성균관대학교 법학연구원 『성균관법학』 10.17008/skklr.2021.33.2.013
제33권 제2호 (2021. 6.)
Sungkyunkwan Law Review Vol.33. No.2 (June 2021) pp 407 - 445

통신비밀보호법과 테러방지법상 영장주의 강화를 위한 법제정비 방안

한웅재* · 김일환**

【목 차】

Ⅰ. 들어가는 말
Ⅱ. 통신비밀보호에 있어 영장주의의 위기
Ⅲ. 통신비밀보호의 강화를 위한 법제정비방안
Ⅳ. 결론

【국 문 요 약】

전통적으로 통신의 자유에 있어 영장주의와 연관되어 문제가 되는 사안은, 신체의 자유를 중심으로 도청 및 감청과 관련된 부분이었다. 그러나 현대에는 정보수집을 위해서는 이보다 다양한 방법이 이용된다. 더구나 다수의 대량 데이터를 교환하고 연결해주는 통신서비스를 제공하는 민간기업을 이용하면 더 심층적이고 더 내밀한 정보를 수집할 수 있다. 또한, 통신기기의 압수를 통해서 국가가 얻어 낼 수 있는 정보는 필연적으로 개인의 사생활에 대한 침해로 이어지는데, 이에 대한 절차적 정교함은 부족해 보인다. 영장주의하에서 이러한 논의들

* 변호사, 주저자.
** 성균관대학교 법학전문대학원 교수, 교신저자.

을 배경으로 실제 운용은 어떠한지 세밀한 논의가 필요하다. 영장주의는 독립된 법관에 의해 체포·구속뿐만 아니라 압수·수색·검증과 같은 다양한 기본권 침해에 개인이 방어할 수 있는 절차적 의의가 있다. 영장주의가 통신비밀보호라는 역할을 제대로 수행하지 못하고 정보수사기관의 재량에 대한 통제가 제대로 작동하지 않는다면, 국가는 국민에 대한 개인정보를 바탕으로 이른바 '감시사회'를 만들 수 있다. 그리고 이러한 감시사회는 헌법이 추구하는 인간 존엄, 사상과 양심, 영업, 학문, 종교, 정치활동 전반에 대한 통제로 이어질 가능성이 크다. 지능정보사회에서 통신비밀보호를 위해서는 영장주의가 강화되어야 한다는 문제의식 하에 통신기기는 물론 범죄수사, 국가안보 전반에 대해 대안을 제안하고자 노력하였다. 특히 영장을 통한 통신제한조치의 기한 및 통지를 개인정보자기결정권의 입장에서 검토하고 「테러방지법」에 대해서는 영장주의를 보강하고자 피의자별 통신제한조치를 제안하고, 본 법을 통한 통신제한조치의 통제를 위한 위원회 및 국회통제 방안을 간략하게 제시하였다.

Ⅰ. 들어가는 말

헌법 제18조에는 통신비밀의 침해 시에 영장이 필요한지는 특별히 명시되어 있지 않다. 그러나 통신비밀보호가 기본권에 속하며, 이에 대한 침해는 통신비밀이라는 가치뿐만 아니라 개인에 대한 다른 자유권에도 중대한 침해가 가능하므로, 법관에 의한 사전적 허가로서 영장주의의 원칙이 적용되는 것은 당연한 헌법적 요청이다.[1] 따라서 입법부는 이러한 헌법적 요청을 이행하기 위해 다양한 법률을 제정하여 통신비밀을 보호하고 있으며 통신비밀이 침해되는 경우에 대한 절차를 규정하고 있다.

전통적으로 통신의 자유에 있어 영장주의와 연관되어 문제가 되는

1) 한수웅, 헌법학, 법문사, 2021, 705면.

사안은, 신체의 자유를 중심으로 도청 및 감청과 관련된 부분이었다. 그러나 현대에는 정보수집을 위해서는 이보다 다양한 방법이 이용된다. 더구나 다수의 대량 데이터를 교환하고 연결해주는 통신서비스를 제공하는 민간기업을 이용하면 더 심층적이고 더 내밀한 정보를 수집할 수 있다. 또한, 통신기기의 압수를 통해서 국가가 얻어 낼 수 있는 정보는 필연적으로 개인의 사생활에 대한 침해로 이어지는데, 이에 대한 절차적 정교함은 부족해 보인다. 영장주의하에서 이러한 논의들을 배경으로 실제 운용은 어떠한지 세밀한 논의가 필요하다. 영장주의는 독립된 법관에 의해 체포·구속뿐만 아니라 압수·수색·검증과 같은 다양한 기본권 침해에 개인이 방어할 수 있는 절차적 의의가 있다.[2] 영장주의가 통신비밀보호라는 역할을 제대로 수행하지 못하고 정보수사기관의 재량에 대한 통제가 제대로 작동하지 않는다면, 국가는 국민에 대한 개인정보를 바탕으로 이른바 '감시사회'를 만들 수 있다. 그리고 이러한 감시사회는 앞서 언급한 대로 헌법이 추구하는 인간 존엄, 사상과 양심, 영업, 학문, 종교, 정치활동 전반에 대한 통제로 이어질 가능성이 크다.[3] 따라서 '안전에 대한 예방'과 '헌법상의 기본권'을 조화시킬 수 있는 절차적 역할로써 영장주의는 큰 의미가 있다. 헌법의 가치는 분리되어 있지 않고 연관되어 있으며 국가의 책무는 이러한 연관된 헌법의 가치를 수호하는 데 있다. 따라서 국가는 구체적인 법률에서 헌법의 가치가 발현되도록 이를 반복하여 검토하고 절차를 준수하는 것은 매우 중요하다.

현재 통신비밀보호와 영장주의가 연관성을 맺는 대표적인 법률은

---

2) 헌법재판소 2012. 12. 27. 2011헌가5 : "우리 헌법제정권자가 제헌 헌법(제9조) 이래 현행 헌법(제12조 제3항)에 이르기까지 채택하여 온 영장주의의 본질은 신체의 자유를 침해하는 강제처분을 함에 있어서는 인적·물적 독립을 보장받는 제3자인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여야만 한다는 데에 있으므로, 우선 형식적으로 영장주의에 위배되는 법률은 곧바로 헌법에 위반되고, 나아가 형식적으로는 영장주의를 준수하였더라도 실질적인 측면에서 입법자가 합리적인 선택범위를 일탈하는 등 그 입법형성권을 남용하였다면 그러한 법률은 자의금지원칙에 위배되어 헌법에 위반된다고 보아야 한다."

3) 이에 관하여는 김일환, 초연결사회에서 개인정보보호법제 정비방안에 관한 연구, 성균관법학 제29권 제3호, 2017, 52면 이하 참조.

「통신비밀보호법」과 「국민보호와 공공안전을 위한 테러방지법(이하 테러방지법)」이다. 이 글에서는 이 중 「통신비밀보호법」의 구조와 내용을 간략히 이해하고, 나아가 이 법률과 현재 진행 중인 통신기술의 발전에 따른 비밀보호의 어려움, 그리고 영장주의의 위기라는 구체적인 문제점에 대해 논하고자 한다(아래 Ⅱ.항). 그리고 통신비밀보호의 강화를 위한 법제정비방안을 논한 후(아래 Ⅲ.항) 맺는다.

Ⅱ. 통신비밀보호에 있어 영장주의의 위기

1. 통신비밀보호법상 통신제한조치의 일반적인 내용

우편물의 검열, 전기통신의 감청 또는 '통신사실 확인자료'의 제공을 하거나 공개되지 아니한 타인 간의 대화를 녹음 또는 청취와 같은 통신제한조치는, 원칙적으로 누구든지 「통신비밀보호법」 제3조 제1항과 「형사소송법」 제107조 또는 「군사법원법」의 제147조 등에 의하지 아니하고는 하지 못한다. 「통신비밀보호법」 제3조 제2항에서는 우편물의 검열 또는 전기통신의 감청은 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다고 규정하고 있다. 「통신비밀보호법」 상의 통신제한조치 규정은 「형사소송법」에 근거조항이 없어서 임의수사인지 강제수사인가를 놓고 다투어지던 도청의 문제를 강제수사로 파악하여 영장주의에 의한 통제를 도입하였다는 점에서 의미가 있다.[4)]

「통신비밀보호법」 상 통신제한조치는 우편물의 검열과 전기통신의 감청을 포괄하는 개념이다. 또한, 동법은 제5조 및 제6조에서 통신제한조치를 구체적으로 범죄수사를 위한 통신제한조치, 제7조에서 국가안보를 위한 통신제한조치, 제8조에서 긴급통신제한조치로 나누어 규정하고 있다. 그리고 제9조에서 통신제한조치의 집행, 제9조의2에서 대상자에의 통지, 제9조의3에서 송·수신이 완료된 전기통신에 대한 압수·수색·검증의 집행에 관한 통지 등을 규정하고 있으며, 제10조 내지 제10의5에서 그

4) 헌법재판소 2018. 6. 28. 2012헌마191.

외에 감청설비의 운용요건, 제11조에서 통신제한조치 등에 관여한 자의 비밀준수의무, 제13조 내지 제13조의5에서 '통신사실 확인자료'의 제공과 관련한 사항 등에 대해서도 함께 규정하고 있다. 이 중에서 해석론상의 논의는 범죄수사를 위한 통신제한조치를 중심으로 통신제한조치와 긴급통신제한조치에 집중되어 왔다.

2. 테러방지법에 의한 통신감시조치의 일반적 내용

(1) 테러방지법의 목적

「국민보호와 공공안전을 위한 테러방지법(이하 테러방지법)」은 2016년 3월 테러의 예방 및 대응을 위해 제정되었으며, 국민의 생명과 재산을 보호하고 국가 및 공공의 안전을 확보하는 것을 목적으로 한다. 동법은 기본적으로 테러예방을 목적으로 하면서도 대테러법 기능도 담고 있다.[5)]

「테러방지법」은 미국의 9·11테러 이후 높아진 테러에 대한 위험과 경각심을 이유로, 여러 차례 국회에 발의되었으나 통과되지 못했다. 테러방지법이 통과되지 못했던 이유는, 기본권 침해의 가능성과 국가정보원과 군의 과도한 권력집중 등에 대한 우려[6)]가 높았고, 이미 존재하는「국가보안법」과 그 운영의 경험에 비추어 국민의 자유와 권리가 과도하게 침해될 가능성이 있다는 시민단체와 정치권의 염려가 강했기 때문이다. 그럼에도 불구하고 지속적으로 국제적인 테러가 발생하는 상황에서 우리나라 역시 테러라는 국가와 공공의 안전에 대한 중대한 위해에서 예외일 수 없고 우리나라를 둘러싼 지정학적인 요인과 같은 타당성을 바탕으로, 테러로부터 국민을 보호하여야 한다는 공익과 기본권보장이라는 사익 사이의 균형과 조화를 바탕으로 악용의 소지를 줄여 통과시켜야 한다는 의견을 바탕으로 2016년 3월 국회 본회의를 거쳐 발효되었다.[7)]

---

5) 김희정, "대테러리즘, 자유와 안전", 한국공법학회, 공법연구 제44집 제4호, 2016, 113면.

6) 2016년 윤종호 의원 등 11인이 제출한 의안(의안번호:2004364), "테러 및 테러위험인물의 개념이 불명확하고 모호할 뿐 아니라, 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 추적과 같이 헌법상의 영장주의 원리, 적법절차의 원리 등 국민의 기본권 보호 원리를 무시하는 위헌적, 인권침해적 요소가 내포되어 있다."

