형사정책연구 Korean Criminological Review
제28권 제2호(통권 제110호, 2017・여름)

독일에서 위치추적 수사방법으로서 IP트래킹의 허용근거에 대한 논의와 그 시사점*

민영성**・박희영***

국 | 문 | 요 | 약

사이버테러와 같은 중대한 범죄가 발생한 경우 범죄혐의를 받고 있는 인터넷 이용자의 신원을 확보하는 것이 무엇보다 중요하다. 이러한 범죄혐의자의 신원을 확인하기 위하여 IP주소를 확보하는 수사방법 중 하나가 소위 'IP트래킹'이다. 이 논문에서는 현재의 법적 상황에서 IP트래킹이 허용되는지 그리고 그 근거규정이 무엇인지를 검토하고 입법방향을 제시하고자 한다.

국내에서는 아직 IP트래킹 수사기법과 이의 근거 규정을 다룬 판례나 문헌이 발견되지 않는다. 따라서 이에 관한 논의를 선행시킨 독일의 판례와 문헌을 비교법적으로 검토한다. 독일의 경우에도 IP트래킹에 직접 적용되는 법률 규정은 아직 존재하지 않지만 최근 연방대법원 수사판사가 형사소송법 관련 규정의 해석을 통하여 IP트래킹을 허용하는 결정을 최초로 내렸다. 하지만 이 결정에 대한 비판적 견해가 제시되면서 이에 관한 법적 논의가 본격적으로 시작되었다. 연방대법원 수사판사는 IP트래킹으로 IP주소가 수집되기 때문에 통신사실확인자료의 수집에 관한 형사소송법 제100g조에 의해서만 허용될 수 있다고 한 반면, 다수 견해는 특정한 기술적 장치를 통해서 대상자를 관찰하도록 한 형사소송법 제100h조 제1항 제2호가 적절한 규정이라고 한다. 기본권 침해의 정도를 고려하면 다수 견해가 타당하다고 본다.

현재 우리의 경우 독일과 같이 해석으로 적용할 수 있는 규정이 존재하지 않는다. IP주소 기반의 인터넷 통신이 4차 산업혁명의 시대에도 더욱 증가할 것이 예상되므로 IP트래킹에 대한 입법이 요구된다. IP트래킹은 상대방에게 비밀리에 수행되기 때문에 정보자기결정권이 침해되지만 기본권 침해의 정도는 그리 중대하지는 않다. 따라서 이를 정당화하는 규정은 법원의 허가와 사후통지를 요건으로 하는 통신사실확인자료 제공요청(통신비밀보호법 제13조)과 법원의 허가나 사후통지조차 없는 통신자료 제공요청(전기통신사업법 제83조) 사이에 두는 것이 적절해 보인다. 기본권 침해의 정도를 고려하면 법원의 허가는 필요하지 않지만 당사자에게 사후통지는 보장되어야 할 것으로 보인다.

❖ 주제어 : 아이피주소, 아이피트래킹, 통신사실확인자료, 통신자료, 통신비밀, 정보자기결정권, 기술적 장치

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

** 부산대학교 법학전문대학원 교수(주저자)

*** 독일 막스플랑크 국제형법연구소 연구원(공동저자)

Ⅰ. 문제 제기

사이버 테러와 같은 중대한 범죄가 발생한 경우 범죄혐의를 받고 있는 인터넷 이용자의 신원을 확보하는 것이 무엇보다 중요하다. 일반적으로 인터넷상에서 범죄혐의자의 신원을 확인하기 위해서는 우선 이메일 주소나 이용자가 이용한 인터넷 서비스의 계정(예를 들어 SNS나 메신저서비스 등의 ID)이 확보되어야 한다. 그런 다음 해당 서비스 제공자가 보관하고 있는 이용자(또는 가입자) 정보를 조회하여 이용자의 신원을 확인할 수 있다.

하지만 이용자가 이용하는 이메일 주소나 인터넷 서비스가 무료이거나 익명 가입이 가능하여 해당 인터넷 서비스 제공자가 이용자의 정보를 보관하고 있지 않는 경우 이용자의 정보를 조회할 수 없다. 또한 혐의를 받고 있는 인터넷 이용자가 진정한 IP주소를 숨기기 위해 프락시 서버를 제공하는 인터넷 서비스를 이용하는 경우 자신의 신분을 속일 수 있고 익명으로 범죄를 행할 가능성이 있다. 이러한 경우 이용자가 서비스 이용 시 부여받은 IP주소를 토대로 이용자의 신원을 확인할 수 있는 방법이 활용된다. 인터넷이 다양한 방식의 익명성을 가능하게 하더라도, 인터넷상 모든 통신은 IP주소를 흔적으로 남기기 때문이다. 따라서 이용된 IP주소가 범죄 혐의가 있는 인터넷 이용자의 신원을 확인함에 있어서 중요한 수사의 단초가 된다.

최근 통신기술의 발달에 따라 수사기관이 범죄혐의를 받고 있는 인터넷 이용자의 IP주소를 실시간으로 추적하여 직접 확보하는 수사방법으로 소위 'IP트래킹'(IP tracking)이라는 수사방법이 등장하여 이를 활용할 가능성이 높아지고 있다.

이 글은 IP트래킹이 현재의 법적 상황에서 허용되는지 그리고 그 근거규정은 무엇인지 검토하고 입법방향을 제시한다. 그런데 국내에서는 IP트래킹 수사기법과 이의 근거 규정을 다룬 판례나 문헌이 아직 발견되지 않기 때문에 이에 관한 논의를 선행시킨 독일의 판례와 문헌을 비교법적으로 먼저 검토한다. 독일의 경우에도 IP트래킹에 직접 적용되는 법률 규정이 존재하지 않아 견해가 대립되고 있으며, 최근 연방대법원의 수사판사가 형사소송법 관련 규정의 해석을 통하여 IP트래킹을 허용하는 결정을 내린바 있다.[1] 하지만 연방대법원이 IP트래킹에 적용한 해당 규정이

1) BGH Ermittlungsrichter Beschl. vom 23.9.2014 – 1 BGs 210/14.

과연 정당한 규정인지에 대하여 비판적 견해가 제시되고 있다. IP트래킹의 법적 문제를 처음으로 다룬 이 판례를 계기로 독일에서도 이에 관한 논의가 본격적으로 시작되고 있다. 이러한 독일의 논의를 비판적으로 살펴보고 우리의 관련 규정에 전용할 수 있는지 검토한다. 독일의 논의를 진행하기 이전에 IP트래킹 방법을 이해하기 위해서 우선 기술적인 부분을 간략하게 설명하기로 한다.

Ⅱ. IP트래킹의 기술적 이해

IP트래킹은 두 가지 유형으로 분류할 수 있다. 인터넷 서비스 제공자의 데이터베이스에 접근하여 조회를 통하는 방법과 수사기관이 통신을 통해서 대상자로부터 직접 IP주소를 확보하는 방법이 그것이다. 데이터베이스 조회를 통해서 IP주소를 확인하는 방법은 인터넷기반의 통신 서비스 및 메신저 서비스 이용자의 데이터베이스를 전제로 한다. 이러한 서비스를 이용하기 위해서는 이용자들은 서비스 제공자에게 미리 등록을 해야 한다. 이 경우 고객정보인 개인정보가 수집되고 특정된 이용자 계정도 등록된다. 또한 구체적인 서비스를 이용하기 위해서 이용자는 로그인해야 한다. 로그인 과정에서 이용자의 IP주소가 수집되고 로그인 해 있는 동안 이용자 계정과 등록되어 있는 정보가 연결된다. 이 과정에서 수집된 IP주소는 인터페이스 프로그램을 통해서 수사기관에게 조회되어 수집될 수 있다.

수사기관이 혐의자의 IP주소를 대상자로부터 직접 확보하는 IP트래킹은 소위 '수신확인서비스'(Read notify)를 이용하여 수행된다. 예를 들어 수사기관이 수신확인 기능을 포함한 이메일을 발송하거나 특정 파일을 다운로드하게 하는 방법이다. 수신 확인 서비스는 특히 수신자가 이메일을 읽었는지를 발신자에게 알려주는 서비스로 오래 전부터 개인이나 기업체에서 사용되고 있다.[2)]

수신확인서비스를 이용하여 혐의자의 IP주소를 확보하는 IP트래킹의 경우 수사기관은 인터넷서비스의 이용자로 등록한 다음 자신의 신분을 숨기고 혐의자와 통신을

2) Lellmann·Pohl, "IP-Tracking, Rechtliche Zulässigkeit und Fallkonstellationen", Kriminalistik 8-9/2015, S.498 ff.

하게 된다. 주로 이메일 서비스를 통해서 수신확인기능이 있는 파일을 메일에 첨부해서 보내는 방법을 사용한다. 하지만 P2P 서비스와 같이 파일을 다운로드 하는 서비스를 이용할 수도 있다.[3] 이용자가 수신확인기능이 첨부된 메일을 읽어보거나 파일을 다운로드하는 경우 수신확인기능이 작동하여 이용자의 실제 IP주소가 수사기관의 서버로 전송된다. 이러한 기능을 이용하면 모바일서비스제공자에게 있는 IP주소도 조회될 가능성이 이론적으로 존재한다.[4] 그런데 IP트래킹의 경우 당사자의 행위를 통해서만 비로소 수신확인서비스가 수행된다. 즉 당사자가 발송된 이메일이나 다운로드로 제공된 문서를 적극적으로 열람해야 한다는 것이다. 가령 이메일을 단순히 수령만 하거나 무시하거나 아예 삭제해 버리면 추적 과정은 더 이상 작동하지 않는다.

