정보운동 액트온 | *Act On*

한국의 이동통신 도감청과 통신비밀보호법

통권 제5호 | 2009년 제1호

진보네트워크센터

계간 정보운동 액트온 ActOn
통권 제5호 | 2009년 제1호

발행일 2009년 3월 23일
등록일 2003년 8월 1일

발행처 진보네트워크센터
발행인 이종회
편집인 오병일
편집 달군
표지 달군
인쇄 천광문화사

등록번호 서울 바03553
주소 서울 서대문구 충정로3가 227-1 우리타워 3층
홈페이지 http://act.jinbo.net
이메일 della@jinbo.net
전화 02-774-4551
ISSN 1976-1953

차례

통권 제5호 | 2009년 제1호

한국의 이동통신 도감청과 통신비밀보호법

※ 이 자료는 진보네트워크센터와 Foundation for Media Alternatives(필리핀), ICT Policy Monitors Network(파키스탄), Open Initiative of Cambodia(캄보디아), Voices for Interactive Choice & Empowerment(방글라데시) 등 아시아 NGO들이 함께 참여한 *ONI : Mobile Phone Censorship and Surveillance – Joint Regional* 프로젝트의 일환으로 작성되었습니다.

한국의 이동통신 도감청과 통신비밀보호법

장여경 · 김지성

I. 정치적 현황

한국은 1980년대 민주화 투쟁으로 오랜 세월 계속되었던 군사 독재 정부 치하를 벗어났고 1997년 처음으로 야당 정권교체를 이루면서 개혁 정부가 들어섰다. 개혁 정부하에서 영화, 음반에 대한 검열 제도가 폐지되는 등 일부 반인권 제도가 개선되고 국가인권위원회가 설립되었지만, 주민등록제도 등 시민을 감시 · 관리하는 기본적인 행정 시스템은 철폐되지 않고 유지되었다. 1997년 IMF 사태 등 신자유주의 세계화의 흐름과 그에 조응하는 정부의 시장 자유화 정책 속에서 민중의 저항이 거세어지자 정보통신기술을 통한 수사기관의 감시와 탄압이 계속되었고 전자감시적 경찰국가의 도래에 대한 우려가 커져 왔다.

2007년 대통령 선거로 권위주의적 보수 정부가 들어섰고 2008년 총선으로 거대 보수 여당이 등장하였다. 2008년 4월 정부가 광우병 위험이 있는 미국산 쇠고기를 수입하기로 미국 정부와 기습적으로 협상하자 5월부터 매일 저녁 최대 수백만 명의 시민들이 휴대폰과 인터넷으로 연락하며 정부를 비판하는 촛불시위에 참여하였다. 이에 대하여 수사 당국은 1,400여 명 이상의 시위 참여자를 무자비하게 연행하고 형사처벌하는 것으로 강경 대응하였고, 휴대폰과 인터넷에 대한 수사기관의 감청 확대 등 인권 관련법률 개악을 준비하고 있다. 다른 한편으로 제도적 보호 대책이 미흡한 가운데 기업 등 민간에 의한 불법 도 · 감청 사례가 자주 발생하여 몇 년째 논란을 빚어 왔다.

II. 무선통신 기술 및 시장 현황

1. 이동통신 기술

1984년 1세대 이동통신 기술 중에서 북미 방식인 AMPS 셀룰러 시스템을 이용하여 한국이동통신

(현재 SK텔레콤)이 800Mhz 대역에서 최초로 상용 서비스를 시작하였다. 1996년 2세대 기술 중에서 미국 퀄컴사가 개발한 CDMA를 이용하여 SK텔레콤이 디지털 이동통신 서비스를 시작하였다. 이후 2000년에는 2.5세대로도 불리는, 화상통화가 가능한 CDMA2000 1x 서비스가 시작되었고, 2002년에는 3세대 기술로 불리는 CDMA2000 1x EV-DO 서비스가 시작되었다. 2006년에는 SKT와 KTF가 WCDMA 방식의 상용서비스를 개시하였다. LGT는 2007년 EV-DO Rev. A를 이용한 서비스를 시작하였다.

현재 이동전화 기술은 2세대 기술과 3세대 기술이 동시에 이용되고 있다. 2006년 이후 SKT의 T 서비스와 KTF의 쇼 서비스의 출시 이후 WCDMA를 중심으로 하여 3세대 서비스의 가입자가 빠르게 늘고 있다. 가장 빠르게 3세대 이동통신에 투자한 KTF의 경우에는 현재 3세대 서비스 가입자 수가 2세대 서비스 가입자 수를 넘어선 상태이다.

이동전화 기술의 발전과 상용 서비스 개시와 더불어 무선 데이타 통신 분야에서는 WiBro가 2006년 상용화되어 데이타 통신 부분에서 이동전화 기술의 대체재가 등장하였다. WiBro는 WCDMA 또는 EV-DO 계열의 기술보다 데이타 전송속도 측면에서 월등히 앞서나 지원하는 이동속도 측면에서 뒤처진다.

표 1: 세대별 이동통신 기술 비교[1]

구분	1세대	2세대	3세대	4세대
표준기술	아날로그 (AMPS, NMT)	TDMA, CDMA, GSM, PDC	WCDMA, CDMA2000, Mobile WiMax	WiMax evolution, 3GPP LTE, 3GPP2 UMB
전송속도	~10kbps	9.6~64kbps	144~2Mbps	100M~1Gbps
다중화 방식	FDMA	TDMA, CDMA	CDMA, OFDM	OFDM
상용화 시기	1984년	1995년	2003~2006년	2012년 이후
주요 서비스	음성 서비스	음성 서비스, SMS, 저속 인터넷	음성, 고속 인터넷, 화상전화	초고속 인터넷, 멀티미디어 서비스
멀티미디어 서비스[2]	제공 불가	6시간 4분	9분 43초	5.6초

1 『2008 · 2009 대한민국 모바일 연감』, (주)아이뉴스24, 1998, p.71.
2 800MB의 영화 1편을 다운로드하는 시간으로 비교

아직까지는 WiBro 서비스가 가능한 지역이 수도권 일부로 제한적이다. 장기적으로 이동전화 부분에서도 WiBro와 같은 무선랜 기반의 기술 발전과 VoIP의 결합을 통한 경쟁이 발생할 수 있다.

표 2: 4세대 후보 기술 비교[3]

구분		LTE	UMB	WiBro+
대역폭		1.25-20MHz	1.25-20MHz	5-20MHz
전송속도	Downlink	100Mbps	275Mbps	> 130Mbps (이동시) < 1Gbps (정지시)
	Uplink	50Mbps	75Mbps	>56Mbps
통신방식	Downlink	OFDMA	OFDMA	OFDMA
	Uplink	SC-FDMA	SC-CDMA	OFDMA
셀 당 동시 Users		200 users	1000 users	-
이동속도		> 350Km/h	> 250Km/h	> 120Km/h
Cell Coverage		5/30/100Km	15Km	< 5Km 5~30Km 30~100Km
Duplexing		TDD/FDD	TDD/FDD	TDD/FDD
Latence		5ms (User Plane)	14.3ms	< 10ms

3세대 서비스가 급격히 확산되는 상황에서 4세대 서비스는 기술 측면에서 데이타 전송률을 높이는 방향으로 발전하고 있다. 이러한 기술 진화의 방향은 음성통신을 주요한 서비스 대상으로 하던 것에서 다양한 멀티미디어 및 데이타 서비스 중심으로 향후 이동통신 서비스가 발전할 것임을 보여준다.

2. 이동전화 보급 현황 및 시장 경쟁 상황

ITU의 2008년 통계에 따르면 한국의 인구는 약 사천팔백만 명으로, 2007년 인구 백 명당 유선전화 회선수는 46.44이며, 2008년 이동전화 가입자 수는 94.24이고, 2007년 인터넷 사용자 수는 76.80이며, 광대역 인터넷 가입자 수는 30.50이다. 아래의 표에서 보듯이 유선전화 가입자는 거의 증감이 없

3 『2008 · 2009 대한민국 모바일 연감』, 앞의 책, p.77.

는 정체 상태라 볼 수 있으며, 이동전화는 지속적으로 가입자가 늘고 있으나 그 증가율이 그리 높지 않다. 이동전화 시장도 포화 상태에 가까워지고 있음을 알 수 있다.

표 3: 방송통신위원회, '유·무선 통신서비스 가입자 현황'

	2002.12	2003.12	2004.12	2005.12	2006.12	2007.12	2008.12
시내전화	23,490,130	22,877,019	22,870,615	22,920,151	23,119,170	23,130,253	22,131,737
이동전화	32,342,493	33,591,758	36,586,052	38,342,323	40,197,115	43,497,541	45,606,984
무선호출	140,284	73,160	45,634	42,003	42,690	39,328	41,082
TRS	210,894	279,896	311,457	322,830	321,125	332,747	353,267
무선데이타통신	80,499	104,608	111,051	111,433	97,272	100,354	90,984
GM-PCS	0	0	0	0	0	4,412	3,897
합계	56,264,300	56,926,441	59,924,809	61,738,740	63,777,372	67,104,635	68,227,951

이동전화 시장을 보면 SKT가 시장의 절반 정도를 차지하고 있으며, 3세대 서비스만을 보면 3세대 서비스에 대한 투자에 적극적이었던 KTF가 SKT와 비슷한 정도의 가입자를 보유하고 있다. IPTV와 다양한 형태의 결합 서비스 등장으로 상당기간 유지되었던 이동통신 시장 점유 구조에 변동이 예상되지만, 단기적으로 현재와 같은 3사에 의한, 특히 SKT와 KTF에 의한 과점 상태가 변화되기는 어렵다. 그러나 장기적으로 4세대 서비스 이상으로 발전하여 데이타 전송률이 높아지고, 차세대 네트워크가 본격화되어 네트워크 환경이 IP 기반의 패킷스위칭을 중심으로 변화할 것으로 예상되고 있어, 현재와 같이 이동전화를 중심으로 한 이동통신 시장 구조와 경쟁 상황은 변화를 맞을 것으로 예상된다.

표 4: 2008년 12월 이동통신사별 가입자 수와 점유율[4]

	SKT	KTF	LGT	전체
전체 가입자 수	23,032,045	14,365,233	8,209,706	45,606,984
3세대 가입자 수	8,239,455	8,266,081	-	-
시장점유율	50.50%	31.50%	18.00%	100%

4 각사가 홈페이지를 통해 발표한 월별 실적 자료를 바탕으로 재구성

III. 도감청 사례

1. 정부의 불법 도청[5]

(1) 유선전화 도청

가) 군사정권

군사정권은 한국에서 감시기술을 선도하는 역할을 하였다. 군사쿠데타로 집권한 박정희 정부하에서는 1961년 중앙정보부 내에 20명으로 구성된 과(課) 단위의 도청 조직이 유선전화 도청을 시작하였고, 1968년에는 60명의 단(團) 규모가 약 70만 명의 전화가입자를 대상으로 도청을 시행하였다. 역시 군사쿠데타로 집권한 전두환 정부의 말기에는 1,000만 회선으로 전화의 대중화가 이루어졌고, 한국통신공사가 발족하여 통신 도청을 협조 지원하는 체계로 확대되었다. 전두환 정부를 이어받은 노태우 정부 시절인 1988년 이후에는 국가기간전산망 사업이 시행될 정도로 청와대가 국가의 정보화를 주도적으로 이끌었고, 이와 더불어 도청을 확대하기 위한 기술개발이 이루어졌다.

