<통신비밀보호법 관련 토론회 자료집>

수사·정보기관 통신감청 국민은 안전한가?

국회의원 이춘석 · 민주당 정책위원회

수사·정보기관 통신감청
국민은 안전한가?

○ 일시: 2008.12.11(목) 15:00~17:00

○ 장소: 국회의원회관 세미나실(104호)

○ 주최: 국회의원 이춘석 · 민주당정책위원회

수사·정보기관 통신감청
국민은 안전한가?

■ 개회행사

- 축　　사 1 ..... 원혜영 원내대표
- 축　　사 2 ..... 박병석 정책위의장

■ 좌장

- 이춘석 / 국회의원(민주당, 법제사법위원회 위원, 익산시 갑)

■ 기조발제 : 통신비밀보호법 개정안 비판

- 오길영(법학 박사, 민주주의법학연구회 기획부위원장).....

■ 토 론(가나다 順)

- 김상겸(동국대 법대 교수) .....
- 김성천(중앙대 법대 교수) .....
- 민경배(경희사이버대학교 NGO학과 교수) .....
- 이창범(한국정보보호진흥원 법제분석팀 팀장) .....
- 장여경(진보네트워크 정책활동가).....
- 최정학(방송대학교 법학과 교수).....

■ 서면 토론

- 강신각(한국전자통신연구원 통합표준연구팀 팀장) .....
- 김성훈(법무부 검사) .....

인사말

“아직도 줄지어 기다려서 통과 하십니까? 차안에서 편안하고 빠르게 통과 하십시오. 하이패스!” 라는 광고가 있습니다. 그런데 이 광고는 한 가지 중요한 사실을 빼먹고 있습니다.

“빠르게 통과하십시오. 그러나 당신의 프라이버시권은 보장받지 못 합니다”라는 말입니다. 그래서 일부러 하이패스를 하지 않는 사람들도 있습니다. 좀 빠르고 편리한 것 보다는 자신의 개인정보가 더욱 중요하기 때문입니다.

지하철이나 버스를 이용할 때 신용카드를 사용하지 않는 사람들도 늘고 있다고 합니다. 언제 어디에 갔는지 모두 기록되기 때문입니다. 그만큼 프라이버시 의식이 높아졌다는 것을 말해줍니다.

어제가 세계 인권선언 60주년 되는 날이었습니다. 우리 국민들의 인권의식은 날로 높아가고 있는데 현 정부는 반민주적이고, 반인권적인 정책을 펴고 있습니다.

그 중 대표적인 것이 통신비밀보호법 개정으로 헌법에 보장된 국민의 통신비밀의 권리를 침해하려는 시도입니다.

오늘 토론회를 통해서 통비법이 개악될 경우 인권침해의 심각성, 빅브라더의 출현 우려 등 심층적인 논의가 진행될 것으로 기대합니다. 감사합니다.

2008년 12월

국회의원 이춘석

축사

오늘 토론회 포스터를 보고 마치 반공포스터를 보는 것 같다는 생각이 들었습니다. 정부여당이 통비법을 개정해서 과거 안기부시절로 회귀하겠다는 발상을 포스터로 지적한 것 같습니다.

통신비밀은 국민의 기본권 중의 기본권입니다. 한나라당의 안대로 개정이 되면 통신사업자의 협력의무가 법제화될 것입니다. 이렇게 되면 모든 통신은 감청이 가능하게 되고 헌법상 보장된 통신비밀의 권리는 무용지물이 되고 말 것입니다.

우리 당은 이러한 시대착오적인 통비법 개정안에 반대하고, 국가인권위원회도 올해 1월 이 법안에 대해, 정확히 말해 당해 개정안의 주요내용과 동일한 2007년 개정안에 대해 “국민의 프라이버시를 크게 위축시키고 개인정보 보호에 역행하고 있음”을 지적한 바 있습니다.

이 법안을 막지 못하면 국정원이 마구잡이로 감청을 할 수 있게 됩니다. 어느 국민이 그것을 좋아하고 공감하겠습니까?

이번 토론회를 통해 반인권적이고 시대착오적인 통비법 개정안을 정부 여당이 더 이상 꺼내지도 못하게 쐬기를 박았으면 하는 바람입니다.

아무쪼록 오늘의 토론회가 성공리에 치러지기 바라고 함께하신 모든 분들의 건강과 행복을 기원합니다. 감사합니다.

2008년 12월

민주당 원내대표 원혜영

축사

통신비밀보호법 일부개정법률(한나라당)안은 인권침해 소지가 많아서 우리 민주당 당론으로 반대해 왔고, 오늘 이춘석 의원과 함께 토론회를 개최하게 되었습니다.

지금 휴대전화에 가입한 대한민국 사람이 4,538만 명입니다. 대다수의 국민이 휴대폰을 가지고 있습니다. 그런데 통비법을 '휴대전화 감청법'으로 바꿔버리면 어떻게 되겠습니까?

지난 9월 한나라당 정몽준 최고위원은 "누군가 내 전화를 엿듣는 것 같다"고 말했고, 국정원에 문의까지 했습니다. 집권여당의 최고위원이 도청에 공포 반응을 보였습니다.

국정원은 지난 정부 때도 X파일이다 뭐다 해서 사회적 물의를 일으켰습니다. 국가정보원법상 직무범위가 명시되어 있음에도 무시했는데, 통비법을 개정해서 합법화 시켜주면 '빅브러더'가 되고도 남을 것입니다.

통신감청이 법원의 영장을 통해 엄격한 통제를 받기 때문에 개정해도 문제될 것이 없다는 주장도 있지만 과연 그런지 의문입니다.

오늘 토론회를 통해 '수사·정보기관의 통신감청으로부터 국민은 안전한가?'를 냉정하게 따져보고 통신비밀이라는 헌법적 권리를 어떻게 보장할 것인지 방안을 모색하는 계기가 되었으면 합니다. 감사합니다.

2008년 12월

민주당 정책위의장 박병석

통신비밀보호법 개정안 비판

오길영[1)]

Ⅰ. 서설

통신비밀보호법은 아날로그 통신시대에 발생한 우리 사회의 불미스러운 경험을 바탕으로 탄생한 법률이다. 학생운동 탄압과 정치공작을 위한 도청으로 고통받아온 우리 역사에 대한 뼈아픈 반성을 담아내면서, 다른 한편으로는 국익을 위한 정보활동과 범죄수사를 위한 감청의 필요성 등 현실적 수요를 고려하여 헌법의 원칙아래 양 법익을 절충·수용한 법률이 바로 통신비밀보호법인 것이다. 즉 통신비밀보호법의 역할은 지속되어온 불법도청을 척결하고 법률이 허여하는 제한적인 경우에 실시되는 감청에 대해 예외적으로 합법성을 부여하는 것이다. 따라서 동법의 취지는 일차적으로 국민의 통신비밀보호권의 보장과 통신의 자유를 신장하기 위함이며, 감청 등의 통신비밀보호권 제한은 어디까지나 예외적·제한적인 경우로써 한정된 범주에서 엄격한 법적 절차를 거쳐야만 한다(통신비밀보호법 제1조.).

그러나 그간의 통신비밀보호법 운용사례를 살펴보면 참으로 많은 문제점이 발생되어 왔음을 알 수 있다. 범죄수사에 있어서의 감청 오남용은 물론, 정치공작사건으로 유명한 소위 X파일 사건, 그리고 대선때만 되면 감초처럼 등장하는 국정원의 불법감청 논란을 기억해 낼 수 있다. 이렇듯 뉴스의 헤드라인을 두들기는 통신비밀보호법의 폐단을 보아 오면서도 왜 정치권은 통신비밀보호법 개선을 의욕하지 않는 것일까? 또한 지속적으로 지적되어온 통신비밀보호법의 문제점을 방치하고 부작용 방지를 위한 학계에서의 논의를 뒤로 하는 이유는 무엇인가?

---

1) 법학 박사, 민주주의법학연구회 기획부위원장.

†

금번 통신비밀보호법 개정안은 또다시 이러한 폐습을 반복하고 있다. 종래의 고질적 병증을 방치한 채 새로운 병균을 주사하고 있어, 이대로라면 말그대로 권력을 위한 유용한 정치수단이자 전국민을 상대로 한 '빅브라더' 장치로 제대로 기능할 수 있겠다.

Ⅱ. 개정안의 주요내용과 문제점

이번 개정안[2]은 크게 다섯 가지의 내용을 담고 있다.

첫째, 휴대통신의 감청을 공식화하였다(개정안 제15조의2 제2항). 물론 현행법의 간접적 해석으로도 휴대통신의 감청은 가능했으나 여론을 의식하여 명시적으로 규정한 것은 아니었는데, 이번 개정안에서는 이를 공식화한 것이다.

둘째, 영업비밀 및 기술유출 범죄를 대상범죄에 추가하였다(개정안 제5조 제1항 제11호・제12호 신설). 너무 광범위하다는 지적이 있었던 대상범죄를 축소한 것이 아니라 오히려 확대하였다.

셋째, 위치정보를 통신비밀보호법의 대상으로 새로이 포함하였다(개정안 제2조 제11호 아목 신설). 법적 의미로서의 통신은 사람의 의사전달이어야 하는데, 위치정보는 말그대로 정보일 뿐 통신과는 무관한 내용이나 추적이 용이하다는 이유로 삽입되었다.

넷째, 통신사업자의 협조의무를 강화하여 감청협조시설 설치의무의 신설 및 Data Retention 제도를 본격화하였다(개정안 제15조의2 이하). 종래에는 단순한 협조의무에 불과하던 것이 이번 개정안을 통하여 모든 통신관련 사업자들의 강제의무로 자리매김하였으며, 감청협조시설 설치의무 위반의 경우 10억원의 과징금을 매년 한차례씩 부과할 수 있도록 하고(개정안 제15조의

2) 본고에서 말하는 개정안은, 이한성의원이 2008년 10월 30일자로 대표발의한 '통신비밀보호법 일부개정법률안'을 말한다. 이하에서는 편의를 위하여 간단히 '개정안'으로 표기하기로 한다.

3) Data Retention 의무위반의 경우에는 3천만원 이하의 과태료를 부과토록 하였다(개정안 제20조 제1항 제2호).

마지막으로 통신사실 확인자료 제공의 통지의무를 국가가 아닌 통신사업자에게 부과하였다. 앞으로는 자신의 통신사실 확인자료가 범죄수사를 위해 취합·제공·사용되었음을 국가로부터가 아니라 통신사업자(예를 들어 휴대통신 사업자나 인터넷통신 사업자)로부터 통지받고, 그 방법도 서면뿐만이 아니라 전자우편 등의 전자적인 방법으로도 가능케 하였다(개정안 제13조의3).

1. 휴대통신 감청의 공식화

> 개정안 제15조의2(전기통신사업자등의 협조의무)
> ① 전기통신사업자**등**은 ……
> ② **전화서비스를 제공하는 전기통신사업자, 그 밖에 대통령령으로 정하는** 전기통신사업자는 이 법에 따른 검사·사법경찰관 또는 정보수사기관의 장의 통신제한조치 집행에 필요한 장비·시설·기술 및 기능을 갖추어야 한다.

현행법의 해석을 통해서도 휴대통신의 감청은 가능하다. 제2조 제3호의 정의규정을 분석해보면 통신비밀보호법의 대상이 되는 '전기통신'은 '전화'를 포함하고 있고, 휴대통신의 특징인 '무선'의 전자적 방식에 의해 '음향'을 송수신하는 것도 전기통신에 포함되므로 휴대통신감청이 이번 개정안을 통해 새로이 등장한 이야기는 아니다.

그러나 현실적으로 휴대통신의 감청이 그리 쉽지만은 않았던 모양이다. CDMA 기술 자체가 통신자의 위치에 따라 감청대상 중계기기의 위치가 달라지므로, 특정 통신장비만을 장악한다고 해서 반드시 당해 대상자를 감청할 수 있는 것이 아니었다. 이러한 문제는 소위 CAS라는 이동식 감청기기로 일부 해결이 되었으나, CAS의 경우 감청을 위해서는 이동중인 통신자로

부터 200미터 이내에 있어야 했기 때문에 물리적 추적이 불가피하여 편리하지도 용이하지도 않았던 것이다.

이에 이번 개정안은 아예 휴대통신의 감청을 공식화해버린 것이다. 여론을 의식하여 직접적·명시적 규정을 피하던 현행법과는 달리 개정안 제15조의2 제2항에서 감청장비 설치대상자로서 '전화서비스를 제공하는 전기통신사업자'를 공식화하였다. 따라서 일반전화는 물론 휴대전화의 경우에도 공식적으로 감청의 대상에 포함됨을 밝힘과 동시에, 수많은 중계기에 흐르는 모든 전화서비스가 감청되어야 하므로 이제는 첩보용 밴을 끌고 다니며 CAS 기기를 작동시키던 수고를 덜게 되었다.

감청도 디지털인 것이다. 통신회사에 앉아 자판만 두들기면 감청도 척척 되도록 하자는 것이다.

(1) 프라이버시 침해의 증가

이미 일반 유선전화가 감청되는 바, 휴대전화의 감청이 새로울 것이 있는가 하는 논의가 있을 수 있다. 그러나 휴대전화에 대한 감청은 오늘날 가장 보편화[3]되어 있는 개인통신 수단인 동시에 그 사용자가 1인으로 특정되는 것이 일반적이므로, 지극히 내밀하고 사적인 부분에 대한 직접적인 침해가 되어 매우 신중한 검토가 필요하다.

지극히 내밀하고 사적인 부분이라는 점이 가지는 의미를 미국판례[4]상의 표현으로 옮기자면 '그에 합당한 프라이버시의 기대'(reasonable expectation of privacy)를 가진다는 점이다. 즉 누구나 사용가능한 공중전화보다는 일반 유선전화가, 가족이 함께 사용하는 일반 유선전화보다는 개인별로 소지하는 휴대전화가 프라이버시에 대한 기대가 높고, 따라서 우리는 잠재적으로 그

3) 방송통신위원회의 통계에 의하면 2008년 10월말 현재 유선전화 가입자는 약 2287만 명(점유율 33.3%), 휴대전화 가입자는 약 4538만 명(점유율 66%)에 달하여, 휴대전화가 일반 유선전화의 두배에 해당하는 점유율을 보이고 있다.
4) Katz v. United States, 389 U.S. 347.

에 합당한 프라이버시의 기대속에 대화의 내밀성을 조절하는 심리를 가지게 된다. 다시 말해, 공중목욕탕에서 타인으로부터 자신의 나신을 목격당할 때 느끼는 수치감과 자신의 집에 있는 샤워부스에서 전혀 예상치 못한 타인으로부터 자신의 나신을 목격당하는 경우에 느끼는 불쾌감을 동일한 수준이라고 볼 수는 없지 않는가?

따라서 가장 사적인 수단으로 파악되는 휴대전화의 감청으로 인한 법익침해의 정도는 공중전화의 감청으로 인한 법익침해에 비해 전반적으로 높다고 할 수 있다.

(2) 소비자와 사업자의 권리박탈

개정안은 전화서비스 통신사업자에게 감청집행에 필요한 장비・시설・기술 및 기능을 갖추어야 하고, 이는 다시 대통령이 정하는 기준・방법・절차에 적합하여야 한다고 규정하면서 강력한 과징금을 내걸고 적극적 추진을 의욕하고 있다.

뒤집어 생각해보면 범죄여부와 무관하게 모든 국민의 통신내용은 잠재적 감청대상이 되고, 한편으론 이제 감청에 적합하지 않은 정보통신사업은 더 이상 영위할 수 없게 하겠다는 취지이기도 하다.

이것은 국민의 자기정보결정권을 박탈하는 처사이다. 왜냐하면 국내의 모든 정보통신상품은 감청에 제공되는 상품으로만 구성되며, 소비자의 입장에서는 감청에 제공되지 않는 정보통신상품을 선택할 권리가 없어져 버리기 때문이다.

따라서 일단 정보통신상품을 구매하는 한, 소비자의 동의여부나 범죄여부와는 무관하게 무조건 감청대상에 포함되므로 헌법에 의해 국민의 손에 쥐어졌던 멀쩡한 권리 하나가 증발되어 없어져 버린다.

또한, 창의적인 기술개발을 저해하고 기업의 영업자유를 침해하는 결과를 초래한다. 사업자의 입장에서는 감청에 적합하지 않는 기술은 배척하게 되므로, 기술개발의 단계에서는 늘 감청적합성이 고려되게 된다. 결국 새롭게 등장하는 기술 및 사업은 시장에서의 성적표를 받아보기 전에 국가의 사전 심사를 받게 되는 셈이다.

이러한 논의의 핵심은 원래 국민에게 주어졌던 고유한 권리들을 국가에게 강제로 내어준다는 점이다. 또한 헌법이 마련한 고유한 권리를 국가의 필요로 인해 소멸시킬 때에는, 국민들과의 심도있는 논의와 깊은 양해가 전제가 되어야 하겠으나 이번 개정과정이 진정 그러했는가 하는 점도 또다른 쟁점이다.

2. Data Retention 제도의 본격화

개정안 제15조의2(전기통신사업자등의 협조의무)

② 전화서비스를 제공하는 전기통신사업자, 그 밖에 대통령령으로 정하는 전기통신사업자는 이 법에 따른 검사·사법경찰관 또는 정보수사기관의 장의 **통신제한조치 집행에 필요한 장비 · 시설 · 기술 및 기능을 갖추어야 한다.**

④ 제2항에 따른 장비·시설·기술 및 기능의 구비에 **소요되는 비용은** 대통령령으로 정하는 바에 따라 **국가가 그 전부 또는 일부를 부담한다.**

⑥ 전기통신사업자는 **1년의 범위 안에서 대통령령으로 정하는 기간 동안 통신사실확인자료를 보관하여야 한다.** 다만, 통신사실확인자료 중 위치정보에 대하여는 그러하지 아니하다.

개정안 제15조의3(이행강제금)

① 방송통신위원장은 제15조의2제2항을 위반하여 통신제한조치의 집

행에 필요한 장비·시설·기술 및 기능을 갖추지 아니한 전기통신사업자에 대하여 **1년 이내의 기간을 정하여 통신제한조치의 집행에 필요한 장비 · 시설 · 기술 및 기능의 구비의무를 이행할 것을 명할 수 있다.**

② 방송통신위원장은 제1항에 따른 이행명령을 받은 전기통신사업자가 시정기간 내에 **당해 시정명령을 이행하지 아니한 경우에는 10억원 이하의 범위 안에서** 대통령령으로 정하는 금액의 **이행강제금을 부과할 수 있다.**

③ 제2항에 따른 이행강제금은 최초의 이행명령이 있은 날을 기준으로 하여 **1년에 1회씩 그 이행명령이 이행될 때까지 반복하여 부과 · 징수할 수 있다.**

이번 개정안의 가장 큰 쟁점은 개정안 제15조의2 이하에 새로이 신설된 감청협조시설설치의무와 Data Retention제도이다. 제15조의2를 간략히 살펴보면 개정안은 통신사업자에게 통신제한조치의 집행에 필요한 장비・시설・기술 및 기능을 갖추어야 할 의무를 부과하면서(개정안 제15조의2 제2항) 그 비용은 국가가 전부 또는 일부를 부담하며(개정안 제15조의2 제4항), 통신사실 확인자료의 보관기간은 최장 1년으로 정하고 있다(개정안 제15조의2 제6항).

제15조의3은 이러한 의무에 응하지 않은 통신사업자를 대상으로 1년 이내의 기간을 정하여 구비의무의 이행을 명하고(개정안 제15조의3 제1항), 이에 따르지 않는 통신사업자에게 10억원 이하의 이행강제금을 부과할 수 있도록 하였는데(개정안 제15조의3 제2항), 이러한 이행강제금의 부과는 그 이행명령이 이행될 때까지 1년에 한번씩 반복적으로 부과・징수할 수 있다(개정안 제15조의2 제3항).

또한 통신사실 확인자료의 보관의무를 위반한 경우에는 3천만원 이하의 과태료를 방송통신위원장이 부과하도록 하고 있다(개정안 제20조 제1항 제2호).

요컨대 종래의 통신제한조치 또는 통신사실 확인자료의 이용에 대하여 통신사업자가 단순한 협조의무만을 가졌던 것에 반해(동법 제15조의2), 이번 개정안은 이를 법적 의무로 승격시킴으로써 통신사업자를 강제할 막강한 수단을 강구하게 된 셈이다. 그러나 이러한 개정안의 내용이 타당성을 가지고 있는지는 의문이다.

(1) 미국입법과의 비교

Data Retention제도를 운영하고 있는 가장 대표적인 국가는 미국이다. 1994년 미국이 입법한 바 있는 「법집행을 위한 통신지원법」(Communications Assistance for Law Enforcement Act of 1994, CALEA)[5]는 통신사업자가 감청 수행을 위하여 일정한 장비설치의무를 가지게 되는 것을 핵심으로 하고 있다. 따라서 금번 개정안의 도입에 있어 가장 큰 근거 또한 CALEA가 되겠다. 그러나 좀 더 면밀하게 살펴보면 몇가지 점에서 양자는 상당한 차이가 있다.

첫째, CALEA는 원래 유선전화나 휴대전화 등 전화통신의 감청에 대한 사업자의 협조의무를 강제하는 내용이였다. 즉 통신제한조치의 내용이 대상일 뿐 통신사실 확인자료에 해당하는 내용은 그 대상에 포함되지 않았다. 그 후, 인터넷전화 등의 IP 서비스 기반의 새로운 전화통신이 개발됨에 따라 CALEA의 적용범위 확대에 대한 이슈가 제기되었다. 즉, 새로운 전화서비스를 빌미로 한 인터넷 통신사실의 축적을 우려한 것이다.

주무기관인 FCC(Federal Communications Commission)는 설비기반 광대역 인터넷접속서비스 제공업자와 상호연동 VoIP(Voice over Internet Protocol)를 CALEA의 규제대상에 포함하기로 하였으나 여론[6]과 법원[7]으로부터 심

5) 47 U.S.C.A. §§ 1001-1010.
6) 이에 관한 내용은 <http://www.politechbot.com/2007/01/24/not-just-isps/>, <http://www.networkworld.com/columnists/2005/101705bradner.html> 등.

각한 반대에 부딪혀왔다. 이를 위해 두 번의 order[8]를 공표하는 등 FCC의 입장은 지속되고 있으나 아직도 CALEA의 적용범위를 둘러싸고 많은 이슈와 논란이 진행중에 있다.

여기에서 살필 수 있듯이 Data Retention제도의 도입은 법률을 개정하면서 조문을 손질하는 형식으로 간단히 해결될 만한 사안이 아니다. Data Retention제도를 도입함에 있어 미국과 같은 혼란을 피하기 위해서는 그 적용대상과 범위에 대한 신중한 고려와 다양한 논의가 선행되어야 하고, 따라서 국민여론의 검증과 통신사업자의 입장을 지속적으로 수렴하는 과정이 필요하다.

