형사정책연구 Korean Criminological Review
제34권 제3호(통권 제135호, 2023 · 가을)

수사목적 온라인 수색의 허용요건
-독일의 논의를 참고한 입법론적 검토-*

박 중 욱**

국 | 문 | 요 | 약

온라인 수색은 기본적으로 국가에 의한 해킹이고, 이러한 수사방법은 오늘날의 정보기술 환경을 고려할 때 시민의 기본권을 심각하게 침해하고 국가의 기본권 보호의무를 극도로 축소시킬 수 있다. 하지만 텔레그램이나 다크넷 등의 온라인 플랫폼을 이용한 테러나 조직범죄 등의 안보범죄 및 디지털 성착취물이나 마약의 유통·거래·소지 등의 범죄에 대한 수사에서 기존의 사이버범죄에 대한 수사방법은 한계가 가진다. 즉 암호화기술에 기반하여 폐쇄성과 익명성을 특징으로 하는 온라인 플랫폼에서 행해지는 범죄는 주로 국가의 기반·존립과 같은 국가의 안전 및 생명·신체·자유와 같은 개인의 안전을 침해하지만, 그에 대처해야 하는 국가가 사용할 수 있는 방법은 제한적이다. 이런 점을 고려할 때, 온라인 수색이라는 수사방법이 그 자체로서 위헌적이거나 무조건 금지되어야 하는 것은 아니라 할 것이다. 이 모든 것을 고려할 때, 온라인 수색의 수권규정은 국가의 기본권 보호의무 및 법치국가 원칙과 비례성 원칙에 따라 그 강력한 기본권 침해강도에 상응하도록 엄격하게 형성되어야 한다.

법치국가의 형사사법은 국가 형벌권의 유효한 실현과 사법 정형적인 절차에 따른 기본권 보호라는 상반되지만 동위에 놓인 두 가치가 이익형량될 것을 요구한다. 정보기술의 발전에 따라 법익보호를 위해 수사기관의 능력이 변화된 기술여건에 발맞추어 강화되어야 하듯이, 기본권 보호를 위해 기본권을 강력히 침해하는 수사처분은 법치국가 원칙에 따라 엄격하게 통제되어야 한다.

DOI : https://doi.org/10.36889/KCR.2023.9.30.3.95.

❖ 주제어 : 다크넷 범죄, 온라인 수색, 통신원감청, IT-기본권, 비례성, 투명성, 수사처분의 비밀성, 절차법적 안전장치, 사후 통지

* 본 논문은 2023년 8월 11일에 한국형사법학회와 한국형사·법무정책연구원이 공동으로 주최한 '2023년 제5회 한국형사법학회 신진형법학자포럼 학술회의(대주제: 형사법입법영역의 당면 과제)'에서 발표한 원고를 수정·보완한 것이다. 본고에 귀한 의견을 주신 학술회의 토론자 3분(김면기 교수, 박소현 박사, 송주용 박사) 및 익명의 심사자 3분께 깊은 감사를 표합니다.

** 동국대학교 비교법문화연구원 전문연구원, 원광대·한남대 강사, 법학박사.

Ⅰ. 글을 시작하며

온라인 수색(Online-Durchsuchung)은 국가의 합법화된 해킹이다. 오늘날의 정보기술 환경 및 인격발현을 위한 정보기술시스템[1]의 중요성을 고려할 때 온라인 수색은 기본권을 심각하게 침해할 수 있고, 그 결과 국가의 기본권 보호의무를 극도로 후퇴시킬 수 있다. 이런 이유로 독일 연방헌법재판소(Bundesverfassungsgericht: BVerfG)는 온라인 수색의 합헌성을 처음 심사한 2008.2.27.의 판결(소위 '온라인 수색 판결')[2]에서 그 판단에 앞서 일반적인격권(Allgemeines Persönlichkeitsrecht)으로부터 '정보기술시스템의 비밀성과 무결성의 보장에 관한 기본권(Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)', 소위 'IT-기본권(IT-Grundrecht)'[3]을 새로이 창설한 후,[4] 이 기본권에 대한 제한으로서 온라인 수색

