사이버안보연구, 2집 2호 2025 겨울, 139-171

통신정보 활동의 변천과 디지털 시대의 도전 과제 연구

유상선 | 고려대학교 정보보호대학원 겸임교수

논문접수일 2025년 9월 28일 | 논문심사일 2025년 12월 1일 | 게재확정일 2025년 12월 8일

논문 요약

통신정보는 국가안보와 군사 작전에서 중요한 역할을 하는 정보 수집 방식 중 하나이다. 이는 통신 수단을 활용하여 적국의 의도를 파악하거나 전술적 우위를 확보하는 데 활용되는 정보를 말한다. 또한, 더 넓게는 수사 과정에서 범죄의 실체적 증거를 획득하기 위해 적법 절차에 따라 수집한 특정 혐의자의 통신 내용을 비롯한 관련 정보를 포함한다.

통신정보 활동은 디지털 시대의 도래와 함께 통신서비스가 개방, 공유, 보안, 암호 등의 복합적인 속성으로 말미암아 통신 이용자의 태도와 사회 문화적 요구에 따라 크게 변하고 있다. 이러한 현상은 통신정보의 수집이나 획득 측면에서 전통적 방식과 기법만으로 대응이 곤란하여 큰 도전 과제로 작용하고 있다. 통신정보 활동을 국가안보와 범죄 수사 측면에서 정상적으로 수행하기 위해서는 무엇보다 법 제도적 안정성을 확보하는 일이 중요하다.

법치 국가 미국의 경우, 통신정보 활동은 1990년대 디지털 시대 전환 과정에서 CALEA를 마련하고, 9.11테러 직후 애국법 제정에 이어, 에드워드 스노든의 NSA 기밀 폭로 이후 자유법을 제정하면서 국가안보와 프라이버시 모두 균형 발전 과정을 거쳤다. 반면, 우리의 통신비밀보호법은 아날로그 통신 시대의 산물로서 범죄의 수사 측면에서 최소한의 보충적 기능조차 못하는 실정이다.

이에 통신정보의 정의와 유형을 검토하고, 통신정보 활동의 역사적 변천 과정을 조사해 디지털 통신 환경에서 통신정보의 한계와 도전 과제를 탐구하였다. 결론은 통신정보 활동의 법적 안정성을 확보하기 위한 정치·사회·안보적 딜레마 해소, 시민 안심과 국민 신뢰 회복, 법령의 구조 개선, 국제 감청 기술 표준 도입 등이 중요하다. 이를 위해 관계 당국의 정책 연구과제 위탁 및 학술 연구 지원을 점차 확대해 나가는 것이 필요하다.

주제어 통신정보, 통신비밀보호법, 애국법, 자유법, 국가안보, 범죄수사, 감청기술표준

Ⅰ. 서론

1980년대 이후 디지털 기술의 비약적인 발전으로 사회 안전에 관한 제도적 요구와 함께 인권과 자유의 성장이 동반하면서 통신정보 활동의 양상도 변화를 요구하고 있다.

통신정보(Communication Intelligence, COMINT)는 국가안보와 군사작전에서 중요한 역할을 하는 정보 수집 방식 중 하나이다. 이는 주로 무선 및 유선 통신을 대상으로 하며, 적국의 의도를 파악하거나 전술적 우위를 확보하는 데 활용된다. 또한, 더 넓게는 법률적으로 범죄의 수사 과정에 허가받은 특정 혐의자의 통신 내용도 포함되는데 이는 범죄의 실체적인 증거를 분석하기 위해 활용된다. 통신정보 활동은 시대와 기술의 발전에 따라 법률과 제도를 바꾸며 점차 변화해 왔는데, 특히 디지털 시대의 도래와 함께 통신서비스가 개방, 공유, 보안, 암호 등의 복합적 속성으로 발전하게 되어 통신 이용자의 태도와 사회 문화적 요구도 크게 변하여 왔다. 이러한 현상은 통신정보의 수집이나 획득 측면에서 전통적 방식과 기법만으로 대응이 곤란하여 통신정보 활동에 새로운 도전과제로 대두하고 있다. 그래서 통신정보 활동은 국가안보와 범죄 수사 측면에서 정상적으로 수행되도록 법제도적 안정성을 확보하는 일이 매우 중요하다.

본 연구의 목적은 디지털 시대 국가의 안전과 국민 생명을 보호하는 데 필수 요소인 통신정보 활동의 보장 방안을 연구하기 위하여 현실적인 통신정보 활동의 도전과제를 발굴하고 제안하는 것이다. 현행 통신비밀보호법은 국민의 통신 자유와 통신비밀 보호의 헌법적 가치를 보장하면서 범죄 행위나 국가안보를 위협하는 통신에 대하여 최소한의 보충적인 수단으로 감청을 허용하고 있다. 그러나 현실은

범죄자 통신의 대부분을 차지하는 휴대폰 통신에 대한 감청[1]은 불가능하다고 알려져 있다. 이는 수사와 정보 활동에 있어 통신정보의 중요한 기능을 상실한 것으로서 국민 보호와 범죄 수사 및 국가안보의 목적으로 그 고유 기능을 구현하는 연구가 필요할 것이다.

본 연구는 저자가 26년 이상 통신정보 활동 분야의 직무 경험과 퇴임 이후 수년간 미국의 전기통신 감청정책과 통제의 효과성에 관한 연구의 바탕에서 기초한다. 통신정보 활동의 기능이 국가안보와 프라이버시 간의 Trade-off로 작용한다고 볼 때, 국가안보 차원의 감청 집행 문제와 프라이버시와 개인정보보호 차원의 감청 통제를 균형적으로 다뤄야 할 것이다. 그럼에 불구하고 그동안 국내 감청 관련 학술 연구가 감청 규제 위주로 전개되어 우리나라 감청 정책의 현실을 제대로 반영하지 못하는 문제가 있는 것으로 분석된다.

따라서 연구의 범위는 미국의 감청 정책 및 통제의 발전 과정과 국내 감청 법제의 현실에 초점을 맞추어 우리나라 통신정보 활동의 구조적인 문제와 현실적 어려움이 무엇인지 연구 제시할 것이다. 다만, 연구의 방향이 범죄 수사와 국가안보 감청 문제에만 국한하여 논증이 편향되었다는 비판 가능성을 우려하여 프라이버시와 개인정보보호 차원의 헌법적 가치를 훼손하지 않도록 감청 통제 장치의 중요성에 특별히 유의할 것이다. 또 통신정보 활동의 고유한 기능을 구현하기 위하여 감청 관련 정치, 사회, 시민 의식, 법 구조, 기술, 정책 등 다양한 언어와 요소에 대한 실질적 상태를 분석할 것이다.

1) "감청"은 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것으로 기지국의 위치추적과 같은 "통신사실확인자료 수집"과는 구별되는 것임

이에 통신정보의 정의와 유형을 검토한 후, 통신정보 활동의 역사적인 변천 과정을 고찰하고, 디지털 통신 환경에서 통신정보의 한계와 도전과제를 연구하고자 한다.

