< 인권시민단체 워크샵 >

패킷 감청,
무엇이 문제인가

일시 : 2012년 1월 4일(수) 오전 10시

장소 : 민주사회를 위한 변호사 모임 회의실

공동주최

민주사회를위한변호사모임, 진보네트워크센터, 참여연대,
천주교인권위원회, 포럼 "진실과 정의", 한국진보연대

< 인권시민단체 워크샵 >
패킷 감청, 무엇이 문제인가

□ 사 회 : 장여경 (진보네트워크센터)

□ 발표

= 헌법과 패킷감청 : 오동석 교수 (아주대학교 법학전문대학원)
= 정보통신기술과 패킷감청 : 오길영 교수 (신경대학교 경찰행정학과)

□ 토론

= 이광철 변호사 (민주사회를위한변호사모임, 헌법소원 대리인)
= 박경신 교수 (고려대학교 법학전문대학원, 참여연대 공익법센터)
= 이호중 교수 (서강대학교 법학전문대학원, 천주교인권위원회)
= 유성 활동가 (인권운동사랑방)

□ 전체토론

패킷감청과 헌법

오 동 석*

1. 헌법소원심판의 대상

(1) 통신제한조치 집행행위로서 패킷감청행위
(2) 법원의 통신제한조치 허가행위
(3) 통신제한조치의 근거 법률조항으로서 통신비밀보호법 제6조

2. 패킷감청행위와 그에 대한 법원의 허가는 영장주의원칙에 위배된다.

감청에 대하여 통신비밀보호법은 영장이 아닌 법관의 허가를 얻도록 하고 있다. 허가는 성질상 영장 발부와 동일한 것으로 본다.[1] 그것은 수사기관이 법원이 한정한 대상과 방식에 따라야 함을 의미하는 것이다. 이때 법원은 대상과 방식을 개별적□구체적으로 한정하여야 한다. 그것은 통신의 자유에 대한 "적절한 사회적 기대"[2]를 보장하는 것이어야 한다. 헌법에서 규정한 영장은 범죄의 내용, 구금할 장소, 압수□수색의 목적물과 범위가 특정되지 않은 일반영장은 금지된다. 따라서 압수의 목적물과 수색의 대상과 범위가 모호하거나 포괄적인 일반영장(general warrant)은 허용되지 않는다.[3]

여기에서 '일반'이란 단어와 '포괄'이란 단어를 법적으로 구별해야 한다. 엄밀하게 말하면 일반영장은 그 용어 자체가 성립할 수 없다. 영장은 개인별로 발급되는 것이어야 하므로[4] 불특정다수에 대하여 발해질 수 없는 까닭이다. 헌법상 금지되는 영장을 정확하게 표현하면, 그것은 포괄영장(또는 백지영장이나 추상적 영장)이다. 왜냐하면 영장은 구체적이어야 하기 때문이다. 따라서 명확하게 그 대상이 한정되어 있어야 한다. 반면 패킷감청은 "말 그대로 데이터가 움직이는 도로를 통째로 감청하도록 허가해 준 것이다. 대상도 없고 범위도 없이, 도로에 움직이는 모든 것을 다 감청하도록 진정한 '포괄 허가서'를 발부해 준 셈이다."[5]

통신제한조치에 대한 법원의 허가와 신체의 자유에 대한 체포□구속영장 또는 물건에 대한 압수□수색영장은 차이가 있다. 영장은 한 사람의 인신 또는 범위를 확정할 수 있는 피의자의 물건을 그 대상으로 한다. 그러나 통신제한조치에는 피의자 외에 또 다른 상대방이 관여되어

---

* 아주대 법학전문대학원 교수, 헌법학

1) 정종섭, 헌법학원론, 박영사, 2009. 다만 그는 감청은 헌법 제12조 제3항에서 정하는 체포□구속□압수□수색에 해당하지 않으므로 헌법 제12조 제3항이 적용되지 않는다고 본다. 그렇지만 일반영장의 금지 등 영장주의의 핵심은 감청허가에도 그대로 타당한 것으로 보아야 할 것이다.

2) Crocker, Thomas P., FROM PRIVACY TO LIBERTY: THE FOURTH AMENDMENT AFTER LAWRENCE, *UCLA law review* 제57권 제1호, 2009, 3.

3) 정종섭, 앞의 책, 514.

4) 영국의 수사권규율법(Regulation of Investigatory Powers Act 2000) 제8조 제1항은 "한 명의 감청대상자" 또는 "영장이 관련되는 감청이 이루어지는 시설물과 관련된 경우에는 한 세트의 시설물" 중 하나가 기재되어야 함을 명시하고 있다.

5) 오길영, "인터넷 감청과 DPI(Deep Packet Inspection)," 민주법학 제41호, 민주주의법학연구회, 2009.12, 411.

있다. 전화인 경우 통화의 상대방, 우편의 경우 송신인 또는 이메일의 경우 송□수신인 등이 그 상대방이다. 피의자 관점에서 보면 그 상대방은 한 두 사람으로 특정될 수 없다. 감청 허가란 피의자를 대상으로 발부되지만, 불가피하게 통신의 속성상 불특정 다수의 상대방이 관계될 수 밖에 없는 구조이다. 그렇기 때문에 통신제한조치는 "다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있"(통신비밀보호법 제5조 제1항)음이 내재되어 있다고 말할 수 있다. 즉 원칙적 금지와 예외적 허가이다.

그런데 정부 측 답변서를 보면 감청이 오용 및 남용되고 있음을 알 수 있다. 정부 측 답변서는 패킷감청의 문제를 감청 일반의 문제로 치환하려 한다. 즉 패킷감청의 문제가 "전화 송수신 내용의 녹취, 무전 송수신의 채록 등 모든 종류의 전기통신의 감청에 공통되는 불가피한 현상"이라고 주장한다. "예를 들어, 유선전화 회선의 감청에 관한 통신제한조치를 집행하는 경우, 대상자뿐 아니라 가족 등 그 전화를 사용하는 모든 사람의 통신도 일정기간 모두 지득, 채록의 대상이 되는 것이며, 그 전화번호로 전화를 걸어오는 제3자의 통신도 마찬가지입니다."[6]

그러나 우선 현재의 감청제도 자체가 절대무변의 합헌성을 보장받는 것은 아니라는 점을 지적하여야 한다. 그것이 헌법적으로 정당화될 수 없을 정도로 국민의 기본권을 침해하고 있지 않은지 늘 헌법적 판단대상이 되어야 한다. 감청은 범죄 관련한 사회적 해악에 대처하는 유일한 대응방법 아니다. 이미 통비법도 보충성원칙을 확인하고 있다.

두 번째로 패킷감청은 전화감청 등과 다르다. 예를 들어 전화의 경우 피의자 또는 피고인이 아닌 경우 감청을 중지하는 것이 가능하지만, 패킷감청은 중지가 가능하지 않다. 일단 몽땅 감청하고 재생하여 "재생된 통신내용 중 범죄 관련 정보만을 활용"[7]하기 때문이다. 전화감청의 경우에도 포괄적 녹취는 헌법 및 통비법 위반이며, 답변서는 그러한 위헌□위법의 수사관행을 고백한 것에 불과하다.

세 번째로 패킷감청이 불가피하다고 볼 만한 사정이 없으며, 오히려 감청의 보충성의 원칙이 전혀 지켜지고 있지 않고 있음을 알 수 있다. 국가안보 관련 피의자 또는 내사자의 행위가 "장기간에 걸쳐 은밀하게 진행"[8]된다면, 다른 수사기법을 동원할 수 있는 기회가 많으며 그러한 가능성이 높기 때문이다. 답변서는 "범행수단도 기존의 유선전화에서 휴대폰이나 컴퓨터 등을 이용한 것으로 다양화"[9]되고 있다고 하지만, 인터넷은 범행수단이 아니라 범행모의수단이 될 수 있을 뿐인데 그것의 범죄와의 연관성 정도는 특정하여 말하기 어렵다. 즉 범행과 무관한 사적인 내용이 포함될 가능성이 그만큼 높다. 예를 들어 "공범자와의 접선"[10]은 잠복 및 미행만으로 충분하다.

네 번째로 답변서가 고백하고 있듯이 감청은 "대상자 동향 파악 등을 위하여" 악용되고 있다.[11] 답변서에서 범죄 수사 및 범죄 예방을 위하여 감청할 수 있다고 주장[12]하는 통비법 제12조는 "통신제한조치로 취득한 자료의 사용제한"에 관한 규정이다. 즉 "제9조의 규정에 의한 통신제한조치의 집행으로 인하여 취득된 우편물 또는 그 내용과 전기통신의 내용은 다음 각 호의 경우 외에는 사용할 수 없다. 1. 통신제한조치의 목적이 된 제5조제1항에 규정된 범죄나 이와

6) 정부법무공단, 2011헌마165 답변서, 정부법무공단, 2011.6, 16.
7) 앞의 답변서, 15.
8) 앞의 답변서, 12.
9) 위와 같음.
10) 앞의 답변서, 13.
11) 앞의 답변서, 5.
12) 앞의 답변서, 24.

관련되는 범죄를 수사 소추하거나 그 범죄를 예방하기 위하여 사용하는 경우"이다. 이것은 감청 후 자료 활용의 문제일 뿐이다. 통신제한조치 자체는 범죄 실행과 밀접한 관련이 있어야 하며, 범죄 예방을 위하여 활용할 수 없다. "통신제한조치는 … 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가"(통비법 제5조)할 수 있기 때문이다. "이메일□메신저□인터넷 카페□게시판□블로그□미니홈피 및 인터넷 전화 등"[13]을 감청한다면 사이버공간에서 사생활의 비밀과 사생활의 자유는 불가능하다. 패킷감청은 물론 감청 자체가 범죄행위와 무관하게 일상적인 감시활동으로 전용되고 있는 것이다. 즉 감청이 보충적 수단이 아니라 예비수단으로서 광범위하게 남용되고 있는 것이다.

마지막으로 패킷감청에서 IP 특정조치가 이루어진다고 하여도 PC 자체에 대한 것이어서 PC를 통해 교환되는 수많은 개인정보가 노출되는 점에서 다른 통신제한조치와 확연히 다르다. IP 특정조치는 패킷감청이 가지고 있는 위헌적 요소를 치유할 정도의 것이 아니다. 답변서는 "전기통신의 감청은 본질적으로 포괄적인 범위에서 정보가 노출될 수밖에 없습니다."[14]라고 주장하지만, 패킷감청 외의 것은 피의자 또는 피내사자가 특정되어 있고 또 감청과정 중 특정할 수 있기 때문에 중지가 가능하다.

법원은 피의자와 특정 통신매체를 대상으로 하여 통신제한조치를 허가하는 것은 그 허가 자체에 있어서도 신중해야 하며, 허가하는 경우에도 구체적 범위를 획정하기 위하여 최선의 노력을 다하여야 한다. 그렇지 않다면 피의자의 통신상대방은 통신의 자유 또는 사생활의 비밀 등을 침해당하기 때문이다. 따라서 피의자의 통신상대방 중 피의자의 범죄행위와 상당 정도 연관성이 있는 통신상대방과의 통신만이 감청대상으로 되어야 된다. 그렇지 않다면 법원은 통신비밀보호법상의 허가주의를 위반한 것이 된다. 왜냐하면 피의자만을 특정하여 그의 모든 통신상대방과의 통신을 감청하도록 허가하는 것은 통신상대방의 관점에서 보면 불특정 다수에 대한 허가라는 점에서 일반허가이기 때문이다. 통비법 제6조 제1항이 "각 피의자별 또는 각 피내사자별로 통신제한조치를 허가"하도록 함은 그 때문이다.

개별적이지만 포괄적인 피의자의 통신행위와 그와 관련된 일반적이고 포괄적인 통신상대방의 통신행위를 일반적이고 포괄적으로 침해하는 패킷감청은 검열 또는 허가처럼 헌법의 금지사항에 해당한다. 패킷감청에 대한 법원의 허가 또한 헌법상 허용되지 않는다. 패킷감청은 헌법이 허용하는 영장주의의 본질에서 벗어나기 때문이다. 패킷감청은 헌법적으로 성립할 수 없는 일반허가이면서 동시에 헌법적으로 금지되고 있는 포괄허가이다.

