【전선】

인터넷 감청과 DPI(Deep Packet Inspection)*

오길영
배재대 강사, 전자상거래법
eclaw@daum.net

<국문초록>

현재 우리의 통신비밀보호법은 그 대상에 있어 아날로그 매체와 디지털 매체를 포괄하여 규제하고 있다. 그러나 매체의 형태와 특성이 전혀 다른 이들을, 동일한 입법하에 동일한 방식으로 규제하고 있는 현재의 규제방식은 전혀 타당하지 못하다.

이 글은 이러한 통신비밀보호법의 규제방식에 대한 문제점을 크게 두 가지 차원에서 논증하고자 하였다.

먼저 송·수신이 완료된 이메일 등의 '저장 데이터'의 경우, 디지털 매체에 있어 '송·수신의 완료 여부'라는 기준이 무의미하다는 점과 송·수신 '완료의 여부'가 불명확하다는 점, 대상메일의 특정가능성이 희박하다는 점, 하드웨어 자체의 압수일 경우 항상 포괄영장의 우려를 안고 있다는 점 등의 쟁점 검토를 통하여 현재의 규제방식이 가지고 있는 한계를 밝힌다.

다음으로 패킷 감청이라 칭해지고 있는 DPI 감청에 대하여, DPI에 대한 기술적 의미와 국제적 규제동향 등에 대한 개괄적 바탕위에 그 적용법규의 모호성과 감청대상의 포괄성을 주요쟁점으로 하여 새로운 입법의 필요성을 강조하고자 하였다.

이러한 검토의 결과로써, 아날로그 감청과 디지털 감청은 그 본질과 내용에 있어 전혀 다르다는 점, 감청의 대상이 되는 '패킷 데이터'와 압수·수색의 대상이 되는 '저장 데이터'가 완전히 동일하다는 점 등을 밝히고, 결국 디지털의 속성에 걸맞는 새로운 전담입법의 필요성을 주장하고자 함이 이 글의 결론이다.

주제어: 통신비밀보호법, 인터넷 감청, 저장 데이터, 패킷 감청, DPI, SPI

* 심사위원: 이호중, 최관호, 최정학
투고일: 2009. 9. 15. 심사개시: 2009. 9. 15. 게재확정: 2009. 10. 15.

< 차 례 >

Ⅰ. 들어가며
Ⅱ. '저장 데이터'의 문제
Ⅲ. 'DPI'의 문제
Ⅳ. 나오며

Ⅰ. 들어가며

통신비밀보호법 개정안을 두고 아직도 논란이 뜨겁다.[1] 개인적으로는 2007년 당시 개정안을 비판하는 글[2]을 쓰면서부터 지금까지, 근 2년여 동안의 길고도 지루한 설전을 관전하여 온 셈이다. 몇 번의 실랑이를 거쳐 다듬어진 여당의 최신 개정안[3]을 살펴보아도 그 내용의 부당함과 문제의 심각성은 변함이 없다. 심각한 문제점으로 지적하였던 주요 쟁점사항들은 부동의 입지를 고수하고 있으며, 이렇듯 줄기차게 개악을 도모하고 있는 것을 보면, 혹시나 지난번 '미디어법 사태'에서처럼 불도저식 덤핑처리를 기대하고 있는 것은 아닌지 심히 걱정이 되기도 한다.

이러한 2년여 동안의 회고 속에서 한 가지 유의미한 사실은, 인터넷 감청과 관련한 일련의 사건들이 쟁점화되어 이에 대한 통신비밀보호법의 허점이 알려졌다는 것이다. 검찰이 주경복 전 서울시교육감 후보의 선거법 위반 사건을 수사하면서 수사 대상자 100여명의 7년간 전자우편을 통째로 압수해 열어 본 사건[4]과, 광우병 보도관련 수사에서 MBC PD수첩

1) 서울신문, "[입법전쟁 5대 뇌관] 통신비밀보호법", 2009.9.9자, <http://www.seoul.co.kr/news/newsView.php?id=20090909005010>, 검색일: 2009.9.10.

2) 오길영, "통신비밀보호법 개정안 비판", 민주법학 제34호(민주주의법학연구회, 2007. 9).

3) 통신비밀보호법 일부개정법률안, 이한성의원 대표발의, 2008.10.30. <http://pds13.egloos.com/pds/200901/09/11/1801650.pdf>, 검색일: 2009.9.10.

4) 한겨레신문, "검찰, '주경복 이메일' 7년치 통째 뒤져", 2009.4.24자, <http://www.hani.co.kr/arti/society/society_general/351489.html>, 검색일: 2009.9.10.

김은희 작가의 이메일을 압수·수색하고 사적인 내용을 공개한 사건[5]이 있었다. 이렇듯 통신비밀보호법의 우려와 감청의 문제점이 현실로 드러나자, 많은 네티즌들은 이에 대한 비판과 질책을 아끼지 않았다. 심지어 이메일의 계정을 '구글' 등의 외국 서버로 옮기는 소위 '사이버 망명'을 한다는 이야기[6]까지 나왔다.

이에 대하여 언론과 정치권은 즉각적인 반응을 보였다.[7] 야당은 이메일 등의 송수신이 완료된 전기통신에 대하여 통신비밀보호법이 아니라 형사소송법상의 압수·수색에 의해야 함을 명문으로 규정하는 것을 주요한 내용으로 하는 통신비밀보호법 개정안[8]을 마련하여 이를 통과시킨 바 있으며, 이에 더하여 이메일의 압수·수색 요건을 강화하는 것을 내용으로 하는 형사소송법 개정안[9]도 마련하였다.

그러나 이러한 인터넷 감청관련 논란은 여기서 끝나지 않았다. 이번에는 하드디스크에 저장된 이메일에 대한 압수·수색이 아니라, 아예 네트워크 회선에서 실시간 감청을 하는 신기술인 패킷 감청(Deep Packet Inspection, 이하 DPI) 문제가 또다시 수면위로 떠올랐다.[10]

---

5) 한겨레신문, "검찰, 'PD수첩 작가 이메일 내용' 수천명에 공개 발송", 2009.6.18자, <http://www.hani.co.kr/arti/society/society_general/361175.html>, 검색일: 2009.9.10.

6) 한겨레신문, "[유레카] 사이버 망명", 2009.8.4자, <http://www.hani.co.kr/arti/opinion/column/369454.html>, 검색일: 2009.9.1.; 한겨레21, "누가 한국 이메일을 믿겠나", 2009.7.21자, <http://h21.hani.co.kr/arti/special/special_general/25402.html>, 검색일: 2009.9.10.

7) MBC TV, "이메일 압수수색 제한법 제출", 2009.6.23자, <http://news.naver.com/main/read.nhn?mode=LPOD&mid=tvh&oid=214&aid=0000109022>, 검색일: 2009.9.10.; MBC TV, "통보없이 '이메일' 압수수색 '3300여 건' 인권침해 논란", 2008.10.11자, <http://news.naver.com/tv/read.php?mode=LOD&office_id=214&article_id=0000082823>, 검색일: 2009.9.10. 등.

8) 통신비밀보호법 일부개정법률안, 박영선의원 대표발의, 2008.11.11. <http://pds12.egloos.com/pds/200901/09/11/1801881.pdf>, 검색일: 2009.9.10.

9) 형사소송법 일부개정법률안, 박영선의원 대표발의, 2009.6.23. <http://likms.assembly.go.kr/filegate/servlet/FileGate?bookId=8501AA77-9A48-E839-C996-7EA13FE27BFC&type=1>, 검색일: 2009.9.10.

10) 한겨레신문, "국정원, 우리집 인터넷 통째로 엿봤다", 2009.8.31자, <http://www.

이러한 보도를 접하면서, 참으로 수단과 방법을 가리지 않는 국정원과 검찰의 끈질긴 감청 노력에 혀를 내두르기도 했으나, 다른 한편으로는 정말이지 우리나라의 IT기술이 세계 최고 수준임을 새삼 깨닫게 되었다. 왜냐하면 DPI 기술을 통해 수사 목적의 감청을 해내었다는 공식 보도는 전세계적으로도 전무후무하기 때문이다.

지금까지의 수사관행과는 달리 비교적 평범한 수사에 있어 이렇듯 굳이 새로운 기술을 활용한 이유는 무엇일까? 이는 아마도 이메일에 대한 압수·수색의 논란을 피하는 동시에 통신비밀보호법의 허점을 이용하여 방대한 자료를 비교적 손쉽게 수집할 수 있기 때문인 것으로 판단된다. 즉 하드디스크를 통째로 압수·수색하거나, 망라된 기간과 범위로 영장을 발부받기가 이전처럼 그리 쉽지 않은 모양이다.

이러한 상황을 배경으로 본 논문은 작성되었다. 인터넷 감청과 관련하여 '이메일 등의 저장데이터'에 대하여 진행되고 있는 현재의 논의들을 정리·분석해 보고, 나아가 소위 패킷 감청으로 불리는 새로운 DPI 기술과 이로 인해 예상되는 문제점을 짚어보는 것을 주요한 내용으로 하기로 한다.

Ⅱ. '저장 데이터'의 문제

1. 규정상의 내용

통신비밀보호법이 규정하고 있는 통신은 '우편물 및 전기통신'을 의미하고(동법 제2조 제1호), '이메일 등의 저장 데이터'와 관련하여 문제가 되는 '전기통신'에 대하여는 '전화·전자우편·회원제정보서비스·모사전

---

hani.co.kr/arti/society/rights/374120.html>, 검색일: 2009.9.10.; 한겨레21, "인터넷·전자우편 실시간 감청 시대", 2009.9.4자, <http://h21.hani.co.kr/arti/cover/cover_general/25658.html>, 검색일: 2009.9.10.; 아이뉴스21, "국정원 인터넷회선 패킷 감청 의혹제기", 2009.8.31자, <http://itnews.inews24.com/php/news_view.php?g_serial=439578&g_menu=020300&pay_news=0>, 검색일: 2009.9.10. 등.

송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것'이라고 규정하고 있다(동법 제2조 제3호).

이렇듯, 일반적인 대화를 시작으로 유선전화·팩스·무전기는 물론 휴대전화·인터넷으로 전달되는 각종의 정보(인터넷 전화를 통한 대화나 채팅)와 전자적 우편물(문자메시지나 이메일) 등 현재 존재하는 모든 통신매체들을 망라하여 무작위로 포섭하고 있는 이러한 입법태도가 문제이라는 점은 지난 원고에서 이미 밝힌 바 있다.[11]

또한 '이메일 등의 저장 데이터'와 관련하여서는, 동법이 2001년 개정에서 전자우편을 새로이 포함하면서 '컴퓨터 통신망을 통해서 메시지를 전송하는 것' 뿐만 아니라 '전송된' 메시지까지 포함하고 있어(동법 제2조 제9호) 통신 개념의 혼란을 가중하고 있다는 점 또한 지적한 바 있다.[12] 즉 법문에서의 전송을 수신인의 관점에서 '수취한'이라고 해석할 경우에는 '송·수신이 완료된 이메일'이나 '문자메시지'까지도 통신비밀보호법상의 '전자우편'에 해당되어 감청의 대상이 된다는 것이다.[13]

---

11) 오길영, 앞의 글, 378-381쪽. 필자는 미국의 입법례에서처럼, 전자적 매체만을 대상으로 하는 독립입법을 주장하였다.