둘째, 대상사업자의 범위에도 차이가 있다. CALEA의 대상이 되는 통신사업자의 범위에 대한 FCC의 해석에 의하면, 우리 개정안의 경우처럼 전화통신사업자를 포괄[9]하는 것은 아니다. 설비기반 광대역인터넷접속서비스 제공업자와 상호연동 VoIP 서비스는 포함되나, PSTN(Public Switched Telephony Network) 연동 VoIP 서비스는 제외된다는 결론을 내린바 있다.[10]

이는 새로운 통신기술에 대한 법률적 함의를 심도있게 검토해가는 과정을 여실히 보여준다. 모든 신기술에 대해 무차별적 포함을 의도하고 있는 개정안은 이러한 기술적 기반에 대한 법적 고려를 담고 있는지 의문이다.

셋째, 개정안에서 밝히고 있는 사업자에 대한 이행명령, 이행강제금 부과, 강제금의 액수의 결정 등 강제조치의 주체는 주무관청의 장인 방송통신위원장이다. 그러나 CALEA의 경우 강제조치에 대한 주체를 법원으로 규정하고

---

7) 이에 관한 내용은 <http://www.techlawjournal.com/topstories/2006/20060505.asp>, <http://www.ipdemocracy.com/archives/2006/05/05/> 등.

8) 이에 관한 내용은 <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf>, <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf> 등.

9) 개정안은 제15조의2 제1항에서 종래의 '전기통신사업자'에서 '전기통신사업자등'으로 확대하여 그 대상을 막연히 확대하고 있으며, 제2항 법문에서는 '전화서비스를 제공하는 전기통신사업자 그 밖에 대통령령이 정하는 전기통신사업자'라고 표현하고 있다.

10) <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf>, 69쪽.

있다.[11] 따라서 사업자에 대한 강제집행은 사법심사를 거치는 구조를 가지고 있으며 법문의 내용 또한 상세한 요건을 마련해두고 있어 신중한 입장을 취하고 있다. 이러한 점은 주무관청의 장이 최악의 경우 10억의 강제금을 매1년마다 1회씩 부과할 수 있다는 우리 개정안의 입법태도와 대비된다.

(2) EU Directive와의 비교

유럽지역에 있어 Data Retention제도의 면모를 볼 수 있는 가장 모범적인 자료는 2006년 3월에 수정된 바 있는 EU Directive 2006/24/EC이다.[12] 당해 Directive는, Retention의 대상이 되는 Data를 정밀하게 분류하고 있는 것이 가장 큰 특징인데 '① 발신자를 확인하고 추적할 수 있는 정보(Article 5.1.(a).), ② 수신자의 신원을 확인하는데 필요한 정보(Article 5.1.(b).), ③ 통신의 날짜, 지속시간을 알 수 있는 정보(Article 5.1.(c).), ④ 통신의 유형을 알 수 있는 정보(Article 5.1.(d).), ⑤ 통신장비를 알 수 있는 정보(Article 5.1.(e).), ⑥ 이동통신장비의 위치를 알 수 있는 정보(Article 5.1.(f).)' 등 총 여섯가지로 구분하고 있다.

각각의 대상정보는 또다시 하부항목에서 정확하게 구분되어 규정되고 있다. 예를 들어, '통신장비를 알 수 있는 정보'는 '고정(네트워크)통신의 경우'와 '이동통신의 경우', 그리고 '인터넷 접속・이메일・전화'의 경우로 나누어지고,

첫 번째의 경우에는 'ⅰ) 전화번호 ⅱ) 가입자의 성명과 주소'를, 세번째의 경우에는 'ⅰ) 할당된 사용자 ID ⅱ) 개방네트워크에 접속한 때 할당된 사용자 ID와 전화번호 ⅲ) 통신당시 할당된 사용자 ID와 전화번호, IP주소를 사용한 가입자의 성명과 주소'를 Data Retention의 내용으로 정하고 있다.

---

11) Sec. 108. Enforcement Orders.

12) [2006] OJ L 105/54 : DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, <http://europa.eu.int/eur-lex/lex/ LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf>.

따라서 각 통신사업자는 해당하는 대상정보를 해당기간[13]동안 Retention하면 족하므로, 과잉수집의 위험을 원천적으로 방지하여 그 남용의 우려에 대처하고 있다.

한편, EU Directive의 가장 핵심적인 내용은 '통신의 내용을 알 수 있는 정보는 수집되어서는 안된다'는 근본원칙을 못박아 두고 있다는 점이다[14]. 즉, EU Directive는 미국의 CALEA와는 반대로 통신사실 확인자료만을 위한 규정일 뿐, 통신제한조치(감청)의 내용이 아니라는 것이다.

따라서 EU Directive를 수용한 유럽 주요국의 경우, 우리의 통신사실 확인자료에 해당하는 Data Retention 제도를 운영하고 있으나 이러한 장비의 설치가 우리의 통신제한조치(즉 감청)를 실시하기 위함은 아니다.[15]

우리의 금번 개정안에서는 남용가능성에 대비한 정교한 규정이나 근본원칙을 찾아볼 수 없다. 그저 통신사실 확인자료의 보관기간이 1년이라는 것만 밝히고 있다.[16] 따라서 우리의 경우 어떠한 목적의 감청이든 일단 시작이 되기만 하면 피의자를 둘러싼 1년 동안의 종합정보를 무차별로 수집할 수 있는 가능성이 있는 셈이다.

3. 위치정보 등 새로운 정보유형 추가

> **개정안 제2조(정의)**
> **11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.**

13) Data Retention의 기간을 6월 이상 2년 이하로 법정하고 있다 : Article 6.
14) Article 5.2.: No data revealing the content of the communication may be retained pursuant to this Directive.
15) 개정안의 해석에 의하면 전기통신사업자등이 설치·운용하게되는 장비는, 통신제한조치(즉 감청)의 집행과 동시에 통신사실확인자료의 1년간 보관을 위해 설치된다.
16) 규정내용에 대한 구체적 검토없이 1년과 2년이라는 Data Retention 기간의 물리적 비교는 큰 의미가 없는 것이다.

아. 「위치정보의 보호 및 이용 등에 관한 법률」 제2조제1호의 위치정보

개정안 제3조(통신 및 대화비밀의 보호)

① 누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다.

6. **위치정보사업 · 위치기반서비스사업 또는 긴급구조를 위한 개인위치정보의 제공** : 「위치정보의 보호 및 이용 등에 관한 법률」에 따른 **개인위치정보 제공의 경우**

이번 개정안에서 또하나 주목해 보아야 할 점은 '제2조 제11호 아목'에 신설한 위치정보의 추가이다.

위치정보는 말그대로 위치에 대한 정보로서 GPS 기능이 탑재된 휴대전화의 경우 단말기가 표시하고 있는 GPS(Global Positioning System)정보가 해당되겠다. 유의해야 할 점은 현재 통신사실 확인자료에 포함되는 발신기지국 위치추적정보와는 구분된다는 점이다. 발신기지국 위치추적정보는 현재 단말기가 가장 근접한 기지국과 휴대전화 단말기사이의 무선통신을 위해 마련된 무선통신분할망의 cell ID(Location Label)로써, 이는 대략 3-5km정도의 단위로 분할되어 있다.

이에 비해 GPS는 본래 높은 위치정확도가 요구되는 항공기의 자동착륙시스템, 측지, 이동체의 자세결정 및 정밀측위 등을 위해 개발된 기술이므로 그 측정오차를 줄이기 위한 보정기술이 정교하고, 따라서 GPS 위성신호를 수신하여 단말기에서 위치를 계산하는 GPS시스템의 측정오차는 대략 5미터 정도로 극히 미미한 것이 특징이다.

이러한 장점을 이유로 최근에는 GPS를 응용한 최신제품들이 쏟아져 나오고 있다. 가장 흔하게는 휴대전화나 차량용 네비게이션기기부터 여행지의 사진 위치를 기록하는 신형 카메라 제품, 심지어는 유아의 실종이나 유괴에 대비한 GPS 추적기능의 의류도 등장하고 있다.

개정안에 의하면 이러한 제품을 구매하여 사용하는 자는 누군가에 의해 저장된 자신의 위치정보를 통해 필요할 경우 근처 5미터의 거리까지 정확히 추적해내는 용도로 사용될 가능성을 용인해야 한다는 것이 된다.[17]

(1) 규정내용의 부적합성

위치정보는 통신비밀보호법상의 통신의 개념에 해당되지 않음이 명백하다. 법적 의미에서의 통신은 의사표시의 전달을 목적으로 하므로 그 내용은 '의사표시'이어야 하는데 반하여, 위치정보는 어떠한 의사표시도 담고 있지 않으며 순수한 정보체계일 뿐이다. 즉 GPS단말기의 위치정보시스템은 의사표시의 교신이 아니라 순수한 기술정보의 전산적 취급에 불과하므로 이는 통신개념에 포함될 여지조차 없다.

또한 위치정보는 통신비밀보호법상의 통신사실 확인자료에도 포함되지 않는다. 통신사실 확인자료는 최소한 통신이 존재함을 전제로 그 통신에 대한 사실 및 관련사항인데 반하여, 위치정보의 경우 통신의 여부와는 무관한 기계적인 신호의 교신일 뿐이다.

즉 등산객이 핸드폰의 GPS 기능을 사용하여 설악산 정상의 위도와 높이를 알아보았다고 해서, 이러한 행위를 전화통화로 보거나 전화통화와 관련되는 행위를 했다고 생각하지는 않지 않는가? 따라서 위치정보는 통신이나 통신관련 개념에 포함될 수 없고, GPS시스템은 전산체계이지 법적 의미에서의 통신체계가 아니다.

17) 즉 피의자의 핸드폰이 GPS기능을 탑재하고 있는 기종이라면 5미터 근처까지 정확히 추적 가능한 셈이다.

(2) 심각한 프라이버시 침해가능성

위치정보를 통한 추적행위는 무선통신분할망의 cell ID와는 달리 그 침해의 정도가 극히 내밀하다는 것이 가장 큰 문제이다. 공간적 비교만을 두고 보아도 기지국추적의 3-5km와 GPS추적의 5m는 현격한 차이가 있으며, 특히 5m라는 공간은 개인의 프라이버시를 말살하기에 충분한 근거리라는 점이다. 따라서 개정안대로 위치정보가 포함된다면, 우리는 항상 단장된 모습으로 생활하는 주의가 필요할 것이다. 이토록 투명한 물에 물고기가 행복하게 살 수 있는가?

이 점에 관하여는 미국에서도 동일한 논의가 있다. 2003년 9월 워싱턴 대법원은 "GPS 추적장치의 사용은 감시에 있어 특히 사생활 침해의 여지가 높은 방식으로 감시받는 사람의 일상에 대해 수많은 정보를 얻을 수 있다. 또한 피감시자는 차를 탈 때마다, 그리고 정차할 때마다 정부에 기록된다는 사실을 알지 못한다"라고 하면서 "워싱턴주 주민들은 이런 유형의 정부 간섭, 즉 GPS 기기가 자동차에 장착됐을 때의 환경에서 자유로울 권리가 있다"고 설시한 바 있다.[18]

(3) 정보통합으로 인한 남용가능성

위치정보가 가지는 또다른 문제점은 다른 유형의 정보와 통합하는 문제이다. 오늘날의 위치정보는 차량용 네비게이션 기기에서와 같이 순수한 위치정보 서비스만을 위해 사용되지는 않는다.

정보의 가치라는 것은 다른 유형의 정보와 통합하여 새로운 정보로 재탄생함에 있는 것인데, 특히 위치정보의 경우에는 단말기의 위치와 통신환경을

18) State v. Jackson, 150 Wash.2d 251, 76 P.3d 217(2003); 이 판결에 관한 논의는 <http://www.wisbar.org/AM/Template.cfm?Section=Wisconsin_Lawyer&template=/CM/ContentDisplay.cfm&contentid=47623>, <http://cyberlaw.stanford.edu/packets001557.shtml>, <http://writ.news.findlaw.com/aronson/20030917.html> 등이 있다.

특정하는 지표가 된다는 점에서 그 결합이 필수적으로 요구되는 핵심정보로서의 역할로 변모해가고 있다.

예를 들어 실내와 같이 제한된 공간에서의 위치추적을 위한 '이동통신 단말기의 위치추적'(Method for location trace of mobile communication station)의 경우나, GPS 위성탐색에 실패했을 경우 휴대통신 기지국을 이용하는 것을 내용으로 하는 'GPS와 중계기를 이용한 이동통신 단말기 위치추적방법'(A Method For Positioning Mobile Terminal with GPS and Repeater) 등은 위치정보 및 GPS기술과 휴대통신 기술의 병합을 잘 보여주는 예이다.

이러한 무선통신기술의 통합은 소위 유비쿼터스시대를 맞고 있는 지금으로서는 또 다른 혁신의 장을 앞두고 있는 상황이다. 현재 기술개발과 보급에 이어 이미 상당부분 상용화단계에 돌입하고 있는 RFID(radio frequency identification)와 USN(Ubiquitous Sensor Network) 기술은 현존하는 다른 통신기술과의 결합을 전제로 새로운 비즈니스 모델을 개발중에 있으며, 여기서 USN이 정보취합의 분류수단으로 위치정보를 기반으로 하고 있다는 점은 중요한 의미를 가진다.

즉 앞으로 대두될 유비쿼터스 컴퓨팅에 있어서는 대부분의 정보가 위치정보를 동시에 담게 되는데, 위치정보가 병합되어 있는 당해 통합정보를 위치정보로 파악하는 한 통신비밀보호법의 대상이 된다. 그러나 RFID와 USN에서의 취급정보는 지극히 사적인 개인정보이거나 실시간의 정황정보가 주를 이룬다[19]는 점에서 심각한 문제가 발생한다.

현재의 통신사실 확인자료와는 그 성질과 양에 있어 현격한 차이가 있어 과잉수집 및 남용에 해당됨은 물론이고, 의도하기만 하면 대상자의 사생활을 철저히 파괴하는 어처구니없는 상황이 연출되는 것이다.

---

19) 즉 한 개인의 현재 소지하고 있는 물건의 종류, 신체사이즈, 속옷의 메이커, 복용하고 있는 약물의 종류, 실시간 혈압·체온 등의 의료정보, 감정적인 흥분의 정도 등을 예로 들 수 있다.

Ⅲ. 개정필요 규정의 외면

법률의 개정은 법률 자체가 담고 있는 문제점을 개선하고 새로운 법적 수요를 수용하는 절차이다. 따라서 개정에 즈음하여서는 현행법의 문제점을 면밀히 검토하는 작업이 선행되어야 하고, 그 이후에야 새로운 법적 수요를 담아내기 위한 의견취합의 과정을 거쳐야만 한다.

그렇다면, 최근 또다시 대두된 통신비밀보호법 개정안은 어떠한가? 그 대답은 간단하다. 정치적 이슈가 되는 법률의 개정이 늘 그래왔듯 별볼일 없는 조항은 전혀 손대지 않았다. 즉 지속적으로 지적받아온 아래와 같은 문제점들을 외면하고 있는 것이다.

1. 부적절한 규정내용

> 통신비밀보호법 제7조(국가안보를 위한 통신제한조치)
> ① 대통령령이 정하는 정보수사기관의 장(이하 "정보수사기관의 장"이라 한다)은 국가안전보장에 대한 **상당한 위험이 예상되는 경우에** 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 다음 각호의 구분에 따라 통신제한조치를 할 수 있다.
>
> 통신비밀보호법 제8조(긴급통신제한조치)
> ① 검사, 사법경찰관 또는 정보수사기관의 장은 **국가안보**를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 **조직범죄 등 중대한 범죄**의 계획이나 실행 등 긴박한 상황에 있고 …… 규정에 의한 절차를 거칠 수 없는 긴급한 사유가 있는 때에는 **법원의 허가없이 통신제한조치**를 할 수 있다.

(1) 규정의 모호성

통신비밀보호법 제7조는 국가안전보장에 대한 상당한 위험이 '예상'되는 경우에 통신제한조치가 가능함을 밝히고 있다. 당해 법문의 표현에 의하면 다의적으로 해석가능한 국가안전보장에 대하여 그 위험이 '예상'되기만 하여도 통신제한조치가 가능하므로 정보수사기관의 자의적 판단에 의한 광범위한 기본권 침해가 가능하여 문제이다.

또한 감청의 주체에 대하여 정보수사기관의 장이라고 표현할 뿐 구체적으로 명시하지 않고, 통신비밀보호법 시행령에 위임하고 있다. 동시행령 제6조에 의하면 당해 주체는 '정보 및 보안업무 기획·조정 규정' 제2조 제6호에 규정된 기관을 말하는데, 이를 살펴보면 국외정보, 국내보안정보, 통신정보, 통신보안, 정보사범 등에 관한 정보 및 보안업무와 정보사범 등의 수사업무를 취급하는 각급 국가기관을 말한다. 결국 이 부분에 정통한 자가 아니고서는 당해 주체가 누구인지를 파악하기가 심히 곤란하다.

이러한 문제점은 동법 제8조 제1항에서도 발견된다. 사전허가의 절차없이 행하여지는 긴급통신제한조치는 그 요건이 명확히 특정될 필요성이 더욱 큰데 반하여, '국가안보'나 '조직범죄 등 중대한 범죄'와 같이 모호한 표현을 사용함으로써 그 남용 및 악용의 위험이 크다고 하지 않을 수 없다.

이러한 부분에 있어서의 내용은 형사법의 일종으로 파악할 수 있다. 즉 당해규정들은 형사법의 대원칙인 '죄형법정주의'와 '명확성의 원칙'에 정면으로 위배되는 것이다.

이러한 우려가 기우(杞憂)가 아님을 명확히 보여주는 통계가 있다. 법무부가 제공한 2001년부터 2006년 사이의 죄명별 감청현황 통계[20]를 살펴보면,

20) 김욱준, 「통신비밀보호법 개정안에 대한 의견」, 『통신비밀보호법 공청회 토론자료』, 2007, 13쪽.

살인(603회), 절도・강도(434회), 마약(48회), 성폭력범죄(27회), 미성년자 약취・유인(18회) 등 통상적으로 감청의 필요성을 공감할 수 있는 범죄에 대한 감청횟수에 비해 국가보안법위반(1023회)의 경우가 월등히 많은 감청영장의 발부가 있었음을 알 수 있다. 심각한 문제가 아닐 수 없다.

(2) 긴급성의 고려

나아가 감청에 있어서 긴급성이 고려될 여지가 있는지도 의문이다. 긴급체포에서의 긴급성은 인신체포를 위해서 발견 등 감각적인 인식과 현실적인 실력의 행사와 유지라는 물리적 행위가 필요하며 그에 임하는 사법경찰관은 현장에 구속되지만, 감청의 경우에는 그 행위 자체가 밀행성(密行性)을 가질 수밖에 없는 특성이 있기 때문에 이러한 물리적 구속은 불필요하다.[21] 단순히 일정한 기계장치를 작동하여 감청대상자의 통신을 추적하는 행위이므로 얼마든지 감청행위와 동시에 허가장을 청구하고 발부받을 수 있다.

따라서 늦어도 감청의 착수와 동시에는 법원의 허가장을 청구할 수 있으며, 허가없이 감청부터 착수하여야 할 긴급성을 상상하기가 어렵다. 또한 범죄의 계획・실행・실행했음을 충분히 의심가능한 범죄 및 국가안보에 대한 상당한 위험이 예상되는 경우에 한하여 통신제한조치가 인정되는 바,

이는 이미 범죄의 존재를 인지한 후의 경우이거나 상당한 정도로 수사가 진행된 후에나 가능하다는 의미이므로,[22] 사법경찰관이나 수사기관의 장이 범죄를 인지한 시점과 감청시점 사이에는 시간적 간격이 존재한다. 따라서 제5조 또는 제6조의 법문 자체가 긴급성을 배제하고 있다고 판단된다.

---

21) 안희출·구모영, 「통신비밀수사에 대한 문제점 연구」, 동아대학교 법학연구소, 『동아법학』 제37호, 2005, 95-96쪽.

22) 감청의 대상을 선정하고 적합한 수단을 강구해야 하므로, 감청을 시도한다는 자체가 대상범죄의 목적·대상·범위가 일정한 수준까지는 특정되었음이 전제되어야 가능하다.

2. 법원통제의 미비

> 통신비밀보호법 제8조(긴급통신제한조치)
> ② 검사, 사법경찰관 또는 정보수사기관의 장은 제1항의 규정에 의한 통신제한조치(이하 "긴급통신제한조치"라 한다)의 집행착수후 **지체 없이** 제6조 및 제7조제3항의 규정에 의하여 법원에 허가청구를 하여야 하며, 그 긴급통신제한조치를 한 때부터 **36시간 이내에 법원의 허가를 받지 못한 때**에는 즉시 이를 중지하여야 한다.
>
> 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차)
> ② 제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 …… 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 **지체 없이** 그 허가를 받아 전기통신사업자에게 송부하여야 한다.
>
> 통신비밀보호법 시행령 제37조(통신사실 확인자료제공의 요청 등)
> ② 동일한 범죄의 수사 또는 동일인에 대한 형의 집행을 위하여 **피의자 또는 피내사자가 아닌 다수의 가입자**에 대하여 통신사실 확인자료제공의 요청이 필요한 경우에는 **1건의 허가청구서에 의할 수 있다.**

통신비밀보호법은 통신제한조치나 통신사실 확인자료 제공의 경우 반드시 법원의 허가서에 의한 승인을 요건으로 하고 있다(동법 제6조-제7조, 제13조-제13조의4). 이러한 법원의 통제는 수사기관의 자의적 감청 또는 남용을 막기 위한 사법심사의 일종이고, 이를 근거로 우리는 기본권제한에 대한 실질적 신뢰성을 갖는다.

즉, "털어도 먼지 안나는 내가 무슨 감청을 당해?!"라는 국가에 대한 막연한 신뢰를 가지게 되는 것이다. 그러나 꼼꼼히 살펴보면, 통신비밀보호법이

규정하고 있는 법원의 통제는 그리 신뢰할 것이 못된다.

(1) 입법의 불비

먼저 법원의 허가서 없이 실시되는 범죄수사를 위한 긴급통신제한조치의 경우, '지체없이' 법원에 허가청구를 하여야 하고 '36시간 이내'에 법원의 허가를 받지 못한 때에는 감청을 중지하게 되어있으나 이를 역으로 생각해보면 36시간 이내이기만 하면 법원의 통제없는 자유로운 감청을 보장하는 셈이 된다. 예를 들어, 36시간 이내에 감청의 목적을 달성하였거나 혐의없음으로 내사종결한 경우에는 사법심사의 대상에서 제외되는 것이다.

둘째, 범죄수사를 위한 긴급 통신사실 확인자료 제공요청의 경우에는 36시간이라는 시간조차 정해진 바 없다. 동법 제13조 제2항은 '지체없이' 그 허가를 받아야 함을 규정하고 있기는 하나, 긴급통신제한조치에서와 같은 구체적인 시간규정이 없다. 따라서 법문의 해석으로는 요청의 중단시점을 알 수 없으므로 '지체없는 허가청구'는 실질적으로 사문화된 셈이다. 명백한 입법의 불비임과 동시에 위헌성을 내포하고 있는 규정이다.

