인 정보를 제공하지만, 이용자의 이메일이나 웹서핑 내용을 보여주진 않는다. 반면 최근의 패킷 감청은 이용자가 보내고 받는 모든 비암호화된 인터넷 트래픽의 '내용'에 접근할 수 있도록 한다. 인터넷 초창기에는 컴퓨터 속도와 자원의 한계 때문에 규모가 큰 패킷 감청은 효과적으로 이루어질 수 없었다. 최근의 기술적 진보로 인하여 ISP와 정보수사기관들이 큰 규모로 패킷 감청을 하는 것이 가능해진 것이다.[1)]

패킷 감청이 과연 현행 법률은 물론 기술적인 측면에서 허용될 수 있는지를 두고 최근 전세계적인 논쟁이 일고 있다. 특히 미국과 영국 등 다른 나라에서는 광고서비스업체들이 패킷 감청을 이용하여 이용자의 통신 내용을 실시간으로 보고 그에 맞춘 광고를 내보내는 소위 '관심기반 광고' 방법을 도입하는 것을 두고 정부와 의회에서 토론이 계속되고 있다.[2)]

---

1) EPIC의 다음 자료 참고. http://epic.org/privacy/dpi/

2) 영국에서는 2008년 BT가 광고서비스를 위하여 폼사의 패킷감청기술을 도입한 문제에 대하여 관련 업계, 정부와 시민단체 간에 많은 논쟁이 벌어졌으며, 이 문제로 EU에서 조사를 하고 있다. The Register. 2008.2.29. "How Phorm plans to tap your internet connection"; The NewYork Times. 2009.7.6. "BT Backs Off From Tracking Internet Customers"; The Guardian. 2009.10.30. "EU goes to next stage in privacy action against Britain" 참조, 미국에서는 역시 광고서비스를 위하여 초고속 인터넷서비스업체인 차터 커뮤니케이션에서 네뷰애드사의 패킷감청기술을 도입한 문제에 대하여, 2008년 7월 17일 하원 에너지 및 통상위원회 산하 통신 및 인터넷 소위원회에서 청문회가 개최되었다. http://energycommerce.house.gov/index.php?Itemid=58&catid=32&id=1400&layout=default&option=com_

한국에서는 남북공동선언실천연대 사건에 대한 재판과정에서 국가정보원이 패킷 감청을 실시한 사실이 드러났고, 2009년 8월 31일 인권단체들이 이를 비판하는 기자회견을 개최함으로써 패킷 감청 문제가 처음 알려졌다.[3] 그리고 이른 바 범민련 사건의 경우에는 검찰의 공소가 제기되기 6년 전인 2003년 7월 30일부터 2009년 5월 7일 구속시까지 단 하루도 빼지 않고 국가정보원이 피고인들의 모든 통신내용을 감청하였는바, 검찰이 제출한 증거에 의하여도 국정원은 적어도 2004월 7월 30일 이후부터 범민련 남측본부 사무실 및 피고인 이경원의 자택에서 이용한 인터넷 통신내용을 패킷감청한 것으로 드러났다. 2009년 정기국회에서는 관련 법률의 보완이 이루어져야 한다는 지적이 여럿 이어졌다.[4]

패킷감청의 가장 큰 문제점은 감청 대상을 특정화하기 쉽지 않다는 점이다. 첫째, 보통의 가정이나 직장에서는 공유기 등을 통해 다수의 PC와 다수인이 해당 네트워크 서비스를 공동이용한다. 대상자의 PC를 임시적으로 다른 이가 사용할 수도 있다. 따라서 현재의 패킷 감청은 감청 대상자가 아닌 타인의 인터넷 통신 내용을 감청하게 되는 경우가 다수 있을 것이다. 그러나 외부에서 감청을 집행하는 입장에서는 지금 전송되는 패킷이 감청 대상자의 행위에 의해 송수신되는 것인지 알 수 없다. 따라서 감청 대상자를 특정할 수 없는 패킷 감청은 각 피의자별로 감청이 이루어지도록 한 현행 「통신비밀보호법」에 위배되고(동법 제6조 제1항), 법정증거로서의 효력도 없다.

둘째, 패킷 감청의 경우 특정 이메일이나 메신저에 대한 감청과 달리 서버로부터 대상자에게 전달되는 모든 통신내용을 대상으로 한다. 이 가운데에는 공개된 통신내용도 있을 수 있지만 비공개 통신내용도 있을 수 있는데, 비공개 통신내용은 단

---

content&view=article&date=2009-11-01. 캐나다 프라이버시위원회에서는 패킷 감청에 대한 특집 사이트를 운영하고 있다. http://dpi.priv.gc.ca/.

