EU 통신데이터 보관지침을 전환한 회원국의 법제 동향

Ⅰ. 머리말

보관용 통신데이터 저장지침(Data Retention Directive, 이하 '통신데이터 보관지침')[1]은 유럽연합 회원국이 정보통신서비스제공자와 공중통신망사업자(이하 '제공자')가 중대범죄의 수사, 확인 및 소추의 목적으로 최소 6개월에서 최대 2년까지 통신사실데이터와 위치데이터를 저장하여 보관할 의무를 규정하고 있다.

각 회원국은 2007년 9월 15일까지 이 지침을 국내법으로 전환하여야 했다. 유럽연합집행위원회는 지난 4월 18일 지금까지 회원국의 전환 법률을 평가한 보고서를 발표하였다.[2] 즉 유럽연합집행위원회는 통신데이터보관지침 제14조에 의하여 회원국에 의한 적용 및 경제계와 소비자들에게 미치는 효과 그리고 지침의 규정들이 특히 데이터의 범주와 저장기간과 관련하여 변경되어야 하는지를 확정짓기 위하여 평가 보고서를 발표한 것이다.

본 글은 이 평가보고서를 근거로 하여 각 회원국이 이 지침의 주요내용을 어떻게 전환하고 있는지를 살펴본다.

Ⅱ. EU의 통신데이터보관의 연혁 및 목적[3]

1. 형사사법 및 형사소추 목적의 데이터 보관

정보통신서비스제공자와 공중통신망사업자

1) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54-63. 이 지침의 한글 번역 자료는 박희영, 유럽 공동체의 통신데이터의 보관에 관한 지침 DIRECTIVE 2006/24/EC, 인터넷법률, 법무부, 2008. 7, 통권 제43호, pp.144-175 참조.

2) Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM(2011) 225 final(이하 '평가보고서').

3) 통신데이터보관지침의 입법과정과 중요내용에 대해서는 박희영, 유럽 공동체 통신데이터 저장 지침과 독일 개정 통신법, 법제처, 법제 제608호, 2008. 8, pp.132-138 참조.

는 그의 활동과 관련하여 통신의 중개, 요금청구, 상호연결 비용, 마케팅, 특정 부가서비스를 위해서 개인정보를 처리한다. 이 과정에서 통신의 발신지, 목적지, 일시, 기간, 유형에 관한 정보뿐 아니라 이용자의 통신장비, 휴대전화의 경우 단말기의 위치데이터를 포함한다. 정보통신의 프라이버시에 관한 유럽연합의 전자프라이버시지침(Directive 2002/58/EC)에서는 전자통신서비스의 이용으로 생성되는 통신데이터는 원칙적으로 이들 데이터가 더 이상 통신의 전송을 위해서 필요하지 않는 경우에는 삭제되거나 익명으로 처리되도록 규정되어 있고, 요금청구에 필요하거나 이용자의 동의를 받은 경우 예외로 하였다. 위치데이터는 부가이용서비스를 제공하기 위해서 필요한 정도에서 그리고 이를 위해 필요한 기간 동안 처리될 수 있다. 다만 이들은 익명으로 처리되거나 이용자의 동의를 받아야 한다.

통신데이터보관지침의 발효 전에는 개별 국가 기관은 특정한 요건하에서 운영자로부터 이러한 데이터에의 접근을 요청하였다. 즉 데이터의 요청은 예컨대, IP주소를 통하여 통신참가자의 신원을 확인하거나 통신활동을 분석하기 위해서 또는 휴대전화를 위치를 특정하기 위하여 이루어졌다.

유럽연합 차원에서 형사소추를 위해서 데이터의 보관과 이용을 처음으로 도입한 것은 '전기통신 분야에서 개인정보의 처리와 프라이버시보호에 관한 Directive 97/66/EC'에 의해서였다. 이 지침은 회원국이 공공 안전과 질서유지 및 국가방위를 위해서 형법상 규정들을 적용하기 위해서 법률을 제정할 가능성을 처음으로 규정하고 있었다.

이 규정들은 정보통신을 위한 데이터보호지침에서 더욱 개선되었다. 이 지침에서는 회원국이 특정한 요건하에서 통신의 기밀성 원칙과 구분되는 다른 법률규정을 제정할 수 있을 뿐 아니라, 형사소추를 위해서 데이터의 보관 및 이에 대한 접근과 이용에 관한 규정들도 제정할 수 있도록 규정하고 있었다. 동 지침 제15조 제1항에 의하면 회원국은 특히 데이터보관을 통하여 데이터보호의 권리 및 의무를 제한할 수 있다. 다만, 이러한 제한은 "국가의 안전, 국가방위, 공공안전 그리고 범죄나 불법적인 정보통신시스템의 예방, 수사, 확인 및 소추를 위해서 필요하고, 적절하며 비례적인 경우에" 한한다.[4]

2. 통신데이터 보관지침의 목적 및 법적 토대

Directive 97/66/EC와 전자프라이버시지침의 규정에 따르면, 상당수 회원국의 제공자는 데이터보관장비를 구입하고 법집행기관에게 데이터를 제공할 직원을 채용하여야 했지만, 일부 회원국에서는 이것을 필요로 하지 않았다. 뿐만 아

4) 앞의 평가보고서, pp.3-4.

