

## 통신사실확인자료에 관한 비교법적 고찰 - 일본과의 비교를 중심으로 -\*

김연진\*\*

김일환\*\*\*

### 【목 차】

#### I. 서론

#### II. 일본의 통신사실확인자료 법제

##### 검토

1. 개관
2. 일본 통신방수법의 법제
3. 통신자료 및 통신사실확인자료 제공
4. 소결

#### III. 우리나라 통신사실확인자료 법제

##### 검토

##### 1. 개관

2. 우리나라의 통신비밀보호법 법제
3. 통신사실확인자료의 제공

#### IV. 우리나라 통신사실확인자료 관련 법제 정비방안

1. 감청 관련 법제
2. 통신사실확인자료 관련 법제

#### V. 결론

### 【국 문 요 약】

ICT의 발전으로 실시간 감청은 물론 실시간 위치정보 제공이 가능해지면서 통신의 비밀과 사생활 침해 우려가 제기되고 있다. 이에 따라 통신사실확인자료에 대한 검토가 요구된다.

특히 일본 통신방수법과의 비교가 요구되는데, 일본이 우리나라와 법제 전반이 유사함에도 일본 통신방수법상 감청의 요건이 우리나라보다

\* 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2022-0-00688, 개인정보보호 관련 정책 변화를 유연하게 반영하여 준수하는 AI 플랫폼 연구 및 개발).

\*\* 주저자, 미국헌법학회 회원, 법학박사(S.J.D)

\*\*\* 교신저자, 성균관대학교 법학전문대학원 교수, 법학박사

더 엄격하게 규정되어 있기 때문이다. 이외에도 통신방수법에 감청집행 시 입회인의 참여가 규정되어 있는 점, 통신사실확인자료가 일본 형사소송법상 압수·수색영장을 통해 제공되고 있는 점은 우리나라의 통신비밀보호법을 개선함에 있어 시사하는 바가 크다.

향후 통신비밀보호법은 이와 같은 점을 반영하여 감청의 요건을 엄격하게 함과 동시에 감청의 대상범죄를 축소할 필요가 있다. 또한, 감청집행시 책임자의 참여를 규정하고, 통신사실확인자료 제공을 형사소송법상 압수·수색절차에 의하도록 함으로써 절차적 투명성을 제고할 필요가 있다. 일본 통신방수법의 비교검토를 통해 우리나라 통신사실확인자료에 대한 법제정비개선방안을 도모할 수 있을 것이다.

## I. 서론

ICT(Information and Communications Technologies)는 인공지능(AI), 사물인터넷(IoT) 등 지능정보기술의 발달을 선도하고 있으며, 통신감청기술도 이에 부응하여 발전을 거듭하고 있다. 그러나 교묘한 기술의 발달은 좁게는 통신의 자유, 넓게는 사생활의 자유의 침해를 야기하고 있어 헌법적 문제를 발생시킨다.

고전적으로 감청은 미행·잠입이나 탐문(聞込み) 등을 통하여 이루어져 왔으며<sup>1)</sup> 과학기술이 점차 발달하면서 한동안 유선감청이 행해지기도 하였다. 그러나 인터넷 등 통신기술의 발달과 AI, IoT 등 지능정보기술의 발달로 실시간 이루어지는 통신의 내용을 지득하는 것뿐만 아니라 실시간 휴대전화 위치정보 추적도 가능해지면서 사생활의 자유가 손쉽게 침해되는 상황이 전개되고 있다.

이와 같은 상황에서 헌법적 관점에서 통신비밀보호법제의 고찰이 요구된다. 즉, 통신비밀보호법제를 구체적으로 살펴봄으로써 통신비밀의 자유 및 사생활의 자유와 기술의 조화를 도모할 수 있다. 일본과 우리나라는 대륙법계를 계수함으로써 헌법뿐만 아니라 형사소송법 등 법제 전반에 있어서 유사한 부분이 존재하며, 통신비밀보호법제와 관련하여서도 상당

1) 笹倉宏紀, “捜査法の体系と情報プライバシー”, 刑法雑誌 55卷 3号 (2016), 424.

부분 비슷한 부분이 발견된다.

본 논문에서는 이러한 부분에 주목하여 일본과 우리나라의 통신비밀보호법제의 비교법적 검토를 통하여 우리나라 통신비밀보호법제를 살펴보기로 한다. 특히, 일본에서는 정보자기결정권과 사생활의 자유로 이루어진 프라이버시권리와 관련된 법제를 ‘정보 프라이버시 보호법제’라고 하고 있는바<sup>2)</sup> 이하에서는 이러한 점을 참조하여 통신내용 감청 및 통신사실확인자료를 검토하기로 한다.

## II. 일본의 통신사실확인자료 법제 검토

### 1. 개관

일본 헌법(憲法) 제21조 제2항에서는 통신의 비밀을 침해하여서는 안 된다고 규정함으로써 통신비밀의 자유를 보호하고 있다.<sup>3)</sup> 일본 형사소송법(刑事訴訟法) 제222조의2에서는 통신의 당사자 어느 쪽의 동의도 얻지 않고 전기통신을 감청하는 강제처분은 별도의 법률이 정하는 바에 의한다고 하면서<sup>4)</sup>, 국가기관에 의한 감청은 법적 근거가 필요하다는 점을 제시하고 있다.

즉, 통신비밀의 자유는 원칙적으로 보호되며, 법률에 근거가 있어야만 감청이 용인된다는 입장을 취하고 있다. 이에 따라 범죄수사를 위한 통신방수에 관한 법률(犯罪捜査のための通信傍受に関する法律)이 제정되게 되었다.

범죄수사를 위한 통신방수에 관한 법률(이하 ‘통신방수법’)은 전기통신

2) 일본의 프라이버시권리는 일본 헌법 제13조의 ‘개인의 존중’으로부터 파생된다. 鈴木 正朝, “「プライバシーの権利と個人情報保護法」”, 마이ナンバーシンポジウム資料 (2012), 10.

3) 日本国憲法 第二十一条 集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。○2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。(일본국헌법 제21조 ① 집회, 결사 및 언론, 출판, 그 밖에 모든 표현의 자유는 보장된다. ② 검열을 하여서는 아니 된다. 통신의 비밀을 침해하여서는 아니 된다.)

4) 日本 刑事訴訟法 第二百二十二条之二 通信の当事者のいずれの同意も得ないで電気通信の傍受を行う強制の処分については、別に法律で定めるところによる。(형사소송법 제222조의2 통신의 당사자 중 어느 쪽의 동의도 얻지 않고 전기통신을 감청하는 강제처분에 대해서는 별도의 법률이 정하는 바에 의한다.)

의 감청을 하기 위한 요건들을 구체적으로 규정하고 있으며, 통신사실화 인자료를 형사소송법상 압수·수색영장을 발부받음으로써 확보받을 수 있다. 이에 따라 이하에서는 일본 통신방수법과 형사소송법을 중심으로 살펴보면서 부수적으로 일본 개인정보보호에 관한 법률(個人情報の保護に関する法律, 이하 ‘개인정보보호법’)을 살펴보기로 한다.

## 2. 일본 통신방수법의 법제

### 가. 일본 통신방수법상 방수(傍受)의 의미

일본 통신방수법은 중대범죄에서 범인 간의 상호연락 등에 이용되는 전화 및 그 밖의 전기통신 감청을 실시하지 않으면 사안의 진상을 규명하기가 현저히 곤란한 경우가 증가함에 따라, 이에 적절히 대처하기 위하여 형사소송법상 전기통신 감청을 실시하는 강제처분에 관하여 요건, 절차 및 그 밖에 필요한 사항을 정하기 위한 목적에서 제정되었다(제1조).<sup>5)6)</sup>

일본 통신방수법상 ‘방수(傍受)’란 우리 통신비밀보호법상 ‘감청’을 의미하는 것으로 볼 수 있다.<sup>7)</sup> 통신방수법 제2조 제2항에서는 현재 행해

- 5) 平成十一年法律第三百七十七号 犯罪捜査のための通信傍受に関する法律(目的)第一条 この法律は、組織的な犯罪が平穩かつ健全な社会生活を著しく害していることにかんがみ、数人の共謀によって実行される組織的な殺人、薬物及び銃器の不正取引に係る犯罪等の重大犯罪において、犯人間の相互連絡等に用いられる電話その他の電気通信の傍受を行わなければ事案の真相を解明することが著しく困難な場合が増加する状況にあることを踏まえ、これに適切に対処するため必要な刑事訴訟法(昭和二十三年法律第三百三十一号)に規定する電気通信の傍受を行う強制の処分に関し、通信の秘密を不当に侵害することなく事案の真相の的確な解明に資するよう、その要件、手続その他必要な事項を定めることを目的とする。
- 6) 조직적인 범죄가 평온하고 건전한 사회생활을 현저하게 해치고 있다는 점에 비추어, 일본 통신방수법 제1조의 중대범죄는 여러 사람의 공모에 의해 실행되는 조직적인 살인, 약물 및 총기 부정거래와 관련된 범죄 등을 의미하며, 동법 제1조에서 동법이 통신의 비밀을 부당하게 침해하지 않고 정확한 진상 규명에 이바지하도록 하기 위하여 그 요건, 절차 및 그 밖에 필요한 사항을 정하는 것을 목적으로 하고 있음을 규정하고 있다.
- 7) 傍受(ぼうじゅ)란 “무전(無電)을 제3자가 수신”한다는 의미를 갖고 있다(ぼうじゅ [傍受], 네이버 일본어사전, <https://ja.dict.naver.com/#/entry/jako/7c170c3261564d7f961198afefed1e86>). “傍受”를 분설하면 “옆에서 받다”라고 해석할 수 있는데, “傍(そば)”은 “곁, 옆”을 뜻하고(傍, 네이버 일본어사전, <https://ja.dict.naver.com/#/entry/jako/b6c8ef17b3ac4d3bbf8ba0d51e53dbe8>), “受(じゅ)”는 “받다”를 뜻하기 때문이며(受, 네이버 일본어사전, <https://ja.dict.nave>

지고 있는 다른 사람과의 통신에 대하여 그 내용을 알기 위하여 해당 통신의 당사자 어느 쪽의 동의도 없이 이를 받는 것을 ‘방수’라고 규정하고 있다.<sup>8)</sup> 즉, 동법은 통신 당사자의 동의를 받지 않고 ‘실시간’에 이루어지는 통신의 내용을 지득하는 것을 규제하고 있다. 따라서 실시간이 아니라 과거에 이루어졌던 통신의 내용을 지득·채록하는 것은 ‘방수’라고 할 수 없다.