따라서 감청대상자와 상당관계에 있는 통신상대방과의 통신내용만을 그 내용 자체를 들여다보지 않고 구체적으로 선별하여 감청할 수 있는 패킷감청 기술이 등장하지 않는 한, 패킷감청은 헌법상 절대적으로 금지되어야 한다. 정부 측도 "현재 상용화된 기술로는 인터넷 회선 감청에서 감청의 대상자, 감청의 대상물을 사건에 관련된 것만으로 특정하는 것은 불가능"하다고 인정하고 있다.[15] 수사기관이 패킷감청 기술의 혜택을 누리려면, 기본권의 최대한 보장을 실현하기 위하여 그 침해 방지책이 충분히 마련될 때까지 기다려야 한다. 법적으로 그렇게 하지 않는다면 헌법상 통신의 자유는 유명무실해질 것이며, 통신비밀보호법에 따른 법관에 의한 감청 허가제 또한 무용지물이 될 것이기 때문이다.

---

13) 앞의 답변서, 13.
14) 앞의 답변서, 16.
15) 앞의 답변서, 22-23.

3. 과학기술의 발전과 기본권 제한법률 그리고 헌법원칙

기본권 제한법률의 기본권 침해성을 판단하는 경우에는 과학기술의 발전에 따라 입법사실을 고려하여 기본권 침해여부를 판단해야 한다. 입법사실이란 법령의 배경을 이루는 사회적·정치적 또는 과학적 사실이다. 이 입법사실은 논자에 따라서는 '법령이 제정되기 이전에 존재하고 있었던 상태, 그것을 개선하기 위하여 제정된 법령의 실효성, 법령의 제정에 의하여 생기는 손실(예를 들면 국민의 권리제약의 정도)보다 적은 희생으로서 같은 실효성을 올릴 수 있는 가능성 등 법령의 목적과 수단의 합리성을 실증적으로 검토하는 것이다.

헌재도 위헌법률심판 관련한 결정이기는 하지만 다음과 같이 판시한 바 있다.

> 구체적 규범통제를 목적으로 하는 위헌법률심판에 관한 헌법재판소법 제45조 전단의 "헌법재판소는 제청된 법률 또는 법률조항의 위헌 여부만을 결정한다"는 규정은, 헌법재판소는 법률의 위헌여부에 대한 법적 문제만 판단하고 법원에 계속중인 당해 사건에 있어서의 사실확정과 법적용등 고유의 사법작용에는 관여할 수 없다는 의미도 포함한다. 그러나 헌법재판소는 법률의 위헌여부에 대한 법적 문제를 판단하기 위하여 입법의 기초가 된 사실관계 즉 입법사실을 확인하여 밝힐 수 있다.[16]

패킷감청기법은 통신비밀보호법 제정 당시는 물론 시행과정에서 범죄수사기법으로서 예상하지 못했던 것이다. DPI 기술이 "가치중립적"이라고 하더라도[17] 그것이 수사기법으로서 활용된다면, 패킷감청은 더 이상 가치중립적이지 않게 된다.

> … DPI 기술은 … 다양한 정보통신서비스 제공기간 (홈페이지를 구축하여 온라인으로 영업하는 모든 회사를 말하며, 금융기관, 대기업, 전자상거래 업체뿐 아니라 정부기관도 포함됩니다)의 애플리케이션 방화벽, 침입차단시스템, 침입방지시스템에서의 각종 감시기능 (바이러스, 악성코드 체크, 내부정보유출 감시 등)에 사용되고 있으며, 서비스 거부공격(DDOS 공격)에 대한 기술적 대응방안으로도 사용되고 있습니다. 또한 그 외에 저작권침해 행위, 음란물배포에 대한 탐지수단으로도 사용됩니다. 정보통신서비스 제공기관 또는 금융기관의 각종 전산시스템과 관련하여 이러한 방화벽, 침입차단시스템, 침입방지시스템은 각종 관련법령(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자금융거래법 등)상 그 설치 및 통제가 강제되고 있는 것이기도 합니다.[18]

통신비밀보호법은 "통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적"으로 하고 있다(동법 제1조). 국가의 통신제한조치에 대한 통신비밀보호법의 허용은 매우 제한적이어야 하며, 그 적용은 매우 엄격해야 한다. 신체의 자유를 보장하기 위한 죄형법정주의에 유추해석 금지가 포함되어 있듯이 통신제한조치에 대한 수권조항도 인터넷 시대에 수사기관의 권력남용을 방지함으로써 통신의 자유를 보장하기 위해서는 유추해석이 금지되어야 한다. 그렇지 않다면 국가권력은 과학기술의 발전을 활용하여 헌법이 요청하는 기본권 보장의 원칙 그리고 법치주의 및 적법절차 등의 헌법원리를 회피하여 위배할 수 있게 되기 때문이다. 이러한 법리는 범죄 수사에 있어서 기존의 다른 수사기법의 활용을 차단하는 것이 아니라 오히려 보충성 원칙에 충실한 것이다. 그렇기 때문에 새로운 감청기술에 대한 적극적 근거로서의 법의 규율이 없는

16) 헌재 1994.4.28. 선고 92헌가3 결정.
17) 앞의 답변서, 12.
18) 앞의 답변서, 11-12.

경우 '원칙적 허용, 예외적 금지'보다는 '원칙적 금지, 엄격한 법치에 의한 허용'이어야 한다.

통신비밀보호법상 감청은 "통신의 음향□문언□부호□영상을 청취□공독"(통비법 제2조 제7호)함을 의미하는데, 패킷감청이 이에 해당하는지 명확하지 않다. 패킷감청은 "데이터(소위 패킷)를 추출"하여 감청하는 기법이다. 이때 "패킷(packet)은 인터넷에서 정보를 전달하는 단위로서, 데이터를 쪼개서 전송하고, 수신측에서 다시 조합하는 방식으로 통신하는 하나의 단위를 의미하는 것"이다.[19] 통비법상 "부호"에 가까워 보이지만 그와 다르며, 패킷의 재조합을 "공독"이라 보기도 어렵다. 오히려 패킷감청은 통비법 제2조 제8의2호에 따라 "이 법의 규정에 의하지 아니하고 행하는 감청 또는 대화의 청취에 사용되는 방식"인 "불법감청설비탐지"라 할 것이다.

결국 패킷감청이 수사기법으로 활용됨으로써 그것이 통비법상의 감청에 해당하는지가 모호해졌다. 이것은 통비법의 해당 규정이 과학기술의 발전에 대응하여 통신의 자유를 보장하기에 적절하게 규정하고 있지 못하고 모호하게 되어 있기 때문에 초래된 일이기도 하다. 패킷감청에 대한 수사기관의 집행행위와 법원의 허가행위에 대하여 통비법은 명확한 기준을 제시하지 못하는데, 패킷감청을 허용하는 근거를 두어서 해결될 수 있는 문제가 아니다. 따라서 패킷감청 기법을 포함하지 않는 한에서 통비법상 통신제한조치는 헌법적으로 허용될 수 있으며, 입법자는 이를 확인할 의무가 있다. 통비법은 감청의 보충성 원칙을 준수하고 있지 못하고, 과잉금지원칙 중 수단적합성 및 피해최소성 그리고 법익균형성의 원칙에 위배되는 패킷감청을 배제하고 있지 못함으로써 통신의 자유를 보장하는데 불충분한 입법이어서 위헌이다.

4. 감청에 대한 합헌적 해석 및 입법 방안

패킷감청은 위헌이다. 첫째, 패킷감청은 국가작용의 측면에서 권력분립원칙에 위배된다. 권력분립원칙은 집행행위에 대하여 개별성 및 구체성을 엄격하게 요한다. 그것이 완화되는 현상이 일어나고 있지만, 적어도 기본권 제한의 영역에서는 그러한 완화가 허용되어서는 안된다. 그런 점에서 보면, 패킷감청은 행정작용과 사법작용의 본질적 한계범위를 넘어선 것이다. 그것은 단순히 법률의 제정 또는 개정으로 해결될 수 없는 사안이다.

둘째, 이미 패킷감청이 행해지고 있으며 이것이 통신비밀보호법상 허용되는 것이라는 의견과 판단은[20] 위헌적인 해석으로서 이러한 해석은 허용되어서는 안된다. 패킷감청의 적법성을 전화감청으로부터 유추하기도 하지만, 휴대폰을 비롯한 전화 통화 내용과 인터넷 활동 내용은 그 범위에 있어서 엄청난 차이가 있다.

따라서 통신비밀보호법을 개정하여 패킷감청의 절대적 금지를 명문화하고, 이에 대한 위반행위를 처벌하는 규정을 신설해야 한다. 그렇기 때문에 패킷감청을 통제하겠다고 제안된, 이정현 의원의 통신비밀보호법 개정안(2009.12.11)은 사실상 패킷감청의 법적 근거를 마련한 것에 불과하다. 법안의 제6조 제6항[21]에 신설된 후단은 "이 경우 인터넷 회선에 대한 감청의 허가서

---

19) 앞의 답변서, 2.

20) 예를 들면, 서울중앙지방검찰청 윤상호검사가 작성한 "검찰 의견서"(2009.10.14). "○ 일부 감청허가서에 허가된 인터넷 회선 감청의 경우 기술적으로 변호인 주장과 같은 패킷감청이 가능한 것은 사실입니다." "○ 하지만, 인터넷 회선 감청은 통신비밀보호법상 적법한 감청입니다. ※ 집행과정에서 수사대상자 외의 자가 송 수신하는 전기통신이 지득 채록될 가능성을 배제할 수 없으나, 이는 전화회선에 대한 감청의 경우와 다르지 않고 집행상 유의할 부분이라고 할 것입니다. - 즉 본건의 경우 설사 인터넷 회선 감청을 하였다고 하더라도 통신비밀보호법의 허가요건, 집행절차에 따른 것으로 적법합니다."

21) 제5항의 허가서에는 통신제한조치의 종류 그 목적 대상 범위 기간 및 집행장소와 방법을 특정하여 기

에는 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 기재하여야 한다."고 규정하고 있기 때문이다.

셋째, 패킷감청의 가능성을 차단하기 위하여 현행 통신비밀보호법의 통신제한조치에 대한 허가절차를 세밀하게 규정하여야 한다. 즉 법관에게 청구되는 허가신청서의 정보가 상세하게 규정되어야 하며, 법원으로 하여금 통신제한조치의 범위를 구체화하여 허가하도록 하는 절차를 마련하여야 한다.

참고로 일본의 '범죄수사를 위한 통신감청에 관한 법률' 제3조는 "판사가 발부하는 감청영장에 의하여 전화번호 기타 발신원(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.

한편 미국의 통신비밀법의 제2518조[22] 제1항은 감청신청서에 다음과 같은 내용을 요청하고 있다.

"제2518조 유선통신, 대화 또는 전자통신의 감청 절차

⑴ 본 장에 따라 유선통신, 대화 또는 전자통신의 감청을 허가 또는 승인하는 명령에 대한 신청은 선서 또는 그에 갈음하는 확약 후에 서면으로 관할판사에게 하여야 하며, 신청자의 신청 권한을 기술하여야 한다. 신청서에는 다음과 같은 정보가 포함되어야 한다.

⑷ 신청서를 작성하는 수사관 또는 법 집행관과 신청을 인가하는 공무원의 신원

⑸ 다음 사항을 포함하여 명령서 발부가 필요하다는 믿음을 정당화하기 위하여 신청자가 의지하고 있는 사실과 정황에 대한 충분하고 완전한 기술

(ⅰ) 이미 실행되었거나 현재 실행 또는 계획되고 있는 특정 범죄에 관한 상세한 설명

(ⅱ) 제11항[23]에 규정된 것을 제외하고, 감청설비의 특성과 위치 또는 통신이 감청되는 장

재하여야 한다.

22) 미국 연방법전(United States Code) 제18편 범죄 및 형사소송 절차(Title 18 Crimes And Criminal Procedure) 제119장 유선 및 전자통신 감청과 대화의 감청(Chapter 119 Wire And Electronic Communications Interception And Interception Of Oral Communications)

23) ⑾ 통신이 감청되는 설비에 관한 세부 설명이나 그 장소에 관련되는 본 조의 제1항⑸(ⅱ)와 제3항⑷의 요건은 다음과 같은 경우 적용하지 아니한다.

