형사정책연구 Korean Criminological Review
제34권 제1호(통권 제133호, 2023・봄)

독일 통신사실확인자료 보관조항의 EU 법 위반과 형사정책적 시사점*

– 2022년 9월 20일 유럽사법재판소 판결을 중심으로 –

박 희 영**

국 | 문 | 요 | 약

구체적인 범죄혐의나 공공안전에 대한 위험이 없음에도 불구하고 이용자의 동의없이 통신사실확인자료(=트래픽데이터)를 사전에 '보관'하여 수사기관의 요청에 따라 제공하도록 전기통신사업자에게 '의무'를 부과하는 것(보관의무)은 개인정보자기결정권, 통신비밀 및 사생활의 비밀, 표현의 자유와 같은 헌법상 기본권을 제약한다. 이러한 보관의무가 정당화될 수 있는 제한인지 아니면 정당화될 수 없는 침해인지 문제가 제기된다.

지난 2022년 9월 20일 유럽사법재판소는 이유없이 거의 모든 국민의 트래픽데이터를 사전에 보관하여 국가기관에 제공하도록 전기통신사업자에게 의무를 부과한 독일 전기통신법 조항들은 유럽연합 기본권 헌장의 관련 기본권을 위반한다고 판결하였다. 다만 유럽사법재판소는 엄격한 조건에서 예외를 인정하였다. 하지만 이러한 예외는 기존의 트래픽데이터 보관의 유형이나 성격과는 전혀 다르다. 따라서 범죄혐의와 무관하게 모든 국민의 트래픽데이터를 사전에 보관하는 것은 이제 더 이상 허용될 수 없게 되었다.

우리 통신사실확인자료 보관의 법적 근거와 법적 성질은 개인정보보호법과 통신비밀보호법의 체계적 분석에서 도출될 수 있다. 이에 따르면 전기통신사업자는 모든 국민의 통신사실확인자료를 아무런 이유없이 보관할 법적 의무를 부담한다. 이러한 법적 의무는 독일 전기통신법의 보관의무와 본질적으로 동일하다. 따라서 유럽사법재판소 판결의 관점에서 보면 우리의 보관조항은 헌법상 사생활의 비밀 및 통신비밀, 개인정보자기결정권, 표현의 자유를 침해할 가능성이 있다. 보관조항이 위헌이라면 당연히 제공조항도 위헌이 될 것이다. 이제 통신사실확인자료 '보관조항'의 위헌 여부가 논의되어야 한다. 만일 위헌가능성이 확실하다면 유럽사법재판소가 제시한 대상 특정 보관제도와 신속보관명령제도가 형사정책적 관점에서 논의되어야 할 것이다.

DOI : https://doi.org/10.36889/KCR.2023.3.31.1.141.

❖ 주제어 : 통신사실확인자료(트래픽데이터), 대상 특정 보관, 신속보관, 개인정보보호, 통신비밀, 표현의 자유

* 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5A2A03053654).

** 독일 막스플랑크 범죄와 안전 및 법 연구소(구 국제형법연구소) 연구원, 법학박사.

Ⅰ. 머리말

구체적인 범죄혐의나 공공 안전에 대한 위험이 없음에도 불구하고 이용자의 동의없이 통신사실확인자료(=트래픽데이터)[1]를 사전에 '보관'하여 수사기관의 요청에 따라 제공하도록 전기통신사업자에게 '의무'를 부과하는 것(보관의무)이 과연 정당화될 수 있는가 하는 문제는 개인정보자기결정권, 통신비밀보호 및 사생활의 비밀, 표현의 자유 등 헌법상 기본권 제약과 밀접한 관련이 있다. 통신사실확인자료는 1차적으로 수집 및 보관의 관점에서, 2차적으로 제공의 관점에서 기본권이 이중적으로 제약된다. 특히 아무런 이유없이 통신사실확인자료가 수집되어 보관되기 때문에 모든 국민이 잠재적 범죄자로 간주될 수 있다는 점에서 기본권 제약의 정도가 상당히 높다. 따라서 이러한 '보관'이 정당화되는 기본권 제한인지 아니면 정당화될 수 없는 기본권 침해인지 문제가 제기된다.

우리 헌법재판소는 2018년 6월 28일 통신비밀보호법의 통신사실확인자료 제공요청 조항에 관한 결정에서 통신사실확인자료의 '보관조항'의 위헌성 문제는 다루지 않았다. 또한 이 헌법재판소의 결정을 전후하여 발표된 선행연구도 주로 요청조항과 관련한 법적인 문제를 다루었다.[2]

지난 2022년 9월 20일 유럽사법재판소는 이유없이 거의 모든 국민의 트래픽데이터를 사전에 보관하여 국가기관에 제공하도록 전기통신사업자에게 의무를 부과한 독일 전기통신법 조항은 유럽연합 기본권 헌장의 관련 기본권과 전자프라이버시지침을 위반한다고 판결하였다.[3] 다만 유럽사법재판소는 엄격한 조건에서 예외를 인정하였다. 하지만 이러한 예외는 기존의 트래픽데이터보관의 성격이나 유형과는 본질적으로 다르다. 따라서 범죄혐의와 무관하게 모든 국민의 트래픽데이터를 사전에 보관하는 것은 이제는 허용될 수 없게 되었다.

이러한 유럽사법재판소의 기본권 판결은 비교법적 관점에서 우리 통신사실확인자료

1) EU 전자프라이버시지침(2002/58/EC)은 '트래픽데이터'(Traffic data)로, 이 지침을 국내법으로 이행한 독일은 전기통신법(TKG)과 전기통신 및 텔레미디어 데이터보호법(TTDSG)에서 페어케어스다텐(Verkehrsdaten)으로 표현하고 있다.

2) 이러한 문제점을 지적하고 있는 문헌으로는 다음 참조: 박소현(a), "개인정보보호적 관점에서의 통확자료요청제도", 형사법연구 제34권 제2호(2022 여름), 187-214; 박소현(b), "전기통신사업자에 의한 통확자료저장에 대한 법적 제한의 필요성", 성균관법학 제34권 제3호(2022.9), 221-246.

3) EuGH, Urteil vom 20.09.2022 - C-793/19 and C-794/19, Spacenet und Telekom Deutschland.

보관조항의 논의에 중요한 계기를 제공하고 있다. 통신비밀보호법도 독일 전기통신법과 유사하게 범죄혐의나 공공안전에 대한 위험과 상관없이 모든 국민의 통신사실확인자료를 제공하도록 전기통신사업자에게 요구하고 있기 때문이다. 더구나 범죄의 경중이나 범죄의 혐의와 상관없이 모든 국민의 통신사실확인자료가 제공되고 있다. 통신사실확인자료가 '제공'되기 위해서는 사전에 '보관'되어 있어야 한다. 따라서 통신사실확인자료 보관이 단순한 권고규정인지 아니면 법적 의무인지가 중요한 쟁점이 된다.

따라서 이 글은 유럽사법재판소의 판결을 분석하고 우리에게 주는 시사점이 무엇인지 밝힌다. 우선 유럽사법재판소의 판결을 이해하기 위해서 판결대상인 독일의 관련 조항의 유형과 법적 성질을 개관하고(Ⅱ.), 유럽사법재판소 선결재판을 제청한 독일 법원의 입장을 소개한 다음(Ⅲ.), 이에 대한 유럽사법재판소 판결을 분석하고(Ⅳ.), 평가한다(Ⅴ.). 끝으로 우리 통신사실확인자료 보관조항의 법적 근거와 법적 성질을 검토한 후 유럽사법재판소 판결의 관점에서 형사정책적 시사점을 도출한다(Ⅵ.).

Ⅱ. 독일의 통신사실확인자료 보관조항의 유형과 법적 성격

독일은 통신사실확인자료(=트래픽데이터)[4]를 두 가지 유형으로 구분하여 법적 성격을 달리하고 있다. 하나는 전기통신사업자가 자신의 영업 목적과 관련하여 수집하여 보관하는 트래픽데이터(영업목적 트래픽데이터)이고, 다른 하나는 범죄수사와 공공 안전에 대한 위험방지 등 공익목적으로 수집하여 일정 기간 보관해야 하는 트래픽데이터이다(공익목적 트래픽데이터).

영업목적으로 보관되는 트래픽데이터는 이용자의 동의가 필요하지 않다. 영업목적이 종료되었을 때는 지체없이 삭제해야 한다. 영업목적의 트래픽데이터의 보관기간은 별도로 정해져 있지 않다. 이 데이터의 보관여부는 기본적으로 전기통신사업자의 자율에 맡겨져 있다.[5] 이런 점에서 이 조항은 임의규정으로 볼 수 있다. 이러한 데이터는 영업목

4) 전기통신법에 의하면 트래픽데이터의 개념은 "전기통신서비스의 제공에 있어서 수집, 처리, 이용되는 데이터를 말한다(TKG 제3조 제70호).

5) 다만 요금정산을 위한 트래픽데이터는 6개월간 보관할 수 있다. 이 기한이 도래하기 전에 요금정산과 관련하여 법원에 소송이 제기된 경우 그 기간은 연장될 수 있다.

적이 종료된 후 지체없이 삭제되어야 하기 때문에 범죄수사나 위험방지기관이 제공을 요청하는 경우 제공받지 못할 수도 있다. 그리하여 특정한 트래픽데이터는 일정 기간 보관하도록 의무를 부과하는 규정이 필요하게 되었다. 그것이 바로 전기통신법에 규정된 공익목적 트래픽데이터보관이다. 따라서 이 조항은 데이터를 의무적으로 보관해야 하는 강제규정이다.

최근까지 트래픽데이터는 모두 전기통신법(TKG)에 규정되어 있었다. 2021년 6월 23일 전기통신현대화법(TKMoG)[6]에 의해서 전기통신법이 전부 개정되어 2021년 12월 1일부터 발효되었다. 이에 따라 전기통신사업자가 의무적으로 보관해야 하는 트래픽데이터는 기존의 전기통신법 제113a조 내지 제113g조에서 현재의 제175조 내지 제181조[7][8]로 조문의 위치가 변경되었다.

