국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향

박희영 | 법학박사, 독일 막스플랑크 국제형법연구소 연구원

Ⅰ 머리말

국가기관이 기술적 수단(원격 통신 감시 소프트웨어)[1]을 이용하여 이용자의 정보기술시스템에 비밀리에 접근하여 이용자의 시스템 이용을 감시하고 시스템에 저장된 내용을 열람하거나 수집하는 것을 온라인 수색(Online Durchsuchung)이라고 한다.[2] 온라인 수색은 테러범죄나 조직범죄와 같은 혐의를 받고 있는 자가 인터넷으로 연결되어 있는 휴대전화나 컴퓨터와 같은 정보기술시스템을 이용하고 있는 경우 이 컴퓨터에 감시 소프트웨어를 몰래 설치하여 거기서 작업하고 있는 내용이나 저장되어 있는 데이터를 열람하거나 복제하는 새로운 정보수집방법으로서 국가의 합법적인 해킹행위라 할 수 있다. 감시 소프트웨어는 이메일의 첨부파일을 이용하거나 특정 인터넷사이트로 유인하거나 시스템의 백도어나 취약점을 이용하거나 해당 시스템에 직접 접근하여 설치하게 된다.

온라인 수색은 또한 인터넷에 연결되어 있는 컴퓨터에 접근하는 것이어서 암호화되기 전 또는 복호화된 후 송신자나 수신자의 통신기기에서 전자우편이나 스카이프와 같은 인터넷전화의 내용을 감청할 수 있다. 이러한 방식의 전기통신감청을 암호통신감청(Quellen TKÜ)이라고 한다.[3] 일반적인 통신감청은 송신자나 수신자의 지배영역을 떠나서 전기통신사업자의 지배영역에 있는 현재 진행 중인 통신을 대상으로 하지만, 암호통신감청은 송신자나 수신자의 지배영역인 통신기기에서 감청이 이루어진다. 암호통신감청에서 독일어 Qullen은 통신의 출처 또는 진원지를 의미하므로 대상자의 통신기기를 말한다. 이러한 통신감청은 암호화된 통신의 내용을 감청한다는 의미에서 암호통신감청이라고 한다. 암호통신감청은 기본적으로 온라인 수색의 기술적 수단을 이용하기 때문에 '작은' 온라인 수색이라고 부른다.

온라인 수색은 그 밖에 외부에서 컴퓨터에 장착되어 있는 마이크나 웹캠을 작동시켜 컴퓨터 작업을 하고 있

---

1 Remote Communication Interception Software (RCIS). 독일에서는 국가 트로이 목마(Staatstrojaner) 또는 연방 트로이 목마(Bundestrojaner)라고 부른다.

2 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018·여름), 30; 독일 형사소송법의 온라인 수색이 도입되기 이전의 온라인 수색의 입법방향에 대해서는 박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 2012.9, 153-186.

3 일반통신감청, 암호통신감청, 패킷감청, 온라인 수색의 차이점에 대해서는 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018 ·여름), 28-31.

는 온라인 수색은 그 밖에 외부에서 컴퓨터에 장착되어 있는 마이크나 웹캠을 작동시켜 컴퓨터 작업을 하고 있는 수색 대상자의 모습이나 작업공간을 관찰할 수도 있다. 이러한 점에서 온라인 수색은 비밀성, 지속성, 대상의 상대적 무제한성이라는 성격을 가지고 있다. 이러한 성격으로 공개적이고 일회적이며 대상이 한정되어 있는 오프라인(offline) 수색과 구별된다. 따라서 온라인 수색은 범죄예방이나 범죄수사 목적으로 지금까지 등장한 국가의 비밀 처분 중에서 가장 강력한 처분이어서 헌법상 국민의 기본권을 침해할 위험성이 상당히 높다.

현재 이러한 온라인 수색이 실무에서 실제로 수행되고[4] 법적 논의도 가장 활발한 곳이 독일이다. 독일은 오래 전부터 위험예방 및 범죄예방 목적의 온라인 수색을 보안 및 경찰 관련 법률에 도입하였으며 이에 관한 연방헌법재판소의 판결도 존재한다. 최근 연방헌법재판소의 연방범죄수사청법(BKAG)에 관한 일부 위헌 판결로 온라인 수색에 관한 논의가 다시 시작되었다.[5] 따라서 이 글은 독일의 온라인 수색에 관한 최근의 법제 동향을 소개하고 우리에게 주는 시사점을 제시한다.

II 2016년 연방범죄수사청법의 일부 위헌 판결 이전의 법적 상황 개관

독일에서 온라인 수색은 국가기관의 정보 수집의 한 방법으로 명확한 법률 규정없이 시행되어 오다가 2006년 12월 20일 노르트라인 웨스트팔렌주 헌법보호법에서 범죄예방 목적으로 처음으로 규정되었다.[6] 하지만 이 규정은 연방헌법재판소로부터 2008년 2월 27일 무효로 선언되어 위헌판결을 받았다.[7][8] 그럼에도 불구하고 연방헌법재판소는 온라인 수색은 원칙적으로 엄격한 요건을 갖추면 허용된다고 판단했다. 또한 연방헌법재판소는 이 결정을 통해서 '정보기술시스템의 기밀성 및 무결성 보장에 관한 기본권'이라는 헌법상의 새로운 기본권, 즉 소위 'IT-기본권'을 창설하였다. 연방헌법재판소의 위헌 결정 이후 독일에서는 연방범죄수사청법[9], 바이에른주 헌법보호법[10], 바이에른주 경찰법[11], 라인란트 팔츠주 경찰법[12] 등에서 이러한 범죄예방 목적의 온라인 수색을 규정하였다. 이에 반해서 연방대법원은 2007년 1월 31일 현행 형사소송법상 온라인 수색은 허용될 수 없다고 결정하였다.[13]

---

4 IT 분야에서 보안기관을 지원하기 위해서 보안분야 정보기술 중앙 센터(ZITiS)가 설립되어 있다. 여기서는 온라인 수색을 포함한 전기통신감청을 담당한다. 하지만 연방범죄수사청(BKA)는 독자적인 온라인 수색 프로그램을 개발하여 사용하고 있다.(https://bit.ly/2NeIwN5)

5 2016년 연방범죄수사청법의 일부 위헌 판결 이전의 법적 상황에 대해서 자세한 내용은 박희영, 독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제동향, 최신외국법제정보, 한국법제연구원, 2011-2호(2011.4.20.), 70-84.

6 2006년 12월 20일 노르트라인 웨스트팔렌주 헌법보호법 제5조.

7 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07(https://bit.ly/2VTdeQi).

8 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1, 92-123. 이 결정에 대한 평석으로는 박희영·홍선기 공저, 독일연방헌법재판소판례연구 Ⅰ [정보기본권], 한국학술정보(2010.12), 1-45. 이 결정에 대한 소개로는 박희영, 정보기술 시스템의 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, 43-68; 법제 612호, 2008. 12, 31-64.

9 연방범죄수사청법 제20k조.

10 바이에른주 헌법보호법 제6a조.

11 바이에른주 경찰법 제34d조.

12 라인란트-팔츠 주 경찰법 제31c조.

13 BGH, Beschluß vom 31. 1. 2007 - StB 18/06.(https://bit.ly/2TCRF9q) 이 판례에 대한 평석으로는 박희영, 독일형사판례연구 Ⅰ [사이버범죄], 한국학술정보(2011.3), 91-202.

최근 독일에서 온라인 수색에 관한 논의가 다시 시작되었다.[14] 연방범죄수사청법(BKAG)에 관한 연방헌법재판소의 일부 위헌 판결이 계기가 되었다. 연방헌법재판소가 이 판결에서 BKAG의 비밀 처분 중 온라인 수색은 헌법에 합치하도록 해석하는 경우 헌법과 일치할 수 있다고 하였기 때문이다. 이를 기화로 범죄수사를 위한 온라인 수색이 드디어 형사소송법에도 도입되었다. 그리하여 현재 독일에서는 범죄예방 및 범죄수사를 위한 온라인 수색이 모두 법률에 규정되어 있다.

Ⅲ 2016년 연방범죄수사청법의 일부 위헌 판결

1. 개정 전 연방범죄수사청법의 온라인 수색

연방범죄수사청(BKA)은 노르트라인 웨스트팔렌주 헌법보호법의 온라인 수색에 관한 위헌 판결에서 연방헌법재판소가 제시한 기준을 토대로 연방범죄수사청법 제20k조에서 온라인 수색을 도입하였다.[15] 제20k조는 온라인 수색을 '정보기술시스템에 대한 비밀 침입'으로 표시하였다.

제20k조 제1항에 따르면 연방범죄수사청은 중대한 법익에 대한 위험[16]을 방지하기 위하여 당사자 모르게 기술적인 수단을 통해서 당사자가 이용하고 있는 정보기술시스템에 침입하여 당사자의 데이터를 수집할 수 있었다. 특정한 사실이 개별적으로 특정인을 통해서 중대한 법익 중 하나에 대해 임박한 위험을 암시하고 있는 한, 이 처분을 실행하지 않으면 가까운 장래에 손해가 발생한다는 충분한 개연성이 아직 확정될 수 없는 경우에도 이 처분은 허용되었다. 또한 이러한 처분은 다른 방법으로는 가망이 없거나 본질적으로 어려운 경우에 취해질 수 있다고 함으로써 비례성 원칙을 구체적으로 명시하고 있었다.

