형사정책연구 Korean Criminological Review
제28권 제4호(통권 제112호, 2017・겨울)

통신비밀보호법상 휴대전화 위치정보의 실시간 추적 허용과 입법방향 : 독일의 통신사실확인자료 수집권과 비교하여*

민영성**・박희영***

국 | 문 | 요 | 약

휴대전화 위치정보의 실시간 추적 수사가 통신비밀보호법 제13조의 해석으로 가능한지 문제가 되고 있다. 형사실무에서는 가능하다고 보는 것 같다. 이와 관련하여 현재 헌법재판소에서 심리가 진행 중이다. 이러한 배경에서 휴대전화 위치정보의 실시간 추적 수사가 통비법의 통신사실확인자료 요청 규정에 의해서 과연 허용될 수 있는지를 독일의 논의와 비교 검토하였다. 독일의 경우 관련 규정의 개정을 통하여 과거, 장래 및 실시간 위치정보를 단계적으로 허용해 왔다. 특히 현행 형사소송법은 실시간 위치정보의 수집 요건을 더욱 엄격하게 요구하고 있다.

통비법의 통신사실확인자료 규정은 2001년 제정 당시 도입되었으며 2005년 개정으로 발신기지국의 위치추적자료가 추가됨으로써 휴대전화의 위치정보를 수집할 수 있게 되었다. 하지만 위치정보를 수집할 수 있는 통비법 제13조의 실체적 요건은 변경되지 않았다. 제13조는 법적인 보관의무라는 점에서 통신정보보관제도의 성격을 갖고 있지만 통신사실확인자료의 수집 요건과 절차는 독일 초기의 법적 상황에 머물러 있다. 이것은 독일 초기의 법적 상황에서 제기된 헌법적 문제점을 그대로 가지고 있다는 것을 의미한다.

이러한 통비법 규정의 해석으로는 휴대전화의 실시간 추적은 허용되지 않는 것으로 판단된다. 특히 통신제한조치의 기간 제한 조항을 준용하지 않고 있다는 점에서 이러한 해석은 더욱 명확하다. 따라서 현재 형사실무에서 행해지고 있는 위치정보의 실시간 추적은 잘못된 해석으로 금지되어야 한다.

과거의 위치정보가 아닌 장래의 위치정보 나아가 실시간 위치정보를 수집하기 위해서는 새로운 규정이 필요하다. 휴대전화의 위치정보와 같은 통신사실확인자료는 이동프로파일이 작성될 수 있기 때문에 상당히 민감한 개인정보이다. 특히 이러한 위치정보가 실시간으로 수집되는 경우 기본권 침해의 강도는 다른 통신사실확인자료와 비교하여 월등하게 높다. 따라서 수사기관이 이에 접근하기 위해서는 보다 엄격한 요건이 필요하다. 해당 규정을 개정할 경우 특히 유럽평의회의 사이버범죄협약의 가입을 고려하여야 할 것이다. 사이버범죄협약 제20조는 통신사실확인자료의 실시간 수집을 규정하고 있기 때문이다.

❖ 주제어 : 통신정보보관(통신데이터저장), 통신사실확인자료, 트래픽데이터, 위치정보, 위치추적, 통신기지국 수사, 통신비밀, 정보자기결정권

---

* 이 논문은 2014년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2014S1A5A2A01012247).

** 부산대학교 법학전문대학원 교수(주저자)
*** 독일 막스플랑크 국제형법연구소 연구원(교신저자)

Ⅰ. 머리말

스마트폰과 같은 휴대전화는 통화가 가능한 이용대기상태를 항상 유지하기 위하여 가장 가까운 통신기지국과 교신하면서 자신의 현재 위치를 알려주게 된다. 실제로 통화가 이루어진 경우는 물론 통화가 이루어지지 않더라도 통신기지국에서 위치정보가 생성되게 된다. 이러한 위치정보는 다양한 위치기반서비스에 이용되고 있다. 하지만 휴대전화가 통신에 이용되거나 이를 위해 이용대기상태에 있는 경우 그 위치정보는 통신의 비밀이 적용되는 통신사실확인자료(이하 '통확자료')[1]가 된다. 이 점에서 다른 위치정보와 구별된다. 위치정보가 실시간으로 추적되면 이동프로파일이 작성될 수 있다. 이러한 위치정보의 추적은 통신의 비밀을 침해할 수 있다.

헌법재판소는 지난 2017년 7월 휴대전화의 위치정보의 실시간 추적과 통신기지국 수사와 관련하여 제기된 헌법소원심판청구 사건의 공개변론을 실시하였다.[2] 청구인들은 위치정보의 추적자료를 제공하도록 한 통신비밀보호법(이하 '통비법') 제13조 제1항과 제2항 그리고 수사기관의 당사자에 대한 사후통지를 규정한 제13조의3 제1항의 위헌성을 제기하고 있다. 이들 규정이 청구인들의 통신의 비밀, 개인정보자기결정권 등 기본권을 침해하는지 여부 등이 그 쟁점이다. 통비법의 관련 조항들이 실시간 위치 추적과 기지국 수사의 허용여부 등을 명확히 하고 있지 않기 때문이다.

이러한 배경에서 이 글은 휴대전화 위치정보의 실시간 추적 수사가 통비법의 통확자료의 요청 규정에 의해서 과연 허용되는지를 다룬다. 이 문제를 해결하기 위해서 이 글은 독일법과 비교법적 연구를 시도한다. 독일은 이미 위치정보의 실시간 추적 수사를 포함한 통확자료의 수집과 이용에 관하여 그 동안 많은 논의를 축적해

1) 통비법의 '통신사실확인자료'는 EU 통신정보보관지침에서 '트래픽데이터'(Traffic data)로, 독일 현행 형사소송법에서는 EU 지침을 이행한 이후 트래픽데이터의 독일어 번역어인 'Verkehrsdaten'(교신데이터, 통신데이터, 통신정보 등으로 번역되고 있음)으로 사용되고 있다. 그 이전에는 '통신접속데이터'를 사용하였다. 통신접속데이터의 개념이 통신사실확인자료와 거의 일치한다. 트래픽데이터는 통비법의 통신사실확인자료를 포함하는 넓은 개념이다. 이 글에서는 통신사실확인자료와 트래픽데이터가 동일한 기능을 하므로 같은 의미로 사용한다. 다만 EU 지침은 과거의 트래픽데이터를, 독일의 규정은 과거와 장래의 트래픽데이터를 모두 포함한다.

2) 헌법재판소 보도자료, 실시간 위치정보 추적 및 기지국 수사 사건, 7월 공개변론 안내, 2017.7.11.

놓고 있다. 우리 통비법의 통확자료 제공 규정이 입법될 당시 독일에도 거의 유사한 규정이 이미 시행되고 있었다. 하지만 독일의 당시 규정은 위법 내지는 위헌의 논란이 있었고 이후 개정을 거치면서 실제로 해당 규정들은 헌법재판소로부터 위헌판결을 받았다. 그런데 현재의 관련 규정도 헌법소원심판이 청구되어 헌법재판소의 판결을 기다리고 있다. 이러한 배경에서 독일의 논의를 검토하는 것은 우리의 논의를 더욱 풍부하게 할 것으로 생각된다.

따라서 이 연구는 독일의 통확자료에 관한 입법적 논의가 어떻게 진행되어 왔는지, 현재 문제점은 무엇인지 그리고 앞으로 해결되어야 할 문제는 무엇인지를 휴대전화의 실시간 위치정보의 추적과 관련하여 검토한 후 통비법의 해당 규정에 관한 해석론과 입법방향을 제시하고자 한다.

우선 독일의 입법적 논의 과정(Ⅱ)과 현재의 관련 규정을 검토하고(Ⅲ) 문제점을 제시한다(Ⅳ). 그런 다음 독일의 논의 결과를 우리의 해당 규정과 비교 검토하고(Ⅴ) 입법방향을 제시한다(Ⅵ).

Ⅱ. 독일의 휴대전화 위치정보 추적[3)]에 관한 연혁적 논의

1. 1989년 통신시설관리법

독일에서 수사기관이 휴대전화의 위치정보를 포함한 통확자료를 수집할 수 있는

3) 통확자료와 관련하여 문제가 되는 휴대전화의 위치정보 추적 방법은 기본적으로 4가지가 고려된다. IMSI Catcher의 이용(소위 가상 기지국 설치), 실제 통화의 경우 통신접속데이터에 근거한 위치정보 수집, 실제 통화가 없는 이용대기상태에 있는 휴대전화의 위치정보 수집, 비밀 SMS 전송 방법(Stealth ping) 등이다. 특히 IMSI Catcher의 이용은 수사기관이 IMSI Catcher라는 특별한 통신장비를 사용하여 직접 소규모 가상의 통신기지국을 설치하여 피의자의 유심번호(IMSI) 및 휴대전화기의 번호(IMEI)를 확인하여 통신감청을 하거나 이 기지국 내에 있는 피의자를 (긴급) 체포하거나 구속영장을 집행하기 위해서 휴대전화의 소재지를 파악하기 위한 것이다. 위치확인 처분은 사실관계를 파악하기 위해서 피의자를 장기간 관찰하는데도 사용된다. 하지만 이를 통해서는 휴대전화의 위치정보를 추적하거나 전기통신을 감청해서는 안 된다. 이 규정을 휴대전화의 위치를 추적하기 위한 비교법적 사례로 인용하고 있는 국내 문헌은 제100i조를 잘못 이해한 것으로 보인다. IMSI Catcher의 가상기지국과 피의자의 휴대전화기가 교신하는 통신신호가 통신비밀의 보호대상인지 논란이 있

최초의 법적 근거는 1928년의 통신시설관리법(이하 'FAG')이다. FAG는 특별한 내용의 변경 없이 1989년 7월 3일 다시 공포되어 2001년 12월 31일까지 적용되었다. FAG 제12조에 따르면 피의자에게 소식이 전달된 경우 또는 그 소식이 피의자에게서 기인했거나 피의자를 위해 특정되었고 전기통신에 관한 정보가 수사를 위해서 의미를 가진다고 추론할 수 있는 사실이 존재하는 경우에는 법관 또는 긴급한 경우 검사도 ISP에게 그 정보를 요청할 수 있었다.

통신사실에 관한 자료의 구체적인 내용은 1991년 6월 24일의 '독일 연방우체국 텔레콤의 서비스제공에서 개인정보보호 법규명령'(이하 'TDSV')[4]에서 규정되었다. TDSV는 제6조에서 ISP가 수집, 처리 및 이용할 수 있는 전기통신접속데이터를 다섯 가지[5]로 열거하고 있었다.

