독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향

I. 머리말

정보통신기술의 급속한 발전으로 경찰은 새로운 도전에 직면하고 있다. 특히 조직범죄나 테러범죄자들이 이러한 정보통신기술을 활용함으로써 기존의 수단으로서는 이들의 범죄행위에 대처할 수 없는 상황에 이르게 된 것이다. 경찰이 이에 효과적으로 대처하기 위해서, 특히 위험예방의 영역에서 새로운 기술적 수단을 관련 법률에 규정하기 시작하였다. 그러한 기술적 수단 중 최근 가장 많이 논란이 되고 있는 것이 '온라인수색'이다.

온라인 수색(Online-Durchsuchung)이란 일반적으로 국가가 정보통신망에 있는 타인의 정보기술시스템(예컨대 컴퓨터, 노트북, 스마트폰 등)에 비밀리에 접근하는 것을 말한다. 즉 테러범죄나 조직범죄와 같은 혐의를 받고 있는 자가 인터넷으로 연결되어 있는 컴퓨터를 이용하는 경우 이 컴퓨터에 트로야너 소프트웨어를 몰래 설치하여 거기서 작업하고 있는 내용이나 저장되어 있는 데이터를 열람하거나 복제하는 새로운 정보수집방법이다. 이러한 기술은 인터넷에 연결되어 있는 컴퓨터에 접근하는 것이어서 암호화되기 전의 전자우편이나 암호화되어 전송되는 스카이프 인터넷전화의 경우에도 감청 이전 단계에서 그 정보들을 획득할 수 있을 뿐 아니라, 외부에서 컴퓨터에 장착되어 있는 마이크나 웹캠을 작동시켜 컴퓨터 작업을 하고 있는 수색 대상자의 모습이나 작업공간을 관찰할 수 있어서 수사기관이나 정보기관에게는 마스터키와 같은 유혹이 아닐 수 없다. 하지만 이러한 기술은 헌법상 국민의 기본권을 침해할 우려가 상당히 크기 때문에 이를 허용하는 데에는 엄격한 법률상의 규정이 필요하다.

이와 관련한 논의와 입법이 가장 활발한 곳이 독일이다. 독일에서는 이미 오래 전부터 온라인 비밀 수색에 관한 논의가 진행되어 왔다. 온라인 비밀 수색에는 경찰이나 정보기관의 예방적 온라인 수색과 범죄수사를 위한 온라인수색이 있다. 독일에서는 온라인 수색이 국가의 정보취득

의 한 방법으로 명확한 법률 규정 없이 시도되어 오다가 2006년 12월 20일 노르트라인 웨스트팔렌주 헌법보호법에서 처음으로 이를 규정하였다. 그러나 독일 연방헌법재판소는 2008년 2월 27일 노르트라인 웨스트팔렌주의 온라인 수색 관련 규정을 무효로 선언하면서도 온라인 수색은 원칙적으로 엄격한 조건하에서만 허용된다고 결정하였다.

연방헌법재판소는 이 결정을 통해서 '정보기술시스템의 기밀성 및 무결성 보장에 관한 기본권'이라는 헌법상의 새로운 기본권, 즉 소위 'IT-기본권'을 창설하였다. 한편 독일 연방대법원은 2007년 1월 31일 현행 형사소송법상 온라인 수색은 허용될 수 없다고 결정한 바 있다. 독일연방헌법재판소의 위헌결정 이후 독일에서는 연방범죄수사청법, 바이에른주 헌법보호법, 바이에른주 경찰법 등에서 이러한 비밀 온라인 수색을 규정하고 있고, 최근 2011년 1월 27일 라인란트 팔츠주 경찰법에서도 이 규정을 입법하여 예방영역에서의 온라인 수색을 확대시키고 있다.

Ⅱ. 판례 동향

1. 2007년 1월 31일 연방대법원 결정[1)]

연방검찰청은 테러단체의 수사와 관련하여 형사소송법의 관련 규정에 근거하여 연방대법원의 영장담당판사에게 온라인 수색 명령을 청구하였다. 즉 형사소송법 제102조, 제105조 제1항, 제94조, 제98조, 제169조 제1항 2문에 근거하여 피의자가 이용한 개인용 컴퓨터와 랩톱, 특히 하드 드라이브와 임시기억장치에 보관되어 있는 데이터의 수색과 이의 압수를 명하고, 수사기관에게 이러한 조치를 비밀리에 수행하도록 허용하며, 컴퓨터의 저장매체에 보관되어 있는 데이터를 복제하고 열람할 목적으로 수사기관에게 전달하기 위해서 이를 위해 고안된 컴퓨터프로그램을 피의자 몰래 설치할 수 있도록 청구한 것이다.

이에 대하여 연방대법원 영장담당판사는 오늘날의 수사현실에 비추어 보면 형사절차에서의 중요한 정보가 컴퓨터에 저장되어 있음을 부인할 수 없지만, 현행 형사소송법은 '비밀 온라인 수색'을 허용하는 근거규정이 없으므로 이는 허용되지 않는다고 판단하여 검찰의 청구를 기각하였다. 이에 대하여 연방검찰청은 항고를 제기하였으나, 연방대법원 역시 '비밀 온라인 수색'은 현행 형사소송법상 수권의 근거가 없어서 허용되지 않는다고 결정하였다.