이에 대해 전기통신사업자의 영업목적 트래픽데이터는 전기통신법 제96조에 규정되어 있었으나, 현재는 새로 제정된 전기통신 및 텔레미디어 데이터보호법(TTDSG) 제9조[9]에 규정되어 있다. 한편 통신으로 생성되는 위치데이터는 트래픽데이터에 해당되지만, 통신과 상관없이 생성되는 위치데이터의 처리는 TTDSG 제13조에 규정되어 있다.

Ⅲ. 독일 연방행정대법원의 유럽사법재판소 선결재판 제청

1. 사실관계

공중에게 인터넷서비스를 제공하는 인터넷접속제공자(SpaceNet AG)와 전화서비스도 함께 제공하는 전기통신사업자(Telekom Deutschland GmbH)는 통신가입자 또는 이용자의 전기통신과 관련한 트래픽데이터와 위치데이터를 사전에 보관하도록 의무를

6) BGBl. I 2021 S.1858.
7) 보관의무자 및 보상의무(제175조), 보관될 트래픽데이터의 종류 및 기간(제176조), 보관데이터의 사용(제177조), 데이터의 보안(제178조), 기록의무(제180조), 보관의무 이행 시 준수사항(제180조), 의무자의 안전구상(제181조).
8) 개별 조문은 다음 사이트 참조(https://www.gesetze-im-internet.de/tkg_2021/).
9) 조문 내용은 다음 사이트 참조(https://www.gesetze-im-internet.de/ttdsg/).

부과하고 있는 전기통신법 제113b조와 제113a조 제1항[10]에 대해서 쾰른 행정법원에 이의를 제기하였다. 이러한 이의제기에 대하여 쾰른 행정법원은 2018년 4월 20일 SpaceNet과 Telekom은 인터넷 접속과 관련한 트래픽데이터를 저장할 의무가 없고, Telekom은 또한 고객의 전기통신과 관련한 트래픽데이터를 보관할 의무가 없다고 판결하였다.[11] 쾰른 행정법원은 유럽사법재판소의 2016년 12월 21일 판결[12]의 법리를 적용하여 이러한 보관의무는 EU법에 위반된다고 판단한 것이다. 전기통신사업자의 직무를 관할하는 연방망규제청(BNetzA)은 이러한 행정법원의 판결에 대하여 연방행정대법원에 상고를 제기하였다.

2. 선결 재판 제청 내용

연방행정대법원은 전기통신법 제113b조와 제113a조 제1항에 의한 트래픽데이터의 보관의무가 EU법에 위반되는지 여부는 전자프라이버시지침의 해석에 달려있다고 보았다. 연방행정대법원은 유럽사법재판소의 2016년 12월 21일 판결에 따르면 트래픽데이터와 위치데이터의 보관 및 이에 대한 국가기관의 접근에 관한 규정들은 기본적으로 이 지침의 적용 범위에 해당된다고 전제한 뒤, 전기통신법의 이러한 보관의무가 지침 제5조 제1항(통신비밀보호), 제6조 제1항(트래픽데이터), 제9조 제1항(트래픽데이터가 아닌 위치데이터)의 권리를 제한하는 한, 지침 제15조 제1항에 의해서 정당화될 수 있다고 한다. 이러한 점에서 연방행정대법원의 견해는 원심인 쾰른 행정법원의 견해와 다르다.

따라서 연방행정대법원은 상고 절차를 중단하고 유럽사법재판소에 선결재판을 제청하였다.[13] 이 제청에서 연방행정대법원은 전기통신법의 트래픽데이터 보관조항의 내용을 7가지로 정리하여 설명하고 있다. 첫째, 트래픽데이터는 장소적, 시간적 또는 공간적 관점에서 특정한 원인을 요건으로 보관되지 않는다.[14] 둘째 및 셋째, 전화서비스 제공 및

10) 유럽사법재판소의 판결 대상인 전기통신법 규정들은 2021년 개정되기 이전의 것이다.
11) VG Köln, 20.04.2018 - 9 K 3859/16
12) EuGH, Urteil vom 21.12.2016, C-203/15, C-698/15, Tele2 Sverige und Watson ua.
13) BVerwG, Beschluss vom 25.09.2019 - 6 C 12.18 - und - 6 C 13.18. 이에 대해서는 이상학, EU개인정보보호와 권리구제, 공법연구 제48집 제4호, 2020.6, 361-365 참조.
14) 이것은 뒤에서 검토할 유럽사법재판소가 예외사유로 요구하는 대상 특정 보관이 아니라는 의미이다.

인터넷 서비스 제공의 경우 보관될 데이터를 한정적으로 열거하고 있다. 넷째, 일정한 트래픽데이터는 보관이 금지되어 있다(통신내용, 호출되는 인터넷사이트에 관한 데이터, 전자우편 서비스 데이터, 교회의 성직자 등 특정인의 회선과 관련하여 접속한 데이터). 다섯째, 모바일 전화 통신 및 인터넷접속 시 무선기지국의 위치데이터는 4주, 기타 데이터는 10주 동안 보관된다. 여섯째, 보관된 데이터는 남용의 위험 및 무권한 접근으로부터 효과적으로 보호조치가 되어 있다. 마지막으로 보관데이터의 이용과 관련하여 특별히 중대한 범죄를 소추하기 위해서, 개인의 생명, 신체 또는 자유에 대한 구체적 위험과 연방 및 주의 존립에 대한 구체적 위험을 방지하기 위해서만 이용될 수 있으나 인터넷 이용 시 통신가입자에게 부여되는 IP주소는 모든 범죄의 소추, 공공의 안전과 질서에 대한 위험 방지, 정보기관의 직무 수행을 위해서 이용될 수 있다(전기통신법 제113c조 제1항 제3호와 제113조 제1항 제3문).

연방행정대법원은 전자적 통신서비스 제공자에게 이용자의 트래픽데이터 및 위치데이터를 보관하도록 의무를 부과하고 있는 트래픽데이터 규정이 유럽연합 기본권 헌장 제7조(사생활 존중권과 통신비밀), 제8조(개인정보보호), 제11조(표현의 자유), 제52조 제1항(법정주의)과 기본권 헌장 제6조(자유 및 안전에 대한 권리) 및 유럽연합조약(EUV) 제4조를 고려하면 지침 제15조에 위배되는 것으로 해석해야 하는지의 문제를 판단해 달라고 요청하고 있다.

지침 제15조에 따르면 특히 국가안전, 국방, 공공 안전을 위해서 그리고 범죄의 예방, 수사, 확인 및 소추를 위해서 이 지침의 제5조, 제6조, 제9조의 권리와 의무를 제한하는 입법 조치를 할 수 있다. 연방행정대법원은 독일의 트래픽데이터 보관조항이 지침 제15조에 일치한다고 보고 있다.

Ⅳ. 유럽사법재판소 판결 분석

유럽사법재판소는 독일 연방행정대법원의 견해와 달리 독일의 트래픽데이터 보관조항은 지침 제15조 제1항의 해석에 의해서 기본적으로 정당화될 수 없다고 판결하였다. 하지만 엄격한 요건으로 트래픽데이터의 보관과 접근에 관한 예외를 허용하였다. 이러한

예외로서 대상을 특정하여 트래픽데이터를 보관할 수 있는 대상 특정 데이터 보관과 이러한 데이터를 신속하게 보관하도록 명령하는 신속보관명령을 제시하고 있다. 아래에서 독일의 관련 규정들이 EU법과 일치할 수 없는 이유와 유럽사법재판소가 제시한 예외를 분석한다.

1. 판결과 관련한 EU법 규정

트래픽데이터는 민감한 개인정보이다. EU에서 개인정보는 기본적으로 EU일반개인정보보호법(GDPR)이 규율한다. 하지만 트래픽데이터와 개인정보는 특별법인 전자프라이버시지침(2002/58/EC)이 적용된다.[15] 이 지침은 회원국의 규정들이 전자적 통신분야에서 개인정보의 처리와 관련하여 기본적 권리와 자유 그리고 특히 프라이버시 및 비밀의 권리를 동등한 수준으로 보호하고 공동체 내에서 이러한 데이터와 전자적 통신기기 및 전자적 통신서비스의 자유로운 이동을 보장하도록 조정하기 위한 것이다(지침 제1조 제1항).

전자프라이버시지침은 제5조에서 통신가입자와 이용자의 통신비밀을 보호하고 있고, 제6조 제1항에서 전자적 통신서비스 제공자가 통신가입자 및 이용자와 관계된 트래픽데이터의 처리 및 보관과 관련하여 통신전달을 위해서 더이상 필요하지 않는 경우 이를 즉시 삭제하거나 익명으로 처리하도록 규정하고 있다. 제6조 제2항에서 요금 정산 등에 필요한 트래픽데이터는 정산이 법적으로 불복될 수 있거나 요금 정산의 청구가 주장될 수 있는 기간이 경과될 때까지 처리될 수 있다고 규정하고 있다. 또한 지침 제9조 제1항에 의하면 '트래픽데이터가 아닌 위치데이터'[16]는 오로지 특정한 요건에서 그리고 익명으로 처리되거나 이용자 또는 통신가입자가 이에 동의한 경우에만 처리될 수 있다.[17] 이러한 조항들은 앞서 언급한 TTDSG 제3조(통신비밀), 제9조(트래픽데이터), 제13조(위치데이터) 등에 이행되어 있다.

하지만 지침 제15조 제1항은 지침 제5조(통신비밀), 제6조(트래픽데이터), 제9조(위

15) GDPR 제95조는 전자프라이버시지침과의 관계를 명확히 하고 있다.
16) 박희영, 이용대기상태의 휴대전화 위치정보 수사의 허용과 입법방향, 형사정책연구 제31권 제2호 (통권 제122호, 2020·여름), 96.
17) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 55.