FAG 제12조의 문언에 따르면 '과거'의 통신접속데이터와 그 속에 포함된 위치

었으나 헌법재판소는 기기 사이에 주고받는 통신신호는 통신비밀의 보호대상에 포함되지 않고 정보자기결정권의 대상이라고 하였으나 당시 형소법 제100i조는 정당화될 수 있다고 했다. 일반적인 행위의 자유도 침해하지 않는다고 했다(BVerfG, Beschluss vom 22. August 2006 - 2 BvR 1345/03, 판례에 대한 분석은 박희영·홍성기, 휴대전화 위치파악과 통신의 비밀, 165-193, 한국학술정보, 2010; 박희영, 경찰의 범죄 예방 및 수사 목적의 휴대전화 위치정보 파악의 허용과 그 한계, 경찰청 치안정책연구소, 2011, 책임연구보고서, 133면 이하). 따라서 이 방법은 통신사실확인자료의 위치정보를 수집하는 것이 아니다. 실제 통화가 이루어진 경우 통신접속데이터에 근거한 위치정보 수집은 전형적인 통신사실확인자료의 수집을 의미한다. 실제 통화가 없는 이용대기상태에 있는 휴대전화의 위치정보 수집은 그 동안 판례와 학설에서 상당한 논란이 있었다. 비밀 SMS 전송 방법은 수사기관이 통신기지국을 통해서 이미 알고 있는 휴대전화 소지자의 위치를 알아내기 위한 수사방법이다. 이것은 IP 트래킹과 유사하다(민영성·박희영, 독일에서 위치추적 수사방법으로서 IP트래킹의 허용근거에 대한 논의와 그 시사점, 형사정책연구 제28권 제2호(통권 제110호, 2017·여름), 259-260). 수사기관이 특별한 프로그램을 이용하여 휴대전화 소지자에게 SMS를 보내면 해당 휴대전화기는 소지자가 알 수 없게 신호를 보내게 되어 기지국의 위치가 확인된다. 이러한 수사방법이 허용되는지 역시 판례와 학설에서 많은 논란이 있었다. 이러한 논란은 2008년 형사소송법 개정으로 해결되었다.

4) 독일 연방우체국 텔레콤의 서비스제공에서 개인정보보호 법규명령(TDSV) v. 24. 6. 1991, BGBl I, 1390)은 전기통신의 민영화 이후 전기통신법의 개정으로 전기통신의 개인정보보호 법규명령(TDSV, Telekommunikations-Datenschutzverordnung)으로 대체되었으나(BGBl. I 2000 S. 1740) 전기통신법의 개정으로 2004년 6월 26일 폐기되었다.

5) TDSV 제6조 제1항 1. 송수신 회선 또는 단말기의 전화번호 또는 표시, 개인관련 권리표지, 고객카드의 이용 시 카드번호, 모바일 회선의 경우 위치표지, 2. 통신요금이 전달되는 데이터의 양에 따라 결정되는 경우 각 접속의 개시 및 종료 일시, 3. 고객이 사용한 전기통신서비스, 4. 유선접속의 경우 목적지 및 이의 개시 및 종료의 일시, 5. 그밖에 접속의 형성 및 유지를 위해서 또는 통신료 정산을 위해서 필요한 접속데이터. 이 조항은 이후 전기통신법 제96조 제1항으로 대체된다.

정보가 수집될 수 있었다.[6] 즉 피의자에게 소식이 '전달된' 경우 등 '과거형'을 사용하고 있었다. 따라서 이에 대해서는 다툼이 없었다.

하지만 장래의 접속데이터를 요청할 수 있는지 판례와 문헌에서 상당한 다툼이 있었다. 하급심 판례와 문헌들은 이 규범의 해석과 관련하여 두 가지로 나뉘어져 있었다. 일부 판례의 경우는 ISP에게 장래의 접속데이터도 수사기관에게 제공되어야 한다고 하였다.[7] 주요 논거는 ISP가 기본적으로 데이터를 기록할 기존의 기술적 가능성을 이용하지 않아 과거의 데이터를 보관하지 않기 때문에 이를 대상으로 한 처분을 소용없게 하여 제12조의 제공의무로부터 벗어난다는 것이었다. 게다가 장래의 접속데이터의 요청은 근접한 장래의 경우 이를 기다렸다가 정보요청을 다시 해야 하는 불편함을 방지할 수 있다고 한다. 하지만 다수의 판례[8]나 일부 문헌[9]은 제12조의 문언이 과거형을 사용하고 있기 때문에 장래의 접속데이터에 대한 제공명령은 할 수 없다고 보았다. 이러한 견해 차이는 결국 2002년 형사소송법에서 장래의 접속데이터를 포함시킴으로써 입법적으로 해결된다.

동일한 이유로 실시간 위치정보도 FAG 제12조에 포섭되지 않는다. 따라서 장래 및 실시간 위치정보는 형사소송법의 전기통신감청 규정(제100a조와 제100b조)에 의해서만 허용되었다. 이처럼 FAG 제12조는 과거의 통신접속데이터와 거기에 포함된 위치정보의 수집만을 허용하고 있었다.[10]

2. 2002년 형사소송법

FAG 제12조는 전기통신감청 규정과 같이 전기통신의 비밀과 개인정보자기결정권을 제한함에도 불구하고 제한 요건이 너무 낮게 설정되어 있고 특히 명확성 원칙

6) Demko, NStZ 2004, 57, 58; Wollweber, NJW 2002, 1554; Gercke, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, 2002, S. 81ff.

7) LG München I, B. v. 29.6.1998 - 6 Qs 26/98, MMR 1998, 613 = NStZ-RR 1999, 85.

8) LG Aschaffenburg, B. v. 12.2.1999 - Qs 8/99; LG Bremen, B. v. 12.4.1999, StV 1999, 307; OLG Hamm, B. v. 29.7.1999 - 3 Ws 407/99, CR 1999, 697; OLG Celle, B. v. 23.9.1999 - 1 Ws 211/99, StV 2000, 70.

9) Palm/Roy, NJW 1996, 1796; Klesczewski, StV 1993, 382, Welp, NStZ 1994, 213.

10) Demko, NStZ 2004, 57, 58; Wollweber, NJW 2002, 1554; OLG Celle StV 2000, 70, 71; Gercke, 2002, S. 81ff.

과 관련하여 헌법상 의문이 제기되었다.[11] 그리하여 FAG 제12조는 2002년 형사소송법 제100g조와 제100h조로 대체되고,[12] FAG의 전기통신에 관한 규정들은 1997년 전기통신법에 포함됨으로써 FAG는 2002년 1월 1일부터 완전히 폐지되었다.

FAG 제12조에서 제기된 비판들을 수용하여 2002년 형사소송법은 제100g조를 통신감청규정에 준하여 통신접속데이터의 수집 요건을 두었다. 제100g조에 따르면 중요한 의미를 가지는 범죄[13], 특히 전기통신감청 대상범죄 또는 전기통신을 수단으로 한 범죄의 혐의가 있고 수사를 위해서 필요한 경우 ISP는 요청에 따라 통신접속데이터를 제공할 의무가 있다(제1항). 그리고 사실관계의 조사 또는 피의자의 소재지 수사가 다른 방법으로는 가망이 없거나 본질적으로 어려울 수 있는 경우가 보충성 요건으로 추가되었다(제2항). FAG 제12조에서와 같이 '통신이 접속된 경우' 과거의 통신접속데이터가 제공될 수 있음은 물론 FAG 제12조에서 해석상 논란이 되었던 장래의 전기통신접속데이터도 요청할 수 있다고 규정하였다.

그런데 실시간 통신접속데이터가 요청될 수 있는지 문제가 되었다. 장래의 통신접속데이터의 수집에 실시간 통신접속데이터도 포함된다고 해석하는 견해가 있었으나,[14] 입법자의 의도는 포함되지 않는 것으로 보고 있다. 하지만 장래의 데이터를 요청할 수 있기 때문에 일정한 간격으로 위치정보가 수집되어 이동프로파일링이 작성될 수는 있다. 하지만 그 이동프로파일링은 정확도가 상당히 떨어지기 때문에 수사에 그다지 도움이 되지 못했다. 따라서 이에 대한 입법이 요구되었다. 위치정보의 실시간 수집은 여전히 FAG 제12조의 법적 상황과 마찬가지로 전기통신감청 규정인 제100a조와 제100b조에 의해서만 가능하였다.[15]

---

11) BT Drs. 14/7008, 2000.10.1.

12) BGBl. I 2001 S. 3879.

13) Wohlers/Demko StV 2003, 241 (245); Bär MMR 2002, 358 (360); BT-Drs. 14/7258, S. 4. 독일 형사소송법은 강제처분을 할 수 있는 범죄를 3가지로 구분하고 있고, 연방대법원과 헌법재판소는 이에 대한 구체적인 기준을 제시하고 있어서 위헌의 문제는 발생하지 않는다. 주거감청을 허용하는 '특별한 중범죄'(형사소송법 제100c조 제2항), 전기통신감청을 허용하는 '중범죄'(형사소송법 제100a 제2항), 법적 평화를 민감하게 교란하고 국민의 법적 안정성을 현저하게 침해하기에 적합한 것으로서 중간 정도의 범죄의 영역을 말하는 '중요한 의미를 가지는 범죄'. 중간정도의 범죄란 4년 이하의 자유형 선고가 예상될 수 있는 범죄를 말한다.

14) Demko, NStZ 2004, 57, 59 ff.

15) BGH MMR 2001, 442 m. Anm. Bär; LG Aachen StV 1999, 590; 반대 견해로는 Bernsmann/Jansen,

3. 2008년 형사소송법

2002년 형사소송법 규정들은 EU의 통신정보보관지침[16]과 유럽평의회의 사이버범죄협약을 국내법으로 이행하기 위하여 2008년 형사소송법 제100g조로 개정되었다.[17] 통신정보보관지침은 ISP에게 일정한 통신정보를 의무적으로 저장하게 하여 이를 수사기관이 이용할 수 있게 한 것이며 사이버범죄협약[18]은 트래픽데이터의 실시간 수집을 국내법으로 이행하게 한 것이다.[19]

형사소송법 제100g조는 2002년의 통신접속데이터의 개념을 전기통신법의 '트래픽데이터'(Verkehsdaten) 개념으로 대체하였다.[20] 트래픽데이터는 전기통신서비스를 제공함에 있어서 수집, 처리 또는 이용되는 데이터(제3조 제30호)로서 전기통신법 제96조에서 이의 수집과 이용에 관하여 구체적으로 규정하고 있다.

개정 규정은 수사기관이 수집할 수 있는 트래픽데이터를 두 가지로 구별하고 있다. 하나는 ISP가 업무상 필요에 의하여 수집하여 보관하고 있는 전기통신법 제96조의 트래픽데이터이고 다른 하나는 ISP가 의무적으로 보관해야 하는 전기통신법 제113a조의 트래픽데이터이다. 후자가 EU 통신정보보관지침을 이행한 것이다. 제113a조의 트래픽데이터는 이동전화서비스를 포함한 공중전화서비스, 전자우편서비스, 인터넷접속서비스로 구분하여 구체적으로 열거되어 있다. 다만 통신의 내용과 방문한 인터넷사이트는 제외되었다. 이들 트래픽데이터는 6개월 동안 보관해야 하

StV 1999, 591f.

16) 박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC, 인터넷법률, 법무부, 통권 제43호(2008. 7).

17) 박희영, 독일의 전기통신의 감청 및 통신데이터의 저장 등에 관한 법률, 법제 통권 제607호, 법제처, 2008. 7, 28-57.

18) 박희영·최호진·최성진, 사이버범죄협약 이행입법 연구, 2015년 연구용역 결과보고서, 대검찰청, 2015.12.

19) 박희영, 독일 형사소송법상 통신데이터 수집권과 한국 통신비밀보호법상 통신사실 확인자료제공요청권의 비교 및 시사점, 경찰학연구 제9권 제3호 통권 21호, 2009.12 33-61.