셋째, 통신제한조치기간의 연장에 대하여 2월[23] 또는 4월[24]의 범위 안에서 연장을 청구할 수 있다고 규정하고 있으나, 그 횟수에 대해서는 함구하고 있다. 따라서 법문의 해석대로라면 2월 또는 4월의 기간 연장 청구를 반복할 수 있다는 것이 되는데, 이 또한 명백한 입법적 불비이자 위헌적 규정이다.

(2) 통제의 미비

긴급 통신사실확인자료의 요청의 경우 그 오남용의 통제가 불가능하다는 점이 문제이다. 피의자의 통신시기를 예측할 수 없는 감청과는 달리 통신사

23) 범죄수사를 위한 통신제한조치 기간의 연장 : 통신비밀보호법 제6조 제7항.
24) 국가안보를 위한 통신제한조치 기간의 연장 : 통신비밀보호법 제7조 제2항.

실 확인자료의 경우 일회의 열람으로 필요한 모든 정보를 지득할 수 있으므로, '긴급성'을 인정하여 법원의 허가이전의 자료취득 가능성을 인정하는 한 '지체없이'나 'xx시간 이내의' 등과 같은 시간적 제한을 통한 사후통제는 실질적으로 무의미하다. 즉, 증거로서의 기능을 고려하지 않는다면 사법경찰관은 옮겨 적거나 암기하면 그만이기 때문이다.

다음으로 한 명의 피의자를 쫓기 위해 발급되는 1건의 허가서에는 비단 피의자의 전화뿐만이 아니라 수명의 감청대상 전화번호가 있을 수 있다는 점이 심각한 문제이다.

통신사실 확인자료의 경우에는 동법 시행령 제37조 제2항에서 '동일한 범죄의 수사 또는 동일인에 대한 형의 집행을 위하여 피의자 또는 피내사자가 아닌 다수의 가입자에 대하여 통신사실 확인자료제공의 요청이 필요한 경우에는 1건의 허가청구서에 의할 수 있다'고 명시적으로 규정하고 있고, 감청의 경우에는 이에 해당하는 명시적 규정은 없으나 시행령 제9조에서 유사한 내용을 엿볼 수 있다.

실제 과거 정보통신부 보도자료에 의하면, 2006년 하반기 통신감청 허가서 1건당 대상 전화번호수는 6.06건이고, 통신사실 확인자료의 경우에는 허가서 1건당 대상 전화번호수는 3.66건이다.[25]

이는 결국 당해규정이 범죄와 무관한 일반국민을 잠재적 범죄자로 취급하는 것임은 물론 법원의 사법심사 기능을 정면으로 부정하는 심각한 위헌적 규정이라는 점을 증명해주는 셈이다.
마지막으로 허가서의 실질적 심사효과에 관한 문제이다. 아래의 자료를 살펴보면 법원의 청구대비 기각률은 실로 탄성을 자아내게 한다.

---

25) <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.

<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%

[자료출처 : 이춘석 의원실]

<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 : 이춘석의원실]

감청의 경우 최대 3.6%이하의 기각률을 보이고 있고, 통신사실 확인자료의 경우 거의 1% 남짓이다. 이러한 법원의 허가서 심사현황을 제대로 된 심사로 신뢰할 수 있는가? 다시말해 법원의 통제는 실제에 있어서는 사문화된 상황이다.

Ⅳ. 비판의 종합

1. 감청주체의 변화

금번 개정안의 가장 큰 특징은 실질적 감청주체의 변화이다. 종래 국가에 의해 직접 실시되던 감청이 이제는 통신사업자에 의해 주도되고 국가는 통신사업자를 통제하는 역할만을 하게 된다. 그렇다면, 이러한 '리모콘' 방식

은 타당한가? 법무부의 주장[26]처럼 '감청주체와 수사주체의 분리'가 감청의 오남용을 줄일 수 있는가?

예를 들어 통신사업자의 손에 놓여진 Data Retention이 과연 안전한가 하는 점을 살펴보자. 통신사업자는 근본적으로 경쟁시장에서 이익추구에 여념이 없는 상인이다. 이러한 상인의 손에 헌법상의 기본권을 제한하는 중요한 권한을 떠안겨도 좋은 것인가? 전망은 그리 밝아 보이지 않는다.

기업이 보유한 개인정보를 CD에 담아 유통·판매하다 적발된 뉴스는 이제 그리 신선한 뉴스가 못되는 상황이고, 게다가 국내최대의 온라인 게임업체인 '엔씨소프트'가 자사의 온라인 게임 '리니지2'에 대해 이용자들의 채팅을 불법감청하여 이를 소송의 자료로 제출하였다가 망신당한 사례가 있었다.[27]

또한 최근에 불거진 '옥션'과 'Daum'의 개인정보유출사건의 경우에는 그 심각성에 대하여 다언이 필요치 않은 상황이다. 이러한 사건들에서 볼 수 있듯이 현재 우리나라 기업의 입장에서는 감청의 합·불법의 여부나 통신비밀보호법의 내용이 무엇인지 또는 독수독과(毒樹毒果)가 무엇인지 하는 점은 그리 문제가 되지 않는다. 기업의 사회적 책임론을 운운하기 이전의 단계로써 오직 이익실현만이 급하고 중요한 시기이기 때문이다.

물론, 국가에 의해 자행된 지금까지의 불법 감청사례들은 우리를 경악시키기에 충분하였다. 그러나 국가에 의한 감청이 말도 탈도 많았다고 해서, 가까운 가게 주인에게 감청의 시행을 맡겨도 좋단 말인가? 이는 명백한 국가책무의 해태이자 포기이다.

2. 개정이유의 은폐

26) 김성천, 「통신비밀보호법 일부개정법률안에 대한 검토」, 『통신비밀보호법 공청회 토론자료』, 2007, 45쪽.
27) 이에 관한 상세는 <http://www.wownet.co.kr/news/vodnews/view2.asp?vodnum=5446> 참조.

이번 개정이 필요한 근본적 이유가 무엇인가 하는 점도 검토되어야 한다. 법무부가 밝히고 있는 바[28]와 같이 통신사업자의 교환설비를 거치지 않고는 감청을 할 수 없기 때문에 불법도청과 감청남용을 방지하기 위함이라는 주장은, 국민을 기만하고 현실적 문제점을 외면한 통신비밀보호법의 입법합리화에 불과하다.

집중된 정보에 비해 분산된 정보를 통제하는 것이 더욱 힘든 것은 자명하고, 미흡한 우리의 정보보호체제와 수많은 정보유출의 경험을 고려할 때 더욱 심각한 부작용이 예상됨을 법무부도 잘 알고 있을 것이다. 그럼에도 불구하고 굳이 개정을 의욕하는 근본적인 이유는, 신기술 기반의 새로운 통신수단의 경우 통신사업자의 협조 없이는 더 이상 감청자체가 불가능하기 때문이라는 기술적 한계에 기인한다.

따라서 이제는 더 이상 감청사실을 은닉할 수 없는 상황에 부딪힌 것이다. 즉 공식적으로 감청장비를 통신회사의 통신장비에다 상시로 설치해 놓고, 필요한 상황마다 손쉽게 연결해서 감청하겠다는 것이 금번 개정안의 정확한 취지이자 이유인 것이다.

결국 국가의 입장에서는 감청의 필요성을 포기할 수 없었기 때문에, 오남용의 위험성을 묵인하면서 불가피한 선택을 한 것이지 종래의 부조리를 개선하고자 함이 아니다.

3. 입법표절의 문제

이미 다른 국가에서 디지털 감청제도를 실시하고 있다는 점이 개정필요의 논거가 될 수는 없다. 통신비밀의 보호와 침해의 이익형량에 대한 대국민적 공감은 각 나라의 구체적 사정이 반영되어야 하기 때문이다.

---

28) 김욱준, 앞의 글, 17쪽.

앞서 살펴본 미국과 유럽의 경우에는, 많은 반발에도 불구하고 Data Retention제도를 도입한 공식적 이유는 끊임없이 발생해온 테러에 대한 우려 때문이었다. 물론 우리의 경우에도 테러위협에서 제외된 안전한 국가라 할 수는 없지만, 적어도 외국과 우리는 제도도입의 사유가 다르다.

한편, 기본권침해의 우려로 인하여 입법을 포기한 사례도 있다. 캐나다의 경우 헌법질서에 반한다는 이유로 정부가 추진한 'Lawful Access' Proposal[29]을 포기한 바 있다. 이는 통신사업자에게 감청이 가능하도록 협력의무를 부과하는 것(interception capability)과 통신사실(통신의 발신자, 수신자, 시간, 종류 등)을 저장하는 것을 내용으로 하는 전형적인 Data Retention 법안이었는데, 오랜 기간의 의견수렴을 거치면서 채택하지 않은 경우이다.

이렇듯 새로운 제도의 도입에 있어 실질적 필요성에 대한 검증과 구체적 배경을 고려하지 않는다면 이는 전형적인 입법표절이라 할 수 있다. 또한 외국의 기입법 사실이 입법필요성을 정당화할 수도 없다. 나아가 금번 개정안의 경우, 앞서 살펴본 바와 같이 그 표절조차 제대로 하지도 못하였다. 외국 기입법의 경우, 금번 개정안의 내용처럼 몰상식한 경우는 없기 때문이다.

4. 국가인권위원회의 의견 무시

지난 1월 국가인권위원회는 금번 개정안과 주요내용이 동일한 제17대 국회의 통신비밀보호법 개정안[30]에 대하여 "국민의 통신의 자유 및 사생활의 자유가 침해될 소지가 있다"는 이유로 반대의견을 표명한 바 있다.[31]

즉 ① 통신사실 확인자료에 위치정보를 추가하는 것에 대해 "개인의 모든

29) 이에 관하여는 <http://www.justice.gc.ca/en/cons/la_al/law_access.pdf>에서 살펴볼 수 있다.

30) 지난 제17대 국회에서 발의된 바 있는 당해 개정안은, '김정훈 의원안·김영선 의원안·최용규 의원안·김충환 의원안·양승조 의원안·정형근 의원안·박찬숙 의원안' 등 7건의 통신비밀보호법 일부개정법률안을 절충한 '법제사법위원회 대안(2007. 3.)'을 말한다.

31) <http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=555406> 참조.

정보가 노출되는 상황의 초래될 수 있어 개인의 프라이버시가 침해될 우려가 있고 수사기관 등에 의해 남용될 우려가 있으므로 이 부분은 삭제되어야 한다"고 판단하였고,

② 통신제한조치 집행에 필요한 장비 등의 의무화 부분에 대하여는 "국민적 공감대를 통해 사실상 금지돼오던 휴대전화 감청을 제도화 하는 것으로 사실상 감청 자체가 예외적 허용이 아니라 상시적으로 행해질 수 있는 것이라는 인식을 조성하면서 개인 사생활 및 프라이버시를 크게 위축시킬 수 있"고, "감청 집행의 필요장비 등의 보유는 규정하면서도 그 통제와 정보유출 차단기술·제도적 장치에 대해서는 미비해 사업자에 의한 악용과 프라이버시 침해 위험의 상시적 존재를 인정하는 결과를 초래할 수 있"다는 이유로 삭제를 권고하였으며,

③ 전기통신사업자가 통신 확인 자료를 보관할 의무를 규정한 부분에 관해서는 "아직 발생되지 않은 범죄 해결 목적으로 범죄 예비단계도 아닌 일반인 통신기록을 최대 1년간 보관하도록 한 것은 법제정 취지에 위배되고, 인권침해의 가능성이 높다"는 판단을 표명하였다.

이러한 국가인권위원회의 의견표명은 지금까지 밝힌 바 있는 필자의 주장과 일맥상통한다. 그러나 금번 개정안은 이러한 국가인권위원회의 의견을 철저하게 무시하고, 또다시 동일한 내용으로 개정을 의욕하고 있다.

참으로 어처구니가 없다. 학계와 시민단체, 그리고 국가인권위원회에 이르기까지 모두 한목소리로 외쳐대는 개정안의 문제점을 외면한 채, 도대체 무엇을 위해 이러는 것인가?!

통신비밀보호법 개정안 토론문

김상겸(동국대 법대 교수)

Ⅰ. 통신의 자유와 그 제한

헌법은 제18조에서 “모든 국민은 통신의 비밀을 침해받지 아니한다.”라고 하여 통신의 비밀불가침을 규정하고 있다. 헌법이 보장하는 통신의 비밀은 통신의 자유를 전제로 하는 것이기 때문에 이 조항은 통신의 자유에 대한 보장을 의미하는 것이다.

통신의 자유는 서신이나 전신, 전화, 팩스, 이메일 등에 의한 격지자간의 의사전달의 자유를 말하는 것이기 때문에 통신의 비밀을 보장한다는 것은 의사전달과정에서 그 내용이 공개되어서는 안 된다는 것을 의미한다.

통신의 자유가 헌법상의 기본권이기는 하지만, 헌법상 보장되는 통신의 자유는 합법적이고 정당한 통신만을 그 대상으로 한다. 우리 헌법은 절대적 기본권을 인정하지 않기 때문에 헌법 제37조 제2항에 의하여 법률로 제한을 할 수 있다.

통신의 자유 역시 국가의 안전보장이나 사회의 질서유지 및 공공복리를 위하여 필요한 경우 제한을 할 수 있다. 물론 자유권적 기본권에 대한 제한은 국가의 최고 규범인 헌법이 이미 그 권리를 보장하고 있기 때문에 최소한의 제한을 통하여 최대한 권리를 보장하자는 것이다.

이러한 취지에서 1993년 제정된 통신비밀보호법은 법의 명칭은 ‘보호’라고 되어 있지만, 헌법이 허용하는 범위 내에서 통신의 비밀을 ‘제한’하는 법이

다. 그렇기 때문에 통비법의 핵심은 그 제한의 범위와 방법이다.

통신의 영역은 정보통신기술의 급속한 발달로 비약적으로 확대되고 있다. 이런 시대의 흐름에 상응하여 통비법은 항상 개정의 필요성이 대두된다. 시대에 상응하는 법률의 개정은 국가권력의 자의적 행사를 방지하고 국민의 권리를 보호하기 위하여 필요하기 때문이다.

더구나 통비법은 과거 도·감청과 관련하여 통신의 자유에 대한 침해를 해결하기 위하여 등장한 법이란 점에서 더욱 그렇다. 시대의 변화에 따른 통신의 자유의 적정한 제한을 통하여 공권력행사의 투명성을 보장함으로써 국민의 권리가 보장될 수 있다. 그런 관점에서 이번 통비법개정안을 들여다보아야 한다.

Ⅱ. 통신비밀보호법 개정안의 내용과 평가

이번 통비법 개정안의 내용에 있어서 핵심은 새로운 통신매체로 자리 잡은 휴대전화에 대한 감청을 명문화한 것이라 할 수 있다. 이와 함께 대상범죄에 있어서 산업기밀의 유출을 방지하기 위하여 기업의 산업비밀과 영업비밀 범죄를 포함하였고, 감청의뢰기관과 감청장비의 운용기관을 분리하였으며, 감청절차에 있어서 투명성을 제고하기 위하여 영장제도르 강화한 것 등이다. 그 외에도 위치정보를 포함하고 통신사업자의 협조를 제도화하고 있다.

이 번 개정안에서 핵심이라 할 수 있는 휴대전화에 대한 감청은 발제문에서 보듯이 가장 논란이 되고 있는 문제이다. 논란의 핵심에는 휴대전화에 대한 감청을 명문화함으로써 합법적으로 개인의 프라이버시권을 침해할 수 있다는 것이다. 휴대전화의 가입자가 거의 전 국민이란 점에서 휴대폰 감청을 법제화하는 경우 전 국민이 대상이 될 수 있다.

그런데 통비법은 법률이기 때문에 당연히 대한민국의 영역에 있는 사람이면 내외국인을 불문하고 대상이 될 수밖에 없다. 그렇지만 감청의 대상은 통비법이 정하고 있는 범죄에만 국한된다.

감청이란 범죄수사를 위한 예외적인 통신제한조치로 통비법이 정한 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할 만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 법원의 허가를 받아서 하는 조치라는 점에서, 휴대폰을 감청의 대상기기로 하는 것에 대하여 개인의 프라이버시를 침해할 가능성이 높다는 것은 논리적으로 맞지 않는 것이다.

특히 오늘날과 같이 유선전화보다 휴대전화가 보편적 통신수단이 되고 있는 현실에서 이를 제외하거나 감청 자체를 무의미하게 하는 것은 법의 기능을 도외시하는 것이다. 그보다는 오히려 감청절차에 있어서 적법절차의 원칙이 지켜질 수 있는지 여부가 중요하다.

그런 점에서 볼 때 개정안은 영장제도를 강화하고 감청의뢰기관과 감청설비기관의 분리를 통하여 감청의 오·남용의 방지를 꾀하고 있다는 점에서 과거보다 진일보했다고 할 수 있다.

또한 개정안은 정보수사기관과 통신사업자에 의한 불법적인 감청과 감청설비의 오·남용을 차단하기 위하여 규정들을 두고 있다. 즉 통신사업자는 감청장비 등을 운용함에 있어 권한 없는 자의 접근 방지, 접근기록의 관리 등 대통령령에 따른 보호조치의무를 규정하고 있다.

이렇게 개정안이 통신사업자에게 감청설비 구축을 의무화한 것은 정보수사기관에 의한 불법적 감청 시도를 차단하기 위한 것이다.

통비법은 기본권제한법률이기 때문에 동 법에 명문의 제한규정이 없으면

국민의 기본권을 제한할 새로운 사유가 발생한 것만으로 제한할 수 없다. 이는 비례성원칙에 위반되는 것으로 위헌이다. 통신사업자에게 휴대전화의 감청에 필요한 설비와 기술 등을 갖출 것을 명문화하는 것은 감청의뢰기관 자체의 감청설비가 감청의 오·남용을 조장할 우려가 있기 때문이고, 감청을 위하여 통신서비스 자체를 제한하는 것은 아니기 때문에 이에 대한 문제는 없다고 본다. 그렇기 때문에 통신사업자가 새로운 기술을 개발하여 통신서비스 영역을 확대하는데 지장을 초래할 우려는 없다.

이 외에도 위치정보에 관한 내용이 개정안에 포함된 것은 휴대전화와 관련하여 밀접한 연관성을 갖고 있으며, 정보수사기관의 오·남용을 방지할 수 있는 제도적 장치가 있기 때문에 별 문제는 없다고 볼 수 있다.

Ⅲ. 기본권보장을 위한 감청제도의 운용을 위하여

법이란 규범은 사회질서의 유지를 통하여 공공의 이익을 보호하기 위하여 등장한 제도이다. 통비법에서 휴대전화의 감청을 허용하는 것은 시대의 변화에 대응하는 경험에 기초한다. 법은 경험의 산물이기 때문이다.

휴대전화의 감청이 전 국민의 잠재적인 통신의 자유를 침해할 지도 모른다는 것은 형사법이 전 국민의 신체의 자유를 위시한 기본권을 침해할 지도 모른다는 것에 다름 아니다. 감청의 오·남용의 문제는 휴대전화의 감청과는 별개의 문제이고, 발생 시에는 제재규정에 의하여 처벌하면 된다.

개정안은 현행 통비법상의 불법감청을 차단하기 위한 사전적·사후적 통제장치를 넘어서 정보수사기관이 영장에 의하더라도 통신회사를 거치지 않고 직접 감청하는 것을 금지하고 이를 위반하면 처벌하여, 자의적인 영장 집행과 영장 없는 감청의 가능성을 엄격하게 차단하고 있다.

그리고 통신사업자에 의한 악용 가능성 역시 차단하는 제도적 장치를 갖고

있다. 그렇기 때문에 오히려 이번 개정안으로 감청제도의 투명성이 제고될 수 있다고 본다.

앞으로도 통신기술의 발달이 법과 제도를 앞서 갈 것은 분명하다. 그렇지만 이 시점에서 통비법 개정안의 감청제도는 법이 정한 대상범죄로부터 국가와 사회 그리고 국민의 자유와 권리를 보호하기 위한 것으로 보아야 한다.

통신비밀보호법 개악이 우려 된다[32)]

민경배 (경희사이버대학교 NGO학과 교수)

전자감시 문제를 이야기할 때면 빠뜨릴 수 없는 인물이 두 명 있다. 제레미 벤담과 조지 오웰이다. 제레미 벤담은 “최대 다수의 최대 행복”을 실현하기 위해 공리주의를 주장한 철학자로 널리 알려져 있다. 그러나 그는 아이러니컬하게도 “최대 다수의 최대 감시”를 가장 효과적으로 실현할 수 있도록 고안된 팬옵티콘(원형감옥)의 설계자이기도 하다.

팬옵티콘은 감옥의 중앙에 높은 감시탑을 세우고, 원형의 벽면 둘레를 따라 죄수들의 방을 배치한 구조이다. 중앙 감시탑은 늘 어둡게 하고, 죄수의 방은 밝게 하여 감시자의 시선이 어디로 향하는지를 죄수들이 알 수 없도록 되어 있다. 팬옵티콘에 갇힌 죄수들은 자신들이 늘 감시받고 있다는 느낌을 가지게 되고, 결국은 죄수들이 규율과 감시를 내면화해서 자발적으로 복종하게 만든다.

이러한 팬옵티콘이 감옥 담장을 넘어 전 사회적으로 확장된 감시 국가를 소설로 묘사한 사람이 조지 오웰이다. 그의 대표작 <1884>의 무대인 가상의 국가 ‘오세아니아’는 절대 권력을 가진 통치자 빅브라더가 텔레스크린, 마이크로폰 등 첨단 감시 장치와 사상경찰을 동원해 사람들의 사생활을 철저히 감시하고 있다. 이곳 사람들은 자신의 의식과 사상까지도 통제당하는 끔찍한 세상을 허우적대며 살아가야 한다.

오늘날 현대인들은 팬옵티콘이 나와 상관없는 감옥 담장 안 일이라고 치부해 버릴 수 없는 상황에 처해 있다. 빅 브라더가 지배하는 오세아니아가 그저 소설 속에서만 존재하는 창작의 산물일 뿐이라고 안심할 상황 역시 아니다.

32) 이 글은 <디지털 타임즈> 2008년 12월 15일자에 게재될 예정인 칼럼입니다. 게재일 전까지 임의의 인용은 삼가해 주시기 바랍니다. 아울러 토론문이라기 보다는 보충의견 성격의 글임을 밝힙니다.

이미 감시의 시선은 현실 사회 곳곳에 뻗쳐 있다. 프랑스의 석학 푸코는 이를 가장 먼저 간파한 사람이다. 그는 자신의 저서 <감시와 처벌>을 통해 팬옵티콘의 원리가 사회 전반으로 파고들어 규범사회의 기본 원리인 팬옵티시즘(panopticism)으로 정착했음을 경고했다.

정보 기술이 빠른 속도로 발달하면서 이러한 푸코의 경고는 이제 엄연한 현실로 성큼 다가왔다. 전자 감시사회의 도래는 정보화의 그늘이 빚어낸 가장 치명적인 위협이다.