1988~89년에는 국회 국정감사에서 국가에 의해 개발되었다고 추정되는 도청 기술, 일명 '블랙박스'를 둘러싼 논쟁이 일었다. 당시 야당의 주장에 따르면 전두환 정부에서부터 '비음성 통신용 전송품질측정시스템'이 전국에 44개 설치되어 있는데, 이것이 전화를 도청하는 '블랙박스'라고 하였다. 이 주장에 따라 국회는 1989년 9월 28일 광화문 국제전화국 ITMC 시설에 대해 현장검증을 시행하였지만 관련자들은 이 시설이 도청 장비가 아니라고 부인하였다.

군사정권하에서의 감시체계는 반공주의를 국민에게 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.

---

5 이 절의 내용은 고성학, "한국의 민주화와 감시권력의 변화 – 민주화 이전 정부와 이후 정부의 비교", 숭실대학교 대학원 정치외교학과 박사학위 논문, 2005.12. 를 주로 참고하였다.

나) 문민정부 이후

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. 여당 후보였던 김영삼 씨가 이 사건을 둘러싼 논란 속에 대통령으로 당선되었고, 집권 초기부터 정부와 국회에서 도청을 방지하기 위한 법률 제정이 논의되기 시작하였다. 1993년 12월 마침내 통신비밀보호법이 제정되어 법률적 근거 없이 시행되던 정보 · 수사기관의 도청이 제도화하기에 이른다.

그림 1: 정보기관 도청 연혁
(* 출처: 서울신문 2005.12.15일자)

그러나 2005년 7월 21일 안기부의 불법도청 테이프(일명 X-파일) 사건이 언론 보도를 통해 밝혀지면서 한국 사회는 또다시 큰 충격에 휩싸였다. 통신비밀보호법에도 불구하고 김영삼 정부는 1994년부터 이전의 군사정권과 마찬가지로 도청을 시작하였으며, 안기부(1999년 1월 국가정보원으로 개편)에서 불법적인 도청전담 조직을 유지하면서 정치적 목적으로 도청하였다는 사실이 드러난 것이다.

당시 안기부 과학보안국은 법원 허가 없이 유선 전화를 도청하였다. 광화문, 혜화, 영동, 신촌, 신사, 목동 전화국에서 매주 1~2회씩, 1회에 도청 대상자 유선전화 회선 2~3개를 안기부 회선에 연결하는 방식으로 도청이 이루어졌다. 전화국 협조가 필요했기 때문에 보안상 대규모 도청은 어려웠지만, 주요 인사들에 대해서는 빠짐없이 도청이 이뤄진 것으로 검찰 수사 결과 드러났다. 해당 전화국 관련자에게는 보안 유지 대가로 매달 10만~50만 원이 지급됐다.

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 공운영 씨의 집에서 압수한 도청 테이프 274개와 녹취록 13권에 나타난 도청 건수는 총 554회에 달했다. 도청 피해자는 정치인이 273명으로 가장 많았고, 고위 공무원 84명, 언론계 인사 75명, 재계 57명, 법조계 27명, 학계 26명, 기타 104명 등이었다.

(2) 이동통신 도청의 등장

이동전화 도감청 기술은 크게 세 가지 방식으로 나뉠 수 있다. 첫째는 휴대폰을 복제하거나 도청 장치를 휴대폰 등에 장착하는 것이다. 둘째는 공중에서 전파를 가로채서 통화내용을 엿듣는 것이다. 휴대폰과 무선 기지국 사이에 전파를 통해 이루어지는 통신을 가로채는 것이다. 셋째는 통화자의 통신이 무선 기지국을 지나서 유선을 통해서 이후 인터넷이나 유선전화망으로 전달되는 과정에서 통신사실 자료와 통신내용을 가로채는 것이다.

이 글에서는 둘째와 셋째 방식을 중심으로 도청 기술을 분석한다. 휴대폰과 무선국 사이의 전파를 가로채는 방식의 경우, 1세대 이동전화의 경우에는 전파를 가로채는 것만으로 간단히 도감청을 할 수 있었으나, 2세대 이동전화의 경우에는 한국에서 채택한 CDMA 기술 자체에 포함된 스펙트럼 확산(spread spectrum) 성질로 인해 의사 잡음 시퀀스(pseudo-random noise sequence; PN sequence)를 모르고는 원래의 신호를 복원할 수 없어 별도의 통신 내용에 대한 암호화가 없이도 일정 수준의 보안 기능이 내재되어 있다. 이러한 특성을 들어 한국의 정보수사기관은 도청 의혹에 대해서 부인해 왔다.

그러나 2005년 검찰의 수사를 통해서 2세대 CDMA 서비스상에서도 전파를 가로채 도청이 이루어졌으며, 또한 서울 시내 전화국 일부에서 유선을 통한 도청 또한 광범위하게 이루어진 것이 밝혀졌다.

가) 2세대 아날로그 이동통신 도청

김영삼 정부는 1996년 1월부터는 이탈리아 B사로부터 아날로그 이동통신 도청 장비 4세트를 구입하여 1999년 12월 아날로그 이동통신 서비스가 중단될 때까지 사용하였다. 이 장비는 1~2개월 단위로 수십 차례 불법 사용됐고, 사용자가 현장에서 번호를 입력하는 식으로 활용됐다.

도청 장비는 10에서 15킬로그램 정도로 서류가방 크기여서 휴대가 가능하고 동시에 6개의 통화를 도청할 수 있었다. 도청대상 휴대폰과 동일 기지국 내에 있고, 휴대폰 번호를 알면 도청이 가능하였다.

안기부 외에도 대검찰청, 경찰청, 세관, 국방부 등 다수 기관이 역시 정부로부터 인가받지 않고 기업체를 통하여 도청 장비를 불법 수입하였다는 사실이 밝혀지기도 하였다. 2005년 8월 24일 국회 예산결산특별위원회에서 천정배 법무장관은 대검찰청이 1995년 3월 미국산 이동통신 도청기를 도입하는 등 1998년까지 총 8대의 아날로그 이동통신 도청기를 구입하여 불법적으로 사용하였다고 밝혔다.

특히 1996-99년 사이에 도청 장비 구입이 급증하였다는 통계적 사실이 흥미롭다. 이 시기 전후로 특별히 범죄율이 급증하였다는 증거는 없다. 다만, 대통령 선거와 정권 교체가 있었으며 IMF로 경제상황이 극도로 불안정하였다는 정치경제적 특수성이 존재할 뿐이다. 이런 시기적 특수성에 더하여

1996년 12월에는 국가안전기획부법이 개정되었던 점이 도청 장비에 대한 수요 증가 요인으로 추정된다. 이때 개정된 내용은 인권유린과 정치적 악용의 소지가 많았던 국가보안법 제7조(찬양고무 등)와 제10조(불고지죄)에 규정에 대한 안기부의 수사권 부활이었다. 안기부의 수사권 부활은 정치권력의 요구에 따라서 남용될 소지가 있는 것으로 지적되어 왔다.

표 5: 2005년도 정보통신부 국회제출자료

구분	1994 ~ 95	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005 .7	계
다우너 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

나) 2세대 디지털 이동통신의 도청

야당으로서 처음 집권한 김대중 정부하에서도 도청이 계속 이루어진 것으로 드러났다. 1998년과 1999년 언론을 통해 "CDMA 휴대폰은 기술적으로 도청이 불가능"하다고 누차 확언하였던 김대중 정부는 이면에서 CDMA 이동통신 도청 장비를 직접 개발한 것으로 밝혀져 주목을 받았다. 당시 국가정보원(국정원)은 1996년 1월부터 디지털 이동통신이 상용화되자 유선중계통신망 도청 장비인 'R2'(1998년 5월 개발 완료)와 이동식 이동통신 도청 장비인 'CAS'(1999년 12월 개발 완료)를 직접 개발해 8국 사무실에 장비를 차려놓고 도청에 활용했다. [6]

CAS와 같이 무선상에서 이루어지는 도청은 도청하려는 대상에 아주 가까운 거리에 있어야 하며 상대적으로 소수 대상으로만 도청이 가능한 반면에, R2와 같이 유선을 통한 도청은 무선상에서와는 비교할 수 없이 많은 수를 더 낮은 비용으로 도청하는 것이 가능하다. 하지만, R2와 같은 방식으로 도청하기 위해서는 직접 전화국에 장비를 설치해야 하기 때문에 도청하려는 자와 도청당하는 자 말고도 제삼자에 의해 도청 행위가 인지될 가능성이 높아 도청 사실을 제삼자 누구에게도 알리고 싶지 않은 경우에는 적합하지 않은 기술이다.

---

6 "국정원의 과거 불법감청 실태 발표문(요약)", 한겨레 2005.8.5; "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. 등 언론보도와 검찰의 "안기부국정원 도청.불법감청 관련 사건 중간수사결과"(2005.12.14) 발표자료 참고.

다) 2세대 디지털 이동통신에서 유선 상의 도청

2005년 검찰의 수사에 따르면, 안기부와 국정원은 유선중계통신망 도청 장비인 R2를 총 14억여 원의 예산을 투입하여 1998년 5월경 1세트, 1999년 9월경 5세트 등 총 6세트 개발하여 사용하였다.

R2 도청 장비는 이동통신사의 상호접속교환기(MSC; Mobile Switching Center)와 KT의 관문교환기(IGS로 여겨짐; Interconnection Gateway Switch)가 연결되어 있는 전화국에서 유선중계통신망 회선을 분리, 연결하여 해당 유선중계통신망을 통과하는 통화를 도청하였다. 중계통신망은 여러 전화번호의 통화가 이루어지는 통로로서 그 구간을 통과하는 모든 통화의 도청이 가능했다. 유선전화의 실선 구간은 전화번호마다 부여된 실선 하나하나에 대해 도청 장비를 연결해야 하지만 중계통신망은 여러 번호의 통화가 이뤄지는 통로인데다, 이동통신이라도 유선망을 통해 중계된다는 점에 착안해 유선중계통신망에 대한 도청을 시행한 것이다. 'R2' 라는 명칭은 당시 사용되던 중계통신망의 신호 방식을 부르던 명칭에서 유래했다.