제20k조 제2항은 온라인 수색에 따른 정보기술시스템의 변경과 원상복구 그리고 무권한 이용에 대한 보호를 규정하고 있었다. 온라인 수색으로 수집한 데이터는 또한 변경, 무권한 삭제, 무권한 인지로부터 보호되어야 했다.

제20k조 제3항은 온라인 수색이 수행되는 경우 기록되어야 할 내용을 규정하고 있었다. 즉 ① 기술적 수단의 표지와 이의 설치 시점, ② 정보기술 시스템의 신원을 확인하기 위한 정보와 여기에서 수행된 오로지 휘발성이 아닌 변경, ③ 수집된 데이터를 확정할 수 있게 하는 정보, ④ 조치를 수행하는 조직의 규모가 기록되어야 했다.

제20k조 제4항은 온라인 수색이 행해질 수 있는 대상자를 연방경찰법의 행위책임자(제17조)와 상태책임자(제18조)로 제한하고 있었다. 온라인 수색에는 법원의 명령이 필요하였다(제5항). 법원의 온라인 수색 명령은 문서로 하며, 명령 기간은 3개월이며 명령요건이 존재하는 경우 3개월이 초과하지 않는 범위에서 매 번 연장이 가능하지만, 명령의 요건이 더 이상 존재하지 않는 경우에는 명령을 근거로 하여 취해진 처분은 지체없이 종료되어야 했다(제6항).

14 2016년 연방범죄수사청법의 일부 위헌 판결 이전의 법적 상황에 대해서 자세한 내용은 박희영, 독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제동향, 최신외국법제정보, 한국법제연구원, 2011-2호(2011.4.20.), 70-84.

15 테러방지를 위한 연방범죄수사청법의 개정에 대해서는 박희영, 독일 연방사법경찰청에 의한 국제테러의 위험 방지를 위한 법률(상), 법제처, 법제 제613호, 2009. 1, 20-43; (하), 법제처, 법제 614호, 2009. 2, 15-49.

16 여기서 '중대한 법익에 대한 위험'이란 ① 사람의 생명, 신체 및 자유에 대한 위험, ② 공공의 이익에 대한 위협이 국가의 기반이나 존립 또는 인간의 존재기반을 위협하는 위험을 말한다.

제20k조 제7항은 온라인 수색 시 헌법상 허용되는 사생활의 핵심영역을 보호하고 있었다. 온라인 수색을 통해서 사생활의 핵심영역이 인지될 수 있는 사실상의 근거가 존재하는 경우에 그 조치는 허용되지 않았다. 사생활의 핵심영역과 관련되는 데이터가 수집되지 않도록 가능한 한 기술적으로 확보되어야 했다. 연방범죄수사청의 데이터보호감독관과 연방범죄수사청의 두명의 공무원(한 사람은 법관의 신분이 있는 자)은 명령을 내린 법원의 지휘를 받아 지체없이 수집된 데이터에서 핵심영역에 관한 내용이 있는지 열람해야 했다. 데이터보호감독관은 자신의 활동을 행사할 때에 지시를 받지 않으며 이로 인한 통지도 받을 필요가 없었다(연방데이터보호법 제4f조 3항). 사생활의 핵심영역과 관련되는 데이터는 사용되어서는 안 되고 지체없이 삭제되어야 했다. 데이터가 사생활의 핵심영역에 속하는지 의심이 있는 경우에는 삭제되거나 지체없이 데이터의 사용가능성이나 삭제에 대한 결정을 위해 명령을 내린 법원에 제출되어야 했다. 데이터의 수집과 삭제는 문서로 기록되어야 했다. 이 문서는 데이터보호통제의 목적을 위해서만 사용될 수 있었다. 이 문서는 이러한 목적을 위해서 더 이상 필요하지 않는 경우에는 삭제되어야 하고, 늦어도 문서의 작성 년도 말까지는 삭제되어야 했다.

2. 연방헌법재판소의 일부 위헌 판결

연방헌법재판소는 2016년 4월 20일 연방범죄수사청법(BKAG)의 국제테러의 위험을 방지하기 위한 비밀감시처분들(예를 들어 주거내 음성 감시[17], 온라인 수색, 전기통신감청, 통신사실확인자료 수집, 데이터를 수집하기 위한 특별한 수단을 사용한 주거외 감시)에 관한 수권규정은 기본적으로 헌법상 기본권과 일치하지만, 사생활의 핵심영역의 보호에 관한 규정은 헌법에 합치하지 않는다고 판결하였다.[18]

온라인 수색 규정인 BKAG 제20k조와 관련해서도 연방헌법재판소는 헌법에 합치하도록 해석하는 경우 이 조항은 일반적인 제한요건의 관점에서 헌법과 일치할 수 있다고 하였지만, 사생활의 핵심영역의 보호에 관한 규정은 헌법상의 요청을 충족하지 못한다고 하였다[19]

제20k조 제1항은 정보기술시스템에 접근하여 온라인 수색을 비밀리에 수행할 수 있도록 허용하고 있다. 이러한 온라인 수색으로 당사자 자신의 컴퓨터나 네트워크로 연결된 타인의 컴퓨터(예를 들어 소위 클라우드)에 업로드되어 있는 사적인 데이터가 수집되고 당사자의 온라인상 행위가 추적될 수 있다. 따라서 이 조항은 기본법상 일반적 인격권(제1조 제1항과 관련한 기본법 제2조 제1항)에서 도출되는 IT 기본권을 제한한다.[20]

헌법은 IT 기본권을 일반적 인격권에서 도출함으로써 오늘 날 사생활 영역에서 인격발현을 위해 정보기술시스템을 이용하는 의미를 충분히 고려하고 있다고 한다. 일기장, 은밀한 영역에서의 내용, 기타 고도의 개인적인 경험을 다룬 글, 영화 또는 음성기록 등은 오늘 날 데이터 형태로 제작되어 저장되고 일부는 교환되고 있다. 고도의 개인적인 통신도 인터넷상의 통신서비스나 인터넷 기반의 소셜 네트워크를 통하여 전자적으로 행해지고 있다. 이 경우

17 주거내 음성 감시는 주거내에서 행해지는 비공개 대화를 기술적 수단을 이용하여 엿듣거나 녹음하는 강제처분을 말한다.

18 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09. 이 판결에 대한 소개로는 박희영, 테러 방지를 위한 연방범죄수사청법의 통신감청권 등 일부 위헌, BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, 최신독일판례연구, 로앤비(www.lawnb.com), 2016.10, 1-10.

19 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 208.(http://www.bverfg.de/e/rs20160420_1bvr096609.html)

20 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 209.

당사자는 데이터의 기밀성에 의존하고 광범위하게 자신의 정보기술시스템만이 아니라 제3자의 정보기술시스템에 있는 데이터도 신뢰한다. IT 기본권은 이에 상응하게 이들 데이터에 대한 비밀 접근을 보호하고 특히 온라인 수색으로부터 보호한다. 온라인 수색으로 사인의 컴퓨터 및 그 밖의 정보기술시스템이 조정되고 열람되고 외부 서버에서 정당한 신뢰에 근거하여 비밀리에 저장되어 있는 개인 데이터가 수집되고 네트워크에서 당사자의 활동이 추적된다. 특히 이러한 연결로부터 발생하는 데이터의 고도의 인격적 성격 때문에 이 기본권의 침해는 특별한 강도가 있다. 따라서 헌법재판소는 온라인 수색으로 인한 침해는 비중의 관점에서 주거의 불가침의 침해와 비교할 수 있다고 평가하였다.[21)]

헌법재판소는 또한 정보기술시스템에 접근하기 위한 제20k조 제1항과 제2항의 요건은 헌법에 합치하도록 해석하는 경우에 헌법상의 요구사항을 충족한다고 하였다.[22)] IT 기본권의 제한은 물론 엄격한 요건하에서 가능하다.[23)] 특히 그 처분은 개별적으로 현저히 중대한 법익에 대한 임박한 구체적 위험이 있다는 사실상의 근거가 존재하는 경우에 가능하다.[24)] 제20k조 제1항은 이러한 요건을 충족한다고 한다.[25)]

제20k조 제1항 2문은 특정한 사실이 개별적으로 특정인을 통해서 중대한 법익 중 하나에 대해 임박한 위험을 암시하고 있는 한, 이 처분을 실행하지 않으면 가까운 장래에 손해가 발생한다는 충분한 개연성이 아직 확정될 수 없는 경우에도 이 처분을 허용하고 있다. 이 조항은 특정한 사실이 개별적으로 테러범죄를 범할 것이라는 임박한 위험을 암시하는 경우 이미 구체적인 위험의 전 단계에서도 처분을 이행할 가능성을 열어놓고 있으므로 헌법합치적으로 제한하여 해석해야 한다. 즉 특정한 사실들이 적어도 그 성격에 따라서 구체화되고 시간적으로 예견할 수 있는 사건들의 추론을 허용하는 경우, 그리고 특정한 자가 참여하고 있고, 적어도 그의 신분이 많이 알려져서 그에 대한 감시처분이 의도적으로 사용되고 나아가서 이것으로 제한될 수 있는 경우에만 그 처분이 허용되는 것으로 해석되어야 한다.[26)] 그러한 점에서 그 성질에 따라서 구체화되고 시간적으로 예견할 수 있는 사건을 아직 인지할 수는 없지만, 당사자가 예견할 수 있는 장래에 그러한 범죄를 행할 것이라는 구체적인 개연성을 그의 개인적인 행위가 뒷받침하는 경우에도 충분하다.[27)]

헌법재판소는 또한 이 조항은 실질적 요건의 관점에서도 비례성 원칙을 충족한다고 하였다. 특히 제20k조 제2항은, 접근을 통해서 발생하는 정보기술시스템의 변경을 최소화하고, 제3자가 이를 이용할 가능성을 피하고, 종료 후 가능한 한 이를 복구할 수 있어야 한다는 것을 규정하고 있다.[28)] 따라서 이 처분은 결과적 손해가 완전히 불가능하지 않다는 것을 처음부터 비례성에 반하는 것으로 보지 않는다. 개별적인 경우 비례성 원칙의 준수에는 대상자의 데이터베이스에 대한 공개 접근은 비밀 침입보다 기본적으로 우선한다는 것도 속한다.[29)]

21 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 210.