테러방지법은 각 기관에 분산된 대테러업무를 국무총리 산하의 '국가테러대책위원회'로 일관하고 이를 중심으로 '대테러센터'를 통해 테러예방과 대응의 전담조직을 두어 테러대응조치를 하는 것을 주요 내용으로 하고 있다. 따라서 테러예방이라는 목적을 위해, 통신제한조치 혹은 통신감시조치 등이 이루어지기 때문에, 통신비밀보호와도 연관성이 높다.

(2) 통신제한조치의 유형

「테러방지법」은 제9조 제1항에서 테러위험인물에 대해 출입국·금융거래 및 통신이용 등 관련 정보를 수집할 수 있다고 규정하고 있으며, 이러한 해당 정보의 수집은 「출입국관리법」, 「관세법」, 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」, 「통신비밀보호법」의 절차를 따르도록 하고 있다. 여기에는 기존의 「통신제한조치」의 유형이 모두 포함되는 것으로 보인다. 「통신비밀보호법」의 경우 제7조의 '국가안보를 위한 통신제한조치' 혹은 제8조의 '긴급통신제한조치'의 규정을 따른다.

또한, 동조 제3항에서 국가정보원장이 테러위험인물에 대한 '개인정보'와 '위치정보'를 통신사업·정보사업자에게 요구할 수 있도록 하고 있다. 이는 「통신비밀보호법」 상의 '통신사실 확인요청'과 유사하다.

동조 제4항의 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 '추적'을 할 수 있는 '추적권'의 경우, '위치정보' 및 감청과 같은 통신제한조치가 여기에 해당하며, 이 역시 「통신비밀보호법」 제7조 혹은 제8조의 규정을 따르게 된다.

나아가 동법 제12조에서는 테러를 선동·선전하는 글 또는 그림, 상징적 표현물, 테러에 이용될 수 있는 폭발물 등 위험물 제조법 등이 인터넷이나 방송·신문, 게시판 등을 통해 유포될 경우 해당 기관의 장에게 긴급 삭제 또는 중단, 감독 등의 협조를 요청할 수 있는 권한이 있는데, 이는 통신비밀보호법 상의 검열에 유사하다. 다만 삭제, 중단 등의 협조요청에 대해 해당 기관의 거부나 이의신청에 대한 방법에 대해서는 구체

7) 김훈영, "테러방지법의 처벌규정에 대한 기본권 보장적 해석", 미국헌법연구 제30권 제3호, 2019, 302면.

적으로 나와 있지 않다.

3. 통신의 발달에 따른 비밀보호의 위기

최근의 통신환경변화는 통신비밀보호에 있어 중대한 위기상황으로 다가오고 있다. 이동통신서비스의 규격의 변화나 통신기술의 발달은 물론 SNS를 비롯한 새로운 통신서비스들이 등장하고 있으며, 이에 따라 통신비밀의 범위도 특정하기 매우 어려워졌다. 이러한 통신비밀의 위기는 결국 사생활의 자유 및 개인정보자기결정권에 영향을 미치게 된다. 이하에서는 이를 구체적으로 살펴본다.

(1) 통신기술의 발달

IT산업의 발달에 따른 인터넷 및 스마트폰의 대중화는 통신기계를 일부 사람들의 전유물이 아닌, 필수품으로 변모시켰다. 최신 통신기술의 발달과 인증시스템, 나아가 결제시스템으로의 확대 인격의 증명을 비롯하여 경제, 사회적 활동의 근간이 되고 있다. 기존에는 전화나 팩스, 이메일 등의 통신매체에 대한 비밀보호가 관건이었으나, 이제는 급속도로 다양화되고 빠르게 변화하는 통신매체 전반에 대한 비밀보호가 필요한 상황이 되었다.

개인이 소지하고 이용하는 통신기기와 통신매체에는 무선인터넷과 전자통신을 이용하여 클릭 한 번을 누르는 것만으로도 각종 데이터와 인격 및 금융, 사상에 대한 정보가 포함되어 있다. 예를 들어 인터넷과 같은 통신망을 통해 데이터를 전송하는 단위로 쓰이는 패킷[8]에는 개인의 사상·신념, 정치적 견해, 건강 등 정보주체의 사생활과 밀접한 관련이 있는 정보, 기업의 영업비밀과 같은 고부가가치를 지닌 정보, 국가의 존립을 좌우할 수 있는 정보 등이 포함될 수 있다.[9] 이는 결국 통신의 개인의 삶에 차지하는 비중과 영향력이 과거와 달라졌다는 데에 기인한다. 따라

8) 패킷은 패키지(package)와 버킷(bucket)의 합성어로서, 데이터를 전송할 때 송신측과 수신측에 하나의 단위가 되어 전송되는 집합체를 의미한다. 이메일, 채팅 메시지, 금융거래 등의 경우 패킷이 모여 데이터를 이루고 데이터가 모여 의미와 내용을 이룬다.

9) 이얼·박웅신, “인터넷 패킷감청의 현황과 과제”, 법학연구, 인하대학교 법학연구소, 2016, 3면.

서 통신의 비밀의 대상이 되는 통신수단을 단순히 나열하는 것은 아무런 실익이 없다.

통신침해의 방법에 대해서도 상당한 기술의 발전이 이루어져 있다. 이미 대부분의 범죄가 정보통신망과 정보통신기기를 매개로 계획·시행되고 있으며, 이에 대한 수사기관의 사전·사후 대응 또한 정보통신기기와 그 기기에 저장되어 있는 정보를 활용하고 있다.[10] 대표적으로 앞서 언급한 인터넷 패킷에 접근하여 수집하는 기법을 패킷분석이라 하는데, 수사기관이 패킷의 데이터 영역까지 심층 분석하고 재구성하여 범죄자의 통신 내용을 감청할 수 있다.[11] 문제는 패킷감청이 감청의 대상자와 감청의 범위를 실질적으로 특정하기 곤란하다는 데에 있다.[12] 즉, 패킷의 어느 부분이 통신의 비밀의 보호범위에 있는 정보인지, 아닌지를 수집 전에 구별할 방법은 아직 없기 때문에, 데이터 패킷감청이 이루어질 경우 통신의 자유 침해는 필연적으로 이루어질 수밖에 없다.[13]

(2) 새로운 통신서비스의 등장

각종 포털사이트, SNS(Social Network Services)와 같은 사회관계망 서비스, 모바일 앱, 온라인 메신저 등과 같은 새로운 통신서비스를 제공하는 매체들 역시 통신제한조치에 대상이 될 수 있다. 전자매체로서 기존에는 이메일 서비스와 같은 전자우편과 같은 대상이 주된 감청, 도청 및 통신사실관계에 대상이었다면, 앞서 언급한 새로운 통신매체에 기록되고 저장된 정보에는 개인의 취향, 건강상태, 개인의 사상 및 신념, 정

10) 이얼·박웅신, 앞의 논문, 3면.

11) 이를 심층패킷분석(Deep Packet Inspection, DPI)이라고 한다.

12) 이에 관한 비교법적 검토로는 박희영, 수사 목적의 암호통신감청(Quellen TKU)의 허용과 한계, 형사정책연구 29(2), 2018, 25면 이하 참조.

13) 헌법재판소는 2016헌마263 결정(2018. 8. 30.)에서 중대한 범죄수사를 위해 통신제한조치의 하나로 패킷감청의 필요성을 인정하면서도, 패킷감청은 그 기술적 특성으로 수사시관이 허가받은 범위 이상의 매우 광범위한 범위의 통신 자료를 취득하게 됨에도, 현행법상 집행 과정이나 그 이후에 객관적인 감독·통제 수단이나 감청자료의 처리 등을 확인할 수 있는 법적 장치가 제대로 마련되어 있지 아니하므로, 이러한 상태에서 패킷감청을 허용하는 것은 과잉금지원칙을 위반하여 청구인의 통신 및 사생활의 비밀과 자유를 침해한다고 판단하였다. 이에 관하여는 김현귀, 패킷감청에 대한 위헌심사 - 헌재 2018. 8. 30. 2016헌마263 결정을 중심으로 -, 헌법학연구 제25권 제2호, 2019, 49면 이하 참조.

치적 견해와 같은 정보주체의 사생활과 밀접한 관련이 있는 정보 등이 포함될 수 있다.[14)]

특히 스마트폰과 개인용 컴퓨터, 태블릿 PC가 대중화된 최근에는 일상을 공유하는 방식으로 데이터를 지불하는 경우가 많다. 업체는 이용자의 데이터를 이용하여 광고비를 받고, 새로운 서비스를 개발해 수익 창출에 나서며, 이는 이용자 정보를 세분하여 수집할수록 상품가치가 높아진다. 이러한 앱이나 프로그램을 이용한 사생활 데이터의 수집은, 사용자가 설치할 때 동의를 받아 해당 앱이나 프로그램이 실행 중에 생성되는 모든 데이터를 자동으로 전송하고 수집한다. 동의하지 않으면 앱이 설치되지 않거나 서비스를 이용받지 못하는 경우가 많기 때문에, 사실상 강제되는 경우로 볼 수 있다. 금융정보나 헬스정보 앱같은 경우에는 성별, 생년월일, 키, 몸무게, 걸음 수, 수면기록, 활동시간 등이 모두 수집되고 저장 및 전송되며, 앱에 따라서는 생리주기, 성관계 여부나 음식이나 약의 섭취정보, 물 섭취량 등과 같은 민감정보도 수집된다. 이러한 민감정보는 제3자 업체에 주고 활용되고 신규 서비스 개발에 쓰인다. 이러한 정보는 회원의 이메일이나 휴대전화 번호, 휴대전화 고유식별번호와 함께 결합하면 개별 식별도 가능하다. 서비스 이용을 위해 저장되는 통화 및 채팅과 같은 대화 내용도 이름, 연락처, 주소, 계좌번호 등이 서버에 저장될 수 있고, 이러한 데이터와 기록들은 앱개발 업체, 앱서비스 제공업체, 위

---

14) 헌법재판소 2018. 8. 30, 2016헌마263 : “헌법 제18조는 ‘모든 국민은 통신의 비밀을 침해받지 아니한다.’라고 규정하여 통신의 비밀 보호를 그 핵심내용으로 하는 통신의 자유를 기본권으로 보장하고 있다. 이 사건 법률조항은 현대 사회에 가장 널리 이용되는 의사소통 수단인 인터넷 통신망을 통해 송・수신하는 전기통신에 대한 감청을 범죄수사를 위한 통신제한조치의 하나로 정하고 있으므로, 일차적으로 헌법 제18조가 보장하는 통신의 비밀과 자유를 제한한다. 헌법 제17조에서 보장하는 사생활의 비밀이란 사생활에 관한 사항으로 일반인에게 아직 알려지지 아니하고 일반인의 감수성을 기준으로 할 때 공개를 원하지 않을 사항을 말한다. 감시, 도청, 비밀녹음, 비밀촬영 등에 의해 다른 사람의 사생활의 비밀을 탐지하거나 사생활의 평온을 침입하는 행위, 사적 사항의 무단 공개 등은 타인의 사생활의 비밀과 자유의 불가침을 해하는 것이다. 인터넷회선 감청은 해당 인터넷회선을 통하여 흐르는 모든 정보가 감청 대상이 되므로, 이를 통해 드러나게 되는 개인의 사생활 영역은 전화나 우편물 등을 통하여 교환되는 통신의 범위를 넘는다. 더욱이 오늘날 이메일, 메신저, 전화 등 통신뿐 아니라, 각종 구매, 게시물 등록, 금융서비스 이용 등 생활의 전 영역이 인터넷을 기반으로 이루어지기 때문에, 인터넷회선 감청은 타인과의 관계를 전제로 하는 개인의 사적 영역을 보호하려는 헌법 제18조의 통신의 비밀과 자유 외에 헌법 제17조의 사생활의 비밀과 자유도 제한하게 된다.”

