

『통신비밀보호법』
일부개정법률안
[정청래 의원 대표발의,
의안번호: 2204138]
의견서

2024. 11.

(사) 오픈넷



대표자: 강정수

주소: 서울시 마포구 월드컵북로5길 13 (서교동, 한국여성재단), 301호

전화번호: 02-581-1643 팩스: 02-581-1642

1. 서설

인공지능 딥페이크 기술을 활용한 디지털 성범죄물의 심각한 사회문제화가 진행됨에 따라 2024. 9. 20. 「성폭력범죄의 처벌 등에 관한 특례법」 및 「아동·청소년의 성보호에 관한 법률」에 규정된 범죄를 「통신비밀보호법」상 통신제한조치 허가 요건에 추가하는 내용의 통신비밀보호법 일부개정법률안(의안번호 : 2204138, 정청래 의원 대표발의)이 발의되었다.

그러나 통신제한조치는 헌법상 사생활의 비밀과 자유 및 통신의 비밀과 자유를 가장 직접적이고 강력하게 침해하는 수사방식이라는 점에서, 이들 기본권 보장의 측면과 디지털 성범죄물의 확산 방지를 위한 필요성 등의 측면을 균형적으로 고찰하여 해당 법률안의 타당성·적정성을 검토할 필요가 있다.

2. 통신제한조치의 의의

통신제한조치(감청)란, 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다(통신비밀보호법 제2조 제7호).

범죄수사를 위한 통신제한조치는 통신비밀보호법 제5조 제1항에 열거된 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로서는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다(통신비밀보호법 제5조 제1항). 즉, 통신제한조치는 ① 계획 또는 실행하고 있는 범죄의 저지나 ② 이미 실행된 범죄의 증거 수집을 위한 수사방식이라 할 수 있다.

이러한 통신제한조치는 헌법상 통신의 비밀과 자유(헌법 제18조)와 사생활의 비밀과 자유(헌법 제17조)에 대한 직접적인 제한을 수반하므로, 헌법상 과잉금지 원칙을 엄격히 준수하고 그 본질적 내용을 침해하지 않아야 한다(헌법 제37조 제2항).

근대 형사소송법은 시민의 자유를 침해할 수 있는 수사는 원칙적으로 공개된 투명한 방식으로 행해질 것을 전제로 하고 있다. 예를 들면, 고전적인 강제처분인 압수

나 수색의 경우, 수사기관이 형사소송법의 규정에 따라 압수·수색을 개시한 때에는 영장이 제시되고 당사자의 참여가 인정되는 등 수사과정에서 피의자가 이러한 사실을 알게 된다. 그러나 통신제한조치는 본래적으로 기밀하게 범죄 혐의자의 통신에 침투하는 데에 그 의의가 있기 때문에 당사자나 관련자가 자신의 통신의 비밀이나 사생활의 비밀이 침해되고 있다는 사실을 알지 못한채 이루어지는 일종의 비밀수사다. 따라서 이러한 수사는 피의자나 관련자가 이에 대응할 수 없다는 점에서 전형적인 강제수사와는 다른 특징이 있다.¹⁾

또한 특히 인터넷 통신 감청은 더욱 큰 문제를 안고 있다. 인터넷 패킷 감청(packet inspection)이란 인터넷 회선을 통해 오가는 전기신호형태의 패킷 정보를 중간에서 실시간으로 가로채는 감청 방식을 말한다. 패킷 감청은 인터넷 회선의 데이터를 수집하는 행위로서 유선 또는 이동전화의 감청과 다른 특징이 있다. 첫째, 대상자를 특정해서 할 수 없다. 직장에서 공유기를 사용하여 다수가 컴퓨터를 사용하거나 가정에서 한 대의 컴퓨터를 온 가족이 사용하는 경우와 같이 감청 대상자를 특정하기 어렵다. 둘째, 감청의 범위를 특정하기 어렵다. 패킷형태의 데이터를 추출하기 때문에 통신제한조치허가서에 있는 개인에 대한 특정한 정보만을 수집하는 것이 기술상 불가능하고 타인 또는 수집범위를 초과한 방대한 개인정보를 수집하게 된다. 셋째, 패킷 형태의 데이터를 재조합하는 절차가 필요하다. 전화선 감청처럼 바로 음성을 실시간 지득하는 공독성과 달리 패킷 데이터를 재조합하여 열람하기 전까지는 내용판별이 불가능한 특징이 있다.²⁾

결국 인터넷 패킷 감청의 경우 수사기관은 감청 집행단계에서 동일한 인터넷 회선을 이용하는 불특정 다수의 통신자료와 대상자의 감청범위를 초과하는 통신자료까지 모두 수집·저장하게 되고, 감청 대상자가 아닌 다수 또는 다량의 통신자료까지 수집·저장할 수 있게 되므로, 국민의 사생활의 비밀, 통신의 비밀을 심대하게 침해하는 조치가 될 수밖에 없다. 이에 패킷 감청은 피의자 및 그와 관련된 불특정한 통신 상대방의 통신행위를 일반적·포괄적으로 침해하는 것으로, 통신 감청이 최소한 보충적으로 이루어져야 한다는 통신비밀보호상의 감청 범위를 본질적으로 벗어난 것이며, 헌법상 과잉금지원칙, 비례의 원칙에도 위반하는 위헌적 조치라는 견해도 있다.

