# 국가정보원의 RCS 활용의 불법성 검토

심 우 민

(국회입법조사처 입법조사관)

□ 현재 국가정보원의 해킹 프로그램(RCS) 구입 경위와 활용 세부내역에 대해 명확하게 사실 확인이 되지 않은 상황에서, 그 불법성을 검토하는 데에는 한계가 있음

□ 따라서 이하에서는 국가정보원 등의 관련 행위에 있어, 향후 법률상 쟁점화 될 수 있는 사항들에 대해 설명하기로 함

## 1) 「통신비밀보호법」상 절차규정

□ 「통신비밀보호법」 제3조는 그 행위의 주체가 누구이든 법률적 근거가 있는 경우를 제외하고는 감청을 금지한다는 원칙을 규정함

□ 국가안보 목적을 위한 국가정보원 등 정보수사기관의 통신제한조치(감청 등)을 위해서는 「통신비밀보호법」 제7조 및 제8조 등의 규정을 준수해야 함

○ 동법 제7조에 따라, 통신 당사자 중 내국인이 포함된 경우에는 고등법원 수석부장판사의 허가가 필요하고, 외국인 등에 대해서는 대통령의 승인이 필요함

**제7조(국가안보를 위한 통신제한조치)** ① 대통령령이 정하는 정보수사기관의 장(이하 "정보수사기관의 장"이라 한다)은 국가안전보장에 대한 상당한 위험이 예상되는 경우에 한하여 그 위해를 방지하기 위하여 이에 관한 정보수집이 특히 필요한 때에는 다음 각호의 구분에 따라 통신제한조치를 할 수 있다.

1. 통신의 일방 또는 쌍방당사자가 내국인인 때에는 고등법원 수석부장판사의 허가를 받아야 한다. 다만, 군용전기통신법 제2조의 규정에 의한 군용전기통신(작전수행을 위한 전기통신에 한한다)에 대하여는 그러하지 아니하다.

2. 대한민국에 적대하는 국가, 반국가활동의 혐의가 있는 외국의 기관·단체와 외국인, 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단이나 외국에 소재하는 그 산하단체의 구성원의 통신인 때 및 제1항제1호 단서의 경우에는 서면으로 대통령의 승인을 얻어야 한다.

……중략……

④ 제1항제2호의 규정에 의한 대통령의 승인에 관한 절차등 필요한 사항은 대통령령으로 정한다.

- 외국인 등의 경우에 대통령의 승인에 관한 구체적인 절차는 동법 제7조 제4항에 따라 대통령령(「통신비밀보호법 시행령」)에 위임되어 있음

> **「통신비밀보호법 시행령」 제8조(국가안보를 위한 통신제한조치에 관한 대통령의 승인)** ① 정보수사기관의 장이 법 제7조제1항제2호에 따라 통신제한조치를 하려는 경우에는 그에 관한 계획서를 국정원장에게 제출하여야 한다.
> ② 국정원장은 제1항에 따른 정보수사기관의 장이 제출한 계획서에 대하여 그 타당성 여부에 관한 심사를 하고, 심사 결과 타당성이 없다고 판단되는 경우에는 계획의 철회를 해당 정보수사기관의 장에게 요구할 수 있다.
> ③ 정보수사기관의 장이 제1항에 따른 계획서를 작성하는 경우에는 법 제6조제4항 및 이 영 제4조를 준용한다.
> ④ 국정원장은 제1항에 따라 정보수사기관의 장이 제출한 계획서를 종합하여 대통령에게 승인을 신청하며 그 결과를 해당 정보수사기관의 장에게 서면으로 통보한다.

