형사정책연구 Korean Criminological Review
제30권 제1호(통권 제117호, 2019・봄)

비식별화된 통신사실확인자료의 제공 절차 도입을 통한 수사기관의 기본권 침해 최소화 방안

박현준*・이상진**

국 | 문 | 요 | 약

2018년 6월 헌법재판소는 “범죄수사의 필요성”이라는 요건만으로 수사기관으로 하여금 전기통신사업자로부터 가입자의 착·발신 전화번호, 착·발신 시간, 통화시간, 수·발신 번호 등의 정보를 취득할 수 있도록 하는 통신비밀보호법상 통신사실확인자료 제공요청 관련 조항에 대하여 위헌이라고 판시하였다.

위와 같은 헌법재판소의 판결 이전에도, 학계에서는 현행 통신사실확인자료를 이용한 통신수사에 관하여 통신비밀의 자유 및 사생활의 자유, 개인정보자기결정권 침해 등의 우려를 지속적으로 제기하였고, 법원의 통제 강화를 위한 법률 개정을 촉구하여 왔다. 그러나 그간 기술적 방법 내지 방식의 개선을 정착시킬 수 있는 법률 개정에 관한 논의는 거의 이루어지지 않았다.

본 논문에서는 수사 실무에서 널리 활용되고 있는 통신사실확인자료를 이용한 통신수사의 실태를 파악하여, 통신수사 시 수사 합목적성 달성 범위 내에서 기본권 침해를 최소화 하는 기술적 조치 방안을 제안하고자 한다. 즉, 수사기관에서 전기통신사업자에게 1차로 비식별화된 통신사실확인자료를 제공받고 그 중에 범죄 수사에 필요한 통신정보만을 선별한 다음, 2차로 해당 정보의 재식별화를 요청하는 형태로 수사 절차를 개선하는 것이 필요할 것이다. 또한 본 논문에서는 이러한 구체적인 기술적 조치 및 수사기법이 정착될 수 있도록 근거 법률의 개선 방안도 함께 제시하고자 한다.

❖ 주제어 : 통신비밀보호법, 통신수사, 비식별화, 개인정보, 프라이버시, 통신사실확인자료, 디지털 증거

* 주저자: 고려대학교 정보보호대학원 석사, hyun8007@hanmail.net
** 교신저자: 고려대학교 정보보호대학원 교수, sangjin@korea.ac.kr

Ⅰ. 서론

수사기관은 범죄 수사를 위하여 범인의 통신정보에서 범죄 관련 정보 또는 증거를 수집하는 방법을 개발하여 왔다. 오늘날 정보통신기술 발달로 인해 대부분의 범죄행위에 통신기기가 이용되고 있으며, 통신정보가 범죄혐의를 입증하는 핵심 증거로 작용하고 있다. 그 중 특히 휴대전화의 통화내역과 같은 통신사실확인자료는 현재 수사기관이 활발하게 수집하는 자료 중 하나이다.

여기서 문제는 수사기관이 통신사실확인자료 등 통신정보를 수집하는 것이 기본권 침해 요소를 내포하고 있다는 점이다.

통신정보는 그 정보의 양이 방대하여 수사기관이 수집과정에서 즉각 분석하여 범죄 수사에 필요한 정보만을 선별하여 압수하는 것이 곤란한 경우가 대부분이다. 이 때문에 수사기관에서는 분석을 차치하더라도, 최대한 많은 양의 통신정보를 수집하려고 하기 때문에 범죄 수사와는 무관한 많은 양의 통신정보가 수집되며, 결국 범죄 수사와 무관한 사람들의 통신비밀이 침해되고 있다.

또한 통신정보는 통상적으로 통신정보 주체뿐만 아니라 전기통신사업자와 같이 통신을 매개한 제3자가 정보를 보유하고 있으며, 수사기관은 제3자를 통해 통신정보 주체의 통신정보를 수집하는 경우가 대부분이다. 통신사실확인자료는 이러한 통신정보의 대표적인 예로 수사기관이 통신 매개자에게 통신사실확인자료의 제공을 요청하는 경우 전기통신사업자 등 제3자는 수사기관에 대한 자료 제공이 자신의 이익과 직접적인 관련이 없으므로, 정보제공에 있어 통신정보주체의 방어권과 같은 권리행사를 적극적으로 하지 않게 된다. 이러한 점 역시 통신정보주체의 기본권 침해 요소로 작용하고 있다.

현재 이와 같은 문제점의 해결방안으로 헌법상 영장주의의 적용, 법원의 통제 강화, 통신정보주체에 대한 통지 등 사후적 통제 강화 방안들이 주로 제시되고 있다. 이러한 쟁점에 대해서 수사기관과 시민단체는 각각 수사의 효율성과 기본권 침해의 축소를 주장하면서 대립하고 있으며 아직까지 별다른 해결책을 마련하지 못하고 있다.

본 논문은 수사의 합목적성 달성이 가능한 범위 내에서 기본권의 침해를 최소화하는 사전적 통제방안으로서 수사기관이 1차로 전기통신사업자 등으로부터 통신사

실확인자료를 비식별화된 형태로 제공받은 뒤, 이를 분석하여 필요한 정보를 선별하고, 2차로 해당 정보의 재식별화를 전기통신사업자 등에게 다시 요청하는 형태로 수사 절차를 전환하는 통신수사 방식의 개선을 촉구하며, 이를 뒷받침할 수 있는 법률의 개정을 제안하고자 한다. 이를 통하여, 수사와 무관한 국민의 기본권을 보호하고, 수사기관에서는 비침익적(非侵益的) 정보를 수사에 활용하여 수사의 합목적성을 달성할 수 있을 것이다.

Ⅱ. 현행 수사기관의 통신사실확인자료 취득과 기본권 침해

1. 통신정보와 통신수사

통신비밀보호법은 '통신'을 우편물 및 전기통신으로 분류(통신비밀보호법 제2조 제1호)하고, 다시 전기통신을 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것으로 규정하고 있다. 이와 같은 정의요소에 따르면, 통신정보란 우편물 내지 전자적 방식에 의하여 통신주체[1]간(이하 통신정보 주체라고 표현한다)의 송·수신 중이거나, 송·수신이 완료된 음향·문언·부호 또는 영상 이에 부수하여 수집·생성·가공되는 유·무형의 자료로 정의할 수 있다.

광의의 통신수사란 관계법령에 근거하여 이러한 통신정보를 수집·분석하여 범죄사실을 입증해가는 일련의 수사 활동으로 정의할 수 있으며,[2] 협의의 통신수사란 통신정보 중 우편물을 제외하고 전기통신 정보를 수집·분석하여 범죄 사실을 입증

1) 통신비밀보호법(법률 제15493호, 2017. 3. 20. 시행) 제2조 제4호에서는 통신 주체를 '당사자'라고 정의하고 있다.

2) 통신수사에 대하여 박노섭 등은 범인이 활용하는 통신수단에 대해 가입자 정보(통신자료), 통화내역 및 발신기지국 확인(통신사실확인자료), 감청 등을 통해 수사진행에 필요한 단서를 확보하는 수사방법이라고 정의하기도 하며, 우편물 또는 전기통신 수단의 사용에 따라 남게 되는 정보를 활용하여 증거를 수집하고 범인을 특정·검거하는 수사방법이라고 정의하기도 한다. 박노섭, 이동희, 이윤, 장윤식, 공저, 범죄수사학, 경찰대학 출판부, 2013, 272면; 김지온, 통신수사절차의 개선방안에 대한 법적연구, 고려대학교 석사학위 논문, 2017, 7면.

해가는 일련의 수사 활동으로 정의할 수 있다.[3)]

2. 법률에 의한 통신수사의 통제

가. 제한되는 기본권

대한민국 헌법 제17조 내지 제18조에서는 사생활의 자유와 통신의 자유를 헌법상 기본권으로 보장하고 있다. 이때 헌법 제17조, 헌법 제18조에 의해 보호되는 통신의 비밀 불가침에 관한 기본권은 개인이 그 의사나 정보를 전달 또는 교환하는 경우에 그 내용 등이 본인의 의사에 반하여 공개되지 아니할 권리를 의미하며[4)], 공개되지 아니할 통신비밀의 범위는 통신의 내용뿐만 아니라 통신의 당사자, 방식, 시간 및 장소, 횟수 등 모든 통신정보를 포함한다.[5)]

또한 헌법은 인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 개인정보자기결정권을 보장한다.[6)] 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 인격 주체성을 특정 짓는 사항으로서 개인의 동일성을 식별할 수 있게 하는 일체의 정보라 할 수 있고, 반드시 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적생활에서 형성되었거나 이미 공개된 개인정보까지 포함된다.[7)] 개인정보자기결정권은 자신의 개인정보를 다른 사람들에게 공개할 것인지 여부에 대한 결정권이 포함되어 있다[8)].

---

3) 통상 수사 실무상 통신수사는 협의의 통신수사를 의미한다. 본 논문에서는 협의의 통신수사의 개념으로 통신수사를 논하고자 한다.

4) 대법원 2016. 10. 13. 선고 2016도 8137 판결.