1) 정보기술시스템은 디지털 정보를 생성·처리·저장할 수 있게 하는 전자기기로서, 여기에는 PC, 태블릿-PC, 스마트폰을 포함한 이동전화기뿐만 아니라 정보저장장치도 포함된다. 후자에는 주로 개인의 사적인 이용을 위한 내외장의 정보저장장치뿐만 아니라 단체, 기업, 정부의 업무상 이용을 위한 업무용 서버도 포함된다. 다만, 온라인 수색의 대상이 되는 정보기술시스템은 개념적으로 네트워크, 즉 인터넷을 통해 연결될 수 있는 통신기기임을 전제로 한다(*BVerfGE* 120, 274, 304 f. [Rn. 174-176]).

2) *BVerfGE* 120, 274 = NJW 2008, 822. 동 판결에서 BVerfG는 온라인 수색의 허용요건을 범죄예방(위험방지)과 형사소추(수사)의 목적으로 구분하지 않고 동일하게 취급하였다(a.a.O. 315 [Rn. 207]).

3) *Gurlit*, NJW 2010, 1035, 1036; Dalby, CR 2013, 361, 367; *Roggan*, StV 2017, 821, 823; *Derin/Golla*, NJW 2019, 1111, 1114; 이원상, "온라인 수색(Online-Durchsuchung)에 대한 고찰 - 독일의 새로운 논의를 중심으로",『형사법연구』제20권 제4호, 한국형사법학회, 2008.12, 335, 347면; 박희영, "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계",『원광법학』제28권 제3호, 2012.9, 153, 160면 등). 한편 일부 문헌에서는 '컴퓨터-기본권(Computer-Grundrecht)'이라고 불리기도 한다(Kudlich, GA 2011, 193, 198; *Singelnstein/Derin*, NJW 2017, 2646, 2648; *Zimmermann*, JA 5/2014, 321, 323).

4) *BVerfGE* 120, 274, 303 ff. [Rn. 168 ff.]. 동 판결에서 BVerfG는 과학기술의 발전과 생활환경의 변화 과정에서 새로운 유형의 인격에 대한 위험에 대처하고 그 기본권적 보호의 흠결을 보충하기 위해 일반적인격권에 기초한 기존의 보호인 정보자기결정권(das Recht auf informationelle Selbstbestimmung)을 초과하는 새로운 기본권적 보호가 필요하다고 판단하였다. 즉 1983년에 창설된 정보자기결정권이 이미 정보보호와 관련하여 확고한 지위를 획득하였음에도 불구하고 BVerfG가 더 나아가 IT-기본권을 인정한 이유는 현재의 기술·사회적 여건 아래에서 개인정보가 포괄적으로 저장되어 있는 정보기술시스템은 국가의 접근으로부터 기본권적으로 특별히 보장되어야 한다는 점에 있다. IT-기본권은 - 개별적인 통신과정이나 저장된 정보를 넘어 – 주거의 불가침과 유사하게 개인에게 귀속된 사이버 공간에 대한 기본권적 보호를 지향한다. 물론 문헌에서 부분적으로 이 기본

의 합헌성 및 그 요건을 판단하였다. 즉 BVerfG는 온라인 수색 판결에서 IT-기본권을 창설함으로써 오늘날 네트워크로 연결된 복합적 정보기술시스템에서의 개인의 정보보호의 중요성을 강조하면서, 동시에 테러 등의 안보 영역에서 중대한 법익을 보호하기 위해 온라인 수색이 엄격한 요건 아래에서 정당화될 수 있음을 확인하였다. 요컨대 온라인 수색은 해킹이고 사적 영역을 깊게 침해하는 처분이지만 그 자체로서 국가가 사용할 수 없는 위헌적인 수사방법은 아니라는 것이다.