○ 기타 사전적인 법원의 허나가 대통령의 승인 없이 이루어질 수 있는 긴급통신제한조치에 대해서는 동법 제8조에 규정하고 있음

> **제8조(긴급통신제한조치)** ① 검사, 사법경찰관 또는 정보수사기관의 장은 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 제5조제1항 또는 제7조제1항제1호의 규정에 의한 요건을 구비한 자에 대하여 제6조 또는 제7조제1항 및 제3항의 규정에 의한 절차를 거칠 수 없는 긴급한 사유가 있는 때에는 법원의 허가없이 통신제한조치를 할 수 있다.
> ……중략……
> ⑧ 정보수사기관의 장은 국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 제7조제1항제2호에 해당하는 자에 대하여 대통령의 승인을 얻을 시간적 여유가 없거나 통신제한조치를 긴급히 실시하지 아니하면 국가안전보장에 대한 위해를 초래할 수 있다고 판단되는 때에는 소속 장관(국가정보원장을 포함한다)의 승인을 얻어 통신제한조치를 할 수 있다.
> ……중략……
> ⑨ 제8항의 규정에 의하여 긴급통신제한조치를 한 때에는 지체없이 제7조의 규정에 의하여 대통령의 승인을 얻어야 하며, 36시간 이내에 대통령의 승인을 얻지 못한 때에는 즉시 그 긴급통신제한조치를 중지하여야 한다.

□ 따라서 위와 같은 규정에 입각하여 국가정보원의 감청 프로그램 활용행위가 법률상 관련 절차를 준수하였는지 여부를 검토해야할 필요성이 있을 것임

## 2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

□ 현행법 체계 속에서 이번 국가정보원의 RCS를 통한 감청행위에 대해 보다 직접적으로 적용될 수 있는 규정들은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)」에 규정되어 있다

고 볼 수 있음

□ 정보통신망 침해행위 및 악성프로그램 유포 등

○ 현행「정보통신망법」제48조는, 당해 규정의 현실적 타당성 여부를 별론으로 하더라도, 매우 포괄적으로 망 침해행위 등에 대해 규율하고 있음

**제48조(정보통신망 침해행위 등의 금지)** ① 누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다.
② 누구든지 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램(이하 "악성프로그램"이라 한다)을 전달 또는 유포하여서는 아니 된다.
③ 누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 하여서는 아니 된다.

○ 위 규정이 이번 사안에 적용되기 위해서는 해킹 프로그램 등을 통해 수행된 소위 저인망식 감청수행(절차 포함)이 '정당한 사유 또는 권한' 등에 해당할 수 없다는 점을 논증해야 할 필요가 있을 것으로 판단됨

□ 속이는 행위에 의한 정보수집

○ 현재 논란이 되고 있는 RCS 기술의 활용을 개괄적으로 검토해 볼 때, 일종의 피싱을 통한 정보수집 행위에 해당한다고 볼 수 있어, 이를 규정하고 있는「정보통신망법」제49조의2가 적용될 수도 있을 것임

**제49조의2(속이는 행위에 의한 개인정보의 수집금지 등)** ① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.
② 정보통신서비스 제공자는 제1항을 위반한 사실을 발견하면 즉시 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다.
③ 방송통신위원회나 한국인터넷진흥원은 제2항에 따른 신고를 받거나 제1항을 위반한 사실을 알게 되면 다음 각 호의 필요한 조치를 하여야 한다.
1. 위반 사실에 관한 정보의 수집·전파
2. 유사 피해에 대한 예보·경보
3. 정보통신서비스 제공자에 대한 접속경로의 차단요청 등 피해 확산을 방지하기 위한 긴급조치

○ 최초로 위 규정을 동법에 포함시킨 2005년 12월 7일 개정법률안의 제안이유와 더불어, 관련 규제의 소관 부처가 방송통신위원회라는 점을 고려해 본다면, 위 규정은 사실 기망행위를 통한 불법적인 '개인정보' 수집(피싱 등의 수법을 이용한 금융사기 피해)을 규제하기 위한 입법취지를 가지고 있다고 판단되지만, 구체적인 법문상에는 다소 포괄적인 표현인 "다른 사람의 정보"로 규정하고 있어 이번 국가정보원 RCS 사안에 적용될 여지가 있음