탁처리업체 등에 이전되기도 한다. 광고사들은 개인의 핸드폰에 직접 접속하거나 앞선 업체들을 통해 정보의 대가를 지불하거나 수집하기도 한다.

다시 말해 SNS나 내비게이션, 각종 플랫폼 업체나 배달서비스, 데이팅 앱 등의 앱이 수집하는 정보는 가입정보, 작성 및 공유 콘텐츠, 전송 메시지 등 광범위한 데 비해, 이에 대해 어떤 내용이 어떻게 사용되고 거래되는지에 대해서는 거의 알려지거나 동의 없이 이루어지거나 동의가 있더라도 간략하게 이루어지는 경우가 많고, 앞서 살펴본 대로 동의를 하지 않으면 서비스 자체가 이용되지 않아서 사실상 강제된다. 이러한 서비스를 이용하여 기업이나 국가가 업무를 수행할 경우, 개인정보 및 기업의 영업비밀과 같은 정보, 국가기밀 정보 등이 포함될 가능성이 매우 크다. 이를 수사기관이 이용할 가능성 역시 매우 크다. 결과적으로 오늘날의 통신환경변화는 이용자의 통신의 자유 및 그와 연관성이 있는 기본권 침해 위험성을 증가시키고 있고, 이에 따라 이러한 침해의 위험성을 통제할 수 있도록 통신 비밀보호와 영장주의의 실질적 실현을 위한 제도적 마련이 필요하다.

(3) 사생활의 자유 및 개인정보자기결정권의 침해

이처럼 통신기술과 장비의 발달은, 통신을 통한 개인정보의 처리가 광범위하게 이루어지고 나아가 그것을 수집하는 기술 역시 광범위하게 이루어질 수 있다는 점에서 보호와 침해의 논의가 과거의 법리로는 한계가 있다고 평가할 수 있다.[15] 이는 결국 통신의 자유에 있어 보호법익을 단순

15) 헌법재판소 2001. 3. 21. 2000헌바25 : “헌법 제18조에서는 ‘모든 국민은 통신의 비밀을 침해받지 아니한다’라고 규정하여 통신의 비밀보호를 그 핵심내용으로 하는 통신의 자유를 기본권으로 보장하고 있다. 통신의 자유를 기본권으로서 보장하는 것은 사적 영역에 속하는 개인간의 의사소통을 사생활의 일부로서 보장하겠다는 취지에서 비롯된 것이라 할 것이다. 그런데 개인과 개인간의 관계를 전제로 하는 통신은 다른 사생활의 영역과 비교해 볼 때 국가에 의한 침해의 가능성이 매우 큰 영역이라 할 수 있다. 왜냐하면 오늘날 개인과 개인간의 사적인 의사소통은 공간적인 거리로 인해 우편이나 전기통신을 통하여 이루어지는 경우가 많은데, 이러한 우편이나 전기통신의 운영이 전통적으로 국가독점에서 출발하였기 때문이다. 사생활의 비밀과 자유에 포섭될 수 있는 사적 영역에 속하는 통신의 자유를 헌법이 별개의 조항을 통해서 기본권으로 보호하고 있는 이유는, 이와 같이 국가에 의한 침해의 가능성이 여타의 사적 영역보다 크기 때문이라고 할 수 있다.”

히 통신과 관련된 상황에 관련된 인격권으로 한정시킬 수 없다는 것을 의미한다. 즉, 일반적인 인격권 외에도, 정신활동과 관련된 양심, 종교, 표현, 학문의 자유 전반과 관련이 있다. 이러한 개별적인 정신활동은 자신의 의사에 반하여 공개되거나 공표되지 않기 때문에, 통신의 비밀을 보호하는 것은 이들의 자유를 보호를 위한 이중의 헌법적 보호라 할 수 있다.

또한, 통신을 이용할 때 표현되고 저장되어 있는 통신의 내용은, 정신활동을 포함하여 상당수가 사적 영역에 포함되어 있다.[16] 사생활의 비밀과 자유에 관하여는 헌법 17조에서 '침해받지 않는다.'고 명시하고 있는바, 통신의 내용이 사생활의 비밀에 관한 자유에 속할 경우 이 역시 통신의 자유와 연관이 있다. 일반적으로 사생활과 관련하여 특히 개인을 식별하는 개인정보, 즉 성명, 나이, 생년월일, 키, 생김새, 주고, 몸무게, 전화번호, 주민번호, 가족관계, 병력[17] 등은, 사생활 비밀의 영역에 속하여 헌법 17조에 의해서도 보호된다고 한다. 정보사회에서는 이러한 내용이 통신을 통해 교류, 교환 및 저장되는데, 이 과정에서 통신의 자유가 침해되는 경우가 발생할 수 있다.

나아가 사생활의 자유를 논함에서, 사생활의 여부에 대한 사적 영역에 대한 판단기준으로서 비밀성에 대한 중요한 기준은 '공개 여부에 대한 본인의 의사'이다. 이 의사에 기인하여 사생활의 정보에 대한 통제권을 인정하는 '개인정보자기결정권[18]'이 인정되고 있는바, 헌법상 통신의 자유가 침해되는 경우 사생활의 비밀 그 중에도 특히 개인정보자기결정권에 대한 침해는 밀접한 연관성을 가지게 된다. 따라서 통신의 자유를 침해하고 이를 통해 습득된 사적인 정보가 침해되어 개인정보자기결정권이 침해되었다면, 통신의 자유의 침해사실에 대한 '확인'과 '열람'이 가능하

16) 헌법재판소 2001. 3. 21. 2000헌바25 : "헌법 제18조에서 그 비밀을 보호하는 '통신'의 일반적인 속성으로는 '당사자간의 동의', '비공개성', '당사자의 특정성'등을 들 수 있는바, 이를 염두에 둘 때 위 헌법조항이 규정하고 있는 '통신'의 의미는 '비공개를 전제로 하는 쌍방향적인 의사소통'이라고 할 수 있다."

17) 헌법재판소 2007. 5. 31. 2005헌마1139.

18) 헌법재판소 2005. 5. 26. 99헌마513 : "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다."

며, 침해된 정보의 '수정'이나 '삭제'를 요구할 수 있으며, 공개의 목적 외로 통신을 통한 자신의 정보가 사용될 경우 '사용중지' 역시 요구될 수 있다. 최근 2019년과 2021년 개정을 통해 '통신사실 확인자료'제공을 받은 사실과 제공요청기관 및 그 기간에 대해 대상이 된 당사자에게 서면으로 통지하게 한 「통신비밀보호법」 제13조의3은 이러한 '개인정보자기결정권'의 관점이 입법에 반영된 것으로 보인다.[19] 그러나 침해된 개인정보가 수사기관 소기의 목적을 달성한 이후에 '변경' 혹은 '삭제'를 요구할 수 있는 규정은 존재하지 않기 때문에, 「통신비밀보호법」상에서 개인정보자기결정권이 완전히 구현되었다고 보기는 이르다.

4. 영장주의의 새로운 위기

영장주의 역시 통신기술의 발달과 마찬가지로 다양한 수사기법의 등장에 따라, 그 도입 당시에는 예정하지 않은 적용의 문제가 생기고 있다. 우선 통신비밀보호와 영장주의와 관련해서는 구속과 체포와 같은 인신의 자유보다는 대물적 영장인 압수·수색·검증의 연관성이 높다. 새로운 수사기법 역시 과학통신기술의 발달에 따른 수색과 관련된 부분이 영장주의와 어떻게 해석되고 포섭될 수 있는지 여부가 난제로 꼽힌다.[20]

이와 관련하여서는 우선 「통신비밀보호법」 상의 '통신사실 확인자료

---

19) 헌법재판소에 따르면 기지국수사란 특정 시간대 특정 기지국에서 발신된 모든 전화번호 등을 통신사실 확인자료로 제공받는 수사방식이며, 주로 수사기관이 용의자를 특정하기 어려운 연쇄범죄가 발생하거나 동일 사건 단서가 여러 지역에서 시차를 두고 발견된 경우, 사건발생지역 기지국에서 발신된 전화번호들을 추적하여 용의자를 좁혀나가는 수사기법으로 활용된다. 실체진실의 발견과 국가형벌권의 적정한 행사를 위하여, 이러한 기지국수사를 일정 요건 하에 허용할 필요성이 있다. 그런데 이 사건 요청조항은 그 요건으로 '수사의 필요성'만 규정하고 있기 때문에, 수사기관의 입장에서 수사의 필요성이 있는 경우라면 법원은 허가할 수밖에 없게 되었다. 그 결과 수사기관의 통신사실 확인자료 제공요청 허가신청에 대한 법원의 기각률은 약 1%에 불과하여, 수사기관의 권한남용과 정보주체의 기본권침해가 우려되는 상황에 이르게 되었다. 이에 헌법재판소는 2012헌마538 결정(2018.6.28.)에서, 범죄예방과 사건의 조기해결을 위해 수사기관의 기지국수사의 필요성을 인정하면서도, 그 요건을 현재의 '수사의 필요성'보다 더 강화함으로써, 범죄수사라는 공익과 정보주체의 기본권 보호라는 사익이 조화되어야 한다는 점을 선언하였다. 이에 관하여는 박종현, 「통신비밀보호법」상 통신사실 확인자료 제공관련 조항들에 대한 헌법적 검토 - 2018.6.28. 2012헌마191등 결정례와 2018. 6. 28. 2012헌마538 결정례에 대한 검토를 중심으로 -, 헌법학연구 제25권 제2호, 2019, 6면 이하 참조.

20) 헌법재판연구소, 영장주의에 관한 헌법적 연구, 2019, 59면 이하.

제공'의 범주에 들어가는지를 살펴보고, 나아가 압수·수색이 동시에 이루어지는 수사관행에 있어 영장이 보장하는 통신비밀보호의 범위는 어디까지인지 그 한계를 논의해 볼 필요가 있다.

(1) 새로운 수사기법을 적용한 수색과 영장주의

첨단과학기술의 발전은 다양한 수사기법의 등장으로 이어졌고, 정보수사기관과 같은 국가의 기본권제한의 형태는 이러한 기술의 변화와 함께 과거에 비해 예상하기 어려울 정도로 달라지고 있다. 감청, 전기통신사업자를 상대로 한 통신사실 확인자료 제공요청, GPS 장치를 부착한 웨어러블 장비나 스마트폰에 탑재된 GPS 기능을 활용한 위치추적은 그 좋은 예이다.[21] 각각의 감청 및 통신제한기법을 이용하면 대상자의 기본권을 침해하지 않을 수 없으므로, 그 법적 성격은 강제수사이다.[22]

나아가 이러한 정보의 전달, 처리에 있어 첨단수사기법을 통한 개인정보의 수집 및 수색, 압수 등은, 해당 정보주체들이 이에 관하여 전혀 알지 못하게 이루어지거나, 안다고 하더라도 이것이 자신의 기본권 제한과 침해에 해당하는지에 대해 인지하기 어렵다.[23] 대표적으로 인터넷 패킷이나 스마트폰 등에 저장된 앱의 정보를 이용한 정보가 그러하다. 자동화된 정보처리를 통하여 공간적으로 떨어져 있는 다른 정보에 수사기관이 순식간에 접근할 수 있으며 이것으로부터 정보가 원래 저장되었던 목적과는 다른 목적으로 이용되거나 기존의 정보와 결합하여 개인정보자기결정권을 침해할 위험성이 높아졌다.[24] 이는 개별적인 국가기관이나 별도의 정보통신사업자가 개인정보를 조사, 저장하고 있다고 하더라도, 행정이 이용하려는 목적에 따라 수사기관이 각각의 정보를 모아 그것을 조합하여 새로운 정보를 생산, 가공, 전달할 가능성이 커졌다는 것을 의미

---

21) 이에 관하여는 이흔재, 독일의 휴대전화 위치정보 추적수사와 당사자에 대한 통보제도 - 통신비밀보호법 일부개정법률안에 대한 평가와 개선방안을 중심으로 -, 법조 제68권 제4호(통권 제736호), 2019, 497면 이하 참조.