니라 영업모델의 변화나 정액요금제서비스, 선불 및 무료정보통신서비스의 제공 등으로 제공자는 항상 보다 적은 통신데이터와 위치데이터를 사용료 정산을 위해서 저장해 왔다. 따라서 이렇게 적은 데이터가 항상 형사사법과 형사소추를 위해서 이용되어 왔다. 이런 와중에 2004년 마드리드와 2005년 런던에서 발생한 테러공격은 유럽연합 차원에서의 이와 같은 문제를 해결하는 계기를 제공하였다.

이러한 배경하에서 통신데이터보관지침은 각 회원국의 국내법에 규정되어 있는 바와 같이 중대범죄의 수사, 확인, 소추의 목적으로 통신데이터를 저장하여 보관할 의무를 제공자에게 부여한 것이다. 이를 통하여 이러한 문제가 유럽차원에서 조화를 이루게 된 것이다.

통신데이터보관지침은 전자프라이버시지침 제15조 제1항을 변경하였다. 즉 전자프라이버시지침에 의해서 저장되어 있는 데이터에는 통신데이터보관지침이 적용될 수 없는 것으로 선언한 것이다. 따라서 회원국은 통신비밀원칙의 적용을 받지 않게 된 것이다. 따라서 통신데이터보관지침은 중대범죄의 수사, 확정, 소추의 제한된 목적을 위해서만 데이터를 저장하여 보관하도록 규정하고 있다.

이 지침의 법적 토대는 '역내시장의 설립과 기능에 관한 유럽공동체의 설립 조약' 제95조(유럽연합의 기능에 관한 조약 제114조에 의해서 교체됨)이다. 이 지침의 제정 후 이의 법적 토대가 유럽법원에 제소된 바 있다.[5] 이유는 지침의 주요 대상이 중대범죄의 수사, 확인 및 소추이기 때문이다. 이에 대하여 유럽법원은 이 지침이 경찰 및 형사사법공조의 수행과는 독립된 업무를 규정하고 있고, 관할 국가기관에 의한 데이터에의 접근이나 국가기관 상호간 이 데이터의 사용과 교환을 규정하고 있지 않다고 판단하였다. 따라서 통신데이터보관지침은 본질적으로 역내시장의 관련 분야에서 제공자의 활동에 직접 적용된다고 결정함으로써 법적 기반을 획득하게 된 것이다.[6]

Ⅲ. 지침을 전환한 회원국의 법제 동향

1. 통신데이터 보관지침의 목적

가. 규정 내용

본 지침의 목적은 공중이 접근 가능한 전자적 통신서비스 제공자 또는 공중 통신망의 운영자에 의해서 생성되거나 처리되는 특정 데이터의 보관과 관련하여 이들의 책임에 관한 회원국의

5) 자세한 내용은 박희영, 앞의 글, p.139 참조.
6) ECJ, C-301/6 Ireland v Parliament and Council, ECR [2009] I-00593.

규정들이 중대한 범죄의 수사, 확인, 소추의 목적으로 데이터를 사용할 수 있도록 확보하도록 조화를 이루는 데 있다(지침 제1조).

나. 법제 동향

유럽연합회원국 중 10개국(불가리아[7], 에스토니아[8], 핀란드[9], 그리스[10], 아일랜드[11], 리투아니아[12], 룩셈부르크[13], 네덜란드[14], 스페인[15], 헝가리[16])은 최저 자유형과 관련하여 '중대한 범죄'의 개념을 규정하고 있다.

8개국(벨기에[17], 덴마크[18], 프랑스[19], 이탈리아[20], 라트비아[21], 폴란드[22], 슬로바키아[23], 슬로베니아[24])은 중대범죄의 수사, 확인 및 소추는 물론, 전체범죄의 예방이나 국가의 안전 및 공공의 안전을 위해서도 데이터를 저장할 수 있다고 규정하고 있다. 그리고 4개국(말타[25], 포르투갈[26], 영국[27], 키프로스[28])은 개념 규정을 두지 않고 단순히 중대범죄로 제한하고 있다.

7) Article 250a (2), Law on Electronic Communications (amended) 2010.

8) Subsection 110(1), Code of Criminal Procedure.

9) Article 14a (1), Electronic Communications Act.

10) Such crimes are defined in Article 4 of Law 2225/1994; Article 1 of Law 3917/2011.

11) Article 6 Communications (Retention of Data Act) 2011.

12) Article 65, Law X-1835.

13) Article 1(1), Law of 24 July 2010.

14) Article 126, Code of Criminal Procedure.

15) Article 1(1), Law 25/2007.

16) For the general purpose of data retention Article 159/A of the Act C/2003, as amended by the Act CLXX-IV/2007; on the purpose ofpolice access Article 68, Act XXXIV/1994; on the purpose of National Tax and Customs Office access, Article 59, Act CXXII/2010.

17) Article 126(1) of Law of 13 June 2005 concerning electronic communications.

18) Article 1, Data Retention Order.

19) The acts that regulate the use of retained data, respectively, for criminal offences, for preventing acts of terrorism and for protecting intellectual property are as follows: are Article L.34-1(II), CPCE, Law no. 2006-64 of 23 January 2006 et Law no. 2009-669 of 12 June 2009.

20) Article 132(1), Data Protection Code.

21) Article 71(1), Electronic Communications Law.

22) Article 180a, Telecommunications Law of 16 July 2004 as amended by Article 1, Act of 24 April 2009.

23) Article 59a (6), Electronic Communications Act.

24) Article 170a(1) Electronic Communications Act.

25) Article 20(1), Legal Notice 198/2008.