다만, 온라인 수색은 법치국가 원칙 및 비례성 원칙에 따라 엄격히 제한되고 통제되어야 한다. 따라서 그 수권규정은 그 기본권 침해강도에 상응하는 제한된 범위의 중대한 범죄 및 엄격한 절차법적 안전장치와 결부되어야 한다. 이때 세부적으로 어느 정도의 처분요건과 절차법적 통제가 요구되는지를 판단하기 위해서는 먼저 온라인 수색으로 수집될 수 있는 정보의 범위 및 그에 따른 기본권 침해강도를 정확히 이해하고 이를 통해 그 개념을 명확히 할 필요가 있다. 아울러 2005년 이래로 온라인 수색을 실제로 도입하고 그 합헌성과 허용요건을 자세히 심사한 후 다시 입법한 독일의 논의 상황이 참고될 필요가 있다. 이때 특히 협의의 비례성, 즉 이익형량의 측면에서 온라인 수색의 수권규정에 포함되어야 하는 내용을 구체적으로 제시하고 있는 BVerfG의 판결이 자세히 검토될 필요가 있는데, 동 재판소는 사적 영역을 깊게 침해하는 비밀의 수사처분의 합헌성을 심사한 최근의 일련의 판결에서 투명성 요청에 근거하여 그리고 사적 생활형성의 핵심영역 보호를 위해 엄격한 절차법적 안전장치를 요구한다.

아래에서는 먼저 본 연구의 전제가 되는 독일에서의 온라인 수색 도입의 배경과 현황 및 한국에서의 논의 상황을 개관한 후(Ⅱ), 그 개념을 비밀성과 정보수집의 유형을 기준으로 구체화할 것이다(Ⅲ). 이어서 온라인 수색이 허용되기 위한 요건, 특히 절차법적으로 형성되어야 하는 안전장치의 구체적인 내용을 BVerfG의 판결을 중심으로 검토한 후(Ⅳ), 수사목적의 온라인 수색을 우리 법제에 도입하기 위한 요건을 검토한다(Ⅴ).

권의 창설이 비판되기도 하지만(*Gurlit*, NJW 2010, 1035, 1037), 정보통신기술의 지속적인 발전 및 이를 통한 완전한 감시의 가능성을 고려할 때, 이 기본권의 적용영역은 앞으로 확대될 것이다(vgl. *Kutscha*, NJW 2008, 1042, 1043: IT-기본권의 보호범위가 아직 명확하지 않다).

Ⅱ. 독일에서의 온라인 수색 도입의 배경과 현황 및 한국에서의 논의 상황

1. 독일에서의 온라인 수색 도입의 배경과 현황

2001년의 9·11 테러 및 2004년의 마드리드 테러와 2005년의 런던 테러 등 연이은 테러 이후 미국과 유럽에서는 정보기관과 수사기관을 중심으로 '예방적 교신데이터의 수집·보관·이용(data retention; Vorratsdatenspeicherung: VDS)'[5]과 함께 암호화된 통신 및 정보은폐에 대처하기 위해 온라인 수색의 필요성이 제기되었다. 우선 전자와 관련해서는 유럽연합(European Union; Europäische Union: EU)이 2006.3.15.에 동 제도의 설치를 위한 지침 2006/24/EC[6]를 통과시킴으로써,[7] EU의 각 회원국은 그것을 국내법에 도입할 의무를 부담했고, 이에 따라 독일은 2007.12.21.의 개정[8]을 통해 예방적

5) 교신데이터(traffic data; Verkehrsdaten)는 우리 통신비밀보호법(이하 "통비법") 제2조 제11호의 '통신사실확인자료'에 상응하는 정보이다.

6) 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. 이 지침은 자유로운 정보교환과 프라이버시 보호를 위해 정보보호와 인격보호가 필요하다는 지침 95/46/EG 및 이러한 보호가 전기통신분야에서도 여전히 유효하다는 것을 확인하는 지침 2002/58/EG의 내용을 승계하면서, 다만 그러한 보호도 공공질서의 유지를 위해 제한될 필요가 있고, 특히 교신데이터가 형사소추에 있어 가치 있는 도구이기 때문에 전기통신서비스제공자(이하 "ISP")에게 동 정보의 예방적 수집·보관 의무를 부과할 필요가 있다는 점을 강조한다(동 지침의 전문(前文)에 기재된 고려사항 중 (4), (7) - (10)의 내용 참고).