12) 오길영, 앞의 글, 380쪽.

13) 현행법의 해석에 의한다면, 이는 감청허가서가 아니라 압수수색영장이 필요한 사안이라고 밝힌 바 있다(오길영, 앞의 글, 379쪽 각주 27). 그러나 이러한 논지를 오해하여 필자의 지난 원고가 마치 '이메일 등의 저장 데이터가 통신비밀보호법상의 감청의 대상이 된다'는 식으로 표현한 견해가 있다(류제성, "통신비밀보호법 개정안(이학재의원 대표발의, 의안번호 제5261호) 및 형사소송법 개정안(박영선의원 대표발의, 의안번호 제5246호)에 대한 검토", 송수신이 완료된 이메일 등 현대적 매체에 대한 통신비밀보호법제 토론회 발제문, 3-4쪽, <http://minbyun.org/?module=file&act=procFileDownload&file_srl=27905&sid=afba7dda73834ac619ad7e8f3f30bdc3>, 검색일: 2009.9.10). 동 견해는 이러한 오해에 뒤이어 이를 부정하면서 그 근거로 ① 통신비밀보호법 제2조 제7호 및 제5조 제2항의 규정의 해석상 그 대상이 송수신중인 통신에 국한됨을 전제하고 있다는 점, ② 통신비밀보호법 제6조 제4항 및 제7항의 해석상 송수신의 현재성이 요구된다는 점 등을 들고 있다. 그러나 필자의 당시 주장은 '송·수신이 완료된 저장 데이터의 경우 형사소송법상의 압수·수색의 대상이나 통신비밀보호법 제2조 제9호의 규정상의 표현이 모호하니 이를 시정해야 한다'는 것이었

이 점에 대하여 야당의 개정안은 당초 제3조 제4항을 신설하여 '송·수신이 완료된 전기통신의 내용을 지득·채록하기 위한 압수·수색·검증은 형사소송법의 규정에 의함'을 명시(개정안 제3조 제4항 신설)하려 하였으나[14] 이는 금번 개정[15]에 반영되지 못했고, '수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 그 처분을 한 날로부터 30일 이내에 서면으로 통지해야 함'을 규정한 제9조의3을 신설하는 정도에 그쳤다.

신설된 제9조의3 각 항의 법문이 "검사는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우"라고 하고 있어, 송·수신이 완료된 전기통신의 경우에 압수·수색·검증의 대상이 됨을 표현[16]하고 있기는 하다. 그러나 이러한 신설 규정으로 인해 해석상의 혼란이 말끔히 해결된 것은 아니다. 왜냐하면 제9조의3의 신설에도 불구하고 동법 제2조 제9호의 '전자우편'의 정의규정에서 '전송된 메시지'를 여전히 포함하고 있기 때문이다.[17] 즉 법문의 내용이 서로 모순되므로 제2조 제9호 규정의 손질이 있거나, 야당의 당초 개정안처럼 '송·수신이 완료된 전기통신'은 통신비밀보호법의 대상이 아님을 명시하는 것이 바람직하다.

한편 이를 뒷받침하는 형사소송법 개정안은 아직 통과되지 못하고 있

고 지금도 그 주장은 변함이 없음을 여기서 다시 한번 밝힌다.

14) 통신비밀보호법 일부개정법률안, 박영선의원 대표발의, 2008.11.11, 1쪽.

15) 통신비밀보호법, 제15차 일부개정 2009.5.28. 법률 제9752호.

16) 법문의 내용을 엄격히 해석하자면, 당해 압수·수색·검증이 형사소송법의 제113조에 의한 압수·수색·검증인지는 불분명하다. 이는 당초 개정안 제3조 제4항에서 '형사소송법의 규정에 의함'이라고 명시하려 했으나 개정에 반영되지 못하고, 당해 제9조의3만 신설되었기 때문이다.

17) 이에 대하여 통신비밀보호법이 규제하고 있는 '통신사실 확인자료'의 경우, 이미 송·수신이 완료된 전기통신을 대상으로 하고 있다는 점(물론 내용은 포함되지 않고 전기통신사실에 관한 자료만이 해당됨)에서 과거의 통신자료도 동법의 보호대상에 해당하므로 타당하지 못하다는 반론이 있을 수 있다. 그러나 이는 동법 제2조 제3호의 규정(전기통신이라 함은 ……전자우편……등과 같이 …… 송신하거나 수신하는 것을 말한다)만으로도 충분할 것이고, 동조 제9호의 규정을 그와 같은 이유로 굳이 현행과 같이 존치시켜야만 할 이유는 없는 것이다.

다.[18] 당해 개정안은 "통신사업자의 서버에 저장된 전자메일 등에 대해서 지나치게 포괄적인 영장이 발부되는 사례"를 시정하기 위하여 "영장 발부 요건을 강화"하고(개정안 제106조 제3항, 제109조 제3항, 제215조 제3항 신설, 제107조 제4항 신설 등), 7년 치의 이메일을 통째로 뒤진 사건의 재발을 방지하기 위해 "대상이 되는 전자메일 등에 작성기간을 추가하여 무분별한 열람을 방지"하고자 하는 규정(개정안 제114조 제1항 단서조항 신설) 등을 담고 있다.[19]

요컨대, 저장 데이터의 경우 통신비밀보호법이 아니라 형사소송법상의 압수・수색의 대상임을 명확히 하는 쪽으로 일련의 개정이 추진되고 있다고 하겠다.

2. 압수・수색이면 충분한가?

종래의 검찰의 입장은 "이메일의 경우 형사소송법상의 압수・수색 조항을 적용해서 서버에 보관된 이메일에 대한 압수수색은 서버관리자에게만 통보가 되고 실제 이메일을 주고받은 이용자에게는 통보하지 않고, 이는 통신비밀보호법에서 이메일과 관련하여 송수신 하는 것으로 정의되어 있기 때문에 서버에 보관된 메일은 이미 송수신이 끝난 상태이므로 형사소송법상의 '물건'에 해당[20]하는 압수・수색이 적용돼 서버관리자에게만[21] 통보"한다는 것이었다.[22] 이에 개정 통신비밀보호법은 제9조의3을

---

18) 국회의 의안정보시스템에 의하면, 현재 '위원회 심사' 단계에 머물러 있는 상황이다, <http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_O0G9U0N6C2P3A1Y5N1K7R3Z7Q2T2P4>, 검색일: 2009.9.10.

19) 형사소송법 일부개정법률안, 박영선의원 대표발의, 2009.6.23., 1-4쪽.

20) 저장 데이터가 형사소송법 제106조・제109조・제219조 상의 '물건'에 해당하는지에 대해서는 학설의 대립이 있다. 이에 관하여는 박문성, "형사소송법과 전자문서", 형사정책연구 제10권 제4호(형사정책연구원, 1999), 310-317쪽; 이은모, "전자적 정보에 관한 수사상의 문제점", 형사법연구 제23호(한국형사법학회, 2005), 158-160쪽 참조. 이에 대하여 판례는 송수신이 완료된 전기통신의 내용을 지득・채록하는 것은 감청에 해당되지 않는다고 판시한 바 있다(대법원 2003. 8. 22. 선고, 2003도3342 판결).

21) 이에 대한 비판으로는 박경신, "헌법복원을 위한 18대 국회 형사소송법-통신비

신설하여 '수사대상이 된 가입자[23]에게 압수·수색·검증을 집행한 사실을 그 처분을 한 날로부터 30일 이내에 서면으로 통지'해야 함을 규정하였다.

그러나 이 조항의 신설만으로 충분한가? 즉 이메일 등의 저장데이터가 압수·수색의 대상이 되기만 하면, 그리고 수사대상이 된 가입자에게 집행사실을 통보하면 디지털 매체에 대한 논란은 끝이 나는가?

물론 지금까지의 상황에 비해서는 다소 진전이 있겠으나, 이런 식의 개정이 궁극적인 해결책은 아니라고 말하고 싶다. 구체적인 이유는 다음과 같다.

2.1. 영장주의의 예외

영장주의는 수사상 필요한 강제처분의 경우 법관이 발부한 적법한 영장에 의하지 아니하고는 할 수 없다는 원칙을 말한다(헌법 제12조 제3항 및 형사소송법 제113조). 따라서 저장 데이터로서의 이메일을 열람하기 위해서는 압수·수색영장에 의해야 한다.

그러나 이러한 원칙의 해석만으로는 저장되지 않은 채로 네트워크상을 달리고 있는 이메일의 경우에는 왜 압수·수색영장에 의하지 않는지에 대한 답변을 마련해 주지 못한다.

밀보호법-전기통신사업법 개정안", 송수신이 완료된 이메일 등 현대적 매체에 대한 통신비밀보호법제 토론회 발제문, 4-7쪽, <http://minbyun.org/?module=file&act=procFileDownload&file_srl=27906&sid=7e682a25b9cefb654cffcc3ac6614252>, 검색일: 2009.9.10.; 류제성, 앞의 글, 5-6쪽.

22) 박영선의원 의정활동 자료, "[보도자료] 서울고검 - 압수수색·통신감청·통신사실확인자료제공 등 올 상반기에만 33만 7천", <http://www.pys21.net/bbs/view.php?DB=assemblyact&num=95&start=0&S=S&val=6&word=형사소송법>, 검색일: 2009.9.10.

23) '수사대상이 된 가입자'라는 표현도 충분하지 못하다. 수사대상이 된 가입자가 수신한 메일을 압수·수색한 경우에는 당해 수사대상이 된 가입자(수신인)의 '통신의 비밀'뿐만 아니라 발신인의 '통신의 비밀'도 침해하기 때문이다. 따라서 통지의 대상을 '수사대상이 된 가입자와 그 상대방'으로 확대하는 것이 바람직하다.

물론 통신비밀보호법에 등장하는 통신제한조치 허가서가 영장의 하나이므로 이는 곧 영장주의의 원칙에 의한 법원의 엄격심사에 의한다고 주장할 수도 있다.[24] 그러나 실제에 있어서도 그러한가? 아래의 자료를 살펴보자.

먼저 통신제한조치 허가서, 즉 소위 감청영장과 통신사실 확인자료에 대한 법원의 청구대비 기각률을 살펴보면 다음과 같다.