22) 이진구, "통신비밀의 보호범위와 한계에 관한 헌법상 연구", 2016, 성균관대학교 박사논문, 114면.

23) 이진구, 앞의 논문, 98면.

24) 김일환, "행정정보의 공동이용으로부터 정보자기결정권의 보호에 관한 헌법상 고찰", 공법연구, 제32집 제4호, 2004 참조.

한다. 이는 수사대상자에 대한 통신의 자유, 개인정보자기결정권, 인격권 등에 대한 포괄적이고 상당한 위기로 이어질 수 있다.[25]

(2) 포괄적 영장에 대한 남용 통제

우리 헌법과 형사소송법에서는 일반영장을 금하고 내용을 특정하여 영장을 발부받을 것을 요구하고 있으나, 일선 실무에서는 '범죄행위와 관련하여 작성보관 중인 수첩 등'처럼 수사기관에게 압수·수색의 대상 선별에 상당한 재량을 주는 압수·수색영장이 발부되고 있는 것이 현실이다.[26] 이러한 상당한 재량이 가능한 영장에 대해 실질적으로 일반영장과 같은 포괄적 영장과 다를 바 없다는 비판이 가능하다. 또한, 통신기기의 발달로 스마트폰이나 태블릿 PC, 컴퓨터 등에 대한 압수·수색의 경우 표면적으로 대상을 특정하더라도 포괄적인 성격의 일반영장이 발행되기 쉽고. 이러한 이유에서 영장의 특정성 요건이 컴퓨터 저장장치의 수색에 있어 충분한 보호를 제공하지 못한다는 비판도 존재한다.[27] 특히 실무상으로는 이와 같은 통신기기에 대한 압수를 임의제출의 형식으로 이루어지는 경우도 많은데, 이러한 방법이 영장주의를 우회하는 방법으로 사용된다면 사실상의 강제력에 기한 강제집행으로 위헌적 방식이라 할 수 있다.

압수의 집행 방식뿐만 아니라, 수색에서도 컴퓨터나 휴대용 통신기기 속에는 다양한 개인정보가 존재하는데, 특정성을 결여하여 저장된 전반에 데이터에 대한 포렌식 분석이 이루어질 가능성이 크다. 이 경우 역시 내용을 특정해야 하는 영장주의의 원칙에 비추어봤을 때 헌법 제37조 제2항에 반하는 것이 될 수 있다. 통신비밀보호와 관련해서는 인터넷 패킷감청이 대표적인 포괄적 수색의 위험이 큰 경우로 꼽힌다.[28] 감청 대

25) 헌재 2005. 5. 26. 2004헌마190.

26) 설민수, "피의자 보관 전자정보의 압수·수색에서 미국과 한국 법원의 영장주의 적용과 변화과정: 이미징을 중심으로", 형사법의 신동향, 통권 제53호, 대검찰청, 2016, 102면.

27) Orin S. Kerr, "Searches and Seizures in a digital World", Harvard Law Review, Vol. 119, No. 2, 2005, pp. 565-566.

28) 헌법재판소는 통신제한조치 허가 위헌확인 등[2018. 8. 30. 2016헌마263] 결정에서 중대한 범죄수사를 위해 통신제한조치의 하나로 패킷감청의 필요성을 인정하면서도, 패킷감청은 그 기술적 특성으로 수사시관이 허가받은 범위 이상의 매우 광범위한 범위의 통신 자료를 취득하게 됨에도, 현행법상 집행 과정이나 그 이후에 객관적인 감독·통제 수단이나 감청자료의 처리 등을 확인할 수 있는 법적 장치가 제대로 마련되어 있지 아니하므로, 이

상자와 감청의 범위가 특정되기 어렵기 때문이다.[29]

(3) 테러 등 국가안보의 위협

21세기 들어서면서 현대 국가는 테러리즘이라는 극단적인 폭력 현상으로 인해 위험 관리에 있어 더 큰 도전에 직면하고 있다. 테러행위는 목적성, 폭력성을 가지며, 일반인 혹은 대중을 대상으로 하기에 불법성이 가중된다.[30]

9·11사건 이후의 미국과 시리아 내전으로 본격화된 이슬람 급진세력의 테러가 일어난 유럽은, 더 이상 사후적인 방식으로는 테러를 억제할 수 없다고 보고 예방의 차원에서 테러리스트와 테러단체를 억제해왔다. 즉, 현대의 테러리즘이 과거와 달리 정치적인 명분이나 협상에 집착하지 않고, 순교적 방식의 대량살상을 수행하는 것으로 성격이 변화하면서, 테러에 대응하기 위한 법률 역시 그 성격이 변하였다.[31]

예상할 수 없는 장소에서 벌어지는 테러는 많은 국가들로 하여금 대응 시나리오를 준비하게 하고, 기존 헌법에서 자유권으로 보호되던 가치들에 대해 예외를 부여하고 있다. 테러공격에 대한 공포와 그 공포에 대한 정치적 선전은 전쟁의 정당성과 비상상황의 논리에 대한 저항을 누그러뜨리고, 국가의 행위에 대한 규범적 한계나 논리를 계속 시험대에 올리며, 자유와 안전에 있어 수단의 적절성과 최소 필요성이라는 헌법상 형량의 틀을 조정하고, 그 조정된 틀을 일상화하고 있다.[32] 이 중 국가안보와 공공의 안전을 위해 기존의 영장주의가 후퇴하는 동향은 미국의 「애국법」이 대표적이라 할 수 있다. 「애국법」에서는 사전 통지 없이 집과 사무실을 수색하고, 변호사와 의뢰인의 대화를 감청하거나, 전자 감시 영장이나 수색영장의 요건을 완화하고 있어, 사실상 영장주의에 대한

러한 상태에서 패킷감청을 허용하는 것은 과잉금지원칙을 위반하여 청구인의 통신 및 사생활의 비밀과 자유를 침해한다고 판단하였다.

29) 민만기, “인터넷 패킷감청의 법적 성격 및 허용 가능성 검토”, 형사법의 신동향, 통권 제53호, 대검찰청, 2016, 216-218, 236-237면.

30) 김훈영, 앞의 논문, 309면.

31) 김희정, 앞의 논문, 101면.

32) 김희정, 앞의 논문, 101면.

전면적인 후퇴양상을 보이고 있다. 뿐만 아니라 개인이 이용하는 인터넷이나 해외에서 사용하는 전자통신망에 대해 사실상의 포괄적인 통신감시조치가 이루어지는 등 테러수사와 정보수집에 관한 막대한 권한이 국가기관에 부여되었다. 국가안보를 위한 테러의 예방은, 국가가 시민을 보호하고 자유를 수호하기 위해 예외적인 상황에 부여된 권한들을 위험의 실현 여부와 관계없이 앞당긴다. 테러의 발생 가능성의 명분으로 예외적인 정보수사기관의 권한이 상시적으로 정당화되고 더욱 효과적이고 강력한 수단이 도입될 가능성이 있다. 더구나 테러와 관련 있는 단체와 개인을 찾기 위해 광범위한 통신비밀의 침해와 사생활의 침해가 상시적으로 이루어진다면, 그 자체가 오히려 헌법질서라는 공공질서에 대한 상시적인 위협이 될 수 있다.

Ⅲ. 통신비밀보호의 강화를 위한 법제정비방안

1. 통신비밀보호법상의 개인정보자기결정권

비록 일반법의 위치에서 「개인정보 보호법」이 존재하고 적용된다고 하더라도 「통신비밀보호법」상에서 정보주체의 '개인정보자기결정권에 대한 원칙'을 다룬 조문은 현재 없다.[33] 따라서 「통신비밀보호법」에서는 '개인정보자기결정권'이 간접적으로 반영되어 있는데, 대표적으로 통신감시조치사실에 대한 '통지규정'이 있다. 통신감시조치에 대한 통지는, 통신제한조치의 절차에서 규정하고 있다. 먼저 통신제한조치의 집행은 「통신비밀보호법」 제9조 제1항에 의해 통신제한조치를 청구 또는 신청한 검사 또는 사법경찰관이 한다. 집행 후에는 「통신비밀보호법 시행령」 제18조 제1항에 따라 집행경위, 취득한 결과의 요지를 조서로 작성하고, 이에 대한 비밀보호 및 훼손·조작의 방지를 위하여 봉인·열람제한 등의 적절한 보존조치가 이루어져야 한다. 이후 동법 제9조의2에 따라 통신제한조치를 종료한 날부터, 30일 이내에 그 대상자에게 집행사실과

33) 개인정보보호에 관한 일반법과 특별법 관계에 대하여는 김일환, 개인정보보호 법제 정합성 강화를 위한 고찰 - 정보통신망법과 신용정보법을 중심으로 -, 단국대학교 법학연구소 법학논총 제42권 제1호, 2018, 255면 이하 참조.

집행기관 및 그 기간 등을 서면으로 통지를 해야 한다. 이러한 규정은 감청이 이루어질 것이라는 점에 대한 사전통지가 있는 경우 감청의 목적이 달성될 수 없는 불가피한 측면이 있어 감청의 비밀처분성을 인정하면서도 사후적으로나마 피감청자의 권리를 보장하기 위한 규정으로 보인다. 또한, 통지제도는 불법적인 경우 피감청자의 국가배상청구가 용이하도록 하는 점, 수사기관 등의 감청에 대한 남용을 방지하는 점 등에도 중요한 의미가 있다. 그러나 무엇보다도 자신의 정보에 대해 스스로 인지할 권리는 개인정보자기결정권의 영향임을 부정할 수 없다.

통신비밀보호에서 헌법이 보호하는 통신이란 '의사소통'이며 보호이익은 '의사소통의 신뢰'이다.[34] 따라서 의사소통의 실제 당사자의 비밀을 보호하는 것이 통지제도의 취지라고 해석되므로 통지의 상대방은 감청의 대상자라 할 것이다.[35] 그러나 현행 「통신비밀보호법」 제9조의2에 의하면 감청집행에 관한 통지의 상대방은 우편물 검열의 경우에는 그 '대상자'로 문제가 없지만, 감청의 경우에는 그 대상이 된 '전기통신의 가입자'로 규정되어 있다. 이는 실제 이용자와 전기통신의 가입자가 다른 경우에 문제가 될 수 있다. 감청의 경우와 달리 통신사실 확인자료의 통지의 경우 「통신비밀보호법」 제13조의3에서 통신사실 확인자료제공의 '대상이 된 당사자'에게 서면으로 통지하여야 한다고 규정하고 있다. 따라서 감청의 경우에도 동일하게 개정될 필요가 있다.

2. 통신감시조치시 영장주의의 강화

통신비밀보호는 헌법이 보장하는 기본권으로써, 영장주의에 의해 제도적 보호를 보장받는다. 그러나 다른 자유권과 마찬가지로 통신비밀보호는 절대적으로 보호되는 권리가 아니라 일정한 예외로 국가에 의해 제한될 수 있으며, 따라서 현행 헌법은 제37조 제2항에서 이러한 제한의 방

34) 헌법재판소 2001. 3. 21. 2000헌바25 : "헌법 제18조에서 그 비밀을 보호하는 '통신'의 일반적인 속성으로는 '당사자간의 동의', '비공개성', '당사자의 특정성'등을 들 수 있는바, 이를 염두에 둘 때 위 헌법조항이 규정하고 있는 '통신'의 의미는 '비공개를 전제로 하는 쌍방향적인 의사소통'이라고 할 수 있다."