22 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 211.

23 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 227 ff, 243 ff.(http://www.bverfg.de/e/rs20080227_1bvr037007.html)

24 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 243 – 250.

25 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 212.

26 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 251.

27 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 213.

28 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 238 ff.

29 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 215.

절차적 규정에 대해서도 헌법적 의문이 존재하지 않는다고 한다. 이 조치의 명령은 오로지 법관을 통해서만 가능하고 동시에 명령 근거가 충분하게 뒷받침되어야 한다.[30]. 이 조치가 명령될 수 있는 가능한 3개월의 긴 기간은, 이 경우 개별적 명령을 위해서 최고한계가 문제되고 사실상의 명령의 기간은 비례성 심사에 의해서 개별적으로 정해진다는 기준에서만 물론 헌법상 수용될 수 있다.[31]

하지만 사생활의 핵심영역의 보호에 관한 규정들은 헌법의 요청을 충족하지 못한다고 한다.[32] 정보기술시스템에 대한 비밀 접근은 전형적으로 고도의 비밀성이 있는 데이터도 수집될 위험을 지니고 있고 특별한 핵심영역의 근접성을 보여주기 때문에 사생활의 핵심영역의 보호를 위한 명백한 법률상 보호조치들이 필요하다고 한다. 이와 관련한 요구사항은 주거내 음성 감시에서의 요구사항과 모든 관점에서 일치하지 않고 그 보호를 수집 단계에서 이후의 선별 및 이용의 단계로 밀어낸다.[33] 이것은 정보기술기스템의 접근의 특별한 성격에서 그 근거를 가진다. 핵심영역 침해 이전의 보호처분은, 주로 사생활 장소에서 오로지 휘발적이고 고도의 비밀성이 있는 순간의 포착을 방해하는 것을 목적으로 하는 것이 아니라, 전체적으로 주거내에서의 행위나 통신과 같은 사생활의 성격 그 자체를 전형적으로 보여주지 않는 디지털 정보의 전체 데이터베이스에서 고도의 비밀스런 정보의 열람을 방해하는 것을 목적으로 한다. 이 경우 이 감시는 다양한 장소에서 시간적으로 분리된 일로서 수행되지 않고, 탐색 프로그램을 이용한 접근으로서 수행되므로, 접근 자체와 관련하여 대안이 전혀 존재하지 않는다.[34]

이와 상응하게 수집단계에서의 핵심영역 보호에 관한 요구사항은 한 단계 더 나아갔다. 물론 이 경우에도 가능한 한 핵심영역에 귀속될 수 있는 정보의 수집은 정보기술적이고 수사기술적으로 중단되도록 규정되어야 한다. 특히 이용가능한 정보기술의 보안이 사용되어야 한다. 이의 도움으로 고도로 신뢰할 수 있는 정보가 탐지될 수 있다면, 이에 대한 접근은 거부되어야 한다.[35]

이에 반해서 핵심영역과 관련된 데이터가 데이터 수집 이전에 또는 수집 시에 분리될 수 없다면, 여기서 고도의 개인적인 데이터도 덧붙여 함께 파악될 수 있는 개연성이 존재하는 경우 정보기술시스템에 대한 접근도 허용된다고 한다. 입법자는 그러한 점에서 사용 단계에서 보안을 통해서 당사자의 보호의 필요성을 고려하여야 하고 그러한 접근의 효과를 최소화하여야 한다. 이에 대해 결정적인 의미를 가지는 것은 이 경우 독립된 기관을 통한 열람이고, 이 열람은 핵심영역 관련 정보를 연방범죄수사청이 알고서 이용하기 이전에 걸러준다.[36]

제20k조 제7항은 이러한 요구사항을 일부만 충족한다고 한다.[37] 헌법에 합치하게 해석하는 경우 물론 데이터 수집 단계에서의 규정들은 이의가 제기되지 않을 수 있다고 한다. 제7항 제2문은, 핵심영역과 관련되는 정보의 수집을 피하기 위해서 모든 기술적 가능성이 이용되어야 한다고 언급한 요구사항과 일치하게 규정하고 있다. 게다가 이

30 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 257 ff.
31 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 216.
32 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 217.
33 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 276 ff.
34 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 218.
35 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 219.
36 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 220.
37 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 221.

조항은 정보기술시스템의 접근을 통해서 오로지 사생활의 핵심영역에 관한 정보만 수집되는 경우에는 이러한 접근을 금지하고 있다. 이것은 설명한 기준들에 의해서 헌법적으로 수용가능하다고 한다. 이 경우 이 조항은 물론 헌법 때문에 고도로 신뢰할 수 있는 정보는 일상적인 정보와 혼합되기 때문에 고도의 신뢰에 관한 통신은 따라서 엄격하게 보호될 핵심영역에서 벗어나지 않는다는 것으로 해석되어야 한다.[38] 이 조항은 그러한 점에서 사생활의 핵심영역의 헌법상의 보호요청과 여기서 근거로 삼고 있는 개념 이해와 일치하는 것으로 이해되어 적용될 수 있다.[39]

이에 대해서 문제가 된 처분들에는 이후의 핵심영역보호 단계에서 헌법상 충분한 보호조치가 결여되어 있다고 한다. 제20k조 제7항 제3문과 제4문은 독립적인 통제를 충분하게 규정하고 있지 않다.[40] 헌법상 요구되는 독립된 기관을 통한 열람은 정당성 통제 외에 핵심영역과 관련한 데이터가 조기에 걸러져서 될 수 있는 한 그것이 보안기관에게 알려지지 않도록 하는 것이다. 이 통제는 본질적으로 보안직무를 수행하지 않는 외부의 사람에 의해서 수행된다는 것을 요건으로 한다. 특별한 비밀준수의무 규정을 두어 연방범죄수사청의 수사 전문가의 입회도 불가능하지 않다. 마찬가지로 또한 연방범죄수사청을 통한 기술적 지원에 의지할 수도 있다. 하지만 실제 이행과 결정 책임은 연방범죄수사청에 있어야 한다.[41]

제20k조 제7항은 제3문과 제4문은 이를 보장하지 않는다. 이 규정은 열람을 본질적으로 연방범죄수사청의 직원에게 직접 맡기고 있기 때문이다. 열람은 일반적인 명령 법원의 지휘하에 두어야 하고 열람하는 공무원 중 한명은 관청내의 데이터보호감독관으로서 지시를 받지 않아야 한다.[42]

이에 대해서 제20k조 제7항 제5문 내지 제7문은 사용 단계에서 허용되는 효과적인 핵심영역보호에 관한 추가적 보호조치를 헌법상 수용하게 한다고 한다. 물론 제20k조 제7항 제8문에 의해서 삭제기록의 보관 기간을 지나치게 짧게 한 것은 헌법에 위반된다고 한다.[43]

Ⅳ 연방범죄수사청법의 온라인 수색

1. 연방범죄수사청법의 개정 배경

연방범죄수사청법은 '2017년 6월 1일자 연방범죄수사청법의 새로운 체계화를 위한 법률'[44]에 의해서 전부 개정되어 2018년 5월 25일부터 발효되었다.[45] 이 법률은 앞서 언급한 연방헌법재판소의 BKAG 판결[46]과 '형사절차

38 BVerfG Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 255.
39 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 222.
40 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 223.
41 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 224.
42 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 225.
43 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 226.
44 Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes.
45 Bundesgesetzblatt 2017 Teil I Nr. 33, 08.06.2017 S. 1354.
46 BVerfG Urteil vom 20. April 2016 – 1 BvR 966/09.

에서 개인정보 보호지침'(RL (EU) 2016/680)[47]을 이행하기 위한 것이다. 개정 법률은 데이터보호의 강화, EU내의 경찰기관 사이에 정보교환의 개선, 중앙기관으로서 연방범죄수사청의 현대화를 목적으로 한다.

연방헌법재판소는 BKAG 판결에서 국제테러의 위험방지를 위한 비밀감시처분의 사용에 대한 연방범죄수사청의 권한은 기본적으로 독일 기본법(헌법)과 일치할 수 있다는 것을 확인하였다. 동시에 헌법재판소는 연방범죄수사청법의 일부는 헌법에 위반된다고 판결하였다. 특히 비밀감시처분의 사용에 대한 연방범죄수사청의 권한들은 사생활의 핵심영역의 보호에서 헌법상 요청을 충족하지 못한 것으로 판단하였다.