20) 지침 2002/58/EC 제2조 b)(traffic data)를 국내법으로 이행하기 위하여 2004년 6월 22일 전기통신법이 전면 개정되면서 TDSV의 전기통신접속데이터의 개념(제2조 제4호)은 트래픽데이터(Verkehrsdaten)의 개념(전기통신법 제3조 제30호)으로 대체되었다. 그리하여 ISP가 수집 및 이용할 수 있는 TDSV 제6조의 전기통신접속데이터는 전기통신법 제96조에서 트래픽데이터의 수집 및 이용으로 새롭게 규정되었다.

며 이 기간 경과 후 삭제해야 한다. 이에 반해서 제96조의 트래픽데이터는 업무상 필요한 경우 통신료정산(제97조), 통신내역증명(제99조), 통신장애(제100조), 악성 전화통지(제101조)를 위해서만 저장되어 이용될 수 있다. 보관 목적은 주로 통신요금을 산정하기 위한 것인데, 요금산정이 필요 없는 정액요금제의 경우 ISP는 기본적으로 통신 접속 종료 후 지체 없이 삭제해야 한다. 이 기간을 대법원 판례는 7일 이내로 인정하고 있다.[21] 하지만 최대 보관 기간은 규정되어 있지 않다. 제96조의 트래픽데이터에는 제113a조의 트래픽데이터가 대부분 포함된다. 즉 통신정보보관 지침을 이행한 제113a조에 의해서 ISP는 업무상 필요 없는 트래픽데이터도 저장해서 보관해야 한다.

형소법 제100g조는 두 가지 트래픽데이터에 대해서는 동일한 요건에서 접근을 허용하고 있다. 개정 규정은 또한 전기통신감청 규정에 준하여 수사기관에게 트래픽데이터를 ISP에게 요청할 수 있을 뿐 아니라 직접 수집할 수 있는 일반적인 수집 권한을 부여하였다. 트래픽데이터가 수집되기 위해서는 전기통신감청대상 범죄와 같이 개별적인 경우에도 중요한 의미를 가지는 범죄나 전기통신을 수단으로 한 범죄에 대한 혐의가 있고, 사실관계의 조사와 피의자의 거주지 수사를 위해 필요한 경우여야 한다. 전기통신을 수단으로 한 범죄에 대한 조치는 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 가망이 없고 데이터의 수집이 사건의 중요성과 적정한 관계에 있는 경우에만 허용된다.

제100g조의 개정으로 과거 및 장래의 데이터가 수집될 수 있을 뿐 아니라 실시간으로도 수집될 수 있게 되었다. 과거의 위치정보는 통신 개시 시 기지국의 위치정보를 저장하도록 되어 있었기 때문에 수집이 가능하였다. 2002년 형소법 제100g조에서는 통신이 '접속'된 경우에만 데이터가 제공될 수 있었는데, 2008년 형소법 개정으로 이것이 삭제됨으로서 장래의 데이터도 수집될 수 있게 되었다. 즉 그 동안 판례와 학설에서 논란이 많았던 이용대기상태의 휴대전화와 소위 Stille SMS(Stealth ping) 전송 방법이 규범적으로 허용된 것이다. 따라서 장래의 위치정보는 실시간으로 또는 일정한 간격으로 모아서 ISP로부터 제공받게 되었다. 하지만 위치정보의

21) 박희영, 유동 IP주소는 일주일간 저장될 수 있다, BGH Urteil vom 3.7.2014, III ZR 391/13, 최신 독일판례연구, 로앤비(www.lawnb.com), 2014.09, 1-9.

실시간 수집은 전기통신감청대상 범죄와 같이 개별적인 경우에도 중요한 의미를 가지는 범죄로 제한되었다.

입법자는 과거, 장래 및 실시간 트래픽데이터의 수집을 법적으로 달리 취급해야 될 특별한 이유가 존재하지 않았고 실제로 정당화되지도 않았다고 평가하였다.[22] 수사처분의 침해의 강도를 판단함에 있어서 중요한 것은 확보된 데이터의 질이 중요하다고 하였다. 즉 데이터의 질이 감청된 통신의 내용에 관한 정보를 제공하는지 또는 오로지 이의 외부적 상황만을 또는 이용대기상태에 있는 휴대전화의 위치정보의 수집과 같이 구체적인 전기통신과 관련이 없는 상황만을 제공하는 지이다.[23] 하지만 입법자의 의도와는 달리 위치정보의 실시간 수집은 ISP의 기술적 이행의 어려움과 위치정보의 부정확성 때문에 실무에서는 크게 활용되지는 못했다.

4. 연방헌법재판소의 무효 판결

연방헌법재판소는 2010년 3월 2일 EU 통신정보보관지침을 국내법으로 이행한 전기통신법 제113a조, 제113b조 그리고 제113a조에 근거해서 트래픽데이터가 수집되는 경우의 형사소송법 제100g조는 통신 비밀의 보호(기본법 제10조 제1항)를 침해한다는 이유로 무효로 판결하였다.[24]

헌법재판소는 형사소추, 위험예방 그리고 정보기관의 직무 수행을 위해서 범죄혐의나 위험혐의와 무관하게 6개월 동안 트래픽데이터를 저장하여 보관하는 것 자체는 기본법 제10조와 일치할 수 있다고 했다. 정당한 목적을 달성하기 위해서 이러한 저장이 비례성 원칙의 의미에서 적합하고 필요하다면 입법자는 이러한 규정으로 정당한 목적을 수행할 수 있다고 하였다. 또한 협의의 비례성 원칙과 관련하여도 이러한 저장 자체는 처음부터 정당성을 인정할 수 있다고 하였다.[25] 하지만 전기통신법

22) BT-Drs. 16/5846, S.51.

23) BVerfG, Urteil vom 27.02.2005 - 1 BvR 668/04(예방적 전기통신감청); BVerfG, Beschluss vom 22.08.2006 - 2 BvR 1345/03(IMSI-Catcher).

24) 이 판결에 대한 분석은 박희영·홍성기, 통신사실확인자료 저장의 통신비밀침해에 대한 위헌결정, 91-120, 한국학술정보, 2010.

25) BVerfG, 1 BvR 256/08 vom 2.3.2010, Rn. 205.

제113a조와 제113b조는 저장으로 인한 기본권 침해의 특별한 비중을 적절하게 고려하지 않았다고 판단하였다. 즉 트래픽데이터의 보관 및 이용을 위해서는 데이터의 안전성, 데이터의 이용목적 및 투명성 그리고 권리 보호의 관점에서 상당히 엄격하고 명확한 규정들이 필요하다고 하였다.

헌법재판소의 무효판결로 전기통신법 제113a조에 따라 ISP가 의무적으로 보관하고 있는 과거의 위치정보는 더 이상 수집할 수 없게 되었으나, 전기통신법 제96조에 따라 ISP가 업무상 필요에 의하여 보관하고 있는 경우에만 매우 한정적으로 과거의 위치정보가 수집될 수 있었고 장래 또는 실시간 위치정보는 여전히 수집될 수 있었다.

Ⅲ. 독일의 현행 형사소송법에 의한 위치정보의 수집 요건 및 절차

1. 개정 배경

헌법재판소는 통신정보보관지침을 이행한 전기통신법에 근거하여 데이터를 수집하는 한 2008년 형사소송법 제100g조는 통신의 비밀을 침해한다고 하여 위헌으로 판결하였다. 그 결과 ISP가 의무적으로 보관하고 있는 과거의 트래픽데이터에 대해서는 더 이상 수사기관이 접근할 수 없었다. 다만 수사기관이 이 데이터를 수집할 시점에 업무상 필요에 의하여 ISP에게 보관되어 있는 과거의 데이터와 장래의 데이터는 접근할 수 있었다. 하지만 저장기간은 개별 사업자마다 달랐기 때문에 트래픽데이터가 접근 시점에 아직 존재하고 있는지 유무는 우연에 달려있었다. 이러한 우연은 형사소추와 위험예방에 어려움을 야기하며 개별적인 경우 다른 수사방법이 존재하지 않는 한 수사가 성공하지 못하게 될 수도 있었다. 특히 테러와 같은 중대한 범죄에 대처하기 위해서는 이에 상응한 수권 규정이 필요하였다.

이러한 상황을 개선하기 위해서 ISP를 통한 트래픽데이터의 저장을 위한 법적 의무의 도입이 절실하게 필요하였다. 물론 상응한 규정은 이와 관련되는 기본권 침해 때문에 저장된 데이터의 범위와 데이터 이용의 관점에서 엄격한 요건이 요구되었다. 하지만 헌법재판소의 판결에 따라 이러한 규정은 절대적으로 필요한 것으로 제한되

어야 하고 높은 수준의 데이터 보안도 규범에 명확하게 그리고 구속력 있게 규정되어야 했다.

또한 유럽사법재판소도 통신정보보관지침이 비례성 원칙에 반하여 EU 기본권 헌장의 제7조(사생활존중)와 제8조(개인정보보호)의 기본권을 제한하고 있다는 이유로 이 지침을 무효로 선언하였다.[26)]

그리하여 독일 정부는 연방헌법재판소와 유럽사법재판소의 판결에서 제시한 기준들을 토대로 '트래픽데이터의 보관의무 및 최고 보관기간의 도입에 관한 법률'을 통하여 통신정보보관제도를 다시 도입하였다.[27)]

2. 트래픽데이터의 수집 요건

형사소송법 제100g조는 2008년 제100g조와 같이 트래픽데이터의 수집을 위한 독자적인 권한 규정이다. 하지만 2008년 규정과는 달리 제1항과 제2항에서 트래픽데이터를 구분하여 수집 요건에 차이를 두고 있다. 제1항은 ISP가 업무상 목적으로 수집하여 이용할 수 있는 전기통신법 제96조의 트래픽데이터의 수집을 규정하고 있고(임의적 보관), 제2항은 전기통신법 제113b조에 의해서 ISP가 의무적으로 보관해야 하는 트래픽데이터의 수집을 규정하고 있다(의무적 보관).

전기통신법 제96조 제1항의 트래픽데이터를 수집하기 위해서는 개별적으로도 중요한 의미를 가지는 범죄(특히 통신감청 대상 범죄)와 전기통신을 수단으로 하는 범죄의 혐의가 있고 사실관계를 조사하기 위해서 필요하고 데이터의 수집이 사건의 의미와 적정한 관계에 있어야 한다. 또한 전기통신을 수단으로 한 범죄는 사실관계

26) 민영성·박희영, 유럽사법재판소의 통신정보보관지침의 무효 판결과 그 시사점, 법학연구 제56권 제4호, 부산대학교 법학연구소, 2015, 53-82; 민영성·박희영, EU 통신정보보관제도의 정당성 - 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서 – 법학논문집 제40집 제1호(Vol. 40, No. 1), 2016, 중앙대학교, 449-473.

27) BGBl. 2015 Ⅰ 2218. EuGH(Große Kammer), Urteil vom 8.4.2014 - C-293/12, C-594/12, EuZW 2014, 459; 사법재판소의 판결과 독일의 법률에 대한 검토로는 정애령, 독일 통신데이터저장제도(Vorratsdatenspeicherung)의 비판적 고찰, - 유럽연합지침과 독일의 통신데이터저장제도 재도입 법률을 중심으로 -, 공법연구 제45집 제3호, 한국공법학회, 2017.2, 121-145; 민영성·박희영, 독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점, 부산대학교, 법학연구 제57권 제2호, 통권 88호, 2016.5, 89-109.