#### 나. 방수(傍受)의 대상범죄

종래 일본 통신방수법상 ‘방수’의 대상범죄는 ① 총기범죄(무기 등 제조법), ② 조직범죄(조직적 범죄의 처벌 및 범죄 수익 규제 등에 관한 법률), ③ 집단밀항(출입국 관리 및 난민인정법), ④ 마약범죄(대마 단속법, 마약 및 향정신성 의약단속법, 아편법, 국제적인 협력 하에 규제 약물에 관한 부정행위를 조장하는 행위 등 방지를 위한 마약 및 향정신성 의약단속법 등 특례에 관한 법률, 각성제 단속법) 4가지에 국한하여 규정되었다.<sup>9)</sup> 그러나 2016년 개정에 따라 ① 폭발물의 사용(爆発物の使用), ② 현주건조물등 방화(現住建造物等放火), ③ 살인(殺人), ④ 상해·상해치사(傷害·傷害致死), ⑤ 체포 및 감금(逮捕及び監禁) 또는 체포등치사상(逮捕等致死傷), ⑥ 미성년자약취·유괴(未成年者略取及び誘拐) 등, ⑦ 절도(窃盜), ⑧ 강도(強盜)·강도치사상(強盜致死傷), ⑨ 사기·전자계산기 사용사기(詐欺·電子計算機使用詐欺), ⑩ 공갈(恐喝), ⑪ 아동포르노등(児童ポルノ等)의 범죄가 추가되었다.<sup>10)</sup>

r.com/#/entry/jako/3e8b7baf05784ef7ab0e808e873b67cd), 이를 사전적 의미와 연결하면, 방수(傍受)란 우연히 혹은 고의로 근방에서 들리는 소리를 지득(知得) 혹은 채록(採録)하는 행위를 포괄적으로 뜻한다고 볼 수 있다.

- 8) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (定義) 第二条 2 この法律において「傍受」とは、現に行われている他人間の通信について、その内容を知るため、当該通信の当事者のいずれの同意も得ないで、これを受けることをいう。
- 9) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 別表第一 (第三条、第十五条関係)
- 10) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 別表第二 (第三条、第十五条関係)

### 다. 방수의 요건

검사 또는 사법경찰원은 범죄의 실행과 관련된 사항을 내용으로 하는 통신이 이루어질 것으로 의심할 만한 상황이 있고, 다른 방법으로는 범인을 특정하거나 범행의 상황이나 내용을 분명히 하는 것이 현저히 곤란할 때에(보충성) 재판관이 발부하는 영장에 의하여 감청할 수 있다(통신방수법 제3조)<sup>11)</sup>.

이는 일본 최고재판소의 판시와도 상통한다. 일본 최고재판소는 1999년 판결에서 “중대한 범죄와 관련된 피의사건에 대하여 피의자가 죄를 범했다고 의심할 만한 충분한 이유가 있고, 또한 해당 전화에 의해 피의 사실과 관련된 통화가 이루어지는 개연성이 있는 동시에 전화 감청 이외의 방법에 따라서는 그 죄에 관한 중요하고도 필요한 증거를 얻는 것이 현저하게 곤란하다는 등의 사정이 존재하는 경우에 있어서 전화방수중에 의해 침해되는 이익의 내용, 정도를 신중하게 고려한 후에, 또한 전화방수를 실시하는 것이 범죄의 수사상 정말로 부득이한 것으로 인정되는 때에는 법률이 정하는 절차에 따라 이를 행하는 것도 헌법상 허용된다고 해석하는 것이 상당하다”고 하면서 방수(傍受), 즉 감청이 제한적인 요건에 따라 이루어져야 한다고 한 바 있다.<sup>12)</sup>

- 
- 11) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (傍受令状) 第三条 “検察官又は司法警察員は、次の各号のいずれかに該当する場合において、当該各号に規定する犯罪(第二号及び第三号にあっては、その一連の犯罪をいう。)の實行、準備又は証拠隠滅等の事後措置に関する謀議、指示その他の相互連絡その他当該犯罪の實行に関連する事項を内容とする通信(以下この項において「犯罪関連通信」という。)が行われると疑うに足りる状況があり、かつ、他の方法によっては、犯人を特定し、又は犯行の状況若しくは内容を明らかにすることが著しく困難であるときは、裁判官の発する傍受令状により、電話番号その他発信元又は発信先を識別するための番号又は符号(以下「電話番号等」という。)によって特定された通信の手段(以下「通信手段」という。)であって、被疑者が通信事業者等との間の契約に基づいて使用しているもの(犯人による犯罪関連通信に用いられる疑いがないと認められるものを除く。)又は犯人による犯罪関連通信に用いられると疑うに足りるものについて、これを用いて行われた犯罪関連通信の傍受をすることができる。
- 12) 最決平成11年12月16日 “重大な犯罪に係る被疑事件について、被疑者が罪を犯したと疑うに足りる十分な理由があり、かつ、当該電話により被疑事実に関連する通話の行われる蓋然性があるとともに、電話傍受以外の方法によってはその罪に関する重要かつ必要な証拠を得ることが著しく困難であるなどの事情が存する場合において、電話傍受により侵害される利益の内容、程度を慎重に考慮した上で、なお電話傍受を行うことが犯罪の捜査上真にやむを得

한편, 통신방수(傍受)의 연장에 대해서는 통신방수법 제7조에서 규정하고 있다. 동법 제7조 제1항에 의하면, 지방재판소의 재판관은 필요하다고 인정하는 때에 검사 또는 사법경찰원의 청구에 의하여 10일 이내의 기간을 정하여 감청을 할 수 있는 기간을 연장할 수 있으며, 다만 감청을 할 수 있는 기간은 합하여 30일을 초과할 수 없다.<sup>13)</sup>

#### 라. 방수의 절차

방수(傍受)를 실시함에 있어서는 동법 제13조에 의하면 통신관리자 등을 입회시켜야 하고, 통신관리자 등을 입회시킬 수 없는 때에는 지방공공단체의 직원을 입회시켜야 하며, 입회인(立会人)은 검찰관 또는 사법경찰원에 대하여 해당 감청의 실시에 관하여 의견을 진술할 수 있다.<sup>14)</sup>

즉, 일본 통신방수법에서는 통신관리자 등이 방수(傍受) 집행 시 입회할 수 있다는 점을 명시함으로써 방수 집행 절차의 투명성을 담보하고 있다고 볼 수 있다. 그러나 입회인의 실시간 감청 집행 참여는 통신사업자뿐만 아니라 수사기관 양측에 모두 부담이 되었는데<sup>15)</sup> 이에 따라 입회인이 들어가지 않은 대신 일시적 보존을 명하는 통신방수(一時的保存を命じて行う通信傍受)와 특정전자계산기를 사용하는 통신방수(特定電子

---

ないと認められるときには、法律の定める手続に従ってこれを行うことも憲法上許されると解するのが相当である。”

- 13) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (傍受ができる期間の延長) 第七条 地方裁判所の裁判官は、必要があると認めるときは、検察官又は司法警察員の請求により、十日以内の期間を定めて、傍受ができる期間を延長することができる。ただし、傍受ができる期間は、通じて三十日を超えることができない。
- 14) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (立会い) 第十三条 “傍受の実施をするときは、通信管理者等を立ち合わせなければならない。通信管理者等を立ち合わせることができないときは、地方公共団体の職員を立ち合わせなければならない。  
2 立会人は、検察官又は司法警察員に対し、当該傍受の実施に関し意見を述べることができる。”
- 15) 통신사업자 측은 일정기간 감청을 집행하기 위한 설비와 장소를 확보함과 동시에 적합한 직원을 입회인으로 선정하여야 하는데, 입회인으로 선정된 직원은 본래의 업무를 할 수 없게 된다는 문제가 발생한다. 수사기관 측도 복수의 수사관이 통신사업자의 시설에 가서 언제 걸려올지 모르는 전화를 오로지 기다려야 한다. 이러한 부담이 크다는 것만으로도, 통신방수 실시에 대한 사실상 장애가 된다. 川出敏裕, “通信傍受法の改正について”, 東京大学法科大学院ローレビュー, 10卷 (2015), 106.

計算機を用いる通信傍受)가 새롭게 규정되어 동법이 개정되었다.

일시적 보존<sup>16)</sup>을 명하는 통신방수란, 검찰관 또는 사법경찰원이 재판관의 허가를 받아 통신관리자 등에게 명하여 감청영장이 기재하는 바에 따라 감청의 실시를 할 수 있는 기간 내에서 검찰관 또는 사법경찰원이 지정하는 기간에 행해지는 모든 통신에 대해 변환부호를 이용한 원신호의 암호화를 시키고 해당 암호화에 의해 작성되는 암호화 신호에 대해 일시적 보존을 시키는 방법으로 감청을 하는 것을 말한다(제20조 제1항).<sup>17)</sup>

특정전자계산기를 사용하는 통신방수란, 검찰관 또는 사법경찰원은 재판관의 허가를 받아 통신관리자 등에게 명하여 감청을 실시하는 동안 이루어지는 모든 통신에 대하여 변환부호를 이용한 원신호의 암호화를 시키고, 해당 암호화로 작성되는 암호화신호를 감청실시 장소에 설치된 특정컴퓨터에 전송하게 한 다음, ① 암호화 신호를 수신함과 동시에 대응 변환 부호를 이용하여 복호를 하고 복원된 통신에 대해 감청을 하는 방법 또는 ② 암호화 신호를 수신함과 동시에 일시적 저장을 하는 방법에 의해 해당 암호화 신호와 관련된 원신호에 의해 그 내용을 전달받는 통신을 감청하는 방법으로 이루어지는 감청을 말한다(제23조 제1항).<sup>18)</sup>

- 
- 16) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (定義) 第二条 5  
この法律において「一時的保存」とは、暗号化信号について、その復号がなされるまでの間に限り、一時的に記録媒体に記録して保存することをいう。(통신방수법 제2조 제5항이 법률에서 '일시적 보존'이란 암호화 신호에 대하여 그 복호가 이루어질 때까지의 기간에 한하여 일시적으로 기록매체에 기록하여 보존하는 것을 말한다.)
- 17) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (一時的保存を命じて行う通信傍受の実施の手続) 第二十条 検察官又は司法警察員は、裁判官の許可を受けて、通信管理者等に命じて、傍受令状の記載するところに従い傍受の実施をすることができる期間(前条の規定により傍受の実施を終了した後の期間を除く。)内において検察官又は司法警察員が指定する期間(当該期間の終期において第十八条の規定により傍受の実施を継続することができるときは、その継続することができる期間を含む。以下「指定期間」という。)に行われる全ての通信について、第九条第一号の規定により提供された変換符号を用いた原信号(通信の内容を伝達するものに限る。)の暗号化をさせ、及び当該暗号化により作成される暗号化信号について一時的保存をさせる方法により、傍受をすることができる。この場合における傍受の実施については、第十三条の規定は、適用しない。
- 18) 平成十一年法律第三百三十七号 犯罪捜査のための通信傍受に関する法律 (特定電子計算機を用いる通信傍受の実施の手続) 第二十三条 検察官又は司法警察員は、裁判官の許可を受