연방헌법재판소는 또한 개별적인 비밀 수사권한에 대한 지금까지의 판례를 종합하여 경찰의 데이터보호에 대한 기본적인 기준을 제시하였다. 지금까지 포괄적인 원칙들을 체계화하고, 데이터의 목적구속과 목적변경의 헌법상 요구사항을 확인하였으며 처음으로 외국의 공공기관으로 데이터의 이전에 관한 기준을 제시하였다. 연방헌법재판소는 특히 국가기관이 수집한 데이터의 이용과 전달에 있어서 요구사항은 목적구속과 목적변경의 기본원칙에 의해서 행해지고 그러한 목적변경을 위한 비례성 요구사항은 가정적 데이터 수집원칙에 따라야 한다고 상술하였다. 데이터를 외국의 공공기관으로 이전하는 것은 목적구속 및 목적변경의 헌법상의 원칙을 따라야 한다.

기존의 연방범죄수사청의 IT 체계, 특히 경찰의 정보시스템(INPOL)은, 이 판결의 기준을 이행하기 위해서 기본적으로 다시 구성되어야 한다. 따라서 연방범죄수사청의 중앙기관의 기능은 고도의 테러 위협 상황의 배경에서 현대화되어야 하고 발전되어야 한다. 연방 및 주의 경찰을 위해서도 헌법상의 기준을 효과적으로 충족시키기 위해서 연방범죄수사청에 데이터를 보관하는 통일적인 통합시스템이 마련되어야 한다.

정보처리의 조화 및 표준화는 장래에 통일적인 정보기술을 이용하고, 절차를 조정하고 논의과정을 현대화하는 중앙기관을 요구한다. 이를 위해서 연방범죄수사청은 원래의 중앙기관으로서의 위치를 더욱 공고히 하여야 한다. 중앙기관으로서 직무를 수행하기 위해서 연방범죄수사청의 구조와 IT 기술이 현대화되어야 한다. 그리하여 연방범죄수사청법이 체계적인 관점에서 개정될 필요가 있었다.

2. 범죄예방 목적의 온라인 수색

개정된 연방범죄수사청법은 제49조에서 온라인 수색을 다시 규정하고 있다. 제49조 제1항에 따르면 연방범죄수사청은, 사람의 생명, 신체 및 자유에 대한 위험이나 공공의 이익에 대한 위협이 국가(연방 또는 주)의 기반이나 존립 또는 인간의 존재 기반을 위협한다는 가정이 특정한 사실로부터 정당화되는 경우 당사자 모르게 기술적인 수단을 통해서 당사자가 이용하고 있는 정보기술 시스템에 침입하여 거기에 있는 당사자의 데이터를 수집할 수 있다고 규정하고 있다(제1항 제1문). 연방범죄수사청은 또한 예견할 수 있는 시기에 적어도 그 성격에 의해서 구체적인 방

47 범죄의 예방, 탐지, 수사, 소추 및 형의 집행을 위해 관할 기관이 행하는 개인정보의 처리에 있어서 개인의 보호에 관한 유럽 의회 및 이사회의 지침'(ABl. L 119, 04.05.2016, S. 89). EU 개인정보보호법이 개인정보 보호 기본 규칙(General Data Protection Regulation, GDPR) 규칙 (EU) 2016/679)과 지침 (EU) 2016/680에 의해서 기본적으로 개정되었다. 개인정보보호 기본 규칙은 2018년 5월 25일부터 발효되어 EU 회원국에 모두 적용되었다. 개인정보보호 기본 규칙은 EU의 개인정보보호지침(Directive 95/46/EC)을 폐지하고 규칙으로 전환한 것이다. EU는 개인정보보호 기본규칙 외에 형사사법분야에서의 개인정보보호에 관한 지침도 함께 입법하였다. 그것이 지침 (EU) 2016/680이다(이 지침에 대해서는 박희영, EU 형사절차에서 개인정보 보호지침, 독일법제동향, 로앤비(www.lawnb.com), 2018.05, 1-9.

법으로 제1문에 언급된 법익의 침해가 발생한다는 가정을 특정한 사실이 정당화하거나 개인의 개별적인 행위가 예견할 수 있는 시기에 제1문에 언급된 법익을 침해하게 될 것이라는 구체적인 개연성을 뒷받침하는 경우에도 이러한 처분을 할 수 있다고 규정하고 있다(제1항 제2문). 이러한 처분은 직무수행을 위해서 필요하고 다른 방법으로는 가망이 없거나 본질적으로 어려운 경우에만 수행될 수 있다(제1항 제3문). 이것은 비례성의 원칙을 구체적으로 밝힌 것이다.

제2항에 따르면 데이터 수집을 위해서 반드시 필요한 경우에만 정보기술시스템의 변경이 행해지고, 이러한 처분의 종료 시 기술적으로 가능한 한 자동으로 복구되도록 해야 한다(제2항 제1문). 사용된 수단은 현재의 기술 수준에서 무권한 이용으로부터 보호되어야 한다(제2항 제2문). 또한 복제된 데이터는 현재의 기술 수준에 의해서 변경, 무권한 삭제, 무권한 인지로부터 보호되어야 한다(제2항).

제3항은 온라인 수색의 대상을 정하고 있다. 즉 온라인 수색은 행위책임자(연방경찰청법 제17조) 또는 상태책임자(동법 제18조)에 대해서만 취해질 수 있다(제3항 제1문). 하지만 이 처분은 다른 사람이 어쩔 수 없이 관련되는 경우에도 수행될 수 있다(제3항 제2문).

온라인 수색은 연방범죄수사청의 장 또는 그 대리인의 청구에 의해서만 법원에 의해 명령될 수 있다(제4항). 온라인 수색 청구서에는 ① 가능한 한 이름과 주소가 첨부되어 있는 처분의 대상자, ② 가능한 한 데이터 수집을 위해서 접근해야 될 정보기술시스템의 정확한 표시, ③ 처분의 방법, 범위 및 기간, ④ 사실관계, ⑤ 사유가 모두 기재되어야 한다(제5항).

그리고 법원의 온라인 수색 명령서에는 ① 가능한 한 이름과 주소가 첨부되어 있는 처분의 대상자, ② 가능한 한 데이터 수집을 위해서 접근해야 될 정보기술시스템의 정확한 표시, ③ 처분의 방법, 범위 및 기간, ④ 본질적인 사유(제6항 제2문)가 모두 기재되어야 한다. 명령은 3개월의 기한이 정해져 있다(제6항 제3문). 수집한 데이터에서 알아낸 내용을 고려하여 명령의 요건이 존속하는 한, 3개월을 초과하지 않는 한 매번 연장이 가능하다(제6항 제4문). 명령의 요건이 더 이상 존재하지 않는 경우에는 명령을 근거로 하여 취해진 조치는 지체없이 종료되어야 한다(제6항 제5문).

제7항은 사생활의 핵심영역의 보호를 규정하고 있다. 온라인 수색을 통해서 사생활의 핵심영역에 관한 정보만을 알게 된다는 사실상의 근거가 존재하는 경우에 그 처분은 허용되지 않는다. 가능한 한 사생활의 핵심영역과 관련이 있는 데이터는 수집되지 않도록 기술적으로 확보되어야 한다. 온라인 수색으로 수집된 데이터는 명령을 내린 법원에 지체없이 제출되어야 한다. 법원은 이의 사용가능성과 삭제를 지체없이 결정해야 한다. 사생활의 핵심영역과 관련되는 데이터는 사용되어서는 안 되고 지체없이 삭제되어야 한다. 데이터의 수집 및 삭제 사실은 기록되어야 한다. 이 기록은 오로지 데이터보호의 통제 목적으로만 사용될 수 있다. 이 기록은 처분 대상자에 대한 통지[48] 후 6개월 또는 유효한 통지의 포기에 관한 법원의 동의를 받은 후 6개월 후 삭제되어야 한다. 제69조 제1항은 이 법률에 따른 데이터 처리에 대하여 데이터보호감독관의 통제를 받을 수 있다고 규정하고 있다. 따라서 데이터보호감독관의

48 BKAG 제74조 제1항 제6호에 따르면 온라인 수색의 처분을 대상자나 함께 관련된 자에게 통지를 해야 한다. 물론 통지의 예외가 규정되어 있다(제1항 제2문 이하).

데이터보호통제가 아직 종료되지 않은 경우에는 그 종결 시까지 이 기록을 보관해야 한다.

임박한 경우에는 연방범죄수사청장 또는 그 대리인은 연방범죄수사청의 데이터보호감독관의 협조로 확보한 정보의 사용을 결정할 수 있다. 수집한 데이터의 열람 시 연방범죄수사청장 또는 그 대리인은 연방범죄수사청의 2명의 공무원의 기술적 지원을 이용할 수 있고, 이 중 한 명은 법관의 자격을 가지고 있어야 한다. 연방범죄수사청의 공무원은 이를 통해서 알게 된 사용되지 않은 정보에 대해서 발설해서는 안 된다. 이 경우 제7항에 의한 법원의 결정을 지체없이 받아야 한다(제8항).

V 형사소송법의 온라인 수색

1. 형사소송법 개정 배경

독일 형사소송법은 '2017년 8월 17일 효율적이고 실무에 적합한 형사절차의 구성에 관한 법률'[49]에 의하여 개정되어 2017년 8월 24일부터 발효되었다.[50] 개정 법률의 핵심 내용은 형사소송법에 암호통신감청과 비밀 온라인 수색을 도입하는 것이었다. 원래 정부안에는 이에 관한 내용이 없었으나 의회 입법과정에서 긴급하게 도입되었다.