5) 강태수, 통신의 비밀보장에 관한 연구, 경희법학(제45권 제4호), 2010, 287~318면, 차진아, 범죄수사를 위한 통신사실확인자료 제공요청의 문제점과 개선방안, 법조 제67권 제2호, 2018, 378면, 그 근거에 대해 황성기는 이들 사항을 통해서도 특정한 통신의 '내용'을 '추정'할 수 있는 가능성이 있기 때문이라는 견해를 밝히고 있고, 황성기, 현행 통신비밀 보호법제의 헌법적 문제점, 언론과 법 제14권 제1호, 2015, 11~12면, 김일환은 누구와 어떤 방식으로 의사소통을 할지에 관한 의사결정과 통제의 권리를 침해할 수 있기 때문이라는 견해를 밝히고 있다. 김일환, 통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰, 형사정책 제16권 제1호, 2004, 34면.

6) 대법원 2014. 7. 24. 선고 2012다 49933판결.

7) 대법원 2014. 7. 24. 선고 2012다 49933 판결.

나. 법률에 의한 통신수사 규율체계

통신수사는 이와 같이 통신의 자유 및 개인정보자기결정권의 직접적인 침해를 가져오는 행위로 법률의 규율을 받고 있다. 이 때 통신정보주체로 부터 직접 통신정보를 수집하는 경우 형사소송법의 수사에 관한 일반적인 법리에 따르지만, 통신정보주체 간의 통신을 매개하거나 통신에 의한 서비스를 제공하여 관련 정보를 보유하게 된 통신정보주체 외 제3자(예컨대, 이동통신사업자 등 전기통신사업자, 포털 등 정보통신서비스 제공자 등이 이에 속한다. 이하 '전기통신사업자 등'이라고 표현한다)로부터 통신주체의 통신정보를 수집하는 경우에는 다소 복잡한 규율체계의 규율을 받는다.

통신수사 관계법령들은 전기통신사업자가 보유하게 된 통신정보들 중 일부를 통신자료, 통신사실확인자료 등으로 규정하고, 해당 정보가 수사기관에 제공되었을 경우 국민 기본권 침해 정도 여부에 따라, 수사기관이 해당 통신정보를 수집할 수 있는 요건을 달리 규정하고 있다.

[표 1] 수사기관의 통신정보 수집의 요건 및 절차

	통신자료	**통신사실 확인자료**	**통신 제한조치**	**기타 (송·수신이 완료된 전기통신 등)**
법률	전기통신사업법	통신비밀보호법	통신비밀보호법	형사소송법
요건	필요성	필요성	필요성 범죄혐의 개연성 *** 충분한 이유** 대상 범죄 한정 보충성	필요성 범죄혐의 개연성 *** 의심 정황** 관련성
절차	기관장 요청	법원 허가서	법원 허가서	영장

관련 법 규정들은 전기통신사업자 등이 적법하게 통신정보주체의 통신정보를 수집하였다고 하더라도, 이를 수집 외의 목적으로 사용할 수 없도록 제한을 두고 있다. 따라서 전기통신사업자 등은 통신정보주체의 통신정보를 수사기관에 임의적으

8) 헌법재판소 2015. 6. 25. 선고 2014헌마4673 결정.

로 제공할 수 없고, 정해진 요건과 절차를 충족하는 경우에 한해서 수사기관에 통신정보주체의 통신정보를 제공할 수 있다.

따라서 수사기관은 개인정보보호법, 통신비밀보호법, 전기통신사업법 등 특별법에 의한 통신정보 수집을 먼저 검토하고, 특별법에 의한 수집이 불가한 경우 형사소송법의 일반원칙에 따라 법원으로부터 압수·수색·검증영장을 발부받아 전기통신사업자 등으로부터 통신정보를 수집하게 된다.

3. 수사기관의 통신사실확인자료 수집으로 인해 침해되는 기본권

가. 수사기관의 통신정보 수집 현황

경찰수사연수원에서 2016년부터 2018년 상반기까지 일선 경찰서 수사·형사 경찰관 30명을 대상으로 진행한 전문교육과정인 추적수사전문과정의 총 10회 세미나 발표 자료를 분석한 결과, 현재 일선 경찰관들이 수집하고 있는 통신정보는 전기통신 행위자의 고유 식별자[9], 전기통신 행위자의 고유 식별자 외 부가정보[10], 송·수신이 완료된 전기통신 내역[11], 송·수신이 완료된 전기통신 내용[12], 송·수신 중인 전기통신 내역[13], 송·수신 중인 전기통신 내용(전기통신 감청) 등 총 6가지 형태로

9) 대표적인 형태로는 정보통신서비스 이용자의 주민등록번호, 생년월일과 결합된 성명, 이동통신 기기 고유번호(전화번호, USIM 카드 번호, IMEI, IMSI, MAC address, 단말기 시리얼번호 등), 이용자의 정보통신망 서비스 ID, 전기통신 역무 제공을 위하여 이용자에게 할당된 IP 및 여타 전기통신사업자 등 정보통신망 서비스 제공자가 이용자 식별을 위하여 이용자에게 부여한 고유번호

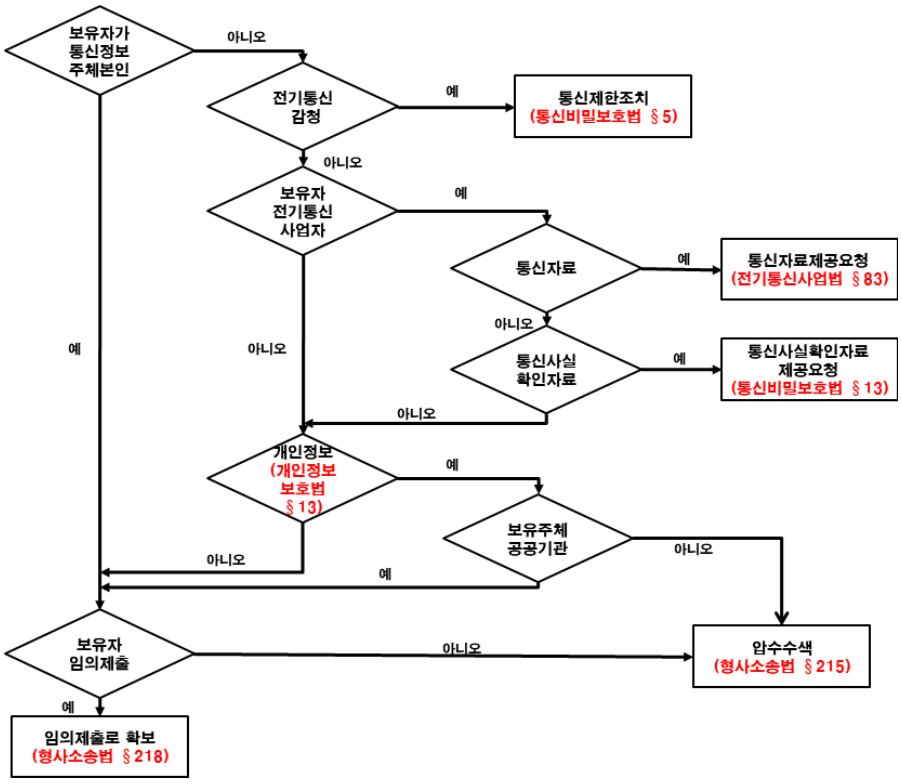
10) 전기통신 역무 내지 정보통신망 이용 서비스를 제공받고자 하는 이용자가 부가적으로 전기통신사업자 등 정보통신망 서비스 제공자에게 제공하여 전기통신사업자 등이 보유하고 있는 정보 내지 전기통신 역무 또는 정보통신망 서비스 제공, 이와 연동된 온라인 상 서비스를 제공하기 위하여 전기통신사업자 등이 수집·생성한 정보

11) 이용자가 전기통신 역무 내지 정보통신망 서비스를 이용한 비 내용적 정보. 즉, 통신정보주체간 송·수신한 문언, 영상, 부호 등 통신 내용을 포함하지 않은 단순 통신량 정보(traffic information)에 대한 로그기록으로, 전기통신사업자 등이 수사기관의 정보를 제공하는 시점 기준으로 과거에 이용자가 언제, 어디서, 누구와 전기통신을 하였는지를 나타내는 정보로 통신정보주체의 과거 통신일시, 통신상대방, 통신에 사용된 기지국 내지 IP가 이에 해당

12) 이용자가 전기통신 역무 내지 정보통신망 서비스를 이용하여 통신상대방에게 전자적 방식에 의하여 송·수신이 완료된 모든 종류의 음향, 문언, 부호, 영상. 즉, 통신 내용정보(contents information)로, 메신저 대화 내용, 포털 사이트 등에 게시한 게시글, 이메일 내용 등이 이에 해당

13) 송·수신 중인 전기통신 내역은 이용자가 전기통신 역무 내지 정보통신망 서비스를 현재 시점에

분류할 수 있고, 각 통신정보는 [그림 1]과 같은 판단절차에 따라 각기 정해진 법률에 의해서 수집되고 있다는 사실을 확인할 수 있었다.