2. 2008년 2월 27일 연방헌법재판소 결정

1) BGH, Beschluß vom 31. 1. 2007 - StB 18/06. 이 판례에 대한 평석으로는 박희영, 독일형사판례연구 Ⅰ [사이버범죄], 한국학술정보(2011.3), pp.191-202 참조.

독일에서 온라인 수색을 처음으로 도입한 법률은 2006년 12월 20일 노르트라인 베스트팔렌주 헌법보호법이다.[2] 이에 대해서 독일 연방헌법재판소는 이 법률의 온라인 수색 관련 규정은 무효로서 위헌이고, 온라인 수색은 원칙적으로 엄격한 조건하에서만 허용된다고 결정하였다. 연방헌법재판소는 이 결정을 통해서 '정보기술시스템의 기밀성 및 무결성 보장에 관한 기본권'이라는 헌법상의 새로운 기본권, 즉 소위 'IT-기본권('온라인 기본권', '컴퓨터 기본권', '정보통신기본권'이라고도 함)'을 창설하였다.[3]

Ⅲ. 법제 동향

1. 노르트라인 베스트팔렌州 헌법보호법[4]

2006년 12월 20일 노르트라인 베스트팔렌주 헌법보호법 제5조[5]는 주헌법보호청의 직무를 수행하기 위한 권한을 새로이 도입하였다. 정보기관으로써 주 헌법보호청이 수행할 수 있는 권한으로는 ① 비밀요원의 투입, ② 감시, ③ 영상촬영, ④ 비밀수사, ⑤ 기술적 수단을 통한 감청, ⑥ 비공개대화의 감청, ⑦ 통신감청, ⑧ 위장상호 등 명칭 사용, ⑨ 위장신분증 사용, ⑩ 우편 검열(서신, 우편 및 통신비밀의 제한에 관한 법률[6]에 의한), ⑪ 온라인 수색, ⑫ 그 밖의 비교가능한 방법들을 규정하고 있었다.

이들 권한 중 온라인 비밀 수색에 해당하는 제11호는 "특히 통신장치에 비밀리에 참여하거나 통신장치를 수색하는 것과 같은 비밀 관찰과 그 밖의 인터넷 수사 및 기술적 수단의 투입으로 정보기술시스템에 비밀리에 접근하는 것. 그러한 조치가 서신, 우편 및 통신비밀을 침해하거나 종류와 중요성에서 이와 동일한 경우에는, 이 조치는 다만 서신, 우편 및 통신비밀의 제한에 관

2) 아래 노르트라인 베스트팔렌주 헌법보호법 참조.

3) 이 기본권을 분석한 초기 문헌으로는 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1, pp.92-123 참조. 독일에 있어서 예방적 온라인수색의 위헌성에 대해서는 박희영, 독일에 있어서 경찰에 의한 '예방적' 온라인수색의 위헌여부, 경찰학연구, 제9권 제2호(통권 제20호), 경찰대학교, 2009. 7, pp.185-209 참조. 이 결정에 대한 최근 평석으로는 박희영·홍선기 공저, 독일연방헌법재판소판례연구 Ⅰ [정보기본권], 한국학술정보(2010.12), pp.1-45참조. 이 결정에 대한 소개로는 박희영, 정보기술시스템의 기밀성 및 무결성 보장에 관한 기본권(상)(하) - 독일 연방 헌법재판소 결정(1 BvR 370/07, 1 BvR 595/07) -, 법제처, 법제 611호, 2008. 11, pp.43-68, 법제 612호, 2008. 12, pp.31-64 참조.

4) Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen - VSG NRW -).

5) 제5조 (권한) (1) 헌법보호청은, 제28조에 의해서 적용될 노르트라인 베스트팔렌주 정보보호법이나 동 법률의 특별규정에 모순되지 않는 한, 직무수행에 필요한 정보 및 개인정보를 처리할 수 있다.

6) 이 법률은 주로 독일의 국가정보기관의 정보활동과 관련한 법률로써 일반경찰활동에는 적용되지 않는다. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Artikel 10-Gesetz 또는 G 10이라고도 함.

한 법률상의 조건하에서만 허용된다"고 규정하고 있었다. 이 규정은 앞서 말한 바와 같이 2008년 2월 27일 연방헌법재판소의 위헌결정으로 무효로 되었다.

2. 연방 범죄수사청법

노르트라인 베스트팔렌주 헌법보호법의 온라인 수색 규정이 연방헌법재판소로부터 위헌결정을 받고 난 이후, 연방범죄수사청은 이 위헌결정을 토대로 하여 연방범죄수사청법 제20k조(정보기술시스템에의 비밀 침입)에서 온라인 수색을 규정하였다.