Ⅱ. 통신정보의 정의 및 활동 유형

1. 통신정보(COMINT)의 정의[2)]

통신정보(COMINT)는 신호정보(SIGINT, Signals Intelligence)의 한 유형으로, 무선, 유선, 위성, 인터넷 등을 통해 송수신되는 통신 신호를 분석하여 정보를 획득하는 활동을 의미한다. 주로 군사, 외교, 정보기관 등에서 활용되며, 대상의 의도를 파악하거나 전략적 판단을 위한 기초 자료로 사용된다. 또한, 정보 수사기관에서 국가안보 목적으로 정보를 수집하거나 범죄 수사의 목적으로 실체적인 증거를 수집하기 위해 특정 혐의자에 대한 통화 사실 조회나 통신 내용을 수집하는데 이것도 통신정보의 범주에 해당한다고 볼 수 있다.[3)]

2) 국가정보학; 전웅, 2015:104

3) 통신비밀보호법 제5조(범죄 수사), 제7조(국가안보), 제13조(통신사실확인자료) 규정에 근거

2. 통신정보 활동의 유형과 근거

통신정보의 활동 목적은 먼저 상대국의 군사, 외교 및 정치적 의도를 파악하고, 전쟁 및 위기 상황에서 적의 명령 체계를 분석할 뿐만 아니라 전략을 예측하기 위해 다양한 통신을 실시간 감청하여 정보를 획득하는 일이다. 이를 통해 국가안보를 위협하는 여러 가지 요소를 조기에 탐지하여 다양한 첩보와 보안 정보를 가지고 국익 정보를 생산한다. 한편, 범죄 수사를 위한 통신정보 활동은 혐의자의 통신 내용을 수집하기 위해 적법한 절차를 통하여 감청 허가를 신청하고 허가된 감청을 효과적으로 집행하여 범죄 증거를 확보한다. 오늘날 통신정보 활동은 통신환경 변화와 프라이버시 보호의 요구가 커져 사회적 합의와 법률 체계를 수립하는 데 현실적인 어려움이 많다.

통신정보 활동은 수집 방식과 목적에 따라 분류할 수 있는데, 먼저 무선통신 감청은 상대국의 무선 송수신 신호를 수집하여 첩보를 처리하는 방식으로서 인공위성을 통해 송수신되는 위성통신이나 마이크로웨이브와 같은 무선 구간에서 데이터를 가로채 분석하는 통신정보 활동이다. 둘째, 유선 통신 감청은 구리나 광케이블과 같은 유선 네트워크를 통해 송수신되는 신호를 가로채기하는 방식으로서 통신업체 내부의 통신 선로나 해저광케이블을 분기하여 첩보를 처리하는 통신정보 활동이다. 셋째, 인터넷과 데이터 통신 감청은 이메일, 메시지, 인터넷 통신 등을 네트워크에서 다양한 방식으로 접속하여 정보를 획득하는 방식이다. 이상은 통신 수집 수단에 따른 분류이다. 넷째, 암호 해독 및 분석으로서 암호화된 통신을 분석하고 해독하거나 전자파를 이용하여 적의 통신을 교란하거나 차단하는 작전과 연계된 전자전 정보 활동도 목적 지향적인 통신정보 활동의 범주에 포함할

수 있다.

통신정보 활동은 「통신비밀보호법」의 제5조(범죄 수사), 제7조(국가안보)에 규정된 통신제한조치의 이름으로 직접 규정하고 있다. 동 법 제3조(통신 및 대화 비밀의 보호)에서 통신정보 활동은 범죄 수사 또는 국가안전보장을 위하여 보충적 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다고 명시되어 비례 원칙을 요구하고 있다. 또 통신정보 활동의 과정에서 법원의 사전·사후 통제를 통하여 명확성을 유지하고 국회의 상임위원회와 국정감사 위원회에서 특정한 통신제한조치에 대하여 관련 기관장의 보고를 요구할 수 있는 엄격한 통제와 감독이 이뤄지고 있다.

Ⅲ. 통신정보의 활동의 변천

한 국가의 통신정보 활동은 기술의 발달과 정치, 사회, 문화 발전과 함께 계속 진화한다. 본 장에서는 세계사 관점에서 군사 안보 목적 통신정보 활동의 변천사를 대략 살펴본 후, 범죄 수사 목적의 통신정보 활동을 중점적으로 고찰하겠다. 그런데 현실적으로 통신정보 활동에 관한 학술 연구는 그리 흔하지 않다. 국내 학술 연구에서도 일부 있긴 하지만 프라이버시 및 개인정보보호 입장에서 통신정보 활동의 위험과 남용에 관한 비판적 연구가 대부분이고, 국가안보와 범죄 수사기관 입장에서 통신정보 활동에 관한 헌법적 가치와 정책에 관한 체계적인 연구 없이 국책 연구소에서 감청 제도의 필요성과 감청 기술 국제표준을 소개하는 정도였으나, 지금은 연구 자체가 극히 드문 것으로 보인다. 이에 법치 국가의 상징인 미국의 1930년대 이후 아날로그

시대부터 1990년대 이후 디지털 시대의 전환 과정에서 법과 기술 관점에서 통신정보 활동의 변천사를 검토하는 것이 유의미할 것이다. 나아가 우리나라 통신정보 활동의 변천사는 통신비밀보호법의 운영 실태와 쟁점을 중심으로 살펴볼 것이다.

1. 세계적 군사 안보 통신정보 활동

제1차 및 2차 세계대전 시기에는 군사 분야 무선통신의 발전으로 전파 가로채기 형식의 감청 기술이 발전했다. 영국은 독일 암호체계 '에니그마' 해독에 성공했으며, 이는 전쟁의 판도를 바꿨다. 이때는 주로 모스 부호 감청과 암호 해독이 통신정보의 핵심이었다. 또 동서 냉전기인 1947~1990년경에는 미국과 소련 사이 첩보전이 치열하게 전개되었다. 미국의 NSA와 소련의 KGB는 위성 감청, 심해 케이블 감청, 무선 감청 등의 다양한 기법을 활용하여 통신 첩보를 수집했다. 특히, 1960년대 이후 등장한 인공위성을 이용한 감청 기술이 주요한 정보 수단으로 발전했다. 1990년대 이후부터 인터넷과 디지털 통신이 보편화하면서, 전통적 무선 유선 감청을 넘어 데이터 트래픽 분석, 이메일 감청, 해킹을 통한 정보 수집이 부상하였다. 미국의 에셜론 시스템은 전 세계의 전자 통신을 감시하는 대표적인 시스템으로 알려져 있다. 2013년 에드워드 스노든의 NSA 기밀폭로에서 정보동맹 5-eyes와 프리즘 프로그램[4]의 통신정보 활동이 드러났다. 오늘날에

4) NSA가 2007년 통신정보 활동 목적으로 해외정보감시법에 따라 운영했던 데이터 마이닝 프로그램

는 인공지능과 빅데이터 분석의 통신정보 활동이 이루어지고 있다. 또 사이버 공간이 새로운 전장으로 부각 되고 세계적으로 테러리스트와 극단주의자들이 다크웹이나 암호화 보안 기술 활용이 늘고 있다. 한편, 자유민주 법치국에서는 국내적으로 시민의 프라이버시 보호 요구[5]가 커지고, 국제적으로 데이터 보호 및 첨단 정보통신과 암호화 서비스의 고도화가 진행되면서 국가안보와 프라이버시에 관한 가치의 충돌 문제로 통신정보 활동에 어려움이 가중되고 있다.[6][7]

2. 미국 통신정보 활동의 변천

1) 아날로그 시대(1930~1980년대)

기술적 발전 측면에서 보면, 1930년대부터 전화와 라디오 방송이 보편화하였으며, 이후 유선 전화와 팩스, 아날로그 무선 통신망이 발전했다. 1960~70년대에는 위성통신이 등장하여 국제 통신이 가능하였다. 이때는 공중전화망(PSTN) 기반의 아날로그 통신 감청 기술도 더불어 발전했다. 통신정보 활동에 관한 정책과 제도가 정착되기 전

5) 2018 EU General Data Protection Regulation, 2020 미국 California Consumer Privacy Act, 2023 한국 개인정보 보호법 시행

6) Going Dark: https://www.fbi.gov/news/stories/senate-committees-briefed-on-going-dark-impact
(검색일: 2025.12.4.)

7) 기술 중심 사회에서 민간 산업이 첨단통신 방식에 적응해 온 것처럼 테러리스트들도 동일한 방식으로 적응해 이들의 통신 방식과 능력이 수사관에게 통신 내용의 합법적 감청을 허용하도록 설계된 법률과 기술을 빠르게 앞지르고 있음: https://www.fbi.gov/news/speeches-and-testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark (검색일: 2025.12.4.)

에는 기술적으로 통신선에서 실시간 대화 내용을 녹음하는 방식으로 수정헌법 4조[8]에 위반하지 않는 범위에서 범죄 수사에 활용했던 사례가 많았다.

