

끝없는 도청·감청의 파장

도청·감청이 사회문제화 되어 국정감사 시즌이 되면 해마다 약방의 감초처럼 제기되고 있다. 이동통신업체들은 아날로그 휴대폰과는 달리 CDMA휴대폰은 데이터가 전화기마다 서로 다르게 암호화되어 전송되기 때문에 엿들을 수 없다고 한다. 하지만 정보통신기술은 초고속으로 발전을 거듭하고 있어 디지털 휴대전화의 감청기술도 머지않아 등장할 것이다. 어쨌든 감청이 국민의 프라이버시를 침해하는 도구가 되어서는 안되겠다.

해마다 9월 국정감사 시즌이 임박하면 한약방의 감초처럼 도청-감청 문제가 온 나라를 뒤흔든다. 감청 건수가 얼마나 늘어났는지, 통신 이용자의 신상 정보나 통화 내역이 얼마나 누설됐는지에 대한 통계수치가 신문에 대서특필된다.

정부의 장관들은 담화문을 발표해 '결코 수사기관의 불법 감청은 없으니 안심하고 통화하라'는 내용의 홍보전을 펼친다. 정치인들은 진지하게 마주 앉아 통신 프라이버시 보호를 위한 법-제도 개선을 노력하기 보다는 한탕주의 스타일의 폭로나 역폭로를 치고 받는데 열중한다. 한치도 바뀌지 않은 너무나 똑같은 풍경이 지난해에 이어 올해도 재현됐다.

디지털 휴대폰 감청 어려워

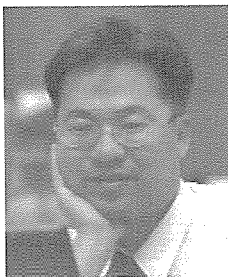
개인적으로 우리나라의 감청 관련 법률은 통신이용자의 통신 비밀을 보호하기 위한 것보다는 수사기관의 편의를 위한 측면이 많다고 생각한다. 개인정보 관리가 너무 허술해 보호받지 못하며 떠돌아 다니고 있다고 판단하기 때문이다.

감청이 사회문제화 될 때마다 나타나는 문제를 법-제도나 국민 감정의 시각이 아닌 기술적 측면에서 살펴보는 것도 의미있는 일이라 생각한다.

보통 유선전화의 감청은 아주 간단한 것으로 알려져 있다. 유선전화는 하나의 전화기에 하나의 가입자 선로(전화회선)가 있고, 이 회선들은 전화국의 실험실(MDF)로 모두 집결한다. 실험실에 모인 수많은 회선들은 각각의 고유번호가 있기 마련.

정확한 방법은 베일에 싸여 있지만 한국통신 전화국에서는 수사기관의 감청 요구가 들어오면 이 실험실의 특정 회선을 수사기관의 감청 장비에 연결시켜준다. 한국통신의 한 관계자는 "자세한 방법은 말할 수 없지만 요즘은 잠음이나 유도음 없이도 감청을 할 수 있는 수준"이라고 말하고 있다.

또 최근에는 감청문제가 불거지자, 경찰청은 휴대용 감청기기를 공개하기도 했다. 이 기기는 전화국의 협조가 있으면 경찰청내 뿐만 아니라 전화국이나 가정의 전화국 단자에서도



黃 順 賢

〈조선일보 경제과학부 기자〉

감청을 할 수 있는 기기이다.

하지만 감청이 이슈가 될 때마다 단골메뉴로 등장하는 디지털 이동전화의 경우는 약간 다르다. 정부와 이동전화 업체들은 “디지털 휴대전화의 통화 내용을 실시간으로 감청하는 것은 불가능하다”고 말한다.

‘듣는 것을 감독한다’는 감청(監聽)의 원래 의미하고는 너무 다르지만 이동전화에서의 감청이란 보통 특정 휴대전화 이용자의 음성사서함 비밀번호를 알아내 메시지를 듣는 것이거나, 실시간(Real Time)으로 통화 상대방의 위치나 전화번호를 알아내는 것이다.

올 상반기의 이동전화 감청 건수 4백25건은 통화내용을 엿듣는 것이 아니고 거의 대부분 상대방의 전화번호를 실시간으로 알아내는 것이었다는 설명이다.