R2 1세트당 최대 600회선 접속 가능하고, 동시에 64회선까지 도청이 가능하였다. 입력은 600회선, 출력은 64회선이었다. 총 6세트의 장비를 운영하여 최대 3,600회선까지 접속이 가능하였다. R2 장비에서는 특정번호를 미리 입력하여 해당 번호의 통화만을 도청할 수도 있고, 무작위로 도청하는 것도 가능하였다. 국정원은 R2에 정치 · 언론 · 경제 · 공직 · 시민사회단체 · 노동조합 간부 등 주요인사 1,800여 명의 휴대폰 번호를 입력해 놓고 24시간 이들의 통화를 도청했다.

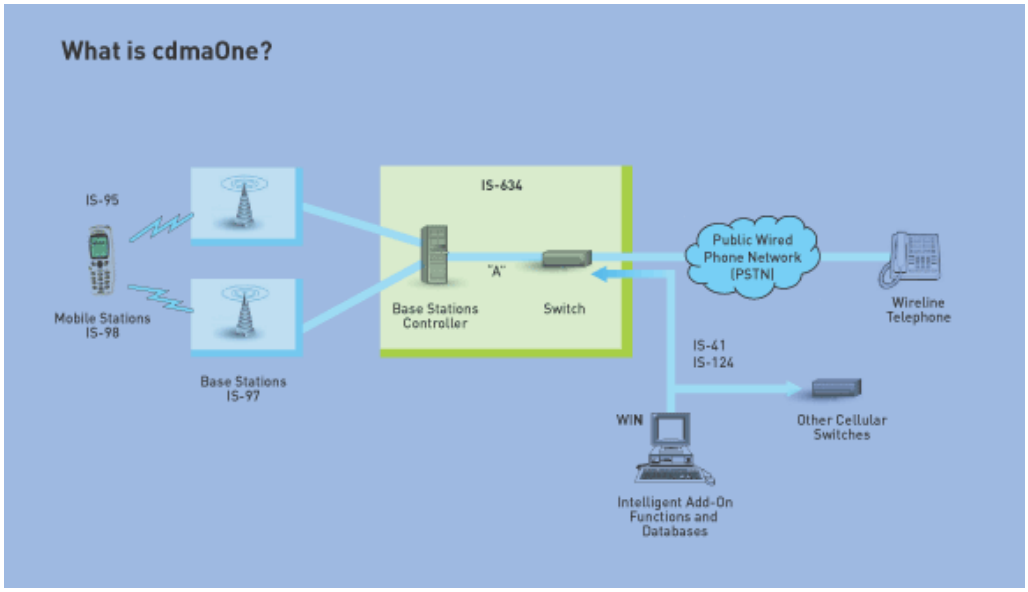

그림 2: 2세대 CDMA (cdmaOne) 네트워크 구성도 (출처: CDMA Development Group, "2G-cdmaOne")

R2 장비를 이용한 유선상에서의 도청에 대해서는 그림 2에서 간략하게 표현된 2세대 디지털 이동통신 망의 구성도를 살펴보는 것이 이해를 도울 수 있을 것이다. 뒤에서 설명할 무선 상의 도청이 망 구성도에서 보면 IS-95라는 표준에 따른 무선 접속 표준에 따른 단말기(그림에서 Mobile Stations)와 기지국(그림에서 Base Stations; Base Transceiver Station; 약어 BTS) 사이의 무선 통신에서의 보안 취약점을 악용한 것이라면, R2를 이용한 유선 상의 도청은 그림에서 Switch(이동통신 교환기; Mobile Switching Center; 약어 MSC)와 공중전화교환망(그림에서 Public Wired Phone Network 또는 Public Switched Telephone Network; 약어 PSTN; 유선전화망) 사이에서 이루어진 것으로 보인다. 여러 개의 기지국은 하나의 기지국 제어기로 연결이 되고, 다시 여러 개의 기지국 제어기는 이동통신 교환기로 연결된다. 한 이동통신 가입자가 유선 전화 가입자나 다른 이동통신사의 가입자와 통화를 하기 위해서는 이동통신 교환기에서 통화 대상자가 속한 망의 해당 가입자에게 전달하는 과정이 필수적으로 이루어지게 된다. 한 이동통신 교환기와 다른 이동통신 교환기 사이 그리고 이동통신 교환기와 유선전화망과의 물리적인 연결은 광케이블로 이루어지게 되고 R2는 이러한 연결에 쓰인 광케이블에서 회선을 분리하여 도청한 것이다.

라) 2세대 디지털 이동통신에서 무선 상의 도청

2005년 검찰의 수사에 따르면, 국정원은 총 19억여 원을 들여 1999년 12월경에 CAS(CDMA Analysis System)를 자체 개발하여, 이 장비 20대를 만들어 도청에 사용하였다. CAS를 통한 도청의 경우, 국정원은 45킬로그램 정도 되는 이 장비를 자동차 등에 탑재하여 단말기의 200미터 정도에 접근하여 도청대상 휴대폰의 주파수, 기지국 위치, 단말기의 ESN(고유번호)을 알아낸 후 암호화된 음성정보를 해독하였다. 이 장비는 2000년 5월경부터 2001년 4월경까지 사용되었다.

CAS를 통해 공중에서 전파를 가로채어 도청할 수 있었던 것은 CDMA의 물리 층위(physical layer)에서 이루어지는 스펙트럼 확산에 쓰인 PN 코드를 ESN으로부터 쉽게 알아낼 수 있었기 때문이다.

2001년 12월 통신비밀보호법이 개정되어 감청설비 신고 등 절차가 강화되고 16대 대선을 앞두고 불법 도청 논란이 커지자 안기부는 2002년 3월 불법 도청팀을 해체하고 CAS는 물론 R2 등 도청 장비들을 전량 폐기하였다고 한다.

(3) 이동통신 도청의 기술적 기반

가) CDMA 기술의 물리 층위에서의 보안성: 대역확산과 스크램블링

무선통신에서 여러 개의 단말기가 하나의 기지국과 특정한 주파수와 시간을 함께 사용하여 통신하기 위해서는 개별 단말기가 주파수와 시간을 이용하여 신호를 보내는 과정에서 다른 단말기와 충돌하지 않고 서로 구별될 수 있어야 한다. 이와 같이 다수의 단말기가 동시 접속하는 방법을 다중접속(multiple access)이라 한다. 이동통신 분야에서 주로 사용된 다중접속 기술로는 아날로그 이동통신에서 많이 사용된 주파수 분할 다중접속(Frequency Division Multiple Access; FDMA), 유럽에서 많이 사용된 2세대 GSM 서비스 등에서 사용된 시간 분할 다중접속(Time Division Multiple Access; TDMA), 한국의 2세대 이동통신에서 사용된 코드 분할 다중접속(Code Division Multiple Access; CDMA) 등이 있다. FDMA는 각 사용자가 서로 다른 주파수를 사용하여 충돌을 피하는 것이고, TDMA는 각 사용자가 서로 다른 시간대를 사용함으로 충돌을 피한다. 이에 반해 CDMA는 확산코드를 통해 각 사용자가 구별되어 수신자 측에서 이 확산코드를 적용하여 역으로 각 사용자의 신호를 복원하는 방식을 취한다. 국정원의 도청의 대상이 되었고, 현재 3세대 기술에서 다중접속 기술로 CDMA2000 계열과 WCDMA(Wideband CDMA) 계열에 채택된 CDMA 기술을 좀 더 자세히 살펴보자. 여기에서 제시하는 구체적인 기술 사항은 한국에서 채택되어 사용되고 있는 2세대 CDMA 기술 표준으로서 IS-95를 기준으로 한다.

CDMA 기술은 기본적으로 스펙트럼 확산을 이용한다. 스펙트럼 확산 방식은 보내고자 하는 신호를 그대로 보내는 것이 아니라 이 신호를 보내는 데 필요한 대역보다 더 넓은 대역을 이용하는 신호로 변환하여 신호를 전송하는 기술이다. 스펙트럼 확산을 위해서는 좁은 대역의 신호를 넓은 대역의 신호로 바꾸는 변환이 필요하게 되고, CDMA 기술에서 이에 해당하는 변환에 쓰이는 코드가 PN 코드(확산 코드)이다.

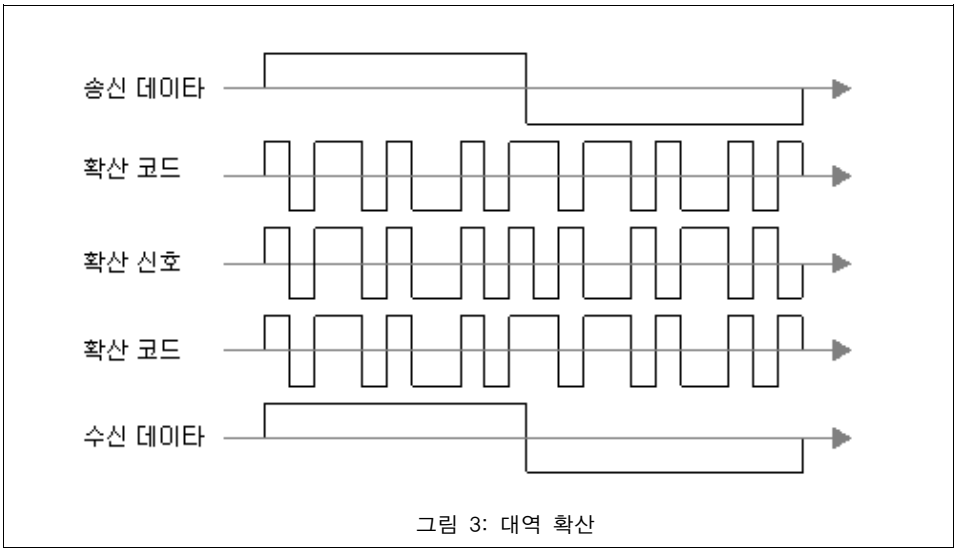

그림 3: 대역 확산

단말기와 무선국 사이에 통신이 이루어지는 과정에서 위의 그림에서처럼 송신하는 측이 1과 0이라는 데이타를 보낸다고 했을 때, 실제 공중에서 잡히는 신호는 확산 코드에 의해 변화된 확산 신호가 된다. 따라서 이 확산 코드를 모르는 상태에서 공중에서 신호를 가로채어도 디지털화된 음성 신호와 같은 의미 있는 데이타로 복구할 수 없다.

이러한 대역확산(spreading)에 따른 신호의 변환과 더불어 IS-95에서는 추가적으로 데이타의 보안을 위해 스크램블링(scrambling)의 과정을 수행한다. 스크램블링은 추정이 어려운 의사 난수(pseudo-random sequence)를 신호에 적용하여 변환하는 것을 말한다. 따라서 IS-95에 따른 무선 통신에서 통화 내용을 엿듣기 위해서는 확산에 쓰인 코드와 스크램블에 쓰인 코드를 동시에 알아야 한다.

2005년 검찰 수사 전까지 과거 정부는 IS-95의 이러한 스펙트럼 확산 기술의 특성과 스크램블 과정을 들어 휴대폰 도감청이 불가능하다고 주장하였다.