[그림 1] 통신정보 수집을 위한 수사기관의 수집 체계도

주목할 점은 통신사실확인자료 제공요청으로 수집되는 송·수신이 완료된 전기통신 내역은 다른 통신정보와는 달리 수사기관이 특정 기간을 정하여 기간 내 발생된 모든 전기통신 내역을 지득하는 방식으로 이루어진다는 것이다. 이 방식으로 수집

이용하고 있는지에 관련된 비 내용적 정보. 즉, 현재 실시간(real-time)으로 이용자가 언제, 어디서, 누구와 전기통신을 하고 있는지, 하고 있다면 어떠한 통신기기를 이용하여 누구와 통신을 하고 있는지를 나타내는 정보로 휴대전화의 실시간 기지국 위치 정보, 정보통신망에 접속 중인 실시간 IP 등이 이에 해당

된 통신정보에는 필연적으로 수사와 전혀 무관한 국민의 통신정보가 포함되기 때문에 수사기관에서 과도하게 국민의 기본권을 침해하는 결과를 낳게 된다. 수사기관이 수집하는 대표적인 송·수신이 완료된 전기통신 내역은 휴대전화 통화내역과 기지국 통신정보로 그 사례는 다음과 같다.

나. 휴대전화 통화내역

다음은 휴대전화 통화내역이 필요한 상황과 이때 수사기관이 수집하는 통신정보를 재구성한 자료이다.[14)]

- 수사관은 수사 중 '010-1234-5678'호를 사용하는 수사대상자가 2019. 1. 1. ~ 2019. 1. 3. 사이 '010-2222-3333'호와 통신했는지에 대한 사실관계 확인이 필요
- 수사관은 '010-1234-5678'호를 식별자 값으로 동 휴대전화의 2019. 1. 1. ~ 2019. 1. 3.까지 발신·역발신 통신정보를 회신받음

국내통화 내역 조회

접수일자 : 2019/01/01 제공문서번호 : OO123456789

NO	전화번호	기간(From)	기간(To)	통화내역건수
1	01012345678	2019-01-01	2019-01-03	58

NO	구분	시화일자	시화시각	통화시간	발신번호	상대전화번호	발신SITE	비고
1	국내음성통화	2019/01/01	06:47:25	02:26	01012345678	01066667777	서울시 성북구 인촌로 89 안암역	
2	폰메일통화	2019/01/01	06:56:06	00:18	01012345678	01033334444	HS11	SMS
3	국내음성통화	2019/01/01	07:52:43	00:18	01012345678	01022223333	서울시 성북구 인촌로 89 안암역	
4	국내음성통화	2019/01/01	11:48:02	01:01	01012345678	01055556666	세종시 조치원읍 세종로 2511 고려대학교 세종캠퍼스	
5	국내음성통화	2019/01/01	14:00:44	00:59	01012345678	01023456789	세종시 조치원읍 세종로 2511 고려대학교 세종캠퍼스	
6	국내음성통화	2019/01/01	17:52:16	00:08	01012345678	01034567890	서울특별시 서초구 양재대로 12길 73-7 만남의광장	

[그림 2] 수사기관에 제공되는 휴대전화 통화내역

위와 같은 상황에서 수사기관은 2019. 1. 1. 07:52:43경 '010-1234-5678'호가 '010-2222-3333'호와 통신한 사실을 확인할 수 있으므로 수사목적을 달성할 수 있게 된다.

그러나 이와 같은 요청 방식에 따라 수집된 통신정보는 '010-1234-5678'호가 '010-6666-7777', '010-3333-4444'호 등과의 통신한 내역(위 자료 NO. 1~2, 4~6

14) 전기통신사업자 등으로부터 회신되는 자료 형태를 기반으로 가상의 휴대전화 '010-1234-5678'호의 통화내역을 임의로 재구성

에 해당하는 통신정보) 등 범죄사실과 무관한 통신정보주체의 통신정보를 수사기관이 수집하는 문제점을 보여준다.

다. 기지국 통신정보

다음은 기지국 통신정보 수사가 필요한 상황과 이때 수사기관이 수집하는 통신정보를 재구성한 자료이다.[15)]

- 인적사항이 특정되지 않은 범인이 ① 2020. 1. 1. 12:40경 서울 성북구 소재 안암역 인근 가게, ② 2020. 1. 1. 13:15경 고려대학교 서울캠퍼스에서 휴대전화를 사용한 사실을 확인
- 수사관은 ①, ② 장소에서 시험통화 한 후, 시험통화를 식별자 값으로 ①지역 기지국의 2020. 1. 1. 12:40부터 같은 날 12:41까지, ② 지역 기지국의 2020. 1. 1. 13:15부터 같은 날 13:16까지 발생된 기지국 통신정보를 회신

기지국발신 내역 조회

접수일자 : 2020/01/01 제공문서번호 : EM123456789

NO	기지국코드	기간(From)	기간(To)	통화내역건수	기지국주소
1	LT83 000A	2020/01/01	2020/01/01	0	LT83 000A
2	WC16 0D01	2020/01/01	2020/01/01	3	서울시 성북구 인촌로 89 안암역
3	WC16 0D02	2020/01/01	2020/01/01	3	서울시 성북구 안암로 145 고려대학교 서울캠퍼스
4	LT83 0001	2020/01/01	2020/01/01	0	LT83 0001

NO	발신번호	시화일자	시화시각	종화일자	종화시각	상대전화번호	발신SITE
1	01012345678	2020/01/01	12:40:20	2020/01/01	12:41:00	01023456789	안암역
2	01066667777	2020/01/01	12:40:37	2020/01/01	12:41:15	01034567890	안암역
3	01022223333	2020/01/01	12:40:57	2020/01/01	12:42:10	01045678901	안암역
4	01033334444	2020/01/01	13:15:19	2020/01/01	13:17:06	01056789012	고려대학교
5	01012345678	2020/01/01	13:15:21	2020/01/01	13:16:19	01067890123	고려대학교
6	01055556666	2020/01/01	13:15:31	2020/01/01	13:16:28	01078901234	고려대학교

[그림 3] 수사기관에 제공되는 기지국 통신정보

위와 같은 상황에서 수사기관은 2020. 1. 1. 12:40경 서울시 성북구 인촌로 89 안암역, 2020. 1. 1. 13:15경 서울시 성북구 안암로 145 고려대학교 서울캠퍼스 인근에서 모두 통신을 시도한 '010-1234-5678'호 휴대전화 번호를 확인 할 수 있고 이후 가입자 조회 등 다른 수사 기법을 조합해 실제 범인의 인적사항을 특정할 수 있으므로 수사목적을 달성할 수 있게 된다.

그러나 이와 같은 요청 방식에 따라 수집된 기지국 통신정보에는 '010-6666-7777'

15) 실제의 자료 형태를 기반으로 임의의 통신기기, 기지국 주소를 토대로 자료 재구성한 것임.

호와 '010-3456-7890'호 간 상호 통신 내역(위 자료 NO. 2.에 해당하는 통신정보), '010-2220-3333'호와 '010-4567-8901'호 간 상호 통신 내역(위 자료 NO. 3.에 해당하는 통신정보) 등이 포함되어 범죄사실과 무관한 통신정보주체의 통신정보까지 수사기관이 수집하는 문제점을 보여준다.

4. 수사기관의 통신사실확인자료 취득에 관한 법률적 쟁점

가. 학설

기본권 침해와 관련 통신사실확인자료 제공제도의 개선과 관련된 논의는 그간 법령상 수집 요건을 중심으로 논의되었다. 통신사실확인자료는 수사기관이 법원에 그 제공요청의 허가신청을 함에 있어 그 요건으로 필요성만을 규정하고 있는데[16], 학계는 '필요성'만을 규정한 현행 통신비밀보호법상 제 조항과 관련하여 유지설과 강화설이 대립하고 있다.

유지설의 입장은 범죄수사나 범죄의 예방 등 정당한 목적을 가지고 있고, 법원의 허가라는 특별요건을 갖추고 있기에 기본권 침해를 예방할 수 있어 위헌으로 볼 수 없으므로 수사 필요성에 따라 현행 제도를 유지하여야 한다는 점을 그 근거로 들고 있다.[17]

강화설의 입장은 통신사실확인자료의 허가요건으로 규정하고 있는 필요성이라는 요건이 모호하여 수사기관의 남용을 방지하기 어렵다는 점, 법원은 사실상, 형식상 심사를 할 뿐이므로 기본권 침해를 방지하기 어렵다는 점 등을 근거로 들고 있다.[18]

16) 차진아, 범죄수사를 위한 통신사실확인자료 제공요청의 문제점과 개선방안, 법조 제67권 제2호, 2018, 366면.

17) 차진아, "통신비밀보호법 제13조 제1항 및 제2항 등의 합헌성 여부에 대한 검토－헌재 2012헌마191등 헌법소원심판청구 사건에 대한 검토를 중심으로", 법조 제66권 제4호, 2017, 286면.

18) 권양섭, "범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안", 법학연구 제59집, 2015, 403면.