<통신감청 영장 청구 및 기각률 통계표>

	청구	기각	기각률
2003년	347	10	2.9%
2004년	193	2	1.0%
2005년	73	1	1.4%
2006년	107	3	2.8%
2007년	112	4	3.6%
2008년 6월	35	1	2.9%

<통신사실 확인자료 청구 및 기각률 통계표>

	청구	기각	기각률
2006년	60,357	557	0.9%
2007년	66,651	585	0.9%
2008년 8월	47,280	579	1.2%

[자료출처 : 이춘석 의원실][25]

감청의 경우 최대 3.6%, 5.5년 평균 2.65%의 기각률을 보이고 있고, 통신사실 확인자료의 경우 거의 1% 남짓이다.

---

24) 김성훈, "통신비밀보호법 개정 관련 질의사항 검토", 국회의원 이춘석 • 민주당 정책위원회, "수사 • 정보기관 통신감청 국민은 안전한가?"통신비밀보호법 관련 토론회 자료집(2008). 78쪽 • 81쪽 • 90쪽.

25) 이 통계는 2008년 12월 11일 국회의원회관에서 있었던, 통신비밀보호법 관련 토론회인 "수사 • 정보기관 통신감청 국민은 안전한가?"의 발제 준비를 위해 민주당 이춘석 의원실로부터 제공받은 자료에 의한 것이다.

다음으로 압수・수색영장의 기각률을 살펴보자.

<압수・수색・검증 영장 기각률 통계표>

법원명	발부	일부기각	기각	기각률	발부율
춘천지법	2924	77	40	4%	96%
울산지법	2794	107	27	5%	95%
대전지법	6874	287	51	5%	95%
부산지법	6702	354	57	6%	94%
대구지법	7575	428	67	6%	94%
창원지법	4835	316	43	7%	93%
전주지법	3590	202	65	7%	93%
광주지법	3590	202	65	7%	93%
인천지법	8355	632	69	8%	92%
서울북부지법	3366	265	70	9%	91%
제주지법	1134	97	19	9%	91%
의정부지법	3789	344	69	10%	90%
수원지법	12618	1300	133	10%	90%
청주지법	2634	295	37	11%	89%
서울남부지법	3724	443	79	12%	88%
서울서부지법	3045	458	25	14%	86%
서울동부지법	3051	423	94	14%	86%
서울중앙지법	7962	1657	146	18%	82%

기간: 2008년 1월-12월. [자료출처: 대법원][26]

압수・수색영장 기각률은 최대 18%, 1년 평균 9%의 기각률을 보이고 있다. 여기서 압수・수색영장의 평균 기각률인 9%라는 수치가 구속영장의 평균 기각률인 22.6%[27]와 상당한 차이(대략 2.5배)가 있다는 점이 심각한 문제이기는 하나, 이 양자의 차이를 '신체의 구속'이라는 구속영장

26) 이 통계는 '투명사회를 위한 정보공개센터'에서 대법원의 공개자료를 토대로 구성한 자료이다. <http://www.opengirok.or.kr/793>, 검색일: 2009.9.10.

27) 이는 '투명사회를 위한 정보공개센터'에서 대법원의 공개자료를 토대로 구성한, 2008년 1년간의 '전국 지방법원별 구속영장 발부율과 기각율' 자료에서 인용하였다. <http://www.opengirok.or.kr/792>, 검색일: 2009.9.10.

의 본질을 고려하여 어느 정도 수긍하여 보기로 하자.

그렇다면 압수·수색영장의 최대 18%, 평균(1년) 9%의 기각률과, 최대 3.6%, 평균(5.5년) 2.65%의 기각률을 보이고 있는 감청 허가서와의 차이(대략 3.4배)는 어떻게 해석할 수 있는가? 특히 통신제한조치의 경우 감청의 당시에는 피감청자가 감청 사실을 알 수 없다는 점에서, 영장을 통해 압수·수색의 사실을 고지받고 시행되는 압수·수색의 경우보다 오히려 그 기본권의 침해정도가 더 크다는 점을 고려한다면, 이러한 수치는 실로 어이가 없는 수준이다. 또한 그 본질과 형태가 제법 유사하다고 판단되는 통신사실 확인자료의 평균 기각률인 1%와 압수·수색영장의 기각률을 비교하여 본다 하여도, 이러한 법원의 심사행태는 탄성을 자아내게 한다.

나아가, 허가서상의 감청의 범위는 어떠한가? 과거 정보통신부 보도자료에 의하면, 2006년 하반기 통신감청 허가서 1건당 대상 전화번호수는 6.06건이고, 통신사실 확인자료의 경우에는 허가서 1건당 대상 전화번호수는 3.66건이다.[28] 이 통계수치를 위의 기각률과 함께 고려한다면, 결국 감청과 관련된 제사항에 있어 법원의 심사기능은 이미 사문화되었다는 것을 증명해주는 셈이다. 이러한 통계를 보고도 영장주의에 의한 것이므로 이론상 아무 문제없다며, 그저 덮어만 두고 있을 수 있는가?

이렇듯 실제에 있어서는 통신제한조치 허가서는, 압수·수색·검증·구속 등의 영장과는 다르게 운영되고 있는 것이다. 다시 말해 감청 허가서는 영장주의의 탈을 쓴 '영장주의의 예외'에 불과한 상황이다.

그렇다면 법원통제의 정도에 있어 이러한 현격한 차이를 보이게 되는 양자의 분류기준, 즉 감청영장에 의해야 하는가 아니면 압수·수색영장에 의해야 하는가의 기준이, 디지털 정보에 있어 '송·수신의 완료 여부'라는 점은 타당한가? 즉 송·수신이 완료된 저장데이터(압수·수색영장의

28) <http://mic.news.go.kr/common/jsp/download.jsp?idKey=893e00c0e2f976760e64d7746006e486> 참조; 통계에 의하면 1건의 통신감청 허가서당 대상 전화번호수가 6개 이상이라는 것인데, 상식적으로 생각하여 볼 때 특정인이 사회적으로 보유하는 전화번호의 수는 3개 정도(자택, 직장, 핸드폰)가 적당할 것이다. 그렇다면 나머지 3개의 전화번호는 결국 오남용된 것이라 추정해 볼 수 있다.

대상)와 저장되지 않은 채로 네트워크상을 달리고 있는 데이터(통신제한조치 허가서의 대상)가, 법원의 차별적 통제행태에 상응하는 정도의 본질적 차이가 있는가 하는 점이다.

2.1.1. 송·수신 완료 여부의 무의미성

1초 전에 통화가 끝난(송·수신의 완료) 전화통화는 1초 후인 지금은 휘발(揮發)되어 존재하지 않지만, 디지털 매체에 있어서는 1초 전에 도착한 음성메일은 휘발되지 않고 1초 후인 지금도 하드디스크나 메일서버에 저장된 채로 재열람이 가능하게 된다. 즉 디지털 매체는 전화통화와는 달리 수신의 완료와 동시에 휘발되지 않는다.[29]

한편 당해 음성메일의 발신은 완료되었으나 수신자의 서버에 문제가 발생하여 아직 수신완료가 되지 못하고 있는 상황이라면, 서버의 에러가 해결될 때까지는 당해 음성메일은 끊임없이(이론상으로는 영원히) 네트워크상을 떠돌아다니게 되고 이에 대해 발신자는 어떠한 조치도 취하지 못하게 되는 상황이 연출된다. 즉 아날로그 매체에서처럼 휘발로 인한 수신의 불능으로 상황이 종료되는 것이 아니라, 분명히 수신이 가능하고 데이터가 확실히 존재하기는 하나 그 완료의 순간을 예측할 수 없는 수신지연의 상황이 전개되는 것이다.[30] 따라서 네트워크상에 흐르는 디지털 정보는 이론상으로는 송·수신의 당사자나 기타 네트워크 관련자의 의사에 의한 임의적 삭제가 없는 한 일단 발신된 데이터의 휘발은 있을 수 없다.

이렇듯 휘발이 불가능하다면, 송·수신의 완료를 기준으로 그 적용법

29) 아날로그 매체에 있어서도 전화통화의 경우에는 몰라도 우편물의 경우에는 이와 유사·동일한 상황이 연출될 수 있다. 수신한 우편물을 다시금 꺼내어 보는 경우가 이에 해당할 것이다.

30) 그러나 아날로그 매체의 경우에는 상황이 다르다. 예를 들어 일반 유선전화의 통화에 있어 발신자가 음성을 송신하였으나 회선장애로 인하여 수신이 불능한 경우, 당해 음성정보는 수신의 불능 순간에 이미 휘발되어 존재하지 않고 통화당사자는 그 의사에 의해 송·수신(통화)을 완료·중단할 수가 있다. 또한 우편물의 경우도 발신 후 증발이나 소멸(즉 휘발)로 인해 수신이 불능한 경우, 이미 당해 우편물은 물리적·영구적으로 존재하지 않으므로 송·수신의 완료가 불능한 상황으로 일단락된다.

규를 구별한다는 것이 어떠한 의미가 있는가? 다시 말해 송·수신중인 통신의 내용을 지득·채록하는 것은 감청이고 송·수신이 완료된 통신물에 대해서는 영장에 의해 압수·수색과 같은 대물적 강제처분을 한다고 구분할 때에는, 적어도 양자의 규제목적이나 규제대상에 차이가 존재해야 하는 것 아닌가 하는 점이다. 예를 들어 휘발이 되어버리는 전화통화를 대화자 몰래 감청하는 것과 우송중인 우편물을 송·수신자 몰래 들여다보는 행위는, 통화가 끝이 나면 더 이상 지득·채록할 수 없다는 차이가 있거나 수신자보다 먼저 우편물의 내용을 지득·채록하게 되므로 통신비밀의 침해정도가 높을 수 있다는 등의 차이가 존재한다고 하자.

그렇다면 1초 전에 도착하여 수신자의 메일서버에 수신이 완료[31]된 이메일과, 그 도착이 지연되어 1초 후에 도착할 이메일을 당해 메일서버의 바로 앞 네트워크상에서 DPI 기술을 사용(즉 패킷 감청)하여 수집·취합한 것은 그 규제의 목적이나 규제의 대상에서 도대체 어떠한 차이가 있는가? 양자 모두 그 내용에 있어서나 정보의 본질에 있어 완전히 동일하고, 양자 모두 수신자가 당해 메일을 열람하기 이전이므로 통신비밀의 침해정도도 또한 똑같다.[32]

다시 말해 이메일 등의 디지털 매체에서는 그 송·수신의 완료 여부가 아날로그 매체에서처럼 그 시점이나 완결의 여부가 아니라, 정보수집의 장소가 서버인가 네트워크인가 하는 공간의 문제로 변모하는 것이다. 이

---

31) 전자거래법 제6조 제2항: 전자문서는 다음 각 호의 1에 해당하는 때에 수신된 것으로 본다. 1. 수신자가 전자문서를 수신할 정보처리시스템을 지정한 경우에는 지정된 정보처리시스템에 입력된 때. 다만, 전자문서가 지정된 정보처리시스템이 아닌 정보처리시스템에 입력된 경우에는 수신자가 이를 출력한 때를 말한다. 2. 수신자가 전자문서를 수신할 정보처리시스템을 지정하지 아니한 경우에는 수신자가 관리하는 정보처리시스템에 입력된 때; 따라서 메일의 경우처럼 수신할 정보처리시스템(메일서버)이 지정된 경우(메일주소의 인지), 그 수신 완료시기는 수신자가 당해 메일을 열람하는 때가 아니라 메일서버에 메일이 도착한 때이다.