26) Article 1, 3(1), Law 32/2008.

27) The Data Retention (EC Directive) Regulations 2009 (2009 No. 859).

28) Article 4(1), Law 183(I)/2007.

다. 평 가

대부분의 전환 국가들은 입법의 준수와 관련하여 동 지침이 보장하는 중대범죄의 수사, 확인, 소추의 범위를 넘어서 일반적인 범죄의 예방과 대책 및 생명과 신체에 대한 위험의 경우에도 보관데이터의 접근과 이의 이용을 허용하고 있다. 이것은 전자프라이버시지침에서 허용되고 있지만, 이 분야에서 유럽연합의 입법에 의해서 달성된 조화의 정도에는 한계가 있다. 데이터보관의 의도에서 차이점은 요청의 분량과 빈도에 영향을 미치고, 반대로 지침에 부여된 의미의 준수로 발생하는 비용이다. 게다가 이러한 상황은 프라이버시를 제한하는 어떤 입법적 조치에서 요건이라는 예견가능성을 충분히 제공하지 못할 수도 있다. 집행위원회는 이 분야에서 강력한 조화가 필요한지, 그리고 어떻게 이를 달성할 수 있는지를 검토할 것이라고 한다.

2. 데이터 보관 의무자

가. 규정 내용

동 지침은 데이터보관의무자를 정보통신서비스제공자 또는 공중통신망사업자로 규정하고 있다(제1조 제1항).

나. 법제 동향

핀란드와 영국은 데이터 보관 의무를 규정하고 있지 않다. 소규모 제공자에게 데이터를 보관할 의무를 부여하고 있지 않다. 왜냐하면 이를 행하는 데 드는 제공자와 국가의 비용이 형사사법시스템과 법집행에 대한 비용보다 훨씬 크기 때문이라고 한다. 라트비아, 룩셈부르크, 네덜란드 및 폴란드는 선택적으로 행정규제와 관련시키고 있다.

다. 평 가

다수의 회원국에 활동하고 있는 대규모 사업자는 규모의 경제로부터 비용을 감당해 낼 수 있지만, 일부 회원국의 소규모 사업자는 비용 절감을 위해서 합작을 하거나 통신데이터의 보관이나 이의 호출을 전문으로 하는 사업자에게 아웃소싱을 해야 한다고 한다. 이러한 방식의 아웃소싱은 처리과정을 충분히 감시하고 필요한 보안조치를 확보해야 할 제공자의 의무에 아무런 영향을 미칠 수 없다. 특히 이러한 점은 소규모 제공자에게 문제로 지적될 수 있다. 따라서 집행위원회는 데이터의 안전성 문제를 검토하고, 데이터 보관 프레임을 수정하기 위한 선택과 관련하여 중소규모 사업자의 영향도 검토할 것이라고 한다.

3. 데이터에의 접근 기관, 절차 및 요건

가. 규정 내용

이 지침에 따라서 보관용으로 저장된 데이터가 특별한 경우 및 국내법에 일치하는 경우에 한해서 국내의 당해 관청에 제공되도록 확보하기 위한 조치를 취해야 한다. 각 회원국은 유럽연합의 법률규정 또는 국제법, 특히 유럽인권법원에 의해 해석된 유럽인권협약의 관련 규정을 고려

하여, 필요성과 비례성의 원칙에 따라 저장 데이터에의 접근을 위해서 이행되어야 하는 절차와 요건을 당해 국내법에서 확정해야 한다(지침 제4조).

나. 법제 동향

모든 회원국은 국내의 경찰[29] 및 검찰에게 보관데이터에의 접근을 허용하고 있다. 14개국은 보안기관 및 정보기관 그리고 군정보기관에게도 이를 허용하고 있다. 6개국은 국세청이나 세관, 그리고 3개국은 국경수비대에게도 이를 허용하고 있다. 11개국은 보관용 데이터에 대한 접근 요청에 법원의 허가를 필요로 하고 있다. 3개국은 대부분의 사례에서 법원의 허가를 필요로 하고 있다. 4개국은 법원의 허가가 아니라 관청의 허가를 규정하고 있다. 2개국에서는 문서로 제출되어야 하는 점을 요건으로 하고 있다(구체적 내용은 아래 표 참조).

보관통신데이터에의 접근		
관할 기관		절차 및 요건
벨기에	사법조정기관, 수사판사, 검찰, 수사경찰	법원 및 검찰의 허가 필요. 제공자는 데이터의 요청을 받은 경우 최근 달에 접속한 통신참가자데이터, 통신사실데이터, 위치데이터를 실시간으로 제공해야 한다. 과거의 통신접속데이터도 가능한 한 제공할 수 있다
불가리아	국가보안기관의 특정된 장 또는 부서, 내무부, 군사정보기관, 군경찰, 국방부, 국가수사기관, 법원 및 특정한 요건하에서 수사기관	전범재판소의 재판장의 명령으로도 접근 가능
체코	위헌결정	
덴마크	경찰	접근에는 법원의 허가 필요. 법원의 명령은 요청이 엄격한 기준(범죄혐의, 필요성, 비례성)을 충족할 경우에만 허용
독일	위헌결정	
에스토니아	경찰 및 국경수비대, 보안경찰, 국세청 및 관세청	접근에는 수사판사의 허가 필요. 제공자는 긴급한 경우에는 10시간 이내에, 그 밖의 경우에는 10일 이내에 요청데이터를 제공해야 함
아일랜드	경찰, 국방부, 국세청	문서에 의한 신청
그리스	사법부, 군, 경찰	접근에는 법원의 결정 필요. 수사가 다른 방법으로 불가능하거나 극히 어려운 경우에 한함
스페인	중대범죄의 수사, 확인, 소추하는 관할 경찰관청, 정보기관, 세관	접근에는 법원의 사전허가 필요
프랑스	검찰, 경찰, 지방경찰	경찰은 국가감청통제위원회의 허가를 받아야 함

29) 코먼로 국가인 아일랜드와 영국은 제외.