7) 연이은 테러 이후 유럽이사회(the European Council; der Europäische Rat)는 2004.3.25.에 대테러 투쟁 선언을 통해 유럽연합이사회(EU이사회/각료이사회, the Council of EU/Council of Minister; der Rat der EU/Ministerrat)에게 '서비스제공자에 의한 교신데이터 보관(저장)에 관한 법규정안(案)'을 검토하도록 요청하였고, EU이사회는 2005.7.13.에 런던 테러를 비난하는 선언 후 2006.3.15.에 위 지침 2006/24/EC를 의결하였다.

8) Gesetz zur Neuregelung der TKÜ und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (TKÜG) vom 21.12.2007, BGBl. I S. 3198, 2008.1.1.에 발효. 이 TKÜG에 의해 비밀의 정보수집에 대해 규정하는 StPO 제100조a 이하가 정비되었다. 이에 따라 당시 제100조a, b는 통신감청을, 제100조b-e는 주거감청을, 제100조f는 주거 외 감청을, 제100조g는 교신데이터 수집을. 제100조h는 주거 외 촬영 및 기타 감시목적의 기술적 수단의 투입을, 제100조i는 IMSI-Catscher의 규제하였다. 물론 이후 2015년에 제100조g가 대폭 수정되었고, 2013년에 가입자정보의 제공을 위한 제100조j가 추가되었다. 그리고 2017년 제100조b의 위치로 온라인

교신데이터의 수집·보관과 수사기관에의 제공을 전기통신법(Telekommunikationsgesetz: TKG) 제113조a, b와 StPO 제100조g에 규정하였다. 하지만 이 규정들에 대해서는 그 발효 전에 BVerfG에 헌법소원이 제기되었고,[9] 동 재판소는 2010.3.2.의 판결(소위 'VDS 판결')을 통해 위 규정들이 위헌무효임을 선고하였다.[10] 이후 독일 의회는 전술한 판결의 취지에 따라 2015.12.10.의 개정을 통해 위 규정들을 개정하였다.[11] 반면, 온라인 수색과 관련해서는 2023년 7월 현재까지 아직 EU나 사이버범죄협약(Convention on Cybercrime: CCC)[12]을 채택한 유럽평의회(Council of Europe) 차원에서의 의결은 없으며, 각국은 그것을 개별적으로 도입하고 있다.[13]

수색이 추가되면서 제100조a-e에 통신감청, 온라인 수색, 주거감청이 함께 규정되었다.

9) 좀 더 정확히 말하면 TKÜG에 대해서는 그 시행 전에 BVerfG에 효력정지 가처분과 함께 위헌법률 심사가 제청되었고, 개정된 내용 중에서 교신데이터 수집(StPO 제100조g)에 대해서는 제1 합의부가 맡아서 심사하였고, 나머지 중에서 통신감청(StPO 제100조a, b)과 비밀의 수사처분에 대한 통지의무(StPO 제101조 제4-6항) 등에 대해서는 제2 합의부가 맡아서 심사하였다. 이때 후자의 심사 결과인 2011.10.12.의 판결(소위 'TKÜG 판결'; *BVerfGE* 129, 208)에서 BVerfG는 심사 대상 규정을 모두 합헌으로 판단하였다.