⑷ 대화감청에 관한 신청에 있어서

(ⅰ) 신청이 연방수사관이나 법 집행관에 의하여 이루어져 법무장관, 법무부장관, 법무차관, 법무차관보나 법무차관보 대리가 인가하고

(ⅱ) 신청서가 위와 같은 세부설명이 실현가능하지 않다는 완전하고 충분한 해명을 포함하고 있고 범죄 혐의자에 대한 신원과 그 혐의자의 통신이 감청된다는 사실을 소명하고 있으며

(ⅲ) 판사가 위와 같은 세부설명이 실현가능하지 않다고 판단하는 경우

⑸ 유선 또는 전자통신 감청에 관한 신청에 있어서

(ⅰ) 신청이 연방 수사관이나 법 집행관에 의하여 이루어져 법무장관, 법무부장관, 법무차관, 법무차관보 또는 법무차관보 대리가 인가하고

(ⅱ) 신청서가 범죄 협의자에 대한 신원과 그 협의자의 통신이 감청된다는 사실을 소명하고 있고, 그 혐의자의 행동이 특정한 설비로부터의 감청을 방해할 소지가 있다고 믿을만한 상당한 이유가 있다는 사실을 제시하고 있으며

소에 관한 특별한 기술

(iii) 통신이 감청되는 방식에 관한 특별한 설명

(iv) 신원이 파악되었을 경우, 범죄 행위자와 감청대상자의 신원

(c) 다른 수사 절차가 시도되어 실패한 적이 있는지 여부와 그러한 절차가 시도되더라도 성공하기 어렵다든지 또는 너무 위험한 것으로 판단하는 이유에 관한 충분하고 완전한 기술

(d) 감청이 필요한 기간에 관한 기술. 수사의 성질상 기술된 유형의 통신이 최초 획득될 때 감청허가가 자동적으로 종료되어서는 아니 되는 경우, 동일한 유형의 통신이 추가 발생하리라 믿을만한 사유에 대한 특별한 기술

(e) 신청서에 명기된 동일 인물, 감청설비 또는 장소와 관련되는 유선통신, 대화 또는 전자통신의 감청허가를 신청한 자가 알고 있는 과거의 모든 신청에 관한 사실과 위와 같은 각각의 신청에 대하여 판사가 취한 조치에 관한 충분하고 완전한 기술

(f) 연장을 신청하는 경우, 감청으로 그때까지 입수된 결과에 대한 상세한 설명과 그러한 결과의 입수에 실패한 경우 그에 대한 합당한 설명"

또한 기본권 보장의 관점에서 판사가 통신제한조치를 허가함에 있어서 실질심사를 담보할 수 있는 과정을 거치도록 의무화하거나 최소한 그것을 위한 재량권한을 판사에게 부여하는 명문의 규정을 두어야 한다. 참고로 미국에서 "(2) 판사는 신청자에게 신청 사유를 뒷받침할 수 있는 추가증언이나 서면 증거의 제출을 요구할 수 있다"(제2518조 제2항). 또한 제2518조 제3항은 감청의 허가요건으로서 ① 범죄 실행의 개연성 ② 증거획득의 개연성 ③ 보충성 ④ 해당 감청설비의 수사대상과의 관련성을 요구하고 있다.[24]

5. 결론

국가권력과 개인의 기본권의 역전현상은 헌법의 근간을 흔든다. 헌법재판소는 국가안보에 대하여 한 치의 빈틈도 없게 하려 하지만, 그 때문에 국민의 기본권은 숨 쉴 수가 없다. 개인의 사생활의 비밀과 자유의 영역이 줄어들고 있지만, 국가의 비밀의 영역은 날로 팽창일로에 있다. 통신의 자유도 마찬가지이다. 근본적인 대책이 필요하다.

헌법 제37조 제2항은 기본권을 제한하는 입법을 옹호하는 이들의 금과옥조이다. 그 때문에

(iii) 판사가 위와 같은 소명이 적절하게 되었다고 인정하고 있고

(iv) 신청서에 소명된 사람이 감청대상 통신이 전송되거나 전송된 기기에 근접하여 있거나 근접하고 있었다고 추정할 만한 상당한 이유가 있는 때에만 감청허가 또는 승인명령이 감청을 허용하는 경우

24) (3) 신청서를 제출 받은 판사는 신청자가 제출한 사실들을 토대로 다음과 같이 결정하는 경우 판사가 재직하고 있는 법원의 영토관할권 내(그리고 같은 관할권 내의 연방법원에 의하여 허가된 이동감청장비의 경우 연방내에서는 그 관할권 밖이라고 해당됨)에서 유선통신, 대화 또는 전자통신의 감청을 요청한 대로 또는 수정하여 허가하거나 승인하는 명령서를 발부할 수 있다.

(a) 어떤 개인이 본 장의 제2516조에서 열거한 범죄를 실행하였거나 실행 또는 계획하고 있다고 믿을만한 상당한 이유가 있다고 결정하는 경우

(b) 그러한 범죄와 관련된 특정한 통신이 감청을 통하여 수집될 것이라고 믿을 만한 상당한 이유가 있다고 결정하는 경우

(c) 통상적인 수사절차가 이미 시도되어 실패하였거나 시도하더라도 합리적으로는 성공하기 어렵거나 너무 위험한 것이라고 판단된다고 결정하는 경우

(d) 제11항에 제시된 것을 제외하고, 유선통신, 대화 또는 전자통신이 감청되는 설비 또는 장소가 그 같은 범죄와 관련하여 사용 또는 사용될 예정이거나 이러한 범죄혐의자에 의하여 임차 또는 일반적으로 사용되고 있다고 믿을만한 상당한 이유가 있다고 결정하는 경우

단서인 본질적 내용 침해 금지 원칙은 거의 죽어 있다. 기본권 문제에 있어서 우리는 늘 타협을 강요당한다. 기본권의 절대적 보호영역은 늘 내심의 영역에만 머물러 있다. 그 내심의 확장된 공간으로서 통신은 철저히 상대화될 것을 강요당한다. 과학기술의 발전이 오히려 인간의 자유 공간을 위축시키고 있는 셈이다. 그것은 필연적이거나 숙명적인 것이 아니다. 오히려 우리의 자유 공간을 절대적 침해금지 구역으로 확보하는 것은 인권의 관점에서 민주주의적으로 방어해야 할 정당한 몫이다. 패킷감청이 바로 그러한 절대적 금지구역이어야 한다. 어떠한 방식으로든 패킷감청을 법적으로 정당화하는 것은 결국 헌법의 근간을 부정하는 셈이다. 국민투표를 거쳐 헌법을 개정하여 그 근거를 마련한다고 하더라도 패킷감청은 정당성 부재를 넘어 '헌법적 불법'[25]일 뿐이다.

25) 라드브루흐가 사용한 '법률적 불법'(Radbruch, Gustav, 이재승 옮김, "역주: 법률적 불법과 초법률적 법," 법철학연구 제12권 제1호, 한국법철학회, 2009, 1-26)으로부터 차용한 변형어이다. 특정 헌법조항 또한 헌법 자체가 불법성을 띠는 경우이다. 대표적으로는 1972년의 이른바 '유신헌법'을 그 예로 들 수 있을 것이다.

【발제】

패킷감청의 위헌성*

오길영
신경대 교수, 정보통신법
eclaw@daum.net

< 차 례 >

I. 들어가며

DPI(Deep Packet Inspection, 이하 DPI)가 또다시 도마에 올랐다. 패킷감청이 헌법소원의 한 가운데에 와있기 때문이다. 이 글은 DPI와 관련한 담론[1]에 있어 수사기관에 의해 진행되는 패킷감청에 관한 논쟁에 종지부를 찍기 위해 작성된다. 즉 패킷감청의 위헌성을 밝히고자 하는 것이다.

주지하다시피, 현재 진행되고 있는 패킷감청은 통신비밀보호법상의 통신제한조치허가서에 의해 집행되고 있다. 소위 감청영장이라 통칭되는 이 한 장의 영장이, 본격적인 디지털 시대를 맞고 있는 지금에 와서는 얼마나 위험천만한 강제처분으로 둔갑하고 있는지를 입증코자 하는 것이 이 글의 목적이다. 따라서 이 글은 국가정보원이 밝힌 패킷감청의 합헌성에 관한 주요 논지[2]를 반박하는 형태로 진행된다.

본격적인 검토에 앞서, 국가정보원이 밝힌 주요 논지를 정리하면 다음과 같다.

첫째, DPI기술은 패킷감청뿐만이 아니라 디도스(Distributed Denial of Service, 이하 DDoS) 공격이나 바이러스 침입 또는 악성코드 체크, 내부정보유출 감시 등을 위한 방화벽이나 침입차단시스템으로 사용되고 있음은 물론 저작권 침해행위, 음란물배포에 대한 탐지수단으로 사용되고 있다. 만약 DPI 기술자체가 기본권 침해성을 가지고 있다면 이러한 다른 용도로의 사용 또한 사인에 의한 기본권 침해를 구성하게 되는데, 관련법령은 오히려 이러한 각종 시스템의 설치 및 통제를 강제하고 있으므로 통신비밀보호법상 통신제한조치가 합헌인 이상 DPI 기술을 사용한다고 하여도 그 위헌성이 부가되는 것은 아니라고 한다.[3]

둘째, 인터넷 기술의 발전에 따라 언제 어디서나 상대방과 간편하게 통신□연락수단 등으로 활용할 수 있는 이메일□메신저□인터넷 카페□블로그□미니홈피 및 인터넷 전화 등이 안보범죄에 광범위하게 사용

---

* 본 원고는 발제용 원고로서 완성된 논문이 아니다. 따라서 논문으로서의 완결성을 위한 여러 요소들을 결한 상태인, 생각을 정리하는 차원에서의 소위 평문으로 작성된다. 토론회에서의 의견을 수렴하여 글을 완성하고, 곧 논문 또는 의견서의 형태로 재가공□발표될 예정임을 미리 밝혀둔다.

1) DPI와 관련된 법적인 이슈는 비단 패킷감청에 그치지 않는다. 최근 뜨거운 이슈가 되고 있는 망중립성 문제는 물론, 인터넷 맞춤광고, 네트워크 관리에 있어서의 ISP의 책임론 등 DPI로 인하여 발생하는 법적 문제점은 여러 가지이다.

2) 정부법무공단, 2011헌마165에 대한 국가정보원장의 '답변서'가 바로 그것이다.

3) 정부법무공단, 위의 글, 11-12쪽.

되고 있는 실정이고, 안보사범들은 수사기관의 추적을 따돌리기 위해 통신한 즉시 관련내용을 삭제하는 등 증거인멸을 시도하는 경우가 빈번하며, 특히 수사권이 미치지 않는 외국계 이메일이나 비밀게시판 등을 사용하는 소위 '사이버 망명'을 시도하고 있기 때문에 그 대처를 위해서 인터넷 회선 감청은 불가피하다고 한다.[4][5]

셋째, 패킷감청은 적법한 심사를 받은 영장을 통해 ISP에 의해 위탁집행되어 수사기관에서 제공되고, 그 수집에 있어 감청대상자가 사용하는 PC의 인터넷회선에 대해서만 감청이 이루어질 수 있도록 기술적인 IP 특정조치를 취하여 인터넷통신 데이터를 추출하므로 제3자의 회선에 대한 침해가능성이 방지되며, 제공받은 데이터를 수사기관이 재조합하면서 일부 암호화된 패킷 등은 재생이 되지 않을 뿐만 아니라 재생된 통신내용 중 범죄관련 정보만을 활용하므로 실시간 대상자의 컴퓨터 화면과 똑같은 화면을 보면서 모든 내용을 감청한다는 주장은 터무니없다는 것이다.[6][7]

넷째, 수사기관이 감청영장의 허가범위를 넘어 로그기록□접속시간 및 인터넷전화 등까지 감청하고 있다는 것은 명백한 오류임을 밝히면서, 인터넷 회선감청의 결과 전기통신의 일시, 개시 및 종료시간, 컴퓨터통신 또는 인터넷의 로그기록자료, 접속지 위치추적자료 등은 당연히 이에 수반하여 수집하는 것이므로 통신제한조치허가는 당해 통신과 관련한 통신사실확인자료제공허가를 포함한다고 보아야 하고, 인터넷전화 감청의 경우 일종의 회선감청에 포함되어 인터넷회선 감청 허가서로도 집행이 가능하나 실제 수사에 있어서는 그 전화번호를 특정하여 인터넷전화에 대한 별도의 허가서를 함께 발부받아 집행하고 있다고 한다.[8]

다섯째, 패킷감청을 통해 수집한 증거를 수사자료나 증거자료로 제출하는 경우가 전무하다는 주장과 관련하여서는, 통신제한조치로 취득한 자료를 범죄의 '소추'뿐만이 아니라 '수사나 예방'을 위해서도 사용할 수 있으므로 수집된 자료를 반드시 증거자료로 제출□활용해야 하는 것은 아니고, 패킷감청의 결과를 바탕으로 추후 이메일이나 홈페이지 등에 대한 압수□수색을 단행하여 감청내용과 동일한 범죄증거를 확보하게 되므로 '최량증거의 원칙'상 그 압수□수색의 결과물을 제출하면 족하지 굳이 패킷감청의 결과까지 제출할 필요가 없다고 한다.