지금 정부와 여당이 또 하나의 팬옵티콘이 법이라는 이름으로 준비하고 있다. 통신비밀보호법 개정안이 그것이다. 얼핏 명칭만 보면 헌법상 보장된 기본권 중 하나인 국민 개개인의 통신 비밀을 보호해주기 위한 법처럼 들린다. 그러나 꼼꼼히 살펴보면 빅 브라더의 공포를 느끼게 하는 아주 위험한 내용들을 담고 있다.

이 개정안에서 가장 심각한 문제는 전 국민의 통신 내용을 수사기관이 감청할 수 있도록 제도적, 기술적 장치들을 마련해 주고 있다는 점이다. 이 개정안이 통과되면 전기통신 사업자는 수사기관의 감청 협조에 필요한 장비 등을 의무적으로 구비하고, 통신사실 확인 자료를 일정 기간 동안 보관하고 있어야 한다. 한 마디로 모든 국민이 자신도 모르는 사이에 감청 대상이 될 수도 있다는 이야기이다.

정부와 여당은 범죄수사나 국가안전보장 목적 외의 감청은 금지하고 있으며, 감청 대상 범죄의 종류도 제한하고 있기 때문에 모든 국민이 감청 대상인 것은 아니라고 말한다. 또한 범죄 예방과 원활한 수사를 위해서 반드시 필요한 조치임을 강조하고 있다.

그러나 팬옵티콘의 핵심 원리가 중앙 감시탑에서 실제로 감시를 하고 있느냐 여부와 무관하게 사람들에게 규율과 감시를 내면화하여 복종을 이끌어

내는데 있음을 다시금 상기할 필요가 있다. 언제든 자신의 통신 내용을 감청할 수 있는 법적 근거와 기술적 장비가 존재하고 있다는 사실만으로도 전자감시의 공포를 느끼기에 충분하다.

범죄 예방과 수사는 국민의 안전한 삶을 보장하기 위해 국가가 담당해야 하는 서비스이다. 그런데 통신비밀보호법 개정안은 오히려 모든 국민에게 수사기관을 위해 자신의 통신기록을 고스란히 제공하는 서비스를 요구하고 있다.

본말이 뒤집혀도 한참 뒤집힌 논리이다. 모든 국민을 잠재적 범죄자이자 수사기관을 위한 서비스 제공자로 취급하는 이 개정안이 도대체 누구를 위한 법인지 다시금 생각해 볼 일이다.

「통신비밀보호법」 개정안에 대한 검토의견

이 창 범[33]

Ⅰ. 개정안에 대한 총평

o 각종 테러, 밀수, 마약범죄, 산업기술유출 등 관련 범죄가 통신수단에 의존하는 비중이 날로 커지고 있는 현실을 고려할 때 수사기관 및 정보기관의 전자적 수사능력 보완 및 향상을 위하여 개정안의 전체적인 취지에는 공감함

o 그러나 발제가가 우려한 것처럼 아직은 수사기관·정보기관·통신사업자 등에 대한 국민의 신뢰가 높지 않고, 통신제한조치의 오남용 가능성이나 도감청 위험이 완전히 사라졌다고 보기도 어렵기 때문에 일부 보완적 조치가 필요함

o 또한, 우리나라 「통신비밀보호법」은 선진 제국의 감청법에 비해서 결코 보호 수준이 낮은 편이 아님에도 불구하고 많은 국민들은 「통신비밀보호법」을 통신비밀보호법으로 보기 보다는 통신감청법으로 보는 시각이 큼. 법의 집행·운용과정에서 그만큼 오·남용이 많았고, 국민들의 신뢰를 잃었다는 증거이기도 함

o 이에 따라 개정안은 범죄수사 또는 국가안전보장 목적 외의 감청 등 금지(안 제3조제2항·제3항 등), 불법적으로 취득한 통신사실확인자료의 증거사용 금지(안 제4조), 통신제한조치 집행위탁 또는 협조요청 의무화(안 제9조제1항), 신고포상금제도 도입(안 제15조의4), 보호조치 미이행에

33) 한국정보보호진흥원 법제분석팀장, 법학박사. **이 토론문의 내용은 토론자 개인의 생각이며 한국정보보호진흥원(KISA)의 입장을 대변하거나 표시하는 것은 아닙니다.**

대한 과태료 부과(안 제20조제1항제1호), 법위반에 다수의 벌칙규정 신설(안 제16조제1항제3호제4호 등), 양벌규정의 도입(안 제19조) 등 다수의 오남용 방지장치를 새로 마련해 두고 있음

o 이와 같이 개정안은 수사기관·정보기관의 불법감청에 대해서는 이번 법개정을 통해서 다양한 제재수단을 도입하고 있으나, 상대적으로 통신사업자에 대해서는 규제수단이 다소 미흡한 것으로 보임. 통신비밀과 사생활 보호는 헌법이 인정한 기본권이고 통신감청에 대해서는 국민들도 매우 민감하게 반응하기 때문에 2중, 3중의 안전장치가 필요함.

o 따라서 개정안에 반영된 다양한 방지장치 외에도 보다 안전한 정보통신 이용환경 정착을 위해 ①사업자의 감청업무 담당자 지정 및 관리·감독 의무, ②감청정보의 열람·복제·저장금지, ③감청정보의 위조·변조 금지, ④감청사실에 관한 정보의 삭제·제거·누락 및 위·변조 금지, ⑤보호조치의 파괴·훼손·변경 금지, ⑥보관중인 통신사실확인자료에 대한 보호조치 등을 추가적으로 검토하는 것이 바람직함

o 통신사실확인자료에 위치정보 추가, 통신사실확인자료의 보관의무화, 휴대전화 감청의 현실화 등을 이유로 이번 개정안을 혹평하는 견해도 적지 않으나, 이번 개정안에는 통신비밀을 보다 안전하게 보호하기 위해 진일보한 장치가 많이 반영되어 있다는 점을 고려할 때 좀 더 신축성 있게 대응할 필요가 있음. 사안별 검토의견은 아래와 같음

Ⅱ. 통신제한조치 대상범죄의 조정(안 제5조제1항)

o 최근 산업기술이나 영업비밀 유출이 주로 정보통신망을 통해서 이루어지고 있는 점을 고려할 때 「영업비밀보호법」과 「산업기술유출방지법」 위반 범죄를 통신제한조치대상에 포함시킨 것은 타당하다고 생각함

o 미국, 영국 등 대다수 선진국에서 일정한 조건하(사전고지의 원칙, 노사협의의 원칙, 사생활보호의 원칙 등)에 영업비밀유출 등의 방지를 위해 사용자에 의한 근로자의 감청을 허용하고 있지만, 우리나라의 경우 통신당사자 쌍방의 동의를 얻어야 하기 때문에 현실적으로 사용자에 의한 적법한 통신감청이 어려움

o 따라서 최소한 수사당국이라도 산업기술 유출 등의 범죄행위를 조기에 발견하여 유출을 차단할 수 있도록 통신제한조치의 대상에 포함시킬 필요가 있음

Ⅲ. 통신제한조치 집행 위탁 또는 협조 요청 의무화(안 제9조제1항)

o 통신제한조치의 집행권한과 실제 집행행위를 구분하는 것은 통신제한조치의 남용 방지를 위해 바람직한 것으로 판단됨

o 다만, 집행행위의 민간위탁으로 인한 통신제한조치의 오용 가능성 및 감청정보의 유용·유출 가능성에 대비하여[34] 개정안에 반영된 기술적·관리적인 보호조치(안 제15조의제5항)와 함께 법제적인 안전장치도 필요함

- 개정안은 감청시설에 대한 권한없는 자의 접근방지, 접근기록관리 등 대통령령으로 정한 보호조치의무를 부과하고(안 제15조의2제5항), 감청으로 지득한 내용을 범죄수사 또는 국가안전보장 외의 목적으로 사용을 금지하고 있으며(안 제3조제3항), 통신제한조치에 관여한 통신기관의 직원 및 관련공무원의 비밀준수의무(법 제11조)를 명시하고 있지만[35] 이것만으로는 충분하다고 볼 수 없음

34) 감청기술은 국제적 기술표준에 의해서 개발·운영되기 때문에 사실상 통신기관의 임직원이 감청내용 등을 열람·복제·유출할 가능성은 희박하지만, 그럼에도 불구하고 법적인 안전장치는 필요함

35) 통신제한조치에 관여한 통신기관직원 및 공무원에 대한 비밀준수 의무 규정은 현재도 있는 조함임(제11조 참조)

o 보다 안전한 장치를 위해 ①통신기관 임직원의 감청정보 열람·복제·저장 행위 금지, ②감청정보의 위조·변조 금지, ③감청사실에 관한 정보의 삭제·제거·누락 및 위·변조 금지, ④보호조치의 파괴·훼손·변경 금지, ⑤통신기관의 감청업무 담당자 지정 및 관리·감독 의무 등을 신설하고 위반한 자에 대한 처벌을 명시해야 함

o 아울러, 안 제15조의2 제6항에 따른 통신사실확인자료 보관의무와 관련하여 보관중인 통신사실확인자료의 유출 및 오남용 방지를 위한 기술적·관리적 보호조치 의무도 추가되어야 함

- 정보통신서비스제공자의 경우 「정보통신망법」에 따라 보관 중인 개인정보에 대해서는 기술적·관리적 보호조치가 의무화되어 있으므로 이미 충분한 보호장치가 마련되어 있다고 볼 수 있으나, 「정보통신망법」에 따른 보호조치의무를 명시하는 것이 바람직함

Ⅳ. 통신제한조치 집행에 필요한 장비등 구비의무(안제15조의2, 제15조의3, 제17조제1항제7호, 부칙 제4조)

o 감청 장비나 설비를 수사기관이나 정보기관이 직접 보유·운영할 경우 지금까지의 경험상 오·남용 가능성이 더 크므로 통신기관이 보유·운영하게 하는 것이 바람직할 것으로 보임

- 미국의 「법집행을 위한 통신지원법」(CALEA)은 그 법의 명칭에서도 알 수 있듯이 통신사업자에게 자신의 통시시스템이나 서비스에 관계없이[36] 법집행기관을 지원하기 위하여 필요한 능력과 충분한 설비를 갖

36) 미국 CALEA상의 감청범위는 전통적인 유선전화 이외에 VoIP, 브로드밴드기반 서비스, 다이얼 업 인터넷액세스, circuit switched voice service(회선교환식 음성서비스) 등도 포함되는 것으로 해석되고 있다.(Congressional Research Service, Digital Surveillance : The Communications Assistance for Law Enforcement Act, June 8, 2007)

추도록 의무화하고 있는 바, 이는 통신비밀보호와 공공이익을 조화하기 위한 조치임

o 다만, 개정안 부칙 제4조에 규정된 감청장비 구비 유예조치를 새로운 통신기술과 서비스에 대해서도 인정받을 수 있도록 현실적으로 감청기술의 개발·채택이 어려운 경우에는 방송통신위원회의 심의를 거쳐 일정기간 감청장비의 구비를 유예해 주는 것이 바람직할 것임

- 개정안 부칙 제4조는 이 법 시행 당시 통신제한조치의 집행에 필요한 장비·설비 및 기능을 갖추지 못한 경우 이동전화사업자는 이 법 시행 후 2년 이내에, 그 밖의 전기통신사업자는 이 법 시행 후 4년 이내에 갖추도록 예외를 인정하고 있고,

- 그 기간 내에 통신제한조치의 집행에 필요한 장비·설비 및 기능을 갖추지 못할 이유가 있는 경우에는 그 기간을 연장하여 줄 것을 방송통신위원장에게 신청할 수 있도록 있도록 하고 있음

V. 불법 도·감청에 대한 신고포상금제도의 도입(안 제15조의4)

o 사회적 감시를 강화함으로써 불법 도·감청을 견제·예방하기 위하여 신고포상금제도를 도입한 것은 바람직한 조치로 사료됨

o 다만, 수사기관 자체도 불법 도·감청의 주체가 될 수 있다는 점에서 포상금의 지급주체를 수사기관으로 하는 것은 실효성이 부족함. 신고자의 신분이 보호될 수 있고 객관적 입장에서 조사가 가능한 제3의 기관으로 하는 것이 바람직함

한국 도감청 역사와 통신비밀보호법 개정

장 여 경[37]

1. 정부의 도감청 약사

(1) 군사정권의 도감청[38]

군사정권은 한국에서 감시기술을 선도하는 역할을 하였다. 군사쿠데타로 집권한 박정희 정부 하에서는 1961년 중앙정보부 내에 20명으로 구성된 과(課) 단위의 도청 조직이 유선전화 도청을 시작하였고, 1968년에는 60명의 단(團) 규모가 약 70만 명의 전화가입자를 대상으로 도청을 실시하였다.

역시 군사쿠데타로 집권한 전두환 정부의 말기에는 1,000만 회선으로 전화의 대중화가 이루어졌고, 한국통신공사가 발족하여 통신 감청을 협조 지원하는 체계로 확대되었다.

전두환 정부를 이어받은 노태우 정부 시절인 1988년 이후에 국가기간전산망 사업을 실시할 정도로 청와대가 국가의 정보화를 주도적으로 이끌었고, 이와 더불어 감청을 확대하기 위한 기술개발을 동시에 병행하였다.

1988~89년에는 국회 국정감사에서 국가에 개발되었다고 추정되는 감청 기술, 일명 '블랙박스'를 둘러싼 논쟁이 일었다. 당시 야당의 주장에 의하면 전두환 정부에서부터 '비음성 통신용 전송품질측정시스템'이 전국에 44개나 설치되어 있는데, 이것이 전화를 감청하는 일명 '블랙박스'라고 하였다.

---

37) 진보네트워크센터 활동가

38) 이 절의 내용은 고성학, "한국의 민주화와 감시권력의 변화 - 민주화 이전 정부와 이후 정부의 비교", 숭실대학교 대학원 정치외교학과 박사학위 논문, 2005.12. 참조.

이 주장에 따라 국회는 1989년 9월 28일 광화문국제전화국 ITMC 시설에 대해 현장검증을 실시하였지만 관련자들은 이 시설이 감청 장비가 아니라고 부인하였다.

군사정권 하에서의 감시체계는 반공주의를 국민들에게 강요하면서 감시의 내면화를 도모하였고 감시기술 면에서 새로운 기술을 습득하고 개발하여 감시의 일상화를 꾀하였다.

감시기구 측면에서는, 중앙정보부와 1980년에 이를 개편한 국가안전기획부(안기부), 국군보안사, 검찰·경찰 등의 국가기구와 당시의 체신부, 한국전기통신공사와 같은 하위기구를 체계적으로 구축하여 감시기술을 활용해 왔다.

군사정권은 자의적인 국가권력을 행사하며 개인의 기본권과 표현·결사의 자유를 보장하지 않았다. 군사정권은 쿠데타를 이용하여 권력을 잡으면서 발생한 정당성의 위기를 극복하기 위하여, 감시권력을 확대하고 합법적인 폭력성을 권력유지의 수단으로 활용하였다.

(2) 문민정부 이후의 도감청

1992년 12월 제14대 대통령 선거를 앞두고 당시 법무장관 등 정부 주요기관장들이 부산의 한 음식점에 모여, 여당 후보를 당선시키기 위해 지역감정을 부추기고 야당 후보를 비방하는 내용을 유포시켜야 한다고 입을 모았다.

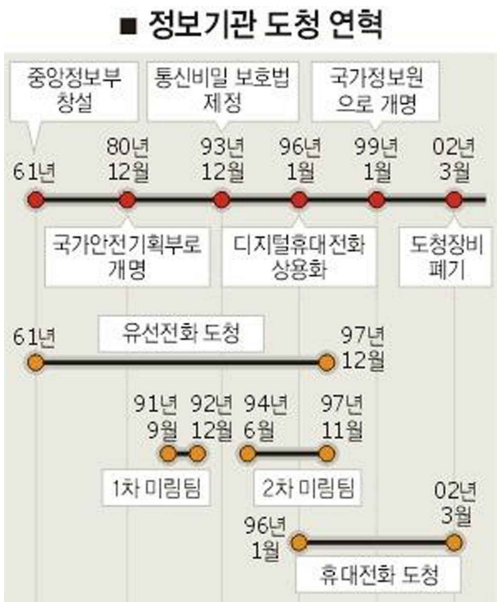
이러한 대화 내용은 한 야당 후보 측의 도청에 의해 언론에 공개됐고 온 나라가 큰 충격을 받았다. 이 사건으로 인하여 여당 후보인 김영삼씨는 대통령에 당선되자마자 집권 초기부터 도청을 방지하기 위한 법률 제정을 논의하기 시작하였다.

1993년 12월에는 마침내 통신비밀보호법이 제정되어 법률적 근거 없이 시

행되던 정보/수사기관의 도청이 제도화하기에 이른다.

그러나 2005년 7월 21일 안기부의 불법도청 테이프(일명 X-파일) 사건이 언론 보도를 통해 밝혀지면서 한국 사회는 또다시 큰 충격에 휩싸였다. 통신비밀보호법에도 불구하고 김영삼 정부 하에서 안기부(1999년 1월 국가정보원으로 개편)는 불법적인 도청전담 조직을 과거와 같이 유지하였고 정치적 목적으로 도청하였다는 사실이 드러난 것이다.

김영삼 정부는 이전의 군사정권과 마찬가지로 1994년부터 본격적인 불법 감청을 시작하고 1996년 1월부터는 이탈리아 B사로부터 아날로그 휴대전화 감청 장비 4세트를 구입하여 1999년 12월까지 사용하였다. 이 장비는 1~2개월 단위로 수십 차례 불법 사용됐고, 사용자가 현장에서 번호를 입력하는 식으로 활용됐다.



* 출처 : 서울신문 2005.12.15자.

또한 안기부의 비밀 도청 조직인 미림팀은 유선전화 도청 부서인 과학보안국에서 대상자의 회동에 대한 도청 자료를 넘겨받은 후 회동 장소에 미리 가서 송신기를 설치한 뒤 대화 내용을 도청했다.

검찰이 전 미림팀장 공운영씨의 집에서 압수한 도청 테이프 274개와 녹취록 13권에 나타난 도청 건수는 총 554회. 도청 피해자 가운데는 정치인이 273명으로 가장 많았고, 고위 공무원 84명, 언론계 인사 75명, 재계 57명, 법조계 27명, 학계 26명, 기타 104명 등이었다.

특히 처음으로 야당으로서 집권한 김대중 정부 하에서도 도청이 계속 이루어

진 것으로 드러났다. 1998년과 1999년 언론을 통해 "CDMA 휴대전화는 기술적으로 감청이 불가능"하다고 누차 확언하였던 김대중 정부는 이면에서 CDMA 휴대전화 감청 장비를 직접 개발한 것으로 밝혀져 주목을 끌었다.

당시 국가정보원(국정원)은 1996년 1월부터 디지털 휴대폰이 상용화되자 유선중계통신망 감청장비인 'R-2'(1998년 5월 개발 완료)와 이동식 휴대전화 감청장비인 '카스'(1999년 12월 개발 완료)를 직접 개발해 8국 사무실에 감청장비를 차려놓고 도청에 활용했다.

R-2는 이동통신사의 상호접속교환기와 KT의 관문교환기가 연결돼 있는 전화국에서 '유선중계통신망' 회선을 분리, 연결해 해당 통신망을 통과하는 통화를 감청하는 방식으로 감청하였다.

유선전화의 실선 구간은 전화번호마다 부여된 실선 하나하나에 대해 감청장비를 연결해야 하지만 중계통신망은 여러 번호의 통화가 이뤄지는 통로인데다, 휴대전화라도 유선망을 통해 중계된다는 점에 착안해 유선중계통신망에 대한 감청을 실시한 것이다.

'R-2'라는 명칭은 당시 사용되던 중계통신망의 신호 방식을 부르던 명칭에서 유래했다. 국정원은 R-2에 정치·언론·경제·공직·시민사회단체·노동조합 간부 등 주요인사 1,800여 명의 휴대전화 번호를 입력해 놓고 24시간 이들의 통화를 도청했다.[39]

CAS는 45kg 정도의 무게인 이동식 휴대전화 감청 장비로 차량에 탑재시켜 감청대상자로부터 약 200미터 이내에 접근해 감청대상 휴대폰의 주파수, 기지국 위치, 단말기의 고유번호 등을 알아낸 뒤 암호화된 음성정보를 해독해 단말기와 기지국간의 무선구간 통화를 감청하는 장비이다.

---

39) "임동원·신건씨 감청장비 개발에도 관여", 연합뉴스 2005.12.2; "수사발표서 등장한 도청장비·용어", 연합뉴스 2005.12.14; "중정·안기부 36년간 전화국 `관리'", 연합뉴스 2005.12.14; "도청정보 이용한 김현철씨도 도청당해", 동아일보 2005.12.15.

CAS는 CDMA(부호분할다중접속) Analysis System의 약자다. 국정원은 카스 20세트를 만드는 데 19억 원을 투입하는 등 불법 도청 장비를 개발하는 데 31억여 원의 예산을 쓴 것으로 나타났다. 2001년 12월 통신비밀보호법이 개정되고 감청설비를 신고해야 할 상황이 되자 안기부는 2002년 3월 불법 도청팀을 해체하고 이들 장비들을 전량 폐기하였다.

안기부 과학보안국은 유선 전화에 대해서도 법원 허가 없이 광화문, 혜화, 영동, 신촌, 신사, 목동 전화국에서 매주 1~2회씩, 1회에 감청 대상자 유선 전화 회선 2~3개를 안기부 회선에 연결했다. 전화국 협조가 필요했기 때문에 보안상 대규모 도청은 어려웠지만, 주요 인사들에 대해서는 빠짐없이 도청이 이뤄졌다고 검찰은 전했다. 해당 전화국 관련자에게는 보안 유지 대가로 매달 10만~50만원이 지급됐다.

한편 안기부와 별도로 대검찰청, 경찰청, 세관, 국방부 등 다수의 기관이 역시 정부로부터 인가받지 않고 기업체를 통하여 감청 장비를 불법적으로 수입하였다는 사실이 밝혀지기도 하였다. 2005년 8월 24일 천정배 법무장관은 국회 예산결산특별위원회에서 대검찰청이 1995년 3월 미국산 휴대전화 감청기를 도입하는 등 1998년까지 총 8대의 아날로그 휴대전화 감청기를 구입하여 불법적으로 사용하였다고 밝혔다.

(3) 평가

한국 정부의 도감청 경향을 평가하여 보면, 범죄 수사보다는 정치적 목적에 의하여 불법적인 감청이 실시되어 왔으며 이를 주도한 것이 안기부와 같은 정보수사기관의 비밀 권력이었다는 점을 알 수 있다.

특히 1996-99년 사이에 감청장비 구입이 급증하였다는 사실이 흥미롭다. 이 시기 전후로 특별히 범죄율이 급증하였다는 증거는 없다. 다만 대통령 선거와 정권 교체가 있었으며 IMF로 경제 상황이 극도로 불안정하였다는 정치

경제적 특수성이 존재할 뿐이다.