의 조사가 다른 방법으로는 가망이 없는 경우의 요건이 추가되었다(제1항). 한편 제100g조 제1항에 의해서 장래 및 실시간 트래픽데이터의 수집이 가능하다.

이에 반하여 형사소송법 제100g조 제2항은 전기통신법 제113b조에 의해서 ISP가 의무적으로 보관해야 하는 트래픽데이터의 수집 요건을 상당히 엄격하게 규정하고 있다. 우선 전기통신법 제113b조에 따라서 공중 전화 서비스 및 인터넷 접속 서비스와 관련하여 생성되는 트래픽데이터는 10주간, 이동통신서비스와 관련한 위치데이터는 4주간 보관해야 된다.[28] 하지만 통신의 내용, 인터넷사이트 방문 데이터, 전자우편서비스의 데이터는 저장에서 제외되었다. 형사소송법 제100g조 제2항에 따라 트래픽데이터가 수집되기 위해서는 '특별히 중대한 범죄'를 범한 혐의가 있어야 하며, 특별히 중대한 범죄는 형사소송법 제100g조 제2항[29]에 21개의 범죄 목록으로 열거되어 있다.[30] 그 행위는 구체적인 경우에도 중대해야 하고, 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 본질적으로 어렵거나 가망이 없어야 하며, 데이터의 수집은 사안의 의미와 적정한 관계에 있어야 한다.[31] 제100g조 제2항에 따른 트래픽데이터의 수집은 데이터가 실제로 저장되어 있는 것을 전제로 하므로 과거의 트래픽데이터를 대상으로 한다. 따라서 장래 또는 실시간 트래픽데이터의 수집은 이 조항에 의해서 허용되지 않는다.

형사소송법 제100g조 제1항의 트래픽데이터 수집은 법관과 긴급한 경우 검사가 명령을 내릴 수 있으나, 제2항의 트래픽데이터의 수집은 긴급한 경우라 하더라도 검사의 긴급명령은 허용되지 않는다(제101a조 제1항). 법원의 명령은 오로지 피의자와 이와 소식을 주고받은 자에 대해서만 내려질 수 있고, 데이터의 종류와 시간이 정확하게 표시되어야 하며, 처분의 이유가 제시되어야 한다. 과도하게 이동프로파일을 작성할 수 없도록 하기 위해서 기본적으로 개별적인 위치데이터만 호출되도록 해야 한다.[32]

수집된 트래픽데이터는 이용 목적에 엄격하게 구속되어야 한다. 수집된 트래픽데

28) 보관의무 위반 시 50만 유로의 과태료의 제재를 받는다(전기통신법 제149조 제1항 제36호).
29) 박희영·최호진·최성진, 앞의 연구용역 결과보고서, 165 참조.
30) BVerfGE 109, 279 (347 f.) = NJW 2004, 999; BVerfGE 125, 260 (328 f.) = NJW 2010, 833.
31) BT-Drs. 18/5088, 31.
32) BT-Drs. 18/5088, 34.

이터는 제100g조 제2항에 의한 처분이 명령될 수 있는 다른 형사절차나 제100g조 제2항의 범죄 혐의가 있는 자의 소재지를 수사하기 위해서만 이용될 수 있다(형사소송법 제101a조 제4항).[33] 목적구속성을 확보하기 위해서 트래픽데이터는 표시되어야 하고 지체 없이 이용되어야 하며 다른 기관으로 전달된 이후에도 수신자는 그 표시를 그대로 유지해야 한다. 트래픽데이터는 통신의 비밀과 관련된 자료이기 때문에 수집 이후 이용하는 경우에도 통신의 비밀이 유지되어야 한다는 의미다. 또한 트래픽데이터의 삭제는 기록되어야 한다(형사소송법 제101a조 제3항).

한편 유럽사법재판소 및 연방헌법재판소의 판결에 따라[34] 형사소송법 제53조 제1항 제1문에 언급된 자의 증언을 거부할 수 있는 내용을 알게 되는 것이 예상될 경우에는 이들의 데이터 수집은 허용되지 않는다. 만일 이미 인식하였다면 이의 사용은 금지된다(형사소송법 제100g조 제4항).

또한 헌법재판소는 트래픽데이터의 수집은 기본적으로 공개 처분이어야 한다는 기준을 제시하였다.[35] 따라서 당사자에게 형사소송법 제33조에 의해서 명령 이전에 의견을 제시할 기회를 부여해야 한다. 하지만 당사자의 의견 제시가 명령의 목적을 위태롭게 할 우려가 있는 경우에는 청문이 중단될 수 있다. 이 경우 그 이유가 제시되어야 한다.[36] 그리고 만일 통지가 당사자의 보호 이익에 중대하게 위반되어 중단되거나[37] 그 통지가 특히 수사의 목적을 위태롭게 하는 경우 유예될 수 있는데, 이 경우에도 항상 관할 법원의 명령이 필요하다. 당사자에 대한 통지가 유예되지 않는 이상 기본적으로 명령 이후 그리고 수집 이전에 행해져야 한다(형사소송법 제101a조 제6항). 이 경우 사후의 권리 보호 가능성을 통지받아야 한다(제101조 제4항 제2문). 통지를 받은 후 2주 이내에 당사자는 이의를 제기할 수 있다.

한편, 형사소송법 제100g조 제3항은 이전 규정과는 달리 기지국 수사의 법적 개념과 그 요건을 도입하였다. 이에 따르면 기지국 수사(Funkzellenabfrage)란 기지국에서

33) BVerfGE 125, 260 (333) = NJW 2010, 833.

34) EuGH, NJW 2014, 2169 Rn. 58; BVerfGE 125, 260 (334) = NJW 2010, 833.

35) BVerfGE 125, 260 (335 f.) = NJW 2010, 833. Rn.240.

36) BT-Drs. 18/5088, 36.

37) 제101a조 제6항은 제101조 제4항을 준용하여 당사자의 중대한 이익의 보호에 반하는 경우(제101조 제4항 제3문)와 당사자가 처분으로 인해 현저한 침해를 받지 않았거나 통지에 관심이 없을 것으로 추정될 수 있는 경우(제4항 제4문)에는 통지를 배제한다.

생성되는 모든 트래픽데이터를 수집하는 것을 말한다(제100g조 제3항 제1문).[38] 기지국 수사는 전기통신법 제96조 제1항과 제113b조에 따라 그 요건이 다르게 규정되어 있다. 전기통신법 제96조 제1항에 따라 저장되어 있는 데이터에 접근될 수 있는 무선기지국 수사는 특히 전기통신감청 대상범죄와 같이 개별적으로 중요한 의미를 가지는 범죄에 대한 혐의가 있어야 하고(제1호), 데이터의 수집은 사건의 의미와 비례관계에 있어야 하며(제2호),[39] 엄격한 보충성 조항으로써 사실관계의 조사 또는 피의자의 소재지 수사가 다른 방법으로는 가망이 없거나 본질적으로 어려워야 한다(제3호). 이 경우 검사의 긴급명령권도 인정된다. 이에 반하여 전기통신법 제113b조에 의해서 저장되어 있는 데이터에 접근해야 하는 기지국 수사는 '특별히 중한 범죄'의 혐의가 있고 그 행위가 개별적인 경우에도 특별히 중한 경우여야 하며 사실관계의 조사 또는 피의자의 소재지 수사가 다른 방법으로는 어렵거나 가망이 없고 데이터의 수집이 사건의 의미와 적정한 관계에 있어야 한다.

3. 위치정보의 실시간 수집 요건

위치정보는 다른 트래픽데이터와는 달리 이동프로파일이 작성될 수 있기 때문에 상당히 민감한 개인정보에 해당되므로 제100g조는 이의 수집에 엄격한 요건을 요구하고 있다. 우선 제100g조 제1항을 근거로 과거의 위치정보는 더 이상 수집될 수 없고 제100g조 제2항 제2문의 목록범죄의 혐의가 존재하는 경우에만 ISP에게 요청할 수 있다. 따라서 앞으로 수사기관의 실무에는 상당한 제약을 받을 수 있다. 왜냐하면 과거의 위치정보는 제100g조 제2항 제2문의 특별히 중대한 범죄가 존재하는 경우에만 ISP에게 조회를 요청할 수 있기 때문이다.[40] 장래 또는 실시간 위치정보

38) 기지국 수사란 신원이 확인되지 않은 행위자의 위치정보를 수집하는 협의의 기지국 수사만을 의미한다. 행위자의 신원이 알려진 경우의 광의의 기지국 수사는 다른 사람의 트래픽데이터가 침해될 소지가 없기 때문에 기지국 수사에서 제외된다. 이 경우에는 일반적인 통확자료 요청 절차에 따른다.

39) '사건의 의미'의 개념은 범죄혐의의 정도와 이 처분의 결과를 추측할 수 있는 개연성을 평가하여 판단해야 한다(박희영, 무선기지국 수사를 위한 법원의 명령 요건, AG Dortmund Beschl. v. 6.1.2016 -701 Gs 18/16, 최신독일판례연구, 로앤비 2017.10. 참조).

40) BeckOK StPO/Bär, 28. Ed. 22.7.2017, StPO § 100g Rn. 13-14.

의 수집은 제100g조 제1항 제3문에 따라서 개별적으로도 중요한 의미를 가지는 범죄에 해당하고 사실관계의 조사나 피의자의 소재지를 파악하기 위하여 필요한 경우에만 허용된다. 따라서 전기통신을 수단으로 행해진 범죄에 대해서는 장래 또는 실시간 위치정보의 수집은 적용되지 않는다.

한편 2008년 형소법에서는 ISP의 기술적 이행의 어려움과 위치정보의 부정확성 때문에 위치정보의 실시간 수집에 어려움이 있었다. 하지만 그 사이 기술적 문제가 보완되고 구체적인 법적 조치가 전기통신법 시행령에 추가되어[41] 이제 위치정보의 실시간 수집은 보다 쉽게 가능해졌다.

Ⅳ. 헌법소원심판청구와 유럽사법재판소 판결

독일 입법자는 헌법재판소와 유럽사법재판소의 무효 판결이 제시한 기준들을 입법에 반영하여 2016년 형사소송법 제100g조를 다시 개정하였다. 그럼에도 불구하고 이 법률은 2015년 12월 발효된 이후부터 2016년 12월 사이에 이의 집행을 정지해 달라는 가처분명령과 헌법소원심판들이 청구되었다.[42] 헌법재판소는 트래픽데이터의 저장으로 야기되는 개인의 자유 및 사생활에 대한 불이익은 이 데이터에 접근됨으로써 비로소 회복될 수 없는 침해가 구체화되기 때문에 데이터의 저장만으로는 아직 해당 규정들의 효력을 중지할 정도로 중대한 불이익은 발생하지는 않는다고 하면서 가처분 명령 신청을 기각하였다.[43]

이에 더하여 이 법률이 발효된 지 얼마 되지 않아 유럽사법재판소는 2016년 12월 21일 통신정보보관지침을 국내법으로 이행한 영국과 스웨덴의 관련 법률이 EU의 전자 프라이버시 지침과 유럽 기본권헌장에 위반된다는 이유로 또 다시 무효로

41) 전기통신감청처분을 이행하기 위한 기술적 조직적 법규명령(TKÜV) 제32조((BGBl. 2017 I 2316) (BeckOK StPO/Bär StPO § 100g Rn. 24-25.)