국가정보원이 밝힌 주요한 논지는 이렇듯 다섯 가지 정도로 압축해 볼 수 있다.[9] 어찌되었건 상당히 많은 내용에다 쟁점도 많아 보이나, 기실 이들 주장의 타당성을 검토하는 것은 그리 힘들지만은 않다. 이들을 종합해보면, 결국 모든 논지가 'DPI 기술자체가 특정성이 있느냐'의 문제와 '기본권 침해의 최소성을 위한 규제가 가능하냐'의 논의로 귀결되기 때문이다. 따라서 이하의 본론에서는 국가정보원이 취하고 있는 논지의 타당성에 대하여 크게 '특정가능성'과 '규제필요성'으로 대분하여 구체적인 검토를 진행하기로 한다.

결론부터 이야기하자면, 이러하다. 이러한 주장은 모두 옳지 않다! 즉, 이러한 국가정보원의 주장이 합헌성의 논거라면 패킷감청은 위헌인 것이다.

---

4) 정부법무공단, 앞의 글, 12-13쪽.

5) 이러한 주장에 연이어, 외국계 이메일인 Gmail을 사용하는 피의자에 대해 패킷감청을 실시하였음을 명시적으로 밝히고 있다.

6) 정부법무공단, 앞의 글, 14-15쪽.

7) 이에 관하여 같은 글, 18쪽에서는 사용자의 모니터 화면을 실시간으로 수사기관이 엿본다는 것은 상상에 불과한 것이라 평가하면서, 나아가 같은 글, 29쪽의 각주 33에서는 "대상자가 인터넷을 통해 범죄와 관련없는 영화나 드라마 등을 시청하거나 메신저를 통해 장시간 사적인 대화를 나누고 있음이 확인되었는데도, 다수의 사건처리 등 공무집행으로 분주한 수사관들이 해당 패킷을 재현하여 이를 감청할 수 있다고 우려하는 것은 비판을 위한 비현실적인 기우에 불과하다"라고 꼬집고 있다.

8) 정부법무공단, 앞의 글, 17-18쪽.

9) 덧붙인 논의가 있기는 하나, 주요한 논지와 그 맥을 같이하거나 내용상 별 차이가 없다.

Ⅱ. 특정가능성과 관련하여

패킷감청과 관련한 특정가능성의 논의는 몇 가지의 의미로 구분하여 생각해 볼 수 있다. 먼저 ① DPI 기술자체가 감청대상을 특정하는 것이 가능한가하는 문제를 생각해 볼 수 있다. 이러한 문제의식은 국가정보원이 밝힌 논지의 곳곳에 면면히 흐르고 있다. 특히 셋째의 논지에서는 패킷감청시에 대상자를 특정하기 위하여 소위 고정IP를 부여하는 별도의 조치를 취하고 있음을 밝히고 있어, 원래는 특정가능성이 없음을 논리적 토대로 깔고 있다. 넷째의 논지에서도 크게 다르지 않다. 인터넷 전화의 경우 당연히 인터넷회선 감청으로 가능한 것임을 밝히고 있다. 별도의 허가서를 발부받아 집행하는 것은 적법절차를 위한 것에 불과하므로, 그 반대해석에 의하면 인터넷회선 감청허가서만으로도 인터넷 전화에 대한 감청이 기술적으로 가능하다는 것을 스스로 밝히고 있는 것이다.

다음으로 이러한 기술적 특정가능성과는 별도로 ② 영장주의의 원칙상 요구되는 특정이 가능하냐의 문제이다. 즉 포괄영장성의 문제이다. 이는 둘째의 논지와 직결된다. 인터넷회선 감청영장 하나로 '이메일□메신저□인터넷 카페□블로그□미니홈피 및 인터넷 전화 등'은 물론 심지어 '수사권이 미치지 않는 외국계 이메일'까지도 수사가 가능함을 밝히고 있는 국가정보원의 표현에서 보듯이 인터넷회선 감청은 성질상 전방위적인 포괄성을 내포하고 있는 것이다. 그리고 셋째의 논지에서 밝히고 있는 바와 같이 범죄와 관련된 정보만을 활용한다는데 이 부분 또한 포괄성과 관련하여 정밀한 검토가 필요하다. 기술적으로 가능하지 않기 때문이다. 또한 넷째의 논지에서도 이러한 문제의식은 여전히 존재한다. 패킷감청의 경우, 일단 통신제한조치 허가서를 발부받으면 통신사실확인자료 제공의 허가는 저절로 취득되는 일종의 부산물임을 밝히고 있는데, 이 또한 인터넷회선 감청영장의 포괄성을 스스로 밝히고 있는 부분이라 할 수 있다.

마지막으로 ③ 디지털 컨버전스(Digital Convergence)의 문제이다. 숙지하는 바와 같이 현재의 스마트폰은 단순히 전화를 걸고 받는 기계가 아니다. 또한 노트북으로 전화를 받기도 하고, 자동차의 네비게이션으로 뉴스방송을 보기도 하며 거실의 TV를 통해 영상통화를 하는 세상이 왔다. 디지털 기술이 발전함에 따라 유선과 무선, 방송과 통신, 통신과 컴퓨터 등 기존의 기술·산업·서비스·네트워크의 구분이 모호해지면서 이들 간에 새로운 형태의 융합 상품과 서비스들이 등장하는 현상을 우리의 두 눈으로 생생히 목격하고 있는 것이다. 이러한 융합의 시점에 서있는 우리는 도대체 무슨 방법으로 인터넷 회선과 전화회선을 구분하여야 하는 것일까? 종래의 채널들이 복잡다단한 융합을 진행하고 있는 지금의 시점에서, 영장상의 표현을 빌자면 "피의자 OOO의 인터넷 회선감청"이라는 표현이 기술적□논리적으로 도대체 어느 정도의 특정성을 가질 수 있는가의 문제가 바로 그것이다.

1. DPI 자체의 불특정성

DPI 기술은 원래 감청을 위해 개발된 것은 아니다. SPI(Shallow Packet Inspection)를 통해 구축하던 보안시스템의 한계를 극복하기 위해 탄생한 기술이 DPI이라는 점은 이미 주지의 사실이다. 앞서 국가정보원이 밝힌 바와 같이 현재 DPI 기술은 보안의 부분에서 매우 중요한 역할을 담당하고 있다. 바이러스(Virus)나 웜(Worm)의 차단, 그리고 최근의 DDoS 사태로 유명해진 서비스 거부(Denial of Service Attack, DoS)를 해결하기 위해 개발되어 사용되어 오고 있다.[10]

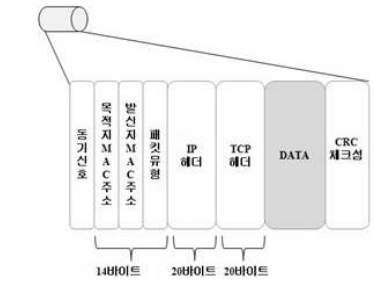
그렇다면 국가정보원의 주장처럼 DPI의 과정에 있어 감청대상자에게 고정IP를 부여한다면 DPI 대상자의 특정이 이루어지는가? 나아가 어떠한 방식으로든 DPI 대상자만을 특정해내는 기술은 무엇인가 하는

10) 지면상의 이유로 여기에 등장하는 기술용어의 기본적인 개념설명은 생략하기로 한다. 패킷의 개념과 구조, SPI와 DPI의 개념과 그 차이, DPI의 국제적 논란과 그 위험성 등에 관한 상세는 오길영, 인터넷 감청과 DPI, 민주법학 제41호(2009), 410쪽 이하 참조.

점이 여기서의 쟁점이 된다.

1.1. 패킷감청의 원리

먼저 패킷감청의 원리에 대하여 생각해 보자. 특정 ISP(예를 들어 KT, 이하 KT)의 회선에 설치된 감청설비는 그 회선을 지나가는 수많은 패킷들 가운데 감청대상자를 향해 가고 있는 패킷들을 선별해야 한다. 물론 KT의 회선을 지나다니는 모든 사용자의 패킷들을 모두 수집□재조합하여 다시금 감청대상자를 선별한다는 것도 이론상 가능은 하겠지만, 그 데이터의 양을 고려해 볼 때 도저히 불가능하기 때문이다. 따라서 일단 SPI를 통해 패킷의 헤더부분을 검토하여 그 송수신 네트워크 주소로 감청대상자를 지목하고 있는 패킷들만 골라 담은 후에, 이들을 DPI하여 재조합하는 방법이 효과적일 것이다. 즉 패킷헤더에 적힌 주소를 활용하여 감청대상 패킷을 특정해야 한다. 이를 위해서는 먼저 감청대상자의 네트워크 주소를 알아야 한다. 즉 감청대상자의 네트워크 주소를 알면 당해 주소가 적힌 패킷만을 선별하여 담을 수 있기 때문이다.



<그림1 패킷의 구조>[11]

이 즈음에서 패킷의 구조를 보여주고 있는 위의 도안을 살펴보자. 흰색 부분에 대한 검사(Inspection)가 SPI, 검은색인 데이터 부분에 대한 검사는 DPI가 되고, 가장 유명한 네트워크 주소인 IP주소는 위의 도안에서 'IP헤더'라는 부분에 포함되어 있다. 그런데 여기서 또 다른 네트워크 주소인 MAC주소(Media Access Control Address, MACA)를 발견할 수 있다. 패킷감청에 있어 사용되는 주소는 둘 중 어떤 것일까? 양자의 차이는 무엇인가 하는 의문이 발생한다.

MAC주소는 네트워크 카드(소위 랜카드)에 물리적으로 각인된 주소이다. 즉 마치 자동차의 엔진이나 몸체에 각인된 차대번호와 같은 것으로, 이를 통해 각각의 네트워크 카드는 전세계적으로 유일무이한 번호를 가지게 된다. 따라서 감청대상자 노트북에 장착된 랜카드의 MAC주소를 안다면 이는 곧 그 노트북으로 향하는 패킷을 지목해낼 수 있다는 것을 의미한다. 한편 IP주소는 우리 일상생활에서의 주소와 유사한 개념이라 할 수 있다. 즉 자동차 자체가 아니라 자동차가 주차되어 있는 차고지 주소라고 비유해 볼 수 있겠다.

결국 KT가 제공한 차고지 주소를 통해 위치를 파악하고, 자동차 차대번호인 MAC주소의 확인을 통해 탑승중인 대상자를 지목한다면 매우 정확한 특정성을 담보하게 될 것이다.

1.2. IP 운용의 원리

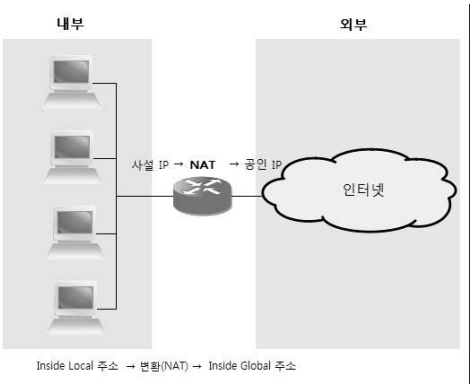
그렇다면 패킷감청을 하기위해 필요한 두 가지의 네트워크 주소를 어떻게 알아낼 수 있는가? IP주소의 경우에 KT가 가입자에게 임의적으로 부가하는 것이므로 국가정보원이 감청영장을 내밀면 KT가 바로 알려줄 것 같지만, 사실은 그리 간단하지만은 않다. 세상에 인터넷 사용자는 많고 IP주소는 유한하기 때문이다.

---

[11] 본 도안은 <http://cafe.naver.com/sec.cafe?iframe_url=/ArticleRead.nhn%3Farticleid=3831&>, 검색일: 2012.1.3.에서 인용한 것이다.

KT는 모든 가입자에게 하나씩의 IP를 제공하지 않는다. 만약 100만 명의 가입자에게 100만 개의 IP를 제공한다면 1:1 매칭이 바로 되어 혼돈의 우려가 없어 깔끔하겠지만, 100만 명의 가입자가 항상 동시에 인터넷을 사용하는 것은 아니므로 유한한 IP자원을 굳이 이렇게 소비할 필요는 없다. 따라서 KT 서비스의 가입자 가운데 현재 인터넷 접속을 희망하는 자에게만 일시적인 IP를 부여하고, 그 가입자가 다음날 또다시 인터넷 접속을 해오면 또 다른 일시적 IP를 부여하는 방식인 소위 '유동IP' 시스템[12]을 기본적으로 사용한다. 그러나 유동IP의 경우 인터넷에 접속할 때마다 IP주소가 바뀌게 되므로, 감청대상자의 IP를 특정해낼 수 없다. 따라서 국가정보원이 밝힌 바와 같이 일단 패킷감청의 대상자로 지목되면, 그는 값비싼 고정IP 서비스를 공짜로 누릴 수 있는 운 좋은 상황이 연출되게 된다. 그렇다면 국가정보원의 주장처럼 고정IP를 부여받으면 특정가능해지는가?