타인의 정보기술시스템의 이용을 감시하고 저장된 내용을 기록할 목적으로 국가가 타인의 정보기술시스템에 비밀리에 접근한다는 의미를 가지는 온라인 수색은 현재까지 형사소추의 목적으로 허용되지 않았다.[51] 타인의 정보기술시스템에 저장되어 있는 데이터는 형사소송법 제94조 이하(압수), 제102조 이하(수색) 그리고 통신의 내용과 관련이 있는 경우에는 비밀 통신감청(제100a조)에 의해서 가능하다. 온라인 수색으로 관계되는 침해는 다양한 관점에서 상당히 중요하다. 정보기술시스템의 공개 수색 및 압수와 달리 이 접근은 비밀이고 일회적이고 특정 시점에 행해지는 것이 아니라 장기간에 걸쳐서 행해진다. 또한 새로 도착하는 통신의 내용뿐 아니라 정보기술시스템에 저장되어 있는 모든 내용 그리고 이용자의 시스템 이용 행태가 감시된다는 점에서 비밀 통신감청과도 구별된다.

온라인 수색은 기본법 제1조 제1항과 관련하여 제2조 제1항의 일반적 인격권에서 도출되는 정보자기결정권의 독자적인 발현으로서 당사자의 IT기본권을 제한한다. 정보자기결정권은 인격권의 위험화를 완전히 고려하지 못한다. 인격의 위험화는 개인이 자신의 인격 발현을 위해서 정보기술시스템에 의존하고 있고 이 경우 이 시스템에 개인 데이터를 맡기거나 반드시 이의 이용을 통해서만 (데이터가) 전달된다는 점에서 발생한다. 이 시스템에 접근하는 제3자는 추가적인 데이터 수집이나 데이터 처리에 의존하지 않고도 엄청난 양의 잠재적인 비밀 데이터를 확보할 수 있다. 그러한 접근은 당사자의 인격의 중요성에서 보면 정보자기결정권이 보호하는 개별적 데이터의 수집을 넘어선다.[52]

---

49 Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens Vom 17. August 2017(Bundesgesetzblatt 2017 Teil I Nr. 58, 23.08.2017 S. 3202.).

50 입법이유에 대한 자세한 내용은 박희영, 효율적이고 실무에 적합한 형사절차의 구성에 관한 법률(2017.8.17) : 암호통신감청과 온라인 수색 등, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.12, 1-16 참조.

51 연방대법원 형사소송법상 온라인 수색은 허용될 수 없다고 결정하였다(BGH, Beschluß vom 31. 1. 2007 - StB 18/06).

52 BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 - Rn. 200.

IT 기본권의 제한은 기본적으로 정당화될 수 있다. 하지만 엄격한 요건이 필요하다. 가령 위험예방법에서 온라인 수색은 오로지 현저히 중대한 법익에 대한 구체적인 위험의 사실상의 근거가 존재하는 경우에만 수행되도록 하고 있다. 따라서 기본권 침해의 강도는 이러한 점을 고려해야 한다. 형사소추의 영역에서도 범죄의 중대성과 의미가 적정하게 고려되어야 한다. 그러한 점에서 온라인 수색의 침해의 강도는 주거내 음성 감시의 그것과 비교할 수 있다고 한 연방헌법재판소의 판결이 중요하다.[53] 따라서 온라인 수색에 관한 형사소송법 제100b조는 이 처분의 명령 요건, 절차법상의 요건, 사생활의 핵심영역의 보호, 이 처분으로 확보한 정보의 사용 및 삭제의 관점에서 기본적으로 주거내 음성 감시에 관한 규정(제100c조)[54] 근거하고 있고, 특히 이 규정은 이미 연방헌법재판소에 의해서 합헌으로 심사되었다.[55]

2. 범죄수사 목적의 온라인 수색

범죄수사목적의 온라인 수색은 형사소송법 제100b조(온라인 수색의 실체적 요건), 제100d조(사생활의 핵심영역의 보호와 증언거부권자), 제100e조(온라인 수색의 절차적 요건), 제101조(비밀처분의 절차), 제101b조(통계작성 및 보고의무)에 각각 규정되어 있다.[56]

가. 실체적 요건

형소법 제100b조는 온라인 수색의 실체적 요건을 규정하고 있다. 제1항에서 온라인 수색이란 당사자의 인식과 상관없이 기술적 수단을 이용하여 당사자가 이용하는 정보기술시스템에 침입하여 데이터를 '수집'하는 것으로 정의하고 있다. 온라인 수색은 데이터의 '수집'을 넘어서 이용자의 시스템 이용을 '감시'할 수도 있지만 규범적으로 '수집'으로 제한하고 있다. 온라인 수색을 하기 위해서는 다음 세 가지 요건을 모두 갖추어야 한다. 첫째, 특정한 사실이, 누군가가 정범 또는 공범으로 제2항에 기술한 특별히 중한 범죄를 범했거나 가벌적 미수 사례에서 미수를 범하였다는 혐의를 뒷받침해야 하며, 둘째, 범죄행위가 개별적으로도 특별히 중한 비중을 가져야 하며, 셋째, 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 본질적으로 어려울 수 있거나 가망이 없어야 한다.

---

53 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 210.

54 형사소송법 제100c조의 주거내 음성 감시는 주거내에서 행해지는 비공개 대화를 기술적 수단을 통하여 엿듣거나 녹음하는 강제처분이다. 주거의 불가침에 관한 기본법 제13조는 주거의 음성 감시(akustische Überwachung von Wohnungen)를 명문으로 규정하고 있어서 감시대상은 음성만 포함되고 영상은 포함되지 않는다. 독일 기본법 제13조에서 주거의 음성 감시를 단순히 '주거 감시'로 번역하는 국내의 일부 문헌은 문제가 있다. 주거외에서의 음성감시는 형사소송법 제100f조에서 규정하고 있다. 형사소송법 제100c조는 우리 통신비밀보호법 제14조의 타인의 비공개 대화의 침해 금지에 대응한다. 하지만 통비법 제14조는 주거내와 주거외를 구분하고 있지 않다. 이에 대해서 연방범죄수사청법 제46조에 따르면 주거내외에서의 비공개 대화를 엿듣거나 녹음할 수 있고 대상자의 사진이나 영상도 촬영할 수 있다.

55 BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR 543/06 – Rn. 64 ff.

56 범죄수사 목적의 온라인 수색의 도입 배경, 실체적 요건 및 조문의 소개로는 김성룡, 독일 형사소송법 최근 개정의 형사정책적 시사 - 수사절차를 중심으로 –, 형사정책 제29권 제3호, 2017.12, 256-261; 허 황, 최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구, 형사법의 신동향 통권 제58호, 대검찰청, 2018.3, 98-122; 민영성·김수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 중앙대학교 법학연구소 법학논총 제31권 제2호, 372-381.

전기통신감청은 기본적으로 '중한 범죄'의 경우에 허용됨에 반하여, 온라인 수색은 주거내 음성 감시와 마찬가지로 오로지 '특별히 중한 범죄'[57]의 혐의가 있는 경우에만 명령될 수 있다. 따라서 온라인 수색이 내려질 수 있는 범죄의 목록(종류)은 지금까지 주거내 음성 감시가 명령될 수 있는 범죄의 목록과 완전히 일치한다.

범죄행위가 개별적으로 특별히 중대한 비중을 가져야 한다는 것은 비례성 원칙의 표현이다. 즉 온라인 수색은 범죄가 일반적 경우는 물론 구체적인 경우에도 특별히 중대한 비중이 있는 경우에 비로소 허용된다. 또한 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 본질적으로 어렵거나 가망이 없어야 한다는 점은 보충성을 의미한다. 즉 다른 수사처분이 부정되는 경우에만 이 조치가 적용될 수 있다. 따라서 온라인 수색의 수행 이전에 특히 공개 수색 및 압수도 고려될 수 없는지를 심사되어야 한다.

온라인 수색은 기본적으로 피의자에 대해서만 가능하다. 피의자가 자신의 정보기술시스템을 스스로 이용하는

57 '특별히 중한 범죄'의 표지는 기본법 제13조의 주거의 불가침에서 사용하고 있다. 형사소송법 제100b조 제2항에서 특별히 중한 범죄가 열거되어 있다. 제100b조 (2) 제1항 1호에서 말하는 특별히 중한 범죄는 다음과 같다.