Ⅲ. 독일에서 IP트래킹의 허용근거에 대한 논의

IP트래킹과 관련하여 최근 연방대법원 수사판사의 결정을 계기로 이에 대한 논의가 시작되고 있다. IP트래킹에 적용될 가능성이 있는 규정들에 관한 견해들을 먼저 검토하고 연방대법원의 판례를 살펴본 다음 어느 규정이 타당한 지 제시한다.

1. 적용 가능한 형사소송법 규정에 관한 견해들

가. 통신자료의 제공에 관한 형사소송법 제100j조[5]

1) 규정 내용

우선 전기통신사업자에게 가입자 정보(Bestandsdaten)를 수사기관에 제공하도록

3) Bär, Kleinknecht/Müller/Reitberger, KMR-StPO, Carl Heymanns Verlag, 2016, §100g Rn. 32.

4) Bruns, KK-StPO, Beck online, 2013, § 100j Rn.4.

5) 독일 형사소송법 제100j조는 2013년 7월 1일부터 형사소송법에 도입되었다. 그런데 현재 독일의 통신자료의 제공에 관하여 소개하고 있는 대부분의 국내 문헌과 이를 재인용하고 있는 문헌들은 형사소송법 제100j조가 도입되기 훨씬 이전의 법적 상황을 소개하고 있다(예를 들어 이성기, "「통신사업자의 통신사실 확인자료 및 통신자료제공의 요건과 절차」에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본의 제도 비교를 중심으로", 법과 정책 제14집 제1호, 한국법정책학회, 2014.3, 52-53).

의무를 부과하고 있는 형사소송법 제100j조가 유추 적용될 수 있다는 견해가 있다.[6] 이 규정은 우리 전기통신사업법 제83조의 통신자료의 제공에 대응하는 규정이고 가입자 정보는 통신자료에 해당된다.

제100j조 제1항에 의하면 사실관계의 조사나 피의자의 소재지 파악을 위하여 필요한 경우 수사기관이 전기통신법(제95조 및 제111조)에 의해서 수집된 가입자 정보를 요청하면 전기통신사업자는 이를 제공해야 한다. 가입자 정보란 전기통신서비스에 관한 계약 관계의 성립, 내용, 변경 또는 종료를 위해서 수집되는 가입자에 관한 정보를 말한다(전기통신법 제3조 제3호). 전기통신사업자는 가입자 정보를 두 가지 방식으로 수집할 수 있다. 하나는 전기통신법 제95조에서 정한 방법인데, 이에 따르면 전기통신사업자는 통신서비스에 관한 계약 관계의 성립, 내용, 변경 또는 종료를 위해서 필요한 경우 가입자 정보를 수집하여 이용할 수 있다. 이 경우 수집 및 이용되는 가입자 정보에는 제한이 없다. 다른 하나는 전기통신법 제111조에서 정한 방법이다. 이에 따르면 전기통신사업자는 6가지 가입자 정보[7]를 수집하여 저장해야 한다. 제95조의 경우 수집 및 이용되는 가입자 정보에 제한이 없으나 제111조의 경우 수집되어 저장되어야 할 가입자 정보는 6가지로 제한되어 있다. 수사기관 및 정보기관 등은 제111조에 의해서 수집되어 전기통신사업자의 데이터베이스에 저장되어 있는 가입자 정보에 법관의 영장 없이 자동적으로 접근하여 이를 확보할 수 있다(전기통신법 제112조). 데이터베이스에 저장되어 있지 않은 다른 가입자 정보는 전기통신사업자에게 직접 요청하여 수집할 수 있다(전기통신법 제113조).[8] 가입자 정보의 제공에 대해서 당사자에게 사후 통지하는 규정은 없으며, 전기통신사업자가 제공에 따르지 않을 경우 제재 규정이 존재한다(형사소송법 제100j조 제5항).

---

6) Lellmann·Pohl, a.a.O., 503.

7) 전기통신법 제111조 : 1. 전화번호 및 다른 회선표지, 2. 회선보유자의 성명 및 주소, 3. 자연인의 경우 생년월일, 4. 유선의 경우 회선이 설치된 곳의 주소, 5. 모바일 회선과 함께 모바일 기기도 양도되는 경우 이 기기의 번호(IMEI), 6. 계약개시일자.

8) 형사소송법 제100j조와 전기통신법 제95조, 제111조, 제112조, 제113조의 구체적인 내용에 대해서는 박희영 외 공저, 「사이버범죄협약 이행입법 연구」, 2015년 연구용역 결과보고서, 대검찰청, 2015.12, 169-172 참조.

2) 검토

형사소송법 제100j조는 IP트래킹에 직접 적용하거나 유추 적용하기 어려운 것으로 보인다. IP트래킹은 가입자 정보의 조회에 선행하는 수사처분이기 때문이다. 즉 제100j조는 타임스탬프가 포함되어 있는 IP주소의 인식을 전제로 함에 반하여, IP트래킹은 그 이전에 IP주소의 수집을 목적으로 한다. 따라서 IP트래킹은 목적의 방향과 법적 효과에 있어서 차이가 있기 때문에 비교가능성이 결여되어 유추 적용도 금지된다고 생각된다.

나. 통신사실확인자료의 수집에 관한 형사소송법 제100g조

1) 규정 내용

IP트래킹에 적용될 수 있는 두 번째의 규정으로 통신사실확인자료(Verkehrsdaten, traffic data)의 수집을 허용하고 있는 형사소송법 제100g조가 제시되고 있다.[9] 이 규정은 우리 통신비밀보호법 제13조와 동일한 기능과 역할을 한다.[10]

우선 통신사실확인자료란 전기통신서비스를 제공함에 있어서 수집, 처리 또는 이용되는 데이터를 말한다(전기통신법 제3조 제30). 통신사실확인자료는 개인정보보호법상 민감한 개인정보에 해당되며 전기통신서비스의 사용과 관련하여 누가 언제 어떤 회선에 의해서 얼마 동안 통신을 하였는지를 알려 준다. 따라서 통신사실확인자료는 통신했다는 사실을 전제로 하기 때문에 기본법 제10조 제1항의 통신비밀의 보호대상이 된다.

형사소송법 제100g조는 수사목적으로 수집되는 통신사실확인자료를 두 가지 경우로 나누고 있다. 즉 전기통신사업자의 영업활동과 관련하여 전기통신법 제96조에

9) BGH Ermittlungsrichter Beschl. vom 23.9.2014 – 1 BGs 210/14; Graf, BeckOK, StPO §100g, Beck online, 2017, Rn.12a.

10) 독일 형사소송법 제100g조는 2010년 3월 2일 헌법재판소로부터 위헌판결을 받아 개정되어 2015년 12월 18일부터 발효되었다. 위헌판결 이전의 규정과 현재의 규정에는 많은 차이가 있다. 이 규정을 소개하고 있는 각 주 5)에서 언급한 국내 문헌은 위헌 판결 이전의 법적 상황을 다루고 있다. 개정된 형사소송법 제100g조에 대한 자세한 내용은 민영성·박희영, "독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점", 법학연구 제57권 제2호(통권 제88호), 부산대학교 법학연구소, 2016.5, 89-109 참조; 박희영 외 공저, 159-167 참조.

따라 수집되거나 수사기관의 정보제공요청과 관련한 제113b조에 따라 수집되는 경우가 그것이다.

형사소송법 제100g조 제1항은 전기통신법 제96조에 의한 통신사실확인자료의 수집을 규정하고 있다. 전기통신사업자는 통신비밀, 개인정보보호, 공공의 안전 등 전기통신법이 정한 목적을 위해서 필요한 경우에 제96조에 따라 5가지의 통신사실확인자료를 수집할 수 있다.[11] IP주소는 제96조 제1항 제1호의 '가입한 회선 및 단말기의 번호 및 표지'에 해당된다.[12] 즉 인터넷 통신에 있어서 고정 IP주소는 가입자 회선의 번호에, 유동 IP주소는 가입자 회선의 표지에 해당된다. 인터넷 전화(VoIP)의 경우에도 유동 IP주소는 통신사실확인자료에 해당된다.

형사소송법 제100g조 제1항에 따르면 전기통신법 제96조의 통신사실확인자료가 수집되기 위한 요건은 다음과 같다. 우선 특정한 사실을 근거로 범죄혐의가 존재해야 하고 대상 범죄는 '중요한 의미를 가지는 범죄'[13]와 전기통신을 수단으로 행한 범죄여야 한다. 비례성원칙과 관련하여 통신사실확인자료가 수집되기 위해서는 사실관계를 조사하기 위해서 필요하고 데이터의 수집이 사건의 의미와 적정한 관계에 있어야 한다. 전기통신을 수단으로 행한 범죄의 경우에는 사실관계의 조사가 다른 방법으로는 예견될 수 없는 경우에만 허용된다. 또한 모바일 기기의 위치정보는, 사실관계의 조사나 피의자의 소재지를 파악하기 위해서 필요한 경우, 개별적으로 중요한 의미를 가지는 범죄에 한해서 현재의 정보로서 실시간으로 수집되거나 미래의 정보로서 수집될 수 있다.