보관통신데이터에의 접근		
관할 기관		절차 및 요건
이탈리아	검찰, 경찰, 수사의 대상인 피고인이나 피의자의 변호인	접근에는 검찰의 명령 필요
키프로스	법원, 검찰, 경찰	접근에는 검찰의 허가 필요. 법관은 중대범죄에 대한 충분한 범죄혐의가 있고 데이터 및 이와 관련한 개연성이 있는 경우에는 해당 명령을 내릴 수 있음
라트비아	수권받은 수사기관 및 보안기관, 검찰, 법원	수권기관, 검찰, 법원은 요청의 적정성과 중요성을 심사함
리투아니아	수사기관, 검찰, 법원, 정보기관	수권기관은 보관용 통신데이터를 문서로 요청해야 함. 수사기관의 접근의 경우에는 법원의 명령이 필요함
룩셈부르크	사법기관(수사판사, 검찰), 범죄의 예방, 수사, 확정, 소추 및 국가의 안전, 국방, 공공의 안전을 관할하는 기관	접근에는 법원의 허가가 필요
헝가리	경찰, 국세청 및 관세청, 보안기관, 검찰, 법원	경찰 및 국세청 및 관세청은 검사의 허가가 필요. 검찰 및 국가보안기관은 법원의 명령 없이 접근 가능
말타	경찰, 보안기관	문서에 의한 요청
네덜란드	수사경찰	법원 및 검찰의 명령 필요
오스트리아[30]	법원, 검찰, 경찰, 정보기관	데이터의 요청은 검찰의 명령에 법원의 동의 요함, 정보기관은 보안경찰법에 의하여 법원의 관여 없이 가능
폴란드	경찰, 국경수비대, 국세청, 국내외정보기관, 부패방지청, 국내외 군사정보기관, 법원, 검찰	요청에는 문서로 경찰, 국경수비대 또는 국세청은 해당 기관의 상급자의 허가 필요
포르투갈	수사경찰, 공화국 정보기관, 공공안전기관, 군수사경찰, 이민청 및 국경수비대, 해양경찰	데이터전송에는 법원의 허가 필요. 법원의 허가에는 필요성과 비례성을 증명해야 함
루마니아	위헌결정	
슬로베니아	경찰, 정보기관, 스파이 및 보안업무를 관할한 방위청	접근에는 법원의 허가 필요
슬로바키아	경찰, 국경수비대, 세관. 비상사태방위청, 해상구조대, 해상구조 지원청	통신참가자의 데이터는 법원의 허가 없이 접근 가능하나 그 밖의 데이터의 접근에는 법원의 허가 필요
스웨덴		
영국	경찰, 정보기관, 국세청 및 관세청, 그 밖의 2차적 법률 규정에 의하여 명시된 기관	데이터의 전달이 법률로 허용되거나 규정되어 있는 특별한 사례와 상황에서만 허가는 허용되는 접근을 위해서는 명시된 자에 의한 허가 및 필요성과 비례성의 심사가 필요하다. 구체적인 절차에 대해서는 제공자와 협의한다

30) 오스트리아 연방의회는 4월 28일 통신데이터의 저장에 관한 법률을 의결하여 2012년 4월부터 발효됨. 따라서 유럽연합집행위원회의 평가보고서에는 포함되어 있지 않음.

다. 평가

위원회는 어떠한 기관이 보관용 데이터에 접근하는지 그리고 어떠한 절차에 의해서 이 기관에게 이러한 접근이 보장되고 있는지와 관련하여 보다 강력한 조화가 필요한지, 그리고 경우에 따라서는 어떻게 조화를 이룰 수 있는지를 심사할 것이라고 한다. 생각해 볼 수 있는 것으로는 관할기관을 보다 명확하게 정의하는 목록의 작성, 데이터의 요청에 법원의 감독을 받게 하거나 독립적인 기관에 의한 감독을 받게 하는 방안, 절차의 최저기준, 제공자가 관할 기관에게 접근을 허용하는 절차의 최저기준 등이 있다고 한다.

4. 보관데이터의 범주 및 데이터의 사용 범위

가. 규정내용

제1조 제2항 : 본 지침은 법인과 자연인의 통신 데이터와 위치데이터 및 가입자 또는 등록된 이용자의 확인에 필요한 관련 데이터에 적용된다. 본 지침은 전자적 통신망을 사용하여 요청된 정보를 포함하여 전자적 통신의 내용에는 적용되어서는 아니된다.

제3조 제2항 : 제1항에 의한 데이터 보관의무는 공중이 사용할 수 있는 전자적 통신서비스 및 공중통신망의 제공자가 관련 회원국의 관할권 내에서 관련 통신서비스를 제공하는 과정에서 이들 데이터를 생성하거나 처리하고, 저장하거나(전화 데이터의 경우) 또는 기록한다면(인터넷 데이터의 경우), 성공하지 못한 통화 시도[31]와 관련하여 제5조에 언급한 데이터의 보관을 포함해야 한다. 이 지침은 연결이 되지 아니한 통화에 관한 데이터의 보관을 요구하지 않는다.