나. 법원의 입장

1) 헌법재판소 2012헌마191 등 결정(헌법재판소, 2018. 6. 28)[19]

위 사안은 2011. 6. 11.부터 2011. 10. 9. 사이 한진중공업 영도조선소 근로자 정리해고 문제에 항의하여 개최된 희망버스 집회 관련 '집회 및 시위에 관한 법률'로 기소된 청구인들이 동 사건 범죄수사를 위한 수사기관의 통신사실확인자료의 수집이 통신의 자유, 사생활의 비밀과 자유, 개인정보자기결정권 등 기본권을 침해당하였다는 점을 이유로 헌법소원 심판을 청구한 사건이다.

해당 사건에서는 수사기관이 현행 통신비밀보호법 규정에 따라 '정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료'(통신비밀보호법 제2조 제11호 바목), '컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료'(통신비밀보호법 제2조 제11호 사목)(이하 위치정보 추적자료)에 해당하는 통신사실확인자료가 필요성만을 요건으로 법원의 허가를 득하여 취득하는 것(동법 제13조 제1항)이 명확성의 원칙에 위배되는지 여부와 과잉금지원칙에 위반되는지 여부가 주된 쟁점이 되었다.

이와 관련 헌법재판소는 통신비밀보호법상 "필요성"이라는 요건이 명확성의 원칙에는 위반되지 아니한다고 결정하였다.[20]

다만, 현행 통신사실확인자료상 위치정보 추적자료의 경우, 광범위한 민감정보를 수사기관이 확보하게 되어 통신정보주체의 기본권을 과도하게 침해하는 한편 수사에 지장을 주지 않는 차원에서 통신정보주체의 기본권을 덜 침해하는 수단이 존재한다는 이유를 들어 수사기관이 필요성만으로 법원의 허가를 득해 위치정보 추적자료를 수집할 수 있는 규정은 과잉금지 원칙을 벗어나 위헌이라고 판단[21]하였다.

---

19) 해당 사건은 같은 취지로 위헌확인소송 청구된 2012헌마191, 550, 2014헌마357호가 병합 판단된 사안이다.

20) "수사를 위하여 필요한 경우'란 위치정보 추적자료가 범인의 발견이나 범죄사실의 입증에 기여할 개연성이 충분히 소명된다는 전제하에, 범인을 발견·확보하며 증거를 수집·보전하는 수사기관의 활동을 위하여 그 목적을 달성할 수 있는 범위 안에서 관련 있는 자에 대한 위치정보 추적자료 제공요청이 필요한 경우를 의미한다고 해석"하였다.

21) "수사기관은 위치정보 추적자료를 통해 특정 시간대 정보주체의 위치 및 이동상황에 대한 정보를

2) 헌법재판소 2012헌마538 결정(헌법재판소, 2018. 6. 28.)

위 사안은 수사기관이 2012. 1. 25. 18:10경 법원의 허가를 얻어 전기통신사업자들에게 2011. 12. 26. 17:00부터 17:10분까지 약 10분간 서울교육문화회관을 관할하는 기지국을 이용하여 착·발신한 전화번호, 착·발신 시간, 통화시간, 수·발신 번호 등의 통신사실확인자료의 제공을 요청하고, 위 전기통신사업자들로부터 청구인을 포함한 총 659명의 통신사실확인자료를 제공받은 행위(이하 기지국 수사)에 대하여 청구인이 사생활의 자유, 통신의 자유, 개인정보자기결정권 등이 침해되었다는 이유로 헌법소원 심판을 청구한 사건이다.

해당 사건에서는 수사기관이 현행 통신비밀보호법 규정에 따라 '가입자의 전기통신일시'(통신비밀보호법 제2조 제11호 가목), '전기통신개시·종료시간'(통신비밀보호법 제2조 제11호 나목), '발·착신 통신번호 등 상대방의 가입자번호'(통신비밀보호법 제2조 제11호 다목), '사용도수'(통신비밀보호법 제2조 제11호 라목)에 해당하는 통신사실확인자료를 필요성만을 요건으로 법원의 허가를 득하여 취득하는 것(동법 제13조 제1항)이 과잉금지원칙에 위반되는지 여부가 주로 쟁점이 되었다.

이와 관련 헌법재판소는 위 판결에서 수사 활동을 보장하기 위한 목적으로 범죄수사를 위하여 필요한 경우 수사기관이 법원의 허가를 얻어 전기통신사업자에 해당 가입자의 전기통신일시, 상대방의 전화번호 등 통신사실확인자료를 제공요청할 수 있도록 하고 있는 현행 통신비밀보호법 관련 규정에 대하여 그 입법목적의 정당성과 수단의 적정성을 인정하였다.

그러나 현행 통신사실확인자료 제공 요건의 경우, 과도한 통신정보의 제공이 가능하며[22], 법원의 통제가 충분히 이루진다고 단정하기 어렵고[23], 수사에 지장을 초

취득할 수 있으므로 위치정보 추적자료는 충분한 보호가 필요한 민감한 정보에 해당되는 점, 그럼에도 이 사건 요청조항은 수사기관의 광범위한 위치정보 추적자료 제공요청을 허용하여 정보주체의 기본권을 과도하게 제한하는 점, 위치정보 추적자료의 제공요청과 관련하여서는 실시간 위치추적 또는 불특정 다수에 대한 위치추적의 경우 보충성 요건을 추가하거나 대상범죄의 경중에 따라 보충성 요건을 차등적으로 적용함으로써 수사에 지장을 초래하지 않으면서도 정보주체의 기본권을 덜 침해하는 수단이 존재하는 점, 수사기관의 위치정보 추적자료 제공요청에 대해 법원의 허가를 거치도록 규정하고 있으나 수사의 필요성만을 그 요건으로 하고 있어 절차적 통제마저도 제대로 이루어지기 어려운 현실인 점 등을 고려할 때, 이 사건 요청조항은 과잉금지원칙에 반하여 청구인들의 개인정보자기결정권과 통신의 자유를 침해한다."

래하지 않으면서도 불특정 다수의 기본권을 덜 침해하는 수단이 존재한다는 이유로 수사기관이 필요성만으로 법원의 허가를 득해 기지국 수사가 가능하게 하는 통신사실확인자료의 정의 규정 및 수집 규정은 과잉금지 원칙을 벗어나 위헌이라고 판단하였다.

다. 소결

수사기관이 통신사실확인자료를 수집하는 것은 통신정보 주체의 개인정보자기결정권 내지 통신비밀의 자유를 침해하는 것이나, 이러한 통신정보를 수집하는 것이 수사기관의 수사목적 달성을 위하여 필요한 것임에는 학계나 법원 모두 다툼이 없다.

다만, 현행 법령상 통신사실확인자료로 규정된 통신정보는 그 수집 요건이 형사소송법상 압수·수색 규정에 비해 완화되어 있음을 이유로, 수집 요건을 형사소송법 수준 내지 그 이상으로 설정하여 일반 국민의 기본권 침해에 대한 통제를 강화하여야 한다는 주장과 범죄의 예방 및 범죄로 인한 사회적 피해 최소화 등 공익을 위한 수사의 효율성을 도모하기 위해 현행 요건을 유지해야 한다는 주장 간 다툼이 있다.

그러나 학계의 논의는 통신사실확인자료 제공요청이 법원의 허가 판단기준으로서 보충성의 요건 추가 등 법원의 통제 강화 여부에 초점이 맞춰져 있을 뿐, 수사에 지장을 주지 않는 차원에서 통신정보주체의 기본권을 덜 침해하는 수단에 관한 연구는 미흡하다.

기술의 고도화에 따라 새로 생성되는 형태의 통신정보가 다양해지고 그 양이 방대해짐에 따라, 법관들의 기술 지식 부족으로 해당 정보의 기본권 침해 정도, 수사 필요성 등의 판단이 어려운 사안들이 늘어나고 있다.

이러한 현실에서 법원의 통제만으로는 국민의 기본권을 보호하는데 한계가 있을

---

22) 위 판결에서는 '1개의 허가서 당 수천여 개의 전화번고 집계되고 있는 실정인 점'을 그 예시로 들었다.

23) 위 판결에서는 '통신제한조치 허가신청에 대한 법원의 기각률은 약 4%인데 반해 통신사실 확인자료 제공요청 허가신청에 대한 법원의 기각률은 1%에 불과한 바, 이는 이 사건 요청조항이 보충성 등을 요구하지 않은 채 수사의 필요성만을 요건으로 규정하고 있음에 기인하는 점을 고려할 때, 현재와 같이 통신사실 확인자료 제공요청에 대한 요건이 완화되어 있는 상태에서 법원이 허가를 담당하고 있다는 사정만으로 수사기관의 제공 요청 남용에 대한 통제가 충분히 이루어지고 있다고 단정하기 어렵다'고 판시하였다.

수밖에 없다. 법령상 제공 요건 강화를 통해 법원의 통제를 강화한다고 하더라도 법원의 허가를 득해 특정 기간 동안 발생된 모든 통신정보를 수집하는 이상 필연적으로 기본권 침해가 수반될 수밖에 없다.