10) *BVerfGE* 125, 260 = NJW 2010, 833. 이 판결에서 BVerfG는 형사소추, 위험방지, 정보기관의 임무수행을 위한 교신데이터 수집·보관·이용은 기본권에 대한 '특별히 중대한 침해(ein besonders schwerer Eingriff)'이지만 그 자체로 처음부터 비례성에 반하는 위헌적인 처분은 아니라고 전제한 후(a.a.O. 316-324 [Rn. 204-219]), 동 처분의 수권규정이 비례성 원칙에 따라 합헌적으로 형성되기 위해서는 강화된 처분요건과 절차법적 안전장치가 요구된다고 하면서(a.a.O. 325-340 [Rn. 220-253]), TKÜG에 의해 도입된 (舊) TKG 제113조a, b 및 (舊) StPO 제100조g는 위헌이라고 판시하였다(a.a.O. 347 ff. [Rn. 269 ff.]). 한편 2014.4.8.에 TKÜG에 의한 교신데이터 수집·보관·이용 제도 도입의 근거가 되었던 지침 2006/24/EG가 유럽사법재판소(European Court of Justice: ECJ; Europäischer Gerichtshof: EuGH)에 의해 무효라고 선언되었다(*EuGH* NJW 2014, 2169). 이때 동 재판소는 위 BVerfG의 판결이유와 유사한 이유를 제시하면서 교신데이터 수집·보관·이용 제도가 유럽 기본권 헌장(Charta der Grundrechte: GRC) 제7조[사생활 존중의 권리]와 제8조[개인정보보호의 권리]에 반한다고 판시하였다.

11) Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, BGBl Ⅰ S. 2218, 2015.12.18.에 발효.

12) CCC는 2001.11.23.에 헝가리 부다페스트(Budapest)에서 의결되어, 2004.7.1.에 발효되었고, 독일은 2007.11.16에 비준하였으며, 2009.3.9.에 비준서를 기탁하였다. CCC는 유럽평의회가 채택한 국제협약이지만, 비유럽국가인 미국, 일본, 호주 등도 가입되어 있으며, 우리나라도 2022년 11월에 그 가입을 위한 의향서를 제출한 상태이다(https://www.mofa.go.kr/www/brd/m_4080/view.do?seq=372854).

13) 2021년에 나온 보고서에 따르면 온라인 수색을 도입한 유럽의 국가로는 영국, 오스트리아, 프랑스, 독일, 네덜란드, 스페인, 스위스 등이 있고, 유럽 외의 국가로는 미국, 호주가 있다고 한다(*Sieber/Mühlen/Tropina*, Access to Telecommunication Data in Criminal Justice, 2021, S. 108, 재인용: 박희영, "유럽에서 온라인수색과 암호통신망 EncroChat 사건", 『형사법의 신동향』 통권

온라인 수색의 도입과 관련해서 독일에서는 그 강력한 기본권 침해성 때문에 전술한 예방적 교신데이터의 수집·보관·이용보다 더 많은 논란이 있었다.[14] 하지만 여론의 강력한 대테러 요청으로 2006.12.20.에 노르트라인-베스트팔렌주(州)(Nordrhein-Westfalen: NRW)가 처음으로 온라인 수색을 – 수사목적이 아닌 – 정보기관[15]의 임무수행을 위해 (舊) 주 헌법보호법(Verfassungsschutzgesetz Nordrhein-Westfalen: 2006 VSG NRW) 제5조 제2항 제11호 후단[16]에 도입하였다.[17] 이 규정에 대해서는 바로 규범통제를 위한 위헌법률심판이 제기되었고, BVerfG는 2008년 초의 온라인 수색 판결을 통해 그 허용요건을 자세히 설시하였다. 이 판결 직후인 2008.12.25.에 독일 의회는 판결의 취지를 반영하여 연방범죄수사청법(Bundeskriminalamtgesetz: BKAG)을 개정하였다.[18] 이를 통해 연방범죄수사청(BKA)[19]에게는 국제테러의 위험을 방지할

제78호, 대검찰청, 2023.3, 36, 40면).

14) 독일 연방검찰청의 고등검사(Oberstaatsanwalt)였던 *Hofmann*은 – 최소한 – 테러 등 안보범죄의 영역에서 유용한 수사방법인 온라인-수색이 StPO의 압수수색 일반규정이나 통신감청 규정에 근거하여 명령·집행될 수 있어야 한다고 주장하였다(*Hofmann*, NStZ 2005, 121, 123 u. 125).