무엇보다 1996년 12월에는 국가안전기획부법이 개정되었다. 인권유린과 정치적 악용의 소지가 많았던 국가보안법 제7조(찬양고무 등)와 제10조(불고지죄)에 규정에 대한 안기부의 수사권이 부활한 것이다.

안기부의 수사권 부활은 정치권력의 요구에 따라서 남용될 소지가 있는 것으로 지적되어 왔다. 정보수사기관은 감청을 '통상적인 범죄수사가 불가능할 경우에만 선택하는 최종적 수단'으로 인식하지 않고, 최초의 수단으로 선택할 수 있는 특권으로 인식하는 경향이 있었다. 정보수사기관의 정보독점을 이용하려는 권력집단의 정치적 이해관계가 도감청을 조장하며 국민의 통신의 비밀과 기본권을 소홀히 취급하였다.

[표1] 2005년도 정보통신부 국회제출자료

구분	1994~95	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005.7	계
다우니 정보통신	-	10	10	5	10	8	10	8	8	14	10	93
한국델콤	-	210	307	114	175	-	-	1	2	4	-	813
기타업체	1	-	-	-	-	-	-	6	2	-	2	11
계	1	220	317	119	185	8	10	15	12	18	12	917

통신사업자는 이 과정에서 불가피하게 불법 감청에 협조하였다. 2000년 5월 12일 감사원은 "통신제한조치 운용실태 감사결과"를 발표하였다. 감사 결과에서는 수사기관에 의한 불법적인 도감청은 물론이고 이에 대한 통신사업자들의 협조가 있었던 것이 문제로 지적되었다.

전화국 담당자들이 법원의 감청 영장 등을 확인하지 않고 감청 요청에 응했는가 하면 협조대장에 감청내역조차 기록하지 않았고, 각 통신회사들이 휴대전화와 무선호출기, 음성사서함 감청을 요청하는 수사기관에 메시지 내용을 제출하는 것이 아니라 아예 비밀번호를 넘겨줌으로써 수사기관이 감청 종료 이후에도 계속 감청을 할 수 있도록 하였다고 한다.[40]

수사기관의 긴급감청이 확인서를 제출하지 않은 채 이루어지거나 허용된 기간을 초과하여 이루어지는 데에도 통시사업자들이 이에 동조하였다. 허가가 만료된 후에도 감청 회선이 해지되지 않고 계속 감청에 사용되기도 하였다. 긴급감청의 절차를 지키더라도 이를 수사기관 직원 누구나가 감청을 집행하는 것으로 드러났다.

긴급감청을 협조 요청할 수 있는 자는 검찰, 경찰, 국정원, 국방부 등에서 일정 직급 이상이어야 하지만, 사실은 검찰직원, 순경, 이병 등 부서 내에서 임의적으로 담당하는 사례가 다수 발견되었다. 그러나 통신회사는 불법임을 인지하더라도 협조를 거부할 경우 신분상 가해질지도 모르는 불이익으로 인하여 이를 거부하기 어려운 입장이다.

또한, 통신 기술의 보급이 늘어나면서 감청 역시 확대되어 왔다. 과거 군사정권은 주로 미행과 신체적 감시를 통하여 정부에 비판적인 세력을 밀착감시하였다. 1970년대 말부터 1980년대 초반까지 한국의 정보화 수준은 매우 낮은 편으로서 1973년 전화가입자는 76만 명에 불과하였다.

1979년 이후 전화의 적체를 해소하기 위하여 정보통신에 대한 투자가 확대되고 1987년 전화가입자가 1,000만 회선을 넘기까지 감청은 특정 소수층을 상대로 시도되었다.

[표2] 통신수단별 가입자 현황 (단위 : 천명, %)

구분	1996	1997	1998	2000	2002	2004
유선전화	19,600	20,425	20,624	21,967	23,490	22,870
이동전화	3,131	6,911	13,983	26,816	32,342	36,586
인터넷이용자	731	1,634	3,103	19,040	26,270	31,580

40) 1997년 1월 1일~1999년 6월 30일까지 14개 별정통신사업자는 2,288회에 걸쳐 모두 3,494개의 비밀번호를 수사기관에 제공하였다. 감사원의 지적 이후에도 불법행위는 계속되어 2000년 5월 정보통신부의 발표에 의하면 휴대폰, 호출기의 음성사서함에 있는 메시지의 내용을 출력하여 수사기관에 제공하는 방식이 아니라 긴급감청용 휴대전화를 포함한 4,050개의 개인 휴대전화, 무선호출 음성사서함의 비밀번호가 그대로 제공되었다.

그러나 전화보급이 대중화되고 연이어 휴대전화나 인터넷의 보급이 늘어나자 이에 부응하는 감청 기술의 개발이 이루어졌다. 특히 휴대전화는 1996년 CDMA 방식의 PCS 상용서비스가 시작되면서 이용자가 급증하여 1999년 유선전화 가입자를 초과하였다.

2008년 3월 현재 국민의 90% 이상(약 4,426만 명)이 이동통신에 가입되어 있으며 이용행태는 전화와 SMS는 물론이고 무선데이터통신, DMB, 위치정보서비스, 영상통화 등으로 확대되고 있다.

2008년 상반기 한국사회를 뒤흔들었던 촛불시위 당시에는 다수의 시위 참가자들이 시위현장 및 이에 대한 경찰의 진압을 와이브로 모바일 기술을 이용하여 인터넷으로 생중계하여 큰 관심을 모았다. 이러한 상황과 비례하여 휴대전화 등 신기술에 대한 감청 역시 증가하여 왔다.(3절 참조)

일반적으로 정보화는 감시권력의 범위와 능력을 신장시킨다고 할 수 있다. 정보화가 진전될수록 권력의 감시 방식은 비인격적이고 전자적인 데이터 감시로 이동하며, 유선전화, 휴대전화, 인터넷 등 모든 통신수단을 아우르는 통합감시가 가능해진다. 이는 미행이나 신체적 감시에 따른 피감시자의 저항과 노출 위험으로부터 자유롭게, 보다 광범위한 사람들에 대한 보다 광범위한 정보 수집이 가능해졌다는 의미이다.

2. 최근의 감청 현황

한국에서 수사기관의 감청 및 통신자료 제공은 다음과 같이 이루어지고 있다. 첫째, 유선전화의 통화 내용에 대한 감청은 통신비밀보호법에 따라 검찰, 경찰, 국정원 등 수사기관이 법원의 허가서를 통신사업자에게 제시하고 협조를 요청한 경우에 이루어진다.

다만 실시간 통신이 아닌 이동전화의 문자메시지, 인터넷·PC통신의 전자우편이나 비공개모임의 게시내용은 통신비밀보호법의 보호대상이 아니기 때문에[41] 압수하는 방식으로 이루어지고 있어 문제를 지적받고 있다.

통화 상대방, 통화일시, 위치정보, 인터넷 IP주소와 같은 로그기록 등 통신사실확인자료는 통신비밀보호법에 따라 수사기관이 법원의 허가를 받아 통신사업자에게 요청한 경우에 제공된다.

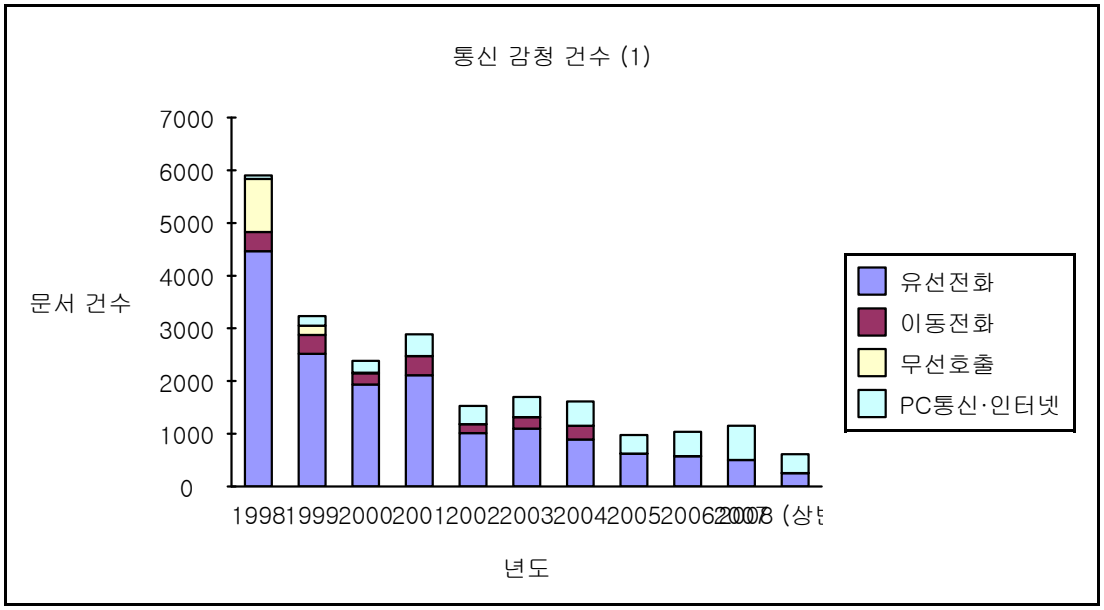
다만 가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료는 통신비밀보호법의 보호대상이 아니기 때문에 수사기관이 통신사업자에게 서면으로 요청서를 제시하면 간단히 제공될 수 있다. 자세한 현황은 다음과 같다.[42]

(1) 통신 감청

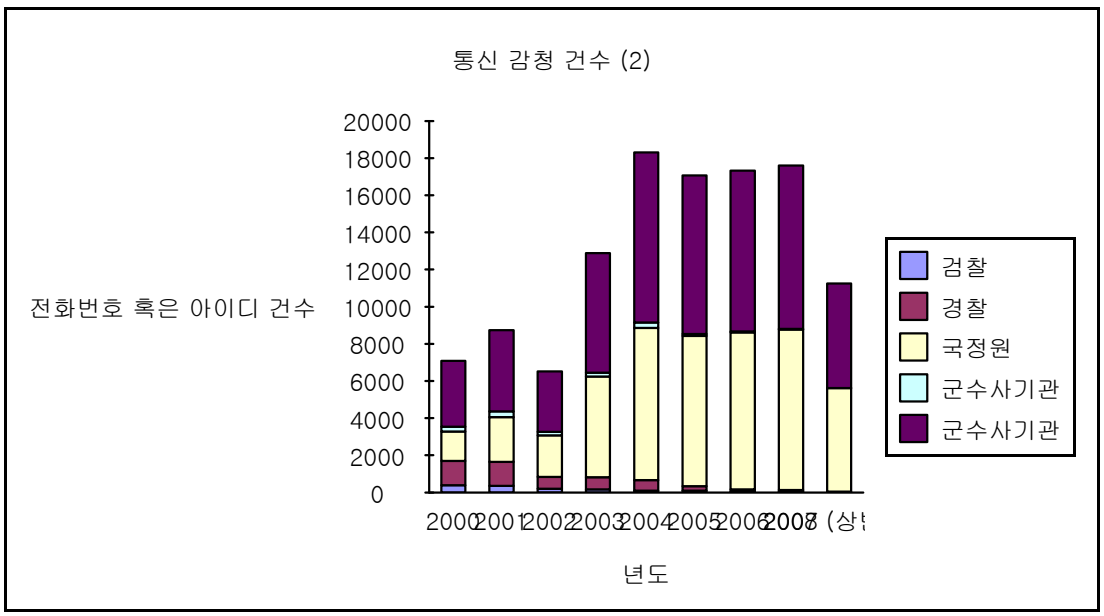
아래 자료에 따르면 감청 요청 문서 건수가 줄어들기 때문에 감청이 표면상 감소하여 온 것으로 보인다. 특히 무선전화 감청이 2005년 자취를 감춘 것은 사실이다.

2004년 12월 대학수학능력시험 부정 사건을 수사한다는 명목으로 수사기관이 수능시험이 있던 날에 보내진 전 국민의 모든 문자메시지를 검색할 수 있는 영장을 법원으로부터 발부받아 실제로 약 2억 건의 문자메시지를 검색했던 사건이 발생하였고, 이로 인하여 수사기관의 마구잡이 문자메시지 감청에 비판 여론이 높아졌던 것과도 관련이 있지 않을까 추정해 본다.

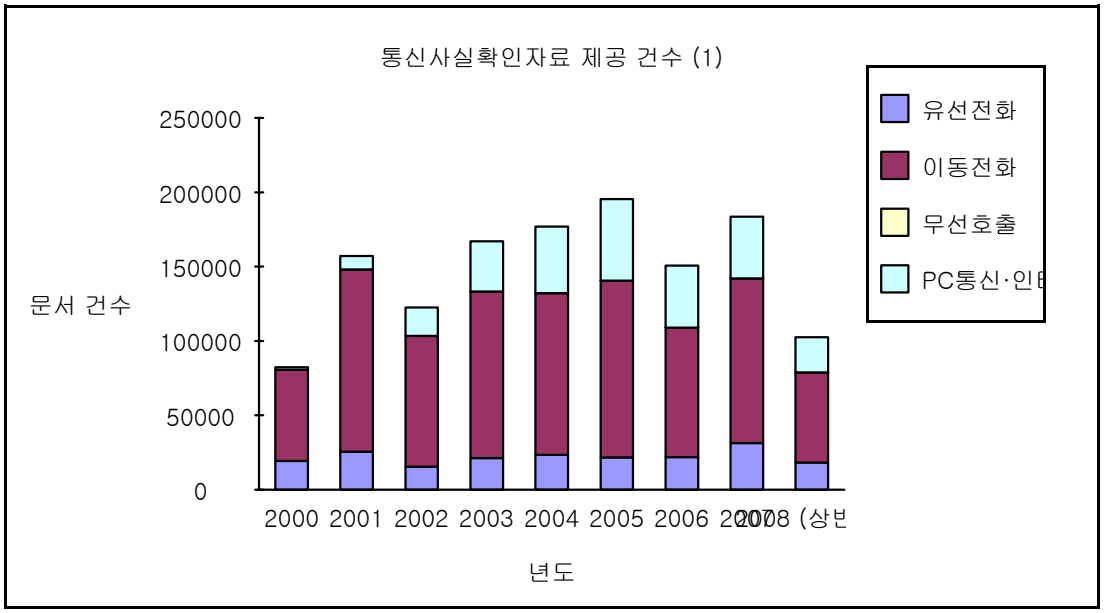
41) 대판 2003. 8. 22, 2003도3344. 다만 정보통신부와 방송통신위원회의 통계에는 모두 포함되어 있다.
42) 이상의 감청 및 통신자료 제공 현황은 2000년 6월 개정된 [전기통신감청 및 통신자료제공 관련업무 처리지침]에 따라 정보통신부와 이를 이어받은 방송통신위원회에서 년2회 공개한 자료를 재가공하였다.



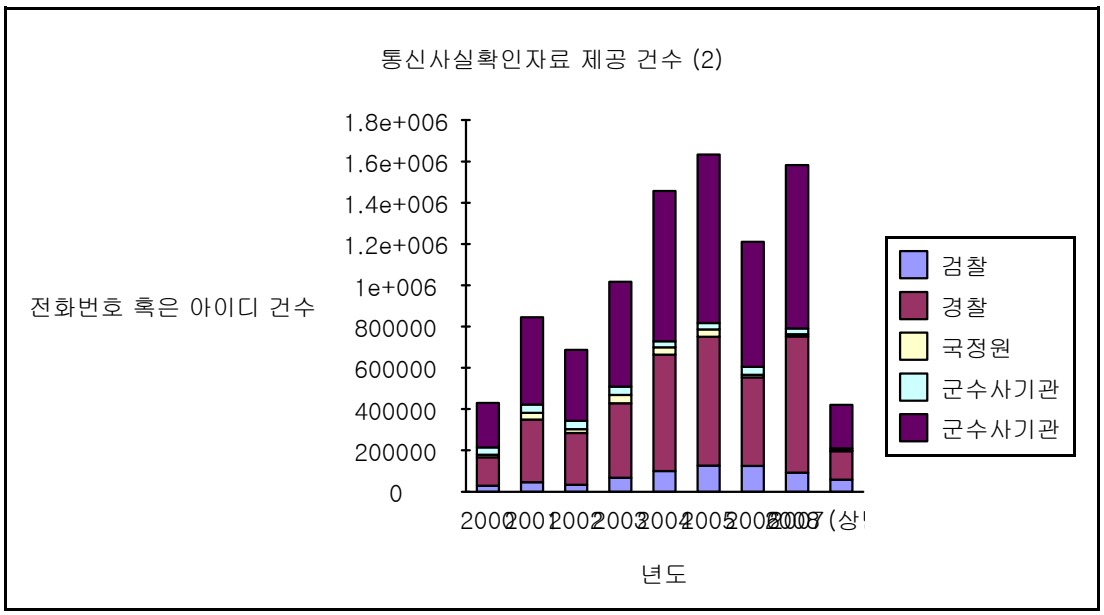
그러나 감청건수를 문서 건수가 아니라 전화번호 혹은 아이디 건수별로 재분석하여 보면, 한 문서당 기재되는 전화번호나 아이디가 증가하였기 때문에 전체 감청건수는 오히려 전반적으로 증가하고 있는 추세이다. 특히 국정원의 감청 분량이 두드러진다.



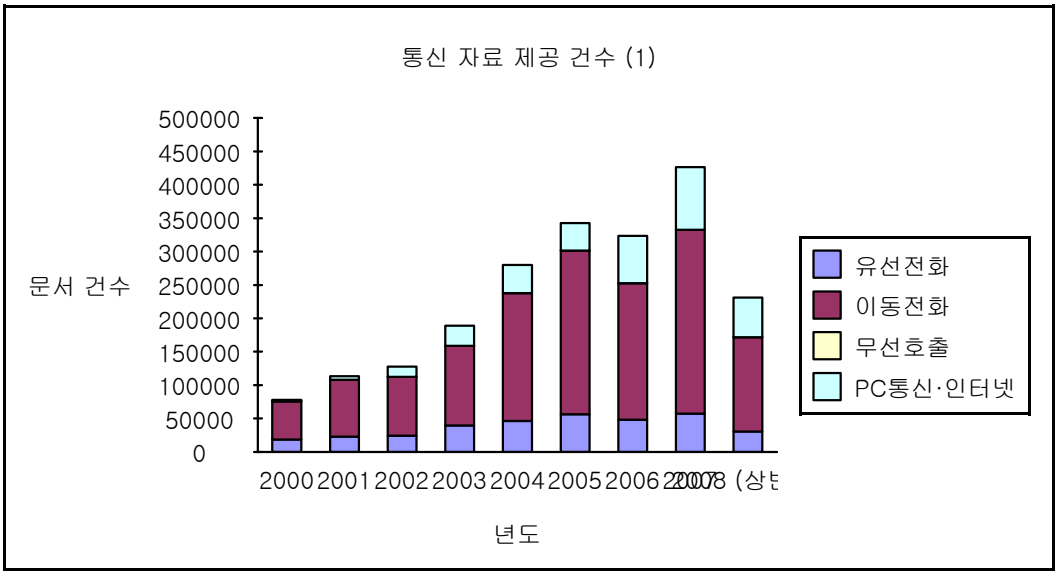
(2) 통신사실 확인자료 제공



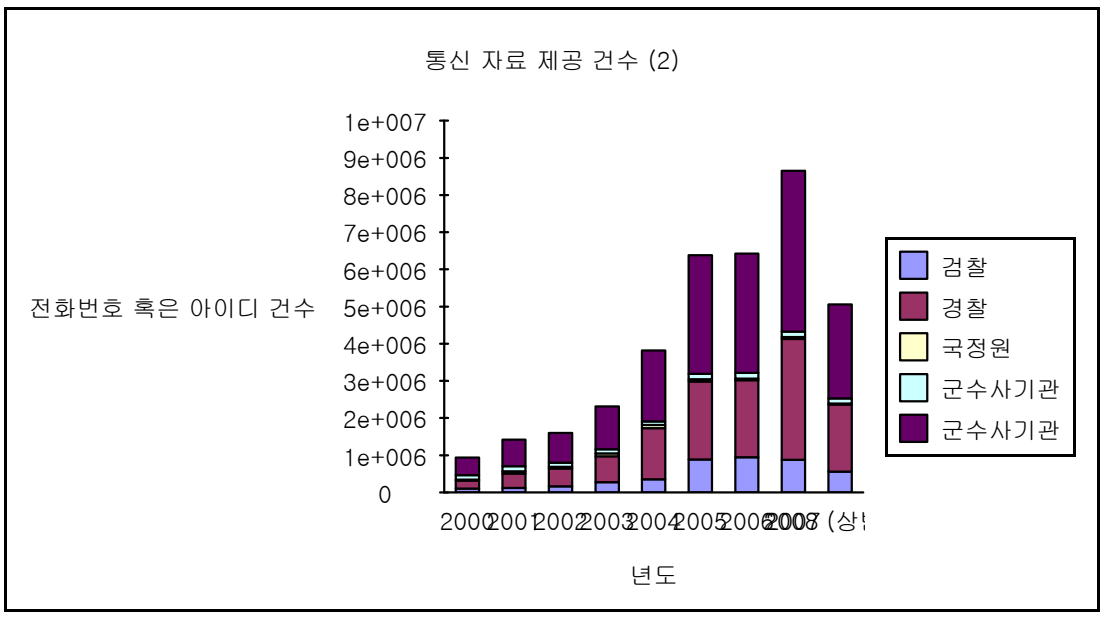
위치정보, 인터넷 IP주소 등에 대한 통신사실확인자료의 제공은 2006년 일시적으로 감소하였다. 이는 2005년 8월 27일 통신비밀보호법이 개정되면서 수사기관의 통신사실확인자료 요청 절차가 검사장 승인에서 법원 허가로 한층 강화되었기 때문인 것으로 보인다. 이동전화에 대한 통신사실확인자료 요청의 비중이 전반적으로 높다는 점도 주목할 만 하다.



(3) 통신자료 제공



가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료 제공은 2007년 특히 인터넷 분야에서 급격히 증가하였다. 2007년 7월 37개 주요 인터넷 사이트에 국가적인 실명제가 의무화되면서 이에 대한 수사기관의 요청이 증가한 것으로 추정된다. 다음, 야후 코리아, 디씨인사이드 등은 이용자의 실명 정보를 의무적 실명제 도입 후부터 수집하기 시작하였다.



3. 통신비밀보호법

(1) 제정 취지

대한민국 헌법 제18조에는 “제18조 모든 국민은 통신의 비밀을 침해받지 아니한다.”라고 하였다. 군사정부 시절 반인권적인 감시와 감청을 경험한 끝에 1993년 12월 마침내 통신비밀보호법이 제정되었다.

통신비밀보호법의 목적에는 “이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.”라고 명시되어 있다.