○ 또한 위 규정상에는 동법 제48조에서와 같은 '정당한 사유' 등을 별도로 요하지 않는다는 특이점이 있음

### 3) 「통신비밀보호법」상 감청설비

□ 감청설비를 직접적으로 규정하고 있는 「통신비밀보호법」상 규정들로는 다음과 같은 것들이 있음

○ 「통신비밀보호법」 제2조(정의), 제10조(감청설비에 대한 인가기관과 인가절차), 제10조의2(국가기관 감청설비의 신고), 제10조의3(불법감청설비탐지업의 등록 등), 제10조의4(불법감청설비탐지업자의 결격사유), 제10조의5(등록의 취소), 제15조(국회의 통제) 등

□ 감청설비의 개념에 대해서는 「통신비밀보호법」 제2조 제8호에서 규정하고 있음

> **제2조(정의)** 이 법에서 사용하는 용어의 정의는 다음과 같다.
> 8. "감청설비"라 함은 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치·기계장치 기타 설비를 말한다. 다만, 전기통신 기기·기구 또는 그 부품으로서 일반적으로 사용되는 것 및 청각교정을 위한 보청기 또는 이와 유사한 용도로 일반적으로 사용되는 것 중에서, 대통령령이 정하는 것은 제외한다.

○ 위 감청설비 개념정의 규정 단서에 의하여 감청설비에서 배제되는 설비 또는 기기들은 동법 시행령(대통령령)에서 정하고 있음

> **「통신비밀보호법 시행령」 제3조(감청설비 제외대상)** 법 제2조제8호 단서에 따라 감청설비에서 제외되는 것은 감청목적으로 제조된 기기·기구가 아닌 것으로서 다음 각 호의 어느 하나에 해당하는 것을 말한다.
> 1. 「전기통신사업법」 제2조제4호에 따른 사업용전기통신설비
> 2. 「전기통신사업법」 제64조에 따라 설치한 자가전기통신설비
> 3. 삭제
> 4. 「전파법」 제19조에 따라 개설한 무선국의 무선설비
> 5. 「전파법」 제58조의2에 따라 적합성평가를 받은 방송통신기자재등
> 6. 「전파법」 제49조 및 같은 법 제50조에 따른 전파감시업무에 사용되는 무선설비
> 7. 「전파법」 제58조에 따라 허가받은 통신용 전파응용설비
> 8. 「전기용품 안전관리법」 제2조제1호에 따른 전기용품 중 오디오·비디오 응용기기(직류전류를 사용하는 것을 포함한다)
> 9. 보청기 또는 이와 유사한 기기·기구
> 10. 그 밖에 전기통신 및 전파관리에 일반적으로 사용되는 기기·기구

○ 「통신비밀보호법」 제10조는 감청설비를 제조·수입·판매 등을 영위하는 자에 대해서는 미래창조과학부의 인가를 받도록 하고 있음

> **제10조(감청설비에 대한 인가기관과 인가절차)** ① 감청설비를 제조·수입·판매·배포·소지·사용하거나 이를 위한 광고를 하고자 하는 자는 미래창조과학부장관의 인가를 받아야 한다. 다만, 국가

기관의 경우에는 그러하지 아니하다.
② 삭제
③ 미래창조과학부장관은 제1항의 인가를 하는 경우에는 인가신청자, 인가연월일, 인가된 감청설비의 종류와 수량등 필요한 사항을 대장에 기재하여 비치하여야 한다.
④ 제1항의 인가를 받아 감청설비를 제조·수입·판매·배포·소지 또는 사용하는 자는 인가연월일, 인가된 감청설비의 종류와 수량, 비치장소등 필요한 사항을 대장에 기재하여 비치하여야 한다. 다만, 지방자치단체의 비품으로서 그 직무수행에 제공되는 감청설비는 해당 기관의 비품대장에 기재한다.
⑤ 제1항의 인가에 관하여 기타 필요한 사항은 대통령령으로 정한다.