15) 독일에서는 총 19개의 정보기관이 운영되고 있다. 국내정보기관으로는 연방헌법보호청(Das Bundesamt für Verfassungsschutz: BfV)과 16개 주의 헌법보호청(Landesbehörde für Verfassungsschutz: LfV)이 있고, 국외정보기관으로는 연방정보부(Der Bundesnachrichtendienst: BND)가 있으며, 군(軍) 관련 정보기관으로는 (연방)군정보부(Der Militärische Abschirmdienst: MAD)가 있다. 이에 대한 자세한 내용과 독일 정보기관 관련 법적 체계에 대해서는 박희영/홍선기, "독일 정보기관의 공법 체계 및 경찰과의 분리원칙", 『법학논집』 제26권 제3호, 이화여자대학교 법학연구소, 2022.3, 235, 237면 참고.

16) (舊) 2006 VSG NRW 제5조 [권한(Befugnisse)] ① [생략] ② 헌법보호청(LfV)은 다음 각호의 처분을 제7조의 기준에 따라 정보수집을 위해 정보기관의 수단으로(정보기관의 임무수행을 위해) 사용할 수 있다: 1. …… 11. 인터넷 비밀감시 및 기타 규명, 특히 통신장치에의 비밀참여나 그 검색 및 기술적 수단을 이용하는 경우를 포함한 정보기술시스템에의 비밀 접근(Zugriff). 전술한 처분들이 편지·우편·통신의 비밀에 대한 침해이거나 그 유형과 중대함에서 그와 유사한 경우, 이 침해는 제10조법(G 10)의 요건 아래에서만 허용된다.
[※ 괄호의 내용 보충 및 밑줄은 필자가 넣었음, 이하 독일 법령에서 동일]

17) Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen: VSG NRW) vom 20. Dezember 2006, GV. NRW. S. 620.

18) Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA vom 25. Dezember 2008, BGBl. Ⅰ S. 3083, 2009.1.1.에 발효.

19) BKA는 독일 연방내무부에는 소속되어 있는 연방 경찰기관이다. 연방내무부에는 BKA 이외에 연방경찰(Bundespolizei)과 연방의회경찰(Polizei beim Deutschen Bundestag)도 독립되어 소속되어 있다.

임무가 새로이 부과되었고,[20] 그 임무의 수행을 위한 수단으로서 온라인 수색을 포함하여 장기감시, 예방적 교신데이터의 수집·보관·이용, 주거감청, 주거 외 감청 등 여러 유형의 비밀의 수사처분이 도입되었다(BKAG 제20조g-x).[21] 하지만 이 신설된 규정들에 대해서는 또다시 헌법소원이 제기되었고, BVerfG는 2016.4.24.의 판결(소위 'BKAG 판결')[22]에서 (협의의) 비례성 심사를 함에 있어 온라인 수색을 주거감청과 동일하게 취급하였다.[23] 이후 독일 의회는 BKAG 판결의 내용을 수용하여 2017.6.1.의 개정[24]을 통해 2017 BKAG 제49조에 국제테러의 위험방지를 위한 온라인 수색의 수권규정을, 그리고 2017.8.17의 개정[25]을 통해 StPO 제100조b에 수사목적를 위한 온라인 수색의 수권규정을 각각 신설하였다.

독일 연방법무부(Das Bundesministerium der Justiz: BMJ)의 최근 공고에 따르면, StPO에 따른 수사목적의 온라인 수색은 2020년에 총 10개의 수사절차에서 총 23회(최초명령 12회, 연장명령 11회) 내려졌으나, 실제로는 8회만이 집행되었다. 명령이 내려진 대상 범죄와 횟수는 테러단체나 범죄단체 조직죄(StPO 제100조b 제2항 제1호 b목) 3회, 아동음란물 배포·취득·소지죄(동호 e목) 1회, 범죄단체구성 절도죄(동호 h목) 1회, 중강도죄와 강도치사죄(동호 i목) 1회, 강도적 공갈죄과 특히 중대한 공갈죄(동호 j목) 8회, 마약유통·거래·수입 등 죄(동 제4호 b목) 9회이다. 2019년에는 동 처분이 총 21개의 수사절차에서 총 33회(최초명령 22회, 연장명령 11회) 내려졌으나, 실제로는 12회만