즉, 현행 통신수사 방식을 그대로 사용하는 경우 필요성 요건 이외의 별도 요건을 추가하여 법원의 통제를 강화한다고 하더라도, 범죄와 무관한 사람의 기본권은 침해될 수밖에 없는 것으로 통신수사 시 통신정보주체의 기본권을 덜 침해할 수 있는 수단의 도입과 이를 위한 기술적 조치가 필요하다. 기술적 관점에서 통신정보주체의 기본권을 덜 침해하는 수단을 검토하여 국민의 기본권 보호와 수사 합목적성의 조화를 꾀하는 것이 필요한 시점이다.

Ⅲ. 비식별화된 통신사실확인자료를 이용한 통신수사 개선 방안

1. 통신수사 기법 개선 방안

전 장에서 살펴본 바와 같이 현행 통신사실확인자료 수집 등 통신수사는 수사기관에서 전기통신사업자 등에게 통신사실확인자료 제공요청 시 수사와 관련 여부를 고려하지 않고 특정 기간 동안 생성된 모든 통신정보를 요청하여 과도한 기본권 침해 요소가 있는 것을 확인하였다.

이와 관련 현행 통신수사의 방식을 변경하여 수사기관이 전기통신사업자 등으로부터 국민의 기본권을 침해하지 않는 형태로 1차 자료를 수집한 뒤, 분석과정을 통해 수사에 필요한 통신정보만을 선별한 후, 해당 통신정보만을 확보하는 방식으로 통신수사 방식을 변경한다면, 통신수사로 인하여 발생되는 기본권 침해를 최소화할 수 있을 것이다.

이에 본 논문에서는 현행 전기통신사업자가 제공하는 통신사실확인자료 중 송신 전화번호, 수신 전화번호 등 통신정보주체를 특정할 수 있는 민감정보를 비식별화하여 수사기관에게 1차적으로 제공한 뒤, 수사기관은 이를 분석하여 범죄혐의 관련 부분만을 재차 특정하여 전기통신사업자에게 재식별화 요청을 함으로써 수사목적

을 달성할 수 있는 통신수사 방식을 제안한다.

가. 수사목적의 통신정보 비식별화 시 고려 요소

통신수사 목적 달성을 위해서는 기지국 통신수사를 진행함에 있어 여러 기지국에서 중복된 통신정보를 추출하거나, 각 전화번호 별 통화 횟수 등 기초 통계의 추출이 가능하여야 하므로, 전화번호 및 기지국 정보의 고유 식별성이 유지되어야 한다. 따라서 고유식별성을 유지할 수 있는 비식별화 조치로서 가명처리, 가명처리 중에서도 암호화 방법이 통신정보 비식별화에 적합하다고 할 수 있다. 이때 고유식별성이 유지되어야 하는 최소 범위는 수사기관이 수사 중인 1개의 사건 내 제공되는 통신정보가 된다.

두 번째로 수사기관에서 수집하는 비식별화 통신사실확인자료는 다른 정보와 결합하여 재식별화가 불가능하여야 한다. 통신사실확인자료 비식별화에 사용되는 암호 함수의 경우 다수의 전기통신사업자가 공유해야 되므로 대중에게 공개될 수밖에 없다. 따라서 암호 함수가 공개되었다 하더라도 비식별값의 재식별화가 불가능한 일방향 암호 함수가 사용되어야 한다.

이와 관련 법원은 재단법인 약학정보원이 다국적 제약회사인 IMS Health Inc.에 처방전 정보를 비식별화 한 후 판매한 사건에서 재단법인 약학정보원이 일방향 암호 알고리즘인 SHA-512 해쉬 함수를 통해 주민번호를 변환시킨 후 IMS에 제공한 것과 관련 해쉬함수가 역함수가 없다는 특성에 주목하여, 주민번호 원문을 복원하는 것이 원천적으로 불가능해졌다고 보아 그 정보가 '개인정보'가 아니라고 판단한 사례가 있다.[24)]

세 번째로 통신사실확인자료 비식별화 조치가 필요한 데이터 평문은 11자리의 휴대전화 번호(사실상 8자리 숫자로 구성된 데이터)이므로, 암호문 데이터의 총 개체수는 99,999,999개에 불가하다. 결국 비식별화된 통신사실확인자료의 가능한 개수가 매우 적다면 이를 미리 다 계산하여 표로 만드는 방식으로 해독될 수밖에 없다. 따라서 데이터의 비식별값(암호화 값)의 가능한 개수는 공격자가 미리 계산하여

24) 서울중앙지방법원 2017. 9. 11. 선고 2014가합 508066, 508302판결.

대응표를 만들 수 없을 정도로 많아야 한다.

이와 관련 전승재·권헌영은 2014가합508066, 508302호 판결에서의 법원의 판단과 관련 일방향 암호화를 한다고 해서 항상 '식별성'이 제거되는 것이 아니며, 단순 해쉬 함수의 경우 원본 데이터와 대응되는 해쉬값으로 이루어진 조합쌍에 의해 원 데이터가 재식별화될 수 있음을 근거로, 단순 해쉬 함수를 통한 비식별화 정보는 개인정보로 볼 수 있음을 지적한 바 있다.[25)]

따라서 이러한 문제점을 해결하기 위해서는 정보를 제공받는 수사기관 내지 해당 통신사실확인자료를 재식별화 하고자 하는 공격자가 알 수 없는 값(솔트, Salt)을 원본 통신사실확인자료에 추가하여 암호화하는 형태로 비식별화 조치가 취해져야 한다.

마지막으로 수사기관이 동일한 암호화 방식으로 비식별화 조치가 이루어진 다량의 데이터를 수집하는 것을 방지할 수 있어야 한다. 2017년 통계자료에 의하면 수사기관은 총 1,052,897개의 휴대전화 번호에 대한 통신사실확인자료를 수집하였다.[26)] 통상 1개의 휴대전화가 수십 개에서 많게는 수백 개의 상대 전화번호를 가지고 있는 점을 고려하면 일년동안 수사기관에서 수집되는 비식별 정보 값은 그 양이 방대하다. 동일한 방식으로 암호화 된 암호문 데이터가 많을수록 취약점은 증가할 수밖에 없으므로, 이를 방지하기 위해 고유식별성 유지가 필요한 최소단위로 솔트(Salt) 값의 변화를 주는 방식이 필요하다.

나. 통신정보 비식별화 방안

1) 통신정보 비식별화 프로세스

본 논문에서는 위와 같은 고려 요소를 모두 충족시키는 통신사실확인자료 비식별화 방법으로, 현행 인터넷 사이트에서 주민등록번호 대체 수단으로 활용하고 있는 DI 값(중복가입확인정보) 생성 절차를 응용하는 방법을 제안한다.

현재 주민등록번호 대체 수단으로 사용하고 있는 DI 값은 가입자의 주민등록번

25) 전승재·권헌영, 일방향 암호화와 개인정보 비식별화의 관계－약학정보원 민사 1심 판결에 대한 비판적 검토, 한국IT서비스학회 학술대회 논문집, 2018, 489～492면.

26) 과학기술정보통신부, 2017년 하반기 통신자료 및 통신사실확인자료 제공 등 현황 발표, 보도자료, 2018. 5. 18. 2면.

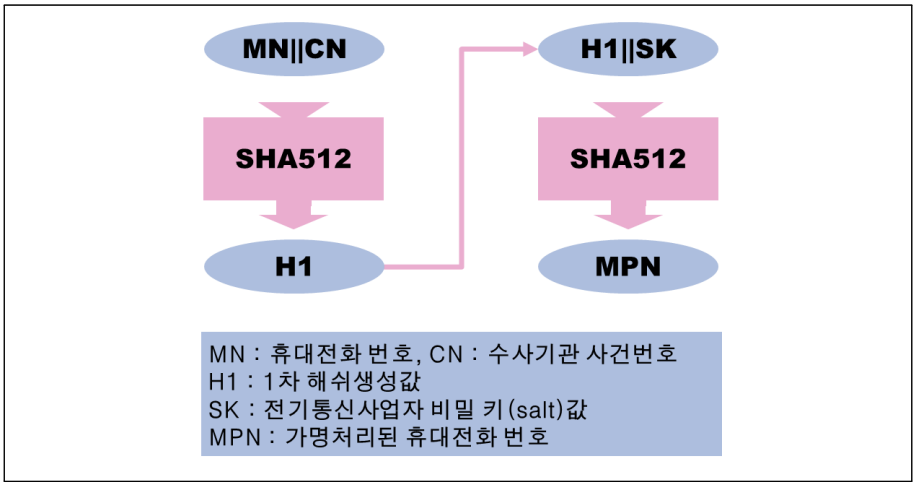
호와 중복가입을 확인하고자 하는 웹사이트의 식별정보를 SHA2 해쉬함수를 통해 해쉬값으로 생성하고, 이후 중복가입을 확인하고자 하는 웹사이트와 본인확인기관 간 공유한 비밀정보를 더하여 SHA2 해쉬함수를 통해 재차 해쉬값을 생성하는 방법으로 생성한다.[27)]

이와 같은 DI 값 생성절차에 착안하여 통신정보를 비식별화하는 절차를 다음과 같이 제안한다.