나) IS-95의 무선통신 도청 가능성

류대현과 장승주는 2003년 논문, "CDMA 서비스의 보안추약성과 개성방안" 에서 기지국에서 단말기로 전해지는 순방향 링크(forward link)를 도청하는 장비와 알고리즘을 제시하고 실험을 통해 도청에 성공하였다.[7]

---

7 류대현 · 장승주, "CDMA 서비스의 보안취약성과 개선방안 *An Enhanced Mechanism of Security Weakness in CDMA Service*", 한국정보과학회논문지: 정보통신 제30권 제6호, 2003.12, pp. 729~742.

IS-95와 이후의 CDMA 기술에서 기지국과 단말기의 무선통신은 기지국에서 단말기로 신호가 보내지는 순방향 리크(forward link)와 단말기에서 기지국으로 신호가 보내지는 역방향 링크(reverse link)로 나누어진다. 그리고 순방향 링크와 역방향 링크는 다시 기능에 따라 논리적으로 여러 개의 채널로 다시 구분이 된다. 이러한 구조는 IS-95만이 아니라 3세대 CDMA 기술에서도 세부적인 채널의 종류 등이 달라지는 점을 빼고는 동일하다. IS-95에서는 순방향 링크는 파일롯(pilot) 채널, 동기(sync) 채널, 호출(paging) 채널, 통화(traffic) 채널로 나뉘고, 역방향 링크는 액세스(access) 채널, 통화(traffic) 채널로 나뉜다. 각각의 채널에 따라 기능도 다르고 확산과 스크램블링의 적용 여부와 쓰이는 확산코드나 스크램블링 시퀀스가 달라진다.

순방향 링크에서 통화 채널의 경우, 신호는 일차적으로 롱코드에 의해 스크램블된 후에 왈시 코드(Walsh code)에 의해 채널화된다. 역방향 링크에서 통화 채널은 왈시 코드에 의해 변조되고 이는 다시 롱코드에 의해 확산이 된다. 이때 사용되는 롱코드는 공적(public) 또는 사적(private) 롱코드가 있다. 사적 롱코드는 음성 보안의 경우에 사용된다.

공적 롱코드와 사적 롱코드 생성에 쓰이는 매스크(mask)의 구조는 다음 그림과 같다.

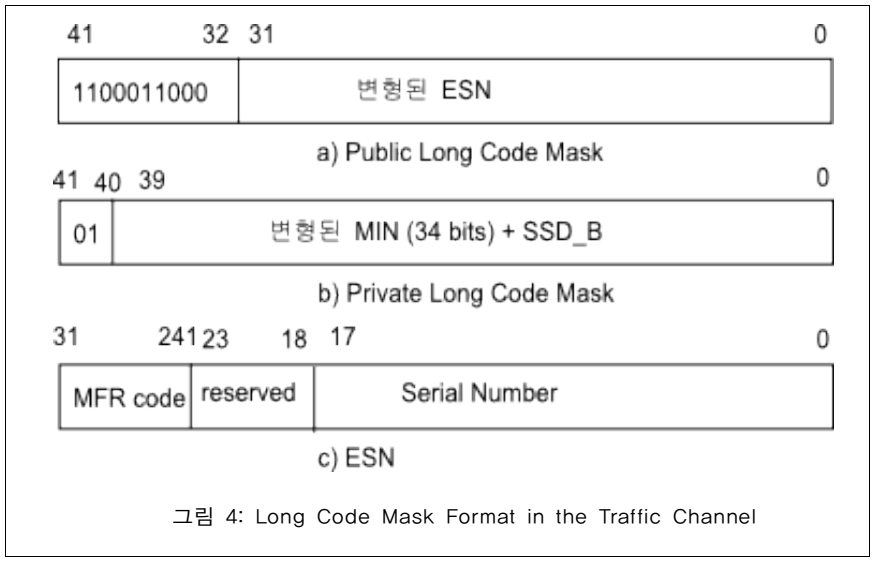

그림 4: Long Code Mask Format in the Traffic Channel

위의 논문에서 저자들은 액세스 채널과 호출 채널을 통해 전파되는 MIN, ESN을 해독함으로 해서 통화 내용의 작성에 쓰이는 롱코드를 알아낼 수 있었다.

호출 채널은 왈시 함수(Walsh function)를 통해 확산된 후에 호출 채널용 롱 코드 마스크로 스크램

블링되며, 액세스 채널은 액세스 채널용 롱 코드 마스크를 이용해 확산되게 된다. 이 두 가지 채널에서 각각 쓰이는 롱 코드 마스크는 다음 그림과 같다.

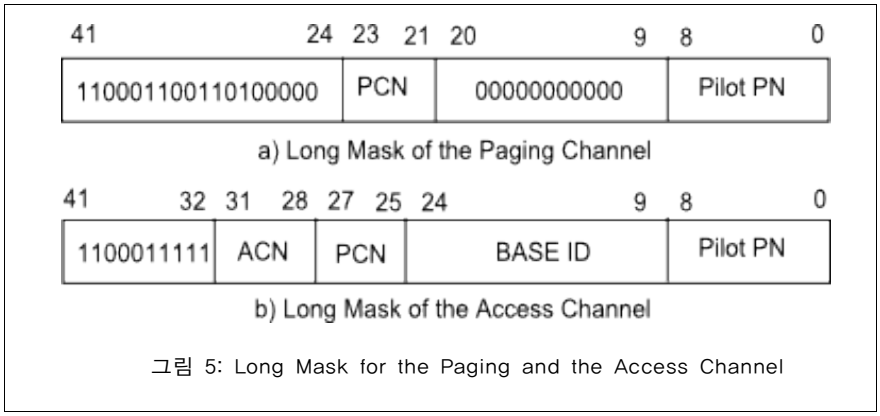

그림 5: Long Mask for the Paging and the Access Channel

저자들은 호출 채널의 롱 코드 마스크에서 Pilot PN은 파일롯 채널을 모니터링함으로써 알 수 있었으며, PCN(Paging Channel Number)는 세 비트로 이루어진 '000' 에서 '111' 사이의 값으로 이 정보는 알려진 데이타를 이용한 해쉬 함수(hash function)에 의해 만들어지고 있었다. 따라서 PCN은 쉽게 해독이 가능했다. 액세스 채널의 BASE ID의 경우는 동기 채널을 모니터링해서 얻을 수 있었으며, ACN(Access Channel Number)은 호출 채널을 통해 얻을 수 있었다.

사적 롱 코드 마스크에서 MIN과 SSD_B로 이루어진 부분은 실제 같은 전화번호의 경우 항상 동일한 값이 생성되었다. 공적 롱 코드 마스크는 ESN의 데이타를 재조합 것에 불과하였다.

(4) 정부의 불법 도청과 통신사업자의 역할

정부와 수사기관의 불법 도청 사건들에서 통신사업자는 꼭 필요한 협조자였다.

통신사업자는 안기부의 요구에 따라 R2와 같은 불법 도청 장비를 자신들의 설비에 설치하거나 불법 회선을 제공한 사실 외에도, 일상적으로 수사기관의 불법 도청 요구에 협조한 사실이 드러나기도 하였다. 2000년 5월 12일 감사원은 "통신제한조치 운용실태 감사결과"를 발표하면서, 수사기관에 의한 불법적인 도감청은 물론이고 이에 대한 통신사업자들의 협조 문제를 지적하였다. 전화국 담당자들이 법원의 감청 영장 등을 확인하지 않고 감청 요청에 응했는가 하면 협조대장에 감청내역조차 기록하지 않았고, 통신회사들이 이동전화와 무선호출기, 음성사서함 감청을 요청하는 수사기관에 메시지 내용을 제출하는 것이 아니라 아예 비밀번호나 복제용 인식부호를 넘겨줌으로써 수사기관이 감청 기간 종료

이후에도 계속 감청을 할 수 있도록 하였다.[8] 48시간 동안 허용되는 수사기관의 긴급감청이 확인서를 제출하지 않은 채 이루어지거나 허용된 기간을 초과하여 이루어지는 데에도 통신사업자들은 이에 동조하였다. 허가가 만료된 후에도 감청 회선이 해지되지 않아 계속 감청에 사용되기도 하였다. 또 통신비밀보호법상 긴급감청을 협조 요청할 수 있는 자는 검찰, 경찰, 국정원, 국방부 등에서 일정 직급 이상이어야 하지만, 검찰직원, 순경, 이병 등 직급에 상관없이 수사기관 직원 아무나 감청을 집행하는 사례도 다수 발견되었다.

2003년 8월에는 검찰과 경찰이 적법 절차를 거치지 않은 채 통신업체 가입자들에 대한 통화내역을 불법으로 조회했다는 의혹이 사실로 드러났다. 당시 한나라당 권영세 의원에 따르면 수사기관이 통신회사에 통화내역 조회를 요청할 때 검사장의 사전 · 사후 승인을 받도록 한 통신비밀보호법상 절차를 거치지 않고 조회된 통화내역 건수가 1,966건에 달하였다. 이후 정보통신부는 권 의원이 지적한 1,966건 중 1,191건은 문제제기 이후 검사장 승인서가 통신업체에 전달됐다고 밝혔고, 나머지 경찰 704건과 검찰 62건, 국방부 8건, 세관 1건 등 775건에 대해서는 경위조사를 의뢰하였다. 경찰과 검찰은 대부분 업무착오나 실수에 의한 것이었다고 해명하였으나 당시 통신업체들은 적법절차 없이도 통화내역 조회에 응한 것으로 나타나 논란이 일었다.[9]

2. 정부의 합법 감청과 자료 제공

한국에서 수사기관의 감청 및 통신자료 제공은 다음과 같이 이루어진다. 첫째, 유선전화의 통화 내용에 대한 '감청'은 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[10] 압수하는 방식으로 이루어지고 있어 문제를 지적받고 있다.[11]

통화 상대방, 통화일시, 위치정보, 인터넷 IP 주소와 같은 로그기록 등 '통신사실확인자료'는 통

8 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 휴대폰을 포함한 4,050개의 개인 휴대폰, 무선호출 음성사서함의 비밀번호가 그대로 제공되었다.

9 연합뉴스 2003.8.3.

10 대판 2003. 8. 22, 2003도3344.

11 박영선 의원 보도자료, 2008.10.10, http://www.pys21.net/bbs/view.php?DB=movement&num=166&start=10&S=&val=&word=.