35) 「통신비밀보호법」 제2조의 정의 규정에 의하면, 여기서 "당사자"라 함은 우편물의 발송인과 수취인, 전기통신의 송신인과 수신인을 말한다.

법과 절차를 법률로서 제한할 수 있도록 명시하고 있다. 또한 헌법은 국가기관이 강제처분을 함에 있어서 중립적인 법관이 구체적 판단을 거쳐 발부한 영장에 의하여야만 한다는 영장주의를 요구하고 있으며,[36] 구체적인 영장의 신청 및 집행 등의 사안은 법률에 근거한다. 따라서 통신비밀보호에 있어도 그 제한이나 침해(즉, 통신감시조치)가 이루어진다면, 구체적인 법률에 근거한 영장제도에 따라 이루어져야 한다는 것이 헌법이 요구한 사안이다.

통신비밀보호에서 이러한 통신제한조치를 다루고 있는 구체적 법률은 「통신비밀보호법」과 「국민보호와 공공안전을 위한 테러방지법(이하 테러방지법)」이다. 앞서 제2장에서 살펴본 바와 같이 이상의 법률들은 변화하는 통신환경, 수사환경의 변화와 국가안보의 위협과 같은 영장주의의 위기 속에 놓여있다. 따라서 이하에서는 이 법률에 대한 헌법상의 영장주의 요청을 어떻게 지켜갈 수 있을지에 대해 논의해본다.

(1) 통신비밀보호법과 영장주의 강화

「통신비밀보호법」 제3조 제1항은 "누구든지 이 법과 「형사소송법」 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실 확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다."라고 규정하여 통신감시조치를 검열·감청 및 통신사실 확인조치로 구분하고 이를 원칙적으로 금지한다. 「통신비밀보호법」은 이를 위반할 경우 동법 제16조와 제17조에서 처벌규정을 마련하고 있어 실효성을 확보하려 노력하고 있다.

통신제한조치는 ① 제5조와 제6조 그리고 제12조2와 제13조, 제13조의3에서 범죄수사를 위한 경우, ② 제7조와 제13조의4에서 국가안보를 위한 경우로 법원의 허가를 받아 허용이 되며, ③ 제8조에서 규정한 긴급통신제한조치도 가능하다. 이하에서는 이상의 분류를 기준으로 핸드폰과 같은 휴대용 통신기기가 「통신비밀보호법」상의 보호범위에 속하는지를 검토해보고, 감청조치와 통신자료 사실확인 조치를 구분하여 통신의 비밀보호와 영장주의의 헌법적 발현 방안을 검토한다.

---

36) 헌재 1997. 3. 27. 96헌바28; 헌재 2012. 12. 27. 2007헌마1468 등.

1) 통신기기에 대한 감시조치와 영장주의

가) 통신기기의 포섭여부

「통신비밀보호법」 제2조 제1호에서 "통신"을 정의하면서, "'통신'이라 함은 우편물 및 전기통신을 말한다"고 규정하고 있으며, 동조 제3항에서 "'전기통신'이라 함은 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다"고 구체적으로 기술하고 있다. 이러한 「통신비밀보호법」의 기술을 살펴보면 "모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것"에 무선통신기능이 설치되어 있는 컴퓨터나, 핸드폰 및 태블릿 PC와 같은 휴대용 무선장치들 역시 동법이 규정하는 '전기통신'의 방법을 이용하는 장치로 「통신비밀보호법」의 보호범위에 포함된다는 해석이 가능하다. 따라서 피의자나 조사자의 휴대용 무선장치에 대해 범죄수사와 관련된 데이터를 수집하는 조치는, 「통신비밀보호법」상의 절차를 따르는 것이 타당해 보인다.

나) 통신기기에 대한 감시조치와 영장주의

「통신비밀보호법」에서 통신기기가 통신의 비밀보호의 범위에 포함되게 되면, 통신기기를 통해 지득하게 된 개인보호와 데이터들은 영장심사를 통해 정당화되게 된다. 앞서 살펴본 바와 같이 통신기기에 포함된 데이터들은 개인정보의 성격을 가지며 광범위하게 개인의 사생활과 연관성을 가지고 있다. 통신기기에 대한 개인정보자기결정권에는 기기 자체에 대한 정보주체의 권리뿐만 아니라 기기에 저장된 내용에 대한 정보주체의 권리도 포함된다. 따라서 통신기기에 대해 압수하여 수색하는 「형사소송법」상의 방법이 아니라, 원거리에서 통신기기에 접속하여 통신기기에 담겨있는 개인정보(메타데이터 수집행위)에 대해 모니터링하는 행위에도 당연히 영장이 필요하게 된다. 이는 「통신비밀보호법」 제2조에서 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 감청의 사례에 부합한다. 따라서 이러한 메

타데이터 수집행위의 경우 「통신비밀보호법」 제6조에 제5항 따라 통신제한조치의 종류·그 목적·대상·범위·기간 및 집행장소와 방법을 특정하여 기재하여야 하며, 동조 제7항에 의해 통신제한조치의 목적이 달성되었을 경우에는 즉시 종료하여야 한다. 동법 제12조에 의해 이를 통해 취득한 전기통신의 내용은 통신제한조치의 목적이 된 범죄나 이와 관련된 범죄를 수사·소추하거나 그 범죄를 예방하기 위하여 사용하는 경우를 제외하고는 사용될 수 없음은 물론이다. 전자정보에 대한 통신제한조치를 통한 수집은, 사생활의 비밀과 자유, 개인정보자기결정권, 재산권 등을 침해할 우려가 크므로 포괄적으로 이루어져서는 아니 되고 비례의 원칙에 따라 필요한 최소한의 범위 내에서 이루어져야 한다.

2) 범죄 수사를 위한 통신감시조치

가) 감청 조치와 관련하여

「통신비밀보호법」 제2조 제7호는 "감청"에 대해 "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 것"으로 정의되어 있다. 이와 같은 감청조치의 허가는 동법 제5조 제1항에 기술된 주요 범죄에 한하며, 동조 제1항에 명시되어 있는 요건은 다음과 같다.

첫째, 감청대상이 되는 "범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유"가 있어야 한다. 여기서 '계획'이란 형법상 '예비'와 '음모'보다 광범위한 개념으로 이해되며, 따라서 적어도 일정한 범죄를 지향하고 있는 사실이 객관적으로 인정될 수 있어야 한다.[37] 이는 "죄를 범하였다고 의심할 만한" 경우에 체포·구속·압수·수색을 인정하는 「형사소송법」 제200조의2 제1항, 제201조 제1항, 제215조 제1항과 비교해 볼 때, 다소 완화된 요건으로 보인다.

또한 「통신비밀보호법」상 '충분한 이유'를, 「형사소송법」 제200조의2 제1항, 제201조 제1항의 체포·구속의 경우 '의심할 만한 상당한 이

37) 권영세, "현행법상 도청에 관한 법적 규제: 통신비밀보호법을 중심으로", 서울대학교 대학원, 법학석사학위논문, 1997, 71면.

유' 그리고 「형사소송법」 제215조 제1항의 압수·수색의 경우는 각각 '의심할 만한 정황'과 비교하여 그 정도를 파악할 필요가 있다. 생각건대 감청조치가 체포·구속의 경우와 같이 신체의 자유에 대한 침해는 아니므로 '의심할만한 상당한 이유'보다 완화한 것으로 해석하는 것이 타당하다고 보인다.[38] 압수·수색의 경우에도 '의심할 만한 정황'과 동시에 '해당 사건과 관계가 있다고 인정할 수 있는 것'에 한하여 영장을 청구하도록 규정하고 있으므로, 감청조치 역시 그 조치를 통해 범죄사실에 대한 정보와 증거를 확보하는 것이므로 「통신비밀보호법」상 '상당한 이유'는 이와 유사한 기준으로 해석되어야 할 것이다.

추가로 '상당한 이유'에 대한 구체적인 해석과 관련해, 독일의 「형사소송법」 제100c조(주거에 관한 감청)[39] 및 제100f조(주거 외에 대한 감청)[40]의 논의를 고려해볼 필요가 있다. 이상의 조항에서 독일 「형사소송법」은 '범죄 혐의의 근거가 되는 사실'을 요구하고 있고, 이에 대해 '다른 피의자의 사실이 있는 경우' 또는 '다른 사람의 진술이 중대한 것으로 판단되는 경우'로 구체화하고 있다. 따라서 현행 「통신비밀보호법」 제5조의 '충분한 이유'의 해석에 있어도 이러한 '사실'을 근거로 하는 것이 통신비밀보호라는 헌법목적에 보다 부합해 보인다.

둘째, "다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여" 허가된다는 보충성이 요구된다. 다른 방법으로는 어려운 경우에 한한다는 보충성의 원칙 자체는, 「형사소송법」 규정과 비교하고 동일한 요건을 필요로 하는 미국과 독

38) 이재상·조균석, 형사소송법, 박영사, 2017, 314면.

39) 주거에 대한 감청은 독일 「형사소송법」 제100 c조에서 별도로 규정하고 있다. 이 조항에 따르면 수사상 중요한 단서를 포착할 수 있을 필요성과 다른 방식으로는 수사가 현저히 어려운 경우 등과 같은 보충성 요건이 만족되어야 한다. 제100 c조 제5항에서는 특히 감청 중 개인의 생활영역의 핵심영역에 속하는 표현이 포착될 경우에는 즉시 중단하도록 규정하고 있으며, 그 기록은 즉시 삭제하여야 하고, 의문이 있을 때에는 법원의 결정을 구하여야 하는 등 엄격한 절차를 규정하고 있다.

40) 주거 외에서의 도청은 독일 「형사소송법」 제100 f조를 따른다. 주거 외에서의 도청은, 동법 제100 a조에 규정된 범죄가 되는 경우, 다른 피의자의 사실이 있는 경우, 또는 다른 사람의 진술이 중대한 것으로 판단되는 경우에 기술적 수단으로 이루어 질 수 있다. 이러한 감청은 피의자 한 명만을 대상으로 이루어지는 것이 원칙이지만, 제3자가 불가피하게 영향을 받는 경우 역시 예외적으로 시행될 수 있다.

일의 규정에 비추어봤을 때 합리적으로 보인다. 다만, 보충성 원칙의 요건으로 '사실관계의 조사'와 '피의자의 소재에 대한 수사'를 규정하는 독일의 사례에 비해 '범죄의 실행을 저지'하기 위한 요건이 적합한지에 대한 비판이 존재한다.[41] 이는 현행 「통신비밀보호법」상의 통신감시조치가 '수사절차상의 목적'임을 전제로 하고 있는 것으로, 일반 예방적인 성격의 포괄적인 통신감시조치는 당연히 포함되지 않는 것으로 해석되어야 한다. 따라서 이러한 논의를 명확히 맺기 위해서는 「통신비밀보호법」 제5조의 "범죄를 계획"의 부분을 형법상 예비와 음모의 범위로 축소하는 해석을 도입할 필요가 있다.