제5조 : 저장될 데이터의 구분, 종류, 범주

1. 회원국은 이 지침에 따라 다음의 데이터 범주가 보관용으로 저장되도록 확보하여야 한다.

(a) 통신의 발신지를 추적하고 확정하는 데 필요한 데이터 :

(1) 유선네트워크 전화와 이동전화와 관련하여 :

(i) 발신자의 자의 전화번호

(ii) 전화가입자 또는 등록된 사용자의 이름과 주소

(2) 인터넷 접속, 인터넷 이메일 그리고 인터넷 전화와 관련하여 :

(i)부여받은 이용자 아이디

(ii) 공중 전화망에서 모든 통신에 할당된 이용자 아이디와 전화번호

(iii) 통신시점에 인터넷 프로토콜 어드레

31) 즉 전화호출이 성공적으로 되었으나 상대방의 응답이 없거나 네트워크관리가 개입한 경우, 그리고 관련 데이터가 운영자에 의해서 생성되거나 처리되고 저장되거나 기록되는 경우.

스(IP주소), 이용자 아이디, 전화번호가 부여된 가입자 및 등록된 이용자의 이름과 주소

(b) 통신의 착신지를 확인하는 데 필요한 데이터 :

(1) 유선네트워크 전화와 이동망 전화와 관련하여 :

(i) 수신자의 전화번호, 콜 포워딩 또는 콜 트랜스퍼와 같은 부수 서비스의 경우에는 통화가 루트된 곳의 번호

(ii) 가입자 또는 등록된 사용자의 이름과 주소

(2) 인터넷 전자메일과 인터넷 폰과 관련하여 :

(i) 이용자 아이디 또는 인터넷 전화의 수신자의 전화번호

(ii) 가입자 또는 등록된 이용자의 이름과 주소 그리고 통신 수신자의 이용자 아이디

(c) 통신의 날짜, 시간, 기간을 확인하는 데 필요한 데이터 :

(1) 유선네트워크 전화와 이동 전화와 관련하여 통신의 날짜, 발·착신 시간

(2) 인터넷 접속, 인터넷 전자메일 그리고 인터넷 전화와 관련하여 :

(i) 인터넷 접속 서비스의 경우 인터넷 접속 서비스 제공자에 의해 제공된 유동 및 고정 IP주소를 포함하여 특정시간대를 기준으로 한 로그인과 로그 오프의 날짜와 시간 그리고 가입자 또는 등록된 이용자의 아이디

(ii) 인터넷 전자메일 서비스 또는 인터넷 전화 서비스의 경우 특정시간대를 기준으로 한 로그인과 로그 오프의 날짜와 시간

(d) 통신이 형태를 확인하는 데 필요한 데이터

(1) 유선네트워크 전화와 이동 전화와 관련하여 : 사용된 전화 서비스

(2) 인터넷 전자메일과 인터넷 전화와 관련하여 : 사용된 인터넷 서비스

(e) 이용자의 통신장비 또는 자칭 이용자의 장비라고 의도하는 것을 확인하는 데 필요한 데이터 :

(1) 유선네트워크 전화와 관련하여 발신자 전화번호와 수신자 전화번호

(2) 이동 전화와 관련하여 :

(i) 발·착신 전화 번호

(ii) 발신자의 국제이동가입자 식별번호 (IMSI)

(iii) 발신자의 국제이동단말기 식별번호 (IMEI)

(iv) 수신자의 국제이동가입자 식별번호

(v) 수신자의 국제이동단말기 식별번호

(vi) 선불 익명 서비스의 경우, 서비스의 초기 개시의 날짜와 시간 그리고 서비스가 개시된 소재지의 표지(Cell ID)

(3) 인터넷 접속, 인터넷 전자메일, 인터넷 전화와 관련하여 :

(i) 다이얼 업(다이얼 호출) 접속의 경우 발신 전화번호

(ii) 디지털 가입자 회선 또는 다른 통신 설치자의 종단점

(f) 이동통신장비의 위치를 확인하는 데 필요한 데이터 :

(1) 통신 개시시의 소재지 표지(Cell ID)

(2) 통신 데이터가 저장되는 동안 소재지 표시(Cell ID)와 관련한 셀의 지리적 위치를 확인하는 데이터

2. 통신의 내용을 나타내는 데이터는 이 지침에 따라 저장되어서는 아니된다.[32]

나. 법제 동향

21개국은 전환조치에서 이러한 데이터범주의 보관용데이터저장을 규정하고 있다. 벨기에는 전화데이터의 종류나 인터넷데이터의 경우 보관데이터저장을 규정하고 있지 않다.

다. 평가

집행위원회는 보관데이터의 범주에 검색요청도 포함시킬 것을 회원국에 설문한 적이 있다. 유럽의회가 지침의 적용범위를 "아동포르노와 인터넷상에서의 성적 괴롭힘에 대해서 신속하게 행동을 취할 수 있도록 하기 위해서 검색엔진으로 적용범위를 확대하자는"[33] 의견을 집행위원회에게 문서로 요청해 왔기 때문이다. 그럼에도 불구하고 설문에 응답한 회원국은 변경의 필요성이 없는 것으로 보고 있다. 제2차 시행조치에 관한 보고서에서 유럽연합 데이터보호위원회[34]는 지침에 규정된 범주는 이에 국한된 것으로 보아야 하고 운영자에게 추가적으로 의무를 부여하여서는 아니된다고 하였다. 집행위원회는 모든 데이터범주의 필요성을 심사할 것이라고 한다.