아날로그 시대의 초창기는 전화기술의 발달 이면에서 범죄자의 도청과 수사관의 감청 남용이 혼재하던 때이다. 1928년 밀주 범죄 Olmstead 사건[9] 이후, 1934년에 연방 통신법(Federal Communications Act)을 제정하여 FCC가 통신을 규제하도록 하였다. 이때 후버 FBI 국장이 플라이 FCC 위원장에게 국제전화에 대한 감청을 요청했지만, 플라이 위원장이 반대하였다. 1968년에는 일명 Title-Ⅲ라고 하는 종합범죄방지법(Omnibus Crime Control and Safe Streets Act)이 제정되어 수사 목적으로 법 집행기관이 법원의 영장을 받아 통신 감청을 수행할 수 있도록 했다. 이 법은 Carles Katz가 공중전화로 도박 정보를 전송하다가 도박 범죄로 기소되었지만, 그가 항소[10]를 통하여 무죄가 되자 마침내 감청을 본격적으로 규율하기 위해 제정된 법률이다. 이 법이 제정되기 전에는 도청과 감청이 혼재하여 수정헌법 제4조의 범위를 넘나드는 수준에서 종종 수사의 도구로 활용하였다 (Danial J. Solove, 2011; Charles Doyle, 2012; 김승진, 2016; 유상선, 2020:64-66)

8) 불합리한 압수와 수색에 대하여 신체, 주거, 서류, 물건의 안전을 확보할 국민의 권리 침해 금지

9) Olmstead v. United States, 277 U.S. 438, 464 (1928), (유상선, 2020:64)

10) 1심에서는 공중전화의 도청이 수정헌법 4조의 위반이 아니라고 판단했으나, 항소심이 정반대로 판결했다. '수정헌법 4조는 사람을 보호하는 것이지 장소를 보호하는 것이 아니다. 누군가가 대중에게 공개될 것을 인지하여 어떤 정보를 공개했다면 그것은 그의 가택이나 사무실 내부에서 이뤄진 일이라 하더라도 수정헌법 4조의 보호를 받지 못한다. 그러나 그가 어떤 정보를 사적인 것으로 두고자 했다면 그 장소가 대중이 접근할 수 있는 곳이라 할지라도 헌법의 보호를 받을 수 있다.' 이는 영장 없이 공중전화를 도청한 것은 위법한 것이라고 최초로 판결한 사건이다

1976년에는 Keith 판례와 워터게이트 사건을 계기로 해외정보감시법(Foreign Surveillance Act)이 제정되었다. 이 법은 FBI가 세계 공산화 세력에 대한 감시를 강화하던 시기에 정치, 이념적 이유로 도청을 남용했던 관행을 혁파한 법률이다. Keith 사건은 1968년 미시간주 CIA 사무실 폭탄 테러와 관련하여 플라먼던 등 3인을 형사 기소한 사건인데, 이 사건의 판사인 Keith가 플라먼던의 대화 녹음이 법무부 장관 승인 외 법원으로부터 허가를 받지 않았다는 점에 주목하여 정당한 영장 없이 이루어졌으므로 수정헌법 4조에 위반했다고 결론을 내렸다. 이에 정부는 Keith 판결에 불복하여 항소법원에 기소하였지만 패소하였다.[11] 이 판례는 나중에 터진 워터게이트 사건[12]에 대한 상원 처치위원회의 조사 결과와 합쳐져 FISA 법을 제정하게 됨으로써 기존 통신정보 활동에 상당한 영향을 미쳤다. 결론적으로, Title-Ⅲ와 FISA를 제정함으로써 국내 수사뿐만 아니라 해외정보에 대한 합법적인 통신정보 활동을 실질적으로 보장하는 중요한 계기가 되었다 (Whitfield Diffie, Susan Landau, 1998:178; 박진수, 2014:45-46, 유상선, 2020:67-74).

11) 이 사건은 수많은 법리적 다툼 끝에 1972년 대법원까지 올라갔고, 대법원은 "국내감시 활동이 법원의 사전 검토를 완전히 면제받을 수 있다고 보기 어렵다. (중략) 국내 안보 개념이 가진 내재적 모호성, 첩보 활동의 지속성과 광범위성 등으로 정치적 반대 세력의 감시에 남용하고자 하는 유혹 등을 생각할 때, 감시는 특히 더 민감한 문제이다. 동 사건은 정당한 영장 청구 절차가 필요했다"라고 판시하였다

12) 1972년 닉슨 대통령의 재선 기간 워터게이트 호텔에서 민주당 선거사무실에 대한 도청 사건

2) 디지털 시대(1980년대 이후)

(1) 기술 발전과 법률적 변화

1980년대 이후 인터넷과 이동통신 기술이 급속히 발전하면서 통신정보의 디지털화가 본격화되었다. 디지털 통신은 원리상 잡음 제거에 강하여 신호 전송 효율성이 높고 음성, 영상, 데이터 등 다양한 아날로그 신호를 통합 처리할 수 있으며 전송의 보안성도 우수하다. 이런 디지털의 특성에 개방과 공유의 특성을 가지는 인터넷이 접목되면서 사회도 급변했다. 2G~5G 이동통신이 발전하면서 휴대전화, 이메일, 메신저, SNS 등 다양한 디지털 통신 수단이 등장하여 정치, 경제, 사회, 문화 패러다임을 바꿨다.

오늘날에는 대부분의 통신이 고급 암호화 기술을 사용하고 있으며 특히 종단 간 암호화를 사용하는 메신저가 대중화되었으며 AI, 빅데이터, 클라우드 컴퓨팅을 활용한 데이터 분석 기술이 통신 네트워크에 공존하고 있다.

미국은 디지털 통신서비스가 시작되자 아날로그 전화 위주의 감청법인 Title-Ⅲ 수준을 넘어 컴퓨터와 디지털 통신의 기술 영향으로 통신회사에 맡겨진 전자 우편이나 메시지 등 저장된 정보와 개인 정보에 무단 접근을 금지하고, 통신정보 활동에 필요할 때 제한적으로 활용할 수 있게 1986년 ECPA(Electronic Communication Privacy Act)을 제정하였다. 이는 네트워킹 컴퓨팅으로 인해 종전에는 없었던 저장 정보를 통제할 필요가 있었기 때문이다. 그 이후 다시 이동통신 기술이 스파이의 비밀통신이나 테러의 무기로 활용되자 수사기관이 종전의 감청 기술로써 감청영장을 효과적으로 집행하지 못하게 되었다. 이에 1994년 법 집행 통신 지원법(CALEA, Communications Assistance for

Law Enforcement Act)을 제정하였다. 이 법을 제정하기 위하여 미 법무부와 FBI는 의회에 디지털 이동통신에 대한 전화 감청이 가능하도록 제도 개선의 필요성을 적극적으로 요청하였는데, 1994.3.18 FBI 국장 Freeh가 의회 증언에서 "기술적인 문제로 인해 허가된 전자감시를 할 수 없는 사건이 총 91건이며 그중 33%가 이동전화를 포함하고 있다"라고 주장하였다. 당시에 연방, 주 및 지방 법집행기관이 기술적 문제를 종합하여 상·하원 법사위에 보고한 자료에 따르면 총 183건의 영장을 집행하지 못한 것으로 나타났다(유상선, 2020:110).

〈표 1〉 법집행 관련 기술적 문제점

법집행기관이 직면한 기술적 문제점	건수
감청 불가 및 셀 포트 용량 부족 문제	54
음성과 동시 발송 번호, 인식 불가	33
단축다이얼, 착신전환, 그룹 통신, 통화대기 등 감청 불가	38
음성 메일 특정 대상, 분리 감청 불가	16
콜백 기능, 역 발신 기능 추적 등 불가	42
합계	183

CALEA는 이동하는 범죄 혐의자에 대한 감청을 효과적으로 수행하기 위해 디지털 이동통신 사업자에게 감청설비에 관한 협조를 의무화한 조치이다. CALEA의 목적은 법집행기관의 통신정보 활동 능력을 보장하여 주는 한편, 수사 대상이 아닌 일반인들의 통신의 비밀을 온전히 보호할 수 있는 균형 장치를 만들고, 나아가 통신산업의 기술 혁신 및 경쟁 촉진을 진흥하는 데 있다. 이에 따라 통신사업자가 법원의 명령 등 합법적인 전자 감청을 원활하게 지원할 수 있도록 법집행지원 이행프로그램까지 법령에 명시하였다.