나) 통신사실 확인조치와 관련하여

「통신비밀보호법」 제2조 제11호에서는 '통신사실 확인자료'를 정의하면서, ① 가입자의 전기통신일시, ② 전기통신개시·종료시간, ③ 발·착신 통신번호 등 상대방의 가입자번호, ④ 사용도수, ⑤ 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, ⑥ 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, ⑦ 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료로 열거하고 있다. 이러한 자료들은 전기적인 데이터 형태로 통신회사의 서버나 저장장치에 기록되어 있는데, 「통신비밀보호법」 제13조의 범죄수사를 위한 '통신사실 확인자료'제공의 절차를 거쳐 전기통신사업자에게 '통신사실 확인자료'의 열람이나 제출을 요청한다.[42]

특히 동법 제13조 제2항에서 규정한 '위치추적자료 중 실시간 추적자료' 및 '특정한 기지국에 대한 통신사실 확인자료'의 경우, "다른 방법으로는 범죄의 실행을 저지하기 어렵거나 범인의 발견·확보 또는 증거의 수집·보전이 어려운 경우에만" 전기통신사업자에게 해당 자료의 열람이나 제출을 요청할 수 있다. 이러한 '통신사실 확인자료'는 서면으로 관한

41) 권영세, 앞의 논문, 75면.

42) 이에 관하여는 차진아, 범죄수사를 위한 통신사실확인자료 제공요청의 문제점과 개선방안, 법조 통권 제728호, 2018, 388면 이하 참조.

지방법원이나 지원의 허가를 받아야 하여, 허가받지 못할 경우 제13조 제4항에 따라 지체없이 폐기되도록 하고 있다.

그러나 '통신사실 확인자료'가 광범위하게 대중을 대상으로 이루어지기 쉽고, 특히 '접속지 추적자료'나 '실시간 확인자료'의 경우 범인의 발견·확보 또는 증거의 수집·보전을 위해 일정 구역에 있는 불특정 다수에 대한 열람이나 제출이 요구될 수 있고, 범죄의 연관성만 입증되면 1개의 허가서로도 피의자 본인은 물론 타인의 통신사실 확인자료까지도 요청할 수 있는 현행 규정의 남용 가능성이 제기된다. 비록 초기 범죄 혐의자 선별을 위해 이러한 일괄적인 청구의 필요성이 존재한다고 하더라도, 긴급한 경우 즉 범죄의 실행을 저지하기 위함이 아닌 한 그 통신제한조치의 대상을 최소한으로 한정할 수 있는 개별 청구의 방식을 도입하는 것이 타당하다.

다) 기간과 관련하여

통신제한조치는 「통신비밀보호법」 제6조에서 집행과 관련된 기간을 규정하고 있는데, 현재는 2개월을 초과하기 못하고, 소명자료를 첨부하여 2개월의 범위에서 연장이 가능하도록 규정하고 있다.[43] 이에 대해 '기본권제한의 최소화'의 관점[44]에서 기간을 더욱 단축하자는 의견이 있을 수 있지만, 생각건대 통신제한조치는 ① 범죄의 특성상 단기간의 내사를 통해서는 관련자 색출이 사실상 불가능한 범죄들이 있고, ② 법원의 제한조치 허가 시 사건의 성격에 따라 법규정상의 허가기간보다 단기간의 허가를 할 수 있기 때문에, 이를 더욱 단축할 필요는 없어 보인다.

---

43) 헌법재판소 2010. 12. 28. 2009헌가30 결정에서 재판관 4(헌법불합치) : 2(단순위헌) : 3(합헌)의 의견으로 통신제한조치기간의 연장을 허가함에 있어 총기간 내지 총연장횟수의 제한을 두지 않고 무제한 연장을 허가할 수 있도록 규정한 통신비밀보호법 제6조 제7항 단서 중 전기통신에 관한 '통신제한조치기간의 연장'에 관한 부분이 과잉금지원칙을 위반하여 청구인의 통신의 비밀을 침해하는 법률로서 헌법에 합치하지 아니한다는 결정을 선고하였다.

44) 헌재 1989. 12. 22. 88헌가13 : "비례의 원칙 혹은 과잉금지의 원칙은 국가작용의 한계를 명시하는 것인데 목적의 정당성, 방법의 적정성, 피해의 최소성, 법익의 균형성(보호하려는 공익이 침해되는 사익보다 더 커야 한다는 것으로서 그래야만 수인(수인)의 기대가능성이 있다는 것)을 의미하는 것으로서 그 어느 하나에라도 저촉되면 위헌이 된다는 헌법상의 원칙이다."

독일의 경우에도 감청의 경우 3개월로 규정하고 있으며, 1회의 연장이 가능하다. 오히려 현행 「통신비밀보호법」에 의하면 2개월인 대신 연장의 횟수의 제한이 없으므로, 이를 제한하는 것이 더 '기본권제한의 최소화' 관점에서는 시급해 보인다. 한편 독일의 경우 모바일 기기에 대한 기술적 조치의 경우 6개월(연장 시 6개월), 온라인 수색이나 주거 외에서의 감청의 경우 1개월(연장 시 1개월씩 총6개월)과 같이 다양하게 기간을 설정하고 있는 바, 우리의 경우도 통신제한조치의 유형에 따라 다양한 기간을 두는 것이 필요하다.

3) 국가안보를 위한 통신제한조치

가) 감청조치와 관련하여

국가안보를 위한 통신제한조치는 「통신비밀보호법」 제7조에 규정되어 있다. 국가안전보장에 상당한 위험이 예상되는 경우와 후술할 「국민보호와 공공안전을 위한 테러방지법」상의 대테러활동에 필요한 경우에 한하여 그 위해를 방지하기 위한 정보수집이 필요할 때 통신제한조치를 허용하고 있다. 이 경우 통신의 일방 또는 쌍방당사자가 내국인인 때에는 고등법원 수석판사의 허가를 받아야 하며, 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도 내의 집단이나 외국에 소재하는 그 산하단체의 구성원의 통신인 때 및 군용전기통신의 경우에는 서면으로 대통령의 승인을 얻어야 한다.

이러한 국가안보를 위한 감청조치는 미국의 수정헌법 제4조의 논의에서처럼 예방을 위한 '공익'과 침해되는 '사익'의 형량에서 '공익'이 우월할 경우 합리적인 제한이 가능하다는 논리에서 비롯되었으며, 특히 국제적으로 테러의 경각심이 높아지는 상황에서 우리나라 역시 예외일 수 없기에 통신감시조치의 필요성은 당연히 인정된다. 그러나 '국가안보'라는 사안에 대한 범위가 비교적 광범위하여 남용의 가능성이 있고, 예방조치의 특성상 기밀성을 요하기 때문에 정보공개가 어려운 점을 생각해본다면, 이에 대한 절차적 통제가 부족한 것도 사실이다.

「미국 자유법」의 경우 영장통제 시 수정헌법 제4조의 '상당한 이유'

에 근거한 것으로 침해조치를 일단 축소하는데 법리가 발전 및 축적되어 있다. 침해조치를 위해서는 합리성이 필요하며, ① 특정 범죄가 발생했거나 저지르고 있다고 믿을 수 있는 가능한 원인(probable cause) ② 감청할 대화의 '특정'을 강하게 요구하고 있다. 또한 통신제한조치나 감시조치에 포괄성을 최대한 줄이고 식별 가능한 특정정보나 특정인을 한정하는 개념인 '특정선별용어'라는 개념을 도입하여 포괄성을 되도록 줄이고 있는데 반해, 우리의 경우 '국가안전보장에 상당한 이유' 및 '필요한 경우'라는 추상적 개념을 구체화하는 논의가 상대적으로 부족해 보인다. 특히「통신비밀보호법」상의 국가안보를 위한 통신제한조치 전반에 대한 통제장치가 부족하다. 동법 제15조상에 국회의 통제가 규정되어 있으나, 이는 상임위원회나 국정감사 및 조사를 위한 위원회가 필요한 경우 특정조치에 한하여 청구하거나 과학기술정보통신부장관에게 보고를 요구할 수 있을 뿐이다. 따라서 「통신비밀보호법」상 국가안보에 대한 의혹 수준이 아니라 형법상 예비와 음모의 범위에 한하는 정당화하는 구체적인 사실과, 필요성 및 비례성이 고려되거나, 안보에 관한 위험의 관련성을 유지한다면 적어도 국회의 정기적인 보고와 같은 감시방안의 확대가 필요해 보인다.

나) 통신사실 확인조치와 관련하여

정보수사기관의 국가안보를 위한 '통신사실 확인조치'의 제공요청 역시 범죄수사의 경우와 유사한 논의를 지적할 수 있다. 현행 「통신비밀보호법」은 제7조에서 감청과 같은 통신제한조치의 경우 '국가안전보장에 상당한 위험이 예상되는 경우'로 요건을 규정하고 있는데 반해, 동법 제13조의4에서는 국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 '필요한 경우' 정보수사기관이 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있기 때문이다.

'필요한 경우(필요성)'라는 요건이 '상당성'에 비해 상대적으로 낮은 단계의 요건인 이유는 통신사실 확인요청이 통신제한조치에 비해 상대적으로 기본권제한의 수준이 낮다고 판단한 것으로 보인다. 헌법재판소는 국가안전보장을 국가의 존립·헌법의 기본질서의 유지 등을 포함하는 개념

으로서 국가의 독립, 영토의 보전, 헌법과 법률의 기능, 헌법에 의하여 설치된 국가기관의 유지 등의 의미로 해석하였으며,[45] '통신비밀보호'와 같은 기본권보장과 '국가안전보장'이라는 가치를 조화시키기 위해, '상당한' 위험 외에 '현존하는' 위험과 같은 개념을 추가하지 않은 것으로 보인다. 그러나 「통신비밀보호법」은 제7조에서 감청과 같은 통신제한조치에 대한 상당성의 요건조차 그 실체에 대한 논의가 부족한 상황에서, 필요성요건은 정보수사당국에 의해 자의적 혹은 포괄적으로 적용될 가능성이 높다.

또한 동법 제13조에서 규정한 범죄수사를 위한 통신사실 확인자료제공의 경우, '필요성' 이외에도 '다른 방법으로는 범죄의 실행을 저지하기 어렵거나 범인의 발견·확보 또는 증거의 수집·보전이 어려운 경우'와 같은 '보충성'을 규정하고 있는 바, 국가안전보장을 위해 보충성까지 요구하지 않더라도 상당한 수준까지는 규정할 필요가 있다고 본다. 따라서 적어도 형법상 예비와 음모에 준하지는 않더라도 범죄를 '계획'하는 상당한 이유 수준의 요건을 규정하는 입법이 필요하다.

다) 기간과 통지에 관련하여

「통신비밀보호법」 제13조의4에 의해 통신제한조치는 4개월을 초과하지 못하며 연장이 되더라도 4개월의 범위 이내에서 법원에 의한 기간연장이 가능하다. 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단이나 외국에 소재하는 그 산하단체의 구성원의 경우에는 대통령의 승인으로도 가능하다. 그러나 이 경우에도 1회에 한하는 등의 제한이 없기 때문에 연속적인 연장이 가능하다. 전시·사변 또는 이에 준하는 국가비상사태나 적과 교전상태에 있는 때에는 작전이 종료될 때까지 대통령의 승인을 얻지 아니하고 기간을 연장할 수 있는 경우를 제외하고 통신제한조치의 이러한 무제한적인 기간연장은 기본권 침해의 소지가 높다. 따라서 기간 연장을 몇 회로 한정하거나 혹은 기간의 축소를 통해 법원의 심사를 자주 받도록 하는 조치가 필요하다. 또한 대

45) 헌법재판소 1992. 2. 25. 89헌가104 참조.

한민국의 적대하는 국가나 우리의 통치권이 사실상 미치지 아니하는 곳의 외국인인 경우에도 대통령의 승인으로 통신제한조치가 이루어지더라도 법원의 사후영장심사 등이 필요하다.