통신비밀보호법은 누구든지 통신비밀보호법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열 또는 전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못하도록 규정하고 있다.(제3조)

검사, 사법경찰관 또는 정보수사기관의 장이 범죄수사나 국가안보를 위하여 우편물의 검열이나 전기통신의 감청을 하는 경우 또는 공개되지 아니한 타인간의 대화를 녹음·청취함에 있어서 법에서 정한 요건을 모두 갖춘 경우에만 한하며, 법에 따른 허가를 받거나 승인을 얻어 감청를 하거나 대화를 녹음·청취한 경우에도 이를 계속할 필요성이 없다고 판단되는 경우에는 즉시 이를 중단함으로써 국민의 통신비밀에 대한 침해가 최소한에 그치도록 하여야 한다.(시행령 2조)

여기서 ‘통신’은 우편물 및 전기통신을 말하며 ‘감청’은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·

수신을 방해하는 것을 말한다.(제2조)

이에 따라서 전화, 팩스, 전신은 당연히 전기통신에 포함되며, 휴대전화와 개인휴대통신도 당연히 전기통신에 해당한다. 이메일을 포함한 컴퓨터 통신상의 자료 및 정보의 전송도 전기통신에 해당한다.

한편 통화내역이나 로그기록과 같은 통신사실 확인자료의 경우 원래는 통신비밀보호법상에 관련 규정이 없고 전기통신사업법에 근거규정이 있었으나 차츰 그 중요성이 인식되면서 통신비밀보호법의 보호 범위 안으로 편입되었다.

2005년에는 수사기관이 통신회사에 통신사실 확인자료를 요청할 때 법원의 허가를 받도록 개정되었다. 감청의 허가요건은 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 법원이 영장을 허가할 수 있다고 한다.(제5조)

다만 감청의 대상 범죄가 형법상 내란, 외환, 국교, 약취와 유인에 관한 죄, 군형법, 국가보안법, 군사기밀보호법상의 범죄 등 10개 법률 300종류가 넘을 만큼 매우 광범위하게 설정하여 제정 당시부터 남용 소지가 있었다.

국가안전보장과 관련하여서는 허가요건이 완화되어, 내국인을 대상으로 할 때는 고등법원 수석부장판사의 인가를 받아야 하고, 외국인에 대한 통신인 때에는 대통령의 승인을 받아 감청을 하도록 하였다.(제7조)

일반 범죄 수사를 위하여 검사가 법원에 대하여 감청 허가를 청구할 때는 기간은 3개월을 초과하지 못하며 다시 3개월까지 연장이 가능하다. 긴급한 사유가 있을 경우에는 법원의 허가 없이 감청을 할 수 있으나 그로부터 36시간 이내에 법원으로부터 허가를 받도록 하였다.

이 조항은 사실상 수사기관이나 정보수사기관이 영장 없이 통화내용을 감청했다가 사후 영장을 신청하지 않고 슬그머니 감청을 중단하는 용도로 악용되어 왔다.

또한 감청의 허가결정이 일단 내려지면 연장에 대한 결정은 계속될 가능성이 높아서 감청의 남용과 직결되어 왔다. 1998년 울산지역 노동단체 관계자 14명을 국가보안법 위반 혐의로 구속하였던 '영남위원회 사건'에서는 법원이 감청 허가의 연장결정을 하면서 원(原)허가서에는 없는 대화녹음이나 대상자, 대상전화가 연장청구서에 추가되었음에도 아무런 제한도 가하지 않았던 점이 알려져 물의를 빚었다. 이러한 관행으로 국가보안법 위반 범죄에 대한 감청은 몇 년간 지속되기도 한다.

김영삼 정부는 통신비밀보호법을 제정하여 국가 정보수사기관의 감청을 법에 의하지 않고서는 할 수 없도록 규정하였으나 국가 정보수사기관의 감청은 오히려 증가한 것은 물론 정치적 목적의 감청이 이루어진 것으로 밝혀졌다.

(2) 개정 취지

결국 김대중 정부 들어서서 휴대전화를 비롯한 불법 감청에 대한 의혹이 꾸준히 제기되어 2001년 12월 통신비밀보호법이 대대적으로 개정되었다.

이때 감청의 대상 범죄를 당초 390개에서 280개로 축소하였고, 감청 기간이 수사목적은 3개월에서 2개월로, 국가안보목적은 6개월에서 4개월로 축소하고 각각 2개월과 4개월의 범위 내에서 연장이 가능하도록 하였다.

긴급감청 기간을 48시간에서 36시간으로 단축하였으며, 감청조치가 집행된 사실을 당사자에게 통지하는 규정을 신설하였다.

또한 통화내역과 같은 통신사실확인자료에 대한 제공을 통신비밀보호법의 적용을 받도록 하였으며, 감청에 대한 국회의 통제기능을 강화하여 년2회 감청현황을 보고하도록 하였다.

또한 감청설비 도입시 정보수사기관은 정보통신부에, 국정원은 국회 정보위원회에 신고하도록 하였다. 그 이후에도 통신비밀보호법은 몇 차례 주요 개정 절차를 거쳤는데 그에 대한 요약은 다음과 같다.

[표3] 통신비밀보호법 주요 개정 현황

제, 개정	공포일	내용	법률개정 배경
제정	1993.12.27	-	1992년 대선에서 도청 이슈
제6차 개정	2001.12.29	대상범죄 축소, 조정 통신제한조치 허가청구시 허가청구대상의 한정 통신제한조치 기간축소 긴급통신제한조치 절차강화 피감청자에 통지제도 신설 통신사실확인자료 제공절차 규정 감청설비의 신고	1998년부터 불법감청과 남용에 대하여 국회에서 지속적인 문제제기 1999년부터 휴대폰 감청 의혹 제기
제8차 개정	2004.1.29	단말기 고유번호제공금지 불법감청설비탐지업 규정	휴대폰 복제남용 불법감청설비탐지업 난립
제9차 개정	2005.1.27	통신사실확인자료에 인터넷 로그기록, 발신자 위치추적 자료, 정보통신기기의 접속지 추적자료를 포함시킴	인터넷 로그기록, IP추적 등 규정미비
제11차 개정	2005.5.26	통신사실확인자료 제공절차 강화 (법원 허가) 통신사실확인자료 보관 의무 통신사실확인 통지제도 도입	통신사실확인자료 요구의 급증과 남용

그러나 감청에 대한 법률적 통제를 개선하려는 노력 이면에서 인터넷 로그기록과 IP주소 등 새로운 통신 영역에 관한 감청 규정이 계속 추가되면서 사실상 감청은 더욱 확대되었다.

특히 안기부 X파일 사건에서 볼 수 있다시피 통신비밀보호법은 정보수사기관의 감청에 대한 통제에 사실상 실패하였다. 이는 통신비밀보호법에서 해

결될 수 있는 문제가 아니라 정보수사기관의 비밀 권력에 대한 민주적 통제에 관한 문제이다.

(3) 개정안 논란

국정원은 감청 장비가 폐기된 후 휴대전화 감청이 불가능하여 범죄수사에 제약이 많다고 계속 주장해 왔고 2007년 국회 법제사법위원회는 이 요구에 부응하는 통신비밀보호법 개정안을 통과시켰다.

개정안에 대한 인권단체들의 반대운동이 활발하게 일었으며, 국회 본회의에서 이에 반대하는 의원들의 수정안이 발의되면서 논란 끝에 통과되지 못했다. 2008년 4월 총선 후 17대 국회가 종료되면서 법안은 자동 폐기되었다.

그러나 2008년 들어선 새 정부는 테러 방지, 첨단기술범죄 대응을 주장하며 통신비밀보호법 개정을 재추진할 의사를 강력하게 표명하였고 10월 30일 18대 한나라당 이한성 의원의 대표발의로 17대와 같은 내용의 통신비밀보호법 개정안이 다시 상정되었다.

이 법안은 첫째, 감청 대상범죄에 기술유출 범죄를 추가하고(안 제5조제1항), 감청에 협조토록 하기 위하여 전기통신사업자에게 감청장비를 구비할 의무를 신설하고 이를 위반할 경우 10억 원 이하의 이행강제금을 부과하였다.(안 제15조의2, 제17조제1항제7호, 부칙 제4조 및 제15조의3 신설) 둘째, 통신사실확인자료에 GPS 위치정보를 추가하고(안 제2조제11호아목 신설) 통신사실확인자료를 보관하지 아니하는 자는 3천만 원의 과태료에 처하도록 하였다.(안 제20조제1항제2조)

이 법안의 가장 큰 문제점은 수사기관의 편의를 위하여 제3자인 통신사업자에게 자료 보관을 강제하였다는 것이다. 이는 통신사업자에 의한 개인정보의 무분별한 수집, 유출 문제가 심각한 우리 현실에서 개인정보 보호에

역행할 뿐 아니라 모든 국민을 잠재적 범죄자로 간주하고 통신의 비밀을 심각하게 제한하고 있다.

국가인권위원회 역시 2008년 1월 16일 발표한 의견에서 “사업자가 보유한 불필요한 개인정보를 즉각 삭제토록 하는 제도적 대책이 필요함에도 오히려 일정기간 자료를 보관케 의무화 한 것은 개인의 정보보호에 역행되고,

범죄수사 목적으로 일정기간 동안 통신기록 확인의 당위성이 인정되지만, 아직 발생되지 않은 범죄 해결 목적으로 범죄 예비단계도 아닌 일반인 통신기록을 최대 1년간 보관하도록 한 것은 법제정 취지에 위배되고, 인권침해의 가능성이 높다”고 판단하였다.

특히 인터넷 로그기록은 설정하기에 따라 이용자가 언제, 어디서 접속을 했는가에 대한 정보 뿐 아니라 통신 내용에 대한 정보도 포함할 수 있는데 법령에서는 이를 세부적으로 다루지 않았다.

예를 들어 이용자가 저작권을 침해하는 파일을 업로드하거나 다운로드한 기록이 수사기관에게 필요하다는 이유로 추후 시행령 차원에서 파일 업로드와 다운로드에 대한 로그기록을 모두 보관토록 강제할 수도 있는 것이다.

이는 결국 이용자의 어떠한 통신 사실에 대한 정보이던지 방대한 양이 축적될 수 있다는 의미이며 이것이 현실화된다면 대한민국 인터넷에서 통신의 비밀이란 존재할 수 없다.

또한 개정안은 감청 집행에 필요한 장비를 전기통신사업자가 보유하도록 강제하였는데, 통신사업자가 감청에 필요한 설비를 보유한다는 것 역시 국민의 통신의 비밀에 중대한 영향을 끼친다.

첫째, 통신사업자가 보유하고 있는 장비를 통해서 누군가 마음만 먹으면 언

제든지 감청이 가능하며 이에 따른 오남용과 유출 위험이 상존하게 되었다. 그런 의미에서 국가인권위원회가 “사실상 감청 자체가 예외적 허용이 아니라 상시적으로 행해질 수 있는 것이라는 인식을 조성하면서 개인 사생활 및 프라이버시를 크게 위축시킬 수 있”다고 지적한 것은 매우 타당하다.

둘째, 통신사업자를 통하여 감청을 실시한다는 것은 휴대전화는 물론 인터넷 전화, 화상 전화, 인터넷 메신저, 인터넷 채팅 등 사실상 모든 통신수단에 대한 감청이 개시되었다는 말이다. 심지어 현재 압수수색 형태로 이루어지는 휴대전화 문자메시지나 이메일처럼 송수신이 완료된 통신에 대한 실시간 감청도 기술발달에 따라 충분히 가능해질 수 있다.

이처럼 새로운 통신수단에 대한 감청이 실시되게 되었는데, 이를 단순한 기술적인 확장으로 간주되어서는 곤란하다. 휴대전화면 휴대전화대로, 인터넷이면 인터넷대로 그 기술이 가지고 있는 특성이 개인의 프라이버시권과 통신의 비밀에 미칠 영향이 매우 신중하게 검토되어야 한다.

하지만 이번 개정안은 새로운 기술에 대한 감청 개시의 문제를, 국민의 인권에 대한 문제가 아니라 단지 각 사업자가 어떤 감청 장비를 보유하느냐에 달린 기술적 차원의 문제로 환원시켜 버렸다.

이는 통신비밀보호법의 취지 자체를 무색케 하는 것이다. 셋째, 수사기관과 통신사업자 간의 권력관계를 상기하여 보았을 때, 불법적인 도청이 이루어진다 하더라도 통신사업자가 이를 거부하거나 고발할 가능성은 매우 희박하다. 과거 감사원이 지적하였다시피 통신사업자가 불법적인 도청의 협조자 노릇을 하도록 강제될 위험이 매우 높다.

근본적인 문제는 현행 통신비밀보호법에도 많은 문제점이 있다는 사실이다. 감청대상이 여전히 매우 광범위하며, 긴급감청이 오남용되고 있다. 또한 정보수사기관의 권한은 예외적으로 인정되어 왔으며 이들에 의한 정치적인

목적의 감청이 마구 자행되어 왔다.

특히 이번 개정안은 사실상 국가정보원과 법무부가 주도하면서도 의원을 통하여 발의가 되었다는 이유로 공청회처럼 전국민적으로 토론하고 여론의 검증을 받을 기회가 사실상 봉쇄되었다는 점은 크게 유감이라 아니할 수 없다.

결론적으로 통신비밀보호법 개정안이 속성으로 처리되는 일이 있어서는 결코 안 된다. 새로운 기술에 대응하는 감청 법률 마련은 국민적 공감대와 관심 속에 그 법이 국민의 기본권인 통신의 비밀에 미칠 영향을 충분히 고려하면서 논의를 해나가야 마땅할 것이라 하겠다.

통신비밀보호법 개정의 필요성과 방향

김 성 천[43]

1. 범죄의 예방과 진압을 위한 투명성 확보

범죄가 가장 효과적으로 잘 예방되도록 하는 방법은 모든 범죄가 저질러지는 족족 그 저지른 사람의 행위가 발각되어 처벌받게 되도록 만드는 것이다. 그리하여 법질서는 준수된다는 신뢰가 일반국민들에게 당연한 것으로 자리를 잡게 될 때 범죄로부터 자유로운 사회가 건설될 것이다.

반대로 범죄인의 입장에서는 자신의 행위가 밝혀지지 않도록 익명성이 보장되는 것이 소원일 것이다. 모름지기 범죄를 저지르고도 처벌을 받지 않는 가장 좋은 방법은 들키지 않는 것이다. 그러한 면에서 익명성을 보장받을 수 있는 도시의 공기가 범죄의 온상이다. 자신의 행동 하나 하나가 관찰의 대상이고 입방아에 오르게 되는 농촌마을의 투명성은 범죄를 힘들게 하는 요소이다.

결국 범죄를 효과적으로 예방하고 진압하기 위해서는 익명성이 제거되고 투명화가 이루어져야 한다. 그러한 면에서 범죄의 혐의가 발견되었을 때 그것이 누구의 행위인지를 밝혀내기 위한 작업인 수사는 범죄방지를 위해서 매우 중요한 역할을 한다.

그런데 우리 사회는 문명이 발달하면서 투명성보다는 익명성이 강화되는 쪽으로 변화해왔다. 범죄인의 입장에서는 반길만한 일이다. 이러한 익명성의 극치는 사이버 공간에서 펼쳐지고 있다. 인터넷 세상에서 이루어지는 일

43) 중앙대학교 법과대학 교수, 법학박사.

에 대해서는 본질적으로 누가 한 것인지를 알 수가 없도록 되어 있다.

누구의 작품인지를 알기 위한 최소한의 단서가 로그인 기록인데 이것도 그저 어느 단말기 또는 어느 아이디가 접속되었는지를 말해줄 뿐 실제로 누가 그 단말기나 아이디를 사용해서 인터넷을 이용했는가 하는 것까지 알 수 있게 해주는 것은 아니다.

통신수단 또한 인터넷과 마찬가지로 익명성이 심화되고 있다. 나아가 통신수단이 인터넷과 접목하게 되면서 익명성은 더욱 강해지고 있는 실정이다. 인터넷을 이용한 통신수단에 대한 투명성을 확보하는 것은 수사기관의 입장에서 큰 일이 아닐 수 없다.

2. 공적 이익을 위한 감청과 정보자기결정권 보호

인터넷을 포함한 현대적 통신수단에 대한 투명성을 얻어내기 위해서 수사기관이 할 수 있는 방법은 장비를 사용해서 엿듣기와 엿보기를 하는 것이다. 이를 「통신비밀보호법[1]」(이하 "통비법"이라 한다.)은 감청이라고 부른다. '감청'이 범죄를 방지하기 위해서 반드시 해야 할 일임은 확실하다.

그렇지만 감청은 개인비밀을 침해한다는 또 다른 측면을 가지고 있다. 수사를 위해서 필요한 일이기는 하지만 정보자기결정권이라는 기본권[2]을 침해하는 속성을 가지고 있기도 한 것이다.

따라서 수사를 한다고 무한정 통신감청을 할 수도 없는 일이고 반대로 기본권을 보장한다고 무조건 금지할 수도 없는 일인 셈이다. 두 가지 이익이

1) 제정 1993. 12. 27. 법률 제4650호, 일부개정 2008. 2. 29. 법률 제8867호.

2) 통신비밀의 법적 성격에 대해서는 자유권적 기본권 가운데 사생활 보호와 관련된 정보자기결정권에 해당하는 것으로 보는 견해(권영성, 헌법학원론, 법문사, 1997, 398면 이하; 김일환, 통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰, 『형사정책』 (한국형사정책학회) 제16권 제1호 (2004), 32면; 성낙인, 통신에서의 기본권 보호, 『공법연구』 (한국공법학회) 제30집 제2호 (2001), 35면 이하)와 표현의 자유로 보는 입장(박용상, 표현의 자유, 현암사, 2002, 620면 이하)이 있다. 비밀은 누설되지 않도록 지켜지는 것이 본질이므로 사생활의 불가침과 관련된 정보자기결정권으로서의 자유권적 기본권으로 보는 것이 타당하다고 생각한다.

충돌하는 경우에는 적절한 위치에서 잘 조화를 이루도록 조치를 취하는 수밖에 없다. 그 해결책은 형사소추라는 공적 이익을 위해서 반드시 필요한 경우에만 제한적으로 통신감청을 허용하는 방법뿐이다.

그리고 형사소추를 위해서 꼭 필요한 경우인가 하는 점에 대한 판단은 수사기관(검찰)이 아닌 법원에 맡겨야 할 것이다. 수사기관이 스스로 필요여부를 판단하도록 하면 남용될 위험이 분명히 있기 때문이다. 현행 통비법이 바로 그러한 방법을 사용하고 있다(법 제5조 내지 제6조).

3. 감청설비의 보유주체와 감청주체의 분리

한편 수사기관의 활동과 관련해서 법원의 허가가 필요한 것은 통신감청 외에도 많이 있다. 압수・수색・체포・구속 등 이른바 강제수사는 모두 법원의 허가를 얻어야만 가능하다.

그런데 통신감청은 기본권을 침해한다는 측면에서는 이들 압수・수색・체포・구속 등의 강제수사와 동일하지만 그들과는 다른 특수성이 한 가지 있다. 다름이 아니라 당하는 사람 쪽에서 자신의 기본권이 침해당한다는 사실 자체를 알 수 없다는 점이다.

그렇기 때문에 수사기관에서 몰래 감청을 하고서도 자신들이 엿듣기를 했다는 사실 자체를 함구하고 있으면 당사자가 자신에 대한 침해사실 자체를 인식하지 못하게 되는 것이다. 침해사실조차 모르고 있으면 기본권 보호는 요원해 질 일이다.

이를 방지하기 위해서는 감청설비를 수사기관이 자체적으로 보유하고 운영하는 것을 금지하는 것이 최상이라고 생각한다. 그리하여 감청설비의 보유와 운영은 통신사업자가 맡고 수사기관은 법원의 허가를 받아 이들의 협조

를 구함으로써 비로소 감청을 할 수 있도록 하자는 것이다. 통신감청설비의 보유주체와 감청주체를 분리하여야 한다는 말이다.

통신감청제도와 관련해서 가장 논란이 많은 부분이 이곳이다. 과거 정보기관이 행한 불법감청 행위가 사회적인 문제로 불거진 후에 불법감청장비는 모두 폐기되었다고 한다.

이에 따라 합법적인 감청만 할 수 있게 되었는데 유선전화와는 달리 무선통신의 경우에는 기지국을 통해서 특정 가입자의 통화내용만을 감청할 수 있는 방법이 현재로서는 없다는 것이다. 법원에서 영장을 발부받더라도 무선통신에 대해서는 기술적으로 감청이 불가능하기 때문에 수사에 어려움이 많다는 말이다.

사정이 이렇게 되자 수사기관 쪽에서는 법무부를 대표로 해서 여러 선진국과 마찬가지로 감청장비를 통신회사에 설치하고 법원의 영장을 발부받아서 특정 가입자의 통화내용을 전용선을 통해 전달받는 식으로 감청하는 방법을 추진하게 되었다.

그러자 시민단체들 쪽에서는 수사기관이 이동통신에 대해서 감청을 하지 못하고 있는 현재의 상황을 유지하고자 그와 같은 방향의 개정작업을 강력하게 반대하고 있는 형편이다.

그러나 남용가능성만 제거된다면 통신감청설비의 보유주체와 감청주체를 분리하는 방향으로의 법개정은 꼭 이루어져야 한다고 본다. 범죄로부터 보호를 받아야 할 권리도 보장되어야 하기 때문이다.

이 문제는 통신사업자가 감청을 위한 설비를 갖추고 법원의 허가가 있는 경우에 한하여 감청대상자의 통신회선을 수사기관으로 보안기준을 충족하는 전용선을 통해 접속시켜주어 감청을 가능하게 해주는 방식을 사용함으

로써 해결될 수 있다.

그런데 감청설비는 통신서비스를 제공한다는 측면에서는 -몰래 뒷돈을 받고 감청을 해주는 것 외에는- 전혀 필요 없는 장비이므로 법적 의무가 없는 한 사업자 입장에서는 이를 구비할 이유가 없다.

그 때문에 현행 통비법은 제15조의2 제1항에서 "전기통신사업자는 검사·사법경찰관 또는 정보수사기관의 장이 이 법에 따라 집행하는 통신제한조치 및 통신사실 확인자료 제공의 요청에 협조하여야 한다"는 규정을 둠으로써 일단 문제를 해결하였다.

나아가 통비법은 제15조의2 제2항에서 "제1항의 규정에 따라 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항, 통신사실확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정한다"고 하여 사업자가 부담하게 되는 협조의무의 구체적인 내용은 시행령에서 정하도록 위임하고 있다.

이에 따라 통신사업자가 감청에 필요한 장비·시설·기술을 구비하여야 할 의무를 시행령에서 규정하여도 될 일이지만, 기본권 제한과 관련되는 일이므로 구체적인 내용을 법률로 정하는 것이 기본적으로 타당한 입법방향이라고 생각한다.

인권·시민·사회단체 쪽에서는 현재 시행령을 통해서도 통신감청설비의 보유주체와 감청주체를 분리해서 감청을 실시하는 방안의 시행이 가능하다는 점에 대해서는 언급을 하지 않고, 이들 내용을 법률 수준에서 구체화하는 것에 대해서만 새로운 입법을 통한 인권침해라고 하고 있다[3].

그러나 통신감청이라는 수사기법은 이미 통신비밀보호법이 허용하고 있는

3) 오동석, 통신비밀보호법 개정안에 대한 반대의견, <통신비밀보호법 공청회 토론자료> (2007. 6. 5.), 62면 이하 참조.