보통 이동전화끼리의 통화는 휴대폰-기지국-교환국-기지국-휴대폰의 단계를 거쳐 이뤄진다. 이동통신업체들은 “아날로그 휴대폰과 달리 CDMA휴대폰의 데이터는 전화기마다 서로 다른 고유번호로 암호화되어 전송되기 때문에 엿들을 수가 없다”고 말한다.

최악의 경우 암호를 해독할 수는 있지만, 이 확률은 4조4000억분의 1이기 때문에, 통화 시간에 특정 시간에 이런 확률을 기대하는 것은 거의 불가능에 가깝다는 설명이다. 게다가 이동전화 시스템은 기지국이나 통신회선이 고정되어 있는 것이 아니고 순간 순간마다 변하기 때문에, 교환국이나 기지국에서도 통화를 엿들을

수 없다는 주장이다. 이동통신 업체들은 “슈퍼컴퓨터로 수십년을 검색해도, 특정 시간에 특정 통화의 데이터를 빼내는 것이 힘들다”고 말한다.

과연 그럴까. 대부분의 과학자 공동의 의는 것이지만 ‘100% 불가능’이라는 명제는 성립하지 않는다. 휴대전화 감청의 경우도 마찬가지라는 판단이 지배적이다.

사실 디지털 휴대전화도 유선전화와 디지털 휴대전화끼리의 통화는 당연히 감청된다. 즉 특정 유선전화 감청대상에 잡혀있을 경우, 이 유선전화기와 통화하는 내용은 그것이 휴대전화이든 일반전화이든지에 상관없이 감청할 수 있다. 즉 이동전화쪽에서는 감청할 수 없어도, 그 반대편인 일반전화쪽에서는 얼마든지 감청이 가능하다.

통신 프라이버시 침해 안돼야

문제는 디지털 휴대전화 끼리의 감청 여부이다. 주파수만 정확히 맞추면, 마치 라디오 중계방송처럼 통화 내용을 들을 수 있는 아날로그 휴대전화와 달리, 디지털 휴대전화는 감청이 무척 어렵고, 지금까지는 마땅한 감청장비도 없다. 하지만 이동통신 업체의 주장대로, 비록 극히 저조한 확률이지만, 디지털 휴대전화도 감청대상에서 벗어나지 못한다는 것이 일반적인 평가이다. 감청이 아니라 도청이지만 휴대전화기의 부품을 약간 조작하거나, 내부에 초소형 감청 기기를 집어넣어 무선으로 통화 내용을 듣는 사건도 최근 발생했다.

하지만 10년 전의 슈퍼컴퓨터와 지

금의 고성능 PC의 처리속도가 비슷한 것을 보라. 지금의 정보통신 기술 발달 속도라면 감청 수요(?)가 발생하면 얼마든지 디지털 휴대전화 감청 기술이 등장하리라는 것은 당연한 귀결이다.

요즘 화제가 되는 또 하나의 감청은 사이버 감청이다. 인터넷이나 PC 통신상에서의 이메일 등을 열람하는 것이 대표적인 사이버 감청이다. 수사기관들은 “비밀번호를 통째로 알아내서 감청하지는 못하고, 일부 이메일만 볼 수 있다”고 말한다. 하지만 파이어월 등 탄탄한 해커 방지 시스템을 채택한 네트워크도 해커의 공격으로 중요한 데이터가 누설된다. 한 인터넷 업체는 “루트(관리) ID를 가진 사람은 언제든지 특정 이용자의 이메일 내용을 열람할 수 있다”고 말한다. 메일 서버 관리자가 특정 메일 이용자의 패스워드를 알아내지는 못해도, 비밀번호를 바꿔 메일 내용을 볼 수 있다는 것은 상식에 속한다.

같은 풀이라도 소가 먹으면 우유가 되고, 독사가 먹으면 독이 된다고 했든가. 초소형 도청 기기 외에도 유리창에 무선 전파를 쏘아 대화 내용을 엿듣는 기술까지 등장했다. 살벌한 범죄가 판치는 이 세상에서 감청이 수사를 위해 꼭 필요한 것이라는 것은 당연한 논리이다. 발달하고 있는 감청 기술이 사회를 건강하게 만드는 버팀목이 될지, 아니면 국민의 통신 프라이버시를 침해하는 도구가 될지는 순전히 우리에게 달려있다. 불행하게도 요즘은 후자쪽이라는 느낌이 강하게 들지만. ㉟