신비밀보호법에 따라 수사기관이 법원의 허가를 받아 통신사업자에게 요청한 경우에 제공된다. 다만, 가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 '통신자료'는 통신비밀보호법의 보호대상이 아니기 때문에 수사기관이 통신사업자에게 서면으로 요청서를 제시하면 간단히 제공될 수 있다. 자세한 현황은 다음과 같다.[12]

(1) 통신 감청

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

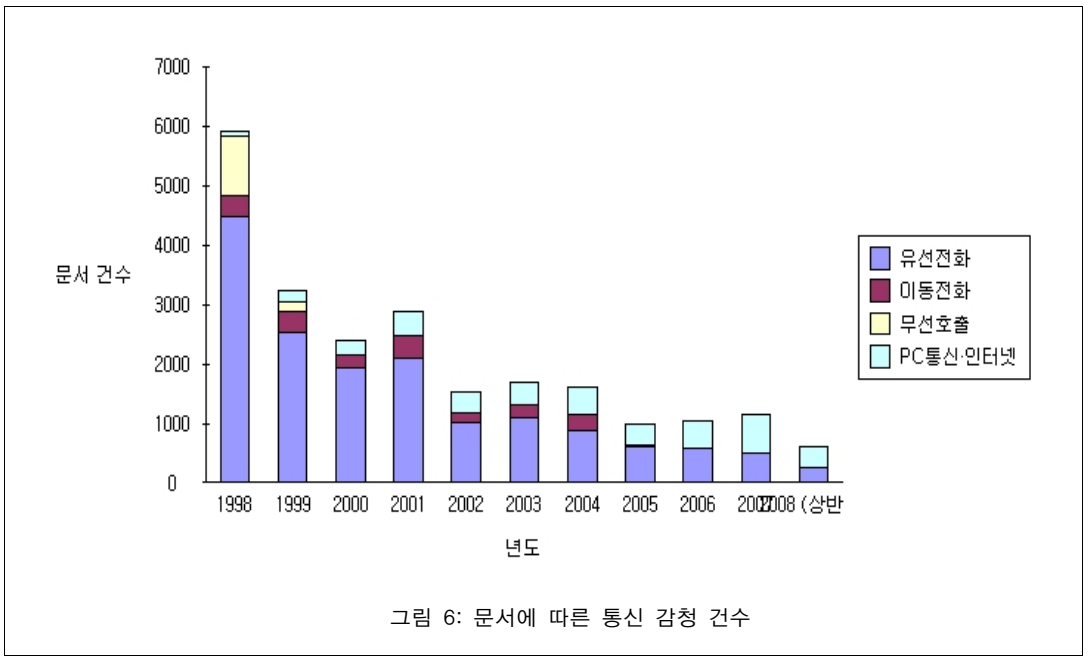

그림 6: 문서에 따른 통신 감청 건수

그러나 감청건수를 문서 건수가 아니라 전화번호 혹은 아이디 건수별로 재분석하여 보면, 한 문서당 기재되는 전화번호나 아이디가 증가하였기 때문에 전체 감청건수는 오히려 전반적으로 증가하는 추세이다. 특히 국정원의 감청 분량이 두드러진다. 2007년 전체 감청건수 8,803건 가운데 국정원 감청은 8,628건에 달하여 전체의 98%를 차지하였다.

12 이상의 감청 및 통신자료 제공 현황은 2000년 6월 개정된 [전기통신감청 및 통신자료제공 관련업무 처리지침]에 따라 정보통신부와 이를 이어받은 방송통신위원회에서 연 2회 공개한 자료를 재가공하였다.

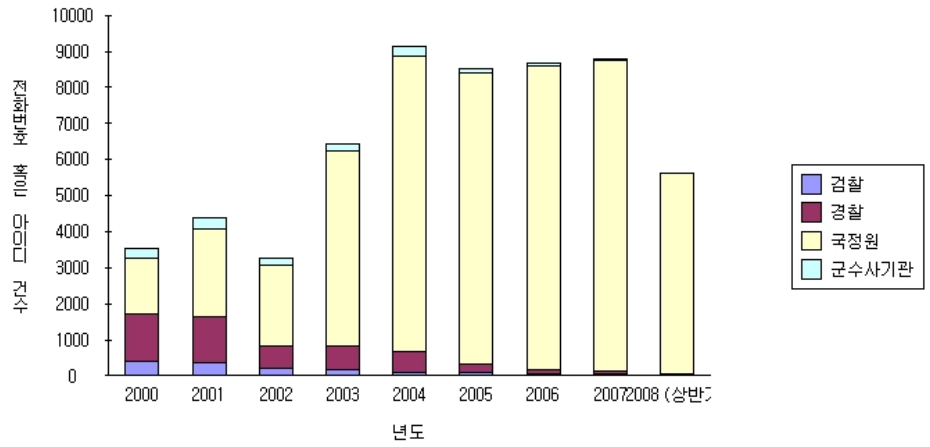

그림 7: 대상에 따른 통신 감청 건수

(2) 통신사실확인자료 제공

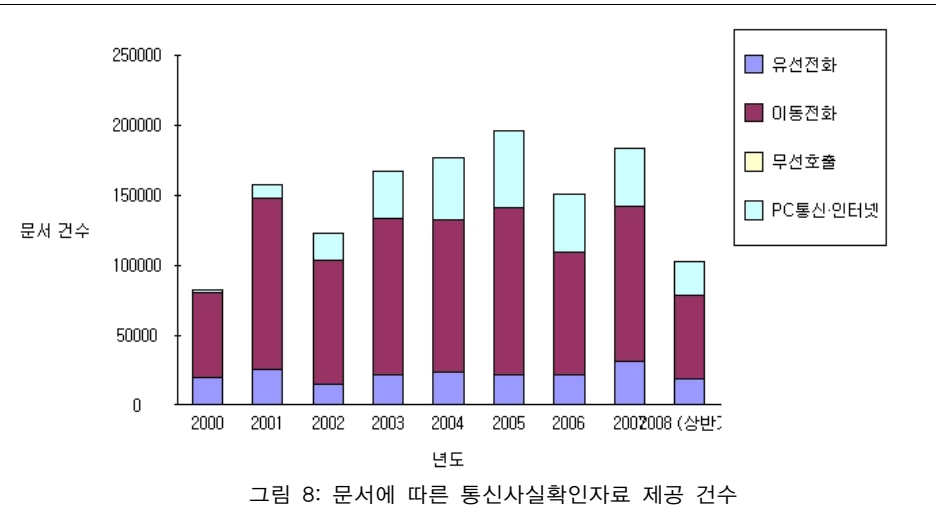

그림 8: 문서에 따른 통신사실확인자료 제공 건수

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

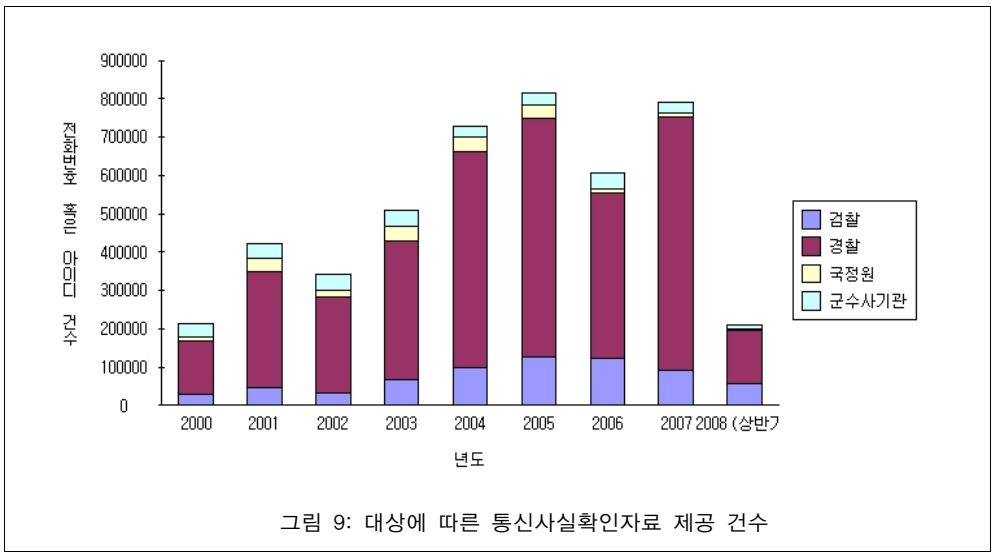

그림 9: 대상에 따른 통신사실확인자료 제공 건수

한편, 국회의 통신비밀보호법 개정과 별도로 정부는 2005년 통신비밀보호법 시행령을 개정하여 통화내역이나 로그기록 등 통신사실확인자료의 보관을 의무화하였다. 그 기간은 매체별로 차등을 두어 시내 · 시외 유선전화 관련 자료는 6개월, 이동전화 관련 자료는 12개월, 인터넷 관련 자료는 3개월을 규정하였다. 이 시행령 개정은 모법에 관련 근거가 없으며(포괄적 위임) 모든 통신 이용자를 잠재적 범죄자로 간주한다는 점에서 그 위헌성을 지적받고 있다.

(3) 통신자료 제공

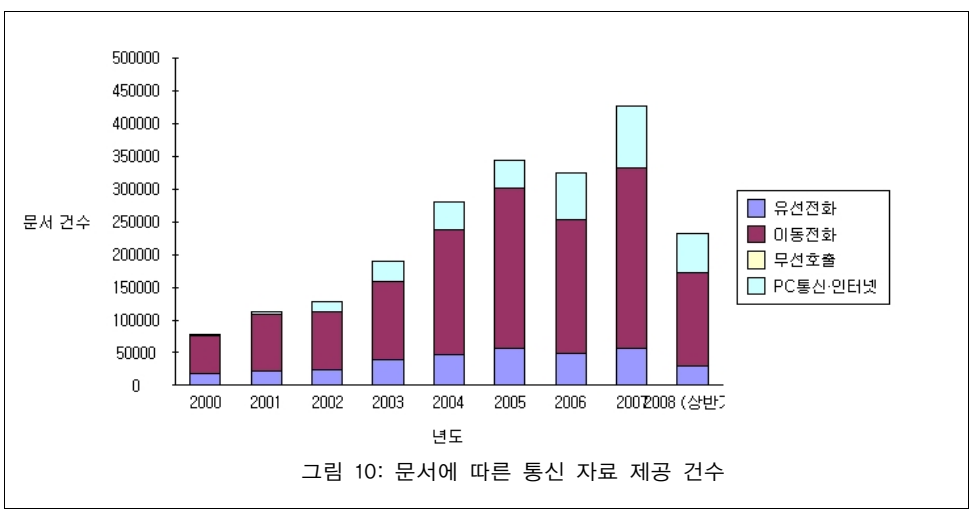

그림 10: 문서에 따른 통신 자료 제공 건수

가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료 제공은 2007년 특히 인터넷 분야에서 급격히 증가하였다. 전화번호 혹은 아이디 건수 등 대상별로 보면 4백만 건을 훌쩍 넘어섰다. 이는 2007년 7월 37개 주요 인터넷 사이트에 국가적인 실명제가 의무화되면서 이에 대한 수사기관의 요청이 증가한 데 따른 것으로 추정된다. 다음, 야후 코리아, 디씨인사이드 등은 의무적 실명제 도입 후부터 이용자의 실명 정보를 수집하기 시작하였기 때문이다.