입법자는 본 규정의 도입과 관련하여 '국가의 안전과 국가가 보장해야 할 국민의 생명, 신체 및 자유에 대한 위험으로부터의 안전은 헌법적 가치가 있으며, 국가는 테러 또는 그 밖의 다른 기도를 통한 이러한 위험에 대처함으로써 헌법상의 직무를 이행한다'고 전제한 뒤, 이러한 목적을 달성하기 위해서는 제20k조에 규정된 정보기술 시스템에의 비밀 접근이 적절하고 필요하다고 입법이유를 밝히고 있다. 이러한 입법이유는 엄격하고 특정한 요건하에서만 그러한 조치가 헌법상 허용되는 것으로 인정한 연방헌법재판소의 결정을 따른 것이다.

즉 기본법 제2조 제1항 및 제1조 제1항에서 도출해낸 'IT 기본권'에 대한 침해는 예방적 또는 억압적 목적을 위해서도 정당화된다. 그러나 이러한 제한은 예방 영역을 위해서 상당히 중대한 법익에 대한 구체적인 위험의 존재를 전제로 하고 있다. 그러한 것으로는 사람의 생명, 신체, 자유에 대한 법익 또는 국가의 존립이나 토대를 위협하거나 인간의 존재를 위협하는 일반적인 법익이 이에 해당한다. 따라서 이러한 조치는, 특정한 사실이 개별적인 경우 특정한 사람을 통해서 위협되는 상당히 중대한 법익에 대한 임박한 위험을 암시하고 있는 한, 이러한 위험이 가까운 장래에 발생한다는 것이 충분한 개연성을 가지고 아직 확정되지 않는 경우에도, 이미 정당화될 수 있다.

- 제1항 : 연방범죄수사청은 중대한 법익에 대한 위험의 방지를 위하여 당사자 모르게 기술적인 수단을 통해서 당사자가 이용하고 있는 정보기술시스템에 침입하여 당사자의 데이터를 수집할 수 있다. '중대한 법익에 대한 위험'이란 ① 사람의 생명, 신체 및 자유에 대한 위험, ② 공공의 이익에 대한 위협이 국가의 기반이나 존립 또는 인간의 존재 기반을 위협하는 위험을 말한다. 특정한 사실이 앞서 언급한 법익 중 하나에 대해서 개별적인 경우에 특정인을 통해 야기된 임박한 위험을 암시하고 있는 한, 그 조치의 수행없이 가까운 장래에 손해가 발생한다는 것이 충분한 개연성으로 아직 확정될 수 없는 경우에도 이 조치는 허용된다. 이러한 조치는 다른 방법으로는 가망이 없거나 본질적으로 어려운 경우에 취해질 수 있다고 함으로써 비례성의 원칙을 구체적으로 밝히고 있다.
- 제2항 : 연방범죄수사청은 이 조치를 수행함에 있어서 정보기술시스템에 변경을 가하는

경우 이것은 오로지 데이터 수집을 위해 반드시 필요한 것이어야 하고, 그 변경은 조치의 종료시에 일반적으로 기술적으로 가능하게 소급하여 복구되도록 해야 한다. 그리고 투입된 수단은 기술의 상태에 의해서 무단 이용으로부터 보호되어야 한다. 복제된 데이터는 기술의 상태에 의해서 변경, 무단 삭제, 무단 인지로부터 보호되어야 한다.

■ 제3항 : 이러한 기술적 수단이 설치되는 경우 기록되어야 하는 내용으로는 ① 기술적 수단의 표지와 이의 설치 시점, ② 정보기술시스템의 신원을 확인하기 위한 정보와 여기에서 수행된 오로지 휘발성이 아닌 변경, ③ 수집된 데이터를 확정할 수 있게 하는 정보, ④ 조치를 수행하는 조직의 규모 등이다. 기록 데이터는 관련자 또는 이에 대한 권한이 있는 공공기관이 제1항에 의한 조치가 정당하게 수행되어 있는지의 여부를 심사할 수 있도록 하기 위해서만 사용될 수 있다. 기록 데이터는 저장기간의 종료시까지 보관되어야 하고 그리고 나서 그 기록이 앞의 심사 목적을 위해서 더 이상 필요하지 아니하는 한, 자동적으로 삭제되어야 한다.

① 기술적 수단의 표지와 이의 설치 시점 : 이에 관한 기록은 설치된 수단을 상세하게 기술적으로 설명할 필요는 없으나, 일반적으로 이해할 수 있는 기능범위에 관한 정보가 요구된다. 예를 들어 대상컴퓨터의 일시적인 수색의 수단 또는 지속적인 감시의 수단이 문제되는지, 대상컴퓨터 자체 또는 이와 연결된 저장매체에도 조치가 수행되어야 하는지, 저장 데이터가 복제되거나 키보드 입력도 기록되어야 하는지 등이 설명되면 족하다.

② 정보기술시스템의 신원을 확인하기 위한 정보와 여기에서 수행된 오로지 휘발성이 아닌 변경 : 잠입한 정보기술시스템의 신원 확인을 위한 정보뿐 아니라 그 시스템에서 시행된 단지 일시적인 변경이 아닌 것은 모두 기록해야 한다. 정보기술시스템의 신원을 명확하게 파악하는 표지가 없기 때문에, 정보기술시스템의 구체적인 개별화를 위해서, 하드웨어나 소프트웨어에 관한 수많은 정보를 기록할 필요가 있을 것이다. 변경보안을 위해서 별로 중요하지 아니하고 다양하게 이미 짧은 시간 후에(예를 들어 완전히 컴퓨터를 끈 이후에) 자동으로 삭제되는 적극적인 소프트웨어는 계속해서 정보기술 시스템의 일시적인 수많은 변경을 가하고 있기 때문에, 정보기술시스템의 일시적인 변경은 문서로 기록하지 않아도 된다. 이 경우 '일시적인 변경'의 개념은 협의로 해석되어야 한다. 즉 일시적 변경은 임시기억장치(RAM)에 저장되는 것을 말한다.