CALEA의 주요 내용을 살펴보면, 첫째 통신사업자가 법원의 명령에 따라 법집행기관에 통신정보를 전달해야 하는 기술적 지원 능력 요건을 규정하였으며, 감청 대상이 아닌 일반 가입자에 대한 통신의 간섭을 최소화하고 통화 식별 정보의 프라이버시를 보장하도록 규정하였다.

둘째 CALEA 제정일로부터 1년 이내에 법무부 장관이 법집행기관, 통신사업자, 통신설비 제조업체 등과 의견 수렴을 거쳐 시스템 용량 요건을 관보에 게재하고, 이를 해당 통신산업협회와 기술 표준설정 기관에 제공하도록 하였으며, 통신사업자는 법원 명령에 관계된 직원만 접근할 수 있도록 감청 시스템의 보안성과 완전성에 관하여 규정하였다. 셋째 감청 능력과 요건이 전체 업계에 효율적으로 지원되도록 법집행기관, 전기통신협회, 표준 제정기관, 통신위원회 등의 협의 의무를 규정하였다. 넷째 감청 지원능력 준수 비용 지급 문제를 명확히 하도록 감청현장에 배치된 장비, 설비 및 서비스에 직접 연관된 모든 합리적인 비용을 국가가 통신사업자에게 지급하도록 규정하였다(유상선, 2020:110-113).

CALEA의 핵심 프레임은 연방통신위원회, 기술표준 제정기관, 기술협회 등이 협의하여 제정한 표준에 따라 통신사업자의 교환기나 라우터에 감청 협조 시스템을 설치하는 것이다. 감청 협조 시스템은 표준 규격을 따르고 제3의 신뢰 기관(TTP)에 의해 제공할 수도 있기 때문에 효율성과 신뢰성을 담보할 수 있는 통신정보 인프라이다. 그러나 이 정도 구체적인 법률 제정에도 불구하고 CALEA의 도입과정은 계획만큼 순조롭지 못했던 것으로 분석된다. 1994년 법 제정 당시 5억 달러의 국가 지원 예산을 1998년까지 편성하고도 법 시행은 지연되었다. FBI가 연방관보에 감청용량 요건을 고시한 이후에도 일부 사업자는 무리한 요구라며 FCC에 청원서를 제출했다. FCC는 1998

년 FBI로부터 감청 기술표준에 관한 규칙제정을 요청받고 나서야 비로소 CALEA 이행 준수 기한을 서둘러 조정하고, CALEA 용량 지침을 발표하였다. FBI는 원래 1995년 이전에 설치된 유무선 통신 시스템에 대하여 CALEA 솔루션 적용의 법정 기한이 1998년까지였으나, 4년이나 지연되어 1999년 9월과 12월에 각각 솔루션 구축계약을 체결하였다(유상선, 2020:130).

FCC 보고서[13]에 따르면, 처음에 CALEA는 디지털 이동전화망에 한정하여 감청 기능을 부여했다. 2000년대 인터넷전화와 같은 광대역 통신에 대한 신기술이 등장하자, FBI는 다시 FCC에 웹 통신에 관한 감청설비 지원을 요구하였다. 이에 대해 시민단체들이 FCC의 확장된 감시 기능 지원 정책에 반대하는 소송을 제기했다. 소송에도 불구하고 FCC는 광대역 인터넷 및 VoIP 제공자들에게 2007.5월까지 CALEA 준수기한을 지키도록 결정을 내렸다. 결국, FBI는 CALEA 제정으로 디지털 시대 통신정보 활동을 법제화하는 데 성공하였다.

(2) 9.11테러 직후 애국법 제정

2001년 미국의 9.11테러 이후 애국법이 제정되고, 2013년 에드워드 스노든의 NSA 기밀폭로 이후 자유법이 제정되기까지 안보위기 상황과 시민단체의 움직임 속에서 일련의 통신정보 활동의 변화 과정을 고찰하겠다. 9.11테러 이전에도 여러 건의 테러 예방을 위한 법률 제정 요구가 있었으나 번번이 의회의 반대로 무산되었다. 그뿐만 아니라

13) FCC Second Report & Order:
https://docs.fcc.gov/public/attachments/FCC-06-56A5.pdf (검색일: 2025.12.3.)

1998년도에 EPIC, EFF, ACLU 등 많은 시민사회단체가 정부의 CALEA 이행프로그램에 관한 프라이버시 보호 의견서를 제출하며 통신정보 활동을 적극적으로 저지하였다. 그러나 9.11테러를 계기로 반대하던 시민사회단체와 의회의 태도가 단숨에 바뀌었고 마침내 디지털 통신정보 활동에 큰 영향을 미친 애국법을 제정했다, 애국법은 '테러 예방에 적절한 도구를 제공하여 미국 통합 및 강화하기 위한 법'(USA PATRIOT Act)은 9.11 직후에 상·하원 보고서도 없이 승인되었다. 애국법은 Title-Ⅲ, ECPA, FISA와 같은 통신정보 활동 관련 법률을 비롯하여 이민 및 국적법, 은행 비밀보호법, 자금세탁방지법, 공정신용신고법, 금융 개인정보보호법 등을 포함하여 테러범 추적 관련 법령을 전부 수정하였다. 정부는 관심 있는 사람의 수발신 전화, 학생 기록 및 인터넷 추적과 같은 정보에 대한 액세스 권한을 확대하였다. 법집행기관이 구체적 사유를 제시하지 않고 범죄 수사의 진행 중인 사실을 단순히 알리는 것만으로 통신정보 활동을 가능하게 하였다(Nerman Syed, 2010:38, 유상선, 2020:134). 미국은 9.11테러 사건을 계기로 부시 대통령의 강력한 통치력 아래 국가안보 강화를 위한 애국법을 제정하고 사회 안전망을 촘촘히 구축하였다. 이는 정보기관과 법집행기관의 정보수집과 수사 활동을 활발하게 하는 데 큰 촉매로 작용하였다.

한편, 애국법 제정뿐만 아니라, 법 집행을 효과적으로 추진하기 위하여 제도 개선도 추진하였다. 첫째 미국 내 18,000여 개의 연방, 주, 지방 지역 법집행기관에 서로 다른 수준의 기술 전문성과 다양한 수사방식의 필요를 충족시키기 위해 2013년에 NDCAC[14]를 출범시켰

14) NDCAC(National Domestic Communications Assistance Center): CALEA 법집행지원 조직

다. 이는 종전에 표준화 기술을 제공할 기관이 없었고, 연구개발 기관을 활용할 방법도 없었으며, 법 집행 공동체에 솔루션을 제공할 메커니즘도 없었던 문제들을 해결하기 위해 집행기관에 기술적 해결과 집행지식의 공유를 촉진하고 중요한 훈련을 제공하며 법 집행 관련 다양한 커뮤니티를 지원하는 역할을 하였다.

둘째 시민의 자유를 보장하고 무리한 감청집행을 감시하고 통제하기 위해 9.11 위원회의 권고에 따라 행정부에 초당적인 독립기관으로 PCLOB[15]를 설립했다. 이 위원회는 프라이버시와 시민의 자유가 보호되고 국가를 보호하기 위한 노력과 관련된 행정 각부 정책, 절차, 규정 및 정보공유 관행을 지속 검토할 권한이 있다. 위원회는 매년 두 번 의회와 대통령에게 그 활동의 결과를 보고해야 하며, 보고서는 최대한 대중에게 공지해야 한다(유상선, 2020:164-165). 이같이 애국법은 9.11테러의 산물로서 공권력을 대폭 강화하는 한편 프라이버시 보호를 위한 안전장치도 만들기 위해 노력했다.