42) 사건번호가 부여되어 공개된 헌법소원심판청구사건은 1 BvR 3156/15, 1 BvR 17/16, 1 BvR 141/16, 1 BvR 229/16, 1 BvR 847/16, 1 BvR 1258/1, 1 BvR 1560/16, 1 BvR 2023/16, 1 BvR 2683/16, 1 BvR 2840/16 등이다.

43) 박희영, 제2차 통신정보보관법률에 대한 가처분 명령 신청 기각, BVerfG, Beschluss vom 08. Juli 2016 - 1 BvR 229/16, 최신독일판례연구, 로앤비(www.lawnb.com), 2016.10, 1-8.

판결하였다.[44] 무효의 핵심 근거는 범죄혐의나 위험혐의도 없이 개인의 민감한 개인정보인 통신정보를 보관해서는 안 된다는 것이었다. 사법재판소의 첫 번째 판결에서는 통신정보의 보관 자체가 EU기본권헌장에 위배되는지 명확하지 않았다. 이에 대한 견해가 나뉘어 있었지만 독일 입법자는 보관 자체는 기본권 헌장에 위배되지 않는다고 해석하였다.[45] 그런데 사법재판소는 두 번째 판결에서 보관 자체가 EU기본권 헌장에 위배된다는 것을 명확히 한 것이다. 이 판결에 따라 최근 독일 하급심 판례는 현행 규정들이 EU법과 일치하지 않는다며 ISP의 데이터 보관의무를 부정하였다.[46]

유럽사법재판소의 판결과 달리 독일 헌법재판소는 2010년의 무효판결에서 엄격한 요건을 갖추면 통신정보의 사전 보관도 가능하다고 하였다. 따라서 EU의 최고법원과 독일 연방헌법재판소의 견해가 대립하는 형국이 되었다. 조만간 독일 헌법재판소는 두 번째 통신정보보관 규정에 대한 헌법소원에서 이에 대한 해답을 제시해야 한다. 만일 헌법재판소가 유럽사법재판소의 의견을 받아들이게 되면 독일의 해당 규정은 위헌 무효가 될 가능성이 높다. 만일 그렇게 되면 의무적 데이터 보관 규정인 전기통신법 제113b조와 관련이 있는 형사소송법 제100g조 제2항과 제3항 제2문은 적용될 수 없다. 하지만 전기통신법 제96조의 트래픽데이터와 관련이 있는 제100g조 제1항과 기지국 수사에 관한 제100g조 제3항 1문에 의해서 여전히 수집이 가능하게 될 것이다. 따라서 위헌 판결이 선고되더라도 과거의 위치정보는 수집될 수 없지만 제96조에 의해서 장래 또는 실시간 위치정보는 계속 수집될 가능성이 높다.

---

44) EuGH(Große Kammer), Urteil vom 21.12.2016 – C-203/15, C-698/15, EuZW 2017, 153-160. 이 판결에 대한 소개는 박희영, 일반적인 통신정보 보관의무는 EU법과 일치하지 않는다, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.2, 1-5.

45) BT-Drs. 18/5088, S.23.

46) 박희영, 이유 없이 통신사실확인자료를 보관하는 것은 EU법에 위반된다, OVG Münster, Beschluss vom 22.06.2017, 13 B 238/17.

Ⅴ. 통신비밀보호법에 따른 위치정보의 실시간 수집의 허용여부

1. 통신정보보관제도와 통신사실확인자료 요청의 관계

위치정보의 실시간 수집에 관하여 논의하기 이전에 우리 통비법의 통확자료요청 규정의 성격이 확인되어야 한다. 국가기관이 국민의 통신정보를 범죄혐의와 상관없이 미리 저장하여 보관하였다가 이후에 특정 범죄가 예상되거나 그러한 위험이 구체화되거나 실제로 발생한 경우 그 범죄에 대한 정보를 수집하거나 그 범죄를 예방하거나 수사하기 위해서 보관된 통신정보를 국가기관이 이용하는 것을 통신정보보관제도(Data Retention System, Vorratsdatenspeicherung)라고 한다.[47] 통신정보보관제도의 핵심은 통신정보를 범죄 및 위험 혐의와 상관없이 의무적으로 미리 저장하여 보관한다는 데 있다. 따라서 통신정보보관제도는 '과거'의 통확자료를 대상으로 한다.

통신정보보관제도는 유럽연합의 통신정보보관지침(2006/24/EC)[48]에서 유래한다. 이 지침은 테러와 같은 중대한 범죄를 예방하고 소추하기 위해서 ISP에 의해서 생성되거나 처리되는 특정 통신정보를 보관하게 하여 이후에 이를 이용할 수 있도록 규정하고 있었다. ISP는 자신의 통신서비스를 제공하는 과정에서 생성되거나 처리되는 통신정보를 최소 6개월에서 최대 2년까지 저장하여 보관해야 한다(지침 제3조 및 제6조). 하지만 이 지침은 사법재판소로부터 무효판결을 받아 현재 EU 차원에서 통신정보보관제도는 존재하지 않는다.

독일의 경우 ISP가 의무적으로 보관해야 하는 전기통신법 제113b조의 트래픽데이터와 이를 근거로 한 형소법 제100g조 제2항과 제100g조 제3항 제2문이 통신정보보관제도에 해당된다.

우리 통비법 역시 범죄수사, 법원의 재판, 국가안보를 위하여 필요한 경우 ISP에게 통확자료를 요청하여 제공받을 수 있다고 규정하고 있다. ISP는 이러한 통확자

47) 민영성·박희영, 통신정보보관제도의 정당성 - 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서 -, 법학논문집 제40집 제1호(중앙대학교 법학연구원), 2016, 450.

48) 이 지침의 전문 번역은 박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC, 인터넷법률, 법무부, 통권 제43호(2008. 7), 144-175.

료를 요청기관에 제공하기 위해서 이들 자료를 수집하여 보관하고 있어야 한다. 이를 위해서 통비법은 통확자료의 보관을 ISP의 협조의무로 규정하고(동법 제15조의 2) 통확자료의 구체적인 보관기간을 시행령에 위임하고 있다(통비법 시행령 제41조). 통비법의 통확자료의 보관은 법적 의무이므로 통신정보보관에 해당된다.[49] ISP가 이러한 협조의무에 근거해서 통확자료를 제공해야 하는 것은 강제수사에 해당된다.[50] 따라서 통확자료의 수집 및 이용에 관한 독일과 EU의 (특히 헌법상의 기본권과 관련한) 논의들이 전용될 가능성이 있다. 하지만 장래의 통확자료도 포함되는지에 대해서는 현재 논란이 되고 있다.

2. 독일과 한국의 통신사실확인자료 수집 요건의 개략적 비교

위치정보의 실시간 추적의 허용여부를 검토하기 이전에 통신사실확인자료의 일반적인 요건을 독일의 규정과 비교하여 차이점을 간략하게 살펴본다.[51]

우선 통비법에 규정되어 있지 않는 차이점은 다음과 같다. 대상 범죄의 구분[52], 통확자료 수집의 원칙적 공개처분, 처분 대상자의 특정(피의자와 피의자를 위한 소식전달자, 피의자가 사용하고 있는 통신회선 및 정보기술시스템 보유자), 기지국 수사, 확보한 자료의 이용과 관련한 목적구속성과 이를 확보하기 위한 트래픽데이터의 표시 의무, 증언거부권자에 대한 수집 제한 및 이의 사용금지, 당사자에 대한 원칙적 사전통지와 권리보호를 위한 불복신청, 데이터 표시의무, 데이터 삭제의무, 데이터 보안, 연방의회 보고 등이다.

---

49) 동일한 견해로 생각되는 문헌은 정애령, 앞의 논문, 126.

50) 차진아, 통신비밀보호법 제13조 제1항 및 제2항 등의 합헌성 여부에 대한 검토 - 헌재 2012헌마191 등 헌법소원심판청구 사건에 대한 검토를 중심으로 -, 법조 2017.8(Vol.724), 261 각주 33.

51) 통비법 제13조와 독일 형사소송법 제100g조의 차이점과 유사점에 대한 상세한 설명은 지면 관계상 여기서는 더 이상 다루지 않는다.

52) 통비법 제13조는 모든 범죄를 대상으로 하고 있다. 이와 관련하여 중범죄를 대상으로 해야 한다는 견해로는 임규철, 전기통신사업자의 수사기관으로의 통신정보 제공 시 문제점과 개선방향 -통신사실확인자료 및 통신자료의 제공을 중심으로-, 헌법학연구(제19권 제3호), 한국헌법학회(2013), 272-273. 모든 범죄를 대상으로 해야 한다는 견해로는 차진아, 앞의 논문, 281.

그리고 요청 대상 통확자료의 범위[53] 및 이의 보관 기간[54], 요청 요건[55], 요청 주체의 제한 등[56]에서도 상당한 차이를 보이고 있다.

전체적으로 보면 독일의 경우 ISP가 업무상 필요에 의해서 보관하는 경우(전기통신법 제96조)와 의무로 보관해야 하는 경우(동법 제113b조)로 이원화하여 통확자료를 수집하고 있으나, 통비법의 경우 의무적으로 보관한 자료만을 수집하고 있다. 통비법은 법적인 보관의무라는 점에서 통신정보보관제도에 해당되는 제113b조와 성격이 같지만 통확자료의 대상이나 범위 등 형식의 면에서는 제96조의 규정과 거의 유사하다.

독일의 전기통신법 제96조의 트래픽데이터는 '그밖에 필요한 정보'라는 표지를 사용하여 통신기술의 발전에 개방되어 있는데 이를 제한적으로 열거하고 있는 우리의 통확자료와 구별되고, 제113b조에서 구체적으로 열거되어 있는 트래픽데이터가 우리의 것보다 양적으로 많다는 점에서도 차이가 있다. 하지만 우리의 규정은 양적으로는 적지만 해석의 가능성이 있다는 점이 고려되어야 한다.[57] 통확자료의 수집은 통신비밀의 침해와 관련되기 때문에 양적인 문제가 아니라 질적인 문제로 접근

53) 통비법 제2조 제11호에서 7가지의 통확자료를 열거하고 있는 데 독일의 경우 전기통신법 제96조와 제113b조에서 분리하고 있다.

54) 독일의 위치정보는 4주간, 나머지는 10주간인데 비하여, 우리의 경우 가목에서 라목, 바목은 원칙적으로 12개월, 시외 및 시내전화역무와 관련된 자료인 경우에는 6개월, 바목과 사목의 자료는 3개월 이상 보관해야 한다.

55) 통비법은 '수사를 위하여 필요한 경우'인데 반하여 독일의 경우 최소한 중범죄와 통신을 수단으로 한 범죄 등 그 요건을 엄격하게 요구하고 있다.

56) 독일의 경우 전기통신법 제113b조의 경우 검사의 긴급청구권을 인정하지 않는다.