③ 수집된 데이터를 확정할 수 있게 하는 정보 : 이것은 수집된 데이터의 확정을 가능하게 하는 정보의 문서화를 말한다. 따라서 문서로 되어야 하는 것은 수집된 데이터 자체가 아니라 메타 데이터뿐이다. 그것은 수집된 데이터의 추론을 신뢰할 수 있게 하는 메

타 데이터이다. 그러한 메타 데이터는 예컨대 문서의 특성에 포함되어 있는 정보(데이터의 이름, 버전번호, 최근 변경 시점, 데이터의 크기)이다.

④ 조치를 수행하는 조직의 규모 : 연방범죄수사청의 어느 기관이 이 조치를 수행할 것인가를 기록해야 한다. 데이터의 기록은 엄격한 목적에 따라 규정되어야 한다. 이것이 의미하는 바는 이에 대해 권한이 있는 감독관청(BfDI)이나 법원 또는 정보청구권과 관련이 있는 당사자가 조치의 정당한 수행을 심사할 수 있도록 하기 위한 경우에 한해서만 데이터가 사용될 수 있다는 것이다. 즉 기록데이터의 사용은 당사자의 일반적인 데이터보호법상의 정보청구권의 수행에 관한 이용으로 제한되어 있다(§19 BDSG).

■ 제4항 : 온라인 수색은 연방경찰청법 제17조 또는 제18조에 의해 책임있는 자에 대해서만 취해질 수 있다(제4항). 따라서 수범자는 행위책임자 또는 상태책임자이다. 경찰법상 형성된 이러한 개념을 준용함으로써 조치의 가능한 수범자의 범위가 충분히 특정되어 제한된다.

■ 제5항 : 온라인 수색에는 법원의 명령이 필요하다. 즉 온라인 수색은 연방범죄수사청의 장 또는 그 대리인의 신청에 의해서만 법원에 의해 명령될 수 있다.

■ 제6항 : 온라인 수색 명령은 문서로 한다. 그 명령서에 기재되어야 할 내용은 ① 가능한 한 성명과 주소를 포함한 이 조치의 대상자, ② 데이터 수집을 위해서 침입되어야 할 정보기술시스템의 가능한 한 충분한 식별표지, ③ 종료시점이 언급된 조치의 종류, 범위 및 기간, ④ 본질적인 사유 등이다. 이 명령은 최고 3개월의 기한이 정해져 있다. 그리고 명령의 요건이 존속하는 한, 3개월을 초과하지 않는 범위에서 매 번의 연장은 허용된다. 명령의 요건이 더 이상 존재하지 않는 경우에는 명령을 근거로 하여 취해진 조치는 지체 없이 종료되어야 한다.

■ 제7항 : 온라인 수색의 경우 헌법상 허용되는 사적 생활형성의 핵심영역이 보호되어야 한다. 온라인 수색을 통해서 사적 생활형성의 핵심영역이 인지될 수 있다는 추측에 대한 사실상의 근거가 존재하는 경우에 그 조치는 허용되지 않는다. 가능한 한 사적 생활형성의 핵심영역과 관련이 있는 데이터는 수집되지 않아야 한다는 사실이 기술적으로 확보되어야 한다. 수집된 데이터는 명령을 내린 법원의 관리하에 지체 없이 연방범죄수사청의 데이터보호 수탁자와 연방범죄수사청의 두 공무원(한 사람은 법관의 신분이 있는 자)에 의해서 핵심영역관련 내용이 열람되어야 한다.

데이터보호 수탁자는 그들의 활동을 행사할 때에 지시를 받지 않으며 그로 인한 통지를 받을 필요도 없다(연방데이터보호법 제4f조 3항). 사적 생활형성의 핵심영역과 관련되는 데이터는 사용되어서는 아니되고 지체 없이 삭제되어야 한다. 데이터가 사적 생활형성의 핵심영역에 귀속되어 있는지의 여부가 의심이 있는 경우에는 이는 삭제되어야 하거나 지

체 없이 데이터의 사용가능성이나 삭제에 대한 결정을 위해 명령을 내린 법원에 제출되어야 한다. 데이터를 파악하는 사실(Tatsachen)과 삭제하는 사실은 문서로 기록되어야 한다. 이 문서는 데이터보호통제의 목적을 위해서만 사용될 수 있다. 이 문서는 이러한 목적을 위해서 더 이상 필요하지 않는 경우에는 삭제되어야 하지만, 늦어도 문서의 작성 연도의 말까지는 삭제되어야 한다.