① 비식별화된 통신정보를 복호화 할 수 없도록 일방향 함수인 해쉬함수 SHA-512를 활용

② 해쉬값 생성에 있어 수사기관 내지 공격자가 휴대전화 번호 가능 조합에 대한 해쉬값을 전부 계산하여 비식별화 값과 대조하는 방법으로 원본 통신정보를 유추할 수 없도록 하기 위하여 수사기관 내지 공격자가 알 수 없는 전기통신사업자만의 비밀키를 솔트(Salt)값으로 조합

③ 또한 해쉬값 생성에 있어 수사기관에서 별건 통신수사로 확보하게 되는 데이터를 축적하여 전기통신사업자만의 비밀키 값을 추론할 수 없도록 하기 위해, 재차 사건번호를 솔트(Salt) 값으로 조합하여 해쉬값을 생성



[그림 4] 통신정보 비식별화(암호화) 프로세스

27) 정찬주, 인터넷상의 개인식별번호 서비스 및 표준, TTA Journal NO.116, 2008. 4, 78면.

2) 전기통신사업자의 비밀키값의 설정 방안

수사기관이 비식별화된 통신정보를 분석하려면, 제공받는 비식별화된 통신정보의 고유식별성이 유지되어야 한다. 즉 전기통신사업자가 달라도 통신정보가 같다면 비식별화된 통신정보도 동일해야 한다. 이를 위해서는 1개의 사건에서 수사기관에게 비식별정보를 제공하는 전기통신사업자끼리 비밀키 값을 상호 공유하여야 수사기관에 제공하는 비식별화 값의 고유식별성을 유지할 수 있다. 다만, 이때 수사기관은 해당 비밀키 값을 알 수 없어야 한다. 따라서 전기통신사업자의 비밀키 분배를 위한 수사기관 외 제3기관의(third party) 키분배 센터가 운영되어야 한다. 제3기관으로는 개인정보 침해 방지 및 실태점검, 개인정보보호 기술지원 등의 업무를 수행하고 있는 한국인터넷진흥원(KISA)이나 개인정보보호를 심의 의결하는 개인정보보호위원회가 적합해 보인다.

제3기관의 키분배 실무상 조치로 한국인터넷진흥원(KISA)이나 개인정보보위원회에서는 전기통신사업자의 비밀키 값 생성을 위하여 키 분배 서버의 운영이 필요하다. 제3기관에 기 구축된 키 분배 서버는 전기통신사업자가 비식별값을 요청하는 수사기관의 고유번호, 관서번호, 사건번호를 토대로 키 생성을 요청하는 경우, 먼저 전기통신사업자 여부 인증을 거친 뒤 제공 받은 정보를 토대로 키 생성함수를 통해 키 값을 생성하여 전기통신사업자에게 전송하는 역할을 수행한다.

이와 같은 조치로 생성되는 전기통신사업자의 키 생성은 수사실무에 있어 1개의 수사사건에서 동일한 비밀 키 값을 전기통신사업자끼리 공유할 수 있도록 하여, 1개 수사사건 내에서 전기통신사업자가 수사기관에 제공하는 비식별값들의 고유식별성은 유지하도록 하되, 별건 수사사건에서의 활용을 막아 수사기관의 광범위한 법익 침해를 견제하는 장치로 활용될 수 있다.

다. 사례분석 – 개선 방식에 따른 실제 수사결과 도출

1) 휴대전화 통화 내역 통신수사

다음은 수사기관이 기지국 통신수사 시 사건번호를 ‘2018123456’, 전기통신사업자가 보유하게 된 키 값을 ‘A1B2C3’라고 가정하였을 때, 전술한 사례에서 전기통

신사업자가 수사기관에게 제공하는 비식별화된 통화 내역(발신내역)을 재구성한 자료이다.

- 수사기관이 수사 중 `010-1234-5678`호가 2019. 1. 1. ~ 2019. 1. 3. 사이 '010-2222-3333'호와 통신했는지에 대한 사실관계 확인이 필요
- 수사관은 `010-1234-5678'호를 키 값으로 동 휴대전화의 2020. 1. 1. ~ 2020. 1. 3.까지 비식별화된 발신·역발신 통신정보를 회신
- 이와 함께 '010-2222-3333호의 비식별값을 회신
  * 비식별값 : 8699471b2524d0d2449a3ef7dd834a098cd8294c02764cedfdcb0d4155745b89

국내통화 내역 조회

접수일자 : 2019/01/01 제공문서번호 : OO123456789

NO	전화번호	기간(From)	기간(To)	통화내역건수
1	01012345678	2019-01-01	2019-01-03	58

NO	구분	시화일자	시화시각	통화시간	발신번호	상대전화번호	발신SITE	비고
1	국내음성통화	2019/01/01	06:47:25	02:26	01012345678	aeda3825128ab4ef5bd86bb44c56a54ac6481dfbb0a804201ddb690150615b99	39eb358e9ffc1fda4bc4c17fd195153a15ef4c508acf220be918797314cb5d72	
2	폰메일통화	2019/01/01	06:56:06	00:18	01012345678	9833d7d23d8744114b1501ad68c2a0083 1965d93b665bbbd5a12e86dbd583d94	85fa1fe9e4d97ca4333fd1f90b1c54675d3 8af86394bb87e26adedce97b2b729	SMS
3	국내음성통화	2019/01/01	07:52:43	00:18	01012345678	8699471b2524d0d2449a3ef7dd834a098cd8294c02764cedfdcb0d4155745b89	39eb358e9ffc1fda4bc4c17fd195153a15ef4c508acf220be918797314cb5d72	
4	국내음성통화	2019/01/01	11:48:02	01:01	01012345678	75099d39ae5cc0b3e85c1d1e467cdc991115236320e2438827758f865fa87ced	db01ac59b03aae43abbad64179632a716873b336bf9caac352d1db44e8305dc9	
5	국내음성통화	2019/01/01	14:00:44	00:59	01012345678	8641f0124c3f9b1d0be8d49623fd1319f0da78c89ae8c5c8c3b2510657da6561	db01ac59b03aae43abbad64179632a716873b336bf9caac352d1db44e8305dc9	
6	국내음성통화	2019/01/01	17:52:16	00:08	01012345678	972e08d8855ca797b0585bae7192a21400da2999bed748f4f537c4490fb5537b	6228797957f873410e7d48e62ab7bcf49e8e799c7783c1806d5fab12d3897ef9	

[그림 5] 개선방식에 의해 수사기관에 제공되는 휴대전화 통화내역

예시에서 볼 수 있듯이 1차로 수사기관이 제공받는 비식별화된 통신정보는 통신정보주체가 통신한 상대전화번호가 가명 처리되어 통신 상대를 인식할 수 없으므로 현행 수사기관이 수집하는 통신사실확인자료에 비해 통신비밀의 침해 정도가 현격하게 줄어든다.

반면, 비식별화 조치를 거친 후에도 수사기관은 '010-1234-5678' 호와 '010-2222-3333호' 사이에 통신한 사실을 알 수 있고, 전기통신사업자에게 해당 정보만을 재식별화

를 요청하여 통신정보로 환원한 뒤, 수사에 활용할 수 있으므로 수사목적을 달성할 수 있다.

2) 기지국 통신수사

다음은 수사기관이 기지국 통신수사 시 사건번호를 ‘2018123456’, 전기통신사업자가 보유하게 된 키 값을 ‘A1B2C3’라고 가정하였을 때, 전술한 사례에서 전기통신사업자가 수사기관에게 제공하는 비식별화된 기지국 통신정보를 재구성한 자료이다.

- 인적사항이 특정되지 않은 범인이 ① 2020. 1. 1. 12:40경 서울 성북구 소재 안암역 인근 가게, ② 2020. 1. 1. 13:15경 고려대학교 서울캠퍼스에서 휴대전화를 사용한 사실을 확인
- 수사관은 ①, ② 장소에서 시험통화 한 후, 시험통화를 키 값으로 ①지역 기지국의 2020. 1. 1. 12:40부터 같은 날 12:41까지, ② 지역 기지국의 2020. 1. 1. 13:15부터 같은 날 13:16까지 발생된 비식별화된 기지국 통신정보를 회신받음

기지국발신 내역 조회

접수일자 : 2020/01/01 제공문서번호 : EM123456789

NO	기지국코드	기간(From)	기간(To)	통화내역건수	기지국주소
1	LT83 000A	2020/01/01	2020/01/01	0	LT83 000A
2	WC16 0D01	2020/01/01	2020/01/01	3	서울시 성북구 인촌로 89 안암역
3	WC16 0D02	2020/01/01	2020/01/01	3	서울시 성북구 안암로 145 고려대학교 서울캠퍼스
4	LT83 0001	2020/01/01	2020/01/01	0	LT83 0001