한편, 통신사업자는 정당한 이유 없이 검사 또는 사법경찰원의 감청 실시에 관한 협력요구를 거부해서는 안 된다(제12조).<sup>19)</sup>

### 3. 통신자료 및 통신사실확인자료 제공

#### 가. 제3자에 대한 통신이력 및 통신자료 제공

일본 개인정보보호법 제27조 제1항에서는 사전에 본인의 동의를 받지 않고 개인정보를 제3자에게 제공하지 않아야 한다고 규정하면서, 다만 법령에 근거가 있는 경우, 타인의 생명·신체 또는 재산의 보호, 공중보건의 향상 등 본인의 동의를 얻기 곤란한 경우, 학술목적에 위한 경우에는 개인정보의 제3자에 대한 제공이 가능하다고 하고 있다.<sup>20)21)</sup>

---

けて、通信管理者等に命じて、傍受の実施をしている間に行われる全ての通信について、第九条第二号イの規定により提供された変換符号を用いた原信号（通信の内容を伝達するものに限る。）の暗号化をさせ、及び当該暗号化により作成される暗号化信号を傍受の実施の場所に設置された特定電子計算機に伝送させた上で、次のいずれかの傍受をすることができる。この場合における傍受の実施については、第十三条の規定は適用せず、第二号の規定による傍受については、第二十条第三項及び第四項の規定を準用する。

一 暗号化信号を受信すると同時に、第九条第二号ロの規定により提供された対応変換符号を用いて復号をし、復元された通信について、第三条及び第十四条から第十六条までに定めるところにより、傍受をすること。

二 暗号化信号を受信すると同時に一時的保存をする方法により、当該暗号化信号に係る原信号によりその内容を伝達される通信の傍受をすること。

19) 平成十一年法律第百三十七号 犯罪捜査のための通信傍受に関する法律（通信事業者等の協力義務 第十二条 検察官又は司法警察員は、通信事業者等に対して、傍受の実施に関し、傍受のための機器の接続その他の必要な協力を求めることができる。この場合においては、通信事業者等は、正当な理由がないのに、これを拒んではならない。

20) 平成十五年法律第五十七号 個人情報の保護に関する法律（第三者提供の制限）第二十七条

21) 일본 「개인정보의 보호에 관한 법률」 제27조에서는 다음과 같은 경우에 한하여 개인정보의 제3자에 대한 제공이 가능하다고 규정한다. ① 법령에 근거가 있는 경우, ② 타인의 생명, 신체 또는 재산의 보호를 위하여 필요한 경우로서 본인의 동의를 얻기가 곤란한 경우, ③ 공중보건의 향상 또는 아동의 건전한 육성 추진을 위하여 특히 필요한 경우로서 본인의 동의를 얻기 곤란한 경우, ④ 국가의 기관이나 지방공공단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 본인의 동의를 얻음으로써 해당 사무의 수행에 지장을 미칠 우려가 있는 경우, ⑤ 해당 개인정보 취급사업자가 학술연구기관 등인 경우로서, 해당 개인정보 제공이 학술연구 성과의 공표 또는 교수로 인해 어쩔 수 없는 경우, ⑥ 해당 개인정보 취급사업자가 학술연구기관 등인

즉, 법령에 근거가 있다면 제3자에게 개인정보를 제공할 수 있는 것이다. 일본 형사소송법 제197조 제2항은 “수사에 관해서는 공무소 또는 공공·민간단체에 조회하여 필요한 사항의 보고를 요구할 수 있다”고 하면서 사실조회에 대해 규정하고 있는데, 이 규정에 따라 전기통신사업자가 수사기관의 사실조회에 응하여야 하는 것인지가 문제된다.

전기통신사업에서의 개인정보 보호에 관한 가이드라인 해설(電気通信事業における個人情報保護に関するガイドラインの解説)에 의하면, 원칙적으로 사실조회에 응해야 하지만, 전기통신사업자의 통신비밀보호의무에 따라 통신의 비밀에 속하는 사항(통신 내용에 머무르지 않고 통신 당사자의 주소·성명, 발신 장소, 통신 연월일 등 통신의 구성요소 및 통신 횟수 등 통신의 존재 사실 유무를 포함)을 제공하는 것은 타당하지 않다.<sup>22)</sup>

이에 따라 통신비밀과 관련이 없는 단순한 통신자료에 대해서는 형사소송법 제197조 제2항의 사실조회절차에 따른 정보조회가 가능하다고 할 수 있으며<sup>23)</sup> 수사기관은 통신비밀과 관련된 자료의 수집을 위하여 법원으로부터 압수·수색영장을 발부받아야 할 것이다. 그러나 사실조회는 임의수사이므로 이를 거부하는 경우 법원의 영장을 발부받음으로써 집행할 수 있으므로 전기통신사업자는 사실상 수사기관에 협조할 수밖에 없는 위치에 있다.<sup>24)</sup>

일본에서 통신자료뿐만 아니라 통신사실확인자료의 제공 또한 형사소송법의 규정에 따라 이루어지고 있다. 이는 일본 통신방수법이 감청에 대해서만 규율할 뿐 통신자료 내지 통신사실확인자료에 관하여 아무런 규정을 두고 있지 않은 데에 기인하고 있다.<sup>25)</sup>

---

경우로서 해당 개인정보를 학술연구 목적으로 제공할 필요가 있는 경우 예외적으로 개인정보의 제3자에 대한 제공이 가능하다.

22) 電気通信事業における個人情報保護に関するガイドライン (令和4年個人情報保護委員会・総務省告示第4号) の解説, 93-94.

23) 이성기, “「통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차」에 관한 비교법적 연구”, 법과 정책연구 제14집 제1호, 한국법정책학회(2014), 17.

24) 이성대·이경열·김일환, “통신비밀자료의 제공과 관련한 주요국의 법제비교와 시사”, 경원법학 제10권 제3호, 가천대학교 법학연구소(2017), 244.

따라서 통신사실확인자료의 제공은 일본 형사소송법상 압수·수색 영장을 통해 가능하다. 한편, 형사소송법 제114조에 따라 압수·수색 영장의 집행에 있어 간수자(看守者) 등의 입회가 요구되므로<sup>26)</sup> 통신사실확인자료의 제공에 있어서도 간수자 등의 입회가 이루어진다고 볼 수 있다.

#### 나. 위치정보의 제공

위치정보는 개인이 방문하는 위치에 관한 정보를 제공할 수 있으며, 개인이 방문하는 정치단체, 병원 진료과 등 개인의 사상 및 건강정보에 관한 정보까지 포함하여 민감정보에 해당할 여지가 크다.

2023년 7월 시행을 앞두고 있는 미국 캘리포니아 주 프라이버시권에 관한 법률(CPRA: California Privacy Rights Act)은 소비자의 정밀한 지리적 위치(a consumer's precise geolocation)에 관한 정보를 민감정보(Sensitive Personal Information)로 규정하기도 하였다. 이는 위치정보가 프라이버시와 관계된다는 점을 제시한다. 일본 학계에서는 위치정보는 통신의 비밀을 침해하는 것이 아니라고 보고 있다.<sup>27)</sup>

이에 따라 위치정보의 수집에 있어서는 영장이 요구된다. 미국 연방대법원 Katz v. United States (1967) 판결<sup>28)</sup>에서는 압수·수

25) 이혼재, “일본의 휴대전화에 대한 통신감청 및 위치정보추적수사”, 법학연구 통권 제60집, 전북대학교 법학연구소(2019), 245.

26) 日本 刑事訴訟法 第百十四條 公務所内で差押状、記録命令付差押状又は搜索状の執行をするときは、その長又はこれに代わるべき者に通知してその処分に立ち会わせなければならない。  
2 前項の規定による場合を除いて、人の住居又は人の看守する邸宅、建造物若しくは船舶内で差押状、記録命令付差押状又は搜索状の執行をするときは、住居主若しくは看守者又はこれらの者に代わるべき者をこれに立ち会わせなければならない。これらの者を立ち会わせることができないときは、隣人又は地方公共団体の職員を立ち会わせなければならない。(일본 형사소송법 제114조 ① 공무소 내에서 압수장 또는 수색장의 집행을 할 때에는 그 장(장) 또는 그를 갈음할 자에게 통지하여 그 처분에 입회하도록 하여야 한다. ② 전항의 규정에 의한 경우를 제외하고, 사람의 주거 또는 사람이 간수하는 저택, 건조물 또는 선박 내에서 압수장 또는 수색장을 집행할 때에는 住居主(주거주)나 간수자 또는 이들을 갈음할 사람을 이에 입회하도록 하여야 한다. 이들을 입회하도록 할 수 없을 때에는 이웃사람 또는 지방공공단체의 직원을 입회하도록 하여야 한다.)

27) 이혼재, 위의 논문, 246에서 재인용.

색의 적법성 판단기준으로서 “프라이버시의 합리적 기대 (reasonable expectation of privacy)”가 제시되었다.<sup>29)</sup> United States v. Miller (1976) 판결에서는 “프라이버시의 합리적 기대”가 인정되지 않아 증거물인 “수표”를 영장 없이 압수·수색하기도 하였으나<sup>30)</sup> Carpenter v. United States (2018) 판결을 통해 “휴대전화의 위치를 추적할 때 마치 휴대전화 사용자의 발목에 감시장치를 장착하도록 한없이 완전하게 가까운 감시가 이루어진다”면서 영장의 발부를 받아야 한다는 점을 분명히 하였다.<sup>31)</sup>

일본에서도 위치정보는 통신사실확인자료로서 수사기관은 법원의 영장을 발부받음으로써 전기통신사업자로부터 이를 수집할 수 있다. 최근 문제되고 있는 휴대전화의 위치정보는 기지국을 특정함으로써 얻을 수도 있고(기지국 정보), 휴대전화에 내장된 GPS(Global Positioning System)에 연결하여 수집될 수 있는데(GPS 정보), 양자는 모두 영장을 발부받음으로써 취득될 수 있다.<sup>32)</sup>

기지국 정보는 수백미터 때때로 몇킬로미터의 오차가 있는데 반해, GPS 정보는 최대 수미터의 오차가 있어 GPS 정보가 더 정확하다고 하는바<sup>33)</sup> 기지국 수사는 GPS 수사보다 정확도가 떨어진다고 할 수

28) Olmstead v. United States, 277 U.S. 438 (1928) 판결에서는 법원의 승인 없이 FBI에 의해 획득된 증거로서 공공지역에서 감청된 사적인 전화대화의 증거가 인정되었으나 Katz v. United States, 389 U.S. 347 (1967) 판결에서 영장없이 취득한 공중전화의 감청은 불법이라고 판시하였다.

29) Katz v. United States, 389 U.S. 347 (1967). It is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a reasonable expectation of privacy, unless certain exceptions apply.

30) United States v. Miller, 425 U.S. 442 (1976). 이 판결에서 미국 연방대법원은 “수표가 기밀통신이 아니라 상거래에서 사용될 수 있는 협상가능한 수단(The checks are not confidential communications, but negotiable instruments to be used in commercial transactions)”이라고 보았기 때문에 Miller에 대해 프라이버시의 합리적 기대가 미치지 않는다고 판시하였다.