이 규정은 2020년 12월 31일까지 기간이 정해져 있으며,[7] 발효 후 5년 동안 연방의회와 협조하여 학술적 전문가의 평가를 받도록 하고 있다.[8]

3. 바이에른州 헌법보호법

바이에른주 헌법보호법[9]은 2008년 7월 8일 법률개정을 통하여 온라인 수색에 관한 규정을 처음으로 도입한 후, 2009년 7월 27일 다시 법률개정을 통하여 관련 규정의 내용을 수정하였다. 현재 동 법률 제6e조에서 온라인 수색을 '비밀 온라인 데이터 수집'이란 표제어로 사용하고 있다.

비밀 온라인 데이터 수집은 우선 제1항에서 온라인 수색의 실질적인 요건들을 규정하고 있다. 이에 의하면 주헌법보호청은 접속데이터와 저장 데이터를 수집하기 위해서 동 법률 제6a조 제2항[10]의 요건하에 현저히 중대한 법익에 대한 구체적인 위험의 사실상의 근거가 존재하는 경우에 개별적인 경우 기술적인 수단을 통하여 비밀리에 정보기술시스템에 접근할 수 있다고 규정하고 있다. 이 조치는 문서로 기록되어야 한다. 이 명령은 사실관계의 조사가 다른 방법으로 불가능하거나 본질적으로 어려울 수도 있는 경우에만 허용된다고 함으로써 비례성의 원칙이 준수되도록 하고 있다. 이 명령은 혐의자와 그의 정보전달자에 대해서만 행해진다. 정보전달자에 대한 조치는 이들이 형사소송법 제53조 및 제

7) BT-Drs. 16/10822, S. 6.

8) BGBl. 2008 Teil 1 Nr. 66, S. 3094.

9) Bayerisches Verfassungsschutzgesetz(BayVSG).

10) 바이에른주 헌법보호법 제6a조(서신, 우편 및 전기통신의 비밀에 관한 법률의 보호영역에서 특별한 기술수단의 설치) (1) 주헌법보호청은 제6조 제3항에 의한 비례성의 원칙을 특별히 고려하여 제6조 제1항에서 말하는 정보기관의 수단으로써 통신비밀보호법의 보호영역에서의 기술적 수단을 설치할 수 있다. (2) 제1항에 의한 조치는, 누군가가 구체적인 경우 연방 또는 주의 존립이나 안전 및 사람의 생명, 신체 및 자유를 중대하게 위태롭게 하기에 적합한 범죄를 계획하거나 행함으로써 제3조 제1항 1문에 의한 시도나 활동을 추구한다는 혐의에 대한 사실상의 근거가 존재하는 경우에 한해서만 허용된다. 그러한 범죄들로는 1. 평화에 대한 죄, 내란의 죄, 간첩죄(형법 제80조, 제81조, 제82조, 제94조). 2. 공공질서에 관한 죄 중 테러단체조직 등에 관한 범죄(형법 제129a조, 제129b조), 3. 생명에 대한 죄(형법 제211조, 제212조, 국제형법 제6조), 4. 개인의 자유에 관한 죄(형법 제232조, 제233조, 제233a조 제2항, 제234조, 제234a조 제1항, 제239a조 제239b조), 5. 공공위험범죄(형법 제306a조, 제306b조, 제307조 제1항 및 제2항, 제308조 제1항, 제309조 제1항, 제310조 제1항, 제313조 제1항, 제314조 제1항, 제315조 제3항, 제315b조 제3항, 제316c조) 6. 무기법에 의한 범죄와 전쟁무기의 통제에 관한 법률에 의한 범죄(무기법 제51조 제1항 및 제2항, 제52조 제1항 및 제5항, 전쟁무기의 통제에 관한 법률에 의한 범죄 제19조 제2항, 제20조 제1항, 또는 제21조와 관련하여, 제22a조 제1항 및 제2항).

53a조에 의한 증인의 묵비권을 가지지 않는 경우에 한해서만 수행된다. 형사소송법 제53조 및 제53a조의 직업상비밀을 통해서 보호되는 신뢰관계의 침해가 인식되는 경우에는, 직업상비밀준수의무자 자신에 대해서 이 조치가 취해지지 않는 한, 이 조치는 허용되지 않는다. 정보기술적으로 그리고 수사기술적으로 가능한 경우, 사적 생활형성의 핵심영역에 속하는 데이터를 수집하는 것을 피할 수 있는 모든 조치들은 수행될 수 있다. 그러한 데이터가 관련되고, 이 데이터가 수집금지를 야기하는 목적에 기여하여야 하는 것에 대한 근거가 존재하지 않는 것을 알 수 있는 경우에는, 더 이상 데이터수집이 허용되어서는 아니된다.

제2항은 제1항에 의한 조치를 준비하기 위하여 정보기술시스템의 특별한 식별번호 및 위치를 조사하기 위해서 기술적 수단도 설치될 수 있다. 제3자의 개인정보는 이것이 기술적인 근거에서 불가피한 경우에만 수집될 수 있다. 조치의 종료 후 이것은 지체 없이 삭제되어야 한다.