57) 독일 전기통신법 제113b조는 SMS와 같은 메신저 서비스도 포함시키고 있다. 하지만 통신의 내용이나 방문한 인터넷사이트에 관한 정보나 전자우편서비스와 관련한 트래픽데이터는 저장하지 못하도록 명시하고 있다. 통비법은 이러한 명문 규정을 두고 있지 않지만, 카톡과 같은 메신저서비스, 전자우편서비스, 방문한 인터넷사이트에 관한 정보는 통비법의 전기통신의 개념에 포섭되기 때문에 통비법의 해석으로 이들 서비스와 관련하여 생성되는 통확자료의 요청이 가능할 수 있다. 특히 현재의 통신기술 수준에 따르면 메신저 서비스의 경우 트래픽데이터와 내용을 분리하는 것이 어렵다. 따라서 메신저 서비스의 통신 내용이 파악될 위험성이 존재한다. 이와 관련하여 연방헌법재판소는 가처분 명령 결정에서 "전기통신법 제113b조 제5항에 규정된 SMS의 경우 트래픽 데이터와 통신내용의 분리가 기술적으로 가능하지 않다면, 이 규정을 폐기할 것이 아니라, 적어도 데이터 보관의무를 이행하기 위해서 우선 기술적 요건을 마련해야 한다"고 하였다(박희영, 제2차 통신정보보관법률에 대한 가처분 명령 신청 기각, BVerfG, Beschluss vom 08. Juli 2016 - 1 BvR 229/16, 최신독일판례연구, 로앤비(www.lawnb.com), 2016.10, 1-8).

해야 한다.[58]

이러한 차이점들로 인하여 우리의 통확자료 요청제공은 독일 헌법재판소의 위헌판결과 유럽 사법재판소의 무효판결이 제시한 수준에 훨씬 미치지 못하는 것으로 보인다.[59] 따라서 아래에서는 서론에서 언급한 헌법재판소의 공개변론에서 제기된 위치정보의 실시간 수집의 허용 여부에 대해서 검토한다.

3. 위치정보의 실시간 수집 허용 여부

가. 과거 위치정보의 수집 여부

휴대전화의 위치 확인과 관련되는 것은 발신기지국의 위치추적자료(제2조 제11호 바목)와 정보통신기기의 접속지 위치추적자료이다(제2조 제11호 사목). 후자에는 스마트폰이나 태블릿 PC와 같이 인터넷기반의 모바일폰의 위치정보가 해당될 수 있다.

통비법 제13조는 수집의 요건이 '수사를 위하여 필요한 경우'만으로 규정되어 있다. 즉 과거의 위치정보는 수사를 위하여 제13조에 의해서 수집될 수 있다. 과거의 위치정보가 수집되기 위해서는 '특별히 중대한 범죄'를 범한 혐의 등 엄격한 요건(형사소송법 제100g조 제3항)을 갖추도록 한 독일의 경우와 비교하면 현저한 차이를 보이고 있다.

나. 장래 및 실시간 위치정보의 수집 여부

장래 또는 실시간 위치정보가 통비법 제13조에 의해서 수집될 수 있는지 문제가 되고 있다. 독일의 경우 장래 또는 실시간 위치정보가 수집되기 위해서는 통신감청 대상 범죄에 준하는 중요한 범죄여야 하고 사실관계의 조사나 피의자의 소재지를 파악하기 위해서 필요한 경우여야 한다. 그러나 통비법 제13조는 이와 같은 요건을 전혀 명시하지 않고 있다. 따라서 제13조의 규정에서 과연 위치정보의 실시간 수집

58) BVerfG, Urteil vom 27.02.2005 - 1 BvR 668/04; BVerfG, Beschluss vom 22.08.2006 - 2 BvR 1345/03.

59) 이에 대한 구체적인 검토는 다음 기회로 미룬다.

이 허용될 해석의 여지가 있는지 의문이 제기된다. 특히 이 규정은 어느 시점의 통확자료가 제공되어야 하는지를 명확하게 언급하고 있지 않기 때문이다. 따라서 세 가지 해석이 모두 가능할 수 있다. 수사기관의 입장에서는 가능한 많은 통확자료가 확보되는 것이 수사에 유리하므로 세 가지 모두 가능하다는 해석을 주장할 수 있고 헌법재판소의 공개변론의 자료에서도 실제로 수사기관이 그렇게 요청하고 법원이 허가하고 있다는 것이 형사실무임을 알 수 있다.

하지만 이러한 실무의 해석과 달리 몇 가지 관점에서 과거 시점의 통확자료만 허용된다는 해석이 타당하다. 첫째, 정보통신부의 통신업무처리지침의 문제점을 지적할 수 있다. 통비법 제13조가 신설된 2001년 12월 29일 정보통신부 통신업무처리지침은 자료제공요청서 접수시점 이전의 자료, 즉 과거의 통확자료로 한정하고 있었다.[60] 그런데 2005년 11월의 통신업무 처리지침은 통확자료의 범위에 장래 발신(착신) 전화번호의 추적을 포함하고 있다.[61] 이 지침은 통확자료의 바목과 사목이 2005년 통비법 개정으로 도입되면서 개정된 것으로 보인다.[62] 하지만 이러한 이유로 개정되었음에도 불구하고 이 지침은 '유독' 전화번호에만 장래 발신(착신)의 추적을 허용하고 있고 바목과 사목의 위치추적 자료에는 그러한 언급이 없다. 전화번호의 추적과 위치정보의 추적은 그 성질이 다르다. 앞서 살펴본 독일 형사소송법도 이를 명확히 구별하고 있다. 휴대전화를 포함한 전화번호의 추적은 전화번호의 확인으로 이해되며 이것은 ISP에게 요청하여 확보될 수 있다. 전화번호의 추적을 휴대전화의 위치를 파악하는 통신기지국 수사에 포함시키는 것은 기본권 침해의 강도가 서로 다르기 때문에 명확한 규정이 필요하다. 따라서 이 지침에 근거하고 있는 형사실무는 위법하다. 이러한 해석은 통비법 제13조 제9항의 의미를 잘못 이해한 것으로 보인다.

둘째, 입법자는 통비법 제13조 제9항을 통해서 과거의 통확자료만 요청하도록 명확히 하고 있다. 즉 통비법 제13조 제9항은 범죄수사를 위한 통신제한조치의 허가절차를 준용하면서 통신제한조치의 기간을 규정하고 있는 제7항을 '제외'하고 있기

60) 김용환, 통비법 중 개정법률안에 대한 의견제시의 건 검토보고서, 과학기술정보통신위원회 수석전문위원, 2001. 2, 6면.

61) 정보통신부, 통신비밀 보호업무 처리지침, 2005. 11.

62) 차진아, 앞의 논문, 273-274.

때문이다. 동조 제7항은 통신제한조치는 2월을 초과하지 못하고, 그 기간 중 통신제한조치의 목적이 달성되었을 경우에는 즉시 종료해야 한다. 통신제한조치의 기간에 관한 이 조항은 장래의 전기통신이나 실시간 전기통신의 감청을 전제로 하고 있다. 따라서 제13조 제9항이 제6조 제7항을 제외한 것은 과거의 통확자료만 해당되고 장래 또는 실시간 통확자료는 해당되지 않는 것으로 해석될 중요한 근거가 될 수 있다. 그런데 이와 반대의 해석도 가능할 수는 있다. 즉 제7항을 제외한 것을 과거, 장래, 실시간 모두 가능하다는 의미로 해석하는 것이다. 하지만 이러한 해석은 기본권 침해가 무한정 확대되는 것을 허용하는 의미이므로 만일 입법자가 그렇게 의욕하였다면 입법형성권의 한계를 넘어선 것이다. 따라서 이러한 해석은 타당하지 않다. 우리 입법자가 통비법 제13조 제9항을 통해서 전기통신감청과 통확자료 요청의 성격이 다르다는 점[63]을 인정한 것으로 보는 것이 더욱 합리적인 해석이다.

셋째, 이러한 점은 비교법적 검토를 통해서도 확인될 수 있다. 앞서 검토한 독일의 경우에도 FAG 제12조에서 장래의 데이터의 요청여부에 대하여 논란이 있었으나 2002년 형사소송법 제100g조에서 감청규정을 준용함으로써 3개월까지 장래의 위치정보도 확보할 수 있도록 하였다. 하지만 이 경우에도 실시간 수집은 허용되지 않았다. 장래의 수집에서 실시간 수집과 일정 기간 모아서 제공하는 것을 명확히 구분한 것이다. 실시간 위치정보 수집은 2008년 형사소송법에서 사이버범죄협약을 이행함으로서 비로소 입법화되었다.

넷째, 통신사실확인자료라는 법문언은 통신사실을 '확인'하는 자료라는 의미로 보면 일단 통신이 발생해 있어야 한다는 것을 전제로 한다. 이것은 앞서 검토한 독일의 통신접속데이터의 해석과 유사한 측면이 있다. 이 조항은 과거형을 사용하고 있었음에도 불구하고 수사의 필요성에 의해서 장래의 데이터도 포함되는 것으로 해석하려고 하였다. 장래의 어느 시점에 발생한 통신(즉 미래완료시제)으로 해석할 수 있다는 점이다. 하지만 이러한 논란은 2001년 개정 형사소송법 제100g조에서 장래의 통신접속데이터가 법문언에 추가됨으로써 명확히 되었다. 그 당시 실시간 수집

63) 이러한 법적 근거에 대한 언급은 없지만 양자의 차이점에 대한 명확한 설명은 황성기, 현행 통신비밀 보호법제의 헌법적 문제점, 언론과 법, 2015.4, 5. 참조. 문헌에서는 대부분 이러한 관점에서 과거의 통확자료로 보는 것 같다(정애령, 앞의 논문, 126면; 조기영, 최근 주요 쟁점과 관련한 통비법 개정방향, - 휴대전화 감청, 패킷감청, 기지국수사, GPS위치정보 추적을 중심으로 -, 132.

이 허용된다는 소수 견해도 있었지만 입법자의 의도나 다수 견해는 실시간 수집이 허용되지 않는 것으로 해석되었다. 실시간 수집은 2008년 형사소송법에서 비로소 허용되었다.[64)]

다섯째, 이용대기상태에 있는 위치정보는 제13조에 의해서 수집될 수 없다. 통신 '사실확인' 자료는 통신이 행해진 것을 전제로 하고 있기 때문이다. 따라서 실제 통신이 이루어지지 않은 이동전화에 대해서 비밀 SMS 전송 등 상대방의 위치를 실시간으로 알아내는 방법은 허용되지 않는다. 뿐만 아니라 이용대기상태에 있었던 과거의 위치정보도 요청될 수 없다.

끝으로 휴대전화와 통신기지국 사이에 주고받는 교신사실을 확인하는 위치정보 추적자료는 기본권 제한의 정도가 결코 낮지 않다. 독일의 경우 통확자료에 해당되는 위치정보의 경우뿐 아니라 가상 기지국을 통하여 휴대전화의 위치를 확보하는 IMSI Catcher 방법(형소법 제100i조)과 GPS 등을 통하여 수집되는 위치정보의 경우(형소법 제100h조)[65)]에 감청에 준하는 범죄를 대상으로 하고 있고 엄격한 보충성 요건을 명확히 하고 있기 때문이다. 따라서 이러한 요건을 전혀 두지 않은 통비법 제13조에 의해서 위치정보를 추적하는 것은 허용되지 않는다.

이상의 검토를 통해서 알 수 있듯이 제13조의 통확자료 요청은 과거의 통확자료에 한해서만 허용되고 장래 또는 실시간 통확자료의 수집은 허용되지 않는 것으로 보아야 한다. 그럼에도 불구하고 장래 또는 실시간 통확자료가 허용되는 것으로 해석하고 실무에서 그렇게 운용되고 있다면 이것은 부당한 공권력 작용으로 보아야 하고 이를 근거로 한 처분은 위법한 것으로 보아야 한다.