31) 伊藤徳子, “犯罪捜査のための基地局情報の取得”, 大学院研究年報 48号 (2019), 238.

32) 高村 紳, “携帯電話位置情報の取得による監視型捜査の適法性についての検討”, 法学研究論集 50号 (2019), 47.

33) GPS 정보는 단말기를 사용하는 자의 주변 5m의 거리까지 추적이 가능한 반면, 기지국의 통신범위가 최소 수백m에서 최대 수km에 이르는 등 그 폭이 다소 넓다. 박찬걸, “통신사

있다.<sup>34)</sup> 그러나 사용자가 임의로 제공하는 것으로 볼 수 없는 점, 평상시 휴대하는 것으로 상세하고 장시간 감시가 가능한 점, 이용자의 동향 파악까지 가능하다는 점에서 프라이버시의 합리적 기대가 미친다고 볼 수 있으며, 이러한 점에서 기지국 수사가 GPS 수사보다 프라이버시 침해가 더 크다고 할 수 있다.<sup>35)</sup>

일본 수사기관은 통신사실확인자료와 마찬가지로 과거의 휴대전화 위치정보자료는 법원으로부터 압수·수색영장을 통해 취득하고 있으며(일본 형사소송법 제222조 제1항, 제100조 제2항), 실시간 또는 장래의 위치정보는 검증영장(일본 형사소송법 제218조)을 발부받음으로써 수집하고 있다.<sup>36)</sup> 그러나 수사기관이 통신사업자로부터 문서의 형식으로 취득하는 행위는 ‘제출’에 가깝기 때문에, 기지국 정보는 검증영장이 아니라 압수·수색영장에 의하여야 한다는 견해도 있다.<sup>37)</sup>

일본은 통신감청에 비하여 위치정보자료수집은 헌법상 보장된 통신의 비밀을 침해하지 않는 강제처분이므로 감청에 비하여 낮은 정도의 보호로 족하다는 입장에 있으나<sup>38)</sup> 실시간 위치정보의 경우 사생활의 자유가 침해될 우려가 있어 보충성의 요건 등이 규정되어야 할 것으로 보인다.

---

실확인자료 제공제도의 현황 및 개선방안”, 형사법의 신동향 제44호, 대검찰청(2014), 209-210.

34) 高村 紳, “携帯電話位置情報の取得による監視型捜査の適法性についての検討”, 47.

35) 高村 紳, “携帯電話位置情報の取得による監視型捜査の適法性についての検討”, 58.

36) 일본 형사소송법 제222조 제1항에 의하면, 제100조의 규정은 검찰관·검찰사무관 또는 사법경찰직원이 제218조, 제220조 및 제221조에 의하여 하는 압수 또는 수색에 대하여 이를 준용한다. 동법 제100조 제2항에서는 진신에 관한 서류로서 법령의 규정에 의해 통신사무를 취급하는 자가 보관하거나 소지하고 있는 것은, 피고사건과 관계가 있다고 인정하기에 충분한 상황이 있는 것에 한하여 이를 압수하거나 또는 제출하도록 할 수 있다고 규정하고 있다. 이혼재(주 25), 247, 249.

37) 이 견해에 의하면 수사기관이 기지국 정보 기록을 통신 사업자 내의 컴퓨터에 표시시켜 직접 확인하는 방법을 취하는 것이 아니기 때문에 검증영장은 적합하지 않다. 즉, 검증은 오관의 작용을 통해 장소·물건·사람의 존재, 위치, 성질 등을 파악하는 처분이므로, 기지국 정보 기록을 문서 등 형식으로 통신사업자로부터 물리적으로 취득하는 데에는 검증영장이 아닌 압수·수색영장을 발부받아야 한다고 한다. 伊藤徳子, “犯罪捜査のための基地局情報の取得”, 大学院研究年報 48号 (2019), 243.

38) 이혼재(주 25), 258.

#### 4. 소결

일본은 통신방수법을 통해 전기통신의 감청에 대한 규정을 마련하고 있으며, 통신사실확인자료는 형사소송법상 압수·수색영장에 의해 취득하도록 규정하고 있다.

이를 구체적으로 살펴보면 통신방수법상 감청 대상범죄를 한정함으로써 엄격한 요건 하에 감청을 인정하고 있음을 알 수 있으며, 입회인의 실시간 감청 집행 참여를 규정함으로써 감청 집행의 투명성을 제고하고 있다. 물론 최근 일정한 경우 입회인의 참여 대신 일시적 보존 또는 특정전자계산기를 사용하는 통신방수의 예외적 허용 규정이 추가되었으나, 이는 암호화를 통한 일시적 보존 또는 일시적 저장으로서 입회인의 참여 배제를 납득시킬 수 있는 장치를 마련하고 있어 감청 집행의 투명성을 크게 저해시킨다고 볼 수는 없다.

한편, 통신사실확인자료 및 과거의 휴대전화 위치정보는 형사소송법상 압수·수색영장을 통하여, 실시간 또는 장래의 위치정보는 형사소송법상 검증영장에 의하여 취득하도록 하고 있다. 이와 같이 통신사실확인자료의 취득이 형사소송법을 통해 이루어지도록 하고 있는 것은 수사의 필요성 및 범죄의 관련성 요건, 간수자 등의 참여를 충족시키기 위함이라고 볼 수 있다. 이는 궁극적으로 통신사실확인자료의 제공 절차의 투명성을 담보하는 것으로 볼 수 있다.

이를 종합하자면, 일본에서는 통신방수법과 형사소송법을 통해 각각 감청과 통신사실확인자료 제공에 대한 규정을 구체화함으로써 통신의 자유 및 사생활의 자유에 대한 보호 강화를 도모하고 있다. 이는 통신비밀보호법에 감청과 통신사실확인자료 제공에 대한 규정을 마련하고 있는 우리나라의 법제와는 상이한 부분으로, 우리나라 통신 관련 법제를 정비함에 있어서 참조할 부분이다. 또한, 일본 통신 관련 법제는 입회인 제도를 통한 집행 절차의 투명성에 초점을 두고 있으며, 통신사실확인자료의 취득을 압수·수색영장에 의하도록 함으로써 범죄의 관련성 요건을 충족하도록 하고 있어 우리나라 법제에 시사하는 바가 상당하다. 이하에서는 이러한 점에 주목하여 우리나라 통신사실확인자료 법제를 검토하기로 한다.

### III. 우리나라 통신사실확인자료 법제 검토

#### 1. 개관

우리나라의 감청 법제는 1993년 제정된 통신비밀보호법을 중심으로 마련되어 있으며<sup>39)</sup> 통신자료에 대한 수사기관에의 제공은 전기통신사업법에 규정되고 있다. 이는 일본의 법제와 다르다고 할 수 있는데, 일본에서는 우리나라의 통신비밀보호법에 상응하는 통신방수법에서 전기통신 감청에 대해 규율하면서, 통신자료 및 통신사실확인자료는 일본 형사소송법 규정에 따라 제공받고 있다.

우리나라의 통신비밀보호법은 제3조 제1항 본문을 통해 원칙적으로 감청을 금지하고 있다.<sup>40)</sup> 그러나 예외적으로 법률에 규정된 요건을 충족한 경우에 범죄수사를 위한 감청(제5조) 또는 국가안전보장을 위한 감청(제7조)을 인정하고 있다. 전기통신사업자에 대한 ‘통신자료’ 제공 요청은 전기통신사업법 제83조 제3항에 따라 가능하며, 범죄수사를 위한 ‘통신사실 확인자료’는 통신비밀보호법 제13조에 따라 법원의 허가를 얻어 열람 또는 제출이 가능하다.

또한 일본 통신방수법상 입회인이 실시간 감청 집행 참여를 할 수 있는 반면, 우리나라 통신비밀보호법에서는 감청 집행 과정에 입회인의 참여를 규정하고 있지 않는 점도 큰 차이점이라고 할 수 있다. 이하에서는 이러한 부분을 구체적으로 살펴보기로 한다.

#### 2. 우리나라의 통신비밀보호법 법제

##### 가. 감청의 의미

통신비밀보호법 제2조 제7호에 의하면 “감청”이란 전기통신에 대하여

39) 1998년 이후 경찰이나 국가정보원에 의한 도청시비, 개인에 의한 도청 등이 심각한 사회 문제로 대두되었다. 이에 따라 이러한 통신비밀의 침해를 막기 위하여 통신비밀보호법을 개정하자는 주장이 끊임없이 제기되었다. 김일환, “통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰”, 형사정책 제16권 제1호, 한국형사정책학회(2004), 38.

40) 통신비밀보호법 제3조(통신 및 대화비밀의 보호) ① 누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다.

당사자의 동의없이 전자장치 등을 사용하여 통신의 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.<sup>41)</sup> 이는 일본 통신방수법의 “방수”에 대응되는 개념이며, “방수”가 ‘현재 행해지고 있는 타인과의 통신’을 개념요소로 하고 있는 것과 마찬가지로 “감청”도 실시간 이루어지는 통신에 대해서만 가능하다.

대법원은 통신비밀보호법 제2조 제7호의 문언과 관련하여, “해당 규정의 문언이 송신하거나 수신하는 전기통신 행위를 감청의 대상으로 규정하고 있을 뿐 송·수신이 완료되어 보관 중인 전기통신 내용은 대상으로 규정하지 않은 점, 일반적으로 감청은 다른 사람의 대화나 통신 내용을 몰래 엿듣는 행위를 의미하는 점 등을 고려하여 보면, 통신비밀보호법상 ‘감청’이란 대상이 되는 전기통신의 송·수신과 동시에 이루어지는 경우만을 의미하고, 이미 수신이 완료된 전기통신의 내용을 지득하는 등의 행위는 포함되지 않는다”고 판시하였다.<sup>42)</sup>

이와 더불어 통신비밀보호법 제9조의3은 송·수신이 완료된 전기통신은 압수·수색·검증의 대상이 된다는 점을 전제로 하고 있는바, 이에 따라 송·수신이 완료된 전기통신은 ‘감청’의 대상에서 제외된다고 할 수 있다.

#### 나. 감청의 대상범죄

범죄수사를 위한 감청의 대상범죄는 통신비밀보호법 제5조 제1항 각호에 규정되어 있다. 제5조 제1항에 의하면 형법상 범죄 상당수를 비롯하여, 군형법, 국가보안법, 군사기밀보안법, 군사기지 및 군사시설 보호법, 마약류관리에 관한 법률, 폭력행위등 처벌에 관한 법률, 총포·도검·화약류등의 안전관리에 관한 법률, 특정범죄 가중처벌 등에 관한 법률, 국제상거래에 있어서 외국공무원에 대한 뇌물방지법 위반 등의 죄가 범죄수사를 위한 감청의 대상범죄가 된다.