4. 바이에른州 경찰법[11)]

바이에른주 경찰법은 2008년 7월 8일자 법률개정에서 온라인 수색에 관한 규정을 처음으로 도입한 후, 2009년 7월 27일자 법률개정을 통하여 내용이 수정되었다. 현재 제34d조에서 온라인 수색을 '정보기술시스템에의 비밀접근'이란 표제어로 사용하고 있다.

■ 제1항 : 경찰은 위험에 대하여 책임이 있는 자의 접속데이터와 저장데이터를 수집하기 위해서 기술적인 수단으로 정보기술시스템에 비밀리에 접근할 수 있다. 정보기술시스템에 비밀리에 접근하는 것(즉 온라인 수색)은 크게 두 가지로 나누어진다. 하나는, a) 연방 또는 주의 존립과 안전, b) 위협이 있는 경우 인간 존재의 토대를 침해하게 되는 일반공중의 법익, c) 사람의 생명, 신체 또는 자유에 대한 긴박한 위험을 방어하기 위하여 필요한 경우(제1항 제1호)이다. 다른 하나는 a) 누군가가 제1호의 사람들에게 특정되어 있는 통지나 이들로부터 기인하는 통지를 받거나 받았고 이와 관련하여 형사소송법 제53조 및 제53a조에 의한 증인의 묵비권을 갖지 않거나 그러한 통지를 전달하거나 전달한 경우 또는 제1호에 언급된 자들의 소속하에 그들의 정보기술시스템을 이용하거나 이용하였다는 근거가 되는 추측을 특정한 사실들이 정당화하는 경우이다(제2호)(제1항 제1문).

다만 제1문에 의한 조치는 경찰직무의 이행이 다른 방법으로 가망이 없을 수 있거나 본질적으로 어려울 수 있는 경우에만 수행될 수 있다(제2문). 데이터는 생명 또는 신체에 대한 현존하는 위험이 달리 방어될 수 없는 경우에

11) GESETZ ÜBER DIE AUFGABEN UND BEFUGNISSE DER BAYERISCHEN STAATLICHEN POLIZEI (POLIZEIAUFGABENGESETZ - PAG).

제1문의 요건하에서 삭제될 수 있다(제3문). 형사소송법 제53조 및 제53a조의 직업상 비밀을 통해서 보호되는 신뢰관계의 침해가 인식될 수 있는 경우에는 그 조치가, 직업상 비밀준수자 자체에 대해서 향해져 있지 않다면 허용되지 않는다(제4문). 이것이 정보기술적으로 그리고 수사기술적으로 가능하다면, 경찰은 적절한 조치를 통해서 사적 생활형성의 핵심영역이 고려되는 데이터의 수집을 중지하는 것을 확보하여야 한다(제5문). 그러한 데이터가 관련되고, 이 데이터가 수집금지를 야기하는 목적에 기여하여야 하는 것에 대한 아무런 근거가 존재하지 않는 것이 인식될 수 있는 경우에는, 이 조치는 허용되지 않는다(제6문). 제1문과 제3문에 의한 조치들은 문서로 기록되어야 한다(제7문).

■ 제2항 : 경찰은 ① 제1항에 의한 조치의 준비를 위한 특별한 인식번호, ② 정보기술시스템의 위치를 조사하기 위해서 제1항의 요건하에서 기술적 수단도 설치할 수 있다. 제3자의 개인정보는 기술적인 이유로 불가피한 경우에만 수집될 수 있다. 수집된 제3자의 개인정보는 조치 종료 후 지체 없이 삭제되어야 한다.

■ 제3항 : 제34조 제4항 제1문[12]은 이를 준용한다. 법원의 명령을 위해서 제24조 제1항 제3문은 동일하게 적용될 수 있다. 법원조직법 제74a조 제4항에 언급한 법원의 관할 내에 청구 경찰관서의 소재지가 있는 법원이 관할한다. 이의제기에 대해서는 법원조직법 제120조 제4항 제2문에 언급한 법원이 판단한다. 제1항과 제2항에 의한 조치의 명령은 문서로 명령하여야 하고 그 근거가 있어야 한다. 가능한 한 이 명령은 이 조치가 취해지는 당사자의 성명과 주소, 접근되어야 할 정보기술시스템의 표지를 포함하여야 한다. 명령에는 조치의 기술, 범위 그리고 기간이 특정되어야 한다. 명령은 최고 3개월의 기간이 정해져 있다. 매번의 연장은 그 요건이 계속 존재하는 경우에 한 달 이상을 넘지 않는 것은 가능하다. 제1항과 제2항에 언급한 요건이 더 이상 존재하지 않는 경우, 이 조치는 지체 없이 종료되어야 한다. 종료는 법원에 통지하여야 한다.

■ 제4항 : 데이터 열람시 데이터가, ① 사적 생활형성의 핵심영역에 속하거나, ② 형사소송법 제53조 및 제53a조에 의한 성직자, 변호인, 변호사, 의사, 마약중독 상담자, 심리치료의사 또는 아동 및 청소년 심리치료의사로서 증언이 거부될 수 있는 내용과 관련되거나, ③ 다른 직업상비밀준수자와 신뢰관계에 속해 있다는 점에 대한 근거가 있는 경우에는, 이 데이터는 지체 없이 삭제되거나 이의 확대 이용에 대한 판단을 구하기 위해서 제1항의 명령을 내린 판사에게 제출되어야 한다. 지체의 위험이 있는 경우 그 결정은 제33조 제5항 제1

12) 제34조 주거 내에서의 기술적 수단의 설치에 관한 특별 규정.