강제수단이다. 지금까지 허용되지 않던 강제수사 방법을 입법을 통해 새롭게 도입하려는 것이 아니라 현행 통비법 체계의 규율내용을 법률수준에서 보다 구체화하려는 것이므로, 입법자 스스로 인권침해의 근거를 마련하는 것이라는 지적은 타당하지 못하다고 생각한다.

통비법을 개정하여 수사기관의 감청행위를 전면적으로 금지하자는 주장을 한다면 몰라도[4], 지금까지 법적으로 허용되고 있던 제도의 내용을 구체화하는 것을 가지고 새로운 인권침해라고 하는 것은 부당한 지적이다.

4. 통신사업자 설비를 이용한 감청의 안전성 확보

통신감청설비의 보유주체와 감청주체를 분리하는 것 자체만으로 개인비밀침해의 모든 위험이 사라지는 것은 아니므로 부가적으로 안전조치를 할 필요가 있을 것으로 생각된다. 이를 위하여 취해져야 할 사항들을 몇 가지 나열해본다.

첫째, 감청설비의 운영자와 감청기관을 분리한다는 취지를 무색하게 하는 수사기관의 자체감청을 금지해야 할 것이다. 통비법 개정안은 이에 대한 처벌규정을 마련하여야 한다.

둘째, 통신사업자가 수사기관의 압력이나 회유를 이기지 못해서 법원의 허가를 받지 않은 감청을 하는데 협력하는 일이 있어서는 곤란하므로 이 또한 철저하게 금지되어야 한다.

셋째, 감청행위의 투명화를 위하여 감청 관련 기록을 보관하고 감청에 관한 기술표준을 제정하여 이를 준수하도록 하여야 할 것이다. 통신사업자가 수

4) 웬일인지 인권·시민·사회단체 쪽에서도 그와 같은 주장까지는 하지 않고 있다. 너무 억지를 부린다는 인상을 줄까봐 그런 것 아닌가 생각된다.

사기관에 통신사실 확인자료를 제공할 때에는 그 사실을 대장에 기록하고 정보통신부장관에게 연 2회 이를 보고해야 하는 등의 의무에 대해서는 이미 현행 통비법이 제13조에서 규정하고 있다. 기술표준을 제정하는 문제는 현행법에 규정이 되어 있지 않은데 통비법 개정안을 통해 상세하게 그 내용을 담아야 한다.

넷째, 통신사업자가 자신의 사적 이익을 위해 감청장비를 운영하는 과정에서 지득할 수 있는 고객의 개인정보를 유출하는 것을 방지하기 위한 장치도 필요하다. 이를 위해서 감청장비를 이용하는 모든 행위가 로그기록으로 보존되도록 하여 추후에 누가 개인정보를 유출했는지 확인할 수 있도록 해야 하겠다. 이 로그기록은 필요하다면 실시간으로 법원 등 제3의 기관에도 동시에 저장되도록 하여야 할 것이다.

이 문제는 독일과 같은 경우 시행령에서 규정하는 방식을 취하고 있으며 대부분의 국가가 기술표준을 제정하면서 이를 포함시키는 방식으로 해결하고 있다. 반드시 필요한 부분이기는 하지만 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 이미 이 내용을 반영하고 있으며(법 제46조의3), 선진국의 경우와 마찬가지로 시행령과 기술표준에 포함시키는 방식으로 조치를 취하면 될 것으로 보인다. 따라서 통비법 개정안 자체에 기술표준의 구체적인 내용까지 포함시킬 필요는 없다고 본다.

다섯째, 감청집행 협조와 관련하여 마련되어 있는 여러 가지 안전장치들이 제대로 작동되고 있는지를 확인하기 위해서 정기적인 보안점검을 하도록 제도화해야 할 것이다. 예를 들어 통신사업자 쪽에서 감청장비를 운영하다가 누군가 개인정보를 유출하면서 그 사실을 숨기기 위하여 로그기록을 삭제할 수도 있는데 이와 같은 조작행위가 발붙이지 못하도록 주기적인 보안점검이 이루어져야 한다.

이에 관한 규정도 이미 「정보통신망 이용촉진 및 정보보호 등에 관한 법률

」 제46조의3에 마련되어 있으므로 개정안에 포함시킬 필요는 없는 것으로 보인다.

여섯째, 통신감청은 개인정보를 침해당하는 사람이 스스로 기본권을 침해당했다는 사실 자체를 인지할 수 없어서 적절한 대응을 할 수가 없다는 속성을 가지고 있는데, 이러한 문제점을 어느 정도 완화시키기 위해서 통신감청이 있게 되면 사후에 이를 당사자에게 통지해 줄 필요가 있다.

감청장비의 보유주체와 감청주체를 분리해서 감청의 남용을 방지해주는 제도를 보완해줄 장치이다. 통신제한조치의 집행에 관한 통지제도는 현행 통비법에도 이미 잘 갖추어져 있다.

특히 통신사실확인자료 제공 사실까지 통지해주도록 하고 있는 것은 선진국의 예에서도 찾아볼 수 없는 강력한 통지제도이다. 개정안에서 굳이 이를 더욱 강화할 필요는 없을 것이다. 그렇더라도 이를 강화한다면 통신감청 집행에 대하여 매우 엄격한 통제를 하려는 것으로서 개인비밀 보호에 만전을 기한다는 측면에서 적절한 입법이 될 것이라고 판단된다.

일곱째, 여러 안전장치에도 불구하고 남아있게 되는 불법감청의 가능성을 위해서 내부고발이 가능하도록 만들어주는 제도가 필요하다. 통신사업자나 수사기관에 근무하는 사람이 외부인보다 불법감청 사실을 알게 될 확률이 높으므로 이들이 안심하고 신고를 할 수 있도록 유도하는 제도를 만들어야 하겠다.

5. 맺는 말

통신감청은 범죄를 방지하여 사회구성원들이 자유로운 삶을 누릴 수 있도록 해주기 위해서 꼭 필요한 수사방법이다. 그러나 동시에 국가기관의 행위

에 의해서 개인의 비밀을 침해한다는 속성을 가지고 있기도 하다.

이처럼 범죄로부터 사회를 보호한다는 공적 이익과 개인의 비밀을 보호한다는 사적 이익의 충돌문제를 해결하기 위해서 현재 우리가 취하고 있는 방법은 범죄수사를 위해서 반드시 필요한 경우에만 감청을 허용하되 필요성 여부에 대한 판단은 법원이 하도록 하는 것이다.

이와 같은 감청조치의 허가요건과 절차 등을 규율하고 있는 것이 현재의 통신비밀보호법이다. 법원의 허가가 있는 경우에 한하여 감청을 할 수 있도록 하는 방법이 형사소추권과 정보자기결정권 사이의 이익균형을 유지할 수 있는 훌륭한 방법이기는 하지만 통신감청의 특성상 한 가지 문제점이 있다.

감청의 경우에는 구속·압수·수색 등 다른 수사기법과는 달리 기본권을 침해당하는 사람이 침해 사실 자체를 인지할 수 없기 때문에 불법감청을 규제할 길이 막막하다는 것이다. 수사기관이 법원의 허가 없이 무단 감청을 하더라도 감청을 하는 사람 외에는 알 수가 없으므로 통제가 불가능해진다는 말이다. 이 문제는 감청설비 보유주체와 감청주체를 분리하는 방법을 통해서 해결하는 수밖에 없다.

그런데 수사기관의 감청 집행에 대하여 통신사업자가 협조해야 한다는 규정은 현행 통비법에 이미 마련되어 있고, 그와 관련하여 필요한 사항은 대통령령으로 규정하도록 되어 있다. 따라서 대통령령으로 통신사업자의 감청설비 구비·협조의무 내용을 구체화하면 되는데 왜 굳이 법률에서 구체적 내용을 규정하려고 하는가 하는 의문이 든다.

이 문제는 법률유보의 한계와 관련하여 생각해 보아야 하겠다. 중대한 기본권 제한은 그 내용과 범위를 법률에서 규정해야 하는데, 통신사업자에게 감청설비의무를 부과하는 것은 일반적 행동자유권을 제한하는 것으로서 대통

령령으로 정할 수는 없는 사항이다. 따라서 법률 수준에서 이를 정하여야 할 것이고 통비법이 그와 같은 방향으로 개정되어야 할 것이다.

통신제한조치 집행설비의 오남용 우려 관련 질의에 대한 검토 의견

강 신 각[5)]

□ 질의 1:

감청 오남용 방지를 위한 기술적 조치로서 크게 1) 감청된 내용정보를 즉시 집행기관에 암호화 통신으로 안전하게 전달하거나 통신사업자 내부에 저장될 경우 비인가자가 접근할 수 없는 시스템 기능 2) 감청설비 운용 상황을 로그기록으로 남기고 그에 대한 위변조 방지 등 안전성을 높이기 위하여 로그기록 정보를 분산 관리하는 방안 등이 거론되고 있으며 이에 대한 내용이 통신비밀보호법의 하위 규정으로 반영될 가능성이 있음. 이에 대한 의견은?

o 감청협조설비의 오남용 방지를 위한 기술적 조치로 두 가지의 중요한 이슈가 검토되고 있음

- 통신사업자가 감청된 내용 정보에 접근하여 감청정보를 불법적으로 유포하거나 제공할 수 없게 하는 보호조치
- 통신사업자가 감청협조설비를 불법적으로 운용하는 것을 차단하기 위해 시스템 운용기록(즉, 로그기록)을 안전하게 관리하기 위한 기술적 조치

o 감청협조설비의 오남용 방지를 위해 미국, 독일, 유럽연합 등은 다양한 제도적, 기술적 조치를 시행하고 있음

5) 한국전자통신연구원 융합 통신 표준연구팀(박사)

- 미국의 감청법이라 부르는 CALEA 제105조에 통신사업자가 구축하는 감청설비에 대해 보안성을 갖출 것을 요구

  ※ CALEA: Communications Assistance for Law Enforcement Act

  ※ 인가자 또는 비인가자에 통신 감청이나 접근에 대한 기록을 안전하고 정확하게 보존하여야 함

- 독일은 감청령 제14조(보호요구사항)에 감청설비를 운용하는 협조의무자에 대해 보호조치 명시

  ※ 감청 설비의 안전성에 대한 보호조치와, 감청 설비가 부정 사용되지 않도록 보호하는 조치 마련

- 유럽연합은 유럽 표준기구인 ETSI에서 개발되는 표준에 감청에서의 보안 유지와 오남용 방지 관련 요구사항을 명시

  ※ 감청설비 운용자(통신사업자)는 감청된 내용을 모니터링하거나 영구 보존할 수 없음

  ※ 통신사업자에 의해 감청협조설비 운용 기록(로그기록)이 부정 조작되지 않고, 인가자 만이 접근할 수 있도록 보장

o 이한성 의원이 대표 발의한 통비법 개정법률안은 통신사업자에 의한 불법적인 감청설비 오남용을 차단하기 위한 조치를 마련할 것을 명시하고 있음

- 제15조의2, 5항: 전기통신사업자는 감청 장비 등을 운용함에 있어 권한 없는 자의 접근 방지, 접근기록의 관리 등 대통령령으로 정하는 바에 따른 보호조치를 취하여야 한다.

o 상기조항에 근거하여 대통령령에서 감청협조설비의 오남용을 막기 위한

세부적인 제도적, 기술적 보호조치를 명시할 예정이나, 기술적 보호조치의 구체적인 방법에 대해서는 아직 정해진 바가 없음

- 대통령령에서는 감청된 정보 및 감청협조설비의 운용기록(로그기록)에 대한 비인가자의 접근을 차단하고 안전하게 보호함으로서 오남용을 차단하기 위한 기술적 조치가 명시될 것으로 예상됨

- 이러한 기술적 보호조치는 감청협조설비에 대한 기술표준 제정에 반영되어 보호조치가 투명하게 시행될 것으로 예상됨

□ 질의 2:

위 기술적 조치는 국내 통신사업자에게 어떠한 형태로 요청될 것으로 예측되는가? 정부에서 기술 표준 규격만을 제시하는 것인가?
아니면 특정한 프로그램을 보급하고 모든 통신사업자가 공통적으로 설치하는 것인가?

o 감청협조설비의 보호 및 오남용 방지를 위한 기술적 조치는 감청협조설비에 대한 기술표준의 형태로 요구될 것을 예상됨

- 미국, 독일 등 감청협조설비의 구축 및 운용제도를 시행하고 있는 주요 국가에서는 수사기관, 통신사업자, 장비제조업체, 시민단체 등이 참여하는 가운데 기술표준을 제정하여 이를 투명하게 적용하고 있음

o 기술표준은 정부가 직접 제정, 적용하기 보다는 공정성 있는 표준화 기관을 통해 감청협조설비 구축 및 운용 관련 이해당사자가 참여하는 가운데 제정하도록 하는 추세이므로 우리나라의 경우에도 이러한 방식을 준용할 것으로 예상됨

o 기술표준에 적합한 시스템 또는 프로그램 등은 통신사업자 또는 장비제조업체 등이 각각 개발하여 적용할 수 있도록 개방될 것으로 예상됨

- 국외의 경우, 다수의 장비제조업체가 기술표준에 적합한 감청협조설비를 개발하여 통신사업자 들에게 상호 경쟁을 통해 납품하고 있음

□ 질의 3:

감청설비를 설치하고 수사기관에 협조하는 타국의 경우 기술적 조치는 어떠한 형태로 이루어지고 있는가? 어떠한 표준에 따르고 있는가? 특정한 프로그램을 공통적으로 설치하는가?

o 앞서 설명한 바와 같이, 감청협조설비의 보호 및 오남용 방지를 위한 기술적 조치를 취할 것을 우선 법률 및 시행령 등을 통해 명시하고, 이를 실현하기 위한 구체적인 방법으로 기술표준을 제정, 적용하는 형태를 취하고 있음

- 그러나, 세부적인 기술적 보호조치를 실현하는 방법은 국가별로 자국의 사회적 분위기, 통신 환경, 기술력 등에 따라 국가에 의해 선택되는 사항임

o 미국, 유럽연합 국가 등은 감청협조설비의 보호조치를 실현하기 위해 감청 대상 통신서비스에 따라 다양한 기술표준을 제정하여 이를 적용하고 있음

- 미국의 경우, 유선 및 이동통신 서비스 감청을 위한 대표적인 기술표준으로 J-STD-025 표준을, 그리고 IP 기반 통신서비스 감청을 위해

ANS T1.678 표준 등을 제정, 적용하고 있으며, 이 밖에도 많은 기술 표준을 개발하고 있음

※ J-STD-025 Lawfully Authorized Electronic Surveillance (LAES) Series
※ ANS T1.678: Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks
※ ANS T1.013, LAES for IP Network Access Service

- 유럽연합은 유럽 국가들이 공통적으로 이용할 수 있는 감청협조설비의 보호조치를 실현하기 위해 다양한 기술표준을 제정하여 이를 적용하고 있음

※ ETSI TS 101 331, Requirements of Law Enforcement Agencies
※ ETSI ES 201 158, Requirements for Network Functions
※ ETSI TS 102 232, Delivery of IP based Interception
※ ETSI TS 102 234, Service specific details for Internet Access Services

- 상기 기술표준 이외에, 통신서비스 유형별로 감청협조설비에 대한 다양한 기술표준이 계속 개발되고 있음

o 감청협조설비 구축을 위해 정부 기관이 특정 프로그램을 개발하여 공통적으로 설치하게 하는 경우는 아직까지 확인된 바 없음

- 미국 및 주요 유럽 국가의 경우 기술표준에 적합한 감청협조설비를 구매하여 설치, 운용하는 추세이며, 여러 장비 제조업체의 제품을 동시 설치하여 운용하는 추세임

※ 표준에 따라 장비를 개발하도록 함으로서, 복수 장비제조업체 개발 장비를 동시 사용하여도 상호 운용에 문제가 없도록 하고 있음

□ 질의 4:

통신사실확인자료 보관의 경우 마찬가지로 통신사업자에 의한 로그기록 위변조 가능성이 있음. 이에 대하여 마찬가지의 기술적 조치를 구상하고 있는 바가 있는가?

o 감청협조설비의 오남용 차단 및 통신사실확인자료의 보관 및 운용에 대한 세부적인 기술적 조치에 대해 아직까지 공식적으로 확정된 바가 없음

- 최근, 유럽연합의 경우 통신사실확인자료의 보관 관련 안전한 보호조치에 대한 기술표준 개발 작업이 진행되고 있음

o 통신사실확인자료의 보관, 접근 등과 관련한 로그기록 역시 감청협조설비의 운용에 대한 로그기록과 마찬가지로 오남용 방지를 위해 관리되어야 할 매우 중요한 정보이며, 이들 로그기록에 대해 동일한 수준의 보호 조치가 적용될 것으로 예상됨

통신비밀보호법 개정 관련 질의사항 검토

김 성 훈[6]

1 국가인권위원회, 올해 1월 법안에 대해 “국민의 프라이버시를 크게 위축시키고 개인정보보호에 역행하고 있음”을 지적한 바 있는데 이러한 국가인권위 입장을 전혀 수용치 않고 있는 점에 대한 입장

국가인권위원회는 2008. 1. 16. 당시 17대 국회 법사위에서 마련한 개정안에 대하여 국민의 프라이버시를 크게 위축시키고 개인정보보호에 역행한다는 등의 이유로 “통신비밀보호법 개정안(국회법제사법위원회 대안) 중 통신사실 확인자료에 위치정보를 추가하는 규정(제2조 제11호 아목), 통신사실 확인자료제공의 통지의무규정(제13조의3 및 제13조의4 제4항 및 제5항), 통신사실 확인자료제공의 요청거부시 처벌하는 규정(제17조 제3항), 통신제한조치 집행에 필요한 장비 등의 강제규정(제15조의2 제2항 내지 제4항, 제15조의3), 전기통신사업자에 대한 보관의무 규정(개정안 제15조의2 제5항, 제20조 제1항)을 각 삭제한다”라는 권고 의견을 발표하였습니다.

그러나 위 권고 의견은 종전 국가기관의 불법감청 전력으로 인한 정서적 거부나, 통신비밀보호법의 규정과 운용실태를 깊게 성찰하지 못한데서 나온 시민단체 등의 우려가 충분한 검토 없이[7] 상당 부분 그대로 반영된 것이 아닌가 생각됩니다.

---

6) 법무부 검찰국 공공형사과 검사

7) 예를 들어 인권위는 통신사실 확인자료제공의 요청거부시 처벌하는 규정(제17조 제3항)의 삭제를 권고하였으나, 심사 대상인 17대 국회 법사위 통과 안이나, 18대 국회에 계류 중인 통신비밀보호법 개정안(이한성 의원 대표발의) 어디에도 이와 같은 규정이 존재하지 않습니다. 법안에 대한 충분한 검토 없이 시민단체 등의 진정서 내용을 그대로 권고문에 기재하였기 때문에 생긴 해프닝으로 보입니다.

인권위 권고의 세부 내용과 위 규정들의 의미에 대한 구체적인 부분은 아래의 다른 질문들과 연관되어 있으므로 그 때 자세히 살펴보기로 하고, 통신비밀보호법 개정안에 대한 의견에 대하여 말씀드리겠습니다.

18대 국회 계류 중인 이한성 의원이 대표발의 통신비밀보호법 개정안(이하 '개정안'이라 한다)은 17대 국회 법사위에서 성안한 법안과 동일합니다.

17대 국회 때 전문가 초청 간담회와 수차례 회의 등에서 인권위에서 지적하는 문제점[8] 등을 포함하여 다각도로 신중한 검토를 거쳐 정부의 의견을 수렴하고, 여야 합의로 마련한 법안으로 통신의 비밀을 최대한 보장하면서 인권침해의 가능성이 있는 진술 위주 수사관행에서 탈피하고 과학수사 역량을 강화하는 법안으로 평가하고 있습니다.

2 전기통신사업자의 장비·기술 등 구비 및 통신사실확인자료의 보관의무를 부과하는 것은 수사·정보기관이 이동통신사를 이용해 국민들의 통신을 제한하겠다는 것으로 반인권적 발상이라는 주장에 대한 입장

가. 국민적 공감대를 통해 사실상 금지되어 오던 휴대전화 감청을 제도화 하는 것으로 사실상 감청 자체가 예외적 허용이 아니라 상시적으로 행해질 수 있는 것이라는 인식을 조성하면서 개인 사생활 및 프라이버시를 위축시킬 수 있다는 지적에 대하여

현행법도 감청 대상으로 유선전화, 이동전화, 전자우편, 문자메시지 등을 가리지 않고 있어 모두 감청이 가능하도록 되어 있습니다. 그러나 법원의 영장을 발부받아도 통신회사에서 감청협조설비를 갖추지 않고 있고, 수사·정

8) 인권위 권고 내용은 권고문 발표 이전부터 시민단체 등에서 꾸준히 제기하여 온 지적들과 대동소이하고 관련 내용은 17대 국회에서 충분히 논의·검토되었습니다.

보기관도 자체 설비를 보유하지 않고 있기 때문에 현실적으로 휴대전화 등에 대한 감청 집행이 곤란한 상태에 있습니다.

개정안은 수사정보기관이 반드시 전기통신사업자의 협조를 받아야만 감청이 가능하도록 함으로써 자체 감청 설비를 운용하면서 발생할 수 있는 감청 오남용 소지를 차단하여 국민의 사생활을 더 두텁게 보호하는 진일보한 방안으로 평가됩니다.

휴대전화 감청은 현행법으로도 가능하기 때문에 현행법이 유지된다면 정보·수사기관은 감청장비를 각자 개발해야 하고, 그러한 경우 오히려 불법 감청에 대한 통제장치 없이 휴대전화 감청이 가능해질 것이며, 불법을 조장하게 되는 결과를 초래될 것이 예상됩니다.

현행법에도 감청을 하기 위해서는 법에서 정하는 법원의 허가 등 엄격한 절차를 거쳐야 하고 이를 거치지 않은 감청의 경우에는 엄한 처벌 규정이 있습니다.

현재 유선전화국은 유선전화의 감청에 필요한 설비를 갖추고 있음에도 유선전화에 대한 상시적, 일상적 감청이 이루어지고 있지는 않기 때문에 통신사업자가 감청설비를 보유하기만 하면 감청이 일상화될 것이라는 것은 지나친 억측입니다.

감청설비는 통신사업자에 의해서 운용하도록 하고, 수사기관은 통신사업자로부터 감청 관련 정보를 제공받도록 하여 감청설비의 직접 접근을 막는 것이 선진국 등 세계적인 입법 추세이자 과거 국정원이 직접 감청 장비를 운용하면서 불법도청한 사례를 교훈 삼아 다시는 그러한 일이 없도록 감청의 남용을 방지하는 효과적인 방안입니다.

나. 감청 집행 필요장비 등의 보유 규정만 있을 뿐 통제와 정보유출 차단기술・제도적 장치에 대해서는 미비해 사업자에 의한 악용과 프라이버시 침해 위험의 상시적 존재를 인정하는 결과 초래 우려 지적에 대하여

현행법에도 불법감청을 방지하기 위하여 많은 사전 통제장치와 사후 통제장치를 규정하고 있습니다.