---

11) 독일 전기통신법 제96조 제1항 : 1. 가입한 회선 및 단말기의 번호 및 표지, 고객카드와 카드번호의 이용의 경우 개인관련 권리표지, 모바일 접속의 경우 위치정보, 2. 개별 접속의 시작 및 종료의 날짜와 시간, 유료요금제의 경우 전달된 데이터의 량, 3. 이용자가 이용한 전기통신서비스, 4. 비교환 회선의 경우 목적지, 이의 시작과 종료의 날짜 및 시간, 유료인 경우 전달된 데이터의 량, 5. 전기통신의 구축 및 유지 그리고 요금산정을 위해서 필요한 그 밖의 통신정보.

12) Bär, a.a.O., §100g Rn.11.

13) 독일 형사소송법은 강제조치를 할 수 있는 범죄를 3가지 단계로 나누고 있다. 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'(대표적인 예로서 통신사실확인자료의 수집에 관한 형사소송법 제100g조이다. 중간정도의 범죄란 4년 이하의 자유형 선고가 예상될 수 있는 범죄를 말한다.

전기통신법 제96조에 의해서 수집된 통신사실확인자료는 그 목적이 달성된 경우 또는 이러한 목적과 상관이 없는 통신사실확인자료는 이용자의 통신이 종료된 후 지체 없이 삭제되어야 한다. 하지만 통신사실확인자료가 삭제되면 범죄자의 통신사실을 확인할 방법이 없으므로 전기통신법 제113b조는 특정한 통신사실확인자료를 일정한 기간 동안 보관하도록 전기통신사업자에게 의무를 부과하고 있다. 즉 전기통신법 제113b조는 공중 전화서비스 제공자(제2항)와 공중 인터넷 접속 서비스 제공자(제3항)가 관리하는 데이터는 10주간, 위치데이터(제4항)는 4주간 저장하도록 의무를 부과하고 있다. 제113b조 제3항은 인터넷접속제공자에게 인터넷접속을 위해서 가입자에게 부여되는 IP주소, 인터넷이용으로 생성되는 회선의 명확한 표지 및 할당된 이용자 표지, 표준시간대의 정보가 포함되어 있는 할당된 IP주소로 인터넷 이용 시작과 종료 날짜 및 시간을 10주간 저장하도록 하고 있다.

형사소송법 제100g조 제2항은 전기통신법 제113b조에 의해서 저장되어 보관되고 있는 통신사실확인자료를 수집하기 위한 요건을 정하고 있다. 특별한 중범죄를 범했거나 그 행위가 개별적으로도 특별히 중대한 경우, 사실관계의 조사나 피의자의 소재지 확보가 다른 방법에 의해서는 본질적으로 어렵거나 예견할 수 없고 데이터 수집이 사건의 의미와 적합한 관계에 있는 경우에 수집될 수 있다.

형사소송법 제100g조에 의한 통신사실확인자료의 요청 절차를 살펴보면 우선 검사의 요청에 따라 법원이 이 조치를 결정한다. 긴급한 경우 검사가 명령을 내릴 수 있지만 3일 이내에 법원의 허가를 받아야 하며 그렇지 않으면 자동으로 그 명령은 효력을 잃게 된다. 통신사실확인자료가 요청되었다는 사실은 당사자에게 통지되어야 하지만 일정한 경우 통지가 제한될 수 있다(제101a조 제6항). 또한 주 검찰 및 연방 검찰은 이러한 조치를 연방법무부에 매년 보고해야 하며 연방법무부는 이를 인터넷에 공개해야 한다(형사소송법 제101b조).

2) 검토

IP트래킹과 관련해서 당사자로부터 수집되는 IP주소는 전기통신법에 규정된 통신사실확인자료에 해당된다. 형사소송법 제100g조는 통신사실확인자료를 형사절차에서 수집하기 위한 일반적인 규정으로서 IP트래킹에 관한 통신사실확인자료의 수

사에도 관련되는 법적 근거에 해당된다. 이후에 살펴볼 연방대법원의 판례도 해당 사안에서 IP주소와 같은 통신사실확인자료를 수집하기 위해서는 항상 형사소송법 제100g조의 요건이 존재해야 한다는 점을 명확히 하고 있다.[14] 하지만 IP트래킹의 경우에도 그 요건이 엄격한 형사소송법 제100g조가 적용되어야 하는지는 의문이다. 이에 대해서는 이 글 Ⅳ.에서 상세하게 다룬다.

다. 관찰 목적으로의 기술적 장치의 사용에 관한 형사소송법 제100h조 제1항 제2호

1) 규정 내용

형사소송법 제100h조는 주거 외부에서 행하는 수사조치로서 대상자를 사진으로 촬영하거나 다른 방식으로 관찰할 목적으로 특정된 기술적 장치를 사용하는 것을 규정하고 있다. 관찰 목적을 위한 특정된 기술적 장치는 대상자를 녹화하거나 녹음하는 것은 아니지만 관찰을 가능하게 하고 구체적인 수사절차에서 사용되는 것을 말하며 그 예로서 GPS 추적기를 들 수 있다.

이 조치는 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 성공할 가망이 훨씬 적거나 어려울 수 있는 경우에 수행될 수 있다. 하지만 관찰 목적을 위한 기술적 장치를 사용하기 위해서는 조사의 대상이 '중대한 의미를 가지는 범죄'여야 한다.[15] 즉 경미한 범죄(2년 이하의 자유형이 예상되는 범죄)에 대해서는 이러한 조치를 행할 수 없다.

제100h조의 기술적 장치의 사용에는 법관의 영장이 필요 없고 검찰이나 검찰 소속의 수사관이 직접 행한다. 범죄 혐의의 정도는 초기혐의로도 충분하다. 그리고 당사자에게 통지되어야 한다(형사소송법 제101조 제4항 제6호).

---

14) BGH Ermittlungsrichter, Beschluss vom 23.9.2014 – 1 BGs 210/14, juris; Graf, 앞의 책, §100a, Rn.133a.

15) BVerfG Urteil vom 12. 3. 2003 - 1 BvR 330/96 u. 1 BvR 348/99, NStZ 2003, 441; BVerfG Urteil vom 3. März 2004 - 1 BvR 2378/98; 1 BvR 1084/99, NStZ 2004, 270; BVerfG, Urteil vom 12. 4. 2005 - 2 BvR 581/01, NJW 2005, S.1338.

2) 검토

입법이유에서 기술적 장치의 사례로 제시한 것은 GPS 추적기(GPS Peilsender)이다.[16] 이것은 관찰 대상자의 자동차에 GPS 추적기를 몰래 설치하여 관찰 대상자와 자동차의 위치를 파악하는 강제수사방법의 하나이다. 기술적 장치는 개방적 개념으로 새롭게 등장한 IP트래킹을 포섭시킬 가능성이 있는 것으로 보인다.

GPS 추적기와 IP트래킹을 비교해 보면, GPS 추적기는 조치의 비밀성의 관점에서 대상자의 기본권 침해가 상당히 높다. IP트래킹의 경우 수사기관의 수신 확인 기능이 첨부된 파일의 열람은 대상자의 자율적인 판단에 달려 있다. IP트래킹의 경우 추적 기능이 첨부된 문서는 수사기관을 통해서 공개로 전달되거나 이용에 제공된다. 따라서 일반적으로 타인의 이메일이나 문서의 개봉과 관련되는 위험에 대처하거나 기술적 장치를 통해서 프락시 서버나 그 밖의 익명서비스를 이용하여 IP트래킹을 보호하는 것은 어디까지나 대상자에게 달려 있다. 하지만 GPS추적기의 경우 완전히 비밀리에 자동차에 설치되기 때문에 대상자는 이에 대한 대응조치를 전혀 할 수 없다.

데이터 수집의 관점에서도 GPS 추적기를 대상자의 차량에 부착하는 것은 기본권 침해의 강도가 높은 처분일 수 있다. GPS 추적은 특정 지점의 위치데이터 뿐 아니라 이동프로파일도 작성할 수 있으나 IP트래킹은 대부분 일회적이거나 적어도 짧은 기간의 데이터 수집을 대상으로 한다. 그럼에도 불구하고 제100h조에 의한 조치는 법관의 영장이 필요하지 않다. 하지만 당사자에 대한 통지의무가 보장되어 있다.

따라서 IP트래킹 보다 기본권 침해의 정도가 더 높은 GPS 추적기의 비밀 설치에도 법관의 영장이 필요하지 않고 당사자에게 사후 통지제도를 두고 있다는 점에서 이 규정은 IP트래킹에도 적용될 수 있을 것으로 보인다.[17] IP트래킹을 통하여 대상자의 위치를 파악하는 것은 이러한 기술적 장치를 이용하는 것에 준하기 때문이다.

16) BT-Drs. 12/989, S. 39.

17) Lellmann·Pohl, a.a.O., 504; Bär, a.a.O., §100g, Rn.22; Krause, “IP-Tracking durch Ermittlungsbehörden”, NStZ 2016, 144; Steinmetz, “Erhebung von IP-Adressen mittels IP-Tracking”, wistra 10/2015, 395.

라. 수사의 일반적 권한에 관한 제161조 제1항 및 제163조 제1항

1) 규정 내용

검찰과 경찰은 일반적 수사권을 각자 가지고 있다(제160조 제1항, 제163조 제1항). 이러한 수사권에 기해서 수사기관은 수사의 목적을 달성하기 위해 모든 관청에 필요한 정보를 요청할 수 있고 모든 종류의 수사를 개시할 수 있다.