32) 따라서 저장 데이터가 통신비밀보호법상의 감청의 대상이 된다는 것이 아니라, 적어도 디지털의 경우 송·수신중인 데이터도 형사소송법상의 압수·수색의 대상이 되어야 한다는 것이다.

는 결국 종래의 송·수신의 완료 여부를 기준으로 한 구분이 디지털 매체에 있어서는 무의미하다는 것을 말해준다.

종래의 구분에 의할 경우, 수사기관에게 그 편의에 따라 적용법규를 임의적으로 선택하게 하는 근거불명의 권능을 부여할 뿐이다.

2.1.2. 송·수신 완료 여부의 불명확성

발신자가 이메일의 발신을 완료하였으나, 당해 이메일이 수신자의 서버를 향해 네트워크상을 질주하고 있어 아직 수신자의 편지함에 완전히 도착하지 못한 경우, 네트워크상에서 벌어지는 상황을 살펴보자.

이메일은 그 도착의 형태에 있어, 완성된 이메일 한 장이 턱하니 도착하는 것이 아니다. TCP/IP를 프로토콜로 사용하고 있는 현재의 네트워크 기술은, 이메일을 발신할 때 한 장의 메일을 통째로 발신하지 않는다. 발신자가 작성한 그 한 장의 메일을 수많은 조각(Packet)으로 분해한 후, 각 조각의 상단에 도착할 서버의 주소와 일련번호를 붙여 발송하며, 이러한 조각들이 주소로 적힌 수신자의 서버에 도착하면 다시금 일련번호의 순서대로 재조합하는 과정을 거치게 된다. 이러한 분해·재조합 방식을 사용하는 이유는 네트워크상의 정체를 줄이기 위해서이며,[33] 이러한 조각들이 일련번호의 순서대로 수신서버에 도착하는 것도 아니다. 결국 수신자의 입장에서는 운좋게 모든 조각들이 무사히 다 도착한 경우에만 그 일련번호의 순서대로 재조합되어 완전한 한 장의 이메일을 열람할 수 있는 것이며, 그렇지 않을 경우에는 종종 있게 되는 '발신 후 수신불능'이나 '수신 후 에러메시지'를 맞게 되기도 한다.

이러한 이메일의 송·수신 방식을 고려하면서, 송·수신의 완료 여부를 기준으로 하는 종래의 구분방식에 의할 경우에는 모호한 해석문제가 발생한다. 즉 어느 정도의 조각들이 도착하여야만 수신이 완료된 것으로 할 것인가 하는 문제이다.

만약 모든 조각들이 도착하여 일련번호 순서대로의 재조합이 완전히

33) 일상생활에서 변기가 막히는 경우를 생각해 보면, 그 이유를 충분히 이해할 수 있을 것이다.

가능할 때를 기준으로 한다면, 일부 조각들이 도착하지 않아 수신자가 이메일을 열람하였으나 그 내용이 깨어져서 해독이 전혀 불가능한 경우나 일부만 해독가능한 경우(즉 수신 후 에러메시지)는 수신의 완료가 없는 상황인 것인가? 나아가 해독이 불가능한 부분이 이메일의 바탕그림이거나 광고문구에 불과하여 완전한 메일의 수신은 아니나 발신자가 작성한 메일 내용(문구)의 주요사항을 모두 다 파악할 수 있는 경우는 어떠한가? 이를 긍정한다면 수신서버에 최초로 도착한 그 하나의 조각은 압수·수색의 대상이고, 서버의 바로 앞 네트워크상에 있는 나머지 조각들은 감청의 대상으로 보아야 하는데 이러한 해석은 타당한가?

이러한 해석상의 문제점은 쉽게 해결할 수 없을 것으로 판단된다. 그 형체나 시점에 있어 '한 덩어리'로 전달되어 그 전달의 가부와 수신의 완료 여부가 비교적 명확한 아날로그 매체와는 달리, 디지털 매체의 전달방법은 그 특성상 전달의 가부와 수신의 완료 여부에 대하여 항상 모호한 해석의 가능성이 존재하기 때문이다.

2.2. 포괄영장의 가능성

앞서 인용한 신문지상의 보도에 의하면, 검찰이 주경복 전 서울시교육감 후보의 선거법 위반 사건을 수사하면서 '수사 대상자 100여명의 7년간 전자우편을 통째로 압수'해 열람하였다고 한다. 이는 영장의 발부 자체가 문제가 아니라, 발부된 영장에 있어 그 압수와 수색의 대상과 범위에 관한 문제이다. 그 대상이 특정되지 않고 망라적이거나 그 범위가 너무 광범위한 경우에는 영장주의의 취지가 무색하게 되기 때문이다. 즉 포괄영장[34]의 우려가 현실로 나타난 것이다.

이에 대하여 야당은 금번 형사소송법 개정안에서 지나치게 포괄적인 영장이 발부되는 경우를 방지하기 위해 영장의 발부 요건을 강화하고(개정안 제106조 제3항, 제109조 제3항, 제215조 제3항 신설, 제107조 제4항 신설 등), 대상이 되는 전자메일 등에 대한 '작성기간'을 추가하여 광

34) 영장의 대상과 범위가 불특정하거나 포괄적인 경우를 이하에서는 편의상 '포괄영장'이라 칭하기로 한다.

범위한 수집을 차단하는 규정(개정안 제114조 제1항 단서조항 신설)을 마련한 바 있다.[35]

그러나 이러한 규정의 마련이 포괄영장의 우려를 불식시킬 수 있을지는 미지수이다.

2.2.1. 대상메일의 특정 문제

개정안에 의하면 메일의 '작성기간'만을 특정하도록 규정하고 있다. 그러나 작성기간의 특정이 메일 송·수신 상대방의 프라이버시를 보호해 줄 수 있을지는 의문이다. 가령 공공건물의 폭파범으로 수사선상에 올려진 피의자의 직업이 상담을 전문으로 하는 '임상심리의'라고 가정해 보자. 동 피의자의 이메일에 대하여 발부된 압수·수색 영장에 '영장발부일로부터 60일 전'이라는 작성기간이 특정되었다고 하여도, 그 60일 동안 피의자가 수많은 환자와 주고받은 의료적 상담메일은 압수·수색의 대상에 포함되게 된다. 즉 범죄수사와 무관하더라도 일단 영장상의 작성기간의 범주에 들어가기만 하면 당해 메일은 공개되게 되고, 이로 인해 노출되는 환자들의 내밀한 프라이버시는 보호될 방도가 없다.

이 점에 관하여 "포괄적 압수는 원칙적으로 인정되지 않고, 피의사실과 관련이 있는 정보만을 플로피디스크 등의 기록매체에 복사하여 압수하는 것이 허용될 수 있다고 보는 것이 합리적인 해석"이라고 보는 견해가 있다.[36] 그러나 구체적으로 피의사실과 관련이 있는 정보만을 선별하는 방법은 어떠한 것이 있는가? 사실 수사기관의 입장에서는 메일을 열어보기 전에는 그 내용을 예단할 수 없으므로, 메일의 제목이나 송·수신 상대방의 이름 또는 ID만으로 범죄수사와의 관련여부를 구분하여 열람하는 것이 처음부터 불가능한 구조이다. 즉 모든 메일을 모두 열람하는 것만이 가장 확실한 수사방법인 것이다.

결국 압수·수색의 대상이 되는 송·수신의 상대방을 선별할 수 없으므로 이미 타인의 프라이버시에 대한 침해가 있다는 점은 공공연히 긍정

35) 형사소송법 일부개정법률안, 박영선의원 대표발의, 2009.6.23., 1-4쪽.
36) 이은모, 앞의 글, 164-165쪽.

하는 것이며, '작성기간'의 특정은 그저 통째가 아니라 적정기간이라는 시간적 범위를 둠으로써 그 침해의 양과 정도를 적정한 수준으로 한정한다는 점에서만 유의미할 뿐이다.

그렇다고 하여, 이러한 침해의 최소화를 담보하면서 수사상 필요한 정보만을 얻을 수 있는 뾰족한 방안도 없다. 즉 수사의 단계에서는 범죄사실 자체가 특정되지 않은 상태이므로 그 압수·수색의 대상은 어느 정도 개괄적일 수밖에 없다. 특히 이메일의 경우에는 결정적 증거물일 경우보다는 주로 범죄의 동기나 배경파악을 위한 기초자료로 사용되는 경우가 많을 것이기 때문에, 영장상의 '특정' 자체가 수사기관의 영장 청구취지와 맞지 않는다. 따라서 이메일에 대한 압수·수색에 있어 그 대상과 범위를 제대로 특정한다면, 수사기관이 영장을 청구할 이유가 없는 것이다.

2.2.2. 하드웨어 자체의 압수

흔히 TV뉴스에서 보도되는 장면에서 보듯, 피의자의 거주지나 사무실에서 컴퓨터나 하드디스크를 통째로 압수하는 경우에는 어떠한가?

먼저 압수·수색 영장이 피의자의 이메일이 아니라 피의자 소유의 물건에 대하여 발부된 경우가 있을 수 있다. 이럴 경우, 당해 컴퓨터나 하드디스크 속에 저장되어 있는 모든 저장 데이터는 자동적으로 영장의 대상이 되는 것인가? 논란의 여지가 있으나, 만약 이를 부정한다면 컴퓨터나 하드디스크의 외관을 통해 수사가 가능하다고 해야 하는데 이 또한 어불성설이다.[37]

다음으로는 압수·수색 영장은 피의자의 이메일에 대하여 발부되었으나, 그 현장에서 시간의 부족이나 장소의 부적절성 등을 이유로 기록매체

37) 예를 들어 절도피의자의 거주지에 대한 압수·수색 영장을 발부하면서 그 대상을 '카메라, 노트북, 보석류 등 본건에 의한 장물로 사료되는 일체의 물건'으로 한정한 경우에 있어서의 컴퓨터(노트북)와, 군사기밀인 미사일의 도면을 해외로 반출한 혐의를 받고 있는 피의자에 대한 압수·수색 영장에 있어 그 대상을 '카메라와 그 필름, 또는 USB 메모리 등의 저장매체, 컴퓨터 및 하드디스크 등의 저장매체'라고 한 경우에 있어서의 컴퓨터는 해석에 있어 그 차원이 완전히 다르다.