문에서 언급한 기관이 관련될 수 있다. 이 경우에는 법원의 결정이 지체 없이 사후에 보완되어야 한다. 삭제는 문서로 기록되어야 한다.

■ 제5항 : 제1항과 제2항에 의한 조치를 통해서 수집된 개인정보는 특히 표시가 되어야 한다. 개인정보들은 수집된 목적을 위해서만 사용될 수 있다. 평가 이후에 ① 이의 수집을 위한 요건이 존재하지 않거나, ② 이들이 형사소송법 제53조 및 제53a조에 의한 성직자, 변호인, 변호사, 의사, 마약중독 상담자, 심리치료사, 아동 및 청소년 심리치료사로서 증언이 거부될 수 있는 내용과 관련이 있거나, ③ 그것이 사적 생활형성의 핵심영역이나 다른 비밀준수자와 신뢰관계에 귀속되고 제1항 제1문에 언급한 위험과 직접 관련이 없다는 것이 명백하게 된 데이터는 사용되어서는 아니된다. 이것은 이의 사용이 개인의 생명, 신체 그리고 자유에 대한 현재의 위험을 방어하기 위해 필요한 경우와 데이터가 제2호 또는 제3호의 데이터와 관련이 없는 경우에는 적용되지 않는다. 이들 사례에서는 사용의 허용에 관한 법원의 판단이 지체 없이 보완되어야 한다. 제3항 제2문은 이에 준용한다.

■ 제6항 : 사적 생활형성의 핵심영역에 속하여 사용될 수 없는 정보는 지체 없이 삭제되어야 한다. 삭제는 문서로 기록되어야 한다. 제1항과 제2항에 의한 조치를 통하여 획득된 개인정보가 ① 제5항 제2문에 언급한 목적을 위해서 사용할 필요가 없거나, ② 이를 위해서 사용금지가 존재하는 경우, 이들 데이터가 관련자의 정보의 목적을 위해서 그리고 데이터의 수집이나 사용에 대한 법원의 심사를 위해서 여전히 필요로 하는 경우에는 차단되어야 한다. 그렇지 않으면 이들은 삭제되어야 한다. 제34조 제7항 제3문과 제4문은 이를 준용한다.

■ 제7항 : 제1항과 제2항에 의한 조치는 ① 그 조치가 취해졌던 자 및 ② 이 조치와 관련하여 개인정보가 수집되거나 삭제되고 그리고 제5조 제2문의 목적으로 사용된 자에게 통지되어야 한다. 조치의 목적이나 투입되어 비공개로 조사하고 있는 공무원 또는 제1조 제1문 1호에 언급되어 있는 법익의 위태화 없이 이것이 발생할 수 있는 즉시 통지되어야 한다. 동일한 사실관계로 관련자에 대해서 수사절차가 수행되고 있는 경우에는, 그 통지는 수사절차의 상태에서 허용되는 즉시 검찰의 동의하에 되어야 한다. 제34조 제6항 제3문 내지 제5문은 이를 준용한다. 법원의 관할과 절차는 제3문의 경우 형사소송법의 규정에 따르고, 그 밖의 경우에는 제3항 제2문 내지 제3문이 적용된다.

■ 제8항 : 주정부는 매년 주의회에 접근데이터를 제외한 제1항 제1문에 의해 수집한 데이터 및 제1항 제3문에 의해 그러한 데이터의 삭제에 대하여 보고한다. 제34조 제9항 제2문은 이를 준용한다. 보고서에 기입되어야 할 내용은 ① a) 첫 명령과 b) 연장명령을 구별하여 수행된 조치를 뒷받침하고 있는 명령의 수, ② 각 명령기간, ③ a) 데이터의 수집, b) 데이터의 삭제에 따라 구별하여 수행된 조치의 수,

④ 조치의 법률상의 근거 등이다.

5. 라인란트-팔츠州 경찰법

라인란트 팔츠주 의회는 2011년 1월 27일 경찰법 개정안을 만장일치로 통과시켰다. 이번 개정안은 주로 정보통신기술의 급속한 발전으로 인한 새로운 도전들에 대한 경찰법상의 대처방안을 규정하고 있다. 그러한 것 중에서는 제31c조는 '기술적 수단을 투입한 정보기술시스템에 있는 데이터의 수집'이란 표제어로 온라인수색을 규정하고 있다.