5. 저장기간(제6조 및 제12조)

가. 규정내용

제6조(보관 기간) : 회원국은 통신을 개시한 때부터 최소 6월에서 최고 2년까지 제5항에 규정된 데이터 범주들이 보관되도록 확보해야 한다.

제12조(장래의 조치)

1. 제6조에 의한 최대저장기간의 일정한 기간

32) 검색요청, 즉 검색서비스에 의해서 작동되는 서버 프로토콜은 지침의 적용범위에 해당하지 않는다. 이유는 이들은 통신사실데이터가 아니라 내용데이터로 고려되기 때문이다(Article 29 Working Party Opinion on data protection issues related to search engines, 4 April 2008).

33) Written Declaration pursuant to Rule 123 of the Rules of Procedure on setting up a European early warning system (EWS) for paedophiles and sex offenders, 19.4.2010, 0029/2010.

34) 이 위원회는 유럽연합 집행위원회 산하의 독립적인 데이터보호 자문위원회로서 유럽연합 데이터보호지침(Directive 95/46/EC) 제29조에 의하여 1995년 10월 24일 설치되었다. 정식명칭 : Working Party on the Protection of Individuals with regard to the Processing of Personal Data(데이터보호지침 제29조 제1항). 약칭 : Article 29 Data Protection Working Party.

동안 연장[35]을 정당화할 특별한 사정이 있는 회원국은 필요한 조치를 취할 수 있다. 이 회원국은 이를 즉시 이사회에 알리고 동조에 의해서 취해진 조치를 다른 회원국에게 통지하고 이러한 조치를 채택한 근거를 제시해야 한다.

2. 위원회는 제1항에 언급한 통지 후 6개월 이내에, 해당 국가의 국내적 조치가 회원국 사이에서 자의적인 차별의 수단인지 아니면 감추어진 거래의 제한인지 또는 그 조치가 국내 시장의 기능을 방해하는 것인지를 심사한 이후에, 그 국내적 조치를 승인하거나 거부해야 한다. 위원회가 이 기간 내에 결정을 하지 않는 경우에 개별 국가의 조치는 승인된 것으로 간주한다.

나. 법제 동향

15개국에서는 모든 데이터범주에 대해서 저장기간을 통일적으로 규정하고 있다. 예를 들어 폴란드는 2년, 라트비아 1년 6개월, 10개국(불가리아, 덴마크, 에스토니아, 그리스, 스페인, 프랑스, 네덜란드, 포르투갈, 핀란드, 영국)은 1년, 키프로스, 룩셈부르크, 리투아니아는 6개월이다. 5개국은 데이터의 범주에 따라서 저장기간을 달리 규정하고 있다. 예컨대 아일랜드와 이탈리아는 유무선전화의 경우 2년, 인터넷접속, 전자우편, 인터넷전화의 경우 1년, 슬로베니아는 전화데이터의 경우 14개월, 인터넷관련 데이터는 8개월, 슬로바키아의 경우 유무선전화의 경우 1년, 인터넷관련 데이터의 경우 6개월, 말타의 경우 유무선전화 및 인터넷 전화 데이터는 1년, 인터넷접속과 전자우편의 경우 6개월, 헝가리의 경우 성공하지 못한 전화의 경우 6개월을 제외한 모든 데이터는 1년으로 규정하고 있다. 이에 대하여 벨기에는 지침에 규정된 데이터의 범주에 해당하는 저장기간을 규정하고 있지 않다.

다. 평 가

통신데이터보관지침상의 이 원칙들은 한 국가 이상에서 활동하고 있는 제공자 및 다양한 회원국에 통신데이터를 저장하고 있는 시민들에게 유럽연합 차원에서 제한적인 법적 안정성과 예견가능성을 제공하고 있다는 사실로부터 기인한다. 데이터처리의 국제화가 증대되고 있고 데이터저장이 아웃소싱되고 있는 점에서 유럽연합 차원에서 저장기간의 조화를 이룰 가능성이 있게 되었다. 비례성의 원칙을 고려하고 회원국에 저장되어 있는 데이터의 질적 · 양적 정보, 통신의 변화, 기술의 발전, 범죄 및 테러의 경향과 관련하여 집행위원회는 다양한 데이터범주와 다양한 중대범죄 또는 이들의 결합에 대한 다양한 저장기간의 이용을 심사할 것이라고 한다. 지금까지 제출된 저장데이터의 기간에 관한 회원국들의 양적 정보를 분석한 결과 형사소추기

35) 최대기간의 연장은 가능한 반면, 6개월 이하로의 기간단축은 규정되어 있지 않다.

간의 접근 요청의 경우 약 90% 이상의 데이터는 6개월을 넘지 않고, 약 70%는 3개월을 넘지 않는다고 한다.

6. 데이터보호, 데이터안전 및 통제기간

가. 규정내용

제7조 : 데이터 보호와 데이터 안전

각 회원국은 공중 전자통신서비스 제공자 또는 공중통신망 제공자가 본 지침에 따라 저장된 데이터와 관련하여 다음의 데이터 안전 원칙을 최소한 준수하도록 확보해야 한다.

(a) 보관 데이터는 네트워크에 있는 데이터와 동질의 것이어야 하며, 동일한 안전과 보호를 조건으로 해야 한다.