20) BKAG에 따르면 BKA는 기본적으로 – 범죄예방과 형사소추 및 기타 위험방지의 임무를 수행하는 – 각 주(州)의 수사기관(검찰과 경찰)을 지원하는 기관이지만(BKAG 제1, 2조), 테러 및 무기·마약거래 등 국제적 조직범죄의 영역에서는 (경찰과 같은) 수사기관이다(BKAG 제4조). 하지만 2008년 개정을 통해 BKA는 현재 국제테러의 위험방지 임무도 수행한다(2017 BKAG 제5조 = (舊) 2008 BKAG 제4조a). 참고로 과거 나치(Nazi)의 정보기관이자 수사기관이었던 게슈타포(Geheimes Staatspolizeiamt, Gestapo)의 부정적 영향 때문에 독일에서 정보기관과 수사기관은 분리되는 것이 원칙이지만, 위 BKAG 개정을 통해 현재 테러 등 안보와 조직범죄의 영역에서는 그 경계가 흐릿해 졌다.

21) 온라인 수색은 (舊) 2008 BKAG 제20조k(= 2017 BKAG 제49조)에 규정되어 있었다.

22) *BVerfGE* 141, 220 = NJW 2016, 1781.

23) *BVerfGE* 141, 220, 268 ff. [Rn. 103 ff.], 특히 303 [Rn. 210 a.E.].

24) Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017, BGBl. I S. 1354, 2018.5.25. 발효. 이 개정법률을 통해 BKAG는 전면개정되었고 조문번호가 전체적으로 다시 정비되었다.

25) Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, BGBl. I S. 3202, 2017.8.24.에 발효.

이 집행되었다. 명령이 내려진 대상 범죄와 횟수는 내란·외환 등의 죄(StPO 제100조b 제2항 제1호 a목) 1회, 테러단체나 범죄단체 조직죄(동호 b목) 2회, 성적자기결정에 대한 죄(동호 d목) 1회, 개인의 자유에 대한 죄(동호 g목) 4회, 중강도죄와 강도치사죄(동호 i목) 2회, 강도적 공갈죄와 특히 중대한 공갈죄(동호 j목) 13회, 자금세탁과 부정수익 은닉죄(동호 l목) 1회, 마약유통·거래·수입 등 죄(동 제4호 b목) 12회, 전쟁무기통제법 위반죄(동 제5호 a목) 1회이다.[26]

2. 한국에서의 온라인 수색 도입의 논의

반면, 우리의 경우 암호화된 통신에 대한 감청의 어려움이 독일과 동일하게 존재하였지만, 독일과 달리 온라인 수색의 법제화 작업은 최근에서야 본격적으로 시도되고 있다.[27] 물론 여러 문헌에서 독일의 온라인 수색과 관련된 BVerfG의 두 판결 및 2017년의 입법상황이 소개되고 그 허용요건과 국내 도입 가능성이 논해졌으나,[28] 학계와 수사기관 외에는 큰 관심을 끌지 못하였다. 하지만 2020년 초에 사회적으로 크게 논란이 되었던 소위 '텔레그램 n번방 사건'[29]을 통해 디지털 성착취물의 제작·유포에 대한 강력

26) https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument44152, 2023. 7. 31. 검색. 다만, 2019년의 통계 자료에는 전체 명령 건수와 범죄별 명령 건수의 합에서 4회의 오차가 있다.

27) 작년에 경찰청은 수사목적 온라인 수색의 도입을 위한 연구용역을 공개 입찰하였고(한국일보, "경찰, '실시간 감시' 온라인 수색 도입 검토... 기본권 침해 우려도", 2022. 4. 29.자, https://m.hankookilbo.com/News/Read/A2022041509320001942, 2023.7.31. 검색), 작년 말에 그 연구결과물이 나왔다(김재희/박희영, 온라인 수색 활동의 적법성 검토 및 도입방안 연구, 2022년도 경찰청 정책연구용역 결과보고서, 경찰청/성결대학교, 2022.12).