(3) 에드워드 스노든의 기밀폭로 이후 자유법 제정

애국법이 한창 작동되던 시기 2013년 6월 에드워드 스노든이 NSA의 기밀 메타데이터 수집 프로그램을 폭로하였다. 스노든의 폭로 이후, NSA 감시 프로그램은 위헌으로 밝혀져 애국법이 자유법으로 개정되었다. 자유법은 '2015년 모니터링을 통하여 권리 충족과 실효적인 규율을 확보함으로써 미국을 통합하고 강화하기 위한 법률'(USA

15) PCLOB(Privacy & Civil Liberty Oversight Board): '9.11 위원회의' 권고로 2007년 설립, 프라이버시 및 시민 자유 감독위원회(상임위원 5명)는 변호사, 정보 책임자, 홍보 및 입법 담당관, 보안 및 기술 전문가, 행정지원 직원 등 약 20명의 직원으로 구성

FREEDOM Act:)로 명명하였다. 자유법의 주요 내용은 첫째 해외정보 수집을 요구할 때 FISC의 절차에 따라 '모든 유형물'을 금지하고, '특정 선정 용어'만을 허용하였다. 둘째 팬 레지스터와 추적장치의 경우에도 '특정 선정 용어'만 허용하고 광범위한 식별자의 사용을 금지하였다. 셋째 미국 밖의 감시 인물에 대해 법무부 장관이나 국가정보 장의 승인 없이 미국인에 대한 정보 활동을 금지하였다. 넷째 해외정보감시법원 판사에게 아미쿠스 큐리에(Amicus curiae)를 최소 5명 지정하여 프라이버시와 시민의 자유 보호를 진전시키고, 정보 수집이나 통신기술 전문지식과 기타 법적 주장을 제공토록 하였다. 다섯째 국가안보문서(NSL)로 정보를 요청할 때 '특정 선정 용어'를 사용하도록 하였다. 여섯째 해외정보감시의 투명성과 신뢰를 위해 유형물 적용 규정 준수를 의회에 연례 보고하되 국제테러 수사 신청 및 승인 건수, 특정 선정 용어가 구체적이지 않은 건수, 수정 및 거부된 신청의 수, 아미쿠스 쿠리에의 인적 사항과 임명의 적절성 등을 제출토록 하였다. 일곱째 일몰 규정이었던 대량 통신기록 수집을 개정해 통신사업자에 수집 권한을 이관하고 로빙 감청을 수정 없이 연장하였다. 결과적으로 자유법은 메타데이터의 대량 수집을 종료하고, NSA가 전화회사에 요청하여 그 응답 정보를 수신하도록 새로운 절차를 만들었다(David Kris, 2018:1, 유상선, 2020:153-155).

결국, NSA가 통화 세부기록의 완전한 세트를 가지지 않기 때문에 정부가 보유하는 메타데이터의 양을 획기적으로 줄였고, 수십 년 동안 거의 밀실 운영되었던 FISC의 법적 해석과 의견에 대해 기밀 해제를 의무화하되 만약 해제가 불가한 경우 의견 요약을 공개하도록 함으로써 시민의 프라이버시를 대폭 강화하였다고 추론할 수 있다.

3. 우리나라 통신정보 활동의 변천

1) 아날로그 시대(1960~1990년대 초)

아날로그 시대에는 우편, 전신, 전화, 팩스 통신이 보편적이었으며, 통신망은 유선 전화망과 무선 통신망이 주류를 이루었다. 유선 통신의 경우 「전기통신기본법」, 무선통신의 경우에는 「전파법」에 기초하여 해당 기술기준을 규정하고 관리하였다. 이 당시는 도청에 관한 규제법률이 없어 수사상 필요한 경우 법원의 허가 없이 검사 지휘 아래 수사관이 직접 통신정보 활동의 결과로 범죄 단서를 획득하면 헌법에 반하지 않는 범위에서 2차 수사를 통해 실체적 증거로 활용했을 것으로 추정된다.

2) 디지털 시대(1990년대 이후)

(1) 기술적 발전

우리나라는 미국보다 약 5년 늦게 디지털 기술로 다중화되면서 전화, 데이터, 영상과 같은 신호종류에 상관없이 송신자와 수신자를 빠르게 연결하는 통신망으로 발전했다. 성격이 서로 다른 망과 상호 연결하는 통신 기술은 정보기기의 개별 망이나 망간 접속을 가능하게 함으로써 인터넷을 급속도로 발전시켰다. 아울러 와이파이와 같은 다양한 무선 기술과 융합하여 시공간을 초월하는 유비쿼터스 시대를 열었다. 전기통신은 IoT 기술을 기반으로 드론, 자율주행차, 스마트 홈 등으로 확장되어 초연결, 초융합, 초지능 사회로 더 빠르게 진화하고 있다. 디지털 통신은 대량의 데이터를 고속 전송하거나 제3 공간 저장 능력이 있는 기술적 특성으로 인하여 다양한 서비스의 제공이

가능하여 유용하지만, 그 기술을 악용하게 되면 위조, 변조, 조작, 탈취, 침해와 같은 취약점도 적지 않다. 사이버 공간에는 해킹, 악성 코드 배포, 정보 조작 등의 부정적인 형태로 혼재하고 있어 사이버 전쟁을 방불케 한다. 일반적으로 새로운 기술은 현재의 법률로 규율하지 못하기 때문에 기존 통신정보 활동에 심각한 공백을 만들어 왔다.

(2) 법률적 변화

우리나라는 1993년 통신비밀보호법 제정으로 통신정보 활동에 대한 규제가 처음 마련되었다. 미국의 전기통신 감청 정책보다 약 25년 뒤졌다. 우리나라는 통신비밀보호법을 처음 제정할 때 미국의 법제를 본받았다. 그런데, 입법 배경도 통신의 비밀과 자유를 보호하고 합법적인 감청을 보장하기 위한 것으로 미국과 비슷하며 법률적인 구조도 유사하다는 평가도 있으나, 법 집행능력 측면에서는 상당한 차이가 있다. 왜냐하면 오늘날 대부분의 통신을 차지하고 있는 스마트폰을 악용하는 범죄에 대하여 통신정보 활동을 위한 법률 집행이 곤란하기 때문이다.

2005년 8월 불법감청 고백[16]에서 밝힌 바에 따르면, 검찰이 보유하던 휴대폰 감청기 8대 모두 98년 이후 디지털 방식에 사용이 어렵게 되자 2001년 외국으로 넘겼다고 당시 법무부 장관과 검찰이 증언[17]하였다. 이후, 수사기관에서 범죄 수사를 위한 스마트폰 감청을 수행하는 소식은 없다.

16) https://www.newswire.co.kr/?md=A10&act=article&no=3485 (검색일: 2025.7.15.)

17) https://www.khan.co.kr/article/200508250756071 (검색일: 2025.12.4.)

스마트폰에 대한 합법적인 통신정보 활동은 이동통신의 특성상 통신사업자의 감청 협조가 불가피하다. 이를 위해 감청 협조 설비구축 비용 보전, 협조 의무 위반 처벌, 감청 설비구축 이행 촉진의 일환으로서 자문을 제공하기 위한 과학기술정보통신부의 '기술지원 자문위원회' 설치 등을 규정하고, 설비의 용량, 규격, 성능 등에 관한 감청기술표준을 제정하는 것을 고려해 볼 수 있다. 이를 반영하여 17대 국회에서 통신비밀보호법 개정법안이 상정되었는데, 학계와 시민단체의 찬성과 반대가 팽팽히 맞서 법률 개정이 무산되었다. 이런 사태는 18대와 19대 국회에서 반복되었고 이와 관련하여 토론회와 공청회가 여러 차례 있었으나, 뚜렷한 접점을 찾지 못하고 장기간 표류하였다. 결국, 스마트폰에 대한 우리나라 통신정보 활동은 합리적 논리와 법리적 시비 수준을 벗어난 상태로 분석된다. 불법감청 고백 사건이 관련자의 형사 처리와 처벌 규정만 강화하고, 스마트폰에 대한 합법적인 통신제한조치 절차와 기준을 마련하지는 못한 것으로 풀이된다.