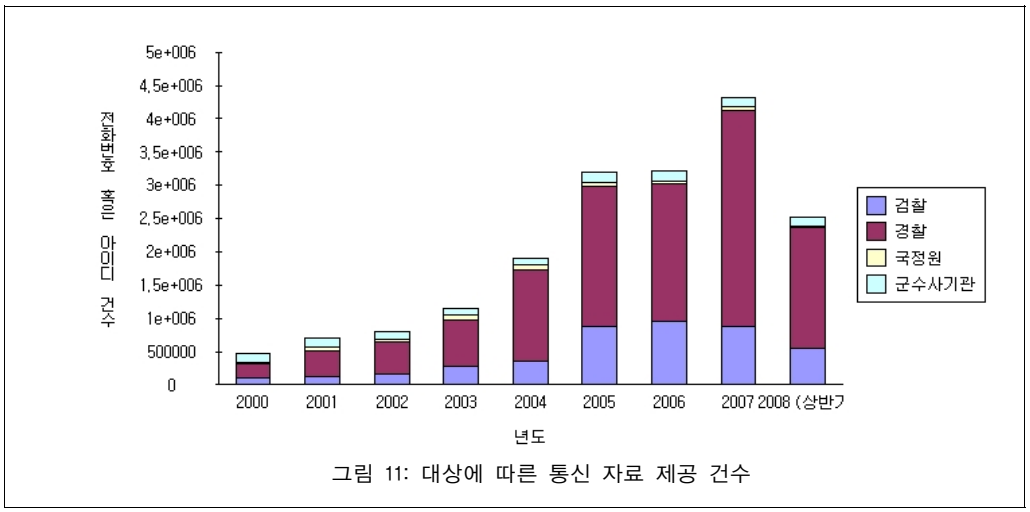

그림 11: 대상에 따른 통신 자료 제공 건수

(4) 자료 제공의 오남용

적법한 절차를 거친 통신 감청 혹은 통신사실확인자료 제공이라 하더라도 수사기관이 정부 출입기자의 통화내역을 조회하는 등 오남용 사례가 드러나 비판받는 경우도 발생하였다.

2003년 10월 대검 중앙수사부가 주요 사건 수사정보 유출자 색출을 명목으로 출입기자 이동전화 통화내역을 수시로 추적해온 것으로 확인돼 언론자유 침해 논란이 일었다. 대검은 이 해 7월 초 현대 비자금 수사에 본격 착수한 직후 수사상황이 언론에 보도될 경우 소속 검사 및 수사관들의 이동전화 착발신 내역과 이를 보도한 해당 기자의 착발신 내역을 서로 비교하는 방법으로 유출자를 색출해온 것으로 전해졌다.

2004년 1월 국정원이 국가안전보장회의(NSC)와 외교통상부의 보안 유출 가능성과 관련해, 일간지 기자의 이동전화 통화내역을 조회한 것으로 밝혀졌다. 특히 이 과정에서 통화내역을 조회한 담당 부서가 지방검찰청장의 승인서가 필요한 국정원 수사국이 아니라 국정원장의 승인서만으로 조회가 가능한 대테러보안국이었음이 밝혀져 논란이 크게 일었다. 이에 국회 과학기술정보통신위원회는 에스케이텔레콤 · 케이티에프 · 엘지텔레콤 등 3개 이동통신회사를 잇달아 찾아 통신사실확인자료 제공에 관한 현

장검증을 벌였으나, 통신회사 쪽이 전기통신사업법과 통신비밀보호법에 저촉된다는 이유로 자료 공개를 거부해 현장검증이 무산됐다.

2009년 1월에는 검찰과 경찰이 국방부 '감사처분 요구서'를 보도한 기자들의 통화내역을 조회한 것으로 드러나 국민의 알권리를 차단할 뿐 아니라 언론의 취재 자유를 근본적으로 제한할 수 있다는 비판이 제기되었다. 국방부와 경찰에 따르면 검 · 경은 2008년 6월 국방부의 주한미군기지 이전사업단에 대한 감사처분 요구서를 보도한 국방부 전 · 현 출입기자 2명의 통화내역을 조회하였다.[13]

3. 민간에 의한 감청

통신비밀보호법상의 여러 규제 속에서도 정보수사기관의 불법 도청이 계속되는 가운데, 정부는 야당의 불법 도청 의혹에 맞서는 과정에서 휴대폰 음성통화에 대한 도청 가능성을 계속 부인해 왔다. 이러한 규제의 공백을 틈타 민간 영역에서 불법 도청이 기승을 부렸다. 통신 이용자가 늘어나는 상황과 비례하여 이에 대한 불법 도청 사례가 증가하였으며, 특히 휴대폰 단말기의 고유번호를 복제하여 통화내용을 엿듣거나 문자메시지를 엿보고 위치를 추적하는 경우가 많았다.

휴대폰 불법복제를 이용한 범죄는 2000년대 초반부터 사회 문제로 대두되어 왔다. 2001년 6월에는 분실한 휴대폰을 수집하여 불법 복제 후 국내외에 팔아온 일당이 검거되었고 2002년 11월에는 대출을 미끼로 신용불량자 명의의 휴대폰을 구입한 뒤 불법 복제하여 시중에 팔아온 일당이 검거되었다. 2003년 2월에는 휴대폰 1천대를 복제하는 수법으로 '쌍둥이폰'을 만든 뒤 이 전화로 휴대폰 유료 위치추적 서비스인 '친구찾기' 서비스에 가입, 유흥업소에서 달아난 여종업원의 위치를 추적한 일당이 검거되는 등 휴대폰 복제 사건이 꼬리를 물었다.[14]

2004년 7월 굴지의 대기업 삼성에서 노동조합을 추진하던 노동자들과 산업재해를 당한 노동자의 가족 등이 본인 모르는 사이에 최소 3개월 이상 하루 30~40차례씩 휴대폰 위치추적을 당한 것으로 밝혀져 큰 충격을 주었다. 위치추적 피해자가 모두 삼성의 노조 설립과 직 · 간접으로 관련돼 있고 위치추적이 이뤄진 장소도 삼성SDI 공장이 있는 울산 · 수원이었지만 이들의 위치를 추적한 휴대폰은 사건 당시로부터 11개월 전 숨진 사람의 소유로 밝혀졌다. 불법 위치 추적을 당한 이들은 삼성 쪽이 불법복제 휴대폰을 이용해 위치 추적을 지시했다고 주장하면서 서울중앙지검에 고소장을 제출하였지만 2005년 2월 검찰은 '누군가' 고소인들의 휴대폰을 몰래 복제한 것은 사실이지만 전화를 불법복제한 '누

13 연합뉴스 2003.10.6; 한겨레 2004.1.30; 한겨레 2004.2.15; 한겨레 2004.2.17; 연합뉴스 2009.1.22.
14 국민일보 2001.6.26; 연합뉴스 2002.11.5; 한겨레 2003.9.25 참고.

군가’를 찾아내는 것이 현실적으로 불가능하다며 기소중지하였다.[15]

정보통신부 중앙전파관리소에 따르면 휴대폰 불법복제 적발 건수는 2004년 858건에서 계속 증가하여 2006년 1월에는 6천574건으로 7.7배 폭증하였다. 이것은 전파관리소가 2002년 사법경찰권을 부여받아 휴대폰 복제 단속에 나선 이래 최대 규모였다. 범죄 수단으로 악용된 휴대폰 복제는 2003년 14건에서 2006년 91건으로 급증했으며 특히 2006년 적발된 91건은 분실된 휴대폰을 자신의 휴대폰과 똑같이 복제하다가 적발된 사례였다. 불법도청설비 역시 2004년 2건에서 2005년 45건, 2006년 54건으로 증가추세를 보이고 있는 것으로 나타났다.[16]

문제가 심각해지자 정부는 2003년부터 휴대폰 동시수신 차단프로그램 운영, 통신비밀보호법 개정으로 휴대폰 단말기의 전자적 고유번호(ESN) 제공 금지, 휴대폰 인증서비스 도입, 단속강화 등의 방지대책을 시행하였다. 2005년 3월에는 신규 단말기에 휴대폰 인증서비스를 무료제공하고 통화도용방지시스템(FMS : Fraud Management System)을 도입하는 등 휴대폰 불법복제 방지 대책을 강화하면서 휴대폰 음성 통화에 대한 도청이 불가능해졌다고 장담하였다. 하지만, 2005년 7월 안기부 X-파일 사건이 공개되자 휴대폰 도감청에 대한 사회적 우려가 더욱 커졌고 정부는 2005년 8월에야 비로소 휴대폰 도감청이 기술적으로 가능하다는 점을 시인하면서 이에 대한 안전성 대책을 발표하였다. 새로운 암호 방식을 도입하고 착 · 발신 때도 인증서비스를 도입하는 한편 단속을 강화하겠다는 내용이었다. 이후 정보통신부와 이동통신사들은 2007년 1월 ‘Private Long Code’를 이용하여 휴대폰 통화내용을 암호화하는 유료서비스를 개시하였고 착 · 발신 인증서비스를 도입하여 이통사의 네트워크 인증 값과 휴대폰에 부여된 인증번호가 불일치할 경우 통화가 자동으로 차단되도록 하였다.[17]

또한 정부는 2006년 3월부터 ‘휴대폰 불법복제신고센터’를 가동, 포상금을 지급하는 일명 ‘폰파라치’ 제도를 운영하였다. 2006년 6월 집계된 바로는 3개월간 1,500대의 불법복제사례가 적발되었고 신고자 15명에게 1,120만 원이 지급되었다. 중앙전파관리소는 “휴대폰 불법복제 하지 맙시다”라며 가두캠페인을 벌이기도 하였다.[18]

그럼에도 불구하고 2009년 1월에는 유명 탤런트 전지현 씨의 휴대폰을 복제해 문자메시지 등을 훔쳐본 심부름센터 직원 등 3명이 경찰에게 붙잡혀 또다시 큰 충격을 주었다. 계약 만료를 앞둔 전씨의 소속사가 동향을 파악하고자 전씨의 휴대폰 복제를 의뢰한 혐의를 받고 있다. 이 논란 후 국회는 이동

15 한겨레 2004.7.11; 한겨레 2004.7.14; 한겨레 2004.7.22; 연합뉴스 2005.2.16; 한겨레 2005.2.16 참고.
16 연합뉴스 2006.1.16; 아이뉴스24 2007.4.30 참고.
17 정보통신부 보도자료 2005.2.16; 세계일보 2005.8.16; 연합뉴스 2006.10.19; 연합뉴스 2007.1.23; 쿠키뉴스 2007.1.15 참고.
18 연합뉴스 2006.3.16; 한국일보 2006.6.8; 정보통신부 보도자료 2006.6.12; 아이뉴스24 2007.4.30 참고.