1) 조기영, “최근 주요 쟁점과 관련한 통신비밀보호법 개정방향 - 휴대전화 감청, 패킷감청, 기지국수사, GPS위치정보 추적을 중심으로”
2) 민만기, “인터넷 패킷감청의 법적 성격 및 허용 가능성 검토”, 『형사법의 신동향』 통권 제53호, 대검찰청, 2016

헌법재판소 역시 인터넷 회선 감청, 패킷 감청의 필요성은 인정하면서도, “인터넷회선 감청으로 수사기관은 타인 간 통신 및 개인의 내밀한 사생활의 영역에 해당하는 통신자료까지 취득할 수 있게 된다... '패킷감청'의 방식으로 이루어지는 인터넷회선 감청은 수사기관이 실제 감청 집행을 하는 단계에서는 해당 인터넷회선을 통하여 흐르는 불특정 다수인의 모든 정보가 패킷 형태로 수집되어 일단 수사기관에 그대로 전송되므로, 다른 통신제한조치에 비하여 감청 집행을 통해 수사기관이 취득하는 자료가 비교할 수 없을 정도로 매우 방대하다는 점에 주목할 필요가 있다. 불특정 다수가 하나의 인터넷회선을 공유하여 사용하는 경우가 대부분이므로, 실제 집행 단계에서는 법원이 허가한 범위를 넘어 피의자 내지 피내사자의 통신자료뿐만 아니라 동일한 인터넷회선을 이용하는 불특정 다수인의 통신자료까지 수사기관에 모두 수집·저장된다. 따라서 인터넷회선 감청을 통해 수사기관이 취득하는 개인의 통신자료의 양을 전화감청 등 다른 통신제한조치와 비교할바는 아니다.”라고 하여 인터넷 회선 감청이 특히 사생활의 비밀, 통신의 비밀을 심대하게 침해하는 성격이 있음을 인정하였다. (헌법재판소 2018. 8. 30 자 2016헌마263 결정, 통신제한조치 허가 위헌확인)

국제인권규범은 사생활의 비밀은 인간 존엄성과 필수적으로 연결되는 근본적인 인권이자 표현의 자유, 정보의 자유, 결사의 자유와 같은 권리들을 강화하는 권리로 민주사회의 유지에 중추적 역할을 한다고 확인하며, 통신감시처럼 사생활의 비밀을 제한하는 활동들은 법률에 의해 규정되고 정당한 목적을 수행함에 필수적이고 그 목적에 비례성이 있을 때만 정당화된다고 천명하고 있다.³⁾

2013년 9월 20일, EFF, Access, Article 19, 프라이버시인터내셔널, 휴먼라이트와치, 국경없는기자회를 포함한 세계의 260여개 정보인권단체들은 국가에 의한 감청, 통신사실정보 취득, 이용자정보 취득 등에 대해 국제인권법이 요구하는 13개의 원칙을 발표하였다. 그 중 ‘필요성’의 원칙은 ‘국가통신감시를 허용하는 법은, 정당한 목적을 성취하기에 엄격하고 입증가능하게 필수불가결한 정도로 감시를 제한해야 한다. 통신감시는 정당한 목적을 성취할 유일한 방법일 경우에만 또는 여러 방법이

3) Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, “Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,” 2009, A/HRC/17/34.

있다면 인권을 가장 덜 침해하는 방법일 경우에만 집행되어야 한다. 감시의 필요성을 사법적 또는 입법적 과정에서 입증할 책임은 국가가 진다.’는 것이고, ‘적정성’은 ‘법이 허용하는 모든 통신감시행위는 명시된 구체적인 정당한 목적을 충족하기에 적절해야 한다.’는 것이며, ‘비례성’은 통신감시는 사생활의 비밀, 견해의 자유, 표현의 자유를 방해하는 고도의 침투적인 행위로서 민주사회의 근간을 위협하는 행위로 간주되어야 한다. 통신감시에 대한 결정은 이를 통해 얻는 혜택을 개인의 권리나 다른 경합하는 이익에 가해지는 해악과 견주어서 내려져야 하며 해당정보의 민감성과 사생활의 비밀 침해의 심각성을 고려해야 한다.’는 것이다.⁴⁾

우리 통신비밀보호법도 제3조 제2항에서 “우편물의 검열 또는 전기통신의 감청(이하 “통신제한조치”라 한다)은 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다.”고 규정하여 통신제한조치가 보충성, 최소침해성, 비례의 원칙을 지키며 행사되어야 함을 확인하고 있다.