2) 검토

수사기관의 일반적 수사권 규정이 IP트래킹에도 적용될 수 있다는 견해가 있다.[18] 이 견해는 그 근거로서 수신 확인 기능이 있는 파일을 발신자에게 다시 전송하는 것은 오늘 날 정상적인 인터넷이용이며 이러한 기능을 가진 파일을 첨부하는 것은 광고 이메일을 발송하는 경우의 마케팅 방법에 상응한다는 점을 제시하고 있다.

이 견해는 또한 수신확인서비스는 완전히 비밀리에 행해지지 않는다고 한다. 메시지의 헤드 부분에 있는 IP주소는 적어도 인식될 수 있다고 한다. 따라서 아무튼 진정한 비밀조치는 아니라는 것이다. 이용자가 스스로 이메일의 열람을 판단하고 발신인 또는 제3자에게 수집될 수 있는 데이터를 전송하는 것을 용인한다고 한다. 따라서 IP트래킹이 일회적인 조치로 행해지는 경우에는 수사기관의 일반적 수사권 규정이 적용될 수 있다고 하는 것이다.

하지만 IP트래킹의 경우 일회적 IP주소의 비공개 수사라는 관점에서 정보자기결정권의 침해가 경미하지는 않기 때문에,[19] 검찰이나 경찰의 일반적 수사권 조항은 적용될 수 없는 것으로 보인다.

마. 소결

현재 독일 형사소송법은 IP트래킹에 적용할 특별한 근거 규정이 없기 때문에 다양한 견해가 제시되고 있음을 살펴보았다. 그 결과 다수 견해는 관찰 목적으로 특별

18) Lellmann·Pohl, a.a.O., 50); Bär, a.a.O., §100g, Rn.22.

19) Krause, a.a.O., S.144.

한 기술적 장치를 사용하는 것을 허용하는 형사소송법 제100h조가 문언이나 체계면에서 무난한 근거 규정으로 보는 것 같다.[20] 다음에서는 형사실무에서 IP트래킹이 구체적으로 어떻게 활용되고 있는지 연방대법원의 수사판사가 다룬 사례를 통하여 살펴보고 연방대법원의 수사판사가 적용한 규정이 과연 타당한지 검토한다.

2. 연방대법원 판례

가. 사건 개요

다른 국가의 정보기관 소속의 성명불상의 요원들(이하 정보요원들)이 2012년 8월부터 독일의 관청이나 연구소 및 기업체를 대상으로 사이버 공격을 감행하였다. 특히 정보요원들은 연방범죄수사청의 컴퓨터 서버를 악성소프트웨어로 감염시켜 놓았다. 국제테러범죄를 전담하고 있는 독일 연방범죄수사청(BKA)은 정보요원들의 이러한 사이버테러 혐의를 포착하고 이들의 신원을 확인하기 위해 연방검찰을 통하여 IP트래킹 수사명령을 연방대법원 수사판사에게 청구하였다.[21]

정보요원들의 신원과 위치를 확인하기 위해서는 이들이 이용한 IP주소가 확인되어야 했다. 이를 위해서 연방검찰청은 명령청구서에서 정보요원들이 악성소프트웨어로 감염시킨 연방범죄수사청의 컴퓨터 서버에 수신확인서비스기능이 첨부된 오피스 문서 파일들을 저장하는 것을 요청했다. 이 파일들은 정보요원들에게 관심을 보여 다운로드 될 가능성이 있었다. 수신확인서비스기능이 첨부된 이 문서가 열람되는 경우 정보요원의 IP주소가 연방범죄수사청의 서버로 전달된다. 연방범죄수사청은 이러한 IP트래킹을 통해서 정보요원들의 IP주소와 접근 시점을 확보하려고 하였다.

연방대법원 수사판사는 연방검찰의 청구를 받아들여 정보요원들의 IP주소를 확보하기 위해서 이들이 다운로드할 수 있는 문서에 수신확인서비스기능을 가진 파일을 심어서 연방범죄수사청의 컴퓨터 서버에 저장하도록 명령하였다.

---

20) Krause, a.a.O., S.144; Steinmetz, a.a.O.,397.

21) 연방검찰은 연방대법원의 형사상고심에서 기소를 전담한다. 그 밖에 국제테러범죄를 전담하고 있는 연방범죄수사청의 요청으로 연방대법원에 영장 등을 청구할 수 있다. 이 때 연방대법원에서 영장업무를 전담하는 판사를 연방대법원 수사판사라고 한다.

나. 연방대법원 수사판사의 결정

연방대법원 수사판사는 IP트래킹에 직접 적용될 수 있는 형사소송법 규정이 없기 때문에, 적용 가능한 규정으로 제100j조, 제100g조, 제100h조를 검토하였다. 이들 중에서 수사판사는 IP트래킹의 경우 IP주소가 수집되기 때문에 통신사실확인자료의 수집을 규정한 제100g조가 적용되어 법관의 명령이 필요하다고 결정하였다.[22]

우선 수사판사는 가입자 정보의 제공에 관한 형사소송법 제100j조는 적용될 수 없다고 보았다. 가입자 정보를 요청하기 위해서는 IP주소와 이를 할당한 전기통신사업자를 알아야 하는데 IP트래킹의 경우 IP주소도 전기통신사업자도 알 수 없기 때문이다.[23]

또한 IP트래킹의 경우 관찰 목적으로 행하는 특정된 기술적 장치의 사용도 아니기 때문에 형사소송법 제100h조 제1항 제2호도 적용되지 않는다고 하였다.[24] 수사판사의 결정에 따르면 IP트래킹은 관찰 대상자에게 이 규정에 따라 특정한 기술적 장치를 사용할 수 있다는 점은 인정하였다. 하지만 연방검찰이 청구한 IP트래킹 방법은 비밀리에 통신사실확인자료를 수집하는 것이기 때문에 이러한 자료의 수집을 규정한 제100g조의 요건 하에서만 허용된다고 하였다.[25]

이 사안에서 IP트래킹의 경우 정보요원들이 다운로드한 수신확인기능이 첨부된 파일을 열람하는 경우 연방범죄수사청의 서버로 통신이 발생한다. 이 파일이 정보요원들의 IP주소와 타임스탬프를 연방범죄수사청의 서버로 전송하기 때문이다. 이러한 과정에서 유동 IP주소가 서비스제공자에 의해서 할당된다. IP주소는 개별 접속의 날짜, 시간, 기간과 함께 서비스제공자에게 수집될 뿐 아니라 수신확인기능이 작동하는 경우 연방범죄수사청의 서버에도 기록된다.

또한 수사기관의 IP트래킹 방법으로 통신사실확인자료를 수집하는 경우 기본법 제10조의 통신의 비밀은 침해되지 않는다고 한다.[26] 이 사안에서 수사기관이 직접 통신의 상대방으로 등장하고 있고 통신이 외부로부터 감시되지 않기 때문이다.[27]

---

22) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.7, juris.
23) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.8, juris.
24) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.9, juris.
25) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.10, juris.
26) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.11, juris.
27) BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822.

하지만 통신사실확인자료의 수집은 정보자기결정권의 침해와 관련된다고 한다. 독일 형사소송법 제100g조의 기본 사례에 의하면 통신사실확인자료의 수집으로 인한 기본권 침해의 정도는 정보자기결정권의 침해에 상응한다고 한다. IP트래킹은 정보요원들을 의도적으로 속이기 때문에 비밀성을 가지며 이 비밀성이 IP트래킹의 침해의 정도를 결정한다고 한다. 따라서 이용된 IP주소를 한 번 조사하는 경우뿐만 아니라 지금까지 알려지지 않은 사람의 신원이 확인되어 인터넷 접속에 이용된 IP 주소의 위치가 장기간에 걸쳐 확보될 수 있다고 한다. 그리하여 IP트래킹을 장기적으로 수행하면 행위자의 이동프로파일도 작성될 수 있다고 한다.[28)]

다. 소결

연방대법원 수사판사의 견해는 앞서 검토한 문헌의 다수 견해와는 달리 IP트래킹 수사조치의 명령을 형사소송법 제100g조를 근거 규정으로 보고 있다. 이러한 법원의 결정은 통신사실확인자료의 수집은 항상 제100g조의 요건 하에서만 가능하다는 것으로 이해될 수 있다.[29)] 그런데 제100j조가 적용될 수 없다는 법원의 결정은 상당한 의문이 제기된다. 아래에서는 연방대법원의 결정을 비판하는 입장에서 항을 바꾸어서 형사소송법의 어느 규정이 IP트래킹에 적절한지 검토한다.

Ⅳ. IP트래킹으로 침해되는 기본권과 적정한 근거 규정

1. IP트래킹으로 침해되는 기본권

가. 통신비밀의 보호

연방헌법재판소는 통신사실확인자료에 관한 판결[30)]에서 기본법 제10조의 전기통

28) BGH Ermittlungsrichter Beschluss vom 23. 09. 2014 – 1 BGs 210/14, Rn.13, juris.

29) Steinmetz, a.a.O., 396.

30) BVerfG Urteil vom 2.3.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, NJW 2010, 833, Rn. 189.