(b) 우연한 또는 불법적인 파기, 우연한 상실 또는 변경, 부당한 또는 불법적인 저장, 처리, 접근 또는 유포에 대해서 데이터를 보호하기 위한 적절한 기술적 그리고 조직적 조치가 취해져야 한다.

(c) 데이터에의 접근은 특별히 권한이 주어진 사람에게만 허용되도록 적절한 기술적, 조직적 조치를 확보해야 한다.

(d) 접근되어 있고 저장되어 있는 데이터를 제외한 다른 데이터는 저장기간이 종료한 때에 폐기되어야 한다.

제9조(감시 기관)

1. 저장 데이터의 안전에 관한 제7조의 전환을 위해 채택한 규정이 자국 내에서 적용되는 것을 모니터링 책임질 한 곳 이상의 공공기관을 각 회원국은 임명하여야 한다. 이 기관은 지침 95/46/EC의 제28조에서 규정하고 있는 기관과 동일할 수 있다.
2. 제1항의 기관은 제1항에서 언급하고 있는 감시를 완전히 독립적으로 수행하여야 한다.

나. 법제 동향

15개국(불가리아, 덴마크, 아일랜드, 프랑스, 키프로스, 리투아니아, 룩셈부르크, 헝가리, 말타, 네덜란드, 폴란드, 포르투갈, 슬로베니아, 슬로바키아, 영국)은 모든 원칙들을 관련 규정에 전환하고 있다. 4개국(벨기에, 에스토니아, 스페인, 라트비아)은 둘 또는 세 가지 원칙들을 전환하고 있지만, 저장기간 종료시 데이터의 폐기를 명확하게 규정하고 있지 않다. 이탈리아와 핀란드는 데이터의 폐기를 규정하고 있지만, 가령 엄격한 신원확인과 상세한 접근프로토콜의 관리와 같은 기술적, 조직적 구체적인 보안조치를 어떻게 취할 것인지가 불명확하다. 22개국은 기본원칙의 적용을 감시할 관할기간이 존재한다. 대부분 데이터보호기관이 이를 수행하고 있다.

다. 평 가

제7조는 통일적으로 전환되어 있지 않다. 보관데이터를 제외하면 잠재적으로 매우 사적이고 민감한 데이터가 문제된다. 이러한 데이터의 처리, 저장, 요청 및 사용을 위해서는 오로지 고도의 데이터보호 및 안정성기준이 통일적으로

투명하게 적용되어야 하는데, 이것은 프라이버시의 침해의 위험을 최소로 줄이고 시민의 신뢰를 유지하기 위해서이다. 집행위원회는 데이터 안전성기준과 데이터보호기준의 개선을 위한 선택을 추가된 데이터보호의 삭제와 함께 심사할 것이다. 이러한 기준들이 저장이나 전달의 경우에도 충족될 수 있도록 배려하기 위해서이다. 또한 이 경우에 시행조치에 관한 유럽연합 데이터보호위원회의 보고서에 포함된 최소보호조치 및 기술적 조직적 보안조치에 대한 권고를 고려하게 될 것이라고 한다.

7. 전환 법률에 대한 회원국 헌법재판소의 판단

통신데이터보관지침을 국내법으로 전환한 법률이 해당 국가의 헌법재판소에서 헌법적 판단을 받은 국가가 있다. 이 중에서 루마니아 헌법재판소, 독일연방헌법재판소, 체코 헌법재판소는 2009년 10월, 2010년 3월, 2011년 3월 해당 국가의 전환법률이 본 국의 헌법에 위반되어 무효로 각각 선언하였다.

가. 루마니아 헌법재판소 위헌결정

루마니아 헌법재판소[36]는 특정한 규정이 준수되고, 국가의 잠재적 자의에 대해서 적절하고 충분한 보장이 존재하는 경우에는, 기본권 침해는 허용되는 것으로 간주하였다. 하지만 헌법재판소는 유럽인권법원의 판례[37]를 원용하여 전환조치의 적용범위와 목적은 오해의 소지가 있고, 보장이 불충분하며, 6개월간 보관용으로 전체데이터를 저장해야 할 법적인 의무는 유럽인권선언 제8조에 의한 프라이버시와 자유로운 표현의 자유의 권리와 일치할 수 없다고 판단하였다.[38]

나. 독일연방헌법재판소 위헌결정

독일연방헌법재판소[39]는 전환법률의 관련 규정이 감시당한다는 느낌을 불러일으키고 자유로운 기본권 행사를 침해한다고 판단하였다.[40] 헌법재판소는 엄격히 제한된 목적을 위한 보관용데이터의 저장은 데이터의 안정성이 충분히 높은 경우에는 독일 법률에 대해서 당연히 침해되는 것은 아니지만, 프라이버시에 대한 중대한 침해가 있고, 특별히 엄격한 요건하에서만 허용되며, 6개월간의 저장기간은 비례성의 평가에서

36) Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court.

37) ECtHR, Rotaru v. Romania 2000, Sunday Times v. UK 1979 and Prince Hans-Adam of Liechtenstein v. Romania 2001.

38) 앞의 평가보고서, P.24 참조.

39) Bundesverfassungsgericht, 1 BvR 256/08, para 1 – 345.