통신사가 복제로 의심되는 휴대폰 전화번호를 검출했을 때 방송통신위원회에 신고토록 의무화하는 내용으로 전기통신기본법을 개정하는 것을 검토하고 있다.[19]

Ⅳ. 통신비밀보호법

1. 제정

대한민국 헌법 제18조에는 “모든 국민은 통신의 비밀을 침해받지 아니한다.”라고 하였다. 군사정부 시절 반인권적인 감시와 도청을 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 않고는 우편물의 검열 또는 전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 않은 타인간의 대화를 녹음 또는 청취하지 못하도록 규정하고 있다(제3조). 또, 검사, 사법경찰관 또는 정보수사기관의 장이 범죄수사나 국가안보를 위하여 우편물의 검열이나 전기통신의 감청을 하는 경우 또는 공개되지 않은 타인간의 대화를 녹음 · 청취함에 있어서 법에서 정한 요건을 모두 갖춘 경우에만 한하며, 법에 따른 허가를 받거나 승인을 얻어 감청을 하거나 대화를 녹음 · 청취한 경우에도 이를 계속할 필요성이 없다고 판단되는 경우에는 즉시 이를 중단함으로써 국민의 통신비밀에 대한 침해가 최소한에 그치도록 하였다(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, 휴대폰과 개인휴대통신도 당연히 전기통신에 해당한다. 이메일을 포함한 컴퓨터 통신상의 자료 및 정보의 전송도 전기통신에 해당한다. 한편, 통화내역이나 로그기록과 같은 통신사실확인자료의 경우 원래는 통신비밀보호법상에 관련 규정이 없고 전기통신사업법에 근거규정이 있었으나 차츰 그 중요성이 인식되면서 통신비밀보호법의 보호 범위 안으로 편입되었다.

---

19 한겨레 2009.1.19; 연합뉴스 2009.2.9 참고.

2005년에는 수사기관이 통신회사에 통신사실확인자료를 요청할 때 법원의 허가를 받도록 개정되었다.

감청의 허가요건으로 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 있도록 하였다(제5조). 다만, 제정 당시 감청의 대상 범죄를 형법상 내란, 외환, 국교, 약취와 유인에 관한 죄, 군형법, 국가보안법, 군사기밀보호법상의 범죄 등 10개 법률 300종류가 넘을 만큼 매우 광범위하게 설정하여 남용 소지가 있었다.

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

일반 범죄 수사를 위하여 검사가 법원에 대하여 감청 허가를 청구할 때는 기간은 3개월을 초과하지 못하며 다시 3개월까지 연장이 가능하도록 제정하였다. 긴급한 사유가 있을 경우에는 법원의 허가 없이 감청할 수 있으나 그로부터 48시간 이내에 법원으로부터 허가를 받도록 제정되었다. 이 조항은 사실상 수사기관이나 정보수사기관이 영장 없이 통화내용을 감청했다가 사후 영장을 신청하지 않고 슬그머니 감청을 중단하는 용도로 악용되어 왔다.

또한 감청의 허가결정이 일단 내려지면 계속 연장에 대한 결정이 내려질 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 법에 의하지 않고서는 수사기관이나 정보기관이 감청할 수 없도록 규정하였으나, 수사기관과 정보기관의 감청은 계속 증가해 왔으며 정치적 목적의 감청도 이루어져 왔다.

2. 개정

김대중 정부 들어서서 야당과 시민사회단체에 의해 불법 도청에 대한 의혹이 꾸준히 제기되어 2001년 12월 통신비밀보호법이 대대적으로 개정되었다. 이때 감청의 대상 범죄를 당초 390개에서 280개로

축소하였고, 감청 기간이 일반 범죄수사 목적은 3개월에서 2개월로, 국가안보 목적은 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 연 2회 감청현황을 보고하도록 하였다. 감청설비 도입시 정보수사기관은 정보통신부에, 국정원은 국회 정보위원회에 신고하도록 하였다.

그 이후에도 통신비밀보호법은 몇 차례 주요 개정 절차를 거쳤는데 그에 대한 요약은 다음과 같다.

표 6: 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 청구대상의 한정 통신제한조치 기간축소 긴급통신제한조치 절차강화 피감청자에 통지제도 신설 통신사실확인자료 제공절차 규정 감청설비의 신고	1998년부터 불법감청과 남용에 대하여 국회에서 지속적인 문제제기 1999년부터 휴대폰 도청 의혹 제기
제8차 개정	2004.1.29	단말기 고유번호제공 금지 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 IP 주소 등 새로운 통신 영역에 관한 감청 규정이 계속 추가되면서 사실상 감청은 더욱 확대되었다. 특히 안기부 X-파일 사건에서 볼 수 있다시피 통신비밀보호법은 정보수사기관의 비밀스런 불법 감청을 통제하는 데 사실상 무력하였다. 이는 통신비밀보호법에서 해결될 수 있는 문제가 아니라 정보수사기관의 비밀 권력에 대한 민주적 통제에 관한 문제인 것이다.

3. 2007년 이후 개정안 논란

(1) 법률적 쟁점

국정원은 도청 장비가 폐기된 후 휴대폰 감청이 불가능하여 범죄수사에 제약이 많다고 계속 주장해 왔다. 마침내 2007년 제17대 국회 법제사법위원회는 이 요구에 부응하는 통신비밀보호법 개정안을 심사하여 통과시켰다. 개정안에 대한 인권단체들의 반대운동이 활발하게 일었으며, 국회 본회의에서 이에 반대하는 의원들의 수정안이 발의되면서 법제사법위원회의 개정안은 논란 속에 통과되지 못하다가 2008년 4월 총선 후 17대 국회가 종료되면서 자동폐기되었다.

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 제5조 제1항), 감청에 협조토록 하기 위하여 전기통신사업자에게 감청 장비를 구비할 의무를 신설하고 이를 위반할 경우 10억 원 이하의 이행강제금을 부과하였다(안 제15조의2, 제17조 제1항 제7호, 부칙 제4조 및 제15조의3 신설). 둘째, 통신사실확인자료에 GPS 위치정보를 추가하고(안 제2조 제11호 아목 신설) 통신사실확인자료를 보관하지 아니하는 자는 3천만 원의 과태료에 처하도록 하였다(안 제20조 제1항 제2조).

이 법안의 가장 큰 문제점은 수사기관의 편의를 위하여 제삼자인 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 의무화한 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 정보뿐 아니라 통신 내용에 대한 정보도 포함할 수 있는데 법령에서는 이를 세부적으로 다루지 않았다. 예를 들어 이용자가 저작권을 침해하는 파일을 업로드하거나 다운로드한 기록이 수사기관에 필요하다는 이유로 추후 시행령 차원에서 파일 업로드와 다운로드에 대한 로그기록을 모두 보관토록 강제할 수도 있다. 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 통신 비밀에 중대한 영향을 끼친다. 첫째, 통신사업자가 보유한 장비를 통해서 누군가 마음만 먹으면 언제든지 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 시행한다는 것은 휴대폰은 물론 인터넷 전화, 화상 전화, 인터넷 메신저, 인터넷 채팅 등 사실상 모든 통신수단에 대한 감청이 개시된다는 말이다. 이처럼 현존하는 통신수단뿐 아니라 미래의 모든 통신수단에 대한 감청이 시행되는데, 이는 단순히 기술적인 차원의 장비 구비 문제를 넘어서는 중대한 인권 문제이다. 휴대폰은 휴대폰대로, 인터넷이면 인터넷대로 그 기술이 가진 특성이 개인의 프라이버시권과 통신의 비밀에 미칠 영향이 매우 신중하게 검토되어야 한다. 하지만, 이번 개정안은 새로운 기술에 대한 감청 개시의 문제를, 국민의 인권 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 크다.

근본적인 문제는 현행 통신비밀보호법에 많은 문제점이 있다는 사실이다. 감청대상이 여전히 매우 광범위하며, 긴급 감청과 긴급 통신사실확인자료 제공이 오남용 되고 있다. 법원의 통제가 사실상 제대로 이루어지지 못하여 통신감청 영장 청구에 대한 법원의 기각률은 3.6%(2007년)에 그치고 있으며 통신사실확인자료에 대한 청구 기각률은 0.9%(2007년)에 그치고 있다.[20] 정보수사기관의 권한은 예외적으로 인정되어 왔기 때문에 통신비밀보호법은 이들에 의한 불법 감청을 방조해 왔다. 현행 통신비밀보호법은 사실상 헌법상 기본권인 통신 비밀을 보호하겠다는 법 제정 취지에 크게 미치지 못하다.

특히 이번 개정안은 사실상 국정원과 법무부가 주도하면서도 의원을 통하여 발의되었다는 이유로 공청회 등에서 국민적으로 토론하고 여론의 검증을 받을 기회가 사실상 봉쇄되었다는 점에서 큰 비판을 받고 있다.

(2) 기술적 쟁점

위에서 언급한 이한성 의원안에서 어떤 기술적인 표준이 마련될지는 구체적으로 알 수가 없다. 이

20 토론회 〈수사·정보기관의 통신감청, 국민은 안전한가?〉, 이춘석 의원실 주관, 2008.12.11.

개정안에서는 기술적인 세부 사항이 전부 대통령령으로 정하도록 하고 있다. 통신제한조치 집행에 필요한 장비 · 시설 · 기술 및 기능이 지켜야 할 기준 · 방법 및 절차는 대통령령으로 정하도록 하고 있으며(제15조의2 제3항), 통신제한조치 집행에 필요한 "장비 등을 운용함에 있어 권한 없는 자의 접근 방지, 접근 기록의 관리 등"은 "대통령령으로 정하는 바에 따른 보호조치를" 취하는 것으로 하고 있다(제15조의2 제5항).

따라서 이 개정안만을 놓고 기술적인 분석을 할 수 없다. 그러나 각종 토론회에서의 발언이나 언론 보도 등에 따르면 정부는 유럽 전기 통신 표준 협회(European Telecommunications Standards Institute; ETSI)의 합법 감청(lawful interception) 표준과 같은 해외의 사례를 미래 감청 시스템으로 생각하고 있다고 보여진다.[21]

이 절에서는 간략하게 ETSI의 감청 표준 모델의 구성을 살펴보고, ETSI가 자신들의 보고서[22]에서 지적한 몇 가지 기술적 우려점을 정리하도록 한다.

가) ETSI 전기통신 합법 감청 모델

이 모델에서 핵심적인 아이디어는 데이타 – 크게 감청 관련 정보(Intercept Related Information; IRI)와 통신 내용(Content of Communication; CC)로 나뉘는 – 의 수집 기능을 사법집행기관(Law Enforcement Agency; LEA)에서 분리한 것이다.