한편 동법 제9조의2 제3항에 의하면 종료한 날로부터 30일 이내에 감정의 대상자에게 집행사실과 그 기간을 서면으로 통지하는 것이 원칙이지만, 동법 제9조의2 제4항에서는 "국가의 안전보장·공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때"에는 그 사유가 해소될 때까지 통지를 유예할 수 있다고 규정하고 있다. 이러한 통지의 유예 역시, 통신제한조치가 '사유의 해소'라는 규정이 모호하고 또한 자의적으로 해석될 가능성이 높으므로 보다 구체화할 필요가 있다.

4) 긴급통신제한조치

법원의 허가 없이 진행할 수 있는 긴급통신제한조치는, 「통신비밀보호법」제8조에 규정되어 있으며 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄 등 중대한 범죄의 계획이나 실행 등 '긴박한 상황'과 절차를 거칠 수 없는 '긴급한 사유'가 있는 경우에 한하여 이루어진다. 위험의 시급함에 비추어봤을 때 정보수사에 있어 특수성이 고려된 규정으로 중대한 범죄에 대처하고 예방하기 위한 조치로 정당성이 인정된다. 다만, 동조 제2항의 규정대로 집행에 착수 후 지체없이 법원에 허가청구를 해야 하며 36시간 이내에 법원의 허가를 받지 못한 때에는 이를 즉시 중지해야 한다고 하고 있다.

긴급조치의 특성상 법원의 허가를 36시간으로 유예한 것이 적절한 지에 대해, ①미국 48시간 ② 영국 5일 ③ 독일 3일 ④ 호주 48시간 등으로 주요 외국의 입법례를 감안하면 현행 36시간은 불가피한 기본권제한이라고 생각된다. 오히려 최소 2일인 48시간으로 확대하는 조치도 검토해볼 만하다.

오히려 '긴박한 상황' 및 '긴급한 사유'에 대한 법리적 논의와 절차에 대한 구체적인 논의가 필요하다. 즉 이상의 긴급성을 판단하는데 있어 정황상의 의혹이나 의심의 수준에 머물러서는 안 되며 '긴급한 사실'이

인정되어야 한다.

나아가 동조 제5항과 제6항에서 긴급통신제한조치가 단시간 내에 종료되어 법원의 허가를 받을 필요가 없는 경우, 긴급통신제한조치의 목적·대상·범위·기간·집행장소·방법 및 통신제한조치허가청구를 하지 못한 사유를 기재하여 7일 이내에 관할 지방검찰청검사장이 (국가안보의 경우, 고등검찰청검사장이) 이에 대응하는 법원장에게 긴급통신제한조치 통보서를 송부하도록 하고 있는데, 이 역시 단기간 내에 종료되었다는 사유로 영장주의의 예외로 삼는 것은 무리가 있어 보인다. 따라서 이 경우에도 사후영장주의를 관철하는 입법이 필요하다.

(2) 테러방지법과 영장주의 강화

1) 국민보호와 공공안전의 개념

「국민보호와 공공안전을 위한 테러방지법 (테러방지법)」은 테러로부터 국민의 생명과 재산을 보호하고 국가 및 공공의 안전을 확보하는 것을 목적으로 한다. 따라서 국민보호와 공공안전의 개념을 명확히 할 필요가 있다. 동법에서 '국민보호'는 생명과 재산의 보호를 의미하는데, 이는 헌법 제12조상의 신체의 자유 및 제23조의 재산권 보장을 구체적 근거로 들 수 있다. 그러나 국민보호의 개념을 신체와 재산에 국한하여 한정할 수 없다. 헌법에서 규정하는 기본권 전반에 '국민보호'의 개념이 깔려있다. 특히 압수 및 수색 등에 있어 법관이 발부한 영장을 요구하는 영장주의와 법치주의원칙, 적법절차원칙 등이 국민보호를 위한 헌법상 원칙이다. 물론 동법은 '테러'를 방지하기 위한 목적에 한정되지만, 국민보호의 목적을 '신체 및 재산'으로 제한하는 해석은 협소하다는 비판이 가능하다.

'공공안전'의 경우, 구체적인 개념분석을 위해 「경찰관직무집행법」상의 '공공의 안녕'의 논의와 비교해 볼 수 있다. 「경찰관직무집행법」상에 명시되어 있지는 않지만, 일반적으로 "개인의 생명·신체·자유·명예와 재산의 온전성 및 국가와 그 시설의 존속과 기능이 아무런 장해도 받지 않고 있는 상태"[46]를 의미한다. 즉 '공공'의 범위는, 단순히 개인적 법익

46) Drews/Wache/Vogel/Martins, Gefahrenabwehr, 9, Aufl. 1986, § 15.

뿐만 아니라 공동체의 법익을 포함한다.[47] 이는 「경찰관직무집행법」과 「테러방지법」상의 '공공'의 의미는 동일한 것으로 보인다.

또한 '안녕(安寧)'의 사전적 의미는 '걱정이나 아무 탈이 없음'을 의미하는데, 「경찰관직무집행법」에서는 '온전성 및 존속과 기능의 장해가 없는 상태'로 기술되어 있다. '안전(安全)'의 의미 역시, '위험이 없어 피해를 입지 않는 것'을 의미하는데, 이에 의하면 '안녕'의 경우 '현재의 온전성과 무탈함'에 중심을 두고 있고, '안전'의 경우 '현재뿐만 아니라 미래의 손해의 가능성이 없음'에 중심을 둔 해석으로 보인다. '테러'는 현존하는 리스크뿐만 아니라 앞으로 닥칠지 모르는 미래에 대한 리스크를 포함하는 개념이기 때문에, '안전'이 「테러방지법」에 더 적합한 표현으로 보인다.

한편 '공공질서'와 '공공안전'을 비교하면, 전자의 경우 "당시의 지배적인 사회적·윤리적 가치관에 따를 때 인간의 유익한 공동생활을 위하여 그 준수가 필수불가결한 요건인 것으로 간주되는 규율의 총체"로 정의할 수 있다.[48] 따라서 여기에는 법규범 이외의 다른 사회규범, 특히 도덕규범이 포함된다고 해석할 수 있다. 이렇게 사회적 의미의 규범이 포함될 경우 개념파악이 쉽지 않고 주관적인 측면이 강하기 때문에 판단이 어렵다. '테러방지'에는 '공공질서'의 개념은 이를 포함한다고 해석하기는 어려우며, '안전'의 개념에서 위험 및 피해의 가능성이 없는 경우와 같은 상황에 국한하는 것이 기본권제한의 내용을 담고 있는 「테러방지법」의 특성에 적합한 해석으로 보인다.

2) 테러행위와 영장주의의 문제

「테러방지법」 제2조에 의하면 "테러"란 국가·지방자치단체 또는 외국 정부의 권한행사를 방해하거나 의무 없는 일을 하게 할 목적 또는 공중을 협박할 목적으로 하는 행위를 말하며, 그 행위의 유형에 대해 살해나 신체를 상해하는 행위, 항공기·선박의 운항과 관련하여 안전을 위태롭게 하는 행위, 생화학·폭발성·소이성 부기나 장치를 차량·시설에 배치하

47) 홍정선, 경찰행정법, 박영사, 2010, 16면; 손재영, 경찰법, 박영사, 2016, 144면.
48) 손재영, 앞의 책, 162면.

거나 사용하는 행위, 핵과 관련된 물질이나 시설을 위태롭게 하는 행위 등이 이에 포함된다. 이러한 테러행위는 국민의 생명과 신체 그리고 재산에 위해를 가하고, 국가 및 공공의 안전에 대한 심각한 위험으로 이를 예방하고 대응하기 위한 국가의 책무가 인정된다.

테러방지행위는 크게 "대테러활동" 및 "대테러조사"로 이루어져 있는데, 동법 제2조 제6호에서는 "대테러활동"이란 제1호의 테러 관련 정보의 수집, 테러위험인물의 관리, 테러에 이용될 수 있는 위험물질 등 테러수단의 안전관리, 인원·시설·장비의 보호, 국제행사의 안전확보, 테러위협에의 대응 및 무력진압 등 테러 예방과 대응에 관한 제반 활동을 말한다고 규정하고 있으며, 동조 제8호에서는 "대테러조사"란 대테러활동에 필요한 정보나 자료를 수집하기 위하여 현장조사·문서열람·시료채취 등을 하거나 조사대상자에게 자료제출 및 진술을 요구하는 활동을 규정하고 있다. 이러한 동법 제3조 제2항에서 규정한 대로 이러한 테러방지행위에 대해 기본권 침해가 이루어지지 않도록 최선의 노력을 할 필요가 있다. 동조 제3항에서 헌법과 법률에서 정한 적법절차의 준수의무를 명시한 이유도 이와 같은 이유로 보인다. 따라서 「테러방지법」에 근거하여 '신체와 재산'과 같은 이러한 기본권 제한의 절차 속에는 당연히 영장주의의 헌법적 요청이 수용되고 적극적으로 검토되어야 한다. 문제는 불특정한 다수를 상대로 가중된 불법성을 가진 테러행위[49]를 사전에 탐지하기 위한 정보수집의 필요성이 형사사법체계가 규정하고 있는 영장주의와 어떻게 조화를 이룰 것인가에 있다.

이러한 맥락에서 테러예방을 위한 대테러활동 중 통신비밀보호와 연관이 있는 법률은 역시 「통신비밀보호법」이다. 「테러방지법」 제9조에서 '테러위험인물'에 대한 정보 수집에 있어 「통신비밀보호법」의 절차를 따르도록 하고 있다. 따라서 국가안보와 관련한 「통신비밀보호법」상의 통신제한조치 및 통신사실확인 요청조치 등과 같은 조치 및 긴급통신제한조치들이 국가정보원장을 통해 이행된다.[50] 따라서 국가안보를 위

49) 김훈영, 앞의 논문, 309면 이하.

50) 따라서 「테러방지법」 제9조에서 이러한 기록을 얻어내기 위한 '절차'가 전혀 규정되어 있지 않고, 정보기관은 그저 요구하기만 된다는 김희정, 앞의 논문, 115면의 지적은 「통신비밀보호법」의 절차를 오해한 것으로 보인다.

한 '통신제한조치'는 통신의 일방 또는 쌍방당사자가 내국인인 때에는 고등법원 수석판사의 허가를 받아야 하며, 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단이나 외국에 소재하는 그 산하단체 구성원의 통신인 때 및 군용전기통신의 경우에는 서면으로 대통령의 승인을 받아야 한다.

그러나 「테러방지법」 제2조에서 "테러위험인물"을 어떻게 특정할 것인지에 대해 영장주의의 관점에서 논의가 부족하다. 동법 제3호에서는 "테러위험인물은 테러단체의 조직원이거나 테러단체 선전, 테러자금 모금·기부, 그 밖에 테러 예비·음모·선전·선동을 하였거나 하였다고 의심할 '상당한 이유'가 있는 사람"이라고 규정하고 있는데, 「테러방지법」 제9조에서 말하는 '테러위험인물에 대한 추적'은 기존의 위험인물을 추적하는 것뿐만 아니라 앞으로 위험인물이 될 사람을 찾는 것을 포함하는 개념이다. 따라서 '상당한 이유'에 대한 보다 정치한 논의가 필요하다.

3) 국회에 보고대상 확대

「테러방지법」의 경우 제9조 제1항에 의해 테러위험인물에 대해 통신이용 등 관련정보와 관해 「통신비밀보호법」의 절차를 따르도록 하고 있다. 이에 대해 「통신비밀보호법」은 제15조에서 국회의 통제에 대해 규정하면서 통신제한조치에 대한 통신제한조치보고서를 국회에 제출하도록 규정하고 있으나, 통신사실 확인요청과 관련된 부분에 대해서는 국회에 어떠한 보고의무를 부과하고 있지 않다. 따라서 이 부분에 대한 개정이 필요하다.