40) 독일연방헌법재판소 결정문의 전문번역에 대해서는 박희영, 통신사실확인자료의 저장과 통신비밀의 침해(상), -독일 연방헌법재판소 2010년 3월 2일 위헌 결정, 법제 제629호, 법제처, 2010.5, pp.5-35; (하), 법제 제630호, 법제처, 2010.6, pp.6-47. 결정문의 평석에 대해서는 박희영, 통신사실확인자료 저장의 통신비밀침해에 대한 위헌결정, 독일연방헌법재판소 판례연구 1[정보기본권], 한국학술정보(주), 2010.12 (박희영·홍성기 저), pp.91-117 참조.

정당화될 수 있다고 한다. 데이터는 오로지 이미 중대범죄에 대한 혐의가 존재하거나 공공의 안전을 위협할 증거가 존재하는 경우에만 요청될 수 있다고 한다. 특정한 통신을 위해서 데이터의 호출, 기밀성이 보장되는 특정한 통신의 호출은 금지된다고 한다. 데이터는 또한 암호화되어야 하고, 이의 사용은 투명하게 감시되어야 한다고 한다.

다. 체코 헌법재판소 위헌결정

체코 헌법재판소[41]는 전환조치들이 기본권을 제한하는 조치를 위해서 명확하고 충분하게 형성되어 있지 않다는 점을 근거로 이 전환조치들을 무효로 선언하였다. 헌법재판소는 보관데이터의 규모와 범위를 고려한 목적설정이 충분하지 않은 것으로 비판하고 있다. 그리하여 헌법재판소는 저장데이터의 접근과 사용이 허용되는 관할 기관의 정의 및 접근절차, 그리고 이용절차가 데이터의 무결성과 기밀성을 보장하기 위해서 전환법률에서는 명확하지 않는 것으로 인정하고 있다. 개별시민은 이를 통하여 공공기관의 권한남용으로부터 충분히 보장과 보호를 받지 못한다고 한다. 헌법재판소는 지침 자체에 대해서는 이의를 제기하지 않았다. 재판소는 체코 정부는 지침을 합헌적으로 전환하기 위해서 충분한 재량의 여지를 가지고 있다고 선언하였다. 물론 재판소는 방론에서 새로운 범죄수법, 예컨대 익명 SIM 카드의 사용의 관점에서 통신데이터의 저장의 필요성, 실효성 및 적절성에 의심이 있다고 보고 있다.

라. 기타

불가리아 헌법재판소는 전환조치의 보완이 필요한 것으로 보았고, 키프로스 헌법재판소는 전환조치와 관련하여 법원의 명령은 위헌으로 선언하였으며, 헝가리는 전환조치에서 데이터처리의 목적의 한계가 결여되어 헌법소원이 현재 계류 중이다.

집행위원회는 개별 국가의 판례에서 제기된 문제점들을 통신데이터보관지침의 개정에 반영할 것이라고 한다.[42]

8. 지침의 미전환 또는 불완전하게 전환한 국가에 대한 조치

집행위원회는 아직 지침을 완전히 이행하지 아니하였거나 국내 헌법재판소에 의해서 무효로 선언된 조치로 아직 전환되지 아니한 회원국들이 이 지침을 가능한 한 빨리 전환하기를 기대하고 있다. 한편 집행위원회는 EU 조약에 의한 권한을 행사할 것을 유보하고 있다. 유럽법원은 판결을 통해서 아직 지침을 전환하지 않은 2

41) Judgment of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No 485/2005; see in particular paragraphs 45-48, 50-51 and 56.

42) 앞의 평가보고서 p.25.

개 회원국(오스트리아와 스웨덴)에 대해서 유럽연합법률에 의한 의무위반이라고 선언한 바 있다.[43] 집행위원회는 2011년 4월 스웨덴에 대해서 다시 법원에 제소하였다. 이유는 스웨덴이 이 판결을 아직 준수하지 않고 있기 때문이다. 또한 집행위원회는 스웨덴 의회가 전환규정을 12개월 연장한 데 대해서 유럽연합의 업무에 관한 조약 제260조에 의해 위약금 판결을 신청하였다.

Ⅳ. 전망 및 시사점

유럽연합의 통신데이터보관지침은 현재 유럽연합회원국 내에서 많은 문제를 제기하고 있다. 특히 각 회원국의 헌법에 정한 기본권에 위반됨은 물론 유럽인권선언의 관련 규정에도 위반된다는 견해도 지속적으로 전문가 및 시민단체들로부터 제기되고 있다. 따라서 집행위원회는 향후 통신데이터보관지침을 어떤 형태로든 개정해야 할 시점에 있다. 유럽연합에서의 통신데이터보관에 관한 논의, 특히 헌법상의 기본권 침해와 관련한 논의는 통신사실확인자료를 규정하고 있는 우리의 현행 통신비밀보호법상의 관련 규정(통신사실확인자료요청에 관한 제13조, 통신사실확인자료의 종류에 관한 제2조 제11호, 보관기관에 관한 통신비밀보호법시행령 제21조의 4 등)들을 검토하는 데 시사하는 바가 크다.[44]

박 희 영
(해외입법조사원,
독일 막스플랑크 국제형법연구소 연구원)

43) 오스트리아 : Case C-189/09, 스웨덴 : Case C-185/09.

44) 이러한 논의에 대해서는 박희영, 독일 형사소송법상 통신데이터 수집권과 한국 통신비밀보호법상 통신사실확인자료제공 요청권의 비교 및 시사점, 경찰학연구 제9권 제3호(통권 제21호), 경찰대학교, 2009. 10, pp.47-55 참조.