그러나 이에 대해서는 대상범죄가 광범위하다는 지적이 제기된다. 물

41) 통신비밀보호법 제2조 (정의) 7. “감청”이라 함은 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.

42) 대법원 2012. 10. 25. 선고 2012도4644 판결.



론, 현행법상 대상범죄는 1993년 통신비밀보호법 제정당시 총 391개의 감청대상 범죄가 규정된 것에 비하면 축소 또는 조정된 것이나, 이는 일본의 법제와 비교해보면 너무 광범위한 것이다.<sup>43)</sup> 범죄를 규율하고 있는 법률도 다양할 뿐만 아니라 대상범죄로 규정된 형법상 범죄의 종류도 다양하여 개인의 통신의 비밀과 사생활의 자유가 과도하게 침해될 위험이 있다.<sup>44)</sup>

#### 다. 감청의 요건

감청은 통신비밀보호법 제5조 제1항의 대상범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고, 다른 방법으로 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가될 수 있다(보충성).<sup>45)</sup>

한편, ‘국가안보를 위한 감청’은 통신비밀보호법 제7조에 따라 이루어지고 있으며, 통신의 일방 또는 쌍방당사자가 내국인인 때에는 고등법원 수석판사의 허가를 받아야 한다.<sup>46)</sup> 그러나 국가안보를 위한 감청은 범죄수사를 위한 감청과는 달리 대상범죄를 규정하고 있지 않다는 점에서<sup>47)</sup> 감청으로 인한 국민의 기본권침해가 우려된다.

43) 나채준, “미국과 우리나라의 통신감청법률에 관한 비교법적 고찰”, 토지공법연구 제52집, 한국토지공법학회(2011), 346.

44) 구체적으로 「형법」에는 내란의 죄, 외환이 죄, 국교에 관한 죄, 공안을 해하는 죄, 폭발물에 관한 죄, 공무원의 직무에 관한 죄, 도주와 범죄은닉의 죄, 방화와 실화의 죄, 아편에 관한 죄, 통화에 관한 죄, 유가증권·우표와 인지에 관한 죄 살인의 죄, 체포와 감금의 죄, 협박의 죄, 약취·유인 및 인신매매의 죄, 강간과 추행의 죄, 신용·업무와 경매에 관한 죄, 권리행사를 방해하는 죄, 절도와 강도의 죄, 사기·공갈의 죄, 장물에 관한 죄 중 일부가 포함된다.

45) 통신비밀보호법 제5조(범죄수사를 위한 통신제한조치의 허가요건).

46) 통신비밀보호법 제7조 제1항 제1호에 따라 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 때와 군용전기통신인 경우에는 통신비밀보호법 제7조 제1항 제2호에 정한 바에 따라 서면으로 대통령의 승인을 받아야 한다.

47) 조 국, “개정 통신비밀보호법의 의의, 한계 및 쟁점: 도청의 합법화인가 도청의 통제인가?”, 형사정책연구 제15권 제4호, 한국형사법무정책연구원(2004), 111.

‘감청’의 기간은 2개월을 초과되지 못하고, 그 기간 중 감청의 목적이 달성되었을 경우에는 즉시 종료하여야 하는데, 동법 제5조 제1항의 허가요건이 존속하는 경우에는 소명자료를 첨부하여 2개월의 범위에서 감청의 연장을 청구할 수 있고, 이 경우 감청의 총연장기간은 1년을 초과할 수 없다.<sup>48)</sup>

헌법재판소는 2010년 통신제한조치기간 연장 무제한 허가제도 사건에서 “통신제한조치기간의 연장을 허가함에 있어 총연장기간 또는 총연장횟수의 제한이 없을 경우 수사와 전혀 관계없는 개인의 내밀한 사생활의 비밀이 침해당할 우려도 심히 크기 때문에” 총연장기간 또는 총연장횟수의 제한을 두지 않은 제6조 제7항 단서가 통신의 비밀을 침해하여 헌법에 위반된다고 판시하였다.<sup>49)</sup> 이에 총연장기간에 제한을 두도록 2019년에 법률이 개정된 것이다.

#### 라. 감청의 절차

통신비밀보호법은 감청의 방법에 관하여 규정하고 있지는 않다. 지능정보사회<sup>50)</sup>에 진입한 오늘날, 통신기술의 발달에 따라 통신매체별로 상이하게 감청이 이루어질 수밖에 없으므로 통신비밀보호법에 감청의 방법에 대해 구체적으로 규정하는 데에는 한계가 있을 수밖에 없다고 보인다.

다만 통신비밀보호법에서는 범죄수사 및 국가안보를 위한 감청과 긴급

48) 한편, 통신비밀보호법 제6조 제8항 단서는 각호에 따라 통신제한조치의 총연장기간을 3년으로 규정하고 있다. 즉, 형법 제2편 중 제1장 내란의 죄, 제2장 외환의 죄 중 제92조부터 제101조까지의 죄, 제4장 국교에 관한 죄 중 제107조, 제108조, 제111조부터 제113조까지의 죄, 제5장 공안을 해하는 죄 중 제114조, 제115조의 죄 및 제6장 폭발물에 관한 죄(제1호), 군형법 제2편 중 제1장 반란의 죄, 제2장 이적의 죄, 제11장 군용물에 관한 죄 및 제12장 위령의 죄 중 제78조·제80조·제81조의 죄(제2호), 국가보안법에 규정된 죄(제3호), 군사기밀보호법에 규정된 죄(제4호), 군사기지 및 군사시설보호법에 규정된 죄(제5호)에 대해서는 감청의 총연장기간이 3년을 초과할 수 없다.

49) 헌법재판소 2010. 12. 28. 선고 2009헌가30 결정.

50) 지능정보사회란 지능정보기술 및 지능정보기술과 다른 기술이나 서비스 등의 융합을 바탕으로 정치·경제·사회·문화를 포함한 모든 분야에서 새로운 가치를 창출하고 발전을 이끌어가는 사회를 말한다. 김일환, “지능정보사회에서 헌법의 역할과 기능”, 성균관법학 제32권 제3호, 성균관대학교 법학연구원(2020), 41.

감청의 허가절차 등에 대하여 구체적으로 규정을 두고 있다. 최근에는 2018년 헌법재판소의 패킷감청에 관한 헌법불합치결정<sup>51)</sup> 이후 제12조의2가 개정되면서 패킷감청 이후 사후관리규정이 2020년 도입되었다.

이에 덧붙여, 감청의 집행(제9조) 및 감청 집행에 관한 통지(제9조의2)에 대한 규정이 존재한다. 통신비밀보호법 제9조에 의하면 감청은 이를 청구한 검사·사법경찰관 또는 정보수사기관의 장이 집행하며, 감청의 집행을 위탁하거나 집행에 관한 협조를 요청하는 자는 통신기관등에 통신제한조치허가서 또는 긴급감청서등의 표지의 사본을 교부하여야 한다.<sup>52)</sup> 수사기관이 가진 감청기술이 급속도로 발전하는 통신기술에 상응하지 못하는 경우에는 전기통신사업자에게 불가피하게 협조를 요청할 수밖에 없는 것이다. 이에 따라 전기통신사업자는 통신비밀보호법 제15조의2에 따른 협조의무를 부담한다.<sup>53)</sup>

51) 헌법재판소 2018. 8. 30. 선고 2016헌마263 결정. 이 사건에서 헌법재판소는 패킷감청이 불특정 대상자에 대한 관련 없는 정보까지 수집하는 이상, “그 집행 단계나 집행 이후에 수사기관의 권한 남용을 통제하고 관련 기본권의 침해를 최소화하기 위한 제도적 조치가 제대로 마련되어 있지 않은 상태에서, 범죄수사 목적을 이유로 인터넷회선 감청을 통신제한조치 허가 대상 중 하나로 정하고 있으므로 침해의 최소성 요건을 충족한다고 할 수 없다”고 판시하면서, 패킷감청을 감청대상 중 하나로 정하고 있는 통신비밀보호법 제5조 제1항이 헌법에 위반된다고 하였다.

52) 통신비밀보호법 제9조(통신제한조치의 집행) ① 제6조 내지 제8조의 통신제한조치는 이를 청구 또는 신청한 검사·사법경찰관 또는 정보수사기관의 장이 집행한다. 이 경우 체신관서 기타 관련기관등(이하 “통신기관등”이라 한다)에 그 집행을 위탁하거나 집행에 관한 협조를 요청할 수 있다.

② 통신제한조치의 집행을 위탁하거나 집행에 관한 협조를 요청하는 자는 통신기관등에 통신제한조치허가서(제7조제1항제2호의 경우에는 대통령의 승인서를 말한다. 이하 이 조, 제16조제2항제1호 및 제17조제1항제1호·제3호에서 같다) 또는 긴급감청서등의 표지의 사본을 교부하여야 하며, 이를 위탁받거나 이에 관한 협조요청을 받은 자는 통신제한조치허가서 또는 긴급감청서등의 표지 사본을 대통령이 정하는 기간동안 보존하여야 한다.

③ 통신제한조치를 집행하는 자와 이를 위탁받거나 이에 관한 협조요청을 받은 자는 당해 통신제한조치를 청구한 목적과 그 집행 또는 협조일시 및 대상을 기재한 대장을 대통령이 정하는 기간동안 비치하여야 한다.

④ 통신기관등은 통신제한조치허가서 또는 긴급감청서등에 기재된 통신제한조치 대상자의 전화번호 등이 사실과 일치하지 않을 경우에는 그 집행을 거부할 수 있으며, 어떠한 경우에도 전기통신에 사용되는 비밀번호를 누설할 수 없다.

53) 통신비밀보호법 제15조의2(전기통신사업자의 협조의무) ① 전기통신사업자는 검사·사법경찰관 또는 정보수사기관의 장이 이 법에 따라 집행하는 통신제한조치 및 통신사실 확

한편, 검사는 감청을 집행한 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정, 참고인중지결정 제외)을 한 때에는 그 처분을 한 날부터 30일 이내에 감청대상이 된 전기통신의 가입자에게 감청을 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.<sup>54)</sup> 또한 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우에도 그 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정, 참고인중지결정 제외)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다.<sup>55)</sup>

### 3. 통신사실확인자료의 제공

#### 가. 통신자료의 제공

전기통신사업법 제83조 제3항에 의하면 ‘통신자료’는 이용자의 성명(제1호), 주민등록번호(제2호), 주소(제3호), 전화번호(제4호), 아이디(제5호), 가입일 또는 해지일(제6호)을 의미한다.<sup>56)</sup> 이는 단순한 ‘통신자료’로서 ‘통신내용’과 관계가 있다고 보기 어려우며, 오히려 전기통신 이용자의 개인정보에 가까운 내용이라고 볼 수 있을 것이다.<sup>57)</sup>

---

인자료제공의 요청에 협조하여야 한다.

② 제1항의 규정에 따라 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항, 통신사실확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정한다.