3. 통신제한조치 대상 범죄 규정

이렇듯 통신제한조치는 수사기관이 사람 간의 통신 내용을 실시간으로 파악하거나 송수신을 방해하며 통신에 개입할 수 있도록 하는 조치로, 본래적으로 헌법이 보장하는 통신의 비밀(헌법 제18조), 사생활의 비밀과 자유(헌법 제17조) 및 인격권 등의 기본권을 매우 심각하게 침해할 우려가 높은 수사방식이다. 따라서 통신제한조치는 모든 범죄가 아니라, 통신의 비밀과 자유, 사생활의 비밀과 자유를 심대하게 제한하면서까지 그 저지나 수사가 반드시 필요한 범죄, 국민의 재산이나 생명·신체의 안전 보호가 중대한 범죄와 관련된 경우에 한하여 이루어져야 한다. 즉, 국가 존립 및 안전을 위협하는 범죄, 통화위조 등 범죄 발생시 피해의 규모가 큰 사회적 법익을 침해하는 범죄, 살인·인신매매 등의 강력범죄 등 통신비밀에 대한 직접적인 제한을 통해 달성하고자 하는 공익(해당 범죄 저지 혹은 증거 수집)이 압도적으로 우위에 있는 범죄들에 한하여 통신제한조치가 허용되어야 헌법상 과잉금지원칙, 비례의 원칙에 위배되지 않는다고 할 수 있는 것이다.

통신제한조치 대상 범죄 규정에 대한 외국의 입법례를 대강 정리하자면 다음과 같다. 독일이나 일본에서의 전기통신 감청은 주로 조직범죄나 마약범죄에 대응하기

4) <https://www.opennet.or.kr/4123>

위한 것이다. 전기통신 감청에 관한 독일 형사소송법 제100조의a는 유괴범죄나 테러범죄에 효과적으로 대응하기 위해 신설된 조문이며, 일본의 통신방수법상 통신방수 대상범죄는 ‘수인의 공모에 의해 실행되는 조직적인 살인, 약물 및 총포 등의 부정거래에 관계있는 범죄 등의 중대범죄’로 한정되어 있으며(동법 제1조), ‘집단밀항’, ‘조직범죄집단의 살인’, ‘조직폭력배의 총기사건’, ‘마약밀수 및 판매에 대한 수사’등으로 제한되어 있다. 형량을 기준으로 감청 대상 범죄를 제한하고 있는 나라는 대표적으로 영국과 프랑스다. 영국은 2000년에 제정된 「수사권규율법(RIPA)」에 의해 ‘중범죄’의 경우 예방과 탐지를 위해 모두 감청의 대상으로 인정하고 있으며, 프랑스는 「전기·전자 통신의 비밀에 관한 법률」에서 중죄 및 2년 이상의 자유형을 규정하고 있는 모든 범죄에 대하여 폭넓게 감청 대상으로 정하고 있다. 미국은 「종합범죄방지 및 가로안전법」을 규정하여 감청 대상 범죄로 정한 죄명을 열거하여 규정하고 있는데, 간첩·살인·핵시설 파괴뿐만 아니라 폭력, 재산은닉, 도박정보의 전달, 금융대출관련, 저작권침해, 우편물 횡령, 장물운송 등 중범죄라고 볼 수 없는 범죄도 감청 대상 범죄로 규정하고 있다.⁵⁾

우리나라의 경우, 제정 「통신비밀보호법」은 통신제한조치의 대상 범죄를 한정적으로 열거하고 있었으나 그 범위가 너무 넓어 위헌성이 높다는 지적이 있었고, 이에 따라 2001년 12월 29일 「통신비밀보호법」(법률 제6546호) 개정을 통하여 통신제한조치 대상 범죄를 기존의 391개에서 280개로 축소하였다.⁶⁾

현행 통신비밀보호법 제5조 제1항은 대상 범죄를 다음과 같이 규정하고 있다.

제5조 (범죄수사를 위한 통신제한조치의 허가요건)
 ① 통신제한조치는 다음 각호의 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다.