아쉽게도 그렇지 않다. 한국내의 모든 컴퓨터가 KT로 부터 직접 IP를 부여받지는 않기 때문이다. 수원의 삼성전자 본사 건물내에 있는 컴퓨터들은 KT가 아니라 삼성전자 전산실에서 운영하는 LAN(Local Area Network))서비스에서 부여한 IP를 부여받고, 화성의 신경대학교내 연구실에 있는 필자의 노트북은 신경대학교 전산담당자가 할당하는 IP를 가지며, 서초동의 민변 사무실에 있는 PC는 창가 벽면에 걸려있는 공유기가 임의적으로 창출한 IP를 통해 인터넷에 접속한다. 이를 도안으로 살펴보면 아래와 같다.



<그림2 NAT의 개요>[13]

사설망(즉 LAN)의 운용자는 사설망내에서만 운용되는 별도의 IP를 각 컴퓨터마다 부여하고, 이 가운데 현재 인터넷 접속을 요청해온 특정 컴퓨터만을 KT에서 할당받은 몇 개의 IP(공인 IP)와 적시에 매칭시켜 사설망을 운용하는 것이다. 즉 인터넷 접속시에 사설IP를 공인IP로 즉시 변환시켜주는 NAT(Network Address Translation) 시스템을 운용하는데, 웬만한 학교나 기업은 물론 소규모의 사무실 공간과 같은 곳에서도 공유기를 통하여 동일한 원리로 운용된다고 할 수 있다. 공유기의 경우 KT로부터 할당받는 IP 개수를 줄여 절약을 도모하는 취지가 크겠으나, 학교나 기업 같은 제대로된 LAN을 구성하고 있는 곳에서는 절약의 목적보다는 보안의 목적[14]이 더 크다고 하겠다. 따라서 바이러스와 악성코드가 난무하는 오늘날에는, 거의 대부분의 사설망에서 필수적으로 NAT 시스템을 사용한다고 보면 된다.

지금까지의 논의를 종합해보면, 국가정보원은 난감해진다. KT에다 요청하여 감청대상자의 유동IP를 고정IP로 고착한다 하여도 특정이 불가능하기 때문이다. 만약 신경대학교가 KT로부터 부여받은 10개의 공

12) 정확히 말하자면 동적 호스트설정 통신규약(Dynamic Host Configuration Protocol, DHCP)이다. DHCP는 네트워크 관리자들이 조직 내의 네트워크상에서 IP 주소를 중앙에서 관리하고 할당해줄 수 있도록 해주는 프로토콜이다. 즉 DHCP는 부여된 IP 주소가 일정한 시간동안만 그 컴퓨터에 유효하도록 하는 '임대' 개념을 사용하는 것이라고 요약할 수 있다.

13) 본 도안은 <http://blog.naver.com/demonicws?Redirect=Log&logNo=40108689465>, 검색일: 2012.1.3.에서 인용한 것이다.

14) 즉 NAT를 통해 외부망과 내부망을 격리하면서 그 접점에다 방화벽을 구성하게 되므로 오늘날 네트워크 보안체제의 핵심적 기술이라 할 수 있다.

인IP를 모두 고정IP로 고착시킨다고 가정해 보자. 국가정보원은 신경대학교에서 실시간으로 고정IP로 둔갑하여 날아오는 패킷가운데 도대체 어느 것이 필자의 패킷인지 구분할 방도가 없다. 신경대학교의 NAT가 매칭하는 필자 노트북의 사설IP를 알 수 없기 때문이다. 물론 신경대학교 전산소장에게 감청영장을 내밀면서 NAT의 매칭정보를 알아내면 될 것이다. 그러나 웬만한 고등학교만한 신경대학교에서 밀행성이 유지될 가능성이 없다는 것이 난점이다. 아마도 2-3일내로 필자의 소문이 자자해질 것이다. 나아가 민변 사무실의 공유기는 어찌해야 하는가? 감청영장을 들이밀 상대조차 없다. 수사관이 잠입하여 공유기를 조작하지 않는 한 특정가능성은 없다.

1.3. DPI의 원리

MAC주소는 어떠한가? 패킷감청은 밀행되어야 하므로, 대상자가 들고 다니는 노트북이나 사무실의 책상아래에 위치한 PC의 랜카드를 수사관이 방문□분해하여 알아낼 수는 없지 않은가? 이 또한 앞서 살펴본 NAT에서의 문제와 크게 다르지 않다. 결국 특정가능성은 존재하지 않는 것이다. 따라서 국가정보원의 주장과는 달리 패킷감청은 불특정다수에 대한 무차별적인 집행이 필연적인 것이다. 별수 없이 신경대학교에 할당된 10개의 고정IP를 모두 DPI하게 되며, 이로써 신경대학교내에 존재하는 100여대의 컴퓨터를 오가는 모든 패킷들은 모조리 감청장비에 담겨진다. 다만 이러한 과정에서 우연히 필자의 이름이 등장하는 메일을 조합해내고 그 메일패킷에 기록된 필자 노트북의 MAC주소를 알아낸다면, 그때부터는 굳이 이러한 수고를 하지 않아도 될 것이다. 10개 회선의 문턱을 지키면서 당해 MAC주소를 담고 있는 패킷들만 담아내면 되기 때문이다.

요컨대 패킷감청은 IP주소가 아니라 MAC주소의 확인을 통해 특정가능성이 생기며, MAC주소의 확인 이전에는 불특정다수에 대한 전방위적인 감청이 필연적이라는 본질적 속성을 가진다.

한편 내용적인 측면에서의 특정가능성은 어떠한가? 패킷감청으로 수집된 필자의 수많은 패킷들 가운데, 범죄와 관련 있는 이메일만을 구분해 낼 수 있는가의 문제이다. 지금까지 살펴본 바와 같이 DPI는 그저 패킷에 기록되어 있는 주소만을 근거로 패킷을 수집해내는 기술에 불과하다. 즉 무조건 수집만 해올 뿐이므로, 패킷을 재조합하여 내용을 완성해내기 이전에는 당해 패킷이 이메일의 일부인지 야동의 일부인지 구분해내는 기술은 아직 현존하지 않는다. 다시 말해 내용적인 측면에서의 특정가능성은 원천적으로 없는 것이다.[15] 결국 수사관은 필자의 모든 야동파일과 모든 이메일파일을 재조합한 후, 범죄와 관련 있는 이메일을 다시금 선별하는 과정을 거치게 된다. 심각한 기본권침해의 현장이라 아니할 수 없다.

만약 KT가 수집된 필자의 패킷의 사본을 실시간으로 수사관의 노트북으로 포워딩한다면 어떠할까? 그 수사관의 노트북에 인터넷을 통해 공짜로 다운로드 받을 수 있는 와이어샤크(Wireshark) 프로그램이 깔려 있다면, 필자의 노트북화면과 동일한 화면을 보는 것은 얼마든지 가능하다. 물론 국가정보원이 밝힌 바와 같이 공무집행으로 분주한 수사관들이 범죄와 관련 없는 사적인 패킷들을 재현하여 이를 감청할 우려가 크지는 않겠으나, 그것이 만약 유명 여배우의 야동패킷이라면 관심을 가져볼만 하지 않은가? 기우가 아니라, 이는 어디까지나 옵션일 뿐이다!

2. 특정불능으로 인한 포괄영장성

2.1. 스마트폰 이야기

요즘 모두들 하나씩 들고 다니는 스마트폰을 살펴보자. 스마트폰은 폰(Phone)이기 때문에 일견 전화기이다. 그러나 우리는 스마트폰을 전화기라고는 잘 호칭하지 않는다. 기실 스마트폰에서의 전화기능은 말

15) 국가정보원도 "현재 상용화된 기술로는 인터넷 회선 감청에서 감청의 대상자, 감청의 대상물을 사건에 관련된 것만으로 특정하는 것은 불가능"하다고 밝히고 있다. 정부법무공단, 앞의 글, 21-22쪽.

그대로 하나의 기능일 뿐이기 때문이다. 스마트폰은 CPU□메모리□네트워킹 장비□모니터□메인보드 등 컴퓨터의 하드웨어와 대동소이한 구성을 가지고 있으며, 그 성능에 있어서도 시시한 노트북을 압도하는 제품도 이미 출시되어 있다. 소프트웨어에 있어서도 iOS를 사용하는 아이폰에서 부터 안드로이드 계열과 윈도우 계열 등 많은 종류의 OS(Operating System)가 존재하고, 소위 '앱(App)'이라 불리우는 모바일 어플리케이션(Mobile Application)의 종류와 수는 이미 일반 컴퓨터용 응용프로그램을 추월하고 있다. 사용의 빈도에 있어서도 압도적이다. 컴퓨터를 켜서 채팅을 하던 시대는 이미 한물이 가버린 지 오래고, 강의 시간에 교수는 학생들의 '카톡질'을 다스리기 바쁜 세상이 온 것이다.

그 기능적인 측면을 종래의 회선(즉 채널)관념을 기준으로 생각해 보자. 일단 전화회선과 인터넷회선이 동시에 존재하므로 통신채널이 있고, 아홉시 뉴스나 라디오를 듣기도 하니 IPTV와 유사한 디지털 방송채널도 있다고 할 수 있으며, GPS위성과 연결되는 네비게이션 기능도 있고 자동차를 원격시동하는 리모콘용 '앱'도 있으니 전파채널도 있다고 해야 할 것이다. 현대인들의 손바닥 위에는 무수한 컴퓨팅 기능과 다양한 채널들이 동시에 담겨 있는 것이다. 만약 이 물건의 압수□수색을 위하여 발부되는 영장에다 "피의자 OOO의 스마트폰"이라고 기재하면 영장주의의 원리에 부합하는 특정이 이루어졌다고 평가해 볼 수 있을 것이다. 그러나 이 스마트폰을 패킷감청하기 위해 발부되는 통신제한조치 허가서상에는 그 문구를 어찌 작성해야 특정성을 담보할 수 있을까?

만약 현재의 영장상 표현처럼 '피의자 OOO의 스마트폰 회선감청'이라고 적는다면 이는 도대체 어느 채널을 감청하게 된다는 것인지 알 수가 없다! 보편적인 3G 스마트폰의 경우 음성통신과 데이터통신이 동시에 3G망을 통해 송수신되고 있고(KT와 SKT), 현재의 4G 서비스는 데이터통신은 LTE망을 사용하면서 음성통신은 2G망을 활용하고 있으나 조만간 기반공사가 끝나면 음성통신조차 LTE망으로 이사를 갈 예정이기 때문에 단순한 '회선'이라는 용어는 특정성이 없다. 한편 현명한 판사가 "오로지 피의자 OOO의 인터넷 회선감청"만을 적시한다면 어떠한가? 먼저 진정한 데이터통신 채널이라 할 수 있는 와이파이(WiFi)망이 그 대상이 되겠으나, 와이파이는 항상 사용가능한 것이 아니라 소위 와이파이존(WiFi-Zone)에 들어가야만 켜지게 된다는 점과 실시간으로 AP(Acess Point)가 변화된다는 속성으로 인해 회선자체를 특정하기가 매우 곤란하다. 더구나 무료 음성통화 앱인 바이버(Viber)나 올리버폰(Oliver Phone) 등을 사용하면서 와이파이존에 들어간다면, 음성통신이 데이터통신망을 이용하게 되어 채널관념이 혼재되어 버린다. 다음으로 3G 또는 4G 라인을 타고 들어오는 데이터 통신은 앞서 살핀 바와 같이 음성통신과 동일한 라인을 쓰게 되므로 여기에서도 특정성을 담보할 수 없다.

요컨대 현재의 패킷감청을 스마트폰에 집행하기 위해 영장에 기재해볼만한, 특정성이 담보되는 용어는 없다. 디지털 컨버전스(Digital Convergence) 시대를 맞아 물리적□관념적으로 독립된 회선(채널)개념이 이미 허물어져 버렸기 때문이다.

2.2. 포괄영장의 필연성

이러한 특정불능의 문제는 비단 스마트폰만의 문제는 아니다. '인터넷 회선'이라는 표현으로 포함되는 많은 종류의 기기들은 다 어찌할 것인가? PC나 노트북은 당연하다고 볼 수 있겠으나, 스마트폰이나 아이패드 또는 갤럭시 탭과 같은 태플릿 컴퓨터(Tablet Computer)□스마트TV나 IPTV 등의 디지털 가전□네트워킹이 가능한 차량용 네비게이션□인터넷 접속이 가능한 PMP나 이북리더(e-Book Reader) 기기(예를 들어 Amazone의 Kindle) 등 네트워킹이 가능한 수많은 디지털 기기들은 모두 그 대상이 되어야 할 것이다. 영장의 특정성을 위해 이 모든 기기들을 하나하나 나열할 것인가? 또한 이렇듯 다양한 기기들에 대한 전방위적 감청을 하나의 영장으로 허가한다는 것이 타당한 것인가도 중요한 논점이다.