1. 형법
   a) 제80조, 제81조, 제82조, 제89a조, 제89c조 제1항 내지 제4항, 제94조, 제95조 제3항과 제96조 제1항, 제94조, 제95조 제3항과 제96조 제1항(각 경우 마다 형법 제97b조와 관련하여), 죄제97a조, 제98조 제1항 제2문, 제99조 제2항과 제100조, 제100조a 제4항, 에 따른 내란죄, 반역죄와 민주적 법치국가를 위해하는 죄 및 형법에 따른 내란죄와 국가의 안전을 위해하는 죄.
   b) 제129조 제5항 제3문과 관련하여 제1항에 따른 범죄단체 조직, 제129조a 제1항, 제2항, 제3항, 제4항, 제5항 제1문 1유형에 따른 테러단체 조직의 죄(각 경우마다 제129b조 제1항과 결부시켜 판단한다)
   c) 제146조와 제151조(각 경우마다 제152조와 결부시켜 판단한다) 및 제152조a 제3항과 제152조b 제1항 내지 제4항에 따른 화폐위조 및 유가증권 위조의 죄
   d) 제176조a 제2항 2호 또는 제3항, 제177조 제6항 제2문 2호에 언급된 요건 하에서 제179조의 사례들에서 성적 자기결정권에 반하는 범죄.
   e) 제184조b 제2항의 사례에서 아동음란물의 유포, 취득 및 소지의 죄
   f) 제211조, 제212조에 따른 모살과 고살
   g) 제234조, 제234조a 제1항, 제2항, 제239조a, 제239조b에 따른 인격적 자유에 반하는 죄 및 제232조 제3항에 따른 인신매매, 제232a조 제3항, 제4항 또는 제5항 두 번째 문단, 제232a조 제4항 또는 제5항 두 번째 문단과 관련하여 제232b조 제3항 또는 제4항에 따른 강제매춘 및 강제노동, 제233a조 제3항 또는 제4항 두 번째 문단에 따른 자유박탈을 이용한 착취.
   h) 제244조 제1항 2호에 따른 범죄단체 절도죄와 제244조a에 따른 범죄단체 절도죄
   i) 제250조 제1항 또는 제2항, 제251조에 따른 중한 강도 또는 강도치사의 죄
   j) 제255조에 따른 강도에 준하는 협박의 죄와 제253조 제4항 제2문의 요건을 충족하는, 제253조에 따른 특별히 중한 사례의 공갈죄.
   k) 제260조, 제260조a에 따른 영업적 장물죄, 범죄단체를 결성하여 행한 장물죄 및 범죄단체를 결성하여 영업적으로 행한 장물죄
   l) 제261조 제4항 제2문에서 언급하고 있는 요건을 충족하는, 제261조에 따른 특별히 중한 돈세탁, 불법영득재산 은닉의 죄, 제261조 제9항 2문에 의한 불가벌성은 제261조 제9항 3문에 의해서 불가능하지만, 그 대상이 제1호 내지 제7호에 언급된 특별히 중한 범죄 중 하나에서 기인하는 경우에만 가능하다.
   m) 제335조 제2항 1호 내지 3호에 언급한 요건을 충족하는, 제335조 제1항에 따른 특별히 중한 증뢰죄와 수뢰죄
2. 망명절차법
   a) 제84조 제3항에 따른 망명신청남용을 목적으로 하는 호도행위
   b) 제84조a 제1항에 따른 망명신청남용을 목적으로 하는 영업적 및 범죄단체구성을 통한 호도행위
3. 외국인체류법
   a) 제96조 제2항에 따른 외국인의 불법유입
   b) 제97조에 따른 인명의 손실을 야기한 불법유입과 영업적 및 범죄단체 구성을 통한 불법유입
4. 마약류법
   a) 제29조 제3항 제2문 1호에서 언급하고 있는 요건을 충족한, 제29조 제1항 제1문 1호, 5호, 6호, 10호, 11호 또는 13호, 제3항의 범죄가 특별히 중한 경우
   b) 제29조a, 제30조 제1항 1호, 2호, 4호 및 제30조a에 따른 범죄
5. 전쟁무기통제에 관한 법률
   a) 제21조와 결부하여 제19조 제2항 또는 제20조 제1항에 따른 범죄
   b) 제22조a 제2항과 결부된 제2항에 따른 범죄의 특별히 중한 경우
6. 국제형법
   a) 제6조에 따른 인종학살
   b) 제7조에 따른 인간성에 반하는 죄
   c) 제8조 내지 제12조에 따른 전쟁범죄
7. 무기법
   a) 제51조 제2항과 결부된 제1항에 따른 범죄의 특별히 중한 경우
   b) 제52조 제5항과 결부된 제1항 1호에 따른 범죄의 특별히 중한 경우

것을 특정한 사실을 근거로 인정할 수 있는 경우에만 다른 사람이 포함될 수 있다. 하지만 이 경우에도 다른 사람의 정보기술시스템에 대한 접근은 피의자 스스로 이의 접근이 오로지 공동피의자의 소재지 수사나 사실관계의 조사를 위해서 충분하지 않는 경우에만 허용된다(제3항).[58]

온라인 수색에는 전기통신감청의 경우에 적용되는 기술적인 확보와 프로토콜 규정이 적용된다(제4항)[59]. 따라서 데이터 수집을 위해 필요한 경우에만 정보기술시스템을 변경할 수 있고, 변경된 것은 조치의 종료 시 기술적으로 가능한 한 자동적으로 복구되어야 한다. 또한 사용된 수단은 현재의 기술 수준에 의해서 무권한 이용으로부터 보호되어야 한다. 수집된 데이터는 현재의 기술 수준에 의해서 변경, 무권한 삭제 및 무권한 인식으로부터 보호되어야 한다. 나아가서 기술적 수단이 사용되는 경우 ① 기술적 수단의 표지 및 투입 시점, ② 정보기술시스템을 확인하기 위한 정보 및 여기서 단지 임시적으로 행해지지 않은 변경, ③ 수집된 데이터의 확인을 가능하게 하는 정보가 기록되어야 한다.

나. 사생활의 핵심영역의 보호 및 증언거부권자

연방헌법재판소는 BKAG 판결에서 개인의 사생활의 핵심영역을 위해서 일반적으로 관련이 있는 침해의 강도가 심한 조치의 경우 수집의 차원에서는 물론 사용의 차원에서도 사생활의 핵심영역을 보호하기 위하여 충분한 보호조치를 취해야 한다고 판결하였다.[60] 이러한 헌법재판소의 견해는 형사소송법 제100d조에 반영되었다. 제100d조는 지금까지 형사소송법의 개별적인 수권근거에서 나누어져 있던 사생활의 핵심영역의 보호와 증언거부권에 관한 조항들을 통합하여 규정하고 있다. 침해의 비중에 따라서 체계화하여 온라인 수색에도 적용하고 있다.

제100d조 제1항[61]은 사생활의 핵심영역에 관한 정보만이 확보된다고 인정할 사실상의 근거가 존재하는 경우에는 제100a조 내지 제100c조[62]에 따른 전체 처분들은 수집의 단계에서 일반적으로 허용되지 않는다는 원칙을 정하고 있다.[63] 오로지 핵심영역 관련성은 특히 당사자가 개인과 접촉하는 경우, 핵심영역과 관련되는 특별한 신뢰관계64)가 존재하는 경우에만 인정될 수 있다.[65] 이러한 신뢰관계가 수사기관에게 알려질 수 있는 한, 이 조치는 수행되어서는 안 된다. 이와 반대로 제1항의 원칙은, 인격권의 핵심영역을 침해하는 사실도 파악될 수 있기 때문에 제

58 제100b조 (3) 이 조치는 피의자에 대해서만 행해질 수 있다. 다른 사람의 정보기술시스템의 침해는, 특정한 사실을 근거로 다음 각 호의 모두가 인정될 수 있는 경우에만 허용될 수 있다. 1. 제100e조 제3항에 따른 명령에서 표시된 피의자가 다른 사람의 정보기술시스템을 이용하는 경우. 2. 피의자의 정보기술시스템의 침입만으로는 사실관계의 조사나 공동피의자의 소재지의 수사가 되지 않는 경우. 이러한 조치는 다른 사람이 부득이하게 관련되는 경우에도 수행될 수 있다.

59 제100b조 (4) 제100a조 제5항과 제6항은 제5항 제1문 제1호를 제외하고 준용한다.

60 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 257; Beschluss vom 12. Oktober 2011 – 2 BvR 236/08, Rn. 209).

61 제100d조 (1) 제100a조 내지 제100c조에 의한 조치를 통해서 사생활의 핵심영역에 관한 정보만 확보된다고 인정할 사실상의 근거가 존재하는 경우 이 조치는 허용되지 않는다.

62 형사소송법 제100a조(전기통신감청), 제100b조(온라인 수색), 제100c조(주거내 음성 감시).

63 BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08, Rn. 209; Urteil vom 20. April 2016 – 1 BvR 966/09, Rn. 119 ff., 125.

64 예를 들어 긴밀한 가족구성원, 성직자, 전화심리상담원, 형사변호인 또는 개별적인 경우 의사도 포함된다.

65 BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08, Rn. 215; 박희영, 현행 전기통신감청법은 합헌, Gesetz zur Neuregelung der TK-Überwachung ist verfassungsmäß, BVerfG, Beschluss vom 12.10.2011 - 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, 최신독일판례연구, 로앤비(www.lawnb.com), 2012. 1, 1-6.

100a조 내지 제100c조의 조치가 처음부터 금지되어야 한다는 것을 의미하지는 않는다.[66] 사생활의 핵심영역의 보호는 이러한 사례들에서 수집 및 사용 단계에서 보충적인 예방조치를 통해서 확보되어야 한다.

제100d조 제2항[67]은 연방헌법재판소의 기준에 맞게 사용단계에서 보호조치를 규정하고 있다. 제100a조 내지 제100c조에 따른 전체 조치들에 적용되는 사용규정들에 의하면 사생활의 핵심영역에 관한 정보는 사용될 수 없다. 이 규정은 그러한 정보의 지체 없는 삭제 원칙과 포괄적인 기록의무 및 삭제의무를 포함한다. 지금까지 이것은 전기통신감청과 주거내 음성감시에 적용되었다. 이제는 하나의 규정으로 통합되었고 온라인 수색에도 적용된다. 상응한 정보의 획득 및 삭제에 관한 기록(삭제프로토콜)은 법원에 의한 형사절차의 종결 시까지 이 조치의 정당성의 통제를 가능하도록 문서로 기록되어야 한다. 그러한 점에서 제101조 제8항의 삭제 및 기록규정이 적용된다.