데이타의 수집 기능은 공중에게 통신 서비스를 제공하는 망운영자(NetWork Operator; now), 서비스제공자(Service Provider; SvP) 그리고 접속제공자(Access Provider; AP)가 수행을 하게 된다. 사법집행기관은 통신사업자들이 수집한 감청 데이타를 전달받을 사법집행감시시설(Law Enforcement Monitoring Facility; LEMF)을 구축하게 된다. 이 모델에서는 정보 수집이 일어나는 통신망(또는 서비스)과 사법집행감시시설 사이의 망간의 연결을 어떻게 할 것인지를 규정하는 것이 중요하다. 이러한 망 간의 연결을 표준화하는 데는 감청과 관련된 기능을 망에 구축하는 것과 이렇게 구축된 감청 기능을 통제하고 감청 결과를 전달하는 인계 인터페이스(handover interface)를 표준화하는 것이 필요하다.

---

21 위 토론회 및 토론회 〈사이버 인권법 제정을 위한 국회 토론회〉, 전병헌 의원실 주관, 2008.12.3. 의 강신각(ETRI) 토론문 참고.

22 ETSI (2006). "Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture" (ESTI TR 101 943 v 2.2.1).

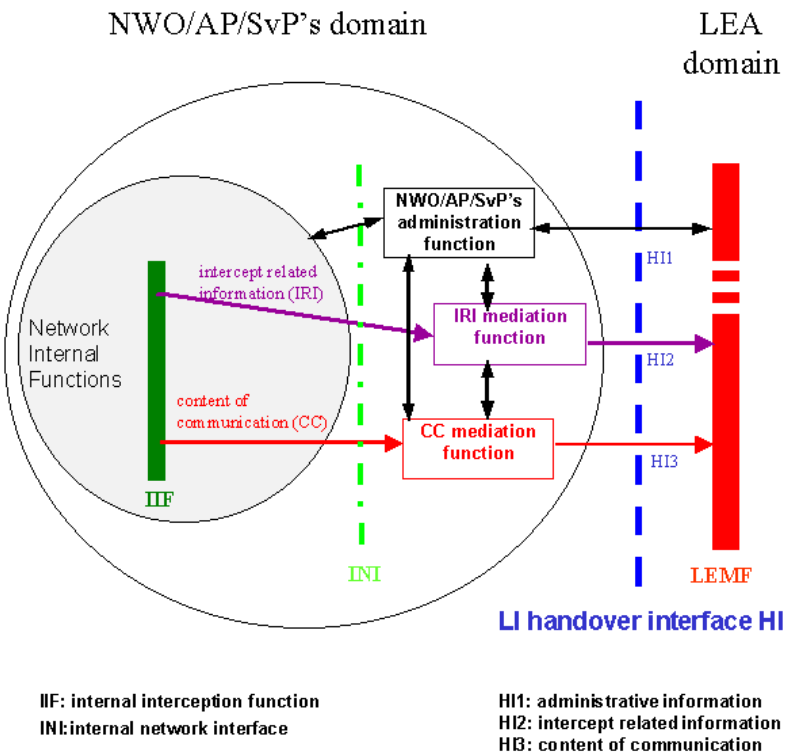

그림 12: ETSI 인계 인터페이스 (handover interface)를 보여주는 블록 다이어그램
(출처: ETSI, "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic", ETSI TS 101 671 V3.4.1, p.20.)

그림 12에서 보여진 것과 같이 LEMF와 통신망의 상호 접속이 가능하기 위해서는 통신서비스 제공자는 매개 기능(mediation function)과 운영 기능(administration function)을 기존의 통신망에 구현하여야 한다. 통신망사업자, 통신망의 종류, 서비스 종류 등에 따라 개별 통신망의 장비와 이 장비들이 감청에 제공하는 기능은 다양할 수 있으나, 이러한 개별 장비들의 차이를 사법집행기관이 고려할 수는 없으므로 표준화된 매개 기능과 운영 기능으로 개별 다양한 장비들을 제어하고 데이타를 수집하여 제공하는 방식을 취하게 된다. 운영 기능은 감청의 대상자, 감청의 기간, 감청 대상 정보, 감청 결과의 전송 목적지 등을 H1 인계 인터페이스(handover interface)를 이용해서 주고받음으로써 감청 과정을 통제하게 되고, 매개 기능은 H2 인계 인터페이스를 이용해서 감청 관련 정보(대상자 신원, 실패한 통화 시도 등 통화 관련 정보, 가입자 서비스 프로파일과 같은 서비스 관계된 정보, 위치 정보 등)를, H3 인계 인터페이스를 통해 통신 내용을 표준화된 데이타 포맷과 전송 기술로 사법집행감시설비로 전달하게 된다.

나) ETSI 전기통신 감청 모델과 우려점

전기통신사업자의 일차적 의무는 사용자들에게 통신을 원활하게 값싸게 제공하는 것이다. 그러나 ETSI 감청 모델과 같은 표준이 통신사업자에게 의무화되는 과정에서 이러한 통신사업자들에게 비용의 증가나 통신 성능의 저하와 같은 문제가 발생할 수 있다. 이는 단순히 감청의 빈도수만이 문제가 아니라 사법집행기관이 원하는 감청 결과의 형식, 암호화 방식 또는 전송 기술 등의 요구 사항에 따라 다양한 결과를 낳을 수 있다.

감청설비가 의무적으로 설치된 상황에서 통신사업자 측의 시설 또는 사법집행감시설비에 전송 또는 축적되는 감청 결과 및 로그 등의 유출 위험성이 상존하며, 이 양측의 한 시설에서 이렇게 설치된 감청설비가 정당한 권한 없는 자에 의해 사용될 가능성도 존재한다. 정보의 전송과 보존에 암호화 기법을 적용하고 감청설비에 대한 물리적 접근(장비 자체나 장비가 있는 건물 등에 대한 접근)이나 장비를 이용하는 데 엄격한 인증과 승인 절차를 두는 것과 같이 논리적 접근을 제한하는 조치 등을 생각할 수 있으나, 이러한 보안 조치들에 대한 우회 방법들이 개발되는 것도 항상 염두에 두어야 한다. 또한, 내부자에 의한 감청 장비의 오용과 감청 결과의 유출 등은 이러한 조치들로 막기 어렵다.

V. 결론

첫째, 정치적 측면에서 한국 정부의 도감청 경향을 평가하여 보면, 범죄 수사보다는 정치적 목적에 의하여 불법적인 감청이 시행되어 왔으며 이를 주도한 것이 안기부나 국정원 같은 정보수사기관의 비밀 권력이었다는 점을 알 수 있다. 현행 통신비밀보호법에는 “다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여” 감청을 허가한다고 명시되어 있다(제5조). 그러나 2005년 드러난 안기부의 불법 도감청 사건 당시 정보수사기관은 감청을 ‘최종적 수단’이 아닌 최초의 수단으로 선택할 수 있는 특권으로 인식했던 것으로 드러났다. 정보수사기관의 정보독점과 이를 이용하려는 권력집단의 정치적 이해관계가 도감청을 조장하면서 국민의 통신 비밀과 기본권을 소홀히 취급하였던 것이다.

둘째, 통신사업자는 불법 도청 과정에서 협조자로 동원되었다. 통신회사는 불법임을 인지하더라도 협조를 거부할 경우 신분상 불이익이 가해질지 모른다는 우려 때문에 이를 거부하기 어려운 입장이다. 수사기관과 통신사업자 간의 권력관계를 상기하여 보았을 때, 앞으로도 통신사업자가 불법 도청을 거부하거나 고발할 가능성은 매우 희박하다. 과거 감사원이 지적하였다시피 통신사업자가 불법적인 도청의 협조자 노릇을 하도록 강제될 위험이 상존하는 것이다.

셋째, 기술적 측면에서 통신 기술의 보급이 확대되고 통신 이용자가 늘어나는 것과 비례하여 수사기관의 도감청 또한 확대되어 왔다. 1970년대 말부터 1980년대 초반까지 한국의 정보화 수준은 매우 낮은 편으로서 1973년 전화가입자가 76만 명에 불과하였다. 따라서 과거 군사정권은 주로 미행과 신체적 감시를 통하여 정부에 비판적인 세력을 밀착 감시하였으며 전화 도청 역시 특정 소수층을 상대로 시도되었다. 그러나 1979년 이후 전화의 적체를 해소하기 위하여 정보통신에 대한 투자가 확대되자 1987년 전화가입자가 1,000만 회선을 넘기는 등 대중화하였고 휴대폰이나 인터넷의 보급이 늘어났다. 이에 부응하여 통신 감청이나 통신 자료를 수사기법에 활용하는 경우가 크게 증가하였으며 감청 대상도 크게 늘었다. 그 과정에서 수사기관이 통신 자료를 불법적으로 취득하거나 오남용하는 사례가 계속 논란을 빚어 왔으며, 국가기관이 불법적으로 최첨단 감청 기술을 수입하거나 직접 개발하여 감청하는 사례도 발생하였다.

넷째, 제도적 측면에서 불법적인 도청을 막기 위하여 통신비밀보호법이 제정되었고 불법 도청을 둘러싼 여러 논란 속에서 일정하게 개선되어 왔다. 그러나 안기부 X-파일 사건에서 드러난 것처럼 정보수사기관 등 권력 내부에서 은밀히 벌어지는 도감청을 규제하는 데는 현행 통신비밀보호법만으로 역부족이었다.

마지막으로, 민간의 불법 도청 역시 증가해 왔다. 통신비밀보호법상의 여러 규제 속에서도 정보수사기관의 불법 도청이 계속되는 가운데 정부는 휴대폰 음성통화에 대한 도청의 기술적 가능성을 계속 부인해 왔다. 이러한 규제의 공백을 틈타 휴대폰 복제를 이용한 불법 도청이 민간 영역에서 기승을 부렸다.

일반적으로 정보화는 감시권력의 범위와 능력을 신장시킨다고 할 수 있다. 정보화가 진전될수록 권력의 감시 방식은 비인격적이고 전자적인 데이타 감시로 이동하며, 유선전화, 이동전화, 인터넷 등 모든 통신수단을 아우르는 통합감시가 가능해진다. 이는 미행이나 신체적 감시에 따른 피감시자의 저항과 노출 위험으로부터 자유롭게, 보다 광범위한 사람들에 대한 보다 광범위한 정보를 보다 은밀하게 수집하는 것이 가능해졌다는 의미이다. 정보화가 고도화할수록 생활의 많은 부분을 통신수단에 의존하게 되는 만큼, 눈에 보이지 않아도 정보 감시의 영향력은 점차 커지고 있다. 특히 통제되지 않는 감시 권력의 비대화는 수집된 정보를 권력의 토대로 국가 권력을 남용하고 사회적 차별과 불이익 등 인권침해로 이어질 가능성이 크다. 따라서 정보화가 확산될수록 정보 인권을 보호하기 위한 시민사회의 문제의식을 더욱 고취하는 한편, 통신비밀보호법 등 관련 법률을 법 제정 취지에 부합하게 개선 · 운영하여 합법적인 감청에 대한 사회적 감시의 사각지대나 불투명한 부분을 일소해야 할 것이다.