통신정보는 범죄 수사를 위한 증거 수집과 국가안보를 위한 정보 수집의 목적으로 활용된다는 점에서 그 필요성이 법적으로 명확히 인정되고 있다. 그러나 정보 활동의 현장에서 중요성을 인정받지 못하는 사례가 늘고 있다. 첫째, 통신비밀보호법의 위헌 소송 사례들이다. 헌법재판소에서 3건의 헌법불합치 판결을 살펴보면, ① 2010.12. 감청 기간 연장의 횟수 제한 문제 ② 2018.6. 기지국에서 이뤄진 휴대전화의 접속기록 전수 조사에 관한 문제 ③ 2018.8. 인터넷 회선으로 송수신하는 전기통신에 대한 감청 문제 등이 대표적인 사례들이다. 둘째, 전문성이 부족한 국회나 시민단체가 통신정보 활동의 기술과 내용에 관한 신뢰가 낮다. 2006.3. 국회 정보위원회 모 의원이 본회의에서 테러방지법 의결 과정에 "외국에서 테러를 준비한 상태로 우리

나라 왔다가도 잡지 못하고, 법이 없어서 처리하지 못했다.”라며, “여태까지 법이 없어 53명 추방 조치했다. 활동을 많이 해도 테러를 일으키기 전까지는 조치할 수 없다.”라고 법안 처리를 강조하였으나, 이에 맞서 더불어민주당 모 의원은 “북한이 로켓을 발사했는데 정부는 국민의 휴대폰을 뒤지려고 한다. 테러방지법은 국민사찰법이다. 이 법이 통과되면 여당 의원 여러분의 휴대폰부터 도청될 수 있다.”라며 반대하였다(김현중 외, 2016.3.3.『뉴데일리』). 또 진보넷 황OO은 “정보인권 운동을 펼쳐나가는 동시에 국가가 시민을 통제하는 수단으로 IT 기술을 사용하지 않도록 감시하는 역할을 이어갈 예정이다.”라고 법 개정에 반대하는 목소리를 높였다(김한주, 2019.3.18.『참세상』. 유상선, 2020:24-25). 국가안보와 범죄 수사에서 헌법적 가치를 존중하는 통신 제한조치의 절차와 기술을 구현할 때 반드시 선행되어야 할 프라이버시와 개인정보보호를 위한 감청 통제 장치 마련이 중요하다. 그러나 이를 위한 법률과 기술의 학술적 논의와 실무적 협의에는 관심이 없고 정치적 공방만 난무한다. 양 진영 간의 감청에 관한 논쟁은 마치 ‘고르디아스의 매듭’과 같은 양상을 보여준다.

Ⅳ. 우리 통신정보 활동의 한계와 도전 과제

1. 통신정보 활동의 한계

앞서 살펴본 대로 미국의 통신정보 활동 변천과 비교해 볼 때, 우리나라 통신정보 활동 변화 과정은 일련의 정책 실패로 분석된다. 예컨

대 정보통신 기술이 아날로그에서 디지털로 변화할 때, 미국은 당시에 정부나 수사기관이 단독으로 법 집행하는 것이 곤란한 점을 인식하여 CALEA를 제정하였다. 반면에 우리나라는 유사한 법률을 제정해야 할 시점에 디지털을 방관하고 아날로그 방식으로 통신비밀보호법을 제정하였다. 결과적으로 디지털 환경에서 통신정보 활동을 편법으로 시행해 불법감청 고백에 이를 정도로 사회적 부작용이 컸다. 뒤늦게 CALEA와 비슷한 규정을 만들어 '통신사업자 협조 의무'를 규정하였으나, 시민단체 반대로 시행령이 제대로 수립되지 않았다. 결국, 우리나라 통신정보 활동은 정치, 국민 정서, 법령 구조, 기술 요소 등 복합적인 문제로 얽혀 지금까지 표류 돼 있다. 그 원인을 따지면 첫째, 정부(수사기관)가 기술 환경 변화에 맞춰 적절한 법령 집행 여건을 개선하지 못한 상태에서 과거 편법적인 정보 활동과 부작용으로 신뢰를 잃은 점. 둘째, 통신정보 활동의 필요성을 공감하나 오남용의 나쁜 경험으로 정치 쟁점화에 쉽게 휩싸이는 점. 셋째, 법령의 구조를 연구하거나 신뢰 회복을 위한 어떠한 정책과 전략이 없는 점. 넷째 투명한 법 집행을 위한 방법으로써 감청 기술에 관한 기술표준을 도입하지 않고 있는 점 등이다. 해법은 단순한 것 같지만, 국민 불신과 정책 포기가 점철되어 당장 무엇부터 해결해야 할지 모르는 형국으로 비친다. 이에 통신정보 활동의 정상화를 위한 도전적 과제를 살펴볼 필요가 있다.

2. 통신정보 활동의 도전 과제

1) 정치·사회·안보적 딜레마 해소

통신정보 활동은 헌법과 법률에 따라서 국가안보와 범죄 수사의

목적으로 수행되는 공권력의 중요한 요소일 것이다. 그 중요성은 헌법 제91조(안전보장), 통신비밀보호법 제5조(범죄 수사) 및 제7조(국가안보)에서 통신정보 활동인 통신제한조치 집행에 관한 규정에서 충분히 포섭되어 있다. 그러나 앞에서 본대로 통신비밀보호법의 개정이 장기간 지연되고 있는 상태에서 정부나 국회 차원의 노력이 부진한 상황을 현실적으로 이해하기 어렵다. 더욱이 범죄 혐의자의 스마트폰에 대한 통신정보 활동을 할 수 없는 나라는 OECD에서 대한민국이 유일하다. 예컨대 미국의 감청보고서[18]에 따르면, 2023년 총 2,101건의 감청이 승인되었는데, 이 중 1,129건은 연방 판사가 승인했고, 972건은 주 판사가 승인했다. 이는 외국정보감시법(FISA)으로 규제하는 안보 감청을 제외하고, Title-Ⅲ에 근거한 일반범죄 수사 목적의 감청만을 보고한 통계이다. 스마트폰이 전체 감청 대상의 95%를 차지한 것으로 나타났다. 감청으로 수사한 가장 많은 범죄가 마약범죄로 전체의 50%를 차지했고, 음모와 같은 불법 모의는 전체의 11%, 살인 및 폭행죄는 5% 정도였다. 2023년 한 해 감청 수사로 총 5,530명이 체포되었으며, 456명이 유죄 판결을 받았다. 일반 수사로는 불가능하다. 우리나라는 산업스파이· 간첩의 안보 위협, 외국인 범죄 증가, 마약과의 전쟁에 통신정보 활동이 미치지 못하고 있다. 이로 인한 국부 유출, 국민 피해, 국가안보 위기 등에 관하여 피해 규모조차 산출할 수 없는 상황이다. 앞으로 정치·사회·안보적 딜레마 해소를 위한 노력이 필요하다.