나아가 이렇듯 다양한 기기에서 사용되는 각각의 프로그램들을 생각해 보라. 도대체 얼마나 많은 종류의 프로그램들이 얼마나 많은 기능을 제공하고 있을런지 정확한 계산을 해보기가 힘든 지경이다. 메일을

읽고, 영상을 보고, 전화를 하는 일반적인 기능에서부터, 버스요금을 결제하고 전자책(e-Book)을 구입하고 음원을 구매하는 쇼핑기능까지 디지털 기기가 제공하는 기능은 가히 끝이 없다고 할 것이다. 즉 디지털 시대를 살고 있는 오늘날의 인류는 디지털 그 자체가 삶인 것이다. 따라서 디지털 감청은 이를 통해 결국 그 삶 전체를 감청하는 것을 의미하는 것이고, 단순히 전화통화 내용을 엿듣는 시대에서의 감청과는 비교조차 불가능한 상황이다. 이렇듯 수많은 기능들 중에 범죄와 관련되는 것들을 선별하는 것이 가능이나 한 일인가? 또한 이를 미리 예측하여 영장에다 특정하여 기재한다는 것은 어떠한가? 아예 원천적으로 특정불능인 것이다!

요컨대 현재에 있어 패킷감청을 허하는 통신제한조치 허가서는 무조건 포괄영장일 수밖에 없고, 디지털 시대의 감청은 처참한 기본권 침해가 필연적으로 뒤따른다는 것이다.

Ⅲ. 규제필요성과 관련하여

패킷감청의 규제필요성과 관련하여서는 두 가지의 논의를 간략히 진행하기로 한다. 먼저 국가정보원의 첫째 논지에서처럼 DPI가 현재 주요한 보안기술로 사용되기 때문에 ① 기술적 중립성을 이유로 동일한 기술에 근거하고 있는 패킷감청 또한 법적으로 무방한 것인지를 살펴보아야 한다. 이는 다시 DPI 기술자체가 기본권 침해성을 가지고 있는 것인지, DPI 기술자체가 아니라 패킷감청만이 문제가 되는 것인지를 검토하여야 할 것이다.

다음으로 국가정보원의 다섯째 논지를 면밀하게 검토하여야 한다. 즉 ② 패킷감청을 통해 수집한 증거가 제출되지 않는 것이 최량증거의 원칙상 타당한 것인지를 고민해 보아야 한다. 이는 소위 디지털 증거와 관련한 문제인데, 현재 우리의 입법은 디지털 증거부문 전반에 관하여 입법의 부재로 인한 혼란의 상태에 있기 때문에 이 쟁점에 관한 분석은 매우 중요하고도 심각한 부분이라 할 수 있겠다.

1. 기술적 중립성 항변에 대한 검토

기술에 대하여 법제가 가져야 할 기본적인 태도가, 기술적 중립성을 견지한 시각으로 기술을 평가해야 함은 분명하다. 그러나 DPI와 같이 유익한 역할을 하는 동시에 침해적 요소를 가지는 복합적인 성격의 기술에 관하여, 기술적 중립성을 이유로 그 침해성을 부인할 수는 없는 것 또한 자명하다. 따라서 패킷감청의 침해성에 관한 논의에 있어 이를 기술적 중립성을 앞세워 덮어보고자 하는 국가정보원의 입론 자체가 비난의 여지가 있다는 점을 먼저 짚어두고 싶다.

다음으로 DPI 기술자체가 본질적으로 침해성을 가지는 것인지, 아니면 패킷감청만이 기본권 침해성을 가지는 것인지를 검토해야 할 것이다. 즉 기술적 중립성을 견지한 입장에서, 침해성의 여부를 기준으로 DPI를 객관적으로 분석해 보는 단계이다. 요즘 DPI는 네트워크의 곳곳에서 다양한 목적으로 맹활약 중에 있다. 패킷감청은 물론, 앞서 살핀 바와 같이 보안시스템 체계의 핵심요소로서 자리 잡고 있기도 하고, 인터넷 맞춤광고 기술로 변신하여 등장한 바도 있으며,[16] 최근 뜨거운 감자가 되고 있는 망중립성 논쟁의 범인이기도 하다. 필자가 지속적으로 관찰해 온 바에 의하면, DPI가 빚어내는 이 모든 작품활동에 있어서의 본질은 동일하다. 불특정 패킷에 대한 무차별적인 납치와 그 재조합을 통한 침해적 분석이 그것이다. 다시 말해 기본권 침해성의 문제는 패킷감청만 가지는 것이 아니라는 것이다. 결국 DPI의 본질적인 속성이 이미 기본권 침해성을 가지고 있는 것이고, 그 용도가 달라진다고 하여 침해성은 사라지지 않는

16) DPI 기술을 활용한 인터넷 맞춤광고의 위법성에 관한 상세는 오길영, 감청의 상업화와 그 위법성, 민주법학 제43호 (2010) 참조.

다. 즉 보안시스템으로 활용되는 DPI에서도 침해적인 절차가 존재하기는 마찬가지이다.

그러나 방화벽에서의 DPI와 패킷감청에서의 DPI, 이 양자에 대하여 동일한 법적 평가를 내릴 수는 없다. 왜냐하면 방화벽에서의 DPI는 분석의 대상이 되는 패킷의 내용에 대하여 인간의 가치판단이 투영될 여지가 없기 때문이다. 여기서의 DPI는 컴퓨터에 유해한 코드를 감별해내는 자동화된 시스템일 뿐인 것이다. 그러나 패킷감청에 있어서의 분석은 상황이 전혀 다르다. 가치판단이 필수적 요소이기 때문이다. 특히 범죄와 관련 있는 내용을 '색출'까지 해야 하므로, 모든 조합내용들을 통독한 이후에 유의미한 데이터만을 분류해내는 고도의 합목적적 가치판단 과정이 뒤따른다. 따라서 국가정보원의 논지와는 달리 양자의 법적 평가는 상이할 수밖에 없다.

이해의 편의를 위하여 유사한 예를 들어 보기로 한다. 과속차량 단속용 CCTV를 생각해 보자. 시속 100km 이상의 물체가 나타나면 무조건 플래쉬를 터뜨리게 프로그램 되어 있는 카메라를 향해 그 위법성을 비난하기란 그리 쉽지 않다. 그러나 동일한 카메라를 사용하여 어느 모니터링 요원이 도로가의 자동차에서 연출되고 있는 이름 모를 연인의 정사 장면을 감상하고 있다면 이는 분명한 위법행위이다. 당해 카메라가 과속단속용으로 사용된다는 항변이 이러한 감상행위의 위법성을 덮을 수는 없지 않는가?[17]

2. 패킷감청과 증거능력에 관한 검토

이 부분은 이메일에 관한 이야기로 시작하는 것이 좋겠다. 디지털 증거와 관련한 각종의 사건에서 가장 빈번히 등장하는 쟁점이기도 하고, 소위 사이버 망명으로 시끄러웠던 기억때문이기도 하다.

2.1. 이메일의 증거능력과 패킷감청

이메일이 증거능력을 가지는 일이 그리 쉬운 일이 아니다. 디지털 증거이기 때문에 복잡한 절차를 통과해야 한다.

범인의 이메일을 압수□수색하는 과정을 살펴보자. 먼저 범인이 사용하는 이메일 서비스 회사를 찾아가 영장을 제시하게 될 것이다. 이에 메일서버 관리자는 메일서버에서 범인의 이메일들을 관리자의 컴퓨터로 다운로드한 후 CD 등의 저장매체에 담아주게 된다. 이 과정에서 관리자는 반드시 당해 이메일의 해쉬값을 산출하여야 한다. 메일서버에서 내려 받은 이메일과 CD에 담아주는 이메일이 완전하게 동일함을 입증하여야 하기 때문이다. 즉 원본과 사본의 무결성을 담보하기 위하여 해쉬값을 산출하고, 그 결과를 별도의 파일에 기록하여 CD에 동봉해주거나 CD표면이나 서류 등에 기재를 하게 될 것이다. 여기까지가 압수에 해당한다. CD를 들고 간 수사관은 수사기관에 위치한 자신의 사무실에서 드디어 본격적인 수색을 시작한다. 범죄와 관련 있는 이메일만을 선별하는 과정을 거치는 것이다. 선별이 끝나면, 수사관은 다시금 메일서버 관리자를 찾아가 선별된 파일만을 담은 CD의 재제작을 요청하게 된다. 물론 이 두 번째의 CD도 동일한 이유로 해쉬값을 산출해야만 할 것이다. 통상 바로 이 CD가 법정에 증거로 제출된다. 법정에 도착한 CD는 가장 먼저 해쉬값의 검증을 받게 된다. 증거로 제출된 CD가 안전하게 보관되어 그 내용이 온전히 존재하는지의 검증과 메일서버 관리자가 제작□교부한 바로 그 CD가 제출되었는지를 검증하기 위해서이다. 그 방식으로 법정에서 산출된 해쉬값과 메일서버 관리자가 교부당시에 기재한 해쉬값의 비교를 하게 되는 것이다. 디지털 증거에 있어 이러한 완전성과 무결성에 대한 입증절차는 철칙이다. 이러한 기본적 검증의 이후에야 이메일 파일을 열어보는 본격적인 증거개시절차가 진행된다.

---

17) 이렇듯 그 법적 평가를 달리한다고 하여, 보안시스템에서 사용되는 DPI가 무조건 합법적이라는 것은 아니다. DPI 기술자체가 태생적 침해성을 가지고 있는 만큼, 보안시스템의 운용과정에서도 다른 기술에 비해 더 많은 위험이 상존한다고 할 수 있다. 이에 상응하는 규제가 필요함은 당연하다. 지면관계상 본고에서 이를 구체적으로 논의할 여유가 없으나 DPI 보안시스템을 운용하는 ISP 규제에 관한 상세는 박희영, DPI 기술의 운영과 ISP의 형사책임, Internet and Information Security 제2권 제1호(2011) 참조.

여기서 발생하는 증거법적인 문제는 크게 두가지이다. 첫째 실제 이메일의 압수□수색의 절차는 '압수→수색→압수'로 진행되는데 반해, 이에 관한 압수□수색영장은 통상 실무에서는 1회만 발부된다는 점이다. 즉 두 번째 CD의 압수는 영장 없이 집행된 압수로서 그 속에 담긴 이메일은 위법수집증거가 된다. 원천적으로 증거능력이 박탈될 가능성이 농후하다. 둘째 형사소송법 제123조의 '간수자 참여규정'이 문제가 된다. 본 규정에 의하면 메일서버 관리자는 압수와 수색의 절차에 지속적으로 참여해야 하는데, 앞서 살핀 예에서 보듯이 압수의 절차는 몰라도 수사기관의 사무실에서 진행되는 수색절차의 전반에 참여할 수 있는 현실적인 가능성이 희박하기 때문이다. 더구나 이는 현행법이 명시적으로 규정하고 있는 사항이므로, 이를 해석상으로 어찌해 볼 도리도 없다. 결국 종래의 유체물에 대한 압수□수색제도가 디지털 증거와 관련하여서는 이렇듯 해결할 수 없는 새로운 문제를 야기하고 있는 것이다.

결국 이메일의 압수□수색은 까다로운 디지털 증거능력의 획득절차를 거쳐야 함은 물론, 입법의 부재로 인한 혼란으로 항상 위법수집증거로서의 가능성을 내포하고 있는 상태인 것으로 요약해 볼 수 있다.

이에 반해 패킷감청으로 수집된 증거는, 이러한 장애물을 너무나도 쉽게 통과할 수 있는 장점을 가지고 있다. 본래 감청은 휘발성을 예정하고 있어 감청으로 지득한 내용의 원본을 상정하고 있지 않다. 따라서 감청으로 지득한 내용을 증거로 제출할 경우 원본과의 대조를 통한 검증을 필수코스이라 주장하기 어렵다. 또한 두 번의 압수에서와 같은 집행의 횟수로 그 유효성이 산정되는 형태가 아니라 감청가능한 시기만을 부여받는 것이므로, 감청기간 이내이기만 하면 몇 번의 감청을 집행하건 전혀 상관이 없다. 나아가 형사소송법 제123조의 간수자 참여규정의 적용도 배제된다. 압수□수색이 아니기 때문이다.