5) 양광모, 이상진, “통신제한조치 대상범죄에 사이버범죄의 포함 필요성”, 형사정책연구 Korean Criminological Review, 제30권 제4호(통권 제120호, 2019 · 겨울)

6) 이 개정을 통하여 제외된 범죄유형은 1) 「형법」 제7장 공무원의 직무에 관한 죄, 제15장 교통방해의 죄, 제16장 음용수에 관한 죄, 제19장 유가증권, 우표와 인지에 관한 죄 중 인지·우표의 위조등, 위조 인지·우표 취득, 소인말소, 인지·우표유사물의 제조등, 제30장 협박의 죄 중 존속협박, 제37장 권리행사를 방해하는 죄 중 권리행사방해, 강요, 점유강취, 중권리행사방해 및 강제집행면탈 등, 2) 「마약류 관리에 관한 범죄」에 규정된 범죄 중 장부 미기재등 행정벌의 성격이 강한 범죄, 3) 「특정범죄가중처벌 등에 관한 법률」 중 산림법 위반행위, 무고죄, 특수직무유기죄 등이다. 그 반대로 추가된 범죄유형은 1) 「형법」 제34장 신용, 업무와 경매에 관한 죄 중 경매, 입찰방해죄, 2) 「폭력행위등 처벌에 관한 법률」의 범죄 중 단체등의 구성·활동, 단체등의 이용·지원에 관한 죄, 3) 「총포·도검·화약류등 단속에 관한 법률」에 규정된 일부 범죄를 대상범죄로 추가하였다.

1. 형법 제2편중 제1장 내란의 죄, 제2장 외환의 죄중 제92조 내지 제101조의 죄, 제4장 국교에 관한 죄중 제107조, 제108조, 제111조 내지 제113조의 죄, 제5장 공안을 해하는 죄중 제114조, 제115조의 죄, 제6장 폭발물에 관한 죄, 제7장 공무원의 직무에 관한 죄중 제127조, 제129조 내지 제133조의 죄, 제9장 도주와 범인은닉의 죄, 제13장 방화와 실화의 죄중 제164조 내지 제167조·제172조 내지 제173조·제174조 및 제175조의 죄, 제17장 아편에 관한 죄, 제18장 통화에 관한 죄, 제19장 유가증권, 우표와 인지에 관한 죄중 제214조 내지 제217조, 제223조(제214조 내지 제217조의 미수범에 한한다) 및 제224조(제214조 및 제215조의 예비·음모에 한한다), 제24장 살인의 죄, 제29장 체포와 감금의 죄, 제30장 협박의 죄중 제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다), 제286조[제283조제1항, 제284조, 제285조(제283조제1항, 제284조의 상습범에 한한다)의 미수범에 한한다]의 죄, 제31장 약취(略取), 유인(誘引) 및 인신매매의 죄, 제32장 강간과 추행의 죄중 제297조 내지 제301조의2, 제305조의 죄, 제34장 신용, 업무와 경매에 관한 죄중 제315조의 죄, 제37장 권리행사를 방해하는 죄중 제324조의2 내지 제324조의4·제324조의5(제324조의2 내지 제324조의4의 미수범에 한한다)의 죄, 제38장 절도와 강도의 죄중 제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조, 제342조[제329조 내지 제331조, 제332조(제329조 내지 제331조의 상습범에 한한다), 제333조 내지 제341조의 미수범에 한한다]의 죄, 제39장 사기와 공갈의 죄 중 제350조, 제350조의2, 제351조(제350조, 제350조의2의 상습범에 한정한다), 제352조(제350조, 제350조의2의 미수범에 한정한다)의 죄, 제41장 장물에 관한 죄 중 제363조의 죄
2. 군형법 제2편중 제1장 반란의 죄, 제2장 이적의 죄, 제3장 지휘권 남용의 죄, 제4장 지휘관의 항복과 도피의 죄, 제5장 수소이탈의 죄, 제7장 군무태만의 죄중 제42조의 죄, 제8장 항명의 죄, 제9장 폭행·협박·상해와 살인의 죄, 제11장 군용물에 관한 죄, 제12장 위령의 죄중 제78조·제80조·제81조의 죄
3. 국가보안법에 규정된 범죄
4. 군사기밀보호법에 규정된 범죄
5. 「군사기지 및 군사시설 보호법」에 규정된 범죄
6. 마약류관리에관한법률에 규정된 범죄중 제58조 내지 제62조의 죄
7. 폭력행위등처벌에관한법률에 규정된 범죄중 제4조 및 제5조의 죄
8. 「총포·도검·화약류 등의 안전관리에 관한 법률」에 규정된 범죄중 제70조 및 제71조제1호 내지 제3호의 죄
9. 「특정범죄 가중처벌 등에 관한 법률」에 규정된 범죄중 제2조 내지 제8조, 제11조, 제12조의 죄
10. 특정경제범죄가중처벌등에관한법률에 규정된 범죄중 제3조 내지 제9조의 죄
11. 제1호와 제2호의 죄에 대한 가중처벌을 규정하는 법률에 위반하는 범죄
12. 「국제상거래에 있어서 외국공무원에 대한 뇌물방지법」에 규정된 범죄 중 제3조 및 제4조의 죄