치데이터)에 의한 권리와 의무를 제한하는 입법을 회원국에게 허용하고 있다. 이러한 제한은 국가안보, 국토방위, 공공 안전 그리고 범죄의 예방, 수사, 확인 및 소추를 위해서 민주사회에서 필요하고, 적합하고, 비례적이어야 한다.[18] 회원국은 이러한 목적을 위해서 특히 열거한 사유에서 '제한된 기간 동안 데이터 보관'에 관한 입법 조치를 할 수 있다. 나아가서 이러한 입법조치는 유럽연합조약(EUV) 제6조 제1항과 제2항에 언급된 기본원칙과 EU의 일반적인 기본원칙들에 상응해야 한다. 지침 제15조는 전기통신법 제113a조 내지 제113g조(현재 제175조 내지 제181조)에 이행되어 있다.

2. 공익목적의 위계질서에 따른 트래픽데이터 보관 기준

유럽사법재판소는 독일의 트래픽데이터 보관조항이 EU법과 일치할 수 없다는 점을 논증하기 위해서 지침의 기본권 제한조항(제15조 제1항)에서 일정한 기준을 도출하였다. 즉 기본권 제약을 정당화할 수 있는 공익목적들 사이에 일정한 위계질서가 존재하고, 이러한 위계질서에 따라 트래픽데이터의 보관기준도 달라야 한다고 한 것이다.[19] 사법재판소가 분류한 위계질서는 첫째, 국가안보, 둘째, 중대한 범죄에 대한 대응 및 공공 안전에 대한 중대한 위험에 대한 대응, 셋째, 일반 범죄에 대한 대응 및 공공 안전에 대한 일반적 위험에 대한 대응이다.[20]

---

18) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 68.

19) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 71.

20) 이러한 위계질서에서 특별히 중대한 범죄는 국가안보와 동일할 수 있지 않는가 하는 의문이 제기되었다. 이에 대해 유럽집행위원회는 지지견해를 밝혔으나, 사법재판소는 이 판결에서 양자를 명확히 구분하였다. 국가안보의 목적은, 헌법, 정치 또는 경제의 영역에서 또는 사회적 영역에서 국가의 전통적인 구조를 중대한 방법으로 혼란스럽게 하고, 특히 공동체, 국민 또는 국가 그 자체를 직접 위협하기에 적합한 활동, 가령 테러 행위와 같은 활동을 예방 및 진압하여 국가의 본질적인 기능과 사회의 기본적인 이익을 보호하는 주된 관심과 일치한다고 하였다. 하지만 (특별히 중대한) 범죄와 달리 국가안보에 대한 위협은 실제로 그리고 현재, 적어도 예견될 수 있어야 한다고 한다. 국가안보에 대한 위협은 일반적이고 구별없는 트래픽데이터와 위치데이터의 보관 조치를 제한된 기간 동안 정당화하기 위해서, 충분히 구체적인 상황의 발생을 요건으로 한다. 따라서 국가안보에 대한 위협은 그 종류, 중대성 그리고 이를 근거짓는 상황의 특수성에 의해서 공공 안전의 긴장 또는 장해가 발생하는 일반적이고 상시적 (중대한) 위험이나 중대한 범죄와 구별된다. 따라서 (특별히 중대한) 범죄는, 국가안보의 위협과 동일하게 취급될 수 없다. 양자를 동일시하는 것은 국가안보의 요건을 공공의 안전에 적용하기 위해서, 국가안보와 공공 안전 사이에 중간 범주를 생성할 가능성이 있다 (EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 92, 93, 94).

가. 국가안보를 위한 보관 기준

지침의 기본권 제한조항(제15조 제1항)은 국가안보, 국방, 공공 안전, 범죄 대응 등을 공익목적으로 열거하고 있다. 사법재판소는 이러한 공익목적 중에서 국가안보가 가장 중요하다고 보았다. 따라서 이 제한조항에 의해서 기본권 헌장 제7조(사생활존중권, 통신비밀), 제8조(개인정보보호), 제11조(표현의 자유) 및 제52조 제1항(법정주의)을 고려하여 '국가안보'를 위해서 전자적 통신서비스 제공자에게 트래픽데이터와 위치데이터를 '일반적이고 구분없이'(generally and indiscriminately) 보관하는 것을 회원국의 의무로 부과하는 입법조치는 허용될 수 있다고 하였다.[21]

하지만 여기에는 다음 세 가지 조건을 요구하였다. 회원국이 일반적이고 구분없이 트래픽데이터를 보관하기 위해서는 첫째, 해당 회원국이 실제로 그리고 현재 또는 예견할 수 있는 국가안보에 대한 중대한 위협에 직면하고 있어야 한다. 둘째, 법원이나 구속력을 가진 독립적 행정관청이 심사를 통하여 그러한 상황이 존재하고 규정된 조건과 보장이 준수되고 있음을 확인함으로써 그 보관 명령이 효과적으로 통제될 수 있어야 한다. 셋째, 트래픽데이터의 보관 명령은 오로지 절대적 필요성으로 제한되는 기간에만 내려지고 위협이 지속하는 경우 기간을 연장할 수 있어야 한다.

따라서 이러한 기준으로 보관된 트래픽데이터는 위계질서에서 하위의 목적을 위해서는 제공될 수 없다.[22] 예를 들어 중대한 범죄를 수사하기 위해서 국가안보 목적으로 보관된 데이터가 제공되어서는 안 된다.

나. 중대한 범죄 및 공공 안전의 위협에 대응하기 위한 보관 기준

사법재판소는 또한 중대한 범죄에 대응하고 공공안전에 대한 중대한 위협을 방지하기 위해서만 트래픽데이터와 위치데이터의 보관으로 야기되는 사생활존중권과 개인정보보호의 제한을 정당화할 수 있다고 보았다.[23]

하지만 사법재판소는 중대한 범죄에 대응하기 위해서 트래픽데이터와 위치데이터를 '일반적이고 구분없이' 보관하고 있는 독일 국내 법규정은 절대적 필요성의 한계를 넘어

21) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 72.
22) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 91.
23) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 73.

서고 민주주의사회에서 정당화될 수 없다고 하였다.[24] 트래픽데이터와 위치데이터에서 발생할 수 있는 정보의 민감성을 고려하면, 그 비밀성은 사생활존중권에서 결정적인 의미를 가진다. 따라서 이러한 데이터 보관이 사생활존중권(헌장 제7조)과 표현의 자유(헌장 제11조)의 행사에 미치는 위축효과(chilling effects)와 이와 관계되는 제약의 비중을 고려하면, 그러한 데이터 보관은 민주주의사회에서 '예외'여야 하고, '원칙'이 되어서는 안 되며, 그러한 데이터는 또한 체계적이고 지속적인 보관의 대상이 되어서도 안 된다고 하였다. 이것은 중대한 범죄의 대응 목적과 공공의 안전에 대한 중대한 위험의 방지 목적을 고려하더라도 마찬가지라고 한다.

하지만 사법재판소는 트래픽데이터를 보관할 수 있는 예외를 인정하고 그 기준을 제시하였다.[25] 따라서 중대 범죄 및 공공 안전에 대한 위협에 대응하기 위해서 트래픽데이터의 보관이 완전히 불가능한 것은 아니다. 기본권 헌장 제7조, 제8조, 제11조 및 제52조 제1항을 고려하면 지침 제15조 제1항에서 중대한 범죄에 대응하고 공공안전에 대한 중대한 위협을 방지하기 위해서 다음 5가지의 입법조치가 예외적으로 허용될 수 있다고 본 것이다.[26]

첫째, 객관적이고 차별없는 기준(objective and non-discriminatory factors)을 근거로 대상자를 범주화하거나 지리적 기준을 이용하여 절대적 필요성으로 제한되는 기간동안 대상이 특정된 트래픽데이터와 위치데이터의 보관(the targeted retention)을 규정하고, 그 기간의 연장을 가능하게 하는 입법조치.

둘째, 절대적 필요성으로 제한되는 기간 동안 통신접속의 출처(발신지)에 할당되는 IP 주소를 일반적이고 구별없이 보관하는 입법조치.

셋째, 전자적 통신수단 이용자의 신원확인과 관련한 데이터를 일반적이고 구별없이 보관하는 입법조치.

넷째, 법원의 효과적인 통제를 받는 관할기관의 결정에 의해서 특정된 기간 동안 전자적 통신서비스 제공자가 보관하고 있는 트래픽데이터와 위치데이터를 신속하게 보관하

24) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 74.
25) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 75.
26) EuGH, Urteil vom 6.10.2020, C-511/18, C-512/18, C-520/18, La Quadrature du Net ua/Premier ministre ua, Rn. 168; EuGH, Urteil vom 5.4.2022, C-140/20, Commissioner of the Garda Síochána ua, Rn. 67.

도록(the expedited retention, quick freeze) 의무를 부과하는 입법조치.

마지막으로 명확하고 간결한 규정을 통해서 통신데이터의 보관 시 이에 적용되는 실체적, 절차적 요건들이 준수되고, 당사자가 남용 위험으로부터 효과적으로 보장되는 보호조치를 확보하는 입법조치.

이러한 기준에 의해서 보관된 데이터에는 위계질서상 상위의 목적인 국가안보를 위해서 제공될 수 있지만, 하위의 목적인 일반범죄를 수사하기 위해서는 제공될 수 없다.

다. 일반 범죄 및 공공 안전에 대한 일반적 위협에 대응하기 위한 보관 기준

일반 범죄의 방지, 수사, 확인 및 소추의 목적이 정당화되기 위해서는 기본권의 제약이 중대하지 않아야 한다.[27] 따라서 일반 범죄에 대응하기 위해서는 중대한 범죄 대응 기준에서 제시된 전자적 통신수단 이용자의 신원확인과 관련한 데이터를 일반적이고 구별없이 보관하는 입법조치만 할 수 있다.