3) 아이뉴스24. 2009.8.31. “국정원 인터넷회선 패킷 감청 의혹제기”; 오마이뉴스. 2009.8.31. “국정원, 인터넷 사용내역도 엿봤다”; 한겨레신문. 2009.8.31. “국정원, 우리집 인터넷 통째로 엿봤다”; 서울신문. 2009.9.1. “국정원, 인터넷회선 통째 감청 의혹” 등.

4) 2009. 10. 8. 국회 법제사법위원회의 법제처 국정감사에서는 패킷감청의 범위가 너무 광범위하여 일반영장금지 원칙에 어긋나고 통신의 자유와 사생활에 대한 심각한 침해가 된다는 박영선의원의 문제제기가 이루어졌고, 이에 대하여 법제처장은 문제를 검토하겠다고 답변하였음. 또 10. 9. 서울고등법원 국정감사와 10. 20. 대법원 국정감사에서도 패킷감청이 사무실이나 아파트 등에서 같이 회선을 쓰는 다른 이들의 모든 개인정보까지 열어볼 수가 있기 때문에 법원의 영장발부가 특별히 신중해야 한다는 박영선의원의 지적이 있었고, 이에 대하여 서울고등법원장과 대법원 행정처장은 패킷감청 문제를 제도적, 기술적으로 검토하겠다고 답변하였음.

지 대상자가 이용하였다는 이유만으로 정보수사기관에게 제공된다. 이 과정에서 이용자의 비밀번호 등이 제공될 가능성도 있는데, 이는 감청을 집행하는 과정에서 비밀번호가 누설되어서는 안된다는 「통신비밀보호법」의 취지에 위배된다(동법 제9조 제4호). 결국 **패킷감청은 감청대상자와 무관한 제3자를 감청하는 결과를 낳을 수 있으며, 수사목적과 무관한 통신내용까지 무제한적으로 포괄감청한다는 것이 가장 큰 문제점이다.**[5]

우리 「통신비밀보호법」 제3조 2항은 전기통신의 감청이 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다는 점을 명시하고 있다. 동법 제5조 제1항에서도 감청은 대상 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가하도록 명시하였다. **패킷 감청은 그 범위가 너무 광범위하여 대상자와 대상 통신내용을 특정할 수 없다는 점에서 우리 「통신비밀보호법」이 허용하는 감청의 범위를 벗어난 위법한 감청이다.**[6]

더구나 패킷이란 목적을 가지고 이동하는 통신 과정상의 자료로서 수사에 필요한 자료는 해당 패킷이 목적지에 도달한 후 기존의 이메일 전달(forwarding) 방식의 감청이나 압수·수색으로도 충분히 입수가능하다. 여러모로 통신비밀보호법에 규정된 감청 방식으로 부적합한 패킷감청이 굳이 인정될 필요가 없는 것이다. 결론적으로 통신 감청이 최소한으로, 보충적으로 이루어져야 한다는 「통신비밀보호법」의 제정 취지대로라면 현재와 같은 형태의 패킷감청은 금지되어야 마땅하다.

개정안은 패킷감청의 요건을 엄격하게 한다는 명분을 내세우고 있지만 현행법에 의하여 금지되는 패킷감청을 허용하고 이를 더욱 용이하게 하는 부작용이 훨씬 크다. 기술적으로도 패킷 상태로 전송되는 데이터 가운데 전자우편 내용 또는 게시판에 올린 의견 등만 따로 걸러 가로채는 기술은 아직 개발되지 않았다는 게 전문가들의 설명이다. 이는 지난 10월29일 서울 내곡동 국가정보원에서 열린 국회 정보위원회의 비공개 국정감사에서도 확인됐다. 이 자리에서 국정원 쪽은 “판사들이 (패킷 감

5) 오길영. 2009. 인터넷 감청과 DPI(Deep Packet Inspection). 민주법학 41호(2009. 11). 391-426쪽.

6) 박영선. 2009. 법원, 인터넷 회선 감청(패킷감청) 허가에 신중해야. 박영선 의원 보도자료(2009.10.9).