현행법하에서도 통신제한조치가 허용되는 대상 범죄의 전체 수는 약 240여개에 달하는 것으로 추산되고 있는데, 해악이 중대하지 않은 범죄나 다른 덜 침해적인 방

식으로도 수사가 가능한 범죄까지도 광범위하고 포괄적으로 규정되어 있어 위헌성이 상당하다고 할 것이다. 헌법재판소 결정의 보충의견에서도, ‘통신감청을 허가할 수 있는 대상범죄의 범위가 지극히 광범위하게 규정’되어있음이 지적된바 있다(헌법재판소 2010. 12. 28. 선고 2009헌가30 결정, 재판관 조대현의 보충의견).

4. 통신제한조치 제도의 합헌적 개정 방향

일부에서는 현행 통신비밀보호법의 통신제한조치 대상 범죄도 이미 폭넓게 인정되고 있어 개인의 기본권이 침해될 우려가 높기에 일본처럼 국가테러와 마약범죄, 총기류 범죄에 한정되어야 한다고 주장하기도 한다. 또한 현행 280개의 대상 범죄 중에도, 협박죄, 추행죄 등과 같이 형량이 낮거나 감청의 필요·보충성을 고려할 때 다른 수사방법으로 대처가 가능하여 현실적으로 감청의 필요성이 낮은 범죄들은 감청 대상 범죄에서 삭제할 필요가 있다는 견해도 있다.

통신제한조치는 수사기관이 사람 간의 통신 내용을 실시간으로 파악하거나 송수신을 방해하며 통신에 개입할 수 있도록 하는 조치로, 본래적으로 헌법이 보장하는 통신의 비밀(헌법 제18조), 사생활의 비밀과 자유(헌법 제17조) 및 인격권 등의 기본권을 매우 심각하게 침해할 우려가 높은 수사방식이다. 특히 위에서 검토한 바와 같이 이제 사람의 모든 활동이 대부분 인터넷을 통해 이루어지고 있는 오늘날, 통신제한조치는 인터넷 감청으로 수렴할 수밖에 없고, 인터넷 감청은 필연적으로 포괄적으로 이루어질 수밖에 없기 때문에 범죄 혐의와 무관한 사생활에 대한 침해, 혐의자가 아닌 수인의 기본권 침해를 수반한다.

따라서 통신제한조치는 헌법상 비례의 원칙에 맞게 침해되는 법익의 중대성을 고려하여 결과적 해악이 매우 큰 중대범죄 수사에 필요한 경우에만 허용되는 방향으로 대상 범죄를 축소하여야 하며, 대상 범죄를 늘이거나 포괄적으로 규정하여 그 대상자를 늘려 국가가 국민의 통신의 비밀과 자유, 사생활의 비밀과 자유를 침해할 위험을 확장하는 것은 헌법 정신에 반하는 방향이라 할 것이다. 특히 우리나라는 정보수사기관이 통신제한조치 권한을 남용하여 반정부 인사를 사찰, 탄압한 역사가 있는만큼, 통신제한조치 권한을 확장하는 입법에는 더욱 신중하여야 할 필요가 있다.

5. 본 개정안의 내용 및 헌법적 검토

2024. 9. 20. 발의된 통신비밀보호법 일부개정법률안 (의안번호:2204138, 정청래 의원 대표발의, 이하 ‘본 개정안’)은 「성폭력범죄의 처벌 등에 관한 특례법」(이하 ‘성폭력처벌법’) 및 「아동·청소년의 성보호에 관한 법률」(이하 ‘청소년성보호법’)에 규정된 범죄 전체를 「통신비밀보호법」상 통신제한조치 허가 요건(대상 범죄)에 추가하는 내용이다.

안 제5조 제1항 제13호 신설

13. 「성폭력범죄의 처벌 등에 관한 특례법」 및 「아동·청소년의 성보호에 관한 법률」에 규정된 범죄

가. 입법 목적

본 개정안의 제안이유는 “불법·허위영상물이 올라오는 서버나 해당 영상물 제작·유통 혐의를 받는 피의자의 인터넷 회선을 감청할 수 있도록 해 딥페이크 범죄물이 무차별적으로 유포되는 것을 적시에 차단할 수 있는 근거를 마련하고자 함”이다. 위에서 이미 검토한 바와 같이 통신제한조치는 계획 또는 실행하고 있는 범죄의 저지나 이미 실행된 범죄의 증거 수집을 위한 수사방식이다. 그리고 본 개정안의 제안이유에 따르면 성범죄물의 ‘유포’를 ‘차단’하기 위한 것이 본 개정안의 주요 목적임을 알 수 있다.