3. 독일 통신사실확인자료 보관조항의 EU법 위반

유럽사법재판소는 이러한 기준들에 따라서 독일의 트래픽데이터 보관조항들이 EU법과 일치할 수 없다고 판단하였다.

가. 보관데이터의 범위

독일의 트래픽데데이터 보관조항은 통신내용 및 방문한 인터넷사이트에 관한 데이터를 보관의무에서 배제하고 있고, 통신의 시작 시 무선기지국 표지만 보관하도록 규정하고 있다. 하지만 보관된 트래픽데이터를 통해서 대상자의 사생활(가령 일상생활 습관, 상시 또는 일시적 체류지, 매일 또는 간혹 발생하는 장소변경, 수행 중인 활동, 대상자의 사회적 관계 및 그가 교류하는 사회적 환경)이 매우 정확하게 추론될 수 있고, 특히 대상자의 프로필이 작성될 수 있다는 점을 분명히 하였다.[28]

---

27) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 73.
28) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 78.

또한 방문한 인터넷사이트에 관한 데이터는 보관되지 않지만, IP 주소가 보관되고 있다는 점도 지적하고 있다. IP 주소는 특히 인터넷 이용자가 방문한 인터넷사이트와 그의 온라인 활동을 포괄적으로 추적하는데 이용될 수 있으므로, 이 데이터는 이용자의 상세한 프로필 작성을 가능하게 한다는 것이다. 따라서 그러한 추적에 필요한 IP 주소의 보관과 분석은 기본권 헌장이 규정한 인터넷 이용자의 사생활존중권(제7조)과 개인정보보호권(제8조)의 중대한 제약이라고 보았다.[29] 또한 이메일 서비스는 보관의무규정에 포함되지 않는다 하더라도, 전체 트래픽 데이터 중 일부에 지나지 않는다고 한다.[30]

또한 데이터 보관에서 제외되는 종교적 사회적 영역에서 상담 등의 업무에 종사하는 사람의 대상은 단지 1,300 곳에 불과하며, 이는 독일 전체 전기통신서비스 이용자 중 경미한 부분에 해당된다고 한다. 특히 업무상 비밀을 준수해야 하는 사람들(예컨대 변호인, 의사, 언론인 등)의 트래픽데이터가 보관에서 제외되지 않고 있다는 점도 지적하였다.[31] 심지어 트래픽데이터 보관조항은 간접적으로도 형사소추의 원인을 제공할 수 있는 상황에 있지 않는 거의 모든 사람들이 관련되어 있다고 한다. 이러한 규정은 또한 이유없이, 인적, 시간적 그리고 지리적 구분없이 대부분의 트래픽데이터와 위치데이터가 일반적으로 저장되고 있다고 한다.[32]

이러한 이유에서 독일의 트래픽데이터 보관 의무는 독일 정부의 주장이나 연방행정대법원의 견해와 달리 사법재판소가 예외로 제시한 '대상 특정 데이터 보관'으로 간주될 수 없다.[33]

나. 데이터의 보관기간

지침 제15조 제1항 제2문에서 일반적이고 구분없는 데이터보관의무를 부과하는 국내입법조치의 보관기간은 제한되어야 한다.[34] 독일 전기통신법 제113b조에 의해서 위치데이터의 경우 4주, 기타 데이터의 경우 10주로 규정하고 있다. 그런데 이 기간들은 그동

29) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 79.
30) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 80.
31) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 82.
32) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 83.
33) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 84.
34) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 85.

안 사법재판소가 다른 국가의 판결[35]에서 다룬 기간보다 훨씬 짧다.[36]

하지만 사법재판소는 전자적 통신수단 이용자의 통신에 관한 정보 또는 그가 사용한 단말기의 위치에 관한 정보를 제공할 수 있는 트래픽데이터 또는 위치데이터의 보관은, 전체 데이터가 관련된 자의 사생활을 정확하게 추론하게 하는 한, 보관기간의 길이와 보관된 데이터의 양과 종류에 상관없이 기본권 제약은 중대하다고 하였다.[37]

그러한 점에서 보관된 트래픽데이터의 양이 제한적이거나 보관기간이 짧더라도 이러한 보관자체는 전자적 통신수단 이용자의 사생활에 관한 매우 정확한 정보를 제공할 수 있다고 한다. 또한 보관된 데이터의 량과 이로부터 도출되는 매우 정확한 관련자의 사생활에 관한 정보는 문제의 데이터를 조사한 후 비로소 판단될 수 있다. 하지만 데이터의 보관에서 나오는 기본권 제약은, 필연적으로 데이터와 이로부터 도출되는 정보가 조사되기 이전에 행해진다. 따라서 보관에 존재하는 기본권 제약의 비중의 판단은 반드시 보관되어 있는 데이터의 범주와 일반적으로 관계되는 당사자의 사생활의 위험을 근거로 행해지고, 게다가 이로부터 도출되는 사생활에 관한 정보가 실제로 민감한 성격을 가지는지는 중요하지 않다[38]고 한다.

따라서 10주 내지 4주간 보관되는 전체 트래픽데이터와 위치데이터는 자신의 데이터가 저장되는 사람의 사생활에 대한 정확한 추론과 특히 이 사람의 프로필의 작성을 가능하게 할 수 있다[39]고 판단하였다. 이러한 이유로 독일의 트래픽데이터 보관조항들이 EU 법과 일치할 수 없다.

4. 중대한 범죄의 대응과 공공안전의 중대한 위험 방지를 위해 허용되는 입법조치

사법재판소는 형사소추의 실효성은 일반적으로 일부의 수사절차에 달려있지 않고, 관할 국내 관청이 이러한 목적을 이용하는 모든 수사수단에 달려있다고 전제한 다음,[40]

35) EuGH, Urteil vom 21.12.2016, C-203/15, C-698/15, Tele2 Sverige und Watson ua; EuGH, Urteil vom 6.10.2020, C-511/18, C-512/18, C-520/18, La Quadrature du Net ua/Premier ministre ua; EuGH, Urteil vom 5.4.2022, C-140/20, Commissioner of the Garda Síochána ua.
36) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 86.
37) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 88.
38) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 89.
39) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 90.

지침 제15조 제1항은 기본권 헌장 제7조, 제8조, 제11조 그리고 제52조 제1항의 관점에서 해석하는 경우 중대한 범죄의 대응과 공공안전의 중대한 위협을 방지하기 위한 일정한 입법조치는 허용될 수 있다고 하였다. 사법재판소는 허용되는 입법조치로서 우선 대상이 특정된 트래픽데이터의 보관과 특정한 데이터의 신속 보관 명령을 제시하였다. 또한 전자적 통신수단의 이용자의 신원확인과 관련한 데이터와 통신접속의 발신지에 할당되는 IP주소는 일반적이고 구분없이 보관할 수 있다고 하였다.[41]

가. 이용자의 신원확인 관련 데이터의 일반적 보관

이용자의 신원확인과 관련한 데이터의 일반적인 보관은 허용된다. 즉 전자적 통신수단 이용자의 신원과 관련한 데이터가 중대범죄에 속하는 범죄의 예비 또는 실행과 관련하여 그러한 통신수단을 사용한 자를 식별하는 것을 가능하게 하는 경우에는, 이러한 데이터의 보관은 중대 범죄의 대응에 기여할 수 있다[42]는 것이다. 이 경우 중대 범죄가 아닌 '일반 범죄'에 대응할 목적으로 신원확인과 관련한 데이터의 일반적 보관도 인정한다. 예를 들어 선불 심카드와 같이 전자적 통신수단의 취득 시 판매자가 구매자의 신분을 증명하는 공문서를 검토하고 판매자는 경우에 따라서 관할 국내 관청에 구매자의 정보를 제공할 의무가 있다.[43]

나. 발신지 IP주소의 일반적 보관

통신접속의 출처(발신지)인 IP주소의 일반적 보관은 기본권 헌장의 사생활존중권(제7조)과 개인정보보호권(제8조)의 중대한 제약이다. 왜냐하면 IP주소는 해당 전자적 통신수단의 이용자의 사생활을 정확하게 추론할 수 있고, 기본권 헌장 제11조에 규정된 표현의 자유의 행사와 관련하여 위축효과를 초래할 수 있기 때문이다.

하지만 사법재판소는 발신지 IP주소의 일반적 보관을 허용하고 있다. 서로 충돌하는 권리와 정당한 이익 사이에 균형을 유지하기 위해서 인터넷에서 범해지고 있는 범죄의

40) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 96.
41) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 97.
42) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 98.
43) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 99.

경우, 특히 인터넷에서 아동포르노의 취득, 배포, 전달, 제공[44]의 경우 IP주소는 범죄가 범해졌을 때 이 주소가 할당된 자의 신분을 수사하는 것을 가능하게 하는 유일한 근거가 될 수 있기 때문이다.[45]

따라서 사법재판소는 통신접속의 출처(발신지)인 IP주소의 일반적이고 구분 없는 보관을 정하고 있는 법규정은, 기본적으로 기본권 헌장 제7조, 제8조, 제11조 및 제52조 제1항을 고려하면 지침 제15조 제1항에 위반되지 않는다고 판단하였다. 다만, 이러한 법규정은 이러한 데이터의 이용을 규율하는 실체적 절차적 요건을 엄격히 준수해야 한다.[46]

이러한 데이터 보관과 관계되는 기본권 헌장의 사생활존중권과 개인정보보호의 제약의 중대성을 고려하면, 국가안보, 중대한 범죄의 대응, 공공의 안전에 대한 중대한 위협의 방지에 한해서는 이러한 제약이 정당화될 수 있다. 또한 저장기간은 추구되는 목적과 관련하여 절대적으로 필요한 범위를 넘어서는 안 된다. 끝으로 이러한 입법조치는 관련자의 온라인 통신 및 온라인 활동과 관련하여 이러한 데이터의 사용에 관한, 특히 추적의 형태에 관한 엄격한 요건과 보장을 규정해야 한다.[47]

다. 대상 특정 보관(targeted retention)

사법재판소는 중대 범죄의 대응과 공공 안전의 중대한 위협 방지를 위해서 일반적이고 구분없는 트래픽데이터를 보관할 수 없지만, 절대적으로 필요한 기간 내에 특정한 사람 또는 지리적 장소를 대상으로 하는 데이터 보관 조치는 지침 제15조에서 허용될 수 있다고 하였다.