54) 통신비밀보호법 제9조의2(통신제한조치의 집행에 관한 통지) 제1항.

55) 통신비밀보호법 제9조의3(압수·수색·검증의 집행에 관한 통지) 제1항.

56) ‘통신자료제공’을 규정하고 있는 전기통신사업법 제83조 제3항에 의하면 전기통신사업자는 법원, 검사 또는 수사관서의 장, 정보수사기관의 장이 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 ‘통신자료’의 열람이나 제출을 요청하면 그 요청에 따를 수 있다.

57) 개인정보 보호법 제6조는 다른 법률과의 관계에 대해 규정하고 있다. 제6조에 의하면, 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보 보호법에서 정하는 바에 따라야 한다. 이에 따라 전기통신사업법 제83조 제3항이 ‘통신자료’에 대해 규정하고 있으므로 ‘통신자료’에 대해서는 개인정보 보호법이 아니라 전기통신사업법에서 정하는 바에 따라야 한다.

헌법재판소는 전기통신사업법상 통신자료 제공을 규정한 법률조항이 “전기통신사업자에게 이용자에 관한 통신자료를 수사관서의 장의 요청에 응하여 합법적으로 제공할 수 있는 권한을 부여하고 있을 뿐이지 어떠한 의무도 부과하고 있지 않으므로, 전기통신사업자는 수사관서의 장의 요청이 있더라도 이에 응하지 아니할 수 있고, 이 경우 아무런 제재도 받지 아니한다”고 하면서, 전기통신사업법상 통신자료 취득행위는 강제력이 개입되지 아니한 “임의수사”에 해당한다고 판시하였다.<sup>58)</sup>

즉, 전기통신사업법상 통신자료는 임의적 협조요청사항으로 규정되었는데(제83조 제3항), 통신사업자는 수사기관의 협조요청을 사실상 거절하기 힘들다고 볼 수 있다.<sup>59)</sup>

#### 나. 통신사실확인자료와 위치정보의 제공

종래 통신사실확인자료는 「통신비밀보호법」의 규제를 받지 않고 있었으며, 그로 인하여 수사기관의 요청에 따라 전기통신사업자가 통화내역자료를 제공함으로써 사실상 통신비밀을 확인하는 편법이 이루어지고 있었다.<sup>60)</sup> 이를 방지하기 위하여 2001년 12월 개정을 통해 통신비밀보호법에 통신사실확인자료 제공제도가 도입되었다.

통신사실확인자료 제공의 요청은 2001년 개정 통신비밀보호법에 의하

58) 헌법재판소 2012. 8. 23. 선고 2010헌마439 결정. 반면, 소수의견(재판관 김종대, 재판관 송두환, 재판관 이정미의 반대의견)은 이와 관련하여, “다수의견은 이 사건 통신자료 취득행위의 근거가 된 이 사건 법률조항이 전기통신사업자에게 어떠한 의무나 부담을 지우고 있지 않다는 점을 이 사건 통신자료 취득행위의 공권력 행사성을 부정하는 근거로 들고 있으나, 통신자료의 제출 여부는 전기통신사업자의 의사에 의해 통신자료의 제공요청시마다 개별적으로 결정되는 것이 아니라, 사실상 이 사건 법률조항에 의한 통신자료 제출 요구가 있으면 전기통신사업자는 이에 응하는 구조로 되어 있다고 보아야 할 것이다. 피청구인은 공권력인 수사권의 행사주체이고 이 사건 통신자료 취득행위는 청구인의 의사에 상관없이 진행되며 청구인의 통신자료를 보관하고 있는 전기통신사업자가 피청구인의 요청을 거절할 가능성은 사실상 희박하고 청구인이 통신자료의 제공을 저지하기 위해 그 과정에 개입할 수도 없는데, 이 사건 통신자료 취득행위는 피청구인이 우월적 지위에서 일방적으로 청구인의 통신자료에 대하여 대물적으로 행하는 수사행위로서 권력적 사실행위에 해당한다”는 입장을 밝혔다.

59) 김민이·이경열, “통신자료 등” 취급 문제의 해결을 위한 법해석론적인 제언”, 성균관법학 제28권 제1호, 성균관대학교 법학연구원(2016), 86.

60) 조 국(주 47), 115.

면 관할지방검찰청의 사전승인을 얻도록 되어 있었으나<sup>61)</sup> 2005년 개정을 통해 법원의 허가를 얻도록 개정되었다.<sup>62)</sup>

“통신사실확인자료”란 가입자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료를 의미한다.<sup>63)</sup>

IoT, ICT 등 정보통신기술의 발달로 인해 위치정보를 포함한 통신사실확인자료의 제공이 단순한 통신사실 내역을 확인한다는 의미를 넘어, 가입자의 대략적인 위치를 실시간으로 추적할 수 있게 되었다.<sup>64)</sup>

이러한 통신사실확인자료 중 사생활의 자유의 침해가 가장 큰 것은 위치정보라고 할 수 있다. 즉, 위치정보가 수사기관에 의해 알려짐으로써 정보주체의 사생활이 침해된다. 헌법재판소는 “수사기관은 위치정보 추

61) 통신비밀보호법 제13조 (통신사실 확인자료제공의 절차) ③ 검사 또는 사법경찰관이 제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 미리 서면 또는 이에 상당하는 방법으로 관할지방검찰청 검사장(검찰관 또는 군사법경찰관이 통신사실확인자료 제공을 요청하는 경우에는 관할 보통검찰부장을 말한다)의 승인을 얻어야 한다. 다만, 관할 지방검찰청 검사장의 승인을 얻을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체없이 그 승인을 얻어야 한다.

62) 통신비밀보호법 제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차) ② 제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.

63) 통신비밀보호법 제2조 제11호. 이를 구체화하면, 통신사실확인자료란 전기통신 가입자가 통화한 일시(가목) 및 통화 시작 및 종료시간(나목), 전기통신 가입자와 통화한 상대방(다목), 통화횟수(라목), 인터넷 접속 및 이용기록(마목), 기지국정보라고 할 수 있는 휴대폰으로 통화한 위치정보(바목), IP주소라고 할 수 있는 인터넷에 접속한 컴퓨터의 위치(사목)를 의미한다고 할 수 있다.

64) 김민지, “수사·정보기관의 통신정보 수집에 관한 비판적 연구”, 법학연구 제59권 제2호 통권 96호, 부산대학교 법학연구소(2018), 16.

적자료를 통해 특정 시간대 정보주체의 위치 및 이동상황에 대한 정보를 취득할 수 있으므로 위치정보 추적자료는 충분한 보호가 필요한 민감한 정보에 해당”된다고 판시하기도 하였다.<sup>65)</sup>

이와 관련하여 통신비밀보호법 제2조 제11호 바목의 “정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료”, 즉 이른바 기지국 정보가 문제된다.

특히 통신비밀보호법 제2조 제11호 바목은 ‘시점’을 명시하지 않아 실시간 기지국 정보가 통신사실확인자료로 제공될 근거로 작용하고 있다. 이에 따라 대다수 정보는 ‘실시간’ 접속중인 기지국 정보를 제공하는 것이 일반화되었고, 대상자의 현 위치를 파악해내는 일종의 ‘위치정보’로 기능하게 됨으로써 실시간 기지국 정보의 기본권침해성이 감청의 침해 정도와 유사한 수준으로까지 높아져 버렸다.<sup>66)</sup>

한편, 헌법재판소는 종래 통신비밀보호법에서 위치정보 추적자료 제공 요청 요건으로 수사의 필요성만을 규정하고 있었던 점을 지적하면서 종래 통신비밀보호법 제13조 제1항이 개인정보자기결정권과 통신의 자유를 침해한다고 판시한 바 있다.<sup>67)</sup> 이에 따라 통신비밀보호법 제13조 제2항에 제2조 제11호 바목·사목 중 실시간 추적자료 및 특정한 기지국에 대한 통신사실확인자료에 대해서는 보충성 요건이 추가되었다.<sup>68)</sup> 이러한 입법은 실시간 추적자료 및 기지국 정보의 기본권 침해가능성을 인정한 헌법재판소의 결정을 반영한 것이라고 할 수 있다.

65) 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정.

66) 오길영, “현행 통신비밀보호법의 문제점과 개선방향”, 언론과 법 제14권 제1호, (사)한국언론법학회(2015), 47.

67) 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정.

68) 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차) ② 검사 또는 사법경찰관은 제1항에도 불구하고 수사를 위하여 통신사실확인자료 중 다음 각 호의 어느 하나에 해당하는 자료가 필요한 경우에는 다른 방법으로는 범죄의 실행을 저지하기 어렵거나 범인의 발견·확보 또는 증거의 수집·보전이 어려운 경우에만 전기통신사업자에게 해당 자료의 열람이나 제출을 요청할 수 있다. 다만, 제5조 제항 각 호의 어느 하나에 해당하는 범죄 또는 전기통신을 수단으로 하는 범죄에 대한 통신사실확인자료가 필요한 경우에는 제1항에 따라 열람이나 제출을 요청할 수 있다.

1. 제2조 제11호 바목·사목 중 실시간 추적자료
2. 특정한 기지국에 대한 통신사실확인자료

## IV. 우리나라 통신사실확인자료 관련 법제정비방안

### 1. 감청 관련 법제

#### 가. 감청의 요건 강화

일본 통신방수법 제3조에 의하면 ① 범죄의 실행과 관련된 사항을 내용으로 하는 통신이 이루어질 것으로 의심할 만한 상황이 있고, ② 범인을 특정하거나 범행의 상황이나 내용을 분명히 하는 것이 현저히 곤란할 때에 재판관이 발부하는 영장에 의하여 감청할 수 있다.

우리나라의 통신비밀보호법 제5조에 의하면 ① 감청의 대상범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고, ② 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 감청이 허가된다.

이를 비교해보면 위 ①의 요건은 “범죄혐의의 상당성”으로, ②의 요건은 “보충성”으로 양국 법제가 비슷하다고 할 수 있다. 다만 일본의 법제는 범죄의 실행에 관한 “통신”이 이루어질 것을 명시하였다는 점에서 “범죄혐의의 상당성”이 좁게 해석될 여지가 있다.

또한 일본 통신방수법은 별표에서 대상범죄를 한정하고 있는 반면, 우리나라의 통신비밀보호법은 대상범죄가 광범위하게 규정되어 있어 개선을 요한다.

#### 나. 입회인 제도 규정의 필요성

일본 통신방수법 제13조에 의하면 통신사업자 측에서 선정한 입회인이 실시간 감청 집행에 참여할 수 있는데, 이는 감청 집행 과정의 투명성을 확보할 수 있는 장치로 기능한다. 즉, 입회인에 의한 상시입회, 방수의 원기록물예의 서명 및 봉인절차는 데이터의 개찬(改竄)·복사 등을 방지할 수 있는 것이다.<sup>69)</sup>

다만, 일본 통신방수법에서는 입회인의 실시간 감청 집행 참여가 통신사업자와 수사기관에 부담이 된다는 점에서, 입회인 참여가 없는 ‘일시적 보존을 명하는 통신방수’와 ‘특정전자계산기를 사용하는 통신방수’가 도

69) 内藤大海, “通信傍受法の拡大”, 刑法雑誌 55卷 1号 (2015), 114.