먼저, 사전 통제 장치로는 ① 감청은 독립된 기관인 법원의 허가 사항, ② 불법감청에 의한 결과물의 증거사용 금지, ③ 다른 방법으로 범죄의 실행 저지, 범인 체포, 증거 수집이 어려운 경우에 한하여 허가, ④ 감청대상범죄의 제한, ⑤ 대상자별 통신제한조치 허가 청구, ⑥ 통신제한조치의 기간 제한(2개월), ⑦ 전화번호 등 불일치시 감청 집행 협조 거부 등을 규정하고 있습니다.

한편 사후 통제 장치로는 ① 통신제한조치 대장 비치 의무화, ② 수탁기관의 긴급감청서 등 표지사본 비치 의무화, ③ 통신제한조치 집행 후 통지의무와 불이행시 처벌, ④ 불법감청 뿐만 아니라 합법감청도 내용 공개, 누설시 처벌 등을 규정하고 있습니다.

현행법상 각종 불법감청 방지 장치가 이중, 삼중으로 규정되어 있음에도 불구하고, 이번에 국회에 발의되어 계류 중인 개정안에는 불법 감청을 방지할 수 있는 제도적 장치가 더욱 강화되어 있습니다.

① 수사・정보기관이 영장에 의하더라도 통신회사를 거치지 않고 직접 감청하는 것을 금지하고 이를 위반하면 처벌하여, 자의적인 영장 집행과 영장 없는 감청의 가능성을 원천적으로 차단하였습니다.

② 불법 도・감청 범죄에 대한 신고포상금 제도를 도입하여 특히 국가기

관에 의하여 이루어지는 불법도·감청 단속의 계기를 마련하고, 불법도·감청 근절의 의지를 표명하였습니다.

③ 정보수사기관에서 감청 후에 당사자에게 통지를 유예하는 것에 대하여 소속 장관의 승인을 받도록 통제장치를 보완하여 자의적인 통지유예로 인한 폐단을 방지하도록 하였습니다.

④ 감청을 위한 접속로그기록을 보관하도록 의무화하여 향후 감청 현황을 비교, 대조함으로써 불법 감청을 원천적으로 차단할 수 있도록 하였습니다. 쉽게 말씀드리자면 현재 음주측정을 할 경우 음주측정기에는 음주측정 기록이 남게 되는데, 그 기록을 사후에 음주운전 사건 대장과 비교·대조함으로써 경찰관들이 음주운전을 적발하고도 사건을 은폐하던 관행이 사라지게 된 것을 생각하시면 이해하실 수 있으실 것으로 생각됩니다.

사업자에 의한 악용 가능성을 특히 우려하고 있으나, 국제적으로 통용되는 기술표준에 의하면 통신업체는 법원에서 허가한 기간 동안 대상자의 통신내용만 분리하여 암호기술을 적용하여 수사기관으로 전송하는 역할에 한정되고, 통신업체는 감청협조에 필요한 설비만을 갖추어 가입자의 통화내용 녹음·저장은 불가능하며, 통신업체 직원은 통화내용을 직접 들을 수 없도록 하고 있기 때문에 충분히 기술적·제도적으로 차단이 가능하리라 생각됩니다.

다. 개인 사생활 정보가 상시적으로 기록되고, 언제든지 정보수사기관에 넘겨질 수 있다는 것만으로도 허용될 수 없는 기본권의 제약이며, 국민 모두를 예비적 범죄자로 보고 상시 감시체계를 꾸리겠다는 발상이라는 지적에 대하여

통신비밀을 보호하고 통신의 자유를 신장하여야 한다는 점에는 이론이 있을 수 없지만 국가안전보장·질서유지·공공복리를 위하여 일정한 부분 통

신의 자유에 대한 제한이 불가피한 것은 사실입니다.

국민의 대표 기관인 국회에서 만든 법률에 의해 감청과 통신사실확인자료 제공 등은 그 필요성 때문에 이미 도입되어 있으므로, 엄격한 통제와 적법 절차의 테두리 내에서 기본권 침해를 최소화하는 방향으로 제도가 잘 운영될 수 있도록 불법감청 가능성을 근본적으로 차단하고 투명화 하는데 묘안을 짜내야 하는 것이지, "허용될 수 없는 기본권 제약"이라고 제도 자체를 백안시 하는 것은 문제가 아닐 수 없습니다.

합법 감청은 법원의 엄격한 통제와 국회의 감독을 피할 수 없기 때문에 남용의 우려가 거의 없으므로 '상시 감시체계 발상'이라는 지적은 부당합니다. (보관의무 문제는 라.항에서 자세히 살피도록 하겠습니다.)

라. 전기통신사업자의 통신사실 확인자료의 보관의무 부과는 수사·정보기관이 이동통신사를 이용해 국민의 통신을 제한하는 것으로 반인권적 발상이라는 지적에 대하여

현행 통신비밀보호법 제15조의2 제5항, 동법 시행령 제21조의4 제2항에 의하면 전기통신사업자는 휴대폰·국제전화는 1년, 시내·시외전화는 6개월, 인터넷 로그기록은 3개월간 보관하도록 되어 있습니다.

개정안은 시행령에 규정되어 있는 보관기관을 법률에 옮겨 규정한 것이고, 시행령상 보관기간을 무제한을 늘려 인권을 침해하지 않도록 최대 보관기간을 법률에서 1년이내로 제한하려는 규정입니다. 반인권적 발상에 의한 규정이 아니라 인권보호를 더욱 강화하는 규정인 것입니다.

다시 한 번 강조하지만 통화내역, 인터넷 로그기록 등은 법원의 허가를 받아 범죄혐의자에 대한 것만 제한적으로 확인이 가능하기 때문에 일반 국민의 통신 자유 위축, 이동통신사를 이용한 상시 감시 등의 주장은 근거가 없습니다.

3 통신사실확인자료를 일정기간 보관하도록 할 경우 민간기업에 의한 개인정보 유출 및 그에 따른 범죄 등의 우려가 있다는 지적에 대한 구체적인 반론과 대안은?

가. "개정안 제15조의 2에는 기존 전기통신사업자를 전기통신사업자 '등'으로 확대하고 있는데, 그 구체적 범위는 시행령에 위임하고 있으므로 감청설비의 설치 및 활용범위가 무제한적으로 확대될 가능성이 있음, 합법적인 절차를 따른 다고 하나 예외적으로 법원의 허가 없이 수사·정보기관이 '긴급감청'을 할 수 있을 뿐만 아니라 긴급감청을 실효적으로 통제할 방법 또한 없음" 지적에 대하여

GPS 위치정보가 통신사실확인자료에 포함됨에 따라서 전기통신사업자 이외에 위치정보사업자 및 위치기반서비스사업자가 포함된 것뿐입니다.

'등'을 넣어서 무제한 사찰이 된다고 주장하지만 법률상 법원의 엄격한 허가 절차를 거쳐 감청·통신사실확인자료 제공 등이 가능하게 되어 있고, 보충적·제한적으로 운용되고 있는 수사 실태에 비추어 볼 때 크게 우려하지 않아도 될 것으로 생각됩니다.

국가안보를 위협하거나 다중의 생명을 위협하는 범죄 등에 있어서 촌각을 다투는 경우가 많은데 이러한 경우를 위해서라도 긴급 통신제한조치는 반드시 필요합니다.

긴급통신제한조치를 하더라도 사후에 지체없이 법원의 허가를 받아야 하고, 36시간 이내에 허가를 받지 못하면 통신제한조치를 중지하여야 하며(통신비밀보호법 제8조 제2항), 추후 국회의 통제를 받게 되어 있기 때문에(통신비밀보호법 제15조) 긴급 통신제한조치의 남용 우려는 크지 않습니다.

실제 수사기관에에 의하여 이루어지는 긴급 통신제한조치의 건수도 2005년 14건, 2006년 10건, 2007년 11건, 2008년 2건(2008년 9월 기준)에 불과하여 아주 예외적인 경우에만 긴급 통신제한조치를 사용하고 있음을 알 수 있습니다.

나. "통신사업자의 협력의무가 법제화되면 모든 통신은 감청이 가능하게 되고, 감청이 가능하지 않은 통신서비스는 제공을 할 수 없게 되는데, 그 적용의 대상범위는 불분명하나, 그 영향은 실로 막대할 것으로 헌법상 통신비밀의 권리보장은 무용지물이 될 것임" 지적에 대하여

앞서 살핀 바와 같이 현행법에도 감청의 대상인 '통신'에 제한이 없기 때문에 유선전화, 이동전화, 전자우편, 문자메시지 가리지 않고 모두 감청이 가능한데, 개정안에 따르면 수사정보기관이 반드시 전기통신사업자의 협조를 받아야만 감청이 가능하도록 함으로써 자체 감청 설비를 운용하면서 발생할 수 있는 감청의 오남용 소지를 근본적으로 차단하도록 하였습니다.

감청 절차를 투명하게 하여 불법감청 가능성을 최소화함으로써 국민의 통신비밀의 자유를 신장하려는 것이 개정안의 취지이므로 헌법상 통신비밀 권리보장이 무용지물이 될 것이라고 주장하는 것은 전혀 타당하지 않습니다.

다. "사업자가 일정기간 자료를 보관케 의무화 한 것은 개인의 정보보호 정책에 전반적으로 역행" 지적에 대하여

개인정보라 할지라도 일반 기본권과 마찬가지로 국가안보와 사회질서 유지를 위해서는 법률상 제한을 받을 수 있는 것이고, 전기통신사업자가 개인정보를 보관한다고 하더라도 전기통신사업자의 직원 역시 법원의 영장 제시나 당사자의 동의가 없는 경우에는 개인정보를 열람할 수가 없는 것이며,

전기통신사업자의 정보보호 장치와 관련해서는「정보통신망이용촉진및정보

보호등에관한법률」등에서 이미 관련 규정이 보완[9]되었기 때문에 단지 전기통신사업자가 통신사실확인자료를 의무적으로 보관하게 한다는 점만으로 개인정보보호에 역행할 것을 강제한다고 할 수 없을 것입니다.

라. "아직 발생되지 않은 범죄의 해결 목적으로 범죄 예비단계도 아닌 선량한 일반인의 모든 통신기록을 최대 1년간 보관하도록 하는 것은 입법취지에 반하고 인권침해 가능성이 높음" 지적에 대하여

범죄수사 목적으로 일정기간 동안의 통신기록을 확인할 필요성은 질문지에서 인정하고 있는 바와 같습니다.

현행법에도 전기통신사업자들의 통신사실확인자료 법적 보관기간이 정해져 있지만 이를 위반하여 수사에 장애를 초래한 경우가 없지 않았기 때문에 개정안에 과태료(3천만원 이하) 규정을 도입하게 된 것으로 보입니다.

우리나라는 전세계 국가 중 유례를 찾기 어려울 정도로 거의 유일하게 법원 허가제로 통신사실확인자료 제공 절차를 규정하고 있으므로 인권침해 가능성은 거의 없습니다.

영세한 전기통신사업자의 영업의 자유의 심각한 제한이라는 지적과 관련해서는 현재 각종 설비의 비용이 급격하게 저렴해 지고 있어 보관으로 인한 비용 부담이 그리 클 것으로 보이지 않고 영세 사업자일수록 보관할 자료의 양이 많지가 않아 비용이 적게 들 것으로 보이기 때문에 실질적으로 영업을 제한하게 될 우려는 크지 않을 것으로 보입니다.

다만, 영세업체에 대한 과태료 부과가 과중한 것으로 비용 분석이 될 경우

---

9) 정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련해야 하고(정통망법 제45조 제1항), 일정 규모 이상의 전기통신사업자는 안전진단수행기관으로부터 정보보호 안전진단을 받아야 하며(동법 제46조의3), 정보보호관리체계를 인증기관으로부터 인증을 받아 운영하도록 규정(동법 제47조)되어 있습니다.

에는 일정 범위의 업체에 대하여는 하위명령 개정시 과태료를 면제해 주는 방안을 검토해 볼 수도 있을 것입니다.

마. 통신사실확인자료를 일정기간 보관하도록 할 경우 민간기업에 의한 개인정보 유출 및 그에 따른 범죄 등의 우려가 있다는 지적에 대한 구체적인 반론과 대책은

위 다.항에서 전기통신사업자에 대한 정보통신망이용촉진및정보보호등에관한법률상 제도적 보완 장치, 개인정보보호 등에 대해 이미 설명하였으므로 검토를 생략합니다.

바. 장비 등의 구비의무를 위반한 경우 10억원 이하의 이행강제금을 1년에 1회 부과할 수 있도록 규정한 것은 국가가 기업의 영업 자유를 지나치게 통제하는 것이라는 지적에 대한 입장과 대안

현행법에도 전기통신사업자의 일반적인 협조의무가 규정되어 있음에도 전기통신사업자들이 이동전화 감청 관련 설비를 구비하지 않는 등 협조가 되지 않고 있기 때문에 감청협조설비 구비를 강제할 수 있는 실효성 있는 수단이 필요합니다.

또한 개정안에는 통신기관을 통하지 않고는 자체 감청을 하지 못하도록 하였으므로 전기통신사업자들의 감청협조설비 구비는 더욱 필수적입니다.

감청협조설비 구비에 많은 비용이 드는 전기통신사업자는 수익 규모가 큰 이동통신사업자들이기 때문에 법에서 요구하는 감청협조설비를 반드시 구비하도록 하기 위해서는 상당한 금액의 이행 강제금이 부득이합니다.

또한 이행강제금은 10억원의 범위 이내에서 대통령령이 정하는 바에 따라 방송통신위원장이 부과하는 것이므로 합리적인 범위에서 운용될 것으로 기

대합니다.

참고로 감청설비를 갖추지 않을 경우 미국은 1일당 1천만원(연간 36억원), 대만은 1일당 7천만원(연간 250억원) 부과하도록 하고 있는 점에 비추어 볼 때 개정안이 우리나라 기업에게 특별히 불이익을 주고 있다고 보기 어렵다고 생각됩니다.

4 위치정보의 경우 '통신'에 대항되지 않는데 위치정보를 규율대상으로 포함할 수 있는 구체적인 근거

가. 위치정보의 '통신' 개념 포섭 가능 여부

통신비밀보호법상 전기통신의 개념은 유선·무선·광선 및 기타의 전자적 방식에 의한 모든 종류의 음향·문헌·부호 또는 영상을 송신하거나 수신하는 것으로 규정(통신비밀보호법 제2조 제2호)되어 있을 뿐 '의사연락'을 요건으로 하지 않습니다.

최근 통신기술의 발전에 따른 각종 정보통신기기의 융합으로 개인의 GPS 위치정보 또한 휴대전화의 '친구찾기' 등 하나의 기능으로 포함되어 있기 때문에 위치정보 또한 광의의 통신 개념에 포함시킬 수 있습니다.

나. 위치정보 포함시 사생활침해·수사기관의 오남용 가능성

흉악범 등 범죄자의 효율적인 검거를 위해서는 정보통신기기의 발신기지국 위치만으로는 반경 1km 수준에 불과하고, 인터넷 로그기록, 정보통신기기의 위치추적자료 등 현행 규정만으로는 부족한 측면이 있습니다.

수사기관이 GPS를 활용할 수 있게 된다면 반경 5m까지 추적이 가능하게

되므로 압구정동 유괴살해범 사건을 영화로 만든 '그놈 목소리'의 '그 놈'과 같은 거악을 척결하는데 획기적인 방안이 될 수 있어 반드시 필요하기 때문에 인권위 삭제 권고에도 불구하고 이번 개정안에 반영된 것이라 생각되고, 법원의 허가 절차와 국회의 통제를 받기 때문에 남용의 우려는 없어 보입니다.

다. "위치정보의 보호 및 이용 등에 관한 법률의 입법취지상 개인위치정보의 즉시 파기를 원칙으로 하고 있음에도 개정안에는 위치정보를 1년 동안 수집하라고 되어 있어 정면으로 충돌하고 있음, 입법미비에 대한 입장과 해결방안" 지적에 대해

위치정보의 활용 필요성은 위에서 살핀 바와 같고, 위치정보의 보호 및 이용 등에 관한 법률은 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하기 위한 법률로서 수사에 필요한 위치정보의 제공 절차를 규정하고 있지 않고, 법원의 엄격한 통제 규정이 없기 때문에 위치정보법에 수사기관의 GPS 활용 관련 규정을 반영하는 것은 부적절하고, 통신비밀보호법에 포함시켜 절차의 통일을 꾀할 필요가 있습니다.

개정안은 제15조의2 제6항에서 다른 통신사실확인자료에 대한 보관의무를 규정하면서 단서 규정에 "다만, 통신사실확인자료 중 위치정보에 대하여는 그러하지 아니하다"라고 덧붙여 위치정보의 불필요한 수집·보관에 의한 폐해를 근본적으로 차단하고 있습니다. 1년 동안 수집하도록 의무화하고 있다는 것은 위 개정안 규정을 깊이 검토하지 않은 부당한 지적이라 생각됩니다.

다시 한 번 말씀드리지만 위치정보는 다른 통신사실확인자료와 마찬가지로 법원의 엄격한 통제, 엄중한 처벌규정, 국회의 감독 등으로 인하여 범죄수사 목적 이외의 남용 우려는 크지 않을 것으로 보입니다.

라. “영업비밀·산업기술 유출에 대한 국내정보 수집은 국정원법상 불가능함에도 각종 언론보도는 국정원이 공식적으로 담당하고 있는 것으로 되어 있는데 이번 개정안이 국정원의 국정원법상 직무범위를 위배하게 하는 문제, 국가가 국민의 통신비밀 및 개인정보에 개입할 가능성이 확대되는 문제를 발생시킨다” 지적에 대해

언론보도를 살펴보더라도 대우조선해양의 핵심 기술, 하이닉스 반도체의 핵심 기술 등 ‘국가기밀’에 속하는 산업기술에 대한 ‘해외유출’과 관련한 정보를 입수한 국정원의 첩보 제공으로 검찰 등 수사기관이 수사 성과를 거둔 것일 뿐이므로 국가기밀에 대한 보안업무는 국정원 직무범위를 벗어난다고 볼 수 없고, “내국인에 대한 국내정보 수집”이라는 불법행위를 저질러 국정원법을 명확하게 위반하였다는 사실 보도는 찾기 어렵습니다.

과거 불법 도청·사찰 사건이 발생하게 된 것은 독자적인 감청장비를 몰래 운용하면서 그 유혹을 이기지 못했기 때문이라고 생각되는데, 현행법상 국정원이 자체 감청 설비를 갖추는 것은 합법이고 허용되어 있으나, 개정안에 의하면 국정원도 통신업체를 통해서만 감청이 가능하게 됩니다.

사회 일각에서는 통신비밀보호법 개정은 국정원의 권한을 강화하여 국민 사생활을 침해할 우려가 높아지는 것으로 생각하지만, 오히려 이러한 자체 감청을 금지하는 법안을 통해 감청의 오남용을 막고, 불법 도청을 근본적으로 차단하도록 하는 것으로서 국정원을 국민을 위한 정보기관으로 제도화하는 근본적인 조치이자 국민의 사생활 보호를 위한 법안이라 생각됩니다.

마. “통신사실확인자료 제공사실 통지의무 신설로 통신사실확인자료의 제공을 요청한 수사기관이 통신사업자에게 일괄 통지하는 것만으로 통지의무를 면제하게 한 것은 통지제도 취지를 제한할 우려”지적에 대해

인권위는 통신사실확인자료 제공에 대해 수사기관이 통신회사에 일괄 통지만 하면 통지의무가 면제되므로 통신사실확인자료를 남용할 여지가 커진다는 등의 이유로 삭제를 권고하였습니다.

통신사실확인자료 제공은 법원의 엄격한 통제를 피할 수 없기 때문에 수사종료 통지 방식의 변경만으로 남용이 우려되지는 않습니다.

통신회사 등은 수사와 무관하므로 오히려 자의적 통지 누락의 필요성이나 개연성이 없고, 통신기관 등은 통지를 데이터베이스 등 시스템으로 관리할 수 있어 통신사실확인자료를 제공한 가입자에 대한 수사종료통지가 없으면 수사기관에 확인하는 등 크로스체크가 가능하게 됩니다.

금융거래내역 역시 금융거래내역을 제공한 금융기관에서 직접 대상자에게 통지하고 있고, 이로 인한 누락의 문제 등은 발생한 적이 없는 점에 비추어 볼 때 간접통지 방식을 도입하려는 이번 개정안은 수사기관의 자의적인 통지 누락을 방지하도록 하여 통신의 비밀 보호를 오히려 강화하는 방안입니다.

참고로 미국, EU, 호주, 중국, 인도네시아, 쿠웨이트, 아르헨티나, 칠레 등은 수사기관의 요청만으로 통화내역을 제공하고, 통화내역 조회에 대한 사후통지제도는 전 세계적으로 한국이 유일합니다.

5 통신사실 확인자료제공의 요청거부시 처벌하는 규정(제17조 제3항) 우려에 대하여

인권위는 협조의무 위반을 이유로 형사처벌하는 것은 가혹하다는 이유로 통신사실확인자료제공의 요청거부시 처벌 규정 삭제를 권고하였고, 이번 토론회 질문서에도 이러한 내용이 있습니다.

17대 국회 논의 과정에서 나온 일부 의견에 대해 위와 같은 권고가 나온 것으로 미루어 짐작되지만, 17대 국회 법사위 통과 안이나 18대 국회에 발의되어 현재 국회 계류 중인 개정안은 제17조 제3항은 물론 전체 법률 규정 중 어디에도 통신회사 협조의무위반을 이유로 하는 형사처벌 규정은 존재하지 않습니다. 시민단체 등의 일방적 주장만 받아들이고 법안을 제대로 검토하지 않았기 때문에 이러한 현상이 발생한 것으로 생각됩니다.

⑥ 감청·통신사실확인자료는 체포영장이나 구속영장에 비교할 때 청구요건도 쉽게 되어 있고 현실적으로 법원의 기각률이 낮기 때문에 실질적으로 통제가 되지 않고 있는 실정이므로 오남용 가능성이 커진다는 지적에 대하여

통신제한조치나 통신사실확인자료는 국민의 기본권을 제한하는 측면이 있어 수사기관이 최후의 수단으로 엄격하게 보충적으로 활용하고 있기 때문에 법원의 기각률이 높지 않은 것으로 평가됩니다.

그럼에도 불구하고, 법원 기각 건수가 상당한 수에 이르고 있는 것은 실질적으로 엄격한 통제를 받고 있다는 것을 뜻합니다.

법원은 현재 구속영장·체포영장 못지않게 통신제한조치와 통신사실확인자료 제공에 대해 엄격하게 심사하고 있습니다.

법원이 부실하게 검토하고 있다는 별다른 근거를 들지도 못하면서 형식적으로 기각률만 비교하여 법원의 노력을 폄훼하는 주장은 사법부에 대한 국민의 신뢰를 저해하는 것으로 사법부 독립을 규정하고 있는 헌법 정신에도 맞지 않고 매우 부당하다고 생각됩니다.