개별 사례에서 유포를 차단하기 위해 어떠한 통신제한조치 방식이 취해질 것인지를 구체적으로 알 수는 없으나, 유포가 이루어지기 전에 인터넷 서비스의 서버나 피의자의 인터넷 회선에서 송·수신을 차단한다는 것인데, ‘온라인상 정보 유포 범죄’가 통신제한조치로 차단할 수 있는 요건을 갖출 수 있는지, 그리고 실제로 목적 달성이 가능할지는 의문이다. 즉, 온라인상 정보 유포 범죄에 있어, 유포 등의 범죄가 행해지기 이전에 어떠한 상황에서 범죄를 계획하고 있다고 의심할만한 충분한 이유가 있다고 인정되어 통신제한조치를 허가받을 수 있을지를 예상하기 어렵고, 허가 이후 인터넷 서비스의 서버나 피의자의 인터넷 회선에 차단 시스템을 설치하여 적시에 이를 차단하는 것이 가능한지 의문이다. 또한 유포 전에 차단을 하여 범죄 실행을 저지하게 되면 범인, 범죄에 대한 엄벌이 불가능해지고, 다른 플랫폼이나 인터넷 회선을 통한 범죄 예방 효과도 함께 감소할 수 있다. (이러한 이유로 범죄 저지

를 위한 통신제한조치는 개인의 법익을 침해하는 범죄보다는 국민의 다수의 안전을 침해할 우려가 높은 범죄에 대해 주로 정당화될 수 있을 것이다.)

한편, 제안이유에서는 ‘서버’에 대한 감청도 예정하고 있는데, 서버에 대한 감청은 보통 인터넷 서비스 사업자에 대한 감청 설비 구축이 요구된다고 할 것이다. 그런데 이는 결국 엄격한 암호화를 통해 대화자간의 비밀 대화를 보장하고, 서비스 제공자를 비롯한 제3자의 감시, 검열에서 자유로운 이용자간의 온라인 대화 서비스를 제공할 사업자들의 직업 수행의 자유 및 이러한 서비스를 이용하려는 이용자들의 표현의 자유, 통신의 비밀과 자유, 사생활의 비밀과 자유를 제한하며, 전반적인 통신 보안 시스템을 취약하게 만들 수 있다.

이러한 이유에서 국가인권위원회는 2009년 전기통신사업자에게 의무적으로 감청 설비를 구비하도록 하는 내용의 통신비밀보호법 개정안에 대해 “국가인권위원회는 국민들에게 수사기관이나 정보기관 등에 의해 휴대전화 등 국민의 일상적 사생활이 상시적으로 감시될 수 있다는 불안감을 조성해 개인의 프라이버시권을 크게 위축시킬 수 있다고 판단했습니다. 또한, 감청장비의 상시적 운용에 따른 개인정보유출에 대한 차단기술이나 제도적 통제장치에 대한 규정이 미비해 사업자에 의한 악용과 프라이버시 침해 위험이 완전히 제거되어 있다고 볼 수 없습니다.”는 의견을 제시한바 있다.⁷⁾

물론 입법목적이 성범죄물 유포의 사전 차단에 국한되지 않고, 증거 수집에도 통신 제한조치를 이용하기 위한 것일 수 있다. 실제 본 개정안과 유사한 유상범 의원안(의안번호 : 2204685)의 제안이유에서는 “디지털 성범죄 수사를 위해 온라인 현장을 확인하는 것이 중요하나, 텔레그램과 같이 사업자가 사법절차에 협조적이지 않은 SNS를 이용한 범죄의 경우 증거자료들을 신속히 확보하기 어려움. 불법허위영상물 제작유통 혐의를 받는 피의자의 인터넷 회선을 감청(이른바 ‘패킷 감청’)하면 사업자의 도움 없이도 증거확보가 가능하나, 현행법상 디지털 성범죄는 감청 대상에서 제외되어 있어 이마저도 어려운 상황임.”이라고 실시되어 있다.