입되었다. 그러나 이에 대해서는 암호화 기능 또는 특정 장치로 인한 부정방지의 기술적 가능성은 일반적으로 장치의 보안에 대한 신뢰성 문제이기 때문에 절대로 문제가 발생하지 않는다고 단언할 수 없으며, 기계의 경우 수사기관에 대한 긴장·견제 기능이 감소한다는 점에서 ‘제3자’의 입회가 필요하다는 지적이 제기된다.<sup>70)</sup>

이러한 지적은 일견 타당하다. 기계는 오류의 위험성을 내포하고 있기 때문이다. 또한, 제3자의 입회는 입회하는 통신사업자 측 직원의 업무를 방해하지 않으며, 수사기관은 통신사업자에 입회를 요구하지 않아도 된다는 점에서 양측의 부담을 경감시킨다.

우리나라의 통신비밀보호법은 감청 집행 과정에서의 입회인의 참여를 규정하고 있지 않다. 이는 압수·수색영장의 집행에 간수자 등의 참여를 규정하고 있는 형사소송법 제123조와 대조적인 것으로 볼 수 있다.<sup>71)</sup>

즉, 송·수신이 완료된 이메일에 대한 압수·수색영장 집행시 간수자(看守者)가 일부 참여할 수 있는 반면, 현행법상 감청은 압수·수색절차에 의하지 않기 때문에 형사소송법 제123조가 적용되지 않는다.<sup>72)</sup>

70) 内藤大海(주 69), 위의 논문, 115.

71) 형사소송법 제123조(영장의 집행과 책임자의 참여) ① 공무소, 군사용 항공기 또는 선박·차량 안에서 압수·수색영장을 집행하려면 그 책임자에게 참여할 것을 통지하여야 한다.  
 ② 제1항에 규정한 장소 외에 타인의 주거, 간수자 있는 가옥, 건조물(建造物), 항공기 또는 선박·차량 안에서 압수·수색영장을 집행할 때에는 주거주(住居主), 간수자 또는 이에 준하는 사람을 참여하게 하여야 한다.  
 ③ 제2항의 사람을 참여하게 하지 못할 때에는 이웃 사람 또는 지방공공단체의 직원을 참여하게 하여야 한다.

72) 이메일 압수·수색의 과정은 다음과 같다. 먼저, 압수와 관련하여 살펴보면, 메일서버 관리자가 메일서버의 이메일들을 관리자의 컴퓨터로 다운로드한 후 CD 등 저장매체에 담아 주며, 관리자는 반드시 당해 이메일의 해쉬값을 산출함으로써 원본과 사본의 무결성을 담보하여야 하며, 그 결과를 별도 파일에 기록하여야 한다(CD에의 동봉 또는 CD표면이나 서류 등예의 기재). 다음으로 수사관의 수색이 이루어지는데, 수사관은 사무실에서 범죄와 관련 있는 이메일만 선별하여 메일서버 관리자를 찾아가 선별된 파일만을 담은 CD의 제작을 요청하게 되며, 이 때에도 해쉬값을 산출해야 한다. 법정에서 CD는 해쉬값 검증을 먼저 받게 되는데, 증거로 제출된 CD의 완전성과 무결성이 입증된다. 메일서버 관리자는 압수절차에의 참여는 가능할 수 있으나, 현실적으로 수사기관 사무실에서 진행되는 수색절차 전반에 참여할 수 없어 형사소송법 제123조의 간수자 참여 규정이 적용되지 않는다는 문제가 발생한다. 오길영, “국가정보원의 패킷감청론에 대한 비판”, 민주법학 제48호, 민주주의법학연구회(2012), 361-362.

감청은 실시간 통신내용을 지득하기 때문에 집행과정에서 개작(改作)이나 변동이 이루어지지 않도록 이를 감독할 입회인 제도의 필요성이 대두된다. 이러한 점은 송·수신이 완료된 상태에서 이루어지는 전기통신에 대한 압수·수색의 경우보다 감청의 경우 집행과정의 투명성이 담보되어야 한다는 점을 보여준다. 또한 입회인은 통신사업자측이 아닌 제3자이어도 무방한바, 통신사업자 소속 직원이 입회인이 되는 경우 객관성을 결여할 수 있고 업무의 지장을 초래할 수 있기 때문이다. 향후 통신비밀보호법에서는 감청집행시 참여하는 입회인 제도를 규정하여 절차적·결과적 투명성을 제고하여야 할 것이다.

## 2. 통신사실확인자료 관련 법제

### 가. 통신사실확인자료와 영장주의

일본 법제하에서는 통신사실확인자료의 제공은 형사소송법상 압수·수색영장을 통해 이루어지고 있다. 반면, 우리나라는 통신비밀보호법 제13조에 따라 법원의 허가를 받은 경우에 전기통신사업자로부터 통신사실확인자료를 제공받고 있다. 양국의 법제는 통신사실확인자료 제공에 있어 법원의 영장을 요구한다는 점에서 다르지 않다고 할 수 있다. 헌법재판소는 위치정보 추적자료 제공요청은 통신비밀보호법이 정한 강제처분에 해당되므로 헌법상 영장주의가 적용된다고 판시하였는바<sup>73)</sup> 이러한 판시에 의하면 법원의 허가를 통한 통신사실확인자료의 제공 또한 영장주의가 적용된다고 볼 수 있다. 영장주의(令狀主義)란 법원 또는 법관이 발부한 적법한 영장에 의하지 않으면 형사절차상의 강제처분을 할 수 없다는 원칙을 말한다.<sup>74)</sup> 헌법상 영장주의는 신체의 안전과 자유를 포함한 국민의 기본적 인권의 보장을 확실하기 위한 것으로서 이와 같은 헌법의 규범력은 확고하게 유지되어야 하는 것이다.<sup>75)</sup>

영장주의의 본질은 강제처분을 함에 있어 중립적인 법관이 구체적 판단을 거쳐야 한다는 점에 있는바, 통신비밀보호법 제13조는 수사기관이

73) 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정.

74) 이재상, 형사소송법(제9판), 박영사(2012), 223.

75) 성낙인, 헌법학(제20판), 법문사(2020), 1178.

전기통신사업자에게 통신사실확인자료 제공을 요청함에 있어 관할 지방 법원 또는 지원의 허가를 받도록 규정하고 있으므로 헌법상 영장주의에 위배되지 아니한다.<sup>76)</sup> 실무에서는 영장청구사건을 담당하는 판사가 통신사실확인자료제공요청의 허가업무를 담당하고 있어 통신비밀보호법 제 13조는 영장주의에 의한 것이라고 볼 수 있다.<sup>77)78)</sup>

#### 나. 통신사실확인자료 제공의 법적 근거

우리나라의 경우 통신사실확인자료 제공이 형사소송법에 따라 이루어지게 되면 통신의 비밀 및 사생활의 자유의 보호가 더욱 강화된다고 할 수 있다. 형사소송법상 영장의 집행에 있어 당사자뿐만 아니라(제121조) 책임자가 참여할 수 있으며(제123조) 참여권자에 통지(제122조)가 이루어지고 있기 때문이다. 일본 통신방수법상 감청 집행 시 참여하는 입회인도 이러한 취지에서 비롯되었다고 볼 수 있다. 일본 형사소송법 제114조에 의하면 통신사실확인자료의 제공에 있어서도 간수자 등 입회가 이루어지고 있는데<sup>79)</sup>, 이러한 점은 통신사실확인자료 제공의 법적 근거를 형사소송법에 의하여야 한다는 사실을 뒷받침하고 있다.

또한 형사소송법상 압수·수색에 있어 관련성을 요구하고 있기 때문에<sup>80)81)</sup> 형사소송법에 의하게 되면 통신사실확인자료를 압수·수색함에

76) 헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정.

77) 통신제한조치 등 허가규칙(대법원규칙 제2949호, 2021. 1. 29.) 제3조(허가 등 업무 담당판사) 범죄수사를 위한 통신제한조치 및 통신사실 확인자료제공요청의 허가업무, 전기통신보관등의 승인업무는 지방법원 및 지원의 영장청구사건을 담당하는 판사가 담당한다.

78) 수사기관의 통신사실확인자료는 ‘법원의 허가’에 의해, 통화내용은 일반적인 압수수색영장에 의해, 통신자료는 권한있는 자의 요청에 의해 획득이 가능하다. 임규철, “전기통신사업자 보유의 통신사실확인자료에 대한 정보주체의 열람권 및 등사권의 인정 유무-대법원 2012.12.27. 선고 2010다79206 판결을 중심으로-”, 외법논집 제37권 제4호, 한국외국어대학교 법학연구소(2013), 85.

79) 주 26 참조.

80) 형사소송법 제215조(압수, 수색, 검증) ① 검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

② 사법경찰관이 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 검사에게 신청하여 검

있어 관련성 있는 정보만 수사기관에 제공될 것으로 보인다. 이에 따라 통신사실확인자료의 경우 형사소송법상 압수·수색절차에 따라야 할 것으로 보인다.<sup>82)</sup>

우리나라의 경우 2019년 개정을 통해 위치정보 제공에 있어 통신비밀보호법에서 보충성과 증거보전의 필요성을 요건으로 추가하는 규정이 신설되었는데, 이는 프라이버시를 보호하는 규정이라 할 수 있다. 이에 따라 형사소송법상 압수·수색영장이 집행되어 위치정보를 제공하게 되더라도 보충성과 증거보전의 필요성 요건이 여전히 적용되어야 한다고 보인다.

#### 다. 개인정보와의 관련성

통신사실확인자료는 식별성이 인정되는 개인정보성이 있기 때문에 개인정보자기결정권의 보호법익에 포함된다.<sup>83)</sup> 이에 일본 개인정보보호법

---

사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

- 81) 형사소송법 제219조에 의하면 제106조가 준용되므로 관련성 있는 정보만 압수·수색될 수 있으며, 정보의 범위를 정하여 출력·복제되는 것이 원칙이다.

형사소송법 제219조(준용규정) 제106조, 제107조, 제109조 내지 제112조, 제114조, 제115조 제1항 본문, 제2항, 제118조부터 제132조까지, 제134조, 제135조, 제140조, 제141조, 제333조 제2항, 제486조의 규정은 검사 또는 사법경찰관의 본장의 규정에 의한 압수, 수색 또는 검증에 준용한다. 단, 사법경찰관이 제130조, 제132조 및 제134조에 따른 처분을 함에는 검사의 지휘를 받아야 한다.

형사소송법 제106조(압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.

② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이항에서 “정보저장매체등”이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.