(1) 인적 기준

객관적 기준에 근거하여 특정된 자의 트래픽데이터와 위치데이터가 적어도 중대한 범죄와 간접적인 관계를 드러내거나 중대 범죄의 대응에 원인을 제공하거나 공공의 안전에

44) 지침 2011/93/EU 제2조c (ABl. 2011, L 335, S. 1, 개정: ABl. 2012, L 18, S. 7.).
45) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 100.
46) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 101.
47) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 102.

대한 중대한 위험이나 국가안보에 대한 위험을 방지하기에 적합한 경우 이 자의 트래픽 데이터를 보관하는 입법조치는 지침 제15조 제1항에 의해서 허용된다.[48]

이 경우 객관적 기준은 중범죄의 예방, 수사, 확인, 소추를 위해서 관련되는 각 조치의 성격에 따라서 다양할 수 있지만, 예를 들어 특히 이전에 관련 국내 절차에서 그리고 객관적이고 차별 없는 기준에 의해서 해당 회원국의 공공 안전이나 국가안보에 위협을 가한 것으로 확인된 자는 이 조치의 대상이 될 수 있다.[49]

따라서 회원국은 특히 이러한 확인을 근거로 현재의 수사나 다른 감시조치의 대상이거나 재범 위험성이 높은 중대 범죄의 전과자로서 국내 범죄등록부에 기록되어 있는 자를 특정하여 이들의 데이터를 보관하는 조치를 할 수 있다. 그러한 확인은 물론 국내법에서 정해진 객관적이고 차별없는 기준에 근거하고 있어야 정당화될 수 있다.[50]

(2) 지리적 기준

대상 특정 보관 조치는, 국내 관할기관이 객관적이고 차별없는 근거에서 하나 또는 다수의 지리적 영역에서 중대 범죄의 예비 또는 실행의 위험이 높아진 정황이 존재하는 경우에도 국내 입법자의 선택에 따라 그리고 비례성원칙을 엄격히 준수하여 지리적 기준에 근거할 수도 있다. 이러한 장소에는 특히 중대한 범죄의 발생률이 높은 장소나 중대 범죄가 발생할 위험이 특별히 높은 장소가 속한다. 후자의 경우에는 일반적으로 많은 사람들이 방문하는 장소나 시설과 같은 곳으로서 공항, 항구, 기차역 또는 톨게이트와 같은 전략적 장소가 포함된다.[51]

또한 국내 관할기관은, 위에서 언급한 장소에서 지리적 기준을 토대로 특히 어떤 지리적 영역의 평균 범죄율을 토대로 대상 특정 보관 조치를 할 수도 있다. 이 경우 국내 관할기관이 해당 영역에서 중대 범죄의 예비나 실행을 위한 구체적인 근거를 반드시 가지고 있어야 하는 것은 아니다. 그러한 기준에 근거하는 대상 특정 보관은, 관련 중범죄와 개별 회원국의 독자적인 상황에 따라서 중대 범죄의 발생률이 높은 장소와 관련될

48) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 105.
49) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 106.
50) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 107.
51) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 108.

뿐 아니라 그러한 범죄의 실행에 특별히 취약한 장소도 관련될 수 있기 때문에, 대상 특정 보관은 기본적으로 차별을 야기하지 않을 수 있다고 한다. 왜냐하면 중대 범죄의 평균 발생률 기준 그 자체는 잠재적으로 차별하는 요소와 전혀 관련이 없기 때문이다.[52]

그리고 특히 정기적으로 매우 많은 사람들이 왕래하는 장소 및 시설과 관련한 대상 특정 보관이나 공항, 기차역, 항구 또는 톨게이트와 같은 전략적 장소와 관련한 대상 특정 보관의 경우 관할 관청은 특정 시점에 이 장소에서 전자적 통신수단을 이용한 모든 사람들의 트래픽데이터와 특히 위치데이터를 수집할 수 있다고 한다. 그러한 대상 특정 보관 조치를 통해서 관할 관청은 보관 데이터에 접근할 수 있고 그리하여 이러한 조치와 관련되는 장소나 지리적 영역에 이러한 사람이 있었다는 정보나 이러한 장소나 지리적 영역 내에서 또는 사이에서 이 사람의 이동에 관한 정보를 확보할 수 있고, 나아가서 이로부터 중대 범죄의 대응 목적으로 보관기간 동안 특정 시점에 이 장소 또는 이 지리적 영역에서 그 사람이 있었다는 사실과 그의 활동에 관한 추론을 할 수 있다[53]고 한다.

대상 특정 보관과 관계되는 지리적 영역은, 그 선택을 정당화하는 조건들이 변경되는 경우에는 변경될 수 있고 사정에 따라서 변경되어야 한다. 그리하여 특히 중대한 범죄의 대응에서 새롭게 전개된 국면에 대처할 수 있다. 따라서 대상 특정 보관 조치의 기간은 추구하는 목적 및 이를 정당화하는 상황을 고려하면 절대적으로 필요한 한도를 넘어서는 안 된다. 하지만 그러한 보관의 요건이 계속 존재하는 경우 연장할 수 있다.[54]

(3) 기타 기준

언급한 인적, 지리적 기준 외에도 대상 특정 보관의 범위가 절대적 필요성으로 제한되는 것을 확보하고 중범죄와 데이터가 보관되는 자 사이에 적어도 간접적 관계를 생성하기 위해서 다른 객관적이고 차별없는 기준도 고려될 수 있다. 이러한 기준을 정하는 것은 지침 제15조 제1항에 의해서 회원국의 업무이다.[55] 하지만 대상 특정 보관이 수행될 수 있는 사례와 조건을 정확하게 규정하는데 어려움이 존재한다고 해서 회원국이 예외를

52) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 109.
53) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 110.
54) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 111.
55) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 112.

원칙으로 하여 일반적이고 구분없는 트래픽데이터와 위치데이터의 저장을 규정하는 것은 정당화될 수 없다[56]고 한다.

라. 신속 보관(the expedited retention)

보관된 트래픽데이터는 기본적으로 법률상 보관 기간이 지나면 삭제되거나 익명으로 처리되어야 한다. 하지만 해당 트래픽데이터가 처리되어 보관되는 동안 중대한 범죄나 국가안보의 침해를 규명하기 위해서 이 기간을 넘어서 보관될 상황이 발생할 수 있다. 사법재판소는 이와 같은 기간이 초과된 경우에도 보관을 인정하고 있다. 이것은 범죄나 국가안보침해가 이미 확인될 수 있었던 경우는 물론 모든 관련된 사정을 객관적으로 검토하여 범죄나 안보침해가 존재한다는 근거있는 혐의가 존재하는 경우에 가능하다.[57]

이런 상황에서 충돌하는 권리와 정당한 이익이 서로 균형을 이루어야 한다는 점을 고려할 때, 회원국은 지침 제15조 제1항에 의해서 효과적인 법원의 통제를 전제로 관할 관청이 전기통신사업자에게 정해진 기간 동안 그가 보유하고 있는 트래픽데이터를 신속하게 보존하는 것을 의무로 부과하는 입법조치를 할 수 있다.[58]

이러한 신속 보관의 목적은 해당 데이터가 원래 수집되어 저장된 목적과는 더 이상 상응하지 못하고, 기본권 헌장 제8조 제2항에 의해서 모든 데이터는 정해진 목적으로 처리되어야 하기 때문에, 회원국은 입법조치에서 어떤 목적으로 데이터의 신속한 보존이 행해질 수 있는지를 정해야 한다. 기본권 헌장 제7조와 제8조의 기본권은 그러한 보관과 관계될 수 있어서 이로 인한 기본권 제약의 중대성을 고려하면, 이러한 조치와 보관데이터에 대한 접근이 절대적 필요성의 한계를 준수하는 경우, 오로지 중대한 범죄의 대응과 특히 국가안보만이 이러한 제약을 정당화할 수 있다[59]고 한다.

이러한 보관 조치는 이전에 해당 회원국의 공공안전 또는 국가안보에 위협적인 것으로 확인된 자 또는 중대 범죄를 범했거나 국가안보를 침해하였다는 구체적인 혐의가 있는 자의 데이터로 제한할 필요는 없다고 한다. 그러한 조치는 입법자의 선택에 따라서

56) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 113.
57) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 114.
58) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 115.
59) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 116.