신비밀의 보호는 전기통신의 내용뿐만 아니라 전기통신의 상세한 상황, 즉 통신사실확인자료도 포함한다고 하였다. 또한 연방헌법재판소의 소위 'IT 기본권' 판결[31]에 따르면 전기통신의 비밀보호는 국가기관이 스스로 전기통신에 참여하거나 통신의 내용을 인지하기 위해 통신참가자의 위임을 받은 경우에도 침해되지 않는다고 하였다. 왜냐하면 전기통신비밀은 통신의 기술적 과정에 대한 권한 없는 제3자의 접근을 보호하는 것이지, 통신상대방에 대하여 개인적인 비밀을 지키지 아니한 데에 대한 실망을 보호하는 것이 아니기 때문이다.[32] 수사기관의 신분을 숨기면서 행하는 수사의 경우에도 일반적으로 통신비밀의 보호와 관련되지 않는다. 통신비밀의 보호는 국가기관이 스스로 전기통신참가자가 아니면서 전기통신의 과정을 외부에서 감시하는 경우에만 고려된다.

수신확인기능이 첨부된 이메일을 대상자에게 발송하거나 파일을 다운로드하도록 하는 IP트래킹의 경우에는 수사기관과 대상자 사이에 직접 통신이 발생한다. 이메일이 대상자에게 전송되어 도달하면 기본적으로 전기통신은 종료된다.[33] IP트래킹의 대상자가 해당 파일을 열어보는 경우 수신확인기능이 첨부된 파일이 자동으로 작동하여 대상자의 IP주소와 타임스탬프가 기술적으로 수사기관의 서버로 전달되어 통신이 이루어진다.[34]

연방대법원 수사판사가 다룬 사례에서도 수사기관과 대상자 사이에 직접 통신 관계가 존재하였다. 정보요원이 수신확인기능이 첨부된 파일을 다운로드하여 열람한 경우 연방범죄수사청의 서버와 통신이 진행된다. 이 파일은 대상자의 IP주소를 전달하기 때문이다.[35] 따라서 수사기관이 통신의 당사자로 참여하기 때문에 연방대법

31) BVerfG Urteil vom 27.2 2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822. 연방헌법재판소는 이 판결에서 온라인 수색과 관련하여 소위 IT 기본권을 창설하였다. 이 판결에 대한 소개로는 박희영, "독일 연방헌법재판소의 '정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권", 인터넷법률(현재 선진상사법률) 통권 제45호, 법무부, 2009.1, 92-123 참조; 온라인 수색에 관한 독일의 논의로는 이원상, 온라인 수색(Online-Durchsuchung)에 대한 고찰 – 독일의 새로운 논의를 중심으로-, 형사법연구 제20권 제4호, 2008; 전현옥·윤지영, 디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구, 형사정책연구원, 2012.10 참조.

32) BVerfG Urteil vom 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822, Rn. 290.

33) BVerfG Urteil vom 2.3.2006 – 2 BvR 2099/04, NStZ 2006, 641, Rn. 4.

34) Bär, a.a.O., § 100g Rn. 32.

35) Krause, a.a.O., S.141.

원의 결정과 같이 IP트래킹의 경우 통신의 비밀은 침해되지 않는다.

나. 정보자기결정권

정보자기결정권(기본법 제2조 제1항 및 제1조 제1항)은 모든 유형의 개인 관련 정보의 수집을 보호한다. 개인은 기본적으로 자신의 개인정보의 처분을 스스로 결정할 수 있다.[36] 하지만 독일 연방헌법재판소는 소위 'IT 기본권' 판결에서 국가기관이 자신을 숨기고 기본권 향유자와 전기통신을 한다면 정보자기결정권은 침해되지 않는다고 하였다.[37] 오히려 정보자기결정권은 수사기관이 통신 상대방의 신원과 동기에 대해 보호받아야 할 비밀을 개인정보를 수집하기 위해서 이용하는 경우에야 비로소 관련된다고 하였다. 하지만 연반헌법재판소는 통신상대방의 신원을 확인하기 위한 아무런 방법이 제공되어 있지 않는 경우, 가령 통신상대방이 익명으로만 알려져 있는 경우에는 통신에 있어서 보호되어야 할 개인 관련 비밀은 존재하지 않는다고 한다.[38] 오늘 날 인터넷에서 익명 ID를 이용하는 것은 일반적인 현상이다. 따라서 국가기관과는 통신을 하지 않을 것이라는 데 대한 비밀은 보호될 수 없다.

이러한 점에서 형사소추기관과 당사자 사이에 인터넷 통신을 한다는 점에서는 정보자기결정권이 아직 침해되었다고 보기는 어렵다. 이러한 조치는 수사의 일반조항에 의해서 비공개 수사기관에게 허용될 수 있다.[39] 이 경우 수사기관은 자신의 진정한 신분을 사용할 의무는 없다. 수사기관은 오히려 자유로이 익명의 이메일 주소나 다른 ID를 사용할 수 있다. 따라서 수사기관이 단순한 통신을 넘어서 의도적으로 비밀리에 IP트래킹을 수행함으로서 상대방이 자신도 모르게 IP주소를 제공한다는 점에서 정보자기결정권이 침해되었다고 볼 수 있다.

수사기관이 의도한 이러한 추적 조치의 비밀은 또한 연방대법원이 다룬 사례에서

36) BVerfG Urteil vom 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822, Rn. 198.
37) BVerfG Urteil vom 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822, Rn. 310.
38) BVerfG Urteil vom 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07 = NJW 2008, 822, Rn. 311.
39) Schmitt, Meyer-Goßner, StPO, 58. Aufl. 2015, §110a Rn. 4; Günther, MüKo-StPO, Beck online, 2014, §100a Rn. 140; Bruns, KK-StPO, Beck online, 2013, §110a Rn. 7; Bär, a.a.O., §100a Rn.33 f.; Eisele,「Computerund Medienstrafrecht」, C.H.Beck, 2013, §52 Rn. 20; Rosengarten·Römer, "Der virtuelle verdeckte Ermittler in sozialen Netzwerken und Internetboards", NJW 2012, S.1767.

수신확인기능이 첨부된 파일의 저장에도 존재하였다. 따라서 연방대법원이 정보자기결정권의 침해를 인정한 것은 정당하다고 본다.

다. 소결

IP트래킹의 방법으로 IP주소를 수집하는 것은 정보자기결정권의 침해에 해당된다. 그 침해의 정도는 그렇게 중대한 것은 아니지만 정보자기결정권의 침해에는 법률상 수권 근거가 필요하고 그 근거는 규범상 명확하고 특정한 영역에 한정되어야 하며 개인정보보호법상 비례성을 갖추어야 한다.[40] 그렇다면 이러한 침해를 정당화하는 적절한 근거 규정이 무엇인지 검토한다.

2. 적정한 근거 규정

정보자기결정권의 침해를 정당화하는 적정한 규정이 무엇인지 통신사실확인자료의 수집과 그 침해의 정도와 관련하여 연방대법원 수사판사의 견해를 비판적으로 검토해 본다. 우선 통신사실확인자료는 그 수집에 엄격한 요건을 전제로 하는 형사소송법 제100g조가 아니더라도 수집될 수 있다는 사실이 검토될 수 있다. 여기서는 통신사실확인자료가 공개 수집되는 경우와 비밀리에 수집되는 경우를 살펴본다.

통신사실확인자료가 공개 수집되는 경우 우선 공개 이메일 통신에 있어서 발신자의 IP주소가 개별 수신자에게 이메일 헤더에 함께 전송된다는 점을 고려해 볼 수 있다. 즉 추적 대상자가 수사기관의 이메일에 응답을 한다면, 대상자는 당연히 자신의 IP주소를 타임스탬프와 함께 수사기관에 전송하게 된다. 이것은 파일 공유 사이트(예를 들어 P2P 네트워크)에서도 발생할 수 있다. 수사기관이 다운로드하도록 P2P 네트워크에 파일을 올려놓고 이용자들이 이를 내려 받게 되면 타임스탬프가 찍힌 이용자들의 IP주소가 수사기관으로 전달되기 때문이다.

이처럼 수사기관과 인터넷 이용자 사이에 공개 통신을 하는 것은 일반적 수사권 조항을 근거로 허용된다.[41] 이 규정은 통신과 관련하여 반드시 생성되는 IP주소와

40) BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/83, NJW 1984, 419.

같은 통신사실확인자료를 확보하는데도 적용될 수 있다. 따라서 통신사실확인자료를 공개적으로 확보하는 일회적인 수사의 경우에는 형사소송법 제100g조에 의한 법원의 결정은 필요하지 않다.[42] 이러한 사례에서는 전기통신비밀의 침해도 정보자기결정권의 침해도 존재하지 않기 때문이다.