극적으로 대비되는 양자의 상황을 종합하면, 어떠한 결과를 예상할 수 있는가? 실제로는 이메일의 압수를 집행하여 획득한 증거들이, 패킷감청으로 지득□채록한 증거로 둔갑하여 법정에 제출되는 경우를 너무나도 쉽게 상상해볼 수 있다. 패킷감청 영장과 이메일의 압수□수색영장을 함께 발부받아 놓고, 영장의 발부시점 이후에 송수신된 모든 이메일 증거들을 패킷감청으로 수집했다고 주장한다면 이를 반박해낼 방도가 전무하기 때문이다. 즉 패킷감청이 디지털 증거절차의 도피처로 사용되는 셈인데, 이는 참으로 심각한 부분이 아닐 수 없다. 이러한 점을 고려한다면, 앞서 살핀 국가정보원의 다섯째의 논지에서처럼 패킷감청의 결과가 증거로 제출되지 않는 현실에 대한 논의가 쟁점이 될 수 없다. 오히려 패킷감청을 통해 수집한 증거의 증거능력 자체를 아예 폐기하는 것을 검토해야 옳다.

2.2. 외국계 이메일의 증거능력

누군가 외국계 이메일 서비스를 사용한다면, 수사기관은 난감하기 그지없다. 외국계 이메일 회사가 수사에 협조하지 않음은 물론 그 이메일에 대한 압수□수색영장 발부한다고 하여도 발부의 시점에 이미 법원의 관할권이 없기 때문이다. 결국 외국계 이메일을 열어보기 위해서는 패킷감청만이 유일한 대안이라는 국가정보원의 표현은 틀린 말이 아니다. 그러나 국내의 사법권이 미치지 못하는 영역에 대하여 수사를 의욕하는 것 자체가 어쩌면 타당하지 못한 발상일지도 모른다. 또한 디지털 증거라는 측면에서는 더욱 많은 문제가 발생한다.

만약 패킷감청으로 입수된 외국계 이메일이 증거로 제출되었다고 가정해보자. 이러한 이메일의 가장 심각한 문제점은, 그 원본과의 대조가 영구적으로 불가능하다는 점이다. 외국계 메일서버의 관리자는 국내 법원이 발부한 영장에 협조하지 않는다. 따라서 원본이 보관되어 있는 외국의 메일서버에 접근권한이 있는 관리자는 패킷감청을 통해 입수한 당해 이메일과 그 원본과의 대조를 위한 일련의 작업을 진행하지 않을 것이다. 따라서 국가정보원이 다섯째 논지에서 밝힌 메일서버에 원본이 보관되어 있는 국내 이메일의 경우에서처럼, 최량증거의 원칙을 논해볼만한 여지가 없다. 원천적으로 증거능력이 없는 이메일을 애써 수집한 셈인 것이다.

또한 그 ID의 주인이 구체적으로 누구인지 확정할 수 없다는 심각한 문제에 부딪히게 된다. 왜냐하면

현재 인터넷 실명제를 실시하는 국가는 이 지구상에서 대한민국이 유일하므로, 외국계 이메일의 경우 서비스 가입시에 우리처럼 주민등록번호를 입력하지 않아도 되기 때문이다. 또한 우리나라의 경우처럼 거의 완벽한 주민등록체제를 가지고 있는 나라가 없기 때문에, ID의 조회로 특정인을 변별해 내는 것을 염두에 두고 메일서비스를 운용하는 경우도 찾아볼 수 없다. 결국 외국계 이메일의 ID 조회를 통해 현실에서의 특정인의 신원을 바로 알아내는 것은 불가능하므로, 당해 이메일의 작성자를 법정에서 확인하는 것이 불가능하다.

Ⅳ. 나오며

지금까지 DPI 기술과 패킷감청에 대하여 특정의 가능성과 규제의 필요성을 중심으로 살펴보았다. 검토의 결과를 종합해보자면, 기술적□논리적으로 대상자와 대상물의 특정이 원천적으로 불가능하여 포괄영장의 발부가 필연적이고, DPI 기술자체가 태생적으로 기본권 침해성을 함유하고 있어 엄중한 규제가 절실하다고 요약해 볼 수 있다. 이를 다시 한마디로 요약한다면, '패킷감청은 위헌이다' 정도가 적절할 것이다. 심각한 기본권 침해성을 인정하지 않을 수 없으나, 이에 반해 포괄영장을 방지할 방안도 폐해를 방지할 실효적인 규제책도 전혀 떠오르지 않기 때문이다.

이러한 필자의 입장에 대하여 국가정보원은 다섯 가지의 논지를 제시하며 그 합헌성을 주장해온 바 있다. 본고에서의 검토를 기반으로 국가정보원이 밝힌 각각의 논지를 최종적으로 반박하면서 결론을 갈음하고자 한다. 합헌이라는 주장에 대한 반박이므로 이는 곧 위헌성의 입증이 아니겠는가?

1. 기술적 중립성의 견지에서 볼 때, 방화벽에 사용되는 DPI가 위헌성이 없으므로 패킷감청도 위헌성이 없다는 첫째의 논지에 관한 반박은 다음과 같다. DPI는 어떠한 형태로 사용되건 태생적으로 기본권 침해성을 가지고 있어 엄격한 규제가 필요함은 동일하나, 보안시스템에서의 DPI와 패킷감청에서의 DPI는 구체적인 분석행위(Inspection) 단계에 있어 그 법적 평가를 달리할 수 있으므로 이러한 논지는 이유 없다.

2. 인터넷 등의 디지털 공간이 범죄에 활용되고 있으며, 사이버 망명 등을 통한 증거인멸에 대처하기 위해 패킷감청이 불가피하다는 둘째의 논지에 관한 반박은 다음과 같다. 디지털 공간이 점점 복잡다단해지고 있어 수사상의 어려움은 충분히 공감할 수 있으나 이러한 현상은 본격적인 디지털 시대인 지금에 와서는 너무나 당연한 것이고, 사이버 망명을 통한 증거인멸은 이미 우리 사법권의 관할이 미치지 못하는 영역임은 물론 원천적으로 증거능력이 배제되므로 이러한 논지도 이유 없다.

3. 패킷감청은 대상자와 회선의 특정을 통해 제3자에 대한 침해가능성이 없고, 실시간으로 대상자의 컴퓨터 화면과 똑같은 화면을 보면서 모든 내용을 감청한다는 것이 터무니없다는 셋째의 논지에 관한 반박은 다음과 같다. 우선 디지털 포렌식 수사의 본고장이라 불리우는 우리네 국가정보원의 기술친화도가 이 정도의 수준 밖에 안되는 것이었는지 실망이 크다고 말해주고 싶다. 다음 패킷감청 기술의 속성은 원천적으로 '특정불능'임을 똑바로 말해주면서, 감청대상자와 실시간으로 공감하고 싶다면 필자가 시키는 대로 프리웨어인 '와어이샤크'를 다운로드 해보라고 권하고 싶다.

4. 특정 회선에 대한 한 장의 통신제한조치 허가서로 통신사실확인자료는 물론 인터넷 전화의 감청까지도 가능한데 반해, 실제 수사에 있어서는 인터넷 전화를 위한 별도의 영장을 발부받아 집행하고 있다는 넷째의 논지에 대해서는 일단 "대단히 감사하다"고 말하고 싶다. 먼저 회선감청의 속성상 인터넷 전화와 디지털 통신을 구분할 수 없는데도 불구하고 별도의 영장을 발부받아 적법절차를 준수하고 있는 국가정보원에 대하여, 법학을 전공한 학자로서 감사의 말씀을 전하고 싶다. 또한 이렇듯 회선자체에 대한 패킷감청이 채널을 특정하여 진행될 수 없음을 스스로 밝혀주어 감사하기도 하다. 특정불능의 속성과 포괄영

장성을 고백한 셈인 것이다.

5. 패킷감청으로 수집한 정보를 증거로 제출□활용하지 않음에 대하여, 원본에 해당하는 증거가 메일서버 등에 결국 보관되게 되므로 압수□수색을 집행하여 최량의 증거를 제출한다는 다섯째의 논지에 관하여는 다음과 같은 주의를 주고 싶다. 디지털 증거의 특성이 불러오는 새로운 문제들에 대하여 아직 제대로 대처가능한 입법이 없는 상태에서, 패킷감청이 디지털 증거능력에 관한 까다로운 절차를 우회하는 도피처로 악용되어서는 안 된다는 것이 그것이다. 이러한 경우를 방지하기 위해 패킷감청을 통해 수집한 증거의 증거능력 자체를 아예 폐기하는 것이 타당하므로, 지금부터라도 패킷감청의 실시를 중단하라고 말하고 싶다. 국가정보원이 밝히고 있듯 패킷감청을 통한 증거는 최량의 증거도 아니지 않은가?

[토론문]

유성 (인권운동사랑방 활동가)

주의: 이 글은 컴퓨터 보안을 전공하거나 관련 경력을 가지지 않은, 컴퓨터 학사 수준의 일반적인 이해를 갖춘 사람이 썼습니다. 부정확하거나 시대에 뒤떨어지거나, 잘못된 내용이 있을 수 있습니다.

인터넷 및 컴퓨터 네트워크 체계에 대한 간략한 이해

물리계층 - 데이터 링크계층 - IP 계층(네트워크 계층) - TCP 계층(네트워크 계층) - 응용계층

물리 계층은 구리/광케이블이나 무선 전파와 같은 실제 물리적 신호를 전달하는 계층이며, 데이터 링크 계층은 적절한 규약에 따라 아래에 있는 물리 계층과 상호 작용하여 데이터를 송수신한다. 흔히 랜, 와이파이라고 불리는 규약들이 여기에 속한다.

IP(Internet Protocol) 계층은 상위 계층으로부터 받은 데이터를 패킷으로 분할, 송수신 주소(IP주소)를 덧붙여 아래의 데이터 링크 계층으로 전달하거나, 데이터 링크 계층으로부터 수신한 패킷을 다시 재조립하여 상위 계층으로 전달한다. 인터넷 망 사업자의 통신 장비(라우터 등)은 이 패킷들을 패킷에 적힌 목적지 주소(IP주소)에 따라 전달에 전달을 거듭, 최종적으로 목적지 주소를 가진 호스트(컴퓨터)로 전달한다.

TCP 계층은 OSI 모델의 트랜스포트 계층에 해당하며, 연결(Connection)이라는 가상적인 회선을 만드는 역할을 담당한다. 이 계층을 통해 여러 응용 프로그램들이 하나의 물리적인 회선을 사용하면서도 여러 호스트(컴퓨터)와 통신할 수 있게 된다. TCP 계층은 상위 계층에게 특정 목적지로의 가상적인 회선을 배정해주며, 이 회선에 입력된 데이터를 목적지 주소와 함께 아래 IP 계층에 전달한다.

응용 계층은 아래의 TCP 계층으로부터 목적지 주소가 명시된 가상적인 회선, 즉 연결(Connection)을 배정받는다. 응용 프로그램이 이 가상적인 회선에 데이터를 전달하면, TCP 계층은 이 데이터를 목적지 주소와 함께 아래의 IP 계층에 전달하며, IP 계층은 이 데이터를 패킷이라는 작은 단위로 분할, 각 패킷에 목적지 주소를 붙여 아래의 데이터 링크/물리 계층으로 전달한다. 데이터 링크/물리 계층은 이 데이터를 전기 등의 물리적 신호로 변환하여 케이블/무선 전파 등의 물리 매체를 통해 송수신한다.

이러한 과정을 통해 웹브라우저, 이메일 프로그램, 메신저 프로그램, 인터넷 전화 등은 하나의 물리적 회선을 사용하면서도, 여러 원격지에서 실행 중인 여러 프로그램들과 복수의 가상 회선을 맺고 데이터를 교환할 수 있다.

인터넷의 진화와 DPI (Deep Packet Inspection)

OSI와 인터넷(TCP/IP)의 모델은 인터넷 망 사업자가 물리 계층 ~ 네트워크 계층만을 담당할 것을 염두에 둔 설계이다. 이 모델에 충실하자면, 망 사업자의 네트워크 장비(라우터 등)는 인터넷 가입자의 호스트(컴퓨터)로부터 물리적 신호를 수신하면, IP 계층에 해당하는 데이터(IP 헤더)까지만 해석하여 패킷의 목적지 주소를 확인한 뒤, 해당 IP 주소 대역을 담당하는 다른 망 사업자의 장비로 전달하기만 하면 된다. 이는 OSI 모델이 정의한 각 계층들의 역할분담에 따른 것이며, 망 사업자의 장비가 그 이상

의 계층에서 담당하는 데이터를 해석하는 것은 그만큼 불필요한 장비 성능(CPU)의 낭비이기도 했다. 인터넷 초창기에 네트워크 장비들은 이러한 역할에만 충실한 편이었다.