■ 제1항 : 경찰은 관련자 모르게 기술적 수단을 통하여 관련자가 이용하고 있는 정보기술시스템에 침입하여 거기에 있는 데이터를 수집할 수 있다. 이러한 조치는 사람의 생명, 신체 및 자유에 대한 위험을 방지하거나 그 위협이 국가의 토대 및 존립 또는 인간 생존의 토대를 침해하는 공공의 이익에 대한 위험을 방지하기 위해서 취해진다. 이 조치의 대상자는 ① 행위책임자(동법 제4조)와 상태책임자(동법 제5조) 그리고 행위 및 상태 책임자가 아니지만, 일정한 요건을 갖춘 자(동법 제7조) 또는 ② 행위책임자(동법 제4조) 및 상태책임자(동법 제5조)에게 특정되어 있는 통지나 그들로부터 기인하는 통지를 받거나 교부한다는 가정이 정당화되는 사람이다(제1문). 다만 이 조치는 제1문에 의한 직무수행이 다른 방법으로는 가능하지 않아 보이거나 본질적으로 어려울 수 있고, 인식한 내용이 오로지 사적 생활형성의 핵심영역에서만 획득된다는 가정에 대한 사실상의 근거가 없는 경우(제39a조 제3항)에만 허용된다. 또한 이 조치는 제3자가 불가피하게 관련되는 경우에도 수행될 수 있다.

■ 제2항 : 이 조치와 관련하여 기술적으로 확보되어야 하는 것은, ① 정보기술시스템에서의 변경은 데이터수집을 위해서 불가피한 경우에만 취해지고, ② 변경이 있는 경우 기술적으로 가능한 경우에는 조치의 종료시에 자동적으로 복구되도록 해야 한다. 취해진 수단은 기술의 수준에 따라서 무단 이용으로부터 보호되어야 하고, 복제된 데이터는 기술의 수준에 따라서 변경, 무단 삭제 그리고 무단 인식으로부터 보호되어야 한다.

■ 제3항 : 제1항에 의한 조치를 준비하기 위하여 필요한 특별한 식별번호와 같은 데이터 및 정보기술시스템의 위치를 조사하기 위하여 제1항의 요건하에서 기술적 수단이 취해질 수 있다. 이 경우 제3자의 개인정보는 기술적 이유로 불가피한 경우에 한해서만 수집될 수 있다.

■ 제4항 : 기술적 수단을 개별적으로 투입하는 경우에 문서로 기록되어야 한다. 기록될 내용은 ① 기술적 수단의 표지와 이의 투입 시간, ② 정보기술시스템을 확인하기 위한 정보와 이를 위해 취해진 변경이 단지 일시적이 아닌 경우, ③ 수집된 데이터의 확인을 가능하게 하는 정보, 그리고 ④ 조치를 수행한 조직단위이다.

문서로 기록된 데이터는 제1항에 의한 조치가 정당하게 수행되어 있는지에 대해서 권한이 있는 공공기관이나 관련자에게 심사를 가능하게 하기 위해서만 사용된다. 문서기록 데이터는 이러한 심사목적을 위해서 더 이상 필요하지 않는 한 지체 없이 삭제되어야 한다.

■ 제5항 : 데이터 수집에는 법원의 결정이 필요하다. 그 명령장에 특히 특정되어야 할 내용은 ① 요건과 본질적인 이익형량, ② 가능한 한 성명과 주소가 포함된 조치의 대상자, ③ 종료시점이 언급된 조치의 방법, 범위 그리고 기간, ④ 가능한 한 기술적 수단 및 데이터 수집을 위해서 취해지는 정보기술 시스템의 충분한 특정 등이다. 이 조치는 최대 3개월로 기한이 정해져 있다. 명령의 요건이 계속 존재하는 경우에 매번의 연장은 한 달 이상 허용되지 않는다.

■ 제6항 : 제29조 제5항과 제8항은 이에 준용한다. 즉 주거 내외에서 기술적 수단을 비밀리에 설치하여 수집된 개인정보는 특별히 표시되어야 하고, 전달 이후 그 표시는 수신인을 통해서 유지되어야 하며, 그 정보가 ① 형사소송법에 의하여 주거감청을 정당화하는 특별히 중대한 범죄의 소추를 위하여, ② 제1항의 임박한 위험을 방지하기 위하여 필요한 경우에는 다른 목적을 위해서 사용될 수 있다. 이러한 목적의 변경은 개별적으로 확정되고 문서로 기록되어야 한다(제29조 제5항). 한편, 주정부는 수행된 기술적 수단의 설치가 법관의 명령을 요하는 경우에는 이를 매년 주의회에 보고한다. 주의회의 통제위원회는 이러한 보고를 근거로 의회의 통제권을 행사한다(제29조 제8항).

Ⅳ. 시사점

한국에서는 아직 온라인 비밀 수색이 현실적인 사회문제로 대두되지는 않았지만, 현재 한국의 정보기술시스템의 인프라 수준을 감안할 때 그럴 위험이 현실화될 여건은 충분히 성숙되어 있다고 보여진다. 따라서 앞으로 한국 사회에서도 발생 가능성이 충분히 있는 온라인 비밀 수색과 관련한 입법론을 모색할 때 독일의 판례와 입법례는 우리에게 시사하는 바가 많을 것이다. 입법시 유의해야 할 점은 온라인 수색의 경우 국민의 기본권 침해가 중대하다는 점이다. 따라서 이를 충분히 보장하는 법규정이 동시에 입법되어야 할 것이다.

박 희 영
(해외입법조사위원,
독일 막스플랑크 국제형법연구소 연구원)