제100d조 제3항[68]은 주거감시와 관련하여 핵심영역의 보호 규정에 근거하고 있고, 온라인 수색의 특수성을 고려하여 수집 및 사용단계에서 보충적인 보호를 규정하고 있다.[69] 온라인 수색과 관련하여 인식내용의 수집의 경우, 가능한 한, 기술적으로 사생활의 핵심영역과 관련되는 데이터는 수집되어서는 안 된다는 점이 확보되어야 한다. 제100b조에 의한 조치를 통해서 확보되고 사생활의 핵심영역과 관련되는 정보는 지체 없이 삭제되거나 검사가 명령을 내린 독립기관인 법원[70]에 데이터의 사용 및 삭제에 관한 결정을 청구해야 한다. 사용가능성에 관한 법원의 결정은 다른 절차에도 구속력이 있다.

제5항[71]은 지금까지 제100c조 제6항에서 포함된 증언거부권자의 보호에 관한 규정을 포함하고 있다(특히 업무상비밀준수자). 이것은 온라인 수색 조치에도 적용된다.

다. 절차적 요건

제100e조 제2항[72]은 법원의 명령절차를 규정하고 있다. 기존의 수사판사[73] 대신에 법원조직법 제74a조 제4항에 언급된 검찰청 소재지를 관할하는 지방법원의 합의부가 명령을 내린다. 이 합의부는 이 조치의 명령과 지속 여

66 vgl. BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08, Rn. 216.

67 제100d조 (2) 제100a조 내지 제100c조에 의한 조치를 통하여 사생활의 핵심영역으로부터 확보한 인식내용은 사용될 수 없다. 그러한 인식에 관한 기록은 지체 없이 삭제되어야 한다. 이의 확보 및 삭제 사실은 문서로 명시되어야 한다.

68 제100d조 (3) 제100b조에 의한 조치의 경우, 가능한 한, 사생활의 핵심영역과 관련되는 데이터는, 수집되지 않도록 기술적으로 확보되어야 한다. 제100b조에 의한 조치를 통하여 확보되고 사생활의 핵심 영역과 관련되는 인식 내용은 지체 없이 삭제되거나 검찰에 의하여 명령 법원에게 데이터의 사용여부 및 삭제에 관한 재판이 요청되어야 한다. 사용가능성에 관한 재판은 다른 절차를 위한 사용하는 경우에는 의무적이다.

69 BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 217 ff., 223 ff.

70 BVerfG Beschluss vom 11. Mai 2007 – 2 BvR 543/06 – Rn. 23, 64 ff.

71 제100d조 (5) 제53조의 사례들에서 제100b조와 제100c조에 의한 조치들은 허용되지 않는다; 조치의 수행 동안 또는 수행 이후 제53조의 사례가 존재한다는 것이 발생한 경우 제2항이 준용된다. 제52조와 제53a조의 사례들에서 제100b조와 제100c조에 의한 조치들로부터 확보된 인식 내용은 이것이 근거가 되는 신뢰관계의 의미를 고려하여 사실관계의 조사나 피의자의 소재지 파악의 이익과 비례관계에 있지 않는 경우에만 사용될 수 있다. 제160a조 제4항은 준용한다.

72 제100e조 (2) 제100b조와 제100c조의 조치는 검사의 요청에 의해서만 법원조직법 제74a조 제4항에 언급한 검찰청 소재지를 관할하는 지방법원의 합의부(LG Kammer)를 통해서 명령될 수 있다. 긴급한 경우 재판장을 통해서도 명령이 내려질 수 있다. 그 명령은 형사재판부로부터 3일 이내에 승인을 받지 못하면 효력이 없다. 명령은 최고 1월로 정해져 있다. 확보한 수사결과를 고려하여 요건이 존재하는 경우 한 번에 1개월 미만으로 연장이 허용된다. 명령 기간이 전체 6개월로 연장되는 경우 그 연장에 대하여 고등법원이 재판한다.

73 우리 형사소송법의 영장담당판사에 대응하는 개념.

부에 관하여 통제한다. 긴급한 경우 재판장이 명령을 내질 수 있지만[74] 3일 이내에 합의부의 승인을 받아야 한다. 이 명령은 최고 3개월을 넘지 못한다. 따라서 기간의 측면에서도 주거내 음성 감시와 동일하다. 이 경우 온라인 수색의 수행은 마련될 기술적 요건의 배경에서 일반적으로 주거내 음성감시의 수행보다 시간이 더 소요된다는 것은 부인되지 않는다. 3개월을 넘지 않는 범위에서 매 연장은 지금까지 적용된 규정에 의해서도 허용된다. 물론 확보된 수사결과를 고려하여 요건이 계속 존재해야 한다. 명령의 기간이 전체 6개월이 초과되는 경우 추가 연장에 대해서는 고등법원이 결정한다.

제3항은 명령결정서에 포함되어야 할 내용을 규정하고 있으며 전기통신감청, 온라인 수색, 주거내 음성 감시에 모두 적용된다.[75]

제4항은 전기통신감청, 온라인 수색, 주거내 음성 감시의 명령 및 이의 연장 요건과 이익형량을 명시하고 있다.[76]

제5항[77]은 처분의 종료 및 과정 통제에 관한 규정이 통합되어 있다. 이 조항은 온라인 수색에 적용된다.

제6항은 전기통신감청, 온라인 수색, 주거내 음성 감시로 확보되어 이용될 수 있는 개인정보를 다른 목적으로 사용할 수 있는 기준을 정하고 있다. 그러한 기준은 다음 세 가지이다. 첫째, 온라인 수색(제100b조) 또는 주거내 음성 감시(제100c조)에 따른 처분이 명령될 수 있었던 범죄의 규명을 위해서 또는 그러한 범죄의 피의자의 소재지를 수사하기 위해서만 감시대상자의 동의 없이 다른 형사절차에서 개인정보가 사용될 수 있다. 둘째, 위험예방의 목적으로 데이터의 사용과 처분의 수행 동안 또는 수행 이후 직무상비밀준수자의 증언거부권이 존재하는 경우의 데이터의 사용은, 개별적인 사례에서 존재하는 개인의 생명의 위험 또는 신체 및 자유에 대한 긴박한 위험의 방지를 위해서, 국가의 안전 또는 존립을 위해서 혹은 국민의 배려에 기여하는 의미 있는 가치의 대상을 위하여, 문화적으로 우수한 가치 있는 대상을 위하여 혹은 형법 제305조(건축물의 파괴)에 언급되어 있는 대상을 위하여만 허용된다. 데이터는 개별적인 경우 존재하는 기타 의미 있는 재산적 가치에 대한 임박한 위험을 방지하기 위해서도 사용될 수 있다. 데이터가 위험방지를 위해서 또는 위험방지를 위해 취해진 조치의 재판외(vorgerichtliche) 혹은 법원의 심사

74 전기통신감청과 달리 긴급한 경우 검사의 명령은 인정되지 않는다.

75 제100e조 (3) 명령은 서면으로 행한다. 재판서에는 다음 각 호가 기재되어야 한다.
1. 가능한 한 이 조치를 받게 될 대상자의 성명과 주소,
2. 조치가 명해지는 근거로서 비난 받는 행위(Tatvorwurf)
3. 조치의 종류, 범위, 기간 및 종료 시점.
4. 조치를 통해 수집될 정보의 종류 및 절차를 위한 이의 의미.
5. 제100a조에 의한 조치의 경우 감시될 회선 및 단말기의 전화번호 혹은 그 밖의 표지. 이것이 동시에 다른 단말기에 귀속되어 있다는 것이 특정한 사실로부터 나오지 않아야 한다; 제100a조 제1항 2문과 3문의 경우 가능한 침입될 정보기술시스템의 정확한 표지.
6. 제100b조의 조치의 경우 데이터가 수집될 가능한 정보기술시스템의 정확한 표지.
7. 제100c조의 조치의 경우 감시될 주거 혹은 감시될 공간.

76 제100e조 (4) 제100a조 내지 제100c조의 조치의 명령 혹은 연장의 근거에는 이의 요건 및 본질적인 이익형량의 관점이 명시되어야 한다. 특히 개별적인 사례와 관련하여 다음 각 호가 기재되어야 한다.
1. 혐의를 뒷받침하는 특정한 사실.
2. 조치의 필요성과 비례성을 위한 본질적인 이익형량.
3. 제100c조의 조치의 경우 제100d조 제4항 제1문의 사실상의 근거.

77 제100e조 (5) 명령의 요건이 더 이상 존재하지 않는 경우, 명령을 근거로 취해진 조치는 지체 없이 종료되어야 한다. 제100b조 및 제100c조에 의한 조치의 경우 명령 법원은 과정도 알려야 한다. 명령의 요건이 더 이상 존재하지 않는 한, 검사가 그 중단을 하지 않는 경우 법원은 조치의 중단을 명령해야 한다. 제100b조와 제100c조에 따른 조치의 중단 명령은 재판장을 통해서도 행해질 수 있다.

가 더 이상 필요하지 않는 한, 위험방지기관의 이 데이터에 관한 기록들은 지체 없이 삭제되어야 한다. 삭제는 문서로 기록되어야 한다. 삭제가 오로지 재판외 혹은 법원의 심사를 위해 유예되어 있는 한, 데이터는 이러한 목적을 위해서만 사용될 수 있다. 다른 목적으로 사용하는 것은 차단되어야 한다. 셋째, 사용될 개인정보가 이와 상응하는 경찰법상의 조치(즉 위험방지를 위한 온라인 수색 또는 주거내 음성감시)를 통하여 확보된 경우에는, 온라인 수색(제100b조) 또는 주거내 음성감시(제100c조)에 따른 조치가 명령될 수 있었던 범죄를 규명하기 위해서 또는 그러한 범죄의 피의자의 소재지를 수사하기 위해서만 감시대상자의 동의 없이 다른 형사절차에서 데이터가 사용될 수 있다.