의 내용을 확인하지 않은 채 컴퓨터나 하드디스크 등의 하드웨어 자체를 압수하는 경우이다. 이러한 압수는 가능한가? 요컨대 수사의 대상이 되는 자료는 하드웨어가 아니라 하드웨어에 담긴 '저장 데이터'들인데, 실제 압수한 것은 하드웨어인 경우이다.

법리적으로는, 전자의 경우에 수사기관이 이미 발부된 압수·수색영장을 근거로 하여 당해 하드웨어를 열고 그 속에 저장되어 있는 데이터들을 수색하여 다시금 압수할 수 있는가의 문제가 발생하고, 후자의 경우에는 영장에 기재된 대상이 아니라 그 대상이 담긴 하드웨어 자체의 압수가 가능한가의 문제와 영장의 실행을 위해 다시금 하드웨어를 열어보는 것이 타당한가의 문제가 동시에 발생한다. 그러나 실제에 있어서는 이러한 법리적 검토는 무시된 채 수사기관의 자의적 해석에 의해 무분별한 하드웨어의 압수가 자행되고 있으며, 학설에 따라서는 이를 일정 부분 긍정하고 있는 경우도 있다.[38] 이러한 수사현실이나 학설의 입장에 의한다면 당해 영장은 결국 포괄영장과 다름없다. 하드웨어의 압수와 그 수색을 긍정하는 한, 그 대상이 특정되지 않아 망라적이게 되거나 그 범위가 광범위하게 되어 영장주의의 취지가 무색하게 되기 때문이다.

이러한 문제는 무체물인 저장 데이터는 항상 유체물인 하드웨어에 저장될 수밖에 없다는 디지털 매체의 특성에 대한 본질적 고려를 간과한 결과에서 비롯된다. 즉 이메일 등의 저장 데이터는 현재의 법체제하에서는 결국 포괄영장을 발부받을 우려를 말끔히 떨쳐버릴 수 없는 것이다.

3. 소결

지금까지 살펴본 바와 같이, '송·수신의 완료 여부'만을 기준으로 하

38) 플로피디스크의 라벨이나 케이스 등의 기재, 보관장소의 상황, 컴퓨터사용자의 설명 등에 의해 그 전자적 기록매체에 관련정보가 기재되어 있다고 인정되는 경우에는 당해 전자적 기록매체를 압수하면 될 것이다: 이은모, 앞의 글, 163쪽; 수사기관이 적법한 절차에 따라 압수한 저장매체에서 데이터의 내용을 알아내는 것은 마치 봉합된 시정을 여는 것과 같은 '필요한 처분'으로서 현행법하에서도 허용된다고 할 것이다: 박문성, 앞의 글, 317-319쪽.

는 구분은 종래의 아날로그 방식에 있어서나 의미가 있는 것이다. 따라서 디지털 매체에 대하여 이렇듯 무의미한 기준을 근거로 적용법규가 달라지는 현재의 입법방식에 근본적으로 찬성할 수 없다.

인터넷을 개발한 미국의 경우, 이러한 아날로그와 디지털의 차이점을 입법에도 반영하고 있다. 수정헌법 제4조[39]의 대원칙 아래, 감청법의 시초로 불리는 통신법(Communications Act of 1934)과 연방감청법(Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 속칭 Federal Wiretap Act) 등이 제정되어 송·수신중인 아날로그 통신을 대상으로 적용된다. 디지털 통신에 대해서는 그 이후에 입법한 전자통신비밀보호법(Electronic Communications Privacy Act of 1986, ECPA)[40]을 적용하고, 여기서 다시 송·수신의 완료로 저장된 디지털 매체에 대해서는 저장통신법(Stored Communications Act, SCA)[41]을 따로 마련하고 있다.[42] 즉 단순한 송·수신의 완료 여부가 아니라 매체의 특성과 형태를 기준으로 체계적인 입법을 하고 있는 것이다.

한편 미국의 경우 하드웨어 자체의 압수에 대해서도 분명한 기준을 가지고 있다. 즉 판례는 컴퓨터 하드웨어를 압수한 후 당해 컴퓨터에 저장된 이메일을 탐색하는 것은 전자통신비밀보호법(ECPA)에 위반되는 행위이며,[43] 이를 위해서는 동법 제2703조에 의한 별도의 영장을 발부받아야만 한다[44]고 판시한 바 있다.

---

39) 합리적인 프라이버시에의 기대가 인정되는 영역에서 정보를 수집하기 위해서는 '상당한 이유(probable cause)'가 있어야 하고 법관이 발부한 영장(judical warrant)에 의해야 함을 규정하고 있다: AMENDMENT 4.

40) 18 U.S.C. §§2510-2521.

41) 18 U.S.C. §2701.

42) "연방감청법은 송·수신중인 메시지의 감청에만 적용되고 저장된 매체에 적용되지 않는다(the Wiretap Act only covers messages intercepted during transmission, not those intercepted in storage)": Konop v. Hawaiian Airlines, 302 F. 3d 868(2002).

43) Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F. 3d 457 (5th Cir. 1994).

44) Davis v. Gracey, 111 F. 3d 1472 (10th Cir. 1997).

조악한 우리의 입법 현실에 비추어보면, 이러한 미국의 입법이나 판례가 다소 요원한 이야기로 치부될 수도 있다. 그러나 앞서 살펴본 바와 같이 디지털 매체에 있어 송·수신의 완료 여부에 의한 구별이 무의미하다는 점은 자명하고, 통신제한조치(즉 감청)의 경우[45]에는 그 매체의 형태를 불문하고 '진정한 영장주의'의 원칙하에 '제대로 된 법원통제'에 의해야 한다는 점은 입법 기술에 있어서의 최소한이라는 것을 명심해야 한다.

또한 이메일에 대한 압수·수색에 있어 그 대상과 범위를 제대로 특정한다면 수사기관이 영장을 청구할 실익이 없다는 점과, 저장 데이터가 담겨진 하드웨어 자체의 압수와 그 수색을 긍정하는 한 영장주의의 취지가 무색하게 되고 포괄영장의 우려가 현실화 된다는 점 등은 결국 디지털 매체에 맞는 새로운 입법체계의 필요성을 자명하게 말해준다.

Ⅲ. 'DPI'의 문제

1. DPI의 개관

근래에 들어 감청과 관련하여 새로이 부각된 이슈가 바로 패킷 감청(Packet Inspection)이다. 국정원에 의해 자행되어 왔으나 그 의혹만 제기된 채 확신을 할 수 없었던 패킷 감청이, 곽동기 남북공동선언실천연대 정책위원을 대상으로 발부된 '통신제한조치 허가서'에서 비로소 그 실체가 드러난 것이다. 서울중앙지법이 지난 6월 12일에 발부한 당해 허가서 상에서, 패킷 감청을 허가한 부분은 "대상자가 근무처에 자신의 명의로

45) 인터넷 사용자의 로그인 기록이나 접속한 웹서버의 목록과 순서 등이 기록되는 '통신사실 확인자료'의 경우에도, 인터넷 매체의 특성상 이를 열람하면 수사자가 직접 당해 사이트에 접속해 봄으로써 사용자가 접촉한 내용과 순서를 쉽게 알아볼 수 있게 되므로. 그 본질에 있어서는 감청과 큰 차이가 없다고 할 수 있다. 따라서 디지털 매체의 경우 통신사실 확인자료도 압수·수색의 대상에 포함하는 것이 바람직하다는 것을 강조하고 싶다.

설치, 사용 중인 하나로텔레콤(주) '광랜W' 초고속 인터넷 회선에 대한 전기통신 내용의 지득·채록 및 실시간 착·발신 IP 추적"이라고 적힌 부분이다.[46] 일반적인 통신제한조치와의 가장 큰 차이는 '인터넷 회선' 자체에 대한 감청을 허가했다는 점이다. 대상자가 소유하는 전기통신(예를 들어 휴대폰)의 내용을 지득·채록하거나 착·발신의 내역을 수집하는 것도 아니고, 이메일의 경우처럼 계정이나 대상물을 지정한 것 또한 아니다. 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.

1.1. DPI의 기술적 개념

소위 패킷 감청(Packet Inspection)이라 칭해지는 기술은 크게 두 가지로 구분된다. 'Shallow Packet Inspection(이하 SPI)'과 'Deep Packet Inspection'이 그것이다.[47] SPI의 경우는 이미 오랜 시간 사용되어 온 전형적인 네트워크 기술이다. 따라서 패킷 감청 자체는 그리 최신기술이 아니다. 또한 SPI의 경우에는 법률적 의미의 감청과 관련하여 특별한 문제도 없기 때문에 패킷 감청 자체가 모두 불법성을 함유하고 있는 것도 아니다. 새로이 개발된 DPI 기술만 문제가 될 뿐이다.[48]

---

46) 또한 서울 성북구에 있는 곽씨의 집에 부인 명의로 개설된 KT '뉴메가패스' 초고속 인터넷 회선에 대해서도 같은 조처를 취할 수 있도록 하고 있다. 허가서는 또 "대상자 명의 이메일 계정(dkk*****@naver.com, de******@hanmail.net)에 대한 전기통신 내용의 지득·채록 및 착·발신 내역"도 감청의 대상으로 포함하고 있다. 한겨레21, "인터넷·전자우편 실시간 감청 시대", 2009.9.4자, <http://h21.hani.co.kr/arti/cover/cover_general/25658.html>, 검색일: 2009.9.10.

47) Allot Communications, "Digging Deeper Into Deep Packet Inspection(DPI)"(Allot Communications Ltd., 2007), 2쪽, <http://www.virtualpressoffice.com/JPContentAccessServlet?fileContentId=1190001699270&source=sd&showId=1152106482591>, 검색일: 2009.9.10.

48) 따라서 '국정원이 패킷 감청을 했다'에서의 패킷 감청이라는 용어는 그리 정확한 표현이 아니다. 'Inspection'이라는 용어가 비단 '감청'의 의미만 있는 것도 아니고, 나아가 패킷 감청이 DPI만 있는 것도 아니기 때문이다.

1.1.1. 패킷(Packet)의 구조

패킷의 개념과 패킷화의 이유에 대해서는 앞서 이메일의 송·수신을 설명하면서 이미 언급하였다. 그렇다면 패킷은 도대체 어떻게 생겼는가?

아래의 도안에서 보듯 패킷은 크게 헤더(Header, 아래의 도안에서 짙은 부분)부와 데이터 영역(Data Field, 아래의 도안에서 옅은 부분)으로 구분된다.