○「통신비밀보호법」제10조의2는 국가기관이 보유하고 있는 감청설비에 대한 신고의무를 규정하고 있는데, 특히 제2항에서는 국가정보원과 같은 정보수사기관의 국회 신고 및 통보의무를 규정하고 있음

**제10조의2(국가기관 감청설비의 신고)** ① 국가기관(정보수사기관을 제외한다)이 감청설비를 도입하는 때에는 매 반기별로 그 제원 및 성능 등 대통령령이 정하는 사항을 미래창조과학부장관에게 신고하여야 한다.
② 정보수사기관이 감청설비를 도입하는 때에는 매 반기별로 그 제원 및 성능 등 대통령령이 정하는 사항을 국회 정보위원회에 통보하여야 한다.

□ 최근 RCS 기술 기반의 해킹 프로그램이「통신비밀보호법」상 감청설비에 해당하는 것으로 볼 수 있는 것인지에 대한 논란이 있음

○ 해킹 프로그램이 감청설비에 포함될 수 있다는 견해는 일반 PC에 해킹을 위한 프로그램이 설치되는 경우, 그 PC는 감청설비로 전환된다고 볼 수 있기 때문에, 이 경우 당해 프로그램도 감청설비에 포함된다는 해석을 제시함

○ "통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다"는「통신비밀보호법」의 입법취지(제1조)를 고려해 볼 때, 이와 같은 목적론적 해석은 타당한 측면이 있음

□ 그러나「통신비밀보호법」제정 이후 이제까지의 실무상, 현행 규정 해석에 있어 해킹 프로그램은 감청설비에 해당하지 않는다고 보는 것이 일반적인 관행인 것으로 판단됨

○ 법해석의 기초 원리인 문리적 해석에만 의존한다면, "감청설비"라는 표현은 물리적 장비 또는 기기(하드웨어)만 포함된다고 볼 여지도 있음

○ 이러한 해석을 뒷받침 해줄 수 있는 실무상 논거로는 불법감청설비탐지업의 등록 및 불법감청설비 조사업무의 위탁을 받고 있는 중앙전파관리소의「전파관련 조사 및 조치에 관한 규정」(중앙전파관리소 예규 제97

호)상에 있는 감청설비 판단기준([별표 2] 감청설비 판단기준 및 [별표 3] 감청설비 제외 대상기준)이 있음

**[표 1] 감청설비 판단기준(별표 2)**

| 장비 유형 | 조치사항 및 관계법령 |
|---|---|
| o 『영상과 음성』을 동시에 촬영·청취할 수 있는 유·무선 설비 | o 사법처리(통신비밀보호법 제17조)<br>- 통신비밀보호법 제2조 8호의 감청설비 제외 대상이 아닌 경우 대화의 감청에 사용될 수 있으므로 감청설비에 해당 |
| o e-메일 감시 등에 사용되는 솔루션의 설비 | o 사법처리(통신비밀보호법 제17조)<br>- **감청목적으로 특별히 개발 또는 제작한 e메일 감시 및 문서 유통경로 추적용 솔루션이나 프로그램 또는 시스템 등은 일반적인 전기통신기기로 볼 수 없음** |
| o 기존 무전기를 모방하여 감청설비로서의(무전기, 고성능이어폰, 안테나의 자체 제작 구성 등)기능을 할 수 있는 설비 | o 사법처리(통신비밀보호법 제17조)<br>- 제조는 새로운 아이디어에 의하여 새로운 감청설비를 제조뿐만 아니라 기존의 모델을 모방하여 감청설비로서의 기능을 할 수 있도록 한 경우도 해당 |
| o 범죄행위 등에 사용되는 초소형카메라에 내장된 마이크 및 고성능이어폰, 송·수신기 등으로 구성된 설비 | o 사법처리(통신비밀보호법 제17조)<br>- 대화 또는 전기통신의 감청에 사용되는 감청설비에 해당 |
| o 감청설비를 이용하여 실행에 착수하였으나 범행에 이루지 못한 미수범 | o 사법처리(통신비밀보호법 제18조)<br>- 통신비밀보호법 제16조 및 제17조에 규정된 죄의 미수범도 처벌 |