청과 관련해) 앞으로 압수수색 영장을 신경 쓰겠다고 했지만 기술적으로 불가능하다"며 "인터넷 패킷 감청은 특정 IP 주소만 적어내면 웹서핑, 전자우편 등이 한꺼번에 감청되기 때문에 법으로 제한하기에 기술적으로 힘들어 보인다"고 설명한 것으로 알려졌다.[7] **따라서 패킷감청을 엄격히 제한한다는 명분하에 오히려 패킷감청에 대하여 법적으로 면죄부만 마련해 줄 가능성이 큰 개정안에 반대한다.**

지금 필요한 것은 패킷감청의 가능성을 열어주는 것이 아니라 차단하는 것이다. 이를 위하여 현행 통신비밀보호법의 통신제한조치에 대한 허가절차를 세밀하게 규정하여야 한다. 즉 통신제한조치 허가신청서를 기재내용을 상세화하고, 법원이 통신제한조치의 범위를 구체화하여 허가하도록 하는 절차를 마련하여야 한다. 참고로 일본의 '범죄수사를 위한 통신감청에 관한 법률' 제3조는 "판사가 발부하는 감청영장에 의하여 전화번호 기타 發信元 또는 발신처를 식별하기 위한 번호 또는 부호(이하 "전화번호 등"이라 한다)에 의하여 특정된 통신의 수단(이하 "통신수단"이라 한다)으로서 피의자가 통신사업자 등과 맺은 계약에 의거하여 사용하고 있는 것(범인에 의한 범죄관련통신에 사용된다고 의심할 수 없다고 인정되는 것을 제외한다) 또는 범인에 의한 범죄관련통신에 사용된다고 의심할만한 것에 대하여 이를 사용하여 행하여진 범죄관련통신의 감청을 할 수 있다."(밑줄은 인용자)고 규정하고 있다. 이것은 패킷감청의 금지를 전제로 한 규정이라고 볼 수 있다. 우리도 전기통신에 대한 통신제한조치의 허가는 해당 피의자가 송신·수신하는 전기통신만을 대상으로 하도록 하고, 해당 전기통신이 허가를 받은 범죄 수사와 관련이 없거나 해당 피의자가 송신·수신하는 것이 아닌 경우에는 해당 전기통신에 대한 감청을 즉시 중단하도록 입법화할 필요가 있다.

(2) 통신제한조치 기간 및 연장횟수 제한(안 제6조제7항 및 제7조제2항).

현행법은 통신제한조치의 기간을 2월로 규정하고 2월의 범위안에서 그 연장을 청구할 수 있도록 하고 있으나 그 회수나 총 기간에 대해서는 아무런 규정이 없다. 통신제한조치 기간 2월은 30일로 정한 미국에 비해 과도하게 긴 기간이다.[8] 일본이 그 기간을 10일로 제한하고 있는 것에 비추어 본다면, 그리고 우리의 경우 통신제한조치를 할 수 있는 범죄

7) 「'패킷감청' 제한법으로 면죄부 주기?」 한겨레21 790호

8) 박경신 「미국의 통신비밀보호법(ECPA) 및 범죄수사통신지원법(CALEA)과 우리나라의 통신비밀보호법 및 18대 국회 개정안의 비교검토」 안암법학 제29호, 2009년 5월, 119-157쪽

의 수와 종류가 일본보다 훨씬 광범위하다는 점을 고려한다면, 이는 심각한 문제이다. 그리고 통신제한조치를 연장할 경우 그 회수에 대한 제한이 없어 법문의 문리적 해석에 의할 경우 연장청구를 무한히 반복할 수 있어 이는 명백한 입법적 불비이자 위헌적 규정이라 할 수 있다.[9] 범민련 사건에서 검사가 동 조항에 근거하여 총 14회에 걸쳐 통신제한조치 기간을 연장하여 이를 통해 취득한 내용을 증거로 제출하자 피고인과 변호인들은 동 조항이 적법절차, 영장주의, 과잉금지 원칙을 위반하여 사생활의 비밀과 통신의 자유를 부당하게 침해하여 위헌이라는 이유로 위헌제청을 신청하였다. 이에 법원은 동 조항이 과잉금지원칙에 위반하여 통신의 비밀 및 사생활의 자유를 과도하게 침해하여 위헌이라고 의심할 상당한 이유가 있다고 인정하여 위헌제청을 하였다.[10] 개**정안이 통신제한조치 기간을 축소하고 연장회수를 제한하고자 하는 방향은 타당하다. 다만 1월도 지나치게 긴 기간이라 할 수 있으므로 10일로 단축할 것을 제안한다.**

(3) 통신제한조치로 알게 된 내용의 열람 또는 복사(안 제9조의2제7항 신설).

개정안의 내용에 찬성한다.

(4) 통신제한조치 허가범위 외의 내용이나 불필요한 내용의 폐기의무(안 제12조제2항・제3항 및 제17조제2항제4호 신설).

개정안의 내용에 찬성한다.

9) 오길영 「통신비밀보호법 개정안 비판」 민주법학 제34호, 2007년

10) 서울중앙지방법원 2009.11.7. 선고 2009고합731 판결 참조