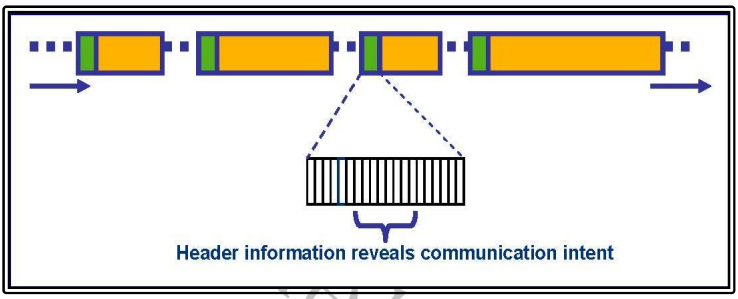

그림 : 패킷 헤더와 SPI[49]

헤더부분은 기본적인 프로토콜 정보인 출발지 주소(Source Address)와 목적지 주소(Destination Address) 등을 담고 있는데, 이를 조사하면 IP주소(IP address)나 저수준의 네트워킹 정보(Low-Level Connection States) 등을 파악할 수 있다. 한편 데이터 영역에는 소스 어플리케이션에 대한 정보(Identity of the Source Application)[50]와 메시지 자체의 내용[51]이 담겨져 있다.[52] 즉 패킷이라는 작은 트럭이 운반하고자 하는 중요한 화물

---

49) Allot Communications, 앞의 글, 2쪽 본문 도안을 인용. 이 그림은 네트워크 회선을 지나는 많은 패킷들 중 하나를 검토하는 장면을 도안화한 것이다. 도안상으로는 4개의 패킷을 표현하고 있다.

50) 예를 들어 웹 브라우저, P2P 프로그램, 이메일 등 당해 패킷과 관련된 프로그램에 대한 정보이다.

51) 패킷화로 인해 조각이 나 있는 웹페이지의 일부, 파일의 일부 또는 이메일의 일부이며 내용 그 자체이다. 따라서 이는 재조합되면 완전한 웹페이지나 파일 또는 이메일의 일부를 구성하게 된다.

52) Riley, M. Chris/Scott, Ben, “Deep Packet Inspection: THE END OF THE

들인 것이다.

이렇듯 크게 2부분[53]으로 나누어져 있는 패킷의 구조는, 우편으로 송달되는 편지에 비유할 수 있다. 헤더부는 편지봉투에 해당하여 그 겉봉에 도착지가 기재되어 있으며, 데이터 영역은 봉투 속에 들어 있는 편지지로써 바로 우편을 통해 전달되어야 할 내용물인 것이다.

1.1.2. SPI와 DPI

원래 인터넷 네트워킹 기술의 기본원칙은 헤더부에 적힌 주소(출발지와 목적지)에 의해 전송되는 방식이다. 따라서 헤더부의 정보가 없다면 주소가 적혀 있지 않은 편지봉투와 같은 운명이 되는 것이다. 우체국에서 그러하듯 때로는 헤더부를 검사해 볼 필요가 있다. 이 우편물이 주소대로 잘 우송되고 있는 것인지, 또는 우편번호가 잘못 적힌 것은 아닌지 말이다. 이렇듯 어떠한 이유에 의해 헤더부의 내용을 검사하는 행위가 SPI이다. 집배원이 우송의 목적으로 겉봉의 내용을 살피는 것이 문제되지 않는 것처럼, SPI는 불법의 이유가 없다.

SPI 기술은 주로 네트워크 방화벽(Firewall) 시스템을 위해 개발되어 왔고 현재 널리 사용되고 있다. 즉 기업이나 조직의 차원에서, 기업·조직의 내부를 구성하고 있는 컴퓨터의 정보 보안을 위해 외부에서 내부, 내부에서 외부의 네트워크에 침입하는 것을 차단하는 기술로 사용된다.[54]

한편 DPI는 데이터 영역까지 살펴보는 검사를 말한다.[55] 즉 집배원이

INTERNET AS WE KNOW IT?"(Free Press, 2009), 3쪽, <http://freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf>, 검색일: 2009.9.10.

53) 간략한 설명을 위하여 크게 2부분으로 표현한 것이지, 사실 그리 간단하지 않다. 헤더와 데이터 영역의 2부분 이외도 다시 몇 겹의 층(Layers)으로 구성되어 있으며, 모든 패킷이 동일한 구조를 취하고 있는 것도 아니다. 패킷의 구조에 대한 상세는 <http://explore.kwangwoon.ac.kr/~capston08/up/DATASHEET/RF_Function.doc>, <http://boanin.tistory.com/33> 검색일: 2009.9.10. 등을 참고.

54) 하드웨어적으로는 라우터(Router)나 응용 게이트웨이 장치(Gateway Unit) 등을 설치하게 되는데, 모든 정보의 흐름이 이를 통해서만 이루어지도록 설계하여 건물에서의 방화벽 역할을 하도록 되어 있다.

그 겉봉을 뜯어 내용물을 살피는 행위에 해당한다. 이러한 행위는 불법임은 물론 감청에 해당하는 것이다. 설사 내용을 다 읽어보고 원래대로 잘 집어넣어서 목적지에 고스란히 전달한다고 하여도, 그 행위의 불법성은 소멸하지 않는다.

원래 DPI 기술은 네트워크 접속문제의 해결, 바이러스(Virus)나 웜(Worm)의 차단, 그리고 최근 DDoS(Distributed Denial-of-Service Attack, 분산 서비스 거부) 사태로 유명해진 '서비스 거부(Denial-of-Service Attack, DoS)'를 해결하기 위해 개발되어 사용되었다.[56] 초창기 DPI의 경우 실시간 감청이 불가능하여 주로 해커들 사이에서나 거론되는 정도이었으므로 이슈화되지 않았으나, 기술의 발전으로 실시간 감청이 가능해지자[57] 근래에는 상업적 목적으로 활용됨은 물론 국정원의 감청수단으로까지 변모하여 신문지상에 등장하게 된 것이다.

1.2. DPI의 국제적 논란

단언할 수는 없으나, DPI와 관련한 논란은 아마도 미국에서 시작되었다고 보는 것이 맞을 것이다. 미국의 최대 케이블(네트워크) 사업자인 컴캐스트(Comcast Corporation)가 자사의 인터넷 서비스 가입자들 중 BitTorrent라는 P2P 프로그램을 사용하는 가입자에 한해 당해 P2P 프로토콜을 제한하여 '망 중립성(Net Neutrality)' 논란을 불러일으킨 바 있다.[58] 주로 큰 용량의 데이터들을 운반하게 되는 P2P 프로그램 덕분에 전체 네트워크에 정체가 빚어진다는 판단하에, P2P 사용자들에 한해 인

55) 이에 관한 상세는 Allot Communications, 앞의 글 2-10쪽; <http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars>, 검색일: 2009.9.10.

56) Riley, M. Chris/Scott, Ben, 앞의 글, 3쪽.

57) 이에 관한 상세는 <http://www.narus.com/index.php/solutions/intercept>, 검색일: 2009.9.10.

58) 이에 관한 상세는 Ohm, Paul, "The Rise and Fall of Invasive ISP Surveillance", University of Illinois Law Review(2009), 21-22쪽, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344>, 검색일: 2009.9.10; Riley, M. Chris/Scott, Ben, 앞의 글, 4-5쪽.

터넷 속도를 낮추는 기술적 제약을 가한 것이다. 이 때 P2P 사용자들을 구분하기 위해 DPI 기술이 사용된 것이다. 컴캐스트는 이 사건으로 인하여 '망 중립성'을 두고 연방통신위원회(Federal Communications Commission, FCC)와 갈등을 빚기는 했으나, 여기서 프라이버시나 감청의 문제는 거론되지 않았다.

그러나 '네부에드(NebuAd)' 사건에서는 상황이 달라진다. 인터넷 광고업체인 네부에드는 '행동기반 맞춤형 광고시스템(behavioral targeting advertising systems)'을 개발하여 이를 세인트루이스주의 ISP인 '차터 커뮤니케이션즈(Charter Communications)'에 판매하기에 이르렀다. 당해 광고시스템은 ISP 가입자들의 인터넷 사이트 방문내역을 추적해 개별 관심사에 부합하는 맞춤형 광고를 제공하는 한편, ISP로 하여금 온라인 광고수익을 누릴 수 있도록 하는 일종의 지능형·맞춤형 광고시스템이다. 그러나 시민단체들은 이러한 광고서비스가 인터넷 사용자들의 웹서핑 내역을 추적·수집·분석한다는 점, 그리고 그러한 사실을 정확히 알리거나 제대로 된 동의를 받지도 않았다는 점 등을 이유로 프라이버시 문제를 제기하였고, 이러한 사실이 이슈가 되자 결국 ISP인 차터 커뮤니케이션즈는 네부에드의 사용을 무기한 연기하였다.[59] 드디어 DPI 기술의 문제점이 부각된 것이다.

이와 유사한 사례로 영국의 폼(Phorm)사가 개발한 'Webwise'라는 맞춤형 광고시스템이 있다.[60] 우리의 KT가 최근 도입하고자 하는 '쿡 스마트웹(Qook Smartweb)'이라는 것이 바로 그 수입품[61]이다.[62]

---

59) 이에 관한 상세는 Ohm, Paul, 앞의 글, 20-21쪽; Riley, M. Chris/Scott, Ben, 앞의 글, 5쪽.

60) 이에 관한 상세는 Ohm, Paul, 앞의 글, 19-20쪽.

61) 오마이뉴스, "KT '쿡 스마트웹'은 당신이 한 일을 알고 있다", 2009.9.3자 <http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001208205>, 검색일: 2009.9.10.; 아이뉴스24, "정부, '인터넷 관심기반광고' 감청논란 개입키로", 2009.9.2자 <http://www.inews24.com/php/news_view.php?g_serial=440167&g_menu=020300>, 검색일: 2009.9.10.

62) 그 외에도 DPI 기술로 인해 이슈가 되고 있는 사례로는 'Front Porch', 'Cox Communications', 'ZillionTV' 등 다수이다.

한편 이러한 DPI 기술의 상업화와 그에 관한 뜨거운 논란과는 달리, 해킹과 감청 수단으로서의 DPI 기술은 아직 그리 큰 이슈가 되지 못하고 있다. 아마도 주사용자가 해커나 우리의 국정원 등 주로 음지에서 활동하는 만큼, 이슈가 되기도 곤란하고 될 수도 없을 것이다.[63]

1.3. DPI 규제의 동향

미국에서는 DPI 기술로 인해 프라이버시 침해의 논의가 부각되자, 주로 이를 ECPA 위반[64]으로 파악하는 일반적 논의가 진행되었다.[65] 그러나 맞춤형 광고시스템의 경우에는 이를 적용하기가 쉽지 않았다. 왜냐하면 ECPA상의 예외규정[66]에 해당하기 때문인데, 특히 '인터넷 사용자의 동의'가 있었다는 것이 핵심적 이유이다.[67] 상황이 이렇게 돌아가자 입법의 필요성이 부각되어,[68] 결국 의회에서 법안 작업에 착수하기에 이르렀다.[69] 에너지 및 통상위원회(Committee on Energy & Commerce) 차원에서 DPI 관련업체에 대한 실태조사 증언이 있었으며, 법안의 주요내용으로는 '정보 수집에 대한 동의요건', '정보의 수집방법과 수집된 정보의

63) DPI 해킹 프로그램은 온라인에서 손쉽게 다운로드 받을 수 있다. 티시피 덤프(TCP Dump), 와이어샤크(WireShark) 등의 무료 소프트웨어를 비롯하여 많은 상용 프로그램이 존재하리라 추정된다.