○ 위 기준은 관련 법 집행을 위한 조사업무에 활용되어 온 기준이기 때문에, 이제까지 현실적으로 감청설비 해당 여부를 판단하는 실무상 기준으로 활용되어 왔음(cf. 밑줄 강조 부분)

○ 이 기준에 의하면 물리적 장비 또는 기기 이외의 소프트웨어나 프로그램은 감청설비에 해당하지 않음

□ 현재 상황에서는 문리적 해석과 목적론적 해석이 서로 충돌하고 있는 상황이어서, 특정 해석 방식을 관철시키는 데에는 어려움이 있을 것으로 판단됨

○ 현실적으로, 향후 필요한 경우에는, 목적론적인 해석이 관철될 수 있도록 국가기관 및 정보수사기관들을 지속적으로 견제하는 방안과, 더 나아가서는 사법부가 목적론적 해석을 수용할 수 있는 논거들을 개발할 필요가

있을 것임

○ 다만 정치적 합의가 이루어진다면, 감청설비 개념정의 규정에 명문으로 소프트웨어 및 프로그램을 포함시키는 방향으로 법률을 개정함으로써 명확한 규범적 기준을 설정해 볼 수 있을 것임

- 그러나 이러한 법문 개정이 해킹 프로그램 등을 통한 감청을 합법화 시켜주는 것이 아니라는 점을 명확히 할 필요가 있음

### 4) 해킹 프로그램을 통한 감청방식 허용여부

□ 이번 국정원 사건과 관련하여, 보다 근본적인 문제는 해킹 프로그램을 이용한 감청방식을 현행법 체계 속에서 감청방식 그 자체로 수용할 수 있는지 여부라고 할 수 있음

○ 현재 언론 등에서는 주로 해킹 프로그램 등을 통한 감청에 초점을 맞추고 있지만, RCS 기반의 해킹 기술은 실시간 대화 내용의 취득은 물론이고, 송·수신이 완료된 대화 내용의 수집까지 가능하게 해주는 경우가 있을 수 있다고 판단됨

○ 위와 같은 행위가 이루어졌다면, 이는 단지 감청뿐만 아니라 실질적으로 「형사소송법」 제106조 및 「통신비밀보호법」 제9조의3 등에 근거한 정보저장매체 또는 전자정보의 압수·수색에 해당할 수 있으며, 결국 「통신비밀보호법」 제7조(국가안보를 위한 통신제한조치) 및 제8조(긴급통신제한조치)에 근거한 정보수사기관의 권한을 넘어선다고 볼 가능성이 있음

□ 정보저장매체 또는 전자정보에 대한 감청 또는 압수·수색, 특히 RCS 해킹 프로그램 등의 활용 문제는, 연혁적인 측면에서 볼 때 현행 법체계가 온전히 고려하지 못하고 있다고 평가할 수 있으며, 향후 이러한 감청방식을 현행 헌법 및 법률체계 하에서 인정할 수 있을 것인지에 대한 논의가 필요할 것으로 판단됨

○ 개인간 미디어 소통이 급격하게 증가하고 있는 상황에서, 해킹 프로그램 등을 통한 전자정보에 대한 감청 등이 이루어지게 되면, 범죄 수사와 관련이 없는 대화 및 참여자 정보 등을 무차별적으로 수집할 가능성이 매우 높아진다는 점에서, 「헌법」 제18조 등에 의해 보장되는 헌법적 가치가 쉽게 훼손될 수 있어 이에 유의할 필요가 있음

○ 현행 「통신비밀보호법」은 감청허가에 있어 감청방식을 제한하는 별도의 규정을 두고 있지 않고 있어, 이에 대한 사법 또는 입법적 차원의 대응이 필요함