다음은 통신사실확인자료가 비밀리에 수집되는 경우를 검토한다. 대상자의 통신사실확인자료를 비밀리에 수집하는 경우에도 반드시 제100g조에 의한 법원의 결정이 필요한 것은 아니다. 통신미디어법(TMG)[43]에 의하면 추적 대상자의 이용정보(Nutzungsdaten)를 수집할 수 있기 때문이다. 통신미디어법 제15조는 서비스제공자에게 통신미디어의 이용과 그 이용료 정산을 위하여 필요한 경우 이용자의 개인관련 정보(이용정보)를 수집하고 이용할 수 있다. 이용정보 중 특히 '이용자의 신원을 확인할 수 있는 표지'에는 통신미디어서비스의 이용과 관련하여 타임스탬프를 포함한 로그인 IP주소가 해당된다. 이 IP주소는 전기통신법의 통신사실확인자료도 되고 동시에 통신미디어법의 이용데이터도 된다. 동법 제14조는 인터넷서비스제공자에게 통신미디어 이용자의 가입자 정보를 수사기관 등에 제공할 수 있도록 규정하고 있고 동법 제15조는 이를 준용하고 있다. 그런데 형사소송법은 이러한 이용정보를 사용할 수 있다는 명확한 규정을 두고 있지 않지만[44] 일반적 수사권 조항에 의해서 수집할 수 있다고 해석되고 있다.[45] 통신미디어서비스에서 이러한 IP주소의 수집은 통신의 비밀에 해당될 수는 있다. 하지만 형사소송법 제100g조에 의하지 않더라도 이처럼 IP주소가 비밀리에 수집될 수 있다는 사실을 확인할 수 있다.

따라서 통신사실확인자료의 공개 수집이나 비밀 수집의 경우 형사소송법 제100g조에 의한 법원의 결정이 반드시 필요한 것은 아님을 알 수 있다.

---

41) Bär, a.a.O., §100g, Rn.22.

42) Krause, a.a.O., S.142.

43) 통신미디어법(TMG)은 인터넷과 같은 통신미디어(Telemedien)를 제공하는 전자적 정보통신서비스에 적용되는 법률로서 정보통신망에서 개인정보의 보호와 인터넷서비스제공자의 책임을 규정하고 있다.

44) 연방범죄수사청법 제20m조 제2항과 헌법수호청법 제8a조 제2항 제1문 제5호에는 이용정보를 이용할 수 있는 명확한 규정을 두고 있다.

45) Bär, a.a.O., §100g, Rn.26.

3. IP트래킹의 기본권 침해 정도

연방대법원 수사판사는 이 사안에서 IP트래킹의 경우 정보자기결정권의 침해가 특별히 중대하기 때문에 법관의 결정이 필요하여 형사소송법 제100g가 적용되어야 하고 제100h조는 적용되어서는 안 된다고 판단하였다. 하지만 IP트래킹의 경우 기본권 침해의 정도가 형사소송법 제100g조가 요구하는 침해의 정도에 상응하는지 의문이 제기된다. 형사소송법 제100g조가 요구하는 기본권 침해와 IP트래킹에 의한 기본권 침해의 정도를 비교해 보면 그렇지 않다는 점을 확인해 본다.

우선 형사소송법 제100g조는 통신비밀의 침해를 전제로 하고 있지만, 일반적인 IP트래킹의 경우나 연방대법원이 다룬 사안에는 그러한 침해가 존재하지 않는다. 형사소송법 제100g조의 기본 사례는 전화 및 인터넷접속 제공자가 통신사실확인자료를 비밀리에 당사자 모르게 그리고 아무런 방해 없이 수집하는 것과 관계된다. 이러한 수집방법은 또한 개별적으로 일회적인 통신접속으로 제한되지 않고 당사자의 전체 통신으로 소급되어 장기간 실시간으로 수집된다. 형사 실무에서 제100g조에 의해서 전화, 모바일, 인터넷접속의 모든 범위의 통신사실확인자료가 3개월 또는 그 이상 수집되는 것은 일상적인 현상이다. 또한 제100g조에 의한 조치의 경우 물리적인 유선접속의 경우든 모바일기지국이든 모든 개별적인 통신의 위치정보를 수집하여 당사자의 이동프로파일을 작성하는 것도 가능하다.[46] 따라서 제100g조의 기본 사례는 당사자에 대한 비밀성, 통신사실확인자료 감시의 포괄성, 조치의 장기성, 이동프로파일의 작성 가능성 등으로 요약될 수 있다.

이에 반하여 IP트래킹의 침해의 정도는 제100g조의 기본 사례와 상당한 차이가 있다. 오늘 날 수많은 웹서비스 제공자들이나 웹사이트 운영자들은 상업적 목적으로 언제 어떤 IP주소가 인터넷사이트에서 접근되는지 또는 이메일이 열람되는지 확인하기 위해서 이러한 기능을 가진 비밀 파일을 이용하고 있다(예를 들어 구글 아날리틱스).

IP트래킹의 경우 주의해야 할 점은 수신확인서비스는 당사자의 행위를 통해서 비로소 수행된다는 점이다. 당사자가 전송된 이메일이나 다운로드로 제공된 문서를

46) Krause, a.a.O., S.143.

실제로 열람해야 한다는 것이다. 만일 이메일을 단순히 수신만하거나 무시 내지 삭제해버리면 추적 과정은 진행되지 않는다.[47] 당사자가 자신의 자율적인 판단으로 이메일을 열고 해당 파일을 다운로드해야 비로소 기술적으로 수신확인기능이 첨부된 파일이 작동되어 당사자의 IP주소가 수사기관의 서버로 전달되는 것이다.

하지만 대상자가 자신의 컴퓨터나 스마트폰에 보안 소프트웨어를 어떻게 설치하느냐에 따라서 수신확인기능이 첨부된 파일의 작동이 중단될 수도 있다. 또한 이메일이나 데이터가 실제로 열람되지 않도록 혹은 첨부파일이 다운로드되지 않도록 할 수도 있다. 나아가서 당사자가 수신확인서비스를 인식하여 우회할 수도 있다. 물론 기술의 발전으로 컴퓨터 등에 설치된 운영시스템의 보안상 허점을 이용하여 이를 무력화시키는 해킹 프로그램을 수사기관이 사용할 수도 있다. 하지만 이러한 경우 성공할 확률은 그리 높지 않다. 또한 IP트래킹은 대부분 일회적인 처분으로 활용된다.

그리고 IP트래킹을 통해서 이동프로파일을 정확하게 작성하는 것은 가능하지 않다. 개별 IP주소가 어떤 제공자에 의해서 어떤 지역에 할당되는지 인터넷 검색을 통해서 조사하는 것은 가능하다. 하지만 IP주소로 그러한 장소를 확인하는 것은 매우 어렵다. 특히 모바일 인터넷에서 IP주소 배당의 경우 장소적인 귀속은 불가능하다. 따라서 IP주소와 인터넷 접속을 결합하여 대상자의 주거까지 위치를 파악할 수 있게 하는 자는 전기통신사업자이다. 전기통신사업자는 어떤 고객에게 IP주소를 할당하였는지 또는 어떠한 기지국에서 모바일 기기가 접속하였는지를 자신이 보관하고 있는 통신사실확인자료를 통해서 알고 있기 때문이다.

또한 IP트래킹 조치는 대부분 일회적이고 당사자의 실제의 행위에 의존하고 있다. 그리하여 IP트래킹을 통해서 작성되는 이동프로파일은 정확성이 떨어지기 때문에[48] 제100g조를 근거로 작성된 이동프로파일과 비교가 되지 않는다.

따라서 IP트래킹의 경우 수사처분은 다음과 같이 요약할 수 있다. 이 조치는 공개적이지 않지만 그렇다고 완전히 비밀리에 수행되는 것은 아니고, 당사자의 실제의 행위에 성공 여부가 달려 있으며, 사전에 설정된 프로그램을 통해서 우회될 수도

47) Bär, a.a.O., §100g, Rn.21.

48) Lellmann·Pohl, a.a.O., 504; Steinmetz, a.a.O., 397.

있다.[49] 또한 수사기관과 대상자 사이의 개별적인 통신만이 추적 대상이고 대상자의 이동프로파일도 정확하게 작성되지 않는다.

4. 중간결론

이상에서 형사소송법 제100g조에 의한 기본 사례에서는 본질적으로 기본권 침해의 강도가 높고, 특정한 개별적인 통신과 상관없이 모든 통신이 수집대상이며, 당사자의 실제 열람과 상관없이 모든 통신사실확인자료가 수집된다[50]는 것을 알 수 있다. 이에 반해서 IP트래킹의 경우에는 특히 통신사실확인자료의 대량 수집과 장기간 수집이 존재하지 않는다.[51] 처분의 비밀성과 이동프로파일의 작성 가능성도 대단히 제한되어 있다. 따라서 IP트래킹의 경우 기본권 침해의 정도는 형사소송법 제100g조의 기본 사례보다 훨씬 낮다. 이러한 점들을 고려할 때에 IP트래킹에 적용될 수 있는 규정은 연방대법원 수사판사가 적용한 형사소송법 제100g조가 아니라 제100h조라고 보는 것이 타당하다고 생각된다. 앞으로 연방대법원 재판부에서 IP트래킹을 판결로 다시 다루게 된다면 수사판사의 결정과는 다른 결론이 나올 수도 있지만, 문제를 명확히 해결하기 위해서는 무리한 해석론보다는 입법으로 해결하는 것도 고려해 볼 필요가 있다.

Ⅴ. 비교 검토 및 입법방향

1. 적용 가능한 규정들

서론에서 언급했듯이 IP트래킹에 대한 국내의 논의는 현재 발견되지 않는다. 따라서 비교법적 관점에서 독일에서의 논의들을 고려하여 IP트래킹에 적용 가능한 규

49) Krause, a.a.O., 144.
50) Bär, a.a.O., §100g, Rn.22.
51) Krause, a.a.O., NStZ 2016, 143.

정들을 검토해 본다. 다만, 헌법상 기본권 침해에 관한 문제는 독일의 경우와 차이가 거의 없기 때문에 여기서는 지면 관계상 따로 논하지 않는다.