라. 비밀처분의 일반적 절차 규정들(제101조)

형사소송법의 비밀 처분에 관한 일반적인 절차 규정들은 제101조에 규정되어 있다. 이 절차규정은 온라인 수색에도 적용된다. 특히 제2항에서 서류를 위한 보관의무가 제100b조의 조치로 확대되고 온라인 수색에서 피의자에 대한 통지의무와 현저히 침해를 받게 되는 자에게 확대되었다.

온라인 수색 처분에 관한 결정 및 그 밖의 서류들은 검찰에 보관한다. 제5항의 통지를 위한 요건들이 충족되면 비로소 소송기록에 첨부한다(제2항). 온라인 수색으로 수집된 개인정보는 상응하게 표시되어야 하고, 다른 기관으로 전달 후에도 이 기관에 의해서 그 표시는 유지되어야 한다(제3항).

온라인 수색에서 통지를 해야 하는 자는 수색 대상자 및 현저히 침해를 받게되는 자이다(제4항). 당해 통지를 할 때에는 제7항에 따른 사후적인 권리보호의 가능성 및 그 기한을 지적하여야 한다. 통지가 당사자의 중대한 이익의 보호에 반하는 경우에는 통지를 하지 않는다. 제1문에 기재한 자의 신원을 확인하기 위한 사후조사는 해당자에 대한 처분의 침해 정도, 신원확인에 소요되는 비용 및 그로 인해 당사자 및 타인에게 유발되는 침해를 고려하여 필요한 때에만 수행한다(제4항).

제5항에 따르면 통지가 수사목적, 사람의 생명, 신체의 불가침, 개인적 자유 및 중대한 재산적 가치, 제110a조의 경우 비밀수사요원의 계속적인 이용가능성을 위협하지 않는 즉시, 당해 통지를 행한다. 이에 따른 통지가 유예된 때에는 그 사유를 문서로 기록한다.

제6항에 따르면 제5항의 유예된 통지가 처분이 종료된 이후 12개월 이내에 이루어지지 않은 경우 이를 계속 유예하고자 할 때에는 법원의 동의가 필요하다. 법원은 계속 유예의 기간을 정한다. 법원은 통지의 요건이 장래에도 성립하지 않으리라고 확실시 되는 경우에는 통지의 완전한 배제에 동의할 수 있다. 다수의 처분이 근접한 시간적 거리를 두고 수행된 때에는 제1문에 언급한 기간은 마지막 처분의 종료와 함께 개시한다. 제100b조와 제100c조의 경우 6개월을 기간으로 한다.

제7항에 의하면 제6조에 따른 법원의 결정은 처분의 명령을 관할하는 법원이, 그 이외의 경우에는 관할 검찰이 소재하는 법원이 내린다. 제4항 제1문에 언급한 자는 통지를 받은 후 2주 내에 제1문에 따른 관할법원에 처분 및 그 집행방식의 적법성에 대한 심사를 신청할 수 있다. 법원의 결정에 대해서는 즉시항고가 허용된다. 공소가 제기되었고 피고인이 통지를 받은 때에는 사건을 담당하는 법원이 절차를 종결하는 재판에서 당해 신청에 대해 결정한다.

제8항에 따르면 처분을 통해 획득된 개인 정보가 형사소추 및 처분에 대한 법원의 심사를 위해 더 이상 필요하지 않게 된 때에는 이를 즉시 삭제해야 한다. 삭제 사실은 문서로 기록한다. 삭제가 오로지 처분에 대한 법원의 심사로 인해 유예된 경우에 당해 데이터는 오로지 이 목적을 위해서만 당사자의 동의 없이 사용할 수 있다. 데이터는 이에 상응하여 접근이 차단되어야 한다.

마. 통계작성의무 및 보고의무

전기통신감청, 온라인 수색, 주거내 음성 감시, 통신사실확인자료에 따른 통계작성의무 및 보고의무는 제101b조에서 통합되어 규정되었다. 이 규정에 따라 각 주 및 연방검찰청은 보고연도의 다음 해에 매년 6월 30일까지 관할 영역에서 명령된 온라인 수색에 의한 조치를 연방사법부에 보고해야 한다. 연방사법부는 보고 연도에 연방차원에서 명령된 조치에 관한 개관을 작성하여 인터넷에 공개한다(제1항). 온라인 수색에 의한 조치의 개관에는 ① 온라인 수색이 명령된 절차의 수, ② 온라인 수색에 의한 감시명령의 수(이 경우 첫 명령과 연장 명령을 구분한다), ③ 온라인 수색 명령의 근거가 된 원인범죄, ④ 당사자가 이용한 정보기술시스템의 침입이 실제로 수행된 절차의 수가 기재되어야 한다(제3항).

Ⅵ 시사점

독일에서 온라인 수색이 등장하기 이전까지 위험방지나 범죄예방 그리고 범죄수사에서 기본권 침해의 정도가 가장 높은 비밀강제처분은 주거내 음성 감시였다. 주거는 개인의 사적이고 은밀한 사생활이 보장되는 공간으로 인간의 존엄성을 보장하는 최후 안식처이다. 주거내 음성감시는 이러한 주거에서 발생하는 사생활의 핵심영역에 관한 대화를 비밀리에 엿듣고 녹음하는 것이다. 그동안 정보통신기술의 발전으로 등장한 새로운 강제처분인 온라인 수색은 기본권 침해의 정도에서 실제로 주거내 음성 감시를 넘어선다. 하지만 독일연방헌법재판소와 입법자는 주거내 음성 감시와 온라인 수색을 규범적으로 동일하게 보고 있다. 우리는 현재 온라인 수색에 관한 규정은 존재하지 않고 이에 대한 법적 논의도 공론의 장에서 이루어지고 있지 않다. 테러범죄와 같은 중한 범죄에 대처하기 위해서는 이러한 비밀처분이 필요한 것으로 보인다. 특히 구체적인 범죄로 이행되기 이전에 위험예방이나 범죄예방 영역에서 온라인 수색은 더욱 필요한 것으로 보인다. 하지만 온라인 수색은 기본권 침해의 정도가 상당하기 때문에 입법 이전에 국민들의 합의가 우선되어야 한다. 향후 입법을 하게 된다면 독일의 법적 상황은 우리에게 중요한 입법자료가 될 것으로 생각된다.

참고문헌

김성룡, 독일 형사소송법 최근 개정의 형사정책적 시사 - 수사절차를 중심으로 -, 형사정책 제29권 제3호, 2017.12, 256-261.

민영성·김수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 중앙대학교 법학연구소 법학논총 제31권 제2호, 372-381.

박희영, EU 형사절차에서 개인정보 보호지침, 독일법제동향, 로앤비(www.lawnb.com), 2018.05, 1-9.

박희영, 독일 연방사법경찰청에 의한 국제테러의 위험 방지를 위한 법률(상), 법제처, 법제 제613호, 2009. 1, 20-43; (하), 법제처, 법제 614호, 2009. 2, 15-49.

박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1, 92-123.

박희영, 독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향, 최신외국법제정보, 한국법제연구원, 2011-2호(2011.4.20.), 70-84.

박희영, 독일형사판례연구 Ⅰ [사이버범죄], 한국학술정보(2011.3), 91-202.

박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018 ·여름), 30.

박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 2012.9, 153-186.

박희영, 정보기술 시스템의 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, 43-68, 법제 612호, 2008. 12, 31-64.

박희영, 테러 방지를 위한 연방범죄수사청법의 통신감청권 등 일부 위헌, BVerfG Urteil vom 20. April 2016 - 1 BvR 966/09, 1 BvR 1140/09, 최신독일판례연구, 로앤비(www.lawnb.com), 2016.10, 1-10.

박희영, 현행 전기통신감청법은 합헌, BVerfG, Beschluss vom 12.10.2011 - 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, 최신독일판례연구, 로앤비(www.lawnb.com), 2012. 1, 1-6.

박희영, 효율적이고 실무에 적합한 형사절차의 구성에 관한 법률(2017.8.17) : 암호통신감청과 온라인 수색 등, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.12, 1-16.

박희영·홍선기 공저, 독일연방헌법재판소판례연구 Ⅰ [정보기본권], 한국학술정보(2010.12), 1-45.

허 황, 최근 개정된 독일 형사소송법 제100조b의 온라인 수색과 제100조a의 소스통신감청에 관한 연구, 형사법의 신동향 통권 제58호, 대검찰청, 2018.3, 98-122.

BGH, Beschluß vom 31. 1. 2007 - StB 18/06.(https://bit.ly/2TCRF9q)

Deutscher Bundestag, Drucksache 18/11163, 14.02.2017, Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes.(https://bit.ly/2O0cDtl)

Deutscher Bundestag, Drucksache 18/12785, 20.06.2017, Beschlussempfehlung und Bericht des

Ausschusses für Recht und Verbraucherschutz (6. Ausschuss).(https://bit.ly/2TJZCtn)
BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR 543/06.(https://bit.ly/2J7kDtT)
BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08.(https://bit.ly/2F1OUF8)
BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09.(https://bit.ly/2kTLfPp)
BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07.(https://bit.ly/2VTdeQi)

인터넷사이트

Online-Durchsuchung: Bundeskriminalamt programmiert eigenen Staatstrojaner, trotz ZITiS (https://bit.ly/2NelwN5)
Nebelkerzen um Staatstrojaner und Online-Durchsuchung(https://bit.ly/2L5WO1A)