18) 미국 연방법원: United States Court - Wiretap Reports. https://www.uscourts.gov/data-news/reports/statistical-reports/wiretap-reports(검색일: 2025.7.15)

2) 시민 안심과 국민 신뢰 회복

시민은 법률에 근거한 통신정보 활동에 관한 합법적·절차적인 내용에 관하여 잘 모르는 경우가 많다. 그러나 과거에 수사기관이 불법적으로 남용해 공분을 샀던 아픈 기억은 남아 있다. 이러한 약점은 일부 시민단체와 정치권에서 통신정보 활동의 정상화를 위한 법률 개정을 추진할 때, 정략적으로 악용되는 측면이 없지 않다. 특히 총선이나 대선 등 선거철이 되면 더 심각하다. 예컨대, 과거 통신비밀보호법 개정안을 발의할 때, 법안 개정에 반대하는 시민단체가 엄격한 법률적 절차를 거쳐 합법적인 감청을 수행하는 일을 마치 '전체 국민을 도청하게 된다' 식으로 침소봉대하고 불안감을 부추기며 집권 여당과 정부를 비방하는 경향이 짙은 현상이 나타났다. 이때 법률과 기술 이해가 부족한 일반 시민은 과거의 나쁜 기억이 소환되어 사실과 다른 잘못된 주장을 지지할 수 있을 것이다. 이는 민주주의 법치 국가에서 합법적이고 투명한 법률 집행 제도를 만들겠다는 정부의 의지를 무색하게 만들 뿐만 아니라 국가와 정부에 대한 국민 불신을 조장하는 모습으로 비추어질 수도 있다. 정치적인 허위 주장에 휩쓸린 시민의 불안과 의혹이 국가의 안전 확보와 통신정보 활동의 법률적인 근거 마련을 방해하는 경향으로 작용한다. 정부나 수사기관의 안일한 대응 방식도 상당한 문제가 있는 것으로 보인다. 앞으로 법안 개정의 목적과 취지를 명확하게 설명하고 외국의 사례와 각계 전문가의 연구와 정책 홍보를 통하여 먼저 국민적 신뢰를 얻어내는 노력이 중요할 것이다.

3) 법령 구조 개선

통신정보 활동에 관한 법률적 근거는 여러 개별법에 산재하고 있

다. 형사소송법, 군사법원법, 전파법, 통신비밀보호법 등이다. 물론 '통신정보 활동'이란 용어를 직접 사용한 규정은 없다. 형사소송법과 군사법원법은 구속 또는 복역자에 대한 통신(우편)을 감시하고, 전파법은 혼신 제거와 같은 전파 질서 유지를 위해 전파를 감시한다. 법원의 허가 없이 고유 직무를 수행하기 위한 통신정보 활동이다. 반면, 통신비밀보호법은 우편물의 검열 및 전기통신의 감청을 '통신제한조치'로 명명하여, 범죄 수사와 국가안보를 위한 보충적인 수단이 국민의 통신 자유에 대한 침해가 최소한에 그치도록 규정하고, 법원의 허가를 받아 통신제한조치를 하도록 허용하고 있다. 통신비밀보호법 제5조 및 제6조에 범죄 수사 목적으로 통신제한조치의 허가요건과 허가절차를 규정하고, 제7조에 국가안보를 위한 통신제한조치를 규정하고 있다. 또 국가기관 감청설비의 신고(제10조의2), 감청 기간과 횟수 제한(제6조), 국회 통제(제15조) 등 엄격한 통제 장치와 함께 전기통신사업자의 협조 의무(제15조의2)까지 규정하여 통신제한조치가 가능하도록 기본적인 골격을 갖추고 있다. 그러나 전기통신사업자가 협조해야 할 사항과 협조에 관하여 필요한 사항을 대통령령에 위임하고도 시행령을 충실히 개정하지 못하였다. 그뿐만 아니라 전기통신사업자가 협조를 이행하지 않을 때 징벌적 조치사항도 없다. 통신비밀보호법이 기본권 보장을 위해 보충적 수단으로 최소한의 집행에 그치도록 엄격하게 통제하고 있지만, 그러한 통제 자체가 무의미할 정도이다. 앞으로 ① 법령의 정비 방안 ② 사업자 협조 사항과 필요 사항 연구 등을 위하여 입법 조사 및 사례 연구가 절실한 실정이다.

4) 국제 감청 기술 표준 도입

국제사회에서는 합법적 감청의 기술표준 개념을 'Lawful Inter-

face'라 통칭한다. 이러한 표준은 국가별 법률과 규제에 따라 다르며, 미국과 유럽은 각각 고유한 규격을 개발하고 있다. 미국은 CALEA에 따라 다양한 기술표준을 개발하여 감청 인터페이스를 구현하고 있다. 미국표준협회(ANSI)와 통신산업협회(TIA)는 CALEA 준수를 위한 구체적인 기술표준을 제정하고 있다. 유럽에서도 전기통신표준협회가 합법적인 감청과 관련된 기술표준을 개발하고 있다. 다양한 통신 환경에서의 감청 요구 사항을 충족하기 위한 표준을 제정하고 있으며, 이는 EU 회원국들이 공통으로 준수하는 지침으로 활용된다. 이처럼 미국과 유럽은 각각의 법률과 규제에 따라 통신 시스템의 합법적인 감청을 지원하기 위한 다양한 기술 표준과 규격을 개발하여 적용하고 있다. 주요한 다섯 가지를 소개하면 다음과 같다.

① 3GPP TS 33.107: 3G 이동통신 시스템에서의 합법적 감청을 위한 기술 사양을 정의
② 3GPP TS 33.128: 5G 시스템에서의 합법적 감청 요구 사항과 아키텍처를 규정
③ ETSI TS 101 671: 합법적 감청의 기본 요소와 전달 인터페이스를 상세히 설명
④ ETSI TS 102 232 시리즈: 인터넷 기반 서비스(예: VoIP, 이메일)에 대한 합법적 감청을 지원하기 위한 기술 사양
⑤ ANSI/TIA-1072: 무선통신 시스템에서의 합법적 감청 기능을 규정

감청 기술 표준은 법률 집행을 투명하게 하고 감청 남용을 방지하는 중요한 기능을 한다. 이뿐만 아니라 앞으로 우리나라 형사절차에

서 도입되어야 할 온라인 압수수색에 관한 방법과 기술도 국제표준을 따르면 될 것이다. 우리나라가 이러한 감청 기술 표준이 없다는 것은 아쉽다. 다만, TTA가 2008.7. 미국, 유럽, 아시아를 대표하는 10개 정보통신 표준화 기구들이 모여 정보통신 표준화에서 협력 방안을 논의하는 제13차 세계 표준 협력 회의에 참석했다고 밝힌 적 있는데 여기서 "국제협력을 통한 네트워크 전환"이라는 주제로 비상 통신, 보안 및 합법적 감청, ID 관리, 사이버 정보보호, U-Healthcare 등 18개 공동 관심 분야의 표준화 협력 방안을 논의하고, 표준과 연관된 지식재산권 문제도 논의하였다고 밝혔다.[19)]

중요한 점은 국내 정보통신기술협회에서 각국의 '합법적 감청'이 주요 의제로 다뤄지는 회의에 참석해서 합법적 감청 동향을 이미 알고 있었다는 것이다. 그럼에 불구하고 이미 국제적으로 널리 표준화되어 있는 감청 기술을 도입하지 않고 디지털 환경에서의 정보 수집이나 범죄 수사를 포기하고 있다는 것은 선뜻 이해하기 어려운 대목이다. 향후 정부가 국내 통신환경에 부합하는 감청 기술 표준제도를 수립하도록 학술 연구를 강화하면 좋을 것이다.

19) https://www.tta.or.kr/tta/selectBbsNttView?key=11&bbsNo=22&nttNo=10361 (검색일: 2025.12.4.)

V. 결론

통신정보 활동은 국가안보와 공공안전 확보를 위한 핵심적인 수단으로 다음과 같은 경우에 법적으로 보장되어야 한다. 첫째, 국가안보에 중대한 위협이 예상되거나 「국민 보호와 공공안전을 위한 테러방지법」에 따른 정보 수집이 필요한 경우. 둘째, 범죄를 계획·실행 중이거나 실행한 것으로 의심할 만한 충분한 근거가 있고, 다른 수단으로는 범죄 저지, 범인 체포, 증거 확보가 어려운 경우이다. 어떤 유형의 통신정보 활동이라 할지라도 당연히 국민의 프라이버시와 개인정보 보호를 최우선 전제해야 한다.