그러나 단순히 ‘신속한’ 증거 확보와 같은 일종의 수사 편의를 위해서 통신제한조치의 대상 범죄로 규정할 수는 없으며, 다른 방법으로도 충분히 범인의 체포나 증거

7)

<https://www.humanrights.go.kr/base/board/read?boardManagementNo=24&boardNo=591701&searchCategory=&page=323&searchType=&searchWord=&menuLevel=3&menuNo=>

의 수집이 가능하다면 특별히 통신제한조치가 필요한 범죄로 볼 수는 없을 것이다. 생각건대, 디지털 성범죄물의 제작 유통 혐의자가 통신제한조치의 대상자가 될 정도로 신원이 특정되고 통신제한조치의 허가 요건까지 갖추게 되었다면 대부분은 이미 충분한 증거가 확보되고 체포가 가능한 상황이라고 봐도 무방할 것이고, 지금까지 디지털 성범죄물 관련 사건들이 상당수 입건되고 수사가 진행되어 재판으로 넘겨진 것으로 보았을 때, 다른 수사방법으로도 충분히 범인의 체포와 증거의 수집이 가능한 범죄라고도 볼 수 있다. ‘사업자가 사법절차에 협조적이지 않은 SNS를 이용한 범죄의 경우 증거자료들을 신속히 확보하기 어렵다’는 이유로 통신제한조치가 허용되어야 한다면 결국 인터넷을 통해 이루어질 수 있는 모든 범죄들이 통신제한조치로 규정되는 것도 정당화될 수 있는 위험이 발생할 수 있다.

나. 대상 범죄 규정과 법익 균형성

본 개정안은 통신제한조치 허가 요건(대상 범죄) 규정에 “「성폭력범죄의 처벌 등에 관한 특례법」 및 「아동·청소년의 성보호에 관한 법률」에 규정된 범죄”를 추가함으로써 해당 법률상의 모든 범죄와 관련된 경우 통신제한조치를 허용하고 있다.

위에서 검토한 바와 같이 통신제한조치는 가장 강력하게 국민의 통신의 비밀과 자유, 사생활의 비밀과 자유를 제한하는 수사방식으로, 모든 범죄가 아니라 이러한 기본권 제한과 법익 침해를 상회할 정도로 그 예방이나 증거 수집이 절실한, 결과적 해악이 중대한 범죄에 한정되어 허용되는 것이 합헌적이라 할 것이다. 그러나 「성폭력범죄의 처벌 등에 관한 특례법」 및 「아동·청소년의 성보호에 관한 법률」에 규정된 모든 범죄들이 통신제한조치가 필요한 성격의 중대 범죄에 해당하는지에 대해서는 각 죄별로 더욱 세부적이고 심층적인 논의가 필요하다.

예를 들면, 최근 통과된 성폭력처벌법 개정안은 ‘반포 목적’을 불문하고 “사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 “영상물등”이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 “편집등”이라 한다)”하는 행위와 이를 “소지·저장 또는 시청”하는 행위도 범죄로 규정하고 있다.⁸⁾ 이러한 행위는 ‘반포·유포’ 행위와는 달리 곧바로 명백하게 어떠한 해악의 결

8) 「성폭력범죄의 처벌 등에 관한 특례법」 제14조의2 (허위영상물 등의 반포등)

과를 발생시키는 외부적, 대외적인 행위라기보다는, 해악을 발생시킬 위험이 있는 사적 영역에서의 행위로서의 성격이 강하며, 이러한 이유로 소지죄의 경우에는 3년 이하의 징역, 3천만원 이하의 벌금형으로 비교적 경하게 규정되어 있다. 또한 동법 제13조 ‘통신매체를 이용한 음란행위’ 조항에서는 “자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화, 우편, 컴퓨터, 그 밖의 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말, 음향, 글, 그림, 영상 또는 물건을 상대방에게 도달하게 한 사람은 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.”고 규정하고 있는데 이러한 범죄 역시 통신제한조치가 필요한 중대 범죄에 해당하고 보기는 어렵다. 또한 청소년성보호법 제2조 제5호는 “아동·청소년성착취물”을 실제 아동, 청소년이 등장하는 것뿐만 아니라, 가상의 아동, 청소년 캐릭터가 등장하는 표현물도 이에 해당한다고 규정하고,⁹⁾ 실제 아동, 청소년의 성을 착취하여 제작한 표현물과 구분없이 같은 규정으로 처벌하고 있는바, 이는 과잉하다는 지적이 있는데, 이러한 경우에도 통신제한조치를 하는 것이 적절한지도 논의가 필요하다. 현행 통신비밀보호법 역시 일반 형법상의 성범죄 중에서도 제302조(17세 이상의 미성년자나 심신미약자에 대한 위계 또는 위력에 의한 간음), 제303조(업무상 위력

① 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 “영상물등”이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 “편집등”이라 한다)한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

② 제1항에 따른 편집물·합성물·가공물(이하 이 조에서 “편집물등”이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 조에서 같다)을 반포등을 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등을 한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

③ 영리를 목적으로 영상물등의 대상자의 의사에 반하여 정보통신망을 이용하여 제2항의 죄를 범한 자는 3년 이상의 유기징역에 처한다.