그러나 인터넷이 발전하고 다양한 응용과 요구사항들을 충족할 필요가 생기고, 또한 네트워크 장비들이 고성능화됨에 따라 망 사업자의 장비도 네트워크 계층(IP 계층)보다 위의 계층에 해당하는 데이터까지 해석하게 되었다. 가령 일반 가정에 인터넷 회선을 제공하는 망 사업자들은 일반 가정에서 인터넷 서버를 작동하는 것을 방해하기 위해 속칭 "포트 막기"를 하고 있는데, 이를 위해 망 사업자의 장비들은 트랜스포트 계층(TCP 계층)의 데이터까지 해석해야만 한다. 그 외에 스팸/바이러스 등을 걸러내는 용도로도 사용되는데, 이렇게 망 사업자의 네트워크 장비가 트랜스포트 계층까지 개입하는 것을 보통 옅은 패킷 분석 (shallow packet inspection)이라고 부른다.

그런데 인터넷의 발전에 따라 더욱 고도화된 필요들이 발생하고 네트워크 장비들의 성능이 그만큼 발전함에 따라, 네트워크 장비들이 그보다 더 상위의 응용 계층의 데이터까지 해석할 수 있게 되었는데, 이를 Deep Packet Inspection이라 부른다.

그런데 Shallow/Deep Packet Inspection의 구분은 OSI 모델의 어느 계층까지 개입하느냐에 따라 개념적으로는 명확히 구분되기는 하지만, 사실 기술적 필요라는 측면에서 바라보면 shallow packet inspection에서 deep packet inspection으로의 발전은 자연스러운 면이 있다. 가령 컴퓨터 바이러스 등 컴퓨터 시스템에 대한 불법적 침입 기법 등이 고도로 발전함에 따라, 더이상 shallow packet inspection만으로는 효과적인 방어가 어려울 수 있기 때문이다. 앞서 예를 든 QoS 역시 마찬가지이며, 이런 종류의 필요들은 컴퓨터 시스템과 인터넷이 진화함에 따라 더욱 확장/강화될 수 있다.

다만 이러한 DPI 기술이 발전함에 따라, 이를 활용하여 망중립성을 침해하는 응용을 사용하려는 욕구까지도 강화되고 있다. 응용 계층에 해당하는 HTTP(웹) 데이터를 분석하여 웹페이지에 망 사업자의 임의로 키워드 광고를 삽입하거나, 무선 망에서 인터넷 전화 서비스를 제한하거나 하는 일들이 그런 예이다.

국가 기구 또한 검열과 감시 목적으로 DPI를 사용할 수 있다. 도메인 주소보다 더욱 세밀한 기준으로 검열/차단하는 것도 가능해졌다(2mb18noma 트위터 계정 차단은 DPI를 활용한 것이다) 또한 DPI를 통해 특정한 서비스(예: 인터넷 전화)에 사용되는 통신만을 골라내어 감청/채록하는 것도 가능할 것이다.

패킷 감청(인터넷 회선 감청)과 음성 회선 감청의 차이점

패킷 감청은 하나의 물리적 회선을 통채로 감청한다는 점에서 음성 회선 감청과 동일하다고 볼 수 있다. 그러나 음성 회선은 기껏해야 한 두 개의 응용(음성통화 및 팩스, 모뎀 통신)에 활용될 뿐이지만, 인터넷 회선에는 수십~수백 개의 가상 회선을 통해 사실상 무한한 종류의 응용이 실린다는 점에서, 감청되었을 때 제한되는 기본권의 폭이 다르다.

가령 인터넷 메일은 실세계의 우편에 상응하며, 인터넷 전화는 유무선 음성 전화에 해당될 것이다. 그런데 우편물 검열이나 음성 전화 감청에 대해선 법원이 각각 그 필요성을 따로 심사하여 별개의 영장을 발부하는데 반해, 패킷 감청의 경우 이를 구분하지 않고 하나의 영장으로 포괄적인 감시가 가능해진다는 점을 주목해볼 수 있을 것이다. 인터넷에 구현될 수 있는 응용이 사실상 무한대라는 것을 감안하면, 패킷 감청으로 제한되는 기본권의 폭은 유선 감청에 비할 바가 아니다.

다만 이 경우 각각의 "응용"에 대해 별개의 영장 발부/감청이 이루어져야 한다고 주장하게 되면, 이는 사실상 DPI를 전제로 하게 된다는 점도 유의해야 한다. 또한 인터넷에 구현될 수 있는 응용의 종류가 사실상 무한대라는 점 역시 각 응용에 대한 개별적 심사가 필요하다는 주장에 반대 논리로 활용될 수 있을 것이다.

SSL 개요

인터넷은 본질상 통신 과정에서 데이터가 수많은 망과 호스트(컴퓨터, 네트워크 장비)를 거치게 되므로, 기본적으로 데이터의 기밀성과 통합성(integrity)가 보장되지 않는다. A → B로 가는 데이터를 중간에 누군가 엿들을 수도, 가로챌 수도, 위조하는 것도 가능하다. A와 B는 서로 송수신한 데이터를 누군가 제3자가 엿들었는지 여부를 알 수 없으며, B는 자기가 수신한 데이터가 정말로 A가 송신한 것인지 확신할 수 없다.

따라서 인터넷에서 송신자와 수신자 간 end-to-end 통신의 기밀성과 통합성을 보장하기 위해 SSL이라는 기술이 널리 활용되고 있다.

이 SSL 기술은 인터넷 뱅킹이나 인터넷 쇼핑 결제, 포털의 로그인 등에 거의 필수적으로 사용되어왔으며, 최근에는 그 활용이 더욱 늘어나고 있다. 대표적으로 GMail은 메일을 열람과 발신에 기본적으로 SSL 기술을 사용하고 있어, 세계적으로 불법적인 도청이나 국가 기관들의 감청을 피하려는 사람들에게 많이 사용되고 있다.

SSL의 작동 방식

SSL은 기본적으로 디지털 서명(digital signature, 이하 "도장"), 데이터 암호화(encryption)라는 암호학적 연산을 사용하며, 디지털 서명을 이용한 디지털 인증서(digital certificate, 이하 "인증서")를 통해 이를 검증한다. (이론적으로 디지털 서명과 데이터 암호화는 위조하거나 적절한 비밀키 없이 해독하는데 무척 긴 시간이 걸린다.)

SSL의 작동 방식을 웹브라우저의 예를 들어 살펴보면 다음과 같다(쉬운 이해를 위해 유추적으로 기술하였으며, 실제 과정은 훨씬 더 복잡하다) :

1. 웹브라우저들은 널리 믿을만하다고 여겨지는 최상위 인증기관(CA, Certificate Authrity)들이 발급한 최상위 인증서를 탑재하고 있다. 이 인증서들에는 각 인증기관들을 나타내는 도장이 찍혀있다. 이 디지털 "도장"들은 위조가 매우 어렵다.
2. B는 임의로 자기 도장을 만든 뒤, 자기 도메인 주소가 적힌 문서에 그 도장을 찍은 후, 최상위 인증기관에게 인감 증명을 받는다. 즉 이 인증서에는 해당 도메인 주소와 그 도메인 주소 소유자의 도장, 그리고 이를 보증하는 최장위 인증기관의 도장이 찍힌다.
3. A의 웹브라우저가 B의 웹사이트인 https://google.com[1]에 접속하면, B의 웹서버는 인감 증명을 A에게 전송한다.
4. B의 인감증명을 수신한 A의 웹브라우저는 거기에 찍혀 있는 최상위 인증기관의 도장과, 자신이 미리 보유하고 있는 최상위 인증기관들의 도장들을 대조한다. 만약 인증기관의 도장이 동일하면, A는 인증서에 찍혀 있는 B의 도장이 실제 B의 도장임을 믿을 수 있다.
5. 이후 B의 웹서버는 A에게 데이터를 전송할 때마다 데이터를 암호화(encryption)하고, B 자

1 HTTPS 는 HTTP와 동일하되, 그냥 TCP 연결이 아니라 SSL로 보호되는 연결을 사용한다.

신의 도장을 찍어서 전송한다. 3에서 A는 그 도장이 실제 B의 것임을 확인하였으므로, 수신한 데이터가 정말로 B가 보낸 것임을 알 수 있다.

인터넷 상으로 금전 거래, 개인 정보 등 민감한 정보들이 교환되는 것이 늘어나는 것에 비례해서, 인증기관/인증서 등의 근본 인프라가 신뢰할만하게/투명하게 구축/유지되는 것은 정보 인권 측면에서 매우 중요하다.

위조 인증서와 SSL 감청

SSL은 완벽하지 않다. 모든 컴퓨터 시스템이 그렇듯이, SSL 역시 취약점을 갖고 있으며, 학계와 업계에서는 SSL과 그것이 기반한 암호학적 연산들의 취약점에 대해 연구하고 있다. 그동안 SSL에 대한 이론적인 공격 방법들은 몇 차례 소개된 바 있으며, "연구실" 조건에서는 실제로 성공한 적도 있다.

그런데 작년에는 두차례 실제로 SSL 감청이 이루어졌다는 증거가 이란에서 발견된 바 있다.[2] 이는 MITM(man-in-the-middle) 공격의 일종으로, 최상위 인증기관으로부터 발급된 가짜 인증서를 활용한 공격 방식이다. 가짜 인증서를 소유한 공격자는 웹브라우져와 웹서버 사이의 로그인 암호 및 거래 정보를 포함한 모든 데이터를 실시간으로 획득할 수 있다. 사람들은 이러한 위조 인증서가 이란 정부가 자국민들의 인터넷 사용을 감시하는데 사용된 것이라고 믿는다.

국가 기관에 의한 이러한 종류의 공격(위조 인증서를 사용한 SSL 감청)이 가능하다는 또다른 정황 증거 중 하나는, SSL 감청을 전문적으로 하는 장비가 판매되고 있다는 사실이다[3]. 2010년에 인터넷 매거진 WIRED지는 위조된 인증서를 사용하여 SSL을 감청하는 장비가 실제로 미 연방정부에 판매되고 있으며, 이 장비를 만든 회사는 미주 지역 국가 감청 기관원들을 상대로 하는 국제 Intelligent Support Systems 컨퍼런스[4]에서 이 장비를 홍보 되었다고 보도한 바 있다.

"To use the Packet Forensics box, a law enforcement or intelligence agency would have to install it inside an ISP, and persuade one of the Certificate Authorities — using money, blackmail or legal process — to issue a fake certificate for the targeted website. Then they could capture your username and password, and be able to see whatever transactions you make online."

SSL의 암호화나 서명 그 자체를 뚫는 것은 쉬운 일이 아니라는 것이 수학적으로 증명되어 있기 때문에, 현재로서 국가기관에 의한 SSL 감청이 일어난다면 이러한 위조된 증명서를 사용했을 가능성이 높다고 봐야 한다.

그런데 국가 기관이 위조 인증서를 사용하는 것은, 마치 국가 기관이 위조된 인감 증명을 사용하는 것과 비슷하게 심각한 일로 볼 수 있다. 인감 증명이 사인 간 계약 등의 신뢰성을 뒷받침하는 근본적인 토대인 것처럼, 인터넷 상에서 SSL 인증서는 신뢰성 있는 데이터 교환에 가장 기초가 되는 요소이기 때

2 http://www.telegraph.co.uk/technology/google/8730785/Google-users-targeted-by-forged-security-certificate.html 최상위 인증기관 DigiNotar와 Comodo로부터 발급된 위조된 인증서가 실제로 이란에서 사용되었다. 디지털 인권 그룹 EFF재단(샌프란시스코 소재)는 이 사건이 SSL과 인증서를 발급하는 인증기관들에 근본적인 문제가 있음을 보여준다고 말했다. "The Electronic Frontier Foundation, a digital rights group based in San Francisco, said the incident demonstrated fundamental problems with SSL and the dozens of authorities such as DigiNotar that are trusted to issue certificates."

3 http://www.wired.com/threatlevel/2010/03/packet-forensics/

4 http://www.issworldtraining.com/ISS_WASH/

문이다.

가정에 가정을 거듭한 것일 뿐이긴 하지만, 국정원은 최근 버젼의 MS 인터넷 익스플로러에 최상위 인증기관으로 등록되어 있는 KISA를 통해 위조 인증서를 발급받는다면, 사실상 국내 대부분의 인터넷 사용자들을 감청할 수 있다고 보아야 한다.

그러나 현재 국내 제도 중에 국정원이 감청을 하는데 이런 종류의 탈법적인 수단을 동원하는지를 감시할만한 수단이 마련되어 있는지는 의문이다.