따라서 다양한 해석상의 문제를 해결하기 위해서는 독일의 규정과 같은 명확한 규정이 필요하다. 특히 위치정보의 경우 아주 민감한 개인정보에 해당되기 때문에

64) 위치추적은 기본적으로 장래 또는 실시간 위치추적을 포함하는 것이라는 견해가 있다(차진아, 앞의 논문, 273 각주 53). 그 근거로 독일 형사소송법 제100g조 제3항을 들고 있다. 하지만 앞서 검토한 바와 같이 독일의 경우 사이버범죄협약 제20조를 국내법으로 이행한 2008년 형사소송법에 비로소 실시간 위치정보의 수집이 허용되었다. 그 이전의 2002년 형사소송법은 과거 및 장래의 위치추적만 허용되었다(물론 '통신이 접속된 경우'라는 법문언이 없는 통비법 제13조에서는 그러한 해석이 가능할 수도 있다). 제100g조 제3항은 전기통신감청대상 범죄와 같은 중대한 의미의 범죄의 경우에만 실시간으로 수집될 수 있고 위치정보의 민감성 때문에 과거의 위치정보는 제1항에 의해서 수집해서는 안 된다는 것을 명확히 한 것이다.

65) 이에 대해서는 민영성·박희영, 앞의 논문, 형사정책연구 제28권 제2호, 265 참조.

그 수집에는 엄격한 요건이 필요하다. 위치정보가 실시간으로 수집되면 이동프로파일이 작성될 수 있어서 통신감청에 준하는 정도의 통신의 비밀이 침해되기 때문이다.

Ⅵ. 위치정보의 실시간 수집의 개정 방향

통비법 제13조의 해석론을 통해서 과거의 위치정보만 수집할 수 있고 장래 또는 실시간 위치정보는 수집할 수 없음을 확인하였다. 따라서 헌법재판소가 통비법 제13조 제9항을 통해서 과거의 통확자료만 요청할 수 있도록 제6조 제7항의 준용을 배제한 것이 입법자의 의도임을 확인할 필요가 있다. 그렇다면 해당 조항의 잘못된 해석과 적용으로 수행되고 있는 현재의 형사실무는 더 이상 허용되어서는 안 된다.

하지만 나날이 발전하는 정보통신환경에서 테러와 같은 중대한 범죄에 대처하기 위해서는 장래 및 실시간 위치정보의 수집 행위는 정당하고 필요하며 적합한 수단이라고 평가될 수 있다. 그렇다 하더라도 이러한 통확자료를 수집하기 위해서는 헌법상의 통신의 비밀 보호와 정보자기결정권이 제한될 수 있다는 점에서 비례성원칙이 충분히 고려되어야 한다.

독일의 검토에서 보았듯이 과거의 통확자료에 비해서 장래의 통확자료에 대한 요건이 상대적으로 덜 엄격하였다. 하지만 위치정보의 실시간 수집은 고도의 민감성과 이동프로파일의 작성 가능성 때문에 다른 통확자료보다 그 요건이 더욱 엄격하였다. 따라서 개정하는 경우 위치정보와 다른 통확자료의 수집 요건에 차등을 두어야 할 것이다. 특히 대상범죄에 따라 요건을 달리해야 한다. 현재의 '범죄수사를 위하여'란 실체적 요건 하나만으로 모든 통확자료를 수집할 수 있도록 한 통비법 제13조 제1항은 비례성 원칙에 위배될 수 있기 때문이다. 물론 제13조 제2항(요청사유, 해당가입자의 연관성 및 필요한 자료의 범위)의 법관유보를 통해서 이를 보완할 수도 있겠지만[66] 통확자료의 요청이 남용되어 온 실무를 보더라도 법관유보를 통해서 기본권 보장을 기대하는 것은 사실상 어렵다고 판단되므로 법관유보가 아니라 법률유보로 규정되어야 한다.

66) 제13조 제2항의 보완으로 가능하다고 보는 견해는 차진아, 앞의 논문 249면 이하.

독일의 경우 통비법 제13조 제2항보다 훨씬 더 엄격하고 구체적인 요건에서 법관유보가 규정되어 있다는 점에 주목할 필요가 있다(형소법 제100g조가 준용하고 있는 제100e조 제3항과 제4항). 특히 명령 이유에서 그 요건 및 본질적인 이익형량의 관점이 제시되어야 하고 개별적으로 혐의를 뒷받침하는 사실, 처분의 필요성과 비례성에 대한 본질적인 이익형량도 기재되어야 한다. 이러한 상세한 규정들은 법률유보를 통해서 법관유보의 폐해를 방지하기 위한 것이다. 그럼에도 불구하고 실체적 요건에서 통비법 제13조 제1항보다 훨씬 더 엄격한 실체적 요건을 두고 있다.

개정 시 주의할 점은 통신의 비밀과 관련되는 통확자료와 그렇지 않은 일반 위치정보를 구별해야 한다는 것이다. 지난 국회 회기와 마찬가지로 이번 국회 회기에도 위치정보법의 위치정보를 통비법의 위치정보에 포함시키자는 통비법 전부개정법률안[67]이 발의되어 있다. 이 법률안은 통확자료의 바목과 사목을 분리하여 범죄수사를 위한 위치정보추적자료의 제공이라는 별도의 조항을 두고 위치정보추적자료에 위치정보법의 위치정보를 포함시키고 있다. 이에 대해서는 비판이 제기될 수 있다. 휴대전화의 경우 위치정보법이 규정하고 있는 이동성이 있는 물건에 해당된다. 따라서 휴대전화의 위치정보는 통비법의 통확자료인 동시에 위치정보보호법의 위치기반서비스에서 제공되는 위치정보에도 해당된다. 하지만 두 가지 위치정보는 규범

67) 통신비밀보호법 전부개정법률안(의안번호 2001357, 전해철의원 대표발의, 2015.8.2.). 이 개정안은 또한 전기통신사업법의 통신자료를 통신비밀보호법의 통신사실확인자료와 동일하게 보호하고 있다는 점에서 비판이 가능하다. 개정안은 통신사실확인자료를 '과거의 통신사실확인자료'임을 명확히 하면서(안 제2조 제11호) 전기통신사업법의 통신자료를 '가입자 정보'로 변경하여 '과거의 통신사실확인자료' 와 '가입자 정보'를 합하여 '통신자료'라는 상위개념으로 포섭하고 있다(안 제2조 제14호). 하지만 현행 전기통신법의 통신자료는 실제 통신의 비밀과는 관련이 없는 가입자 정보를 말한다. 헌법상 통신의 비밀 보호 영역은 통신의 내용과 통신의 내역, 즉 통신사실에 관한 자료를 포함한다. 통신자료와 통신내용 및 통신 사실에 관한 자료는 엄격하게 구별되어야 한다. 통신자료는 개인정보자기결정권이 관련되고 통신내용 및 통신 사실에 관한 자료는 통신의 비밀보호와 개인정보자기결정권이 중첩된다. 통신의 비밀보호와 개인정보자기결정권이 중첩되는 경우 통신의 비밀보호가 우선된다. 이 조항은 그 동안 통신자료가 수사기관에 의해서 무분별하게 수집되고 있어서 정보주체의 개인정보자기결정권이 침해되고 있다는 점을 지적한 현실을 고려한 것으로 보인다. 하지만 보호의 필요성은 충분히 인정되지만 통신의 비밀을 보호하는 통비법에 포함시키는 것은 이 법률의 목적이나 체계에 맞지 않다. 오히려 전기통신사업법에 규정하거나 수사절차에서의 개인정보 내지 통신과 관련된 정보의 수집 및 이용이란 관점에서 형사소송법에 체계적으로 도입하는 것이 더 적합하다. 비교법으로 독일 형사소송법은 이를 명확하게 구별하고 있다. 우리의 통신자료에 해당되는 사항은 형사소송법 제100j조에서 규정하고 있고 이것은 헌법재판소의 판결에 따른 것이다.

적으로 구별되어야 한다.[68] 전자는 통신의 비밀과 관계되는 것이고 후자는 이와 상관이 없이 단지 위치기반서비스로서 제공된다. 따라서 법적 성격이 다르므로 이들은 달리 취급되어야 한다.

휴대전화로 실제 통화가 이루어진 경우에는 통확자료에 해당된다. 통비법이 규정하고 있는 전기통신을 하기 위해서 기지국과 항상 교신을 하고 있는 이용대기상태에 있는 휴대전화의 경우도 장래 또는 실시간 위치정보를 확보할 수 있으므로 통확자료에 해당될 수 있다.[69][70] 하지만 순전히 위치기반서비스에 제공되는 위치정보, 예를 들어 GPS를 통해서 제공되는 휴대전화의 위치정보는 통확자료가 아니다. 따라서 이러한 위치정보를 구별하지 않고 통확자료에 포함시키는 것은 통확자료의 대상을 통신의 비밀이 아닌 영역으로 확대시키는 것이어서 통비법의 성격이나 체계에 맞지 않다. 비교법적으로 독일 형소법은 이러한 상황을 이미 규범적으로 구분하고 있다. 예를 들어 가상 기지국을 이용한 휴대전화의 위치 확보에 관한 제100i조나 GPS 위치추적이나 IP 추적과 같이 관찰 목적으로 기술적 장치를 이용하게 하는 제100h조[71] 등이다. 따라서 휴대전화의 위치정보가 통확자료임을 명확히 하기 위해서는 현행 규정처럼 통확자료에 포함시켜야 하고 위치정보의 민감성 때문에 항을 달리하여 규정하는 것이 조문의 체계에도 적합하다.[72] 이용대기상태에 있는 위치정보는 실시간 위치추적을 가능하게 하므로 이동프로파일이 작성될 수 있기 때문에 수집 요건을 더욱 엄격하게 하여 개정안처럼 별도의 조항을 두는 것도 고려해 볼 수 있다.

---

68) 이원상, 형사사법에 있어 개인위치정보에 대한 고찰, 형사정책연구 제23권 제2호(통권 제90호, 2012·여름), 125.

69) 이용대기상태의 위치정보가 진정한 통신사실확인자료에 해당되는지는 검토가 더 필요하다.

70) 실시간 위치추적과 전통적인 의미의 통신사실확인자료는 구별하여 '실시간 위치정보'에 대한 정의 규정을 신설하고 별도의 수집절차를 규정해야 한다는 견해로는 권양섭, 범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안, 법학연구, 한국법학회, 411. 하지만 이를 분리해야 될 특별한 이유는 없는 것으로 보인다. 앞서 검토한 독일의 입법례가 이를 보여주고 있기 때문이다.

71) 민영성·박희영, 앞의 논문, 형사정책연구 제28권 제2호(통권 제110호, 2017·여름), 265.

72) 사이버범죄협약 제20조의 이행과 관련한 법률안의 제안으로는 박희영·최호진·최성진, 대검찰청 연구용역 결과보고서, 2015, 258-266.

Ⅶ. 결론

헌법상 기본권으로 보호되는 통신의 비밀은 통신의 내용 뿐 아니라 통신사실에 관한 자료도 포함된다. 휴대전화의 위치정보와 같은 통확자료는 이동프로파일이 작성될 수 있기 때문에 상당히 민감한 개인정보이다. 특히 이러한 위치정보가 실시간으로 수집되는 경우 기본권 침해의 강도는 다른 통확자료와 비교하여 월등하게 높다. 따라서 수사기관이 이에 접근하기 위해서는 보다 엄격한 요건이 필요하다.