가. 통신자료 제공에 관한 전기통신사업법 제83조

전기통신사업법 제83조는 통신자료의 제공이란 측면에서 독일 형사소송법 제100j조와 유사한 기능을 한다. 제83조는 통신가입자에 관한 개인정보로서 통신자료를 6가지[52]로 열거하고 있고 수사기관이 수사를 위하여 이를 요청하면 전기통신사업자는 이에 따를 수 있다고 규정하고 있다. 독일 형사소송법 제100j조와 비교해 보면 통신자료의 제공 사실이 당사자에게 통지되지 않으며 법관의 관여 없이 제공이 가능하다는 점에서 유사한 점이 있다. 하지만 독일의 경우 가입자 정보는 사실관계의 조사나 피의자의 소재지를 수사하기 위해서만 요청될 수 있으나 우리의 경우 수사라고만 되어 있어 그 범위가 포괄적인 점, 독일의 경우 제공되는 가입자 정보에 제한이 없는 점, 전기통신사업자에게 제공의무가 있는 점[53] 등에서 상당한 차이점이 존재한다. 뿐만 아니라 독일 형사소송법 제100j조는 통신가입자에 대한 개인정보로서 통신사실과는 관련이 없기 때문에 통신비밀의 보호가 적용되지 않고 정보자기결정권이 관련된다. 우리 통신사업법 제83조를 통신비밀의 보호 대상으로 보는 견해가 있지만[54] 통신자료 역시 실제 행해진 전기통신과는 관련이 없는 통신가입자에 관한 개인정보에 해당되기 때문에 정보자기결정권이 관련된다고 보는 게 타당하다.[55] 전기통신이란 개념에서 알 수 있듯이 전기통신의 개시에서 종료까지 통신망에서 전달되는 통신의 내용과 이러한 내용을 전달하는 과정에서 발생하는 트래픽

52) 이용자의 성명, 주민등록번호, 주소, 전화번호, 컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호인 아이디, 이용자의 가입일 또는 해지일.

53) 전기통신사업자가 가입자 정보를 제공하지 않는 경우 과태료 처분을 받거나 질서벌인 구류처분을 받을 수 있다(형사소송법 제100j조 제5항 제2문).

54) 황성기, 현행 통신비밀 보호법제의 헌법적 문제점, 「언론과 법」 제14권 제1호, 2015, 12; 권양섭, “범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안”, 「법학연구」 제59집, 한국법학회, 2015. 9, 402.

55) 근거는 다르지만 결론에 있어서 동일한 견해로는 박민우, “통신자료 제공요청의 법적 성격과 합리적인 제도 개선 방향, -영장주의 및 사후통지의 도입 여부와 관련하여-”, 「법조」 718호, 법조협회, 2016.8, 127-130 참조.

데이터만 통신비밀의 보호영역에 포함되기 때문이다.

이러한 유사점과 차이점을 전제로 하여 제83조가 IP트래킹에 (유추) 적용될 수 있는지 검토해 보면, 이 규정은 독일 형사소송법 제100j에서 검토한 바와 같이 이미 확보한 IP주소가 누구에게 귀속되는지 확인하기 위한 것임을 알 수 있다. 예컨대 이메일 주소나 IP주소 등 통신사실확인자료를 확보한 다음 이들 통신자료가 누구에게 해당되는지 확인하기 위해서 통신자료의 제공을 요청하는 것이다. 따라서 IP주소를 확보하기 위한 IP트래킹에는 전기통신사업법 제83조가 적용될 수 없다.

나. 통신사실확인자료에 관한 통신비밀보호법 제13조

범죄수사를 위한 통신사실 확인자료제공의 절차를 정하고 있는 통신비밀보호법 제13조는 일정한 통신사실확인자료를 사전에 보관하여 수사기관의 요청이 있으면 제공한다는 측면에서 독일 형사소송법 제100g조와 유사한 기능을 한다.

전체적으로 보면 통신사실 확인자료 제공에 법원의 개입, 전기통신사업자의 협조의무, 일정한 기간 보관의무, 사후 통지 등에서 유사한 점이 있다. 하지만 자세하게 들여다보면 상당한 차이점들이 존재한다. 우선 요청할 수 있는 통신사실확인자료가 우리의 경우 7가지로 한정되어 있으나 독일의 경우 의무적으로 보관해야 될 자료(전기통신법 제113b조)는 한정되어 있지만 그렇지 않은 자료(전기통신법 제96조)는 사실상 한정되어 있지 않는 점, 요청할 수 있는 대상범죄가 독일의 경우 중범죄 위주로 제한되어 있으나 우리의 경우 아무런 제한이 없는 점, 요청할 수 있는 실질적 요건이 우리의 경우 '수사를 위하여 필요한 경우'에 불과하지만 독일의 경우 범죄혐의는 물론 사실관계를 조사하기 위해서 필요하고 데이터의 수집이 사건의 의미와 적정한 관계에 있어야 하는 등 엄격한 보충성 원칙을 적용하고 있는 점 등에서 차이점이 존재한다. 특히 IP트래킹과 관련하여 중요한 차이점은 우선 우리의 경우 수사기관이 직접 IP주소를 실시간으로 수집할 수 없다는 점이다. 통신사실확인자료 요청의 경우 전기통신'사실'에 관한 자료로서 과거의 자료에 한정되고 있으므로 실시간 또는 장래의 통신사실확인자료는 수집될 수 없다. 만일 실시간 또는 장래의 자료를 수집하기 위해서는 법원의 영장이 필요한 통신비밀보호법 제5조와 제6조의 통신제한조치에 따라야 한다. 따라서 IP주소를 수사기관이 실시간으로 직접 수집할 수

있는 IP트래킹의 경우에는 통신비밀보호법 제13조가 적용되기 어렵다.

다. 수사의 일반규정에 관한 형사소송법 규정들

독일 형사소송법의 일반적 수사권 조항인 제161조 제1항과 제163조 제1항에 대응하는 규정은 형사소송법의 검사의 수사권에 관한 제195조, 사법경찰관의 수사개시권에 관한 제196조 제2항, 그리고 수사 목적을 달성하기 위해 필요한 사실을 조회할 수 있는 제199조를 들 수 있다. 이들 규정은 기본적으로 임의수사를 전제로 하고 있다. 강제처분은 법률에 특별한 규정이 있는 경우에 한하며 강제처분을 하더라도 필요한 최소한도의 범위 안에서만 해야 한다.

IP트래킹은 당사자 모르게 통신사실확인자료인 IP주소를 수집한다는 측면에서 임의수사가 아니라 강제수사에 해당된다. 따라서 검사의 일반적 수사권이나 경찰의 수사개시권 또는 사실조회에 관한 규정으로는 IP트래킹을 수행할 수 없다.

라. 소결

이상의 검토에서 우리의 경우 IP트래킹에 적용될 규정이 없다는 점을 알 수 있다. 특히 독일 형사소송법 제100h조의 관찰 목적의 기술적 장치에 대응하는 규정은 현재 존재하지 않는다. 따라서 이러한 수사조치에 법적 흠결이 발생하고 있다.

2. 입법 방향

인터넷 이용의 익명성과 진정한 IP주소를 숨길 수 있다는 점에서 인터넷은 범죄의 도구로 악용될 가능성이 늘 잠재해 있다. 따라서 사이버 공격이나 사이버 테러와 같은 중대범죄의 경우 통신의 발신지를 신속하게 파악하는 것이 무엇보다 중요하다. IP주소 기반의 인터넷 통신에서 IP주소가 그 발신지에 해당된다. 앞으로 제4차 산업혁명시대에는 사물인터넷으로 연결되는 사회에서 IP기반의 통신이 더욱 증가할 것이고 사물인터넷과 관련하여 발생될 사이버범죄는 지금까지의 현상과는 차원을 달리할 가능성이 많다.[56] 따라서 이러한 사이버범죄에 대처하기 위해서 IP주소를

확보하기 위한 IP트래킹이 적합한 수사방법으로 도입될 필요가 있다고 본다. 또한 기본권 보장의 관점에서도 도입될 필요가 있다. 만일 IP트래킹이 수사실무에서 아무런 법적 권한 없이 암암리에 행해지고 있다면 이에 대한 일정한 제재가 필요하다. 현재 수사기관들이 통신자료를 무분별하게 요청하고 있다는 통계자료는 이러한 추론을 가능하게 한다. 특히 인터넷 이용자들 몰래 비밀리에 수행되는 인터넷 순찰은 이러한 행위로 나아갈 가능성이 있다. 공개된 인터넷 사이트를 수사기관이 순찰하는 것은 일반적 수사권 조항으로 가능할 수 있다. 하지만 페이스북과 같은 소셜 네트워크에서의 비밀 순찰이 이 규정에 의해서 정당화될 수 있는지는 의문이다. 따라서 IP트래킹에 대한 입법은 수사의 효율성이란 측면과 기본권 보호라는 측면에서 모두 요구된다고 할 수 있다.

다음으로 입법 시 고려되어야 할 주요한 사항을 검토해 보면 우선 IP트래킹은 대상자 모르게 IP트래킹이 수사기관에게 전달된다는 점에서 비밀성이 존재하므로 개인정보자기결정권이 침해되기 때문에 이러한 침해를 정당화하는 요건들이 필요하다.