나아가 「테러방지법」 제9조 제4에서 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 추적을 할 수 있도록 규정하고 있는데, 이 경우 사전 또는 사후에 국가테러대책위원회 위원장에게 보고하도록 규정하고 있다. 이 경우에도 국회에 국가정보업무에 대한 효율적 통제와 국가기밀보호를 위한 상임위

원회로서 정보위원회가 존재하는 만큼, 관련 내용의 정기적 혹은 비정기적인 형태의 국회보고가 필요하다. 정보위원회는 국회법 제54조의2에 의해 인사청문회나 공청회를 제외하고는 원칙적으로 공개되지 않으므로, 국가정보의 기밀성을 감안하여 대테러활동에 필요한 정보나 자료를 수집과 대테러조사 및 테러위험인물에 대한 추적 역시 비공개 및 비밀유지의 형태로 이루어질 것이다.

4) 위원회의 구성 및 권한

「테러방지법」은 제5조에서 '국가테러대책위원회'를 설치하도록 하고 있고 여기서 대테러활동에 관한 정책의 중요사항을 심의 및 의결하도록 하고 있다. 여기서 중요사항이란 ① 대테러활동에 관한 국가의 정책 수립 및 평가, ② 국가 대테러 기본계획 등 중요 중장기 대책 추진사항, ③ 관계기관의 대테러활동 역할 분담·조정이 필요한 사항, ④ 그 밖에 위원장 또는 위원이 대책위원회에서 심의·의결할 필요가 있다고 제의하는 사항을 의미한다.

또한 「국민보호와 공공안전을 위한 테러방지법 시행령」 제3조에 따르면 '국가테러대책위원회'는 위원장으로 국무총리 외에, 기획재정부장관, 외교부장관, 통일부장관, 법무부장관, 국방부장관, 행정안전부장관, 산업통상자원부장관, 환경부장관, 국토교통부장관, 해양수산부장관, 국가정보원장, 국무조정실장, 금융위원회 위원장, 원자력안전위원회 위원장, 대통령경호처장, 관세청장, 경찰청장, 소방청장, 질병관리청장 및 해양경찰청장의 총21명으로 구성되며, 안건 심의에 필요한 경우 관계 기관의 장이나 관계자가 참석할 수 있다. 이와는 별도로 테러활동의 임무 및 협조사항에 대한 실무를 조정하기 위한 '대테러센터'도 존재하는데, 시행령의 규정을 보아도 본 센터는 실질적인 임무 및 실무를 위한 수행기관으로서 성격을 가진다. 따라서 테러정책과 집행에 있어 최고기관은 '국가테러대책위원회'임에 틀림없어 보인다.

그러나 그 위상에 비해 위원회의 구성과 권한이 너무 간략하게 마련되어 있다. 현행 '국가테러대책위원회'는 행정부로 구성되어 정책수립 및 테러대응에 관한 의사결정에 맞춰져 있기 때문에 조직의 성격상의

차이가 있을 수 있다. 그러나 테러대응이 국민의 기본권 보호에 직접적인 영향을 끼칠 수 있는 이상, 위원회 내부에서도 이에 대해 전문적인 목소리를 낼 수 있는 방안이 필요하다. 위원회가 독립성을 가져 독자적으로 운용되는 것이 현실적으로 어렵다 하더라도, 준사법적 기관으로 기능한다면 정책설계를 위한 현실적 기구가 될 수 있다. 지금의 형태는 단순히 행정기관 사이의 협의회 혹은 테러정책에 있어 요식행위에 불과할 가능성이 크다. 「테러방지법」이 다루고 있는 내용이 국민은 물론 해외의 테러관련 정보를 광범위하게 수집하는 바, 이에 대한 정보보호와 테러정책 전반에 대한 논의를 나눌 수 있는 민간전문가나 전문기관의 참여는 물론 일정부분에 있어 독립성을 확보하는 것이 필요하다.

5) 피의자 별 통신제한조치와 통보

「테러방지법」은 「통신비밀보호법」 상의 국가안보를 위한 통신제한조치 규정을 따르는데, 「통신비밀보호법」 제7조 제3항에 의하면 통신제한조치를 법원에 신청함에 있어 '각 피의자 별 또는 각 피내사자별로 통신제한 조치'를 하지 않고 신청이 가능하도록 하고 있다. 이를 통해 국가안보를 통한 광범위한 통신제한조치가 가능한 점은 기본권 보호에 있어 문제가 있어 보인다.

또한 통신제한조치의 집행에 대한 통지 역시 「통신비밀보호법」의 절차를 따르는데, 따라서 이를 규정한 「통신비밀보호법」 제9조의2 제3조에 의하면 통신제한조치를 종료한 후 30일 이내에 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 하고 있지만, 동조 제4조에 의해 국가의 안전보장·공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때 그 사유가 해소될 때까지 통지를 유예할 수 있도록 하고 있다.

이러한 피의자별 통신제한조치의 신청과 통신제한조치 대상에 대한 통지의 예외를 범죄사실을 목적으로 하는 통신제한조치와 동일하게 규정할 수 없다는 정보수사의 현실을 감안하더라도, 이는 '공공안전'의

목적을 '범죄의 계획'으로 한정하거나 '사실의 근거'로 축소하지 않은 상황에서 남용될 우려가 크다. 따라서 공공안전의 범위를 축소하기 어렵다면, 적어도 통신제한조치를 법원에 신청함에 있어서는 피의자별로 통신제한조치를 하는 것이 헌법의 영장주의를 반영한 입법적 조치라 생각된다. 또한 감청의 대상자인 피의자 및 피내사자에게 그 사실을 통지하기 어려운 사유가 있다면 횟수의 제한을 두거나 기간의 제한을 두어 통지를 유예하는 것이 법치주의와 적법절차원칙에 적합할 것으로 보인다. 국가에 의한 광범위한 정보조사가 '공공안전'이라는 목적하에 법원의 판단을 거치지 않은 채로 당사자도 모르는 상황이 언제까지 유예될지 모르는 상태로, 국회 역시도 이런 상황을 파악하지 못하는 채로 이루어질 수 있다는 것은, 기본권에 대한 과도한 침해로 판단된다.

Ⅳ. 결론

앞서 보듯이 영장주의의 관점에서 「통신비밀보호법」과 「테러방지법」의 내용을 검토하였다. 지능정보사회에서 통신비밀보호를 위해서는 영장주의가 강화되어야 한다는 문제의식 하에 통신기기는 물론 범죄수사, 국가안보 전반에 대해 대안을 제안하고자 노력하였다. 특히 영장을 통한 통신제한조치의 기한 및 통지를 개인정보자기결정권의 입장에서 검토하고 「테러방지법」에 대해서는 영장주의를 보강하고자 피의자별 통신제한조치를 제안하고, 동법을 통한 통신제한조치의 통제를 위한 위원회 및 국회통제 방안을 간략하게 제시하였다.

(논문투고일: 2021.4.28., 심사개시일: 2021.6.8., 게재확정일: 2021.6.23.)

한웅재 · 김일환

통신비밀보호법, 테러방지법, 영장주의, 통신제한조치, 개인정보자기결정권

【참 고 문 헌】

Ⅰ. 단행본

손재영, 경찰법, 박영사, 2016.
이재상·조균석, 형사소송법, 박영사, 2017.
한수웅, 헌법학, 법문사, 2021.
홍정선, 경찰행정법, 박영사, 2010.

Ⅱ. 논문

김일환, 초연결사회에서 개인정보보호법제 정비방안에 관한 연구, 성균관법학 제29권 제3호, 2017.
김일환, 행정정보의 공동이용으로부터 정보자기결정권의 보호에 관한 헌법상 고찰, 공법연구, 제32집 제4호, 2004.
김종현, 영장주의에 관한 헌법적 연구, 헌법재판연구원, 2019.
김현귀, 패킷감청에 대한 위헌심사 - 헌재 2018. 8. 30. 2016헌마263 결정을 중심으로 -, 헌법학연구 제25권 제2호, 2019.
김희정, 대테러리즘, 자유와 안전, 한국공법학회, 공법연구 제44집 제4호, 2016.
김훈영, 테러방지법의 처벌규정에 대한 기본권 보장적 해석, 미국헌법연구 제30권 제3호, 2019.
민만기, 인터넷 패킷감청의 법적 성격 및 허용 가능성 검토, 형사법의 신동향, 통권 제53호, 대검찰청, 2016.
박종현, 「통신비밀보호법」상 통신사실 확인자료 제공관련 조항들에 대한 헌법적 검토 - 2018. 6. 28. 2012헌마191등 결정례와 2018. 6. 28. 2012헌마538 결정례에 대한 검토를 중심으로 -, 헌법학연구 제25권 제2호, 2019.
박희영, 수사 목적의 암호통신감청(Quellen TKU)의 허용과 한계, 형사정책연구 29(2), 2018.
설민수, 피의자 보관 전자정보의 압수·수색에서 미국과 한국 법원의 영장

주의 적용과 변화과정: 이미징을 중심으로, 형사법의 신동향, 통권 제53호, 대검찰청, 2016.

이흔재, 독일의 휴대전화 위치정보 추적수사와 당사자에 대한 통보제도 - 통신비밀보호법 일부개정법률안에 대한 평가와 개선방안을 중심으로 -, 법조 제68권 제4호(통권 제736호), 2019.

이얼·박웅신, 인터넷 패킷감청의 현황과 과제, 법학연구, 인하대학교 법학연구소, 2016.

이진구, 통신비밀의 보호범위와 한계에 관한 헌법상 연구, 2016, 성균관대학교 박사논문.

차진아, 범죄수사를 위한 통신사실확인자료 제공요청의 문제점과 개선방안, 법조 통권 제728호, 2018.

헌법재판연구소, 영장주의에 관한 헌법적 연구, 2019.

Abstract

Legislative Reorganization plan to strengthen Warrant Requirement Principle under the Communications Secret Protection Act and the Anti-Terrorism Act

Han, Woongjae · Kim, Ilhwan

Traditionally, the issue associated with Warrant Requirement Principle in the freedom of communication has been related to eavesdropping and interception, centering on the freedom of the body. However, in modern times, various methods are used to collect information. Moreover, private companies that provide communication services that exchange and connect large volumes of data can be used to collect deeper and more intimate information. In addition, the information that the state can obtain through the seizure of communication devices inevitably leads to infringement on the privacy of individuals, but the procedural sophistication seems to be insufficient. It is necessary to discuss in detail how the actual operation is based on these discussions under Warrant Requirement Principle. Warrant Requirement Principle has procedural significance that allows individuals to defend against various infringements of basic rights such as seizure, search, and verification, as well as arrest and detention by independent judges. If Warrant Requirement Principle does not properly play the role of protecting communications secrets and the discretionary control of intelligence agencies

does not work properly, the state can create a so-called “monitoring society” based on personal information about the people. And this surveillance society is likely to lead to the control of human dignity, ideology and conscience, business, academic, religious, and political activities as pursued by the Constitution. In an intelligent information society, under the awareness that Warrant Requirement Principle should be strengthened for the protection of communications secrets, efforts have been made to propose alternatives not only for communications devices, but also for criminal investigations and national security in general. In particular, review the time limit and notification of communication restriction measures through warrants from the standpoint of self-determination of personal information, and propose communication restriction measures for each suspect to reinforce Warrant Requirement Principle for the 「Terrorism Prevention Act」, and control the communication restriction measures through this act and the committee and the National Assembly control plan were briefly presented.

Han, Woongjae · Kim, Ilhwan

Communications Secret Protection Act, Anti-Terrorism Act, Warrant Requirement Principle, Limitation on Telecommunication, Personal Information Self-Determination Right