④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조 제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다.

- 82) 우리나라의 현행 통신비밀보호법 제13조 제1항에 의하면 ‘수사 또는 형의 집행을 위하여 필요한 경우’에 통신사실확인자료의 제공이 이루어지고 있다. 즉, 피의사실과의 관련성 요건이 통신비밀보호법 제13조에 규정되어 있지 않다.

제27조 제1항에서는 법령에 근거가 있는 경우 개인정보의 제3자에 대한 제공이 가능하다고 규정하고 있으므로, 개인정보가 포함된 통신이력의 제공과 관련하여 개인정보보호법과 형사소송법과의 관계가 문제된다.

앞에서 살펴본 바와 같이 단순한 통신자료는 일본 형사소송법 제197조 제2항의 사실조회에 의하여 제공될 수 있으나, 통신사실확인자료는 형사소송법상 압수·수색절차에 따라 제공된다. 이는 통신사실확인자료가 개인정보에 해당되더라도 형사소송법상 요건이 충족된 경우 법원의 압수·수색영장에 따라 제공될 수밖에 없다는 점을 나타낸다.

우리나라에서도 전기통신 가입자가 통화한 상대방, 상대방과 통화한 시간과 사용빈도 등을 포함한 통신사실확인자료는 가입자의 개인정보에 해당하지만, 통신비밀보호법 제13조에 따라 법원의 허가를 받은 경우 이를 제공받을 수 있도록 함으로써 일본의 법제와 유사한 태도를 취하고 있다고 볼 수 있다. 그러나 통신사실확인자료의 법적 근거가 형사소송법이 아닌 통신비밀보호법이라는 점은 일본 법제와 상이한 부분이라고 할 수 있다.

## V. 결론

감청 기술은 ICT의 급속한 발전에 상응하여 진화해왔다. 이에 따라 오늘날에는 전통적인 유선전화 감청이 아닌 SNS감청, 이메일감청 등이 등장하였으며, 수사기관이 전기통신사업자의 협조를 얻어야만 감청이 이루어지는 상황에 있다.

그러나 통신기술의 발달은 사생활의 침해를 야기하고 있다. 스마트폰의 상시 휴대는 기지국 정보를 통해 위치정보의 제공을 야기하고 있다. 위치정보는 이용자의 자발적인 동의 없이도 제공된다는 점에서 문제가 되며, 이를 통해 이용자의 동향과약까지 가능하다는 점에서 사생활을 중

83) 현행 개인정보 보호법상 개인을 알아볼 수 있는 정보에 해당하는 한 모든 종류 및 모든 형태의 정보가 개인정보가 될 수 있으며, 특정한 개인을 '식별할 수 있는' 정보가 개인정보가 된다. 즉, 개인정보가 되기 위한 기준은 "식별가능성"과 "결합용이성"이 된다. 김일환, "성폭력범죄의 처벌 등에 관한 특례법 제42조 제1항 위헌확인 - 현재 2016. 3. 31. 2015헌마688 결정에 대한 평석 -", 헌법재판연구 제3권 제2호, 헌법재판연구원(2016), 90-91.

대하게 침해한다고 할 수 있다. 이에 따라 통신사실확인자료에 대한 법제의 개관이 불가피하게 요구된다.

우리나라뿐만 아니라 일본의 경우에도 통신사실확인자료에 대한 법제 검토의 필요성은 동일하게 제기된다. 대륙법계를 따르고 있는 일본과 우리나라는 헌법, 형법, 형사소송법, 민법 등 법체계가 전반적으로 유사하며, 통신비밀보호 법제도 대동소이하다.

일본과 우리나라는 엄격한 요건 하에 감청을 허용하고 있다. 즉, 범죄를 실행하였다고 의심할만한 충분한 이유가 있고, 다른 방법으로는 범행의 수사가 현저히 곤란한 경우여야 감청을 허용하고 있다.

그러나 구체적으로 일본은 우리나라보다 감청의 허가를 더 어렵게 하고 있다고 볼 수 있다. 먼저, 감청을 함에 있어 통신방수법에 범죄혐의의 상당성 요건에 범죄실행과 관련된 “통신”이 이루어질 것을 명시함으로써 감청의 요건을 더 엄격하게 하고 있다. 다음으로, 우리나라 통신비밀보호법에 규정된 감청의 대상범죄가 광범위한 데에 비하여, 일본의 통신방수법은 감청 대상범죄를 한정하여 규정하고 있다. 또한 일시적 보존을 명하는 통신방수와 특정전자계산기를 사용하는 통신방수를 제외하고 감청 집행에 있어서 입회인의 참여를 허가함으로써 감청 집행 절차의 투명성을 확보하고 있다. 이에 덧붙여 일본에서는 감청을 통신방수법에 의하여 규정하고 있는 반면, 단순한 통신자료 및 통신사실확인자료는 형사소송법상 절차에 따라 제공받도록 함으로써 절차의 합법성을 더욱 강조하는 태도를 보이고 있다.

이러한 점은 향후 통신비밀보호법의 개선방향에 대한 시사점을 제공한다. 즉, 통신비밀보호법에 감청의 대상범죄를 축소하여야 한다는 점, 감청 집행시 입회인의 참여가 이루어져야 한다는 점이 반영되어야 한다. 이와 더불어 감청과 통신사실확인자료의 제공을 통신비밀보호법에 의하여, 통신자료에 대해서는 전기통신사업법에 따라 제공을 하고 있는 우리나라의 법제 또한 개선되어야 한다. 즉, 일본과 같이 통신사실확인자료의 제공을 형사소송법상 압수·수색영장을 발부받도록 함으로써 사생활의 자유 보호 강화를 도모하여야 할 것이다.

(논문투고일: 2022.11.30., 심사개시일: 2022.12.8., 게재확정일: 2022.12.22.)



▶ 김연진 · 김일환

통신방수법, 통신비밀보호법, 형사소송법, 감청, 통신사실  
확인자료

## 【참 고 문 헌】

### I. 국내문헌

- 김민이·이경열, ““통신자료 등” 취급 문제의 해결을 위한 법해석론적인 제언”, 성균관법학 제28권 제1호, 성균관대학교 법학연구원(2016)
- 김민지, “수사·정보기관의 통신정보 수집에 관한 비판적 연구 - 전기통신사업법 및 통신비밀보호법의 문제점 및 개선방안을 중심으로 -”, 법학연구 제59권 제2호 통권 96호, 부산대학교 법학연구소(2018)
- 김일환, “성폭력범죄의 처벌 등에 관한 특례법 제42조 제1항 위헌확인 - 헌재 2016. 3. 31. 2015헌마688 결정에 대한 평석 -”, 헌법재판연구 제3권 제2호, 헌법재판연구원(2016)
- 김일환, “지능정보사회에서 헌법의 역할과 기능”, 성균관법학 제32권 제3호, 성균관대학교 법학연구원(2020)
- 김일환, “통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰”, 형사정책 제16권 제1호, 한국형사정책학회(2004)
- 나채준, “미국과 우리나라의 통신감청법률에 관한 비교법적 고찰”, 토지공법연구 제52집, 한국토지공법학회(2011)
- 박찬걸, “통신사실확인자료 제공제도의 현황 및 개선방안”, 형사법의 신동향 제44호, 대검찰청(2014)
- 성낙인, 헌법학(제20판), 법문사(2020)
- 오길영, “국가정보원의 패킷감청론에 대한 비판”, 민주법학 제48호, 민주주의법학연구회(2012)
- 오길영, “현행 통신비밀보호법의 문제점과 개선방향”, 언론과 법 제14권 제1호, (사)한국언론법학회(2015)
- 이성기, “「통신사업자의 통신사실 확인자료 및 통신자료 제공의 요건과 절차」에 관한 비교법적 연구”, 법과 정책연구 제14집 제1호, 한국법정책학회(2014)
- 이성대·이경열·김일환, “통신비밀자료의 제공과 관련한 주요국의 법제



비교와 시사”, 경원법학 제10권 제3호, 가천대학교 법학연구소 (2017)

이재상, 형사소송법(제9판), 박영사(2012)

이훈재, “일본의 휴대전화에 대한 통신감청 및 위치정보추적수사”, 법학 연구 통권 제60집, 전북대학교 법학연구소(2019)

임규철, “전기통신사업자 보유의 통신사실확인자료에 대한 정보주체의 열람권 및 등사권의 인정 유무-대법원 2012.12.27. 선고 2010다 79206 판결을 중심으로 -”, 외법논집 제37권 제4호, 한국외국어대학교 법학연구소(2013)

조 국, “개정 통신비밀보호법의 의의, 한계 및 쟁점: 도청의 합법화인가 도청의 통제인가?”, 형사정책연구 제15권 제4호, 한국형사법무정책연구원(2004)

## II. 해외문헌

高村 紳, “携帯電話位置情報の取得による監視型捜査の適法性についての検討”, 法学研究論集 50号 (2019)

内藤大海, 通信傍受法の拡大, 刑法雑誌 55卷 1号 (2015)

鈴木 正朝, “「プライバシーの権利と個人情報保護法」”, マイナンバーシンポジウム資料, (2012)

笹倉宏紀, “捜査法の体系と情報プライバシー”, 刑法雑誌 55卷 3号 (2016)

伊藤徳子, “犯罪捜査のための基地局情報の取得”, 大学院研究年報 48号 (2019)

電気通信事業における個人情報保護に関するガイドライン (令和4年個人情報保護委員会・総務省告示第4号) の解説, (2022)

川出敏裕, “通信傍受法の改正について”, 東京大学法科大学院ローレビュー, 10卷 (2015)

Abstract

## Comparative Study on Communication Fact Confirmation Data

– Focusing on Comparison with Japan –

Younjin Kim

Ilhwan Kim

Concerns over infringe on privacy and confidentiality of communication are raised as it is possible to provide real time location information as well as real time monitoring with the development of ICT. The study of communication fact confirmation data is required, therefore.

The comparison with Japan's Communication Interception Act is required because the requirements for interception under Japan's Communication Interception Act are stricter than those of Korea, even though Japan's overall legislations are similar to Korea. In addition, the facts that the Communication Interception Act stipulates participation of the person in charge when executing interception and that communication fact confirmation data is provided through seizure and search warrants under Japan's Criminal Procedure Act have great implications in improving Korea's Communications Privacy Protection Act.

The Communications Privacy Protection Act should reflect these points and strict requirements for interception are needed in the future. Reducing the crime subject for interception is also required. It is necessary to stipulate the participation of the person in charge when executing interception and enhance procedural transparency by requiring the provision of communication

fact confirmation data to be subject to seizure and search procedures under the Criminal Procedure Act. Comparing Japan's Communication Interception Act would be possible to promote measures to improve legislation of communication fact confirmation data in Korea.



---

**Younjin Kim · Ilhwan Kim**

Communication Interception Act, Communication Privacy Act, Criminal Procedure Act, Interception, Communication Fact Confirmation Data