현재 통비법 규정의 해석으로는 휴대전화의 실시간 추적은 허용되지 않는 것으로 판단된다. 또한 통확자료를 요청할 수 있는 요건이 너무 낮게 설정되어 있는 것으로 보인다. 따라서 해당 규정의 개정이 필요하다. 개정될 경우에는 통확자료의 제공요청에 관한 규정 외에 통비법의 다양한 문제점들[73]이 동시에 개정되어야 한다. 현재의 통비법 조항들은 아날로그 통신환경에 머물러 있기 때문이다. 비교법적 검토를 통해서 개정 시 고려되어야 할 것으로는 대상범죄의 특정, 정보통신 기술의 발전에 따른 통확자료의 확대, 최대 보관 기간의 제한, 통신기지국 수사의 허용여부, 통확자료 요청의 공개 처분으로의 전환 및 당사자에 대한 사전 통지와 사후 권리보호, 통확자료의 보관과 관련한 보안의 문제, 통확자료 표시의무 등이 지적될 수 있다. 이러한 문제들은 이미 입법의 단계를 지나 이미 시행하고 있는 외국의 사례를 비교법적으로 수용할 필요가 있다. 그런 면에서 독일의 입법 경험은 우리에게 시사하는 바가 크다.

끝으로 통확자료에 관한 규정은 유럽평의회의 사이버범죄협약의 가입을 염두에 두고 개정되어야 한다. 사이버범죄협약 제20조는 통확자료의 실시간 수집을 규정하고 있기 때문이다. 유럽평의회 회원국은 물론 비회원국인 미국, 일본, 호주, 캐나다 등 대부분의 선진국가들은 이미 가입하여 사이버범죄에 대한 국제공조에 기여하고

---

73) 박찬걸, “통신사실확인자료 제공제도의 현황 및 개선방안”, 형사법의 신동향(제44호), 대검찰청(2014); 권양섭, “범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안”, 법학연구(제59집), 한국법학회(2015); 김봉수, “위치정보의 보호를 위한 형법적 고찰 - 범죄수사를 위한 위치정보의 수집 및 활용에 대한 통제방안를 중심으로-”, 법학논총(제32집 제3호), 전남대학교 법학연구소(2012); 오길영, “현행 통신비밀보호법의 문제점과 개선방향”, 언론과 법(제14권 제1호), 한국언론법학회(2015).

있다. 국제사회의 일원으로서 IT 선진국임을 자부하는 한국의 조속한 가입이 요구된다.[74)]

74) 사이버범죄협약의 이행에 따른 국내 관련 법규의 개정 방안에 대해서는 박희영·최호진·최성진, 대검찰청 연구용역 결과보고서, 2015 참조.

참고문헌

권양섭, 범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안, 법학연구(제59집), 한국법학회(2015).

김봉수, 위치정보의 보호를 위한 형법적 고찰 - 범죄수사를 위한 위치정보의 수집 및 활용에 대한 통제방안를 중심으로 -, 법학논총(제32집 제3호), 전남대학교 법학연구소(2012).

김용환, 통비법 중 개정법률안에 대한 의견제시의 건 검토보고서, 과학기술정보통신위원회 수석전문위원, 2001. 2, 6면.

민영성·박희영, 유럽사법재판소의 통신정보보관지침의 무효 판결과 그 시사점, 법학연구 제56권 제4호, 부산대학교 법학연구소, 2015, 53-82.

민영성·박희영, EU 통신정보보관제도의 정당성 - 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서 - 법학논문집 제40집 제1호(Vol. 40, No. 1), 2016, 중앙대학교, 449-473.

민영성·박희영, 독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점, 부산대학교, 법학연구 제57권 제2호, 통권 88호, 2016.5, 89-109.

민영성·박희영, 독일에서 위치추적 수사방법으로서 IP트래킹의 허용근거에 대한 논의와 그 시사점, 형사정책연구 제28권 제2호(통권 제110호, 2017·여름), 265.

박찬걸, 통신사실확인자료 제공제도의 현황 및 개선방안, 형사법의 신동향(제44호), 대검찰청(2014).

박희영, 독일 형사소송법상 통신데이터 수집권과 한국 통신비밀보호법상 통신사실확인자료제공 요청권의 비교 및 시사점, 경찰학연구 제9권 제3호 통권 21호, 2009.12 33-61.

박희영, 무선기지국 수사를 위한 법원의 명령 요건, AG Dortmund Beschl. v. 6.1.2016 – 701 Gs 18/16, 최신독일판례연구, 로앤비 2017.10.

박희영, 유동 IP주소는 일주일간 저장될 수 있다, BGH Urteil vom 3.7.2014, III ZR 391/13, 최신독일판례연구, 로앤비(www.lawnb.com), 2014.09, 1-9.

박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC,

인터넷법률, 법무부, 통권 제43호(2008. 7), 144－175.

박희영, 이유 없이 통신사실확인자료를 보관하는 것은 EU법에 위반된다, OVG Münster, Beschluss v. 22.06.2017, 13 B 238/17, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.7, 1-5.

박희영, 일반적인 통신정보 보관의무는 EU법과 일치하지 않는다, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.2, 1-5.

박희영, 제2차 통신정보보관법률에 대한 가처분 명령 신청 기각, BVerfG, Beschluss vom 08. Juli 2016 - 1 BvR 229/16, 최신독일판례연구, 로앤비(www.lawnb.com), 2016.10, 1-8.

박희영·홍성기, 휴대전화 위치파악과 통신의 비밀, 독일연방헌법재판소 판례연구 Ⅰ, 정보기본권, 165-193, 한국학술정보(2010).

박희영·최호진·최성진, 사이버범죄협약 이행입법연구, 대검찰청, 연구용역 결과보고서, 2015(다운로드 : http://www.prism.go.kr/).

박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC, 인터넷법률, 법무부, 통권 제43호(2008. 7).

박희영, 경찰의 범죄 예방 및 수사 목적의 휴대전화 위치정보 파악의 허용과 그 한계, 경찰청 치안정책연구소, 책임연구보고서(2011).

오길영, 현행 통신비밀보호법의 문제점과 개선방향, 언론과 법(제14권 제1호), 한국언론법학회(2015).

이원상, 형사사법에 있어 개인위치정보에 대한 고찰, 형사정책연구 제23권 제2호(통권 제90호, 2012·여름), 125.

정애령, 독일 통신데이터저장제도(Vorratsdatenspeicherung)의 비판적 고찰, - 유럽연합지침과 독일의 통신데이터저장제도 재도입 법률을 중심으로 -, 공법연구 제45집 제3호, 한국공법학회, 2017.2, 126.

조기영, 최근 주요 쟁점과 관련한 통비법 개정방향, - 휴대전화 감청, 패킷감청, 기지국수사, GPS위치정보 추적을 중심으로 -, 132.

차진아, 통신비밀보호법 제13조 제1항 및 제2항 등의 합헌성 여부에 대한 검토 - 헌재 2012헌마191등 헌법소원심판청구 사건에 대한 검토를 중심으로 -, 법

조 2017.8(Vol.724), 247-255.

Bär, Wolfgang, Auskunftsanspruch über Telekommunikationsdaten nach den neuen §§ 100g, 100h StPO, MMR 2002, 358-264.

Bär, Wolfgang, BeckOK StPO/Bär, 28. Ed. 22.7.2017, StPO § 100g.

Bär, Wolfgang, Anmerkung zu BGH (BGH-Ermittlungsrichter), Beschluss vom 21.2.2001 - 2 BGs 42/2001, MMR 2001, 442.

Bernsmann, Klaus/Jansen, Kirstin, Anmerkung zu LG Aachen, StV 1999, 590.

Demko, Daniela, Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme, NStZ 2004 Heft 2, 57-64.

Füllkrug Kriminalistik 1990, 349, 350.

Gercke, Björn, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, 2002, Duncker & Humblot.

Kleinknecht/Meyer-Goßner, StPO, 45. Aufl. 2001, § 100a Rdnr. 3;

Lampe, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 12 FAG Rdnr. 12.

Franz, Palm/Rudolf, Roy, Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, Heft 28, 1719-1797.

Klesczewski, Diethelm, Das Auskunftsersuchen an die Post: die wohlfeile Dauerkontrolle von Fernmeldeanschlüssen, StV 1993, 382.

Ruhmannseder, Felix, Strafprozessuale Zulässigkeit von Standortermittlungen im Mobilfunkverkehr, JA 2007, Heft 11, 47-55.

Welp, Jürgen, Verbindungsdaten zur Reform des Auskunftsrechts (§§100g, 100h StPO, GA 2002, 535 (539).

Welp, Jürgen, Strafprozessuale Zugriffe auf Verbindungsdaten des Fernmeldeverkehrs, NStZ 1994, 209-215.

Wohlers, Wolfgang/Demko, Daniela, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241.

Wollweber, Harald, Verbindungsdaten der Telekommunikation im Visier der Strafverfolgungsbehörden, NJW 2002, 1554.

Regarding the permission of the real-time tracking of mobile phone location information of the Protection of Communications Secrets Act and its legislative proposal : Compared to Germany's traffic data collection*

Min, Young-sung**·Park, Hee-young***

It is a question whether real-time tracking of mobile phone location information can be allowed under Article 13 of the Protection of Communications Secrets Act(Act No. 14071, Mar. 3, 2016)(PCSA). Criminal practice is considered to be possible. The Constitutional Court is dealing with this issue.

In order to solve this problem, this paper attempted a comparative study with German law. In the case of Germany, past, future and real-time location information was allowed by revising the relevant provisions several times. In particular, the current Criminal Procedure Act requires more stringent requirements for the collection of real - time location information. Through this series of legislative processes, it can be seen that allowing the collection of location information does not necessarily mean real-time collection of location information.

Article 13 has been prescribed since the enactment in 2001. With the revision in 2005, the location information of the mobile phone could be collected by adding the location tracking data of communication base station. However, the substantive requirements of Article 13 have not changed. The collection requirements and procedures of Article 13 remain in the legal situation in the early days of Germany.

* This work was supported by the National Research Foundation of Korea Grant funded by the korean Government (NRF-2014S1A5A2A01012247).

** Professor, School of Law, Pusan National University, PhD in Law.

*** Researcher, Max Planck Institute for Foreign and International Criminal Law, Germany, PhD in Law.

This implies that the Constitutional problems raised at that time are still present.

Interpretation of this regulation does not seem to allow real-time tracking of mobile phones. This is because Article 13 of PCSA excludes §6 Abs. 7. This provision limits the duration of the communication surveillance to three months or less. Therefore, real-time tracking of location information currently being used in criminal practice should be prohibited because it is based on misinterpretation.

Therefore, new regulations are needed to collect real-time location information. Real-time collection of location information is an individual sensitive personal information, so higher requirements are needed. In the case of amendment of the provisions, it is necessary to consider the accession of the Council of Europe's he Convention on Cybercrime. Article 20 of the Convention on Cybercrime stipulates the real-time collection of traffic data.

❖ Keyword: 2006/24/EC, Data Retention(Vorratsdatenspeicherung), traffic data (Verkehsdaten, Communication Confirmation Data), location information(Standortdaten), cell site investigation(Funkzellenabfrage), Protection of Communications Secrets, information self-determination

투고일 : 11월 30일 / 심사일 : 12월 15일 / 게재확정일 : 12월 15일