절대적 필요성의 한계를 준수하여 중대한 범죄나 국가안보의 침해를 계획하고 있거나 계획하였다는 혐의가 있는 자가 아닌 자로 확대될 수 있다고 한다. 다만 이러한 데이터가 객관적이고 차별없는 기준을 토대로 그러한 범죄의 규명이나 국가안보의 침해를 규명하는데 기여할 수 있어야 한다. 여기에는 그러한 범죄 피해자의 데이터나 그의 사회적 또는 직업상 환경에 관한 데이터가 해당된다.[60]

따라서 입법조치는, 특히 피해자가 공공 안전에 대한 중대한 위협이 발생하기 전에 또는 중대 범죄가 범해지기 전에 그의 전자적 통신수단을 사용하여 접촉을 한 자의 트래픽데이터와 위치데이터를 신속하게 보관할 것을 전자적 통신서비스 제공자에게 명하도록 허용할 수 있다.[61]

그러한 신속보관은 또한 범죄의 실행 및 예비 장소 또는 해당 국가안보의 침해 장소와 같은 특정한 지리적 영역으로 확대될 수 있다. 그러한 조치의 대상은, 예를 들어 중대 범죄의 피해자가 사라진 장소와 관련되는 트래픽데이터와 위치데이터일 수도 있다. 다만, 이 조치 및 이러한 방법으로 보관된 데이터에 대한 접근은, 중대 범죄의 대응 또는 국가안보를 위해서 절대적 필요성의 한계를 준수해야 한다.[62]

또한 지침 제15조 제1항에 의해서 관할 국내 관청은 공공 안전의 중대한 위협이나 가능한 중범죄와 관련하여 이미 수사의 첫단계에서, 즉 이 관청이 국내법의 관련 규정들에 의해서 그러한 수사를 수행할 수 있는 시점부터 신속한 보관을 명령할 수 있다.[63]

트래픽데이터와 위치데이터의 다양한 보관 조치는 국내 입법자의 선택에 따라 그리고 절대적 필요성의 한계를 준수하여 함께 사용할 수 있다. 이러한 상황에서 지침 제15조 제1항은 기본권 헌장 제7조, 제8조, 제11조 및 제52조 제1항을 고려하여 이러한 조치의 결합을 배제하지 않는다.[64]

마. 조치의 비례성 준수

지침 제15조 제1항에 의한 입법조치는 적합성, 필요성, 균형성을 모두 갖추어야 한

60) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 117.
61) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 118.
62) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 119.
63) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 120.
64) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 121.

다.[65] 따라서 중대한 범죄의 대응은 공공 안전의 보장에 상당히 중요하고 그 실효성은 대부분 현대 수사기술의 이용에 달려있다고 하지만, 그러한 공익 목적 자체가 트래픽데이터와 위치데이터의 일반적이고 구분없는 보관 조치의 필요성을 정당화할 수는 없다.[66] 그뿐만 아니라 범죄에 실효적으로 대응하기 위한 규정을 제정하는 회원국의 적극적 의무라고 하더라도, 관련된 자의 데이터가 추구하는 목적과 적어도 간접적인 관계도 드러내지 않는 상황에서 거의 모든 국민의 트래픽데이터와 위치데이터의 보관을 규정하고 있는 국내 법규정은 기본권 헌장 제7조와 제8조의 기본권의 중대한 제약을 정당화할 수 없다.[67]

Ⅴ. 유럽사법재판소 판결의 평가 및 전망

유럽연합은 통신데이터보관지침(2006/24/EC)을 통해서 전기통신사업자의 트래픽데이터 보관의무를 처음으로 도입하였다. 하지만 이러한 트래픽데이터 보관의무는 독일을 비롯한 유럽연합 회원국 내에서 기본권 침해와 관련하여 최근까지 지속적으로 문제가 되었다. 독일 입법자는 트래픽데이터 보관의무를 '2007.12.21의 전기통신감시의 새로운 규정을 위한 법률'[68]을 통해서 이 지침을 전기통신법에서 이행하였다. 독일 연방헌법재판소는 2010.3.2 이 법률의 트래픽데이터 보관의무 조항들이 기본법(헌법)에 위반되어 무효라고 판결하였다.[69] 유럽사법재판소도 2014.4.8. 이 지침은 EU법에 위반되어 무효라고 선언하였다.[70] 사법재판소는 이 판결에서 세계평화와 국제적 안전보장을 위하여 국제테러 대응 및 공공안전 보장을 위한 중대한 범죄의 대응은 EU의 공익목적이지만, 이 자체가 트래픽데이터의 보관을 정당화할 수는 없다고 선언한 것이다.

그럼에도 불구하고 독일 입법자는 '2015.12.10. 트래픽데이터 보관의무 및 최고보관

65) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 122.
66) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 123.
67) EuGH, Urteil vom 20.09.2022 - C-793/19, C-794/19, Rn. 124.
68) BGBl. I 2007, S. 3198.
69) BVerfG, Urteil vom 02. März 2010 - 1 BvR 256/08 -.
70) EuGH, 08.04.2014 - C-293/12 und C-594/12; 민영성/박희영, 유럽사법재판소의 통신정보보관지침의 무효 판결과 그 시사점, 법학연구 제56권 제4호, 부산대학교 법학연구소, 2015, 53-82.

기간의 도입 법률'을 통하여 연방헌법재판소와 유럽사법재판소의 판결을 참조하여 트래픽데이터 보관의무를 다시 도입하였다.[71] 이 법률을 통해서 전기통신법에 도입된 트래픽데이터 보관의무는 그 기간을 종전의 6개월에서 위치데이터의 경우 4주, 나머지 트래픽데이터는 10주로 줄였고, 성직자 등과의 상담에 관한 데이터를 제외하였으며, 이메일 및 웹이용의 URL 주소의 수집도 제외하였다. 그뿐만 아니라 데이터를 사용할 기관의 권한을 분명히 하였고, 보관된 데이터에 대한 특별한 보호조치도 마련하였다. 2019.6.23. 전기통신현대화법(TKMoG)에 의해서 전기통신법이 개정되었으나 트래픽데이터보관조항은 기존의 제113a조 내지 제113g조에서 현재의 제175조 내지 제181조에 내용 변경없이 그대로 유지되었다. 이번 유럽사법재판소의 심판 대상은 개정 전 전기통신법 제113a조 내지 제113g조이지만, 개정된 제175조 내지 제181조에도 적용된다.[72] 따라서 개정된 규정들은 EU법에 위반되므로 더 이상 적용될 수 없다.

한편 유럽사법재판소가 2014년 통신데이터보관지침을 무효라고 판결하였지만, 이 지침을 국내법으로 이행한 트래픽데이터 보관조항은 여전히 회원국 내에서 집행되고 있었다. 그 근거는 전자프라이버시지침 제15조 제1항이다. 앞서 살펴본 바와 같이 지침 제15조 제1항은 통신내용이나 트래픽데이터의 보호를 일정한 경우 제한할 수 있는 입법조치를 회원국에 허용하기 때문이다. 하지만 이러한 입법조치가 구체적인 이유나 구분없이 전체 국민의 트래픽데이터를 포괄적으로 사전에 저장하여 보관하는 것도 허용하는지 문제가 되었다. 특히 보관의무를 이행해야 하는 전기통신사업자들은 이러한 입법조치가 허용될 수 없다는 입장이었다. 그리하여 다수 회원국에서 트래픽데이터의 보관의무와 관련한 법적 분쟁이 제기되었고, 결국 유럽사법재판소의 선결재판을 받게 되었다. 회원국 내에서 EU법의 적용이 문제된 사안에서는 EU법이 우선 적용되기 때문이다.

유럽사법재판소가 전자프라이버시지침 제15조 제1항과 관련하여 트래픽데이터 보관의무규정을 처음으로 다룬 사건은 2016.12.21 스웨덴 및 영국의 통신데이터 보관에 관한 법률이다. 사법재판소는 이들 국가의 트래픽데이터 보관조항들이 일반적으로 모든 통신가입자 및 등록된 이용자에 적용되고 모든 전자적 통신수단 및 전체 트래픽데이터를

71) BGBl. I 2015, S. 2218; 민영성/박희영, 독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점, 부산대학교, 법학연구 제57권 제2호, 통권 88호, 2016.6, 89-109.

72) Roßnagel, Vorratsdatenspeicherung - was geht noch und was nicht mehr?, ZD 2022, 650.

포함하고 추구하는 목적에 따라서 구분이나 제한 또는 예외를 규정하지 않아 절대적 필요성의 한계를 넘어서므로 지침 제15조에 위반된다고 판결하였다.[73] 하지만 이 판결에서는 지침 제15조 제1항에서 허용되는 예외를 전혀 언급하지 않았다.

그 후 사법재판소는 2020.10.6 프랑스, 벨기에 및 영국의 통신데이터보관에 관한 법률의 판결에서 일반적이고 구분없는 트래픽데이터 및 위치데이터의 보관은 기본권 제약이 절대적 필요성으로 제한되지 않았기 때문에 기본적으로 EU법과 일치하지 않는다고 판결하였다.[74] 하지만 사법재판소는 이러한 원칙에서 엄격한 요건으로 허용되는 예외를 지침 제15조 제1항에서 처음으로 도출하였다. 이러한 예외는 그 후 2021.3.2 에스토니아 통신데이터보관법 판결[75], 2022.4.5 아일랜드 통신데이터보관법 판결[76]에서 확인되었으며, 이번 독일 판결에서 이러한 예외를 더욱 구체화하여 재확인하였다. 이러한 사법재판소의 입장은 2022.11.17. 불가리아 통신데이터보관법에 관한 판결에서 다시 한번 확인되었다.[77]

이러한 일련의 판결로 이제 EU내에서는 일반적이고 구분없이 모든 국민들의 트래픽데이터를 포괄적으로 보관하는 규정은 법적으로 허용되지 않게 되었다. 다만, 사법재판소가 기본권 헌장의 여러 기본권과 지침 제15조의 해석을 통해서 엄격한 요건에서만 예외적으로 가능하게 되었다. 이러한 예외적 허용은 기존의 트래픽데이터 보관제도와는 완전히 다른 성격과 유형을 가지게 된 것이다.[78]

---

73) EuGH, Urteil vom 21.12.2016, C-203/15, C-698/15, Tele2 Sverige und Watson ua.(이에 대한 소개는 박희영, 통신사실확인자료의 일반적인 보관의무는 EU법과 일치하지 않는다, 최신독일판례연구, 2017.12, 로앤비, 1-9).

74) EuGH, Urteil vom 6.10.2020, C-511/18, C-512/18, C-520/18, La Quadrature du Net ua/Premier ministre ua)(이에 대한 소개는 박희영, 프랑스 국가안전법: 통신사실확인자료의 '일반적' 보관의무는 EU법에 위반되지만, '예외적'으로 허용, 독일법제동향, 2020.10, 로앤비, 1-6).