NO	비식별화된 발신번호	시화일자	시화시각	종화일자	종화시각	비식별화된 상대전화번호	발신SITE
1	ee15450fe9bf8e30daa81d7ccb257ce42b57f46b71c1e39b164e757da8d41a34	2020/01/01	12:40:20	2020/01/01	12:41:00	8641f0124c3f9b1d0be8d49623fd1319f0da78c89ae8c5c8c3b2510657da6561	안암역
2	aeda3825128ab4ef5bd86bb44c56a54ac6481dfbb0a804201ddb690150615b99	2020/01/01	12:40:37	2020/01/01	12:41:15	972e08d8855ca797b0585bae7192a21400da2999bed748f4f537c4490fb5537b	안암역
3	8699471b2524d0d2449a3ef7dd834a098cd8294c02764cedfdcb0d4155745b89	2020/01/01	12:40:57	2020/01/01	12:42:10	2397b7c45192f20d52aa22f734cd0ebe23534665f43cafc2d0279f0c26cd072e	안암역
4	9833d7d23d8744114b1501ad68c2a00831965d93b6	2020/01/01	13:15:19	2020/01/01	13:17:06	beb3b74bfe7df4c264e3a6bba03f40eaba78eea3bb33a8	고려대학교
5	ee15450fe9bf8e30daa81d7ccb257ce42b57f46b71c1e39b164e757da8d41a34	2020/01/01	13:15:21	2020/01/01	13:16:19	dea66456d797381dfb0216687dfe36069adb2c6f360a82f5198dd80cbefa3225	고려대학교
6	75099d39ae5cc0b3e85c1d1e467cdc991115236320e2438827758f865fa87ced	2020/01/01	13:15:31	2020/01/01	13:16:28	f24921b7e44c7a5d32ec1f14f784b6346148f9238807d061b8be2aaed0e1761b	고려대학교

[그림 6] 개선방식에 의해 수사기관에 제공되는 기지국 통신정보

예시에서 볼 수 있듯이 1차로 수사기관이 제공받는 비식별화된 통신사실확인자료는 발신번호와 상대전화번호가 가명 처리되어 통신정보주체를 인식할 수 없으므로 통신정보에 해당하지 않고 나아가 개인정보에도 해당하지 않는다. 따라서 1차로 제공된 자료만으로는 특정인의 통신비밀 침해 등 기본권 침해 요소가 없다.

반면, 비식별화 조치를 거친 후에도, 2개 이상의 기지국에서 중복으로 존재하는 비식별값을 확인할 수 있으므로, 수사기관은 전기통신사업자에게 중복된 비식별값인 'ee15450fe9bf8e30daa81d7ccb257ce42b57f46b71c1e39b164e757da8d41a34'로 가명처리되어 있는 데이터만을 전기통신사업자에게 재식별화를 요청하여 인식가능한 통신정보로 환원한 뒤, 수사에 활용할 수 있으므로 수사목적을 달성할 수 있다.

2. 통신수사 절차 개선을 위한 법률 개정방안

가. 정의 조항

우선 제2조에 비식별화된 통신사실확인자료 통신사실확인자료, 비식별화된 통신정보의 재식별화, 특정정보의 비식별값의 정의가 필요하다. 비식별화된 통신사실확인자료는 '전기통신사업자가 보유하고 있는 가입자의 전기통신에 관한 자료 중 전기통신의 송신인과 수신인, 송·수신 위치(기지국), 송·수신된 음향, 문언, 부호 또는 영상(단, 이때 수사기관이 전기통신사업자에게 식별정보로 제공한 정보는 제외한다)을 비식별화한 자료를 말한다.'로 정의하고, 비식별화된 통신정보의 재식별화는 '전기통신사업자가 비식별화한 통신정보를 본래의 전기통신에 관한 정보로 전환하는 것을 말한다'라고 정의하며, 특정정보의 비식별값은 '전기통신사업자가 보유하고 있는 가입자의 전기통신에 관한 정보 중 수사기관이 전기통신사업자에게 제공한 식별정보를 비식별화한 값을 말한다.'고 정의해 볼 수 있을 것이다.

나. 통신사실확인자료 제공요청 요건 조항

1) 비식별화된 통신사실확인자료의 제공요청 요건

비식별화된 통신사실확인자료 제공요청의 경우에는 통신비밀보호법 제13조에서

규정하고 있는 통신사실확인자료 제공요청의 요건 및 절차에 관한 규정에 추가하여 범죄수사를 위한 비식별화된 통신정보의 제공의 절차로써 '검사 또는 경찰 수사관서의 장은 수사에 필요한 경우 전기통신사업자에게 비식별화된 통신정보의 열람이나 제출(이하 "비식별화된 통신정보 제공")을 요청할 수 있다'고 규정하여 수사 필요성이 있는 경우 법원의 허가 없이 비식별화된 통신정보의 제공을 받을 수 있도록 하되, 비식별화된 통신정보의 재식별화 및 특정 통신정보의 비식별화값 제공 요청의 경우 필요성을 소명하여 관할 지방법원 또는 지원의 허가를 받아 수사기관이 이를 수집할 수 있도록 규정되어야 한다.

2) 비식별화된 통신사실확인자료 수집에 있어 관련성 요건의 규정 필요성

관련성의 법적 기능은 압수·영장의 발부에 있어 그 대상과 범위를 제한하는 역할을 하고 압수·수색 집행과정에서의 하자를 사후적으로 심사하여 증거능력을 판단할 수 있게 해주는 기준이 된다.[28)]

개선된 통신수사 방식은 통신사실확인자료 등 전자정보에 있어 비식별화된 통신사실확인자료를 우선적으로 수집하고, 1차적으로 수집한 자료의 분석을 거쳐 수사의 필요한 정보만을 재식별화를 요청하거나 수사에 필요한 특정 통신정보만의 비식별값을 요청하는 것으로 2단계에 걸친 수집 과정 자체가 수집하는 정보의 대상과 범위를 한정하는 역할을 한다. 또한 통신사실확인자료 제공요청의 경우 일반 압수·수색·검증영장 집행과는 달리 허가서의 집행 방식(영장 집행 방식)이 정형화[29)] 되어 있기 집행방식에 있어 하자가 발생할 가능성도 미미하다. 따라서 비식별화된 통신사실확인자료 수집에 있어서는 법령 상 관련성 요건을 규정할 필요는 없어 보인다.

3) 통신사실확인자료의 별건 활용 규제

수사기관에서는 특정사건에서 적법하게 수집된 통신사실확인자료를 별건 사건

28) 박민우, 수사기관의 압수에 있어 관련성 요건의 해석과 쟁점에 대한 검토, 경찰학연구 제16권 제1호, 통권 45호), 2016, 10면

29) 법원의 허가서를 전기통신사업자 등에게 제시하고, 전기통신사업자 등이 허가서에 기재된 내용을 해석하여 해당하는 자료를 수사기관에게 제공하는 방식

수사에 활용하고자 한다. 그 이유는 전기통신사업자 등의 통신사실확인자료를 보관기간 문제로 수사기관에서 범죄 발생 후 12개월이 도과된 범죄 수사에 있어 이를 수집하기 어렵고, 현행 수집되는 통신사실확인자료가 광범위한 기간 동안의 통신정보를 내포하고 있어 별건 수사 활용 가치가 높기 때문이다.

현행 통신비밀보호법은 제13조의5에 의하여, 수사기관은 제공받은 통신사실확인자료를 해당 수집의 목적이 된 범죄나 관련된 범죄를 수사하는 용도로만 활용하도록 한다. 그러나 관련성 판단은 증거법적 측면에서 증거능력 관련 압수 당시의 상황을 기초로 구체적·개별적으로 법관이 사후적으로 판단하는 것으로[30] 해당 규정은 수사기관의 별건 수사 활용을 사전적으로 통제하는 장치가 될 수 없으며, 사후적 통제 기능 역시 객관적 관련성, 주관적 관련성을 사람인 법관이 판단할 수 밖에 없는 이상 일정부분 판단의 오류가 발생할 수 있다는 비판에 직면할 수 있다. 따라서 관련성의 판단기준을 법령상 구체적으로 명시하거나 별도 요건을 두어 통신정보의 별건 수사 활용을 엄격히 통제할 수 있는 장치가 필요하다.

이와 관련 통신사실확인자료의 비식별화 조치는 그 자체로 통신정보의 별건 활용 규제의 효과가 있다. 본 논문에서 제안하는 비식별화된 통신사실확인자료를 이용한 통신수사 방식 따르면 특정사건별로 키 값을 달리하여 통신정보의 비식별화 조치가 이루어지기 때문에 특정사건에서 수집된 비식별화된 통신사실확인자료가 별건 수사 내지 공소과정에서 활용가치가 없다. 따라서 수사기관이 수집한 통신사실확인자료를 별건 수사에 활용하는 것을 원천적으로 방지할 수 있다.

4) 일반 통신사실확인자료 제공요청 요건

비식별화된 통신사실확인자료 제공요청 제도를 도입하더라도 부득이하게 수사목적을 달성할 수 없는 경우 비식별화조치가 이루어지지 않은 일반 통신사실확인자료를 수집할 수 있도록 하는 현행 통신사실확인자료 제공요청 제도는 유지하는 것이 바람직하다. 다만, 원칙적으로 비식별화된 통신사실확인자료 제공요청 제도를 이용하되, 부득이하게 수사목적을 달성할 수 없는 경우에 활용되는 일반 통신사실확인

30) 정한중, 적법하게 취득한 통신사실 확인자료와 관련성 있는 범죄－대법원 2017. 1. 25. 선고 2016도13489판결 -, 법조 2017·4(Vol. 722), 2017, 753면

자료 제공요청 요건은 필요성뿐 아니라 범죄 관련성 및 보충성의 요건을 추가하여 법원의 통제를 강화하도록 하는 것이 바람직할 것이다.