본론에서 통신정보 활동의 중요성, 필요성, 시급성 위주의 논거로 인하여 프라이버시와 개인정보보호의 이론과 논거가 상대적으로 부족했던 점이 학술적 측면에서 연구 편향으로 인식될 수 있으나, 연구 범위상 통신정보 활동의 한계 극복 측면에서 불가피했던 점이 있음을 밝힌다. 그러나 앞서 언급하였듯이 감청 규제 및 프라이버시 보호의 이론을 대신해 감청 통제 장치의 필요성을 충분히 제안하였다. 앞으로 경찰행정법·헌법·개인정보보호법의 국내 학술논문 및 EU-·ECHR·GDPR 등 국제 인권·데이터보호에 대한 후속 연구가 있으면 좋겠다.

결론적으로 디지털 환경에서는 국경 개념이 모호해지고 있으며, OECD 국가 중 유일하게 우리나라만이 스마트폰에 대한 통신정보 활동을 하지 못하는 현실은 국가안보와 법치 유지에 대한 최소한의 책임조차 방임하는 것이라 볼 수 있다. 통신의 비밀과 정보인권 보호를 이유로, 혹은 국민적 합의가 부족하다는 명목으로 국내 잠입 테러, 간첩, 마약, 산업스파이 등에 대한 통신정보 활동을 장기간 제한하는

것은 헌법적 가치에 반하는 태도이다.

특히, 국가안보와 프라이버시의 양 가치를 존중하며 통신비밀보호법의 정상화를 바라는 법안 개정 과정에 사실 왜곡과 허위 주장으로 시민의 불안을 조장하거나 통신정보 활동의 법적 근거 마련을 저해하는 행위는 대한민국의 법치를 파괴하는 것이고 나아가 범죄로부터 안심하고 삶을 영위할 국민의 행복추구권을 박탈하는 것이라 볼 수 있을 것이다.

이에 대한 국가 수사기관의 소극적인 문제의식과 무책임이 통신정보 활동의 한계 문제를 더욱 심화시키고 있다는 합리적 의구심을 가지지 않을 수 없다. 향후 법안 개정의 목적과 이유를 명확히 설명하고, 외국의 사례와 전문가 연구, 정책 홍보를 통해 국민적인 신뢰를 확보하는 노력이 필요하다.

현행법은 감청을 보충적 수단으로 제한하고 엄격한 통제 장치를 규정하며 통신사업자의 감청 협조 의무까지 규정하고 있으나, 실제로 범죄 수단으로 활용하는 범죄자의 스마트폰 통신에 대한 감청이 안 된다는 것은 자유 법치 국가의 모순이다. 이런 점에서 현재 감청의 통제 장치는 유명무실하다고 추론해 볼 수 있다. 국제적으로 표준화된 감청 기술은 디지털 환경에서 정보 수집과 범죄 수사를 효과적으로 할 뿐만 아니라, 오남용을 방지할 수 있는 기술적 통제 방식이다. 국내 통신환경에 적합한 감청 기술 표준제도를 도입하여 실질적인 감청 통제가 가능하게 될 때, 비로소 감청 통제를 위한 독립적인 감독기구도 의미가 있을 것이다. 관련 법령 정비를 위하여 필요한 사항에 대한 입법 조사가 이루어지기를 기대한다.

〈참고문헌〉

강신각. 2009. “제18대 국회 법제사법위원회 회의록. 제282회(5차),” 국회 법제사법위원회 회의록.

김상겸. 2009. “선진국의 통신감시 제도와 국민인권 침해방지 방안- 선진한국을 위한 통신비밀보호법 개정 방향,” 『국가안보전략연구』.

김성천. 2008. “통신감청제도에 대한 개선방안 연구,” 『중앙법학』. 10(1)

박경신. 2009. “미국의 통신비밀보호법(ECPA) 및 범죄수사통신지원법(CALEA)과 우리나라의 통신비밀보호법 및 18대 국회 개정안의 비료 검토,” 『안암법학』. 29.

박소영·김은숙·강신각. 2006. “미국의 IP 서비스 감청 규제 동향,” 『전자통신동향 분석』. 21(5)

박진수. 2014. “국가정보 개혁과 의회 감시 - 처치위원회와 파이크위원회 사례를 중심으로,”『국가전략』. 20(4)

박찬걸·강동욱. 2014. “통신제한조치의 집행에 관한 법정책적 고찰,” 『법과정책』. 20(1)

백수원. 2023. “‘감청’ 허용 기준과 ‘감청’ 범위에 관한 입법적 제안,” 『서울법학』. 31(1-34)

오길영. 2014. “통신데이터 남용의 실태와 그 쟁점,” 『민주법학』. 55

오길영. 2015. “통신비밀보호법의 문제점과 개선방향.” 『언론과 법』. 14(1)

유상선. 2020. “미국의 전기통신 감청정책과 통제의 효과성에 관한 연구.” 건국대학교 박사학위

유 훈. 2016. 『정책집행론』. 서울: 대영문화사

윤상필. 2025. “감청자료 관리제도의 요구와 통신비밀보호법의 역할,” 『공법학연구』. 26(1)

전 웅. 2015. 『현대 국가정보』. 서울: 박영사.

Charles Doyle. 2012. “Privacy: AN Overview of Electronic Communications Privacy Act.” Congressional Research Service.

Daniel J. Solove 저·김승진 역. 2016.『숨길 수 있는 권리』. 서울: 동아시아.

David S. Kris & Douglas Wilson. 2012. “National Security & Prosecutions 2d.” West.

Daniel J. Solove. 2011. “Nothing to Hide : The False Tradeoff between Privacy and Security.” Yale University Press.

Nerman Syed. 2010. “Effectively Diffusing Terrorism: How Successful Have U.S. Policies Been in Combating and Deterring Al-Qaeda Post-9/11?.” Georgetown University.

Orin S. Kerr. 2014. “A Rule of Lenity for National Security Surveillance Law.” Virginal Law Review. Vol. 100.

Whitfield Diffie, Suan Landau. 2010. “Privacy on the Line: The Politics of Wiretapping and Encryption.” The MIT Press

United States Court - Wiretap Reports. https://www.uscourts.gov/data-news/reports/statistical-reports/wiretap-reports

United States FBI. https://www.fbi.gov/@@search?SearchableText=going+dark&searchHelpText=To+narrow+your+search%2C+select+a+content+type+option+listed+under+%E2%80%9CMore.%E2%80%9D+To+broaden+your+search+to+other+FBI+sites%2C+select+a+subdomain+listed+under+%E2%80%9CSource.%E2%80%9D&pageSize=20&page=1&sort_on=&sort_order=descending&after=

A Study on the Transition of Communication Intelligence Activities and Challenges of the Digital Age

Yu Sangseon | Korea University

Communication intelligence activities are changing significantly according to the attitudes of communication users and socio-cultural demands due to the complex attributes of communication services such as openness, sharing, security, and encryption. This phenomenon is acting as a big challenge because it is difficult to respond only with traditional methods and techniques in terms of collecting or acquiring communication information. In order to carry out communication intelligence activities normally in terms of national security and criminal investigation, it is more important to secure legal and institutional stability than anything else.

In the U.S., a country under the rule of law, communications and intelligence activities went through a balanced development process in both national security and privacy by preparing CALEA in the 1990s during the digital transition, enacting the Patriot Act immediately after the 9/11 terrorist attacks, and enacting the Freedom Act after Edward Snowden's disclosure of NSA secrets. On the other hand, our Communication Secret Protection Act is a product of the analog communication era and does not even have a minimal supplementary function in terms of criminal investigation.

Accordingly, the definition and type of communication information were reviewed, and the historical transition process of communication information activities was investigated to explore the limitations and challenges of communication information in a digital communication environment. The conclusion is that it is important to resolve the political, social, and security dilemma to secure the legal stability of communication intelligence activities, restore citizenship and public trust, improve the structure of laws and regulations, and introduce international intercept technology standards. To this end, it is necessary to gradually expand the support for academic research and entrust policy research tasks to related authorities.

Keyword Communication Information, Communication Secret Protection Act, Patriot Act, Freedom Act, National Security, Criminal Investigation, Intercept Technology Standards