75) EuGH, Urteil vom 2.3.2021, C-746/18, Vorabentscheidungsersuchen des Riigikohus Estland (이에 대한 소개는 박희영, 통신사실확인자료는 중대한 범죄나 공공의 안전에 대한 진지한 위험이 있는 경우에만 보관될 수 있다. 독일법제동향, 2021.3, 로앤비, 1-8).

76) EuGH, Urteil vom 5.4.2022, C-140/20, Commissioner of the Garda Síochána ua (이에 대한 소개는 박희영, 유럽사법재판소: 중대범죄에 대응하기 위해서 일반적이고 구분없는 통신사실확인자료의 보관은 EU법에 위반됨(아일랜드 통신사실확인자료 사건), 독일법제동향, 2022.4, 로앤비, 1-7).

77) EuGH, Urteil vom 17.11.2022, C-350/21, Spetsializirana prokuratura u.a.

78) 특히 대상 특정 트래픽데이터 보관이나 신속보관명령은 사실상 입법행위나 다름없어 보인다. EU지침은 그 대강만을 정하고 구체적인 내용은 회원국의 국내법에서 정하도록 되어 있다. 이러한

독일 정부와 유럽사법재판소에 선결재판을 제청한 연방행정대법원은 독일 규정의 경우 보관기간이 다른 국가와 비교하여 상대적으로 매우 짧고, 이메일 서비스나 인터넷 이용 데이터는 보관에서 제외되며, 성직자 등 일정한 범위의 사람의 데이터도 제외되며, 중대한 범죄 등으로 이용이 제한되어 있고, 데이터 보관 및 접근에 대한 보호조치가 되어 있다는 점에서 EU법과 일치한다는 판결을 기대하였다. 하지만 유럽사법재판소는 이러한 기대와 달리 일반적이고 구분없는 데이터 보관 자체가 EU기본권 헌장이 규정하고 있는 기본권을 침해한다는 점에 방점을 두고 있다. 유럽사법재판소는 비례성원칙에 따라 비교형량을 한 다음 유럽시민의 기본권 보호가 우선되어야 한다고 천명한 것이다.

이번 사법재판소가 자신의 기존 입장을 재확인함으로써 EU 내에서 전기통신사업자가 트래픽데이터를 일반적이고 구분없이 예방적으로 보관할 수 없게 되었고 엄격한 요건에서 예외적으로만 허용되게 되었다. EU 회원국은 이제 사법재판소가 허용한 예외기준에 따라서 새로운 트래픽데이터 보관제도를 도입해야 한다.

특히 사법재판소 판결은 독일의 관련 규정에 직접 효력을 가지므로 독일 연방법무부는 그 후속조치로서 '형사소송에서 트래픽데이터의 보존명령 도입 법률안 초안'[79]을 이미 제안하였다. 이 초안은 트래픽데이터의 보관 및 이용 등에 관한 규정인 전기통신법 제175조 내지 제181조와 범죄수사를 위해서 이에 접근할 수 있는 규정인 형사소송법 제100g조 제2항을 폐지하고, 이미 존재하는 트래픽데이터와 장래에 생성되는 트래픽데이터의 수집과 신속보존명령제도(초안 제100g조 제5항)를 도입하는 것을 주요 내용으로 한다. 이 법률안 초안에는 연방내무부의 위험방지기관의 접근 권한이 보완될 것으로 예상된다. 따라서 연방정부 법률안으로 확정되어 연방의회에 제출되기까지 상당한 시일이 걸릴 것으로 보인다.

배경에서 사법재판소의 지침에 관한 해석권한의 범위는 때로는 입법행위와 구분하기 어려운 경우가 있다. 대표적인 사례가 이용자의 저작권 침해에서 플랫폼 제공자의 책임을 전통적인 국내법 이론에 따르면 과실 방조책임에 해당되는 사례를 행위자책임으로 인정한 것이다. 형법적 관점에서 보면 불가벌인 과실방조자를 정범으로 격상시킨 것이다. 이후 이 판례의 법리는 EU DSM 지침으로 제정되었다. 유럽사법재판소의 EU법 해석의 한계는 중요한 법적인 연구주제이지만 여기서는 다루지 않는다.

79) Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung (https://kripoz.de/wp-content/uploads/2022/10/refE-quick-freeze.pdf)(2023. 2.22. 방문). 이에 대한 소개로는 박희영, 연방법무부: 형사소송에서 통신사실확인자료의 보존명령 도입 법률안, 독일법제동향, 2022.11, 로앤비, 1-9.

한편 사법재판소도 인정하였듯이 예외적 허용 기준들을 구체적으로 입법하는 것은 상당히 어려울 수 있다. 이러한 점에서 EU에서 새로운 트래픽데이터 보관제도의 도입을 추진하고 있는 독일의 입법조치는 다른 회원국에 입법모델로 작용할 것으로 보인다. 그렇다 하더라도 허용된 예외에 따라 도입된 회원국의 입법조치가 EU법에 일치하는지에 대해서 앞으로 사법재판소에 선결재판을 제청할 것도 예상된다.

한편 EU는 현재 전자프라이버시 '지침'(Directive) 대신 전자프라이버시 '규칙'(Regulation)[80]을 제정하기 위한 입법절차를 진행하고 있다. 집행위원회가 제출한 전자프라이버시규칙안에는 트래픽데이터 보관과 관련한 구체적인 조항은 포함되어 있지 않지만, 전자프라이버시지침 제15조의 본질적인 내용을 유지하고 있다(규칙안 제11조). 규칙안은 사법재판소의 판례와 일치하는 경우 특히 대상 특정 보관제도를 도입하는 것은 회원국에 허용하고 있다.[81]

Ⅵ. 통신사실확인자료 보관조항의 법적 성질의 관점에서 본 형사정책적 시사점

유럽사법재판소는 아무런 이유없이 전체 국민의 트래픽데이터를 포괄적으로 보관하여 국가기관이 제공할 수 있도록 의무를 부과한 독일의 트래픽데이터 보관조항은 유럽연합 기본권 헌장이 보장하고 있는 사생활존중권(제7조), 개인정보보호(제8조), 표현의 자유(제11조)와 일치할 수 없다고 판결하였다. 따라서 이러한 보관의무규정은 더이상 효력을 가질 수 없게 되었다.

유럽사법재판소의 판결 대상인 독일 전기통신법의 트래픽데이터 보관조항은 우리 통신비밀보호법의 통신사실확인자료 보관조항과 거의 유사한 방식으로 규정되어 있다. 따라서 유럽사법재판소의 판결은 우리 통신비밀보호법의 통신사실확인자료 보관조항의 위

80) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final 2017/0003(COD).

81) 앞의 전자프라이버시규칙안(각주 80), 3.

헌성 여부를 논의할 수 있는 계기를 제공하고 있다. 보관조항의 위헌성은 보관을 전제로 한 제공조항의 위헌성도 당연히 문제된다.

독일의 트래픽데이터 보관조항의 핵심은 아무런 이유없이(특히 범죄혐의도 없이) 거의 모든 국민의 전체 트래픽데이터를 의무적으로 보관하여 수사기관 등에 제공할 수 있다는 점에 있다. 그렇다면 우리 통신사실확인자료 보관조항이 독일과 마찬가지로 전기통신사업자에게 보관의무를 강제로 부여한 것인가?

그동안 통신사실확인자료의 보관의 법적 근거와 법적 성질이 무엇인지에 대한 선행연구는 거의 존재하지 않는다.[82] 헌법재판소도 2018년 실시간 위치정보의 제공에 대한 요청조항의 위헌성만을 다루었다. 통신비밀보호법은 통신사실확인자료, 이의 제공요청조항 그리고 이와 관련하여 전기통신사업자의 협조의무로서 보관기간을 정하고 있고, 이의 법적 근거나 법적 성질을 직관적으로 알 수 있는 조항들을 두고 있지 않다.

하지만 통신사실확인자료는 민감한 개인정보라는 점에서 개인정보보호법과 통신비밀보호법의 관계를 연혁적, 체계적으로 고찰해 보면 그 해답을 찾을 수 있다. 1999년 정보통신망법[83]에 정보통신서비스제공자의 이용자 개인정보보호조항이 처음 도입되었다. 이 조항의 도입으로 전기통신사업자는 이용자의 동의없이 개인정보를 수집할 수 있게 되었다. 이러한 예외사유는 세 가지로 규정되어 있다. 첫째, 이 법 또는 다른 법률에 특별한 규정이 있는 경우, 둘째, 정보통신서비스 이용계약의 이행을 위하여 필요한 경우, 셋째, 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우이다. 통신서비스 이용계약의 이행과 요금정산은 통신사실확인자료의 수집과 관련된다. 통신서비스의 제공으로 통신사실확인자료는 자동으로 생성되고 요금정산을 위한 근거가 된다. 전기통신사업자는 이러한 통신사실확인자료를 이러한 목적으로 수집하여 보관할 수 있다. 이 조항은 여러 번 개정되면서 내용이 보완되었지만, 본질적 내용은 변경되지 않았다. 마침내 이 조항은 2020년 정보통신망법이 개인정보보호법에 통합되면서 개인정보보호법 제39조의2에서 다시 규정되었다. 이 통합으로 정보통신망법에만 적용될 수 있는 조항들은 개인정보보호법 제6장(정보통신서비스 제공자 등의 개인정보 처리 등 특례)의 특례조항에 규정되

82) 통신비밀보호법 제15조의2 및 동법 시행령 제41조의 보관기간이 법적의무라는 견해로는 최호진, "저장된 데이터의 보전명령제도 도입을 위한 시론(試論)", 형사정책 제31권 제2호(통권 제58호: 2019.7.), 304면; 박소현(a), 앞의 논문(각주 2), 196.

83) 정보통신망 이용촉진 등에 관한 법률 [시행 1999. 7. 1.] [법률 제5835호, 1999. 2. 8., 전부개정].