64) 18 U.S.C. §2511(a)(1); §2510(12); §2510(4).

65) Ohm, Paul, 앞의 글, 66쪽; Public Knowledge, "Filtering Whitepaper: Legal Analysis" <http://www.publicknowledge.org/paper/pk-filtering-whitepaper_5#ftn116>, 검색일: 2009.9.10.

66) 18 U.S.C. §2511(2)(a)(i); §2511(2)(c); §2511(2)(d).

67) 이에 관한 상세는 Ohm, Paul, 앞의 글, 72-73쪽.

68) 이에 관하여는 <http://www.betanews.com/article/Deep-packet-inspection-could-become-the-target-of-legislation/1240611260>, 검색일: 2009.9.10.; <http://www.freepress.net/node/49008>, 검색일: 2009.9.10. 등 참조.

69) 이에 관하여는 <http://www.pcworld.com/article/163740/us_lawmakers_target_deep_packet_inspection_in_privacy_bill.html>, 검색일: 2009.9.10; <http://comlaw.wordpress.com/2009/04/24/nyt-online-privacy-bill-on-deep-packet-inspection-dpi/>, 검색일: 2009.9.10; <http://comlaw.wordpress.com/2009/04/24/nyt-online-privacy-bill-on-deep-packet-inspection-dpi/>, 검색일: 2009.9.10 등 참조.

활용상황에 대한 공개' 등이 논의되고 있다.[70]

그러나 맞춤형 광고시스템에 대한 영국의 입장은 달랐다. 영국의 정보위원회(The Information Commissioner's Office, ICO)가 폼(Phorm)사의 DPI기술에 대하여 '사용자의 선택권이 있는 한 DPI는 위법이 아니다'라는 공식 입장을 내놓은 것이다.[71] 상황이 이렇게 되자, 이번에는 유럽위원회(European Commission, EC) 차원에서 이러한 영국정부의 대응을 문제 삼고 나왔다.[72] 'EU 데이터 보호지침(1995 EU Directive concerning Data Protection)'[73]과 'EU 전자통신지침(2002 EU Directive concerning Electronic Communication)'[74]의 위반이라는 것이다.

2. DPI의 위험성

일반적인 DPI에 대한 실정법적 해석은 자명하다. 어느 국가에나 하나씩은 꼭 있는 도청법 위반이 될 것이다. 우리나라의 경우 통신비밀보호법

---

70) 이에 관하여는 <http://www.theregister.co.uk/2009/04/24/deep_packet_inspection/>, 검색일: 2009.9.10.; <http://energycommerce.house.gov/index.php?id=22&view=section&option=com_content&layout=blog&cx=015314877951007841936%3Ansgszcxrcvg&cof=FORID%3A11&ie=UTF-8&q=dpi#1006>, 검색일: 2009.9.10. 등 참조.

71) Marc Rotenberg, "Communications Networks and Consumer Privacy: Recent Developments", 5쪽, <http://energycommerce.house.gov/Press_111/20090423/testimony_rotenberg.pdf>, 검색일: 2009.9.10.

72) 이에 관하여는 BBC, "EC starts legal action over Phorm", 2009.4.14자, <http://news.bbc.co.uk/2/hi/technology/7998009.stm>, 검색일: 2009.9.10.; Marc Rotenberg, 앞의 글 5쪽.

73) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://www.cdt.org/privacy/eudirective/EU_Directive_.html>, 검색일: 2009.9.10.

74) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, <http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>, 검색일: 2009.9.10.

제3조 1항의 위반이 되고, 미국의 경우에는 ECPA §2511(a)(1)의 위반[75] 이 된다. 그러나 미국의 사례에서 보듯 DPI는 일반적인 도청이나 데이터 리텐션(Data Retention)과는 달리 수많은 형태(서비스나 프로그램 등)로 변모가능한 디지털 기술이기 때문에, 현존하는 도청법 체계로 이를 규제하기란 불가능에 가깝다. 디지털 매체에 관하여 우리보다 훨씬 더 정교한 체계를 가지고 있는 미국에서조차 새로운 입법을 준비하고 있다는 점은, 그리 쉬운 상대가 아니라는 것이다.

2.1. 적용법규의 모호성

국정원이 했다는 DPI 감청을 생각해 보자. 먼저 감청이라는 명목으로 통신제한조치 허가서를 발부받는다. 그리고는 피의자가 사용하는 인터넷 회선에다 준비해온 감청용 회선을 브릿지(Bridge)하고, 거기에 노트북을 연결한 후 문제의 DPI 프로그램을 가동시킨다. 만약 감청 당시 피의자가 메일을 작성하여 송신한다면 어떠한가? 패킷으로 조각난 데이터들이 피의자의 컴퓨터를 떠나 회선으로 들어서자 마자 DPI 프로그램들이 작동하여 이들을 낚아챈다.

낚아채는 방식을 좀 더 구체적으로 살펴보자면, 크게 2가지 방식을 생각해 볼 수 있겠다. 먼저 패킷 자체를 납치한 후 국정원의 컴퓨터상에서 DPI하고, DPI가 끝나면 다시금 가던 길로 돌려보내는 방법이 있다.[76] 다음으로는 원본과 동일한 복사본을 즉시 만들고, 원본은 가던 길을 보내고 복사본을 국정원의 노트북 메모리나 하드디스크로 옮긴 후 천천히 DPI하는 방법이 있겠다.

이 양자 모두에 대하여 통신제한조치 허가서를 발부받는 것이 타당한가? 즉 후자의 경우 방금 작성을 완료하여 피의자의 하드디스크에 저장된 원본과, 패킷상태로 납치되어 국정원의 노트북에 재조합[77]해 담겨진

---

75) United States v. Councilman, 418 F. 3d 67, 79 (1st Cir. 2005).

76) 이 경우에는 패킷 전달의 지연현상이 발생할 것이다.

77) 패킷의 납치당시에는 조각들에 불과하더라도, 국정원이 당해 메일의 내용을 열람하기 위해서는 반드시 재조합이 필요하다.

사본은 어떤 차이가 있는가? 완벽하게 동일하다. 차이가 있다면 피의자의 컴퓨터에는 완성된 메일이 있을 것이나, 국정원의 노트북에는 일단 패킷화된 수많은 조각들이 들어왔다가 열람하는 순간 즉시 재조합되었다는 차이가 있을 뿐이다. 이는 결국 피의자의 하드디스크에 있는 메일 파일을 국정원의 노트북 하드로 복사한 행위와 동일하다. 두 컴퓨터의 랜카드에 다 랜선을 물려놓고 하드카피를 하는 경우와 같은 메커니즘인 것이다. 그렇다면 이는 통신제한조치 허가서가 아니라 압수·수색 영장이 필요한 것이 아닌가? 왜냐하면 영장을 발부한 법관이 그 대상을 '피의자의 당해 메일'이라고 지정했다면, 바로 이러한 복사의 방식[78]을 사용해서 압수를 실행할 것이기 때문이다.

이러한 문제점은 전자의 경우에도 동일하다. 왜냐하면 패킷을 납치하여 DPI한 후 돌려보낸다고 하지만, DPI를 하는 순간에 DPI프로그램이 당해 패킷을 읽어 들이면서 노트북의 메모리나 임시폴더에 저장하는 방식을 사용하기 때문이다. DPI가 끝나면 납치하여 담아두었던 원본은 가던 길로 돌려보내고 메모리나 임시폴더에 남아있는 복사본을 삭제하는 방식으로 프로그램은 진행된다. 즉 100개의 패킷을 DPI했다면 메모리나 임시폴더에 이미 100번의 저장이 있었던 것이다. 패킷을 잠깐 국정원의 노트북으로 이동하였다가 조사한 후 이를 다시 회선으로 이동시킨 것이 아니라,[79] 이 방식의 본질도 결국은 복사인 것이다.[80] 따라서 앞서 말한

78) 플로피디스크나 USB 메모리를 사용해도 동일하다. 이때에는 그 연결회선이 랜선이 아니라 플로피디스크 포트나 USB 포트가 되고, 저장매체가 노트북의 하드디스크가 아니라 플로피 디스크나 USB속의 메모리가 된다는 차이점이 있을 뿐이다.

79) 컴퓨터의 세계에 있어 진정한 물리적 이동은 있을 수 없다. 언제나 복사만이 있을 뿐이다. 예를 들어 A라는 장소의 B라는 파일을 C라는 장소로 옮긴다고 하자. 컴퓨터는 먼저 A장소의 B파일을 복사하여 C장소에 복사본을 만든다. 그 다음 A장소의 B파일을 삭제하고 사용자에게 C장소로 이동이 완료되었음을 알리는 것이다. 컴퓨터는 결코 B파일을 옮긴 적이 없다.

80) 메모리나 임시폴더에의 단 0.1초의 순간적 저장(소위 Buffering)도, 우리 법원의 해석에 의하면 엄연한 '복제(복사)'에 해당한다. 스트리밍 방식의 음원전송에 대하여 법원은 "인터넷 음악파일 컨텐츠 제공업체가 제공한 HTTP 방식에 의한 서비스의 경우, 이용자들이 노래듣기를 선택하면 위 업체 측의 서버에서 전송된 해

경우와 동일한 문제가 발생한다.

2.2. 감청대상의 포괄성

위의 사례에서 국정원은 피의자의 인터넷회선에 대한 통신제한조치 허가서만을 발부받았다고 가정하자. 이를 준수하는 것이 가능한가?