현재 우리의 법적 상황에서 IP트래킹의 기본권 침해의 정도는 법원의 허가와 사후통지를 요건으로 하는 통신사실확인자료 제공요청보다는 낮고 법원의 허가나 사후통지조차 없는 통신자료 제공요청보다는 높다는 것을 알 수 있다. 따라서 이들의 중간단계에서 IP트래킹에 관한 규정을 두는 것이 적절한 것으로 보인다. IP트래킹의 입법에 관한 구체적인 내용들은 앞서 살펴본 독일의 형사소송법 제100h조를 고려해 볼 수 있다. 이 규정에 따르면 관찰 목적을 위한 기술적 장치를 사용하기 위해서는 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 성공할 가망이 훨씬 적거나 어려울 수 있는 경우여야 하고 그 대상 범죄는 경미범죄가 아니라 중대한 의미를 가지는 범죄여야 한다. 그런데 이 규정의 실질적 요건은 관점에 따라서 우리 통신사실확인자료에 관한 통신비밀보호법 규정의 요건보다 더 엄격하다고 말할 수 있다. 우리의 규정은 대상 범죄에 아무런 제한이 없고 수사상 필요한 경우로만 되어 있기 때문이다. 따라서 IP트래킹을 입법적으로 해결한다면 통신사실확인자

56) 사물인터넷으로 연결되는 기기들은 인체에 착용할 수 있는 기기(예컨대 웨어러블 디바이스)는 물론 심지어 의료장비도 존재하기 때문에 생명이나 신체 등에 중대한 결과를 야기할 가능성이 있다.

료에 관한 규정도 함께 개정할 필요가 있다. 범죄의 대상에 아무런 제한이 없고 사후에 범죄가 발생한 경우 수사상 필요하다는 이유로 국민의 통신사실확인자료가 특정 범죄와는 상관없이 사전에 저장되어 보관된다는 것은 모든 국민을 범죄자로 본다는 비난을 면하기 어렵기 때문이다.

Ⅵ. 결론

사이버 테러와 같은 중대한 범죄에 대처하기 위하여 범죄혐의자의 IP주소를 확보하는 것이 무엇보다 중요하다. 이러한 IP주소를 확보하는 IP트래킹은 범죄혐의를 받고 있는 인터넷 이용자의 위치를 확인하기 위한 기술적 조치로서 활용되고 있다.

비교법적 검토 대상인 독일의 경우 IP트래킹에 직접 적용될 규정은 없지만 다수견해는 관찰 목적을 위해 특정된 기술적 장치를 이용하도록 한 형사소송법 제100h조 제1항 제2호가 해석을 통해서 적용될 수 있다고 보고 있다.

우리의 현재 법적 상황은 해석을 통하여 이러한 IP트래킹에 적용 가능한 법규정 자체가 존재하지 않는다. 우리의 일상생활을 지배하고 있는 거의 모든 통신은 IP주소를 기반으로 하는 인터넷 통신이 그 중심에 있다. 이러한 현상은 4차 산업혁명을 배경으로 더욱 확산될 것이다. 이에 비례하여 사이버범죄도 역시 증가할 것으로 전망된다. 따라서 IP트래킹이 중요한 수사방법으로 활용될 가능성이 매우 크므로 이에 대한 입법이 요구된다. IP트래킹은 상대방에게 비밀리에 수행되기 때문에 정보자기결정권이 침해된다. 기본권 침해의 정도는 법원의 허가와 사후통지를 요건으로 하는 통신사실확인자료 제공요청보다는 낮고 법원의 허가나 사후통지조차 없는 통신자료 제공요청보다는 높다. 따라서 이를 정당화하는 규정은 이들의 중간에 IP트래킹에 관한 규정을 두는 것이 적절할 것으로 보인다. 기본권 침해의 정도는 그렇게 중대하지 않으므로 법원의 허가는 필요하지 않지만 당사자에게 사후통지는 있어야 할 것으로 보인다. 보다 구체적인 법률안에 대한 연구는 다음으로 미룬다.

참고문헌

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

박희영·홍선기, 독일연방헌법재판소판례연구 1, [정보기본권], 한국학술정보, 2010.

전현옥·윤지영, 디지털 증거 확보를 위한 수사상 온라인 수색제도 도입 방안에 대한 연구, 형사정책연구원, 2012.10

권양섭, "범죄수사에 있어서 통신자료제공제도의 문제점과 개선방안", 법학연구 제59집, 한국법학회, 2015. 9.

민영성·박희영, "독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점", 법학연구 제57권 제2호(통권 제88호), 부산대학교 법학연구소, 2016.5.

박민우, "통신자료 제공요청의 법적 성격과 합리적인 제도 개선 방향, -영장주의 및 사후통지의 도입 여부와 관련하여-", 법조 718호, 법조협회, 2016.8.

박희영, "독일 연방헌법재판소의 '정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권", 인터넷법률(현재 선진상사법률) 통권 제45호, 법무부, 2009.1.

박희영, "휴대전화 비밀번호와 PIN 번호에 대한 접근은 위헌", 최신독일판례연구, 로앤비, 2012.6.

박희영, IP 주소를 수집하기 위한 IP-Tracking 수사방법의 법적 근거, 최신독일판례연구, 로앤비, 2017.05.

이성기, "「통신사업자의 통신사실 확인자료 및 통신자료제공의 요건과 절차」에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본의 제도 비교를 중심으로", 법과 정책 제14집 제1호, 한국법정책학회, 2014.3.

이원상, 온라인 수색(Online-Durchsuchung)에 대한 고찰 - 독일의 새로운 논의를 중심으로-, 형사법연구 제20권 제4호, 2008..

황성기, "현행 통신비밀 보호법제의 헌법적 문제점", 언론과 법 제14권 제1호, 2015, 12.

Bär, Wolfgang, KMR-StPO, Carl Heymanns Verlag, 2016, §100g Rn.32.

Bruns, Michael, KK-StPO, Beck online, 2013, §110a Rn.7, §100j Rn.4.

Eisele, Jörg, 「Computerund Medienstrafrecht」, C.H.Beck, 2013, §52 Rn.20.

Graf, Jürgen-Peter, BeckOK, StPO §100g, Beck online, 2017, Rn.12a.

Günther, Ralf, MüKo-StPO, Beck online, 2014, §100a Rn.140.

Schmitt, Bertram, Meyer-Goßner, StPO, C.H.Beck, 2015, §110a Rn. 4.

Krause, Benjamin, "IP-Tracking durch Ermittlungsbehörden: Ein Fall für § 100 g StPO? – Zugleich Besprechung des BGH-Beschl. v. 23.9.2014 – 1 BGs 210/14", NStZ 2016 Heft 3, 139.

Lellmann, Katrin·Pohl, Stefan, "IP-Tracking, Rechtliche Zulässigkeit und Fallkonstellationen", Kriminalistik 2015, 8-9, S.498.

Rosengarten, Carsten·Römer, Sebastian, "Der virtuelle verdeckte Ermittler in sozialen Netzwerken und Internetboards", NJW 2012 Heft 25, S.1767.

Steinmetz, Wolfhard, "Erhebung von IP-Adressen mittels IP-Tracking", wistra 2015 Heft 10, S.396.

Legal discussions on IP tracking as a location tracking investigation in Germany and its implications*

Min, Young-sung**·Park, Hee-young***

In the event of a serious crime such as cyber terrorism, it is most important to secure the identity of the internet user who is suspected of the crime. In order to verify the identity of such criminal suspects, IP tracking, which obtains IP address, can be used as an investigation method. This paper examines whether IP tracking is allowed in the current legal context and what are the ground rules.

In Korea, there are no legal cases or research papers dealing with the IP tracking and its ground rules. Therefore, the legal situation in Germany which preceded this discussion is examined comparatively. Even in Germany, there are no legal provisions that apply directly to IP tracking, but recently an investigative judge of Supreme Court Justice(BGH) has decided to allow IP tracking through the interpretation of a related regulation of the Criminal Procedure Act(StPO). However, as the critical opinion on this decision was presented, the legal debate about it has begun in earnest.

The investigative judge of Supreme Court found that IP tracking could be permitted only under section 100g of StPO for the collection of traffic data(Verkehrsdaten) because IP addresses were collected and infringed on the right to self-determination. However, the majority view is that §100h(1) StPO is an appropriate provision. This regulation allows observation of suspects through a specific technical device. Considering the degree of infringement of fundamental

* This work was supported by the National Research Foundation of Korea Grant funded by the korean Government(MOE)(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.

rights, the majority opinion is reasonable.

Currently, there are no regulations in Korea such as §100h(1) StPO in Germany, so legislation is required. Because IP tracking is done secretly to suspect, the right to information self-determination is violated. But the degree of infringement is not so serious. Therefore, it seems appropriate to place a provision that justifies this between Article 13 of Protection of Communications Secrets Act(Act No. 12229, Jan. 14, 2014) and Article 83 of Telecommunications business Act(Act No.12035, 13. Aug, 2013., Partial Amendment). Considering the degree of infringement of the basic rights, the court's permission is not required, but the post-notification must be guaranteed to the parties.

❖ Key words : IP Address, IP Tracking, Communication Confirmation Data(Traffic Data, Verkehrsdaten), Communication Data(Subscriber Information, Bestandsdaten), Right to Informational Self-Determination, Technical Devices for Surveillance

투고일 : 6월 5일 / 심사일 : 6월 16일 / 게재확정일: 6월 16일