었고, 나머지 조항들은 개인정보보호법의 일반조항에 규정되었다.[84]

전기통신사업자는 이렇게 수집한 통신데이터를 수집목적이 달성된 경우 지체없이 파기해야 한다(1999년 정보통신망법 제17조 제3항, 개인정보보호법 제21조). 만일 수집목적을 달성하였음에도 불구하고 개인정보를 파기하지 아니한 경우에는 제재를 받게 된다(1999년 정보통신망법 제32조 제1항 제5호의 과태료 처분, 개인정보보호법 제73조 제1호의2의 형사처벌). 그러나 개인정보가 다른 법령에 따라 보존되어야 하는 경우에는 이를 파기해서는 안된다(제21조 제1항 단서). 개인정보처리자가 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다(개인정보보호법 제21조 제3항). 이를 위반한 경우 과태료 처분을 받게 된다(제75조 제4항 제1호).

이러한 법적 상황에서 통신비밀보호법의 통신사실확인자료 제공요청조항들을 대입해 보면 법적 근거와 법적 성질의 퍼즐이 완성된다. 2001년 통신비밀보호법에 통신사실확인자료 제공요청조항이 도입되면서, 1999년 정보통신망법에 의해서 이미 수집되어 보관되어 있는 통신사실확인자료 중 통신비밀보호법 제2조 제11호에 열거된 통신사실확인자료는 수사기관 등의 요청에 제공될 수 있고, 이러한 제공을 위해서 전기통신사업자의 협조의무와 통신사실확인자료의 보관기관이 명시되었다. 특히 보관기간을 명확히 함으로써 전기통신사업자는 영업목적으로 수집한 통신사실확인자료를 삭제하지 못하고, 이 기간 동안 강제로 보관해야 할 법적의무를 지게 되었다. 따라서 통신사실확인자료보관의 수집 및 보관의 법적 근거는 개인정보보호법이며 보관의 법적 의무는 통신비밀보호법 제15조의2 및 동법 시행령 제41조의 보관기관과 개인정보보호법 제21조의 보존의무에서 나온다.[85] 통신비밀보호법과 개인정보보호법의 관련 규정이 결합함으로써 개인정보 수집의 목적변경을 통하여 모든 국민의 통신사실확인자료가 아무런 이유없이(즉 범죄혐의도 없이) 체계적이고 지속적으로 보관되고 있다는 것을 알 수 있다. 이러한 형태는 유럽사법재판소가 EU법 위반이라고 판결한 독일 전기통신법의 트래픽데이터 보관조항과 그 성격이 동일하다. 따라서 유럽사법재판소 법리의 관점에서 보면 우리 통신사실확인자

84) 개인정보보호위원회, 개인정보 보호 법령 및 지침·고시 해설, 2020.12, 405.

85) 이에 대한 자세한 설명은 박희영, 통신사실확인자료 보관의 법적 근거와 성질, 형사법연구 제35권 제1호(2023년 봄호) 참조.

료 보관조항은 헌법상 사생활의 비밀 및 통신비밀, 개인정보자기결정권, 표현의 자유를 침해할 가능성이 있다. 보관조항이 위헌이라면 제공조항도 당연히 위헌이 된다. 따라서 통신사실확인자료 보관조항의 위헌성 논의를 시작해야 한다. 만일 위헌가능성이 확실해진다면 유럽사법재판소가 제시한 대상 특정 보관과 신속보관명령이 그 대안으로써 형사정책적 관점에서 논의되어야 할 것이다.

Ⅶ. 맺음말

유럽사법재판소는 아무런 이유없이 전체 국민의 트래픽데이터를 포괄적으로 보관하여 국가기관이 이에 접근할 수 있도록 한 독일의 트래픽데이터 보관조항은 유럽연합헌장이 보장하고 있는 사생활존중권(제7조), 개인정보보호(제8조), 표현의 자유(제11조)와 일치할 수 없다고 판결하였다. 따라서 EU에서는 이유없이 모든 국민의 트래픽데이터를 포괄적으로 보관하는 규정은 허용되지 않게 되었다.

우리 통신사실확인자료보관의 수집 및 보관의 법적 근거는 개인정보보호법에서 도출할 수 있고, 보관의 법적 의무는 통신비밀보호법 제15조의2 및 동법 시행령 제41조의 보관기관과 개인정보보호법 제21조의 보존의무에서 나온다. 통신비밀보호법과 개인정보보호법의 관련 규정이 결합함으로써 모든 국민의 통신사실확인자료가 아무런 이유없이(즉 범죄혐의도 없이) 체계적이고 지속적으로 보관되고 있다. 따라서 우리 통신사실확인자료의 보관의 법적 성질은 독일 전기통신법의 트래픽데이터 보관의 법적 성질과 본질적으로 동일하다. 따라서 유럽사법재판소 법리의 관점에서 보면 우리의 보관조항은 헌법상 사생활의 비밀 및 통신비밀, 개인정보자기결정권, 표현의 자유를 침해할 가능성이 있다. 보관조항이 위헌이라면 당연히 제공조항도 헌이 될 것이다. 이제 통신사실확인자료 보관조항의 위헌성을 논의해야 한다. 만일 위헌가능성이 확실해진다면 유럽사법재판소가 제시한 대상 특정 보관과 신속보관명령이 그 대안으로써 형사정책적 관점에서 논의되어야 할 것이다.

참고문헌

민영성/박희영, 독일에서의 통신정보보관제도의 재도입에 대한 평가와 시사점, 부산대학교, 법학연구 제57권 제2호, 통권 88호, 2016.6.

민영성/박희영, 유럽사법재판소의 통신정보보관지침의 무효 판결과 그 시사점, 법학연구 제56권 제4호, 부산대학교 법학연구소, 2015.

박소현, 개인정보보호적 관점에서의 통신사실확인자료요청제도, 형사법연구 제34권 제2호(2022 여름).

박소현, 전기통신사업자에 의한 통신사실확인자료저장에 대한 법적 제한의 필요성, 성균관법학 제34권 제3호(2022.9).

박희영, 이용대기상태의 휴대전화 위치정보 수사의 허용과 입법방향, 형사정책연구 제31권 제2호(통권 제122호, 2020·여름).

박희영, 통신사실확인자료 보관의 법적 근거와 성질, 형사법연구 제35권 제1호(2023년 봄호).

이상학, EU개인정보보호와 권리구제, 공법연구 제48집 제4호, 2020.6,

최호진, 저장된 데이터의 보전명령제도 도입을 위한 시론(試論), 형사정책 제31권 제2호(통권 제58호, 2019.7.)

Roßnagel, Alexander, Vorratsdatenspeicherung - was geht noch und was nicht mehr?, ZD 2022, 650-655.

BVerfG, Urteil vom 02. März 2010 - 1 BvR 256/08 -.

BVerwG, Beschluss vom 25.09.2019 - 6 C 12.18 - und - 6 C 13.18.

EuGH, Urteil vom 08.04.2014 - C-293/12 und C-594/12

EuGH, Urteil vom 2.3.2021, C-746/18, Vorabentscheidungsersuchen des Riigikohus Estland.

EuGH, Urteil vom 20.09.2022, C-793/19 and C-794/19, Spacenet und Telekom Deutschland.

EuGH, Urteil vom 21.12.2016, C-203/15, C-698/15, Tele2 Sverige und Watson

ua.

EuGH, Urteil vom 5.4.2022, C-140/20, Commissioner of the Garda Síochána ua.

EuGH, Urteil vom 6.10.2020, C-511/18, C-512/18, C-520/18, La Quadrature du Net ua/Premier ministre ua.

VG Köln, 20.04.2018 - 9 K 3859/16

Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung.

German Traffic Data Retention Violates EU law and Criminal Policy Implications*

- Focusing on the Judgement of the CJEU on 20.09.2022, C-793/19 and C-794/19 -

Park, Hee-young**

The question is whether imposing an “obligation” on telecommunications providers to “retain” traffic data without the user’s consent in advance and provide it upon the request of an investigative agency, even if there is no specific criminal suspicion or risk to public safety, is a justifiable restriction or an unjustifiable infringement of constitutional fundamental rights such as the right to self-determination of personal information, protection of communication secrets and privacy, and freedom of expression.

On September 20, 2022, the CJEU (=EuGH) ruled that a provision of the German Telecommunications Act that obliges telecommunications providers to retain and make available to state authorities the traffic data of almost all citizens without any justification(Vorratsdatenspeicherung) violates the relevant fundamental rights of the Charter of Fundamental Rights of the EU. However, the CJEU recognized an exception under strict conditions. These exceptions are inherently different from the type and nature of the existing traffic data retention. It is now impermissible to retain the traffic data of all citizens, regardless of criminal suspicion.

The legal basis and legal nature of the retention of our traffic data can be derived from a systematic analysis of the Personal Information Protection Act(PIPA) and the Protection of Communications Secrets Act(PCSA). According to this,

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5A2A03053654)

** Researcher, Max Planck Institute for the Study of Crime, Security and Law, Ph.D. in Law

telecommunications providers are legally obliged to systematically and continuously store the traffic data of all citizens without any reason. This legal obligation is essentially the same as the retention obligation under the German Telecommunications Act(TKG). Therefore, in the light of CJEU's judgement, our retention provisions are likely to violate the constitutional rights to privacy and secrecy of communications, the right to self-determination of personal data, and freedom of expression. If the retention clause is unconstitutional, then of course the provision clause will also be unconstitutional. The constitutionality of the retention clause should be discussed. If the unconstitutionality of the retention clause is clear, the targeted retention and expedited retention(quick freeze) proposed by CJEU should be discussed from a criminal policy perspective.

❖ Key words: Traffic Data Retention (Vorratsdatenspeicherung), targeted retention, expedited retention(quick freeze), the right to self-determination of personal information, protection of communication secrets and privacy, the freedom of expression

투고일 : 2월 28일 / 심사일 : 3월 27일 / 게재확정일 : 3월 27일