피의자의 컴퓨터를 오가는 길목을 지키고 있으므로, 피의자가 접속하는 모든 웹페이지 주소의 목록과 이동경로 및 로그인 정보, 해당 웹페이지에의 접속한 시간과 기간, 컴퓨터를 켜고 끈 시간 등 가장 정확한 통신사실 확인자료[81]를 손쉽게 덤으로 얻어낼 수 있다.[82]

그 뿐만이 아니다. 피의자가 만약 요즘 유행하고 있는 인터넷 전화를 사용하고 있다면 허가서에 없는 전화통화까지 저절로 들어볼 수 있다. 나아가 요즘 KT가 판매에 열을 올리고 있는 '쿡(Qook) 삼종세트'를 사용하고 있다면, 피의자의 거실에 상영되고 있는 '선덕여왕' 드라마를 같이 볼 수도 있다.[83]

당 곡의 컴퓨터압축파일(asf파일)이 이용자 컴퓨터의 하드디스크 임시폴더에 다운로드되어 재생되는데, 이와 같이 임시폴더에 다운로드된 파일은 미리 설정된 위 임시폴더의 사용공간이 다 채워지기 전에는 삭제되지 않고 위 임시폴더에 저장된 상태로 계속 남아 있게 되어, 이용자가 별도로 음원파일에 대한 복제행위를 하는지의 여부와 관계없이 HTTP 방식에 의한 서비스 자체만으로도 해당 곡의 음원파일에 대하여 저작권법 제2조 제14호에서 정한 복제가 이루어졌다고 할 것이므로, HTTP 방식에 의한 인터넷 음악제공 서비스는 음반제작자의 저작인접권을 침해하는 행위에 해당한다"고 판시한 바 있다(서울중앙지법 2006. 2. 15. 선고, 2005노480 판결). 이는 확정판결로서 이에 대한 대법원의 입장을 현재로서는 확인할 수 없으나, 미국의 경우에는 'Buffering'이 'Copy'인지에 대하여 소위 'cablevision 사건'에서 본격적으로 다루어진 바 있다.

81) 주소를 알게 되면, 클릭 한번으로 피의자가 보고 있는 동일한 웹 페이지를 국정원의 노트북 화면으로 출력해 볼 수 있다.

82) 즉 통신사실 확인자료의 요청을 위한 별도의 허가서는 필요없다.

83) 인터넷 회신에 대한 감청으로 전화와 TV까지 동시에 감청이 되는가 하는 의문이 있을 수 있다. 여기서 언급한 전화와 TV는 소위 인터넷 전화로 불리우는 'IP전화(VoIP)'와 'IPTV'를 말한다. 이들은 모두 인터넷 회선을 통하여 패킷화된 데이터로 서비스를 제공하고 있다. 사례로 든 '쿡 삼종세트'의 경우는 바로

피의자가 사용한 컴퓨터와 관련된 모든 정보와 내용은 기본이고, 피의자가 좋아하는 음악과 드라마, 최근 구입한 인터넷 쇼핑의 품목과 가격, 거실에서 받은 친구와의 전화통화 내용은 물론, 문을 걸고 혼자 몰래 감상한 야한 동영상까지, 말 그대로 전방위적인 정보를 단 한장의 허가서에 의해 몽땅 취합하게 된다. 그야말로 진정한 '포괄 허가서'의 사례에 해당한다.

국정원도 할 말은 있을 것이다. 일단 회선을 연결하여 DPI를 실행하면, 원래 계획에 없었던 정보까지 저절로 다 보인다고 항변할 것이다. 다시 말해 허가서에 특정된 정보만을 볼 방도가 없으니 통제가 불가능한 것이다. 이런 상황이라면 굳이 법원장이나 법관이 그 대상을 특정할 의미가 없으므로, 현재의 허가서나 영장의 양식은 더 이상 필요가 없다. 그냥 '종합감청'이라는 제목 아래에 승인 여부를 밝히는 서명란만 마련하면 충분할 것이다.

3. 소결

지금까지 살펴본 바와 같이, DPI 기술을 이용한 인터넷 감청은 현재의 우리 법체계로는 어림도 없는 상대이다. DPI를 활용하여 지득·채록한 데이터는 압수·수색 영장을 통해 입수한 저장 데이터와 구별되지 않는다. 이렇듯 적용법규가 모호하므로 수사기관의 입장에서는 어느 법률을 선택하든지 무방하다. 결국 당시의 상황에 따라 쉽고 유리한 법규를 선택하면 그만이다. 이러한 것이 헌법 제18조 및 제12조 제3항과 통신비밀보호법 제1조가 의도하는 바인가?

나아가 일단 DPI 기술이 감청의 목적으로 사용되면, 그 통제의 가능성이 전무하다는 점을 주목해야 한다. 법원의 사법적 통제는 물론이고, 그 내용과 대상에 있어서도 특정의 가능성이 없기 때문이다. 이로 인해 포괄영장(허가서) 금지의 원칙에 위반됨은 물론 심각한 프라이버시의 침해 또한 헤아릴 수 없는 정도이다. 이는 결국 현재의 통신비밀보호법 체계가

이러한 서비스들의 결합상품이다.

더 이상 디지털 매체를 상대로 유지될 수 없음을 보여주는 단면이다. 높아만 가는 기술현실과 고루한 법규정의 괴리가 너무나 현저하다는 것이다.

이제는 정말이지 새 틀을 짜야만 한다. 아날로그 감청을 상정하여 입법된 통신비밀보호법의 체계로는, 복잡·정교한 디지털 매체의 특성을 반영하여 함께 담아둘 수 없기 때문이다. 이미 디지털 매체를 전담하는 정교한 입법을 가지고 있는 미국의 경우에도, DPI 덕분에 또 다른 법안을 마련하고 있다. 웬만한 디지털 매체를 잘 감당해내던 미국입법조차도, DPI 앞에 와서는 그 독특한 특성덕분에 새로운 대응을 준비해야만 하는 것이다.

앞서 살펴보았듯, 미국에서 대응코자 하는 바로 그 DPI 서비스가 이미 우리나라에도 도입되고 있다(맞춤형 광고시스템). 동일한 기술에 대해 우리는 아직 아날로그 대응 입법으로 대강 꿰맞추어 보고자 하고 있는 셈이다. 가능이나 하겠는가?

Ⅳ. 나오며

지금까지 디지털 매체에 대한 감청에 관하여 '저장 데이터'와 '패킷 감청'으로 구분하여 살펴보았다. 결론적으로 이야기하고 싶은 것은 3가지이다.

첫째, 아날로그 감청과 디지털 감청은 그 본질과 내용에 있어 전혀 다르다는 것이다. 단지 두 경우 모두 '감청'이라는 용어를 함께 사용할 뿐이다.

둘째, 저장매체에 저장된 '저장 데이터'와 네트워크 회선상에서 DPI로 수집한 '패킷 데이터'는 그 본질과 내용에 있어 완전히 동일하다는 점이다. 단지 '분리와 합체'라는 형태적 상이와 '재조합의 완료'와 '재조합의 대기상태'라는 시간적 간격만 있을 뿐이다.

셋째, 현재 우리의 감청관련 규제체제가 디지털 매체에 대해서는 너무

나 무력하다는 사실이다. 저장 데이터를 제대로 규율하는 것도 아니고, 새로이 다가오는 DPI에 제대로 대응할 수도 없다.

결국 디지털의 속성에 걸맞는 새로운 전담입법이 필요하다는 주장을 하고 싶다.

글을 마치는 시점에서, 국제적으로도 문제가 된 바 있고 우리나라에서도 그 도입을 두고 논란이 일고 있는 'DPI형 맞춤 광고 시스템'에 관하여 마지막으로 언급하고 싶다. 이는 표면상의 형태에 있어서는 사용자 친화적인 색채를 띠는 흔한 상업프로그램에 불과하다. 그러나 그 실체에 있어서는 감청회선의 제공자와 감청수단의 개발자가 결탁한 형태이라는 점을 명심해야 한다. 감청의 주체로서 등장할 주인공이 비단 수사기관에 한정되라는 법은 없기 때문이다. 어쩌면 '감청의 상업화'야말로 가장 무서운 공포일지도 모른다.

<참고문헌>

김성훈, “통신비밀보호법 개정 관련 질의사항 검토”, 국회의원 이춘석·민주당 정책위원회, 수사·정보기관 통신감청 국민은 안전한가?, 통신비밀보호법 관련 토론회 자료집, 2008.

류제성, “통신비밀보호법 개정안(이학재의원 대표발의, 의안번호 제5261호) 및 형사소송법 개정안(박영선의원 대표발의, 의안번호 제5246호)에 대한 검토”, 송수신이 완료된 이메일 등 현대적 매체에 대한 통신비밀보호법제 토론회 발제문, 2009.

박경신, “헌법복원을 위한 18대 국회 형사소송법-통신비밀보호법-전기통신사업법 개정안”, 송수신이 완료된 이메일 등 현대적 매체에 대한 통신비밀보호법제 토론회 발제문, 2009.

박문성, “형사소송법과 전자문서”, 형사정책연구 제10권 제4호, 형사정책연구원, 1999.

오길영, “통신비밀보호법 개정안 비판”, 민주법학 제34호, 민주주의법학연구회, 2007. 9.

이은모, “전자적 정보에 관한 수사상의 문제점” 형사법연구 제23호, 한국형사법학회, 2005.

Allot Communications, “Digging Deeper Into Deep Packet Inspection(DPI)”, Allot Communications Ltd., 2007.

M. Chris Riley/Ben Scott, “Deep Packet Inspection: THE END OF THE INTERNET AS WE KNOW IT?”, Free Press, 2009.

Marc Rotenberg, “Communications Networks and Consumer Privacy: Recent Developments”, <http://energycommerce.house.gov/Press_111/20090423/testimony_rotenberg.pdf>.

Ohm, Paul, “The Rise and Fall of Invasive ISP Surveillance”, *University of Illinois Law Review*, 2009.

Public Knowledge, “Filtering Whitepaper: Legal Analysis”, <http://www.publicknowledge.org/paper/pk-filtering-whitepaper_5#ftn116>.

<Abstract>

Internet Wiretapping and Deep Packet Inspection

Oh, Kil-Young
Lecturer, Pai Chai Univ.

The Protection of Communications Secrets Act regulates both analog and digital media together without any distinction, which makes no sense because the one is totally different from the other in both form and characteristics. This article aims at demonstrating controversial issues about the regulation method of the Act in two ways.

This thesis intends to show that the limits of such regulation is clear especially in the case of 'stored data' like e-mails. It is not so clear in digital medium whether the transmission and reception is completed or not, and thus the completion of transmission and reception cannot be a meaningful standard for regulation. Also, specifying the target mail (account) of wiretapping is almost impossible. Furthermore, a seizure of the hardware itself would raise a serious concern about a blanket warrant.

Second, as to the DPI, usually called the Packet Inspection, this article emphasizes the necessity of a new legislation to eliminate the vagueness of related provisions and limit the scope of interception based on the general understanding of the technical meaning of DPI and the international trends of regulation.

Through these analyses, I reached a conclusion as follows:

First, the digital wiretapping is fundamentally different from the analog one in both essence and contents.

Second, the packet data as the target of a wiretap is completely

identical with the stored data as that of a search and seizure.

Third and finally, a totally new legislation suitable for the attributes of the digital medium is required.

Key Words: the Protection of Communications Secrets Act, internet wiretapping, stored data, packet inspection, deep packet inspection(DPI), shallow packet inspection(SPI)