5) 소결

비식별화된 통신정보 요청의 경우 전기통신사업법상 통신자료 제공 요청 규정에 비추어 수사기관의 필요성에 따라 수사관서의 장이 요청하면 전기통신사업자 등이 이를 제공할 수 있도록 하여 수사의 합목적성을 제고하도록 하되, 비식별화된 통신정보의 재식별화 내지 특정 통신정보의 비식별값을 제공할 경우에는 통신비밀 등 기본권 침해요소를 내포하고 있으므로, 필요성을 요건으로 법원의 통제를 거치도록 하여 헌법상 영장주의 원칙과 기본권 침해의 통제를 꾀하는 것이 합리적인 입법 개선 방안이라고 할 것이다. 다만, 예외적으로 수사목적 상 불가피한 경우 활용할 수 있도록 현행 통신사실확인자료 제공요청제도를 유지하도록 하되, 법원의 허가요건을 강화하여 관련성 및 보충성의 요건을 추가하는 것이 바람직하다.

[표 2] 제안하는 법령개정에 따른 수사기관의 통신정보 수집의 요건 및 절차

	통신자료	비식별화된 통신정보	제식별화 비식별값 요청	통신사실 확인자료	통신 제한조치	기타 (송·수신이 완료된 전기통신 등)
법률	전기통신 사업법	통신비밀 보호법	통신비밀 보호법	통신비밀 보호법	통신비밀 보호법	형사소송법
요건	필요성	필요성	필요성	필요성 관련성 보충성	필요성 혐의 개연성 대상 범죄 한정 보충성	필요성 혐의 개연성 관련성
절차	기관장 요청	기관장 요청	법원 허가서	법원 허가서	법원 허가서	영장

다. 비식별화를 위한 키 형성 절차와 제3기관의 기술적 조치 협조 의무 조항

통신비밀보호법에서는 키 분배 서버를 운영을 위한 제3기관의 협조의무와 수사기관의 정보 제공시 전기통신사업자 등의 통신정보 비식별화 의무를 규정하고, 법

령 내지 법령에 위임을 받은 동법 시행령에 전술한 비식별화 조치 방법을 상세 규정할 필요가 있다. 마지막으로 이를 위한 국가 예산 지원 조항을 신설하여 원활한 키 분배 서버 운영과 전기통신 사업자 등의 비식별화 조치를 보조할 필요가 있다.

Ⅳ. 결론

본 논문에서는 통신수사에서 발생하는 기본권 침해와 관련해서 학계에서 논의되고 있는 법관에 의한 통제 강화만으로는 근본적인 기본권 침해 요소를 극복할 수 없다는 점을 강조하였다.

이에 따라 수사기관의 통신수사 방식상 문제를 검토하기 위하여 일선 수사 현장의 통신수사 실태를 검토하였으며, 그 결과 일선 수사 현장의 통신수사 실무 중 통신사실확인자료 제공 요청과 관련하여 특정한 기간 동안 발생된 모든 통신정보를 수집하는 현행 방식은 근본적인 기본권 침해 요소를 내포하고 있음을 확인하였고, 이를 두 단계로 개선할 경우 기본권 침해를 최소화 할 수 있음을 보였다.

이에 현행 통신수사 방식을 개선하여 수사기관이 통신사실확인자료를 수집하는 과정에서 전기통신사업자에게 우선적으로 범위를 정한 기간 동안의 비식별화된 통신사실확인자료를 회신받은 뒤, 추가적으로 필수적인 정보의 비식별값만을 회신받거나, 비식별화된 통신사실확인자료 분석과정을 거쳐 필요한 최소 정보만을 재식별화하는 방법으로 기본권 침해를 최소화 할 것을 제안하였다.

이와 같은 개선 방식에 있어 통신정보의 비식별화 방안으로 제3기관을 통하여 수사기관에게 비식별화된 통신정보를 제공하는 전기통신사업자 간 비밀키 공유와 사건번호, 일방향 암호화 함수를 통한 가명처리 방안을 구체적으로 제시하였고, 비식별화 통신정보를 회신받았을 때, 수사기관에서 행하여야 하는 구체적인 수사절차를 제시하였다.

또한 이러한 두 단계 통신수사 방식을 적용하였을 때, 수사의 합목적성 달성이 가능하며 기본권 침해를 최소화 할 수 있음을 검증하였다.

마지막으로 본 논문에서는 이와 같은 통신수사 방식의 전환을 유도하기 위한 법

률 개선방안으로서 통신비밀보호법의 개정방안을 제시하였다.

또한 향후 후속 연구에서는 통신사실확인자료 뿐 아니라 금융거래정보, 신용정보 등의 수집에 있어서도 유사한 형태로 다량의 금융, 신용정보 역시 최종적으로 수사에 활용되는 정보만을 선별 압수할 수 있는 방안이 제시되어 수사로 인한 국민의 기본권 침해를 최소화 할 수 있는 수사방식에 대한 연구가 지속되기를 기대해 본다.

참고문헌

[단행본]

이동희, 이윤, 장윤식, 공저, 범죄수사학, 경찰대학 출판부, 2013.

[논 문]

강태수, 통신의 비밀보장에 관한 연구, 경희법학 제45권 제4호, 2010.

권양섭, 범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안, 법학연구 제59집, 2015.

김일환, 통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰, 형사정책 제16권 제1호, 2004.

김지온, 통신수사절차의 개선방안에 대한 법적연구, 고려대학교 석사학위 논문, 2017.

박민우, 수사기관의 압수에 있어 관련성 요건의 해석과 쟁점에 대한 검토, 경찰학연구 제16권 제1호, 통권 45호), 2016

전승재·권헌영, 일방향 암호화와 개인정보 비식별화의 관계 - 약학정보원 민사 1심 판결에 대한 비판적 검토, 한국IT서비스학회 학술대회 논문집, 2018.

정찬주, 인터넷상의 개인식별번호 서비스 및 표준, TTA Journal No.116, 2008.

정한중, 적법하게 취득한 통신사실 확인자료와 관련성 있는 범죄 - 대법원 2017. 1. 25. 선고 2016도13489판결 -, 법조 2017·4(Vol. 722), 2017.

차진아, “통신비밀보호법 제13조 제1항 및 제2항 등의 합헌성 여부에 대한 검토 - 헌재 2012헌마 191등 헌법소원심판청구 사건에 대한 검토를 중심으로”, 법조 제66권 제4호, 2017.

차진아, 범죄수사를 위한 통신사실확인자료 제공요청의 문제점과 개선방안, 법조 제67권 제2호, 2018.

황성기, 현행 통신비밀 보호법제의 헌법적 문제점, 언론과법 제14권 제1호, 2015.

[인터넷 검색]

과학기술정보통신부, (2018년 8월 기준) 무선통신서비스 가입회선 통계, www.msit.go.kr (2018. 10. 4. 검색).

[판 례]

대법원, 2014. 7. 24. 선고 2012다 49933 판결

헌법재판소 2015. 6. 25. 선고 2014헌마4673 결정

헌법재판소 2018. 6. 28. 선고 2012헌마191 등 결정

헌법재판소 2018. 6. 28. 선고 2012헌마538 결정

대법원 2016. 10. 13. 선고 2016도 8137호 판결

서울중앙지방법원 2017. 9. 11. 선고 2014가합 508066, 508302판결

Minimization of Personal Information Infringement in Criminal investigation by Utilizing De-identified Communication Information

Park, Hyun-jun·Lee, Sang-jin

Recently, the Constitutional Court ruled that the provision of communication confirmation data for criminal investigation is unconstitutional under the Protection of Communications Secrets Act.

The Protection of Communications Secrets Act provides that if the necessary requirements are met, the law enforcement agency can collect information such as the date of telecommunications by subscribers, the time that the telecommunications commence and end, and the communications number of outgoing and incoming call, etc.

Prior to the ruling of the Constitutional Court, academia raised concerns about privacy and infringement of personal information self-determination, and urged the improvement of the provisions of the Protection of Communications Secrets Act.

However, discussions on the improvement of the cell site investigation process seems to be inadequate, while the discussion of the academia has been focused on strengthening the requirements of requests for communication confirmation data.

This study attempts to analyze the process of the existing cell site investigation method performed by the law enforcement agency, presents an example of the cell site information collected according to the current method, and explores the elements that could infringe the human rights and privacy.

As a solution, this study proposes a transformation of the investigation paradigm. Specifically, first, after the investigation agency obtains the unidentified information from the communication service providers, then analyzes it and re-identifies only

the information necessary for criminal investigation.

In addition, this study suggests specific de-identification measures and legal improvement measures accordingly.

To protect the human rights of the public, it is necessary to revise the Protection of Communications Secrets Act by taking into consideration both the strengthening of the requirements of the law and the paradigm shift of the cell site analysis and investigation.

❖ Key word: Cell-site Investigation, Protection of Communications Secrets Act, Traffic Data, De-identification, Personal Information, Privacy, Digital Evidence

투고일 : 2월 27일 / 심사일 : 3월 14일 / 게재확정일 : 3월 14일