④ 제1항 또는 제2항의 편집물등 또는 복제물을 소지·구입·저장 또는 시청한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

⑤ 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중한다.

9) 아동·청소년의 성보호에 관한 법률 제2조(정의)

5. “아동·청소년성착취물”이란 아동·청소년 또는 아동·청소년으로 명백하게 인식될 수 있는 사람이나 표현물이 등장하여 제4호 각 목의 어느 하나에 해당하는 행위를 하거나 그 밖의 성적 행위를 하는 내용을 표현하는 것으로서 필름·비디오물·게임물 또는 컴퓨터나 그 밖의 통신매체를 통한 화상·영상 등의 형태로 된 것을 말한다.

제11조(아동·청소년성착취물의 제작·배포 등)

① 아동·청소년성착취물을 제작·수입 또는 수출한 자는 무기 또는 5년 이상의 징역에 처한다.

② 영리를 목적으로 아동·청소년성착취물을 판매·대여·배포·제공하거나 이를 목적으로 소지·운반·광고·소개하거나 공연히 전시 또는 상영한 자는 5년 이상의 유기징역에 처한다.

③ 아동·청소년성착취물을 배포·제공하거나 이를 목적으로 광고·소개하거나 공연히 전시 또는 상영한 자는 3년 이상의 유기징역에 처한다.

④ 아동·청소년성착취물을 제작할 것이라는 정황을 알면서 아동·청소년을 아동·청소년성착취물의 제작자에게 알선한 자는 3년 이상의 유기징역에 처한다.

⑤ 아동·청소년성착취물을 구입하거나 아동·청소년성착취물임을 알면서 이를 소지·시청한 자는 1년 이상의 유기징역에 처한다.

⑥ 제1항의 미수범은 처벌한다

⑦ 상습적으로 제1항의 죄를 범한 자는 그 죄에 대하여 정하는 형의 2분의 1까지 가중한다.

에 의한 간음)와 같이 상대적으로 경한 범죄는 통신제한조치 대상 범죄에서 제외하고 있다는 것도 고려할만하다.

비교적 경한 범죄에까지 통신제한조치를 허용하게 되면 다수의 사람들이 통신제한조치의 대상자가 되고, 그 대상자와 대화한 다수인의 통신과 사생활의 비밀까지도 제한되게 되므로, 국가의 국민에 대한 기본권 침해의 정도도 더욱 중대해진다는 점도 고려해야 한다. 예를 들면 온라인상에서 영상물등의 “소지, 시청” 등의 행위는 적극적, 능동적, 대외적 행위를 수반하지 않는 경우가 있고, 고의 없이 우연한 기회에 수동적으로 이루어질 수도 있는 것인데, 단순히 유포 혐의자가 있는 단체 채팅방에 있었다는 이유, 혹은 특정 서비스에 접속한 기록이 있다는 이유 등만으로 많은 사람들이 ‘혐의자’가 되기 쉽고, 통신제한조치 대상자가 될 수 있으며, 이들과 대화한 수많은 사람들의 통신의 비밀, 사생활의 비밀도 함께 침해될 위험이 높아지는 것이다.

또한 특정 법률에 규정된 범죄 전체를 통신제한조치 대상 범죄로 포괄적으로 규정하면 추후 해당 법률에 추가될 수 있는 경범죄까지 자동으로 포괄되게 되고, 이로써 경범죄 혐의자에 대한 통신제한조치도 가능하게 되는바, 이 역시 헌법상 과잉금지원칙에 위반하여 국민의 통신의 비밀의 자유와 사생활의 비밀의 자유를 침해하는 결과로 이어질 위험이 크다.¹⁰⁾

6. 결론

결론적으로, 범죄의 경중을 따지지 않고 「성폭력범죄의 처벌 등에 관한 특례법」 및 「아동·청소년의 성보호에 관한 법률」이라는 특정 법률에 규정된 범죄 전체를 통신제한조치 대상 범죄로 규정하는 본 개정안은 다수 국민들의 통신의 비밀과 자유, 사생활의 비밀과 자유를 침해할 위험은 매우 큰 반면, 달성할 수 있는 공익은 불분명하므로, 헌법상의 과잉금지원칙, 비례의 원칙에 위배할 소지가 높다.

<끝>

10) 실제 최근 발의된 법안 중에는 일반 명예훼손, 모욕까지 성폭력처벌법상의 성폭력범죄에 포함시키도록 하는 개정안이 있어 논란이 되고 있다.