28) 대표적으로 2008년의 온라인 수색 판결 직후의 글로는 이원상(주 3), 335면; 박희영, "독일에 있어서 경찰에 의한 '예방적' 온라인 수색의 위헌여부", 『경찰학연구』 제9권 제2호, 경찰대학, 2009.8, 185면; 2017년의 입법 직후의 글로는 허황, "최근 개정된 독일 형사소송법 제100조b의 온라인 수색(Online-Durchsuchung)과 제100조a의 소스통신감청(Quellen-Telekommunikationsüberwachung)에 관한 연구", 『형사법의 신동향』 통권 제58호, 대검찰청, 2018.3, 94면; 박희영, "수사목적의 암호통신감청(Quellen TKÜ)의 허용과 한계", 『형사정책연구』 제29권 제2호, 한국형사법무정책연구원, 2018.6, 26면.

29) '텔레그램 n번방 사건'의 사실관계에 따르면 암호화·익명화된 메신서 플랫폼인 텔레그램을 통해 성착취물이 불법적으로 유통되었을 뿐만 아니라, 텔레그램이 현실에서의 성범죄 공모의 수단으로 활용되었다. 자세한 사실관계는 윤신명, "텔레그램 등 익명·비대면 공간에서의 조직범죄 수사절차와 한계", 『4차산업혁명에 있어서 정보화 시대의 당면 과제』, 4차산업혁명융합법학회/한국형사소

한 형사법적 대응이 공론화되었고, 이때부터 잠입수사와 함께 온라인 수색의 도입 필요성이 강력히 주장되었다.[30] 이에 따라 국회는 먼저 '디지털 성착취물'[31]의 제작·유통 및 그 소비행위 등을 처벌하기 위해 2020.5.19.에 「성폭력범죄의 처벌 등에 관한 특례법」("성폭력처벌법")을, 2020.6.2.에 「아동·청소년의 성보호에 관한 법률」("청소년성보호법")을 개정한 후,[32] 곧이어 2020.6.9.에 「전기통신사업법」 제22조의5 제1, 2항을 개정하여 부가통신사업자에게 디지털 (아동·청소년)성착취물의 삭제·접속차단 등의 유통방지 조치의무와 기술적·관리적 조치의무를 부과하였다(2020.12.10. 시행).[33] 하지만 형사절차법적 대응으로서의 입법적 조치는 잠입수사와 온라인 수색의 강력한 기본권 침해강도와 수사기관에 의한 그 오남용의 우려 때문에 늦어지다가 2021.3.23.의 청소년성보호법 개정(2021.9.24. 시행)을 통해서야 비로소 신분비공개수사와 신분위장수사만이 제한된 범죄영역과 비교적 엄격한 절차를 조건으로 도입되었다(동법 제25조의2 이하).[34] 반면 온라인 수색의 도입을 위한 입법적 조치는 아직 행해지지 않고 있다.

송법학회 2022년 하계 학술대회 자료집, 63, 75면 이하 참고.

30) 대표적으로 윤지영, "디지털 성범죄 대응을 위한 수사법제 개선 방안 - 온라인 수색과 잠입수사 법제화를 중심으로", 『형사정책』 제32권 제2호, 한국형사정책학회, 2020.7, 41면. 온라인 수색과 관련해서는 이원상, "온라인수색의 도입 필요성과 한계 – 아동·청소년 대상 디지털 성범죄를 대상으로", 『비교형사법연구』 제24권 제2호, 한국비교형사법학회, 2022.7, 183면.

31) '디지털 음란물'과 '디지털 성착취물'의 개념상 구분에 대해서는 전윤정, "'n번방' 사건으로 본 디지털 성범죄 규제현황과 개선과제", 『이화젠더법학』 제13권 제3호, 이화여자대학교 젠더법학연구소, 2021.12, 1, 4면 참고.

32) 구체적으로 보면 성폭력처벌법 개정을 통해 통신매체를 이용한 음란행위(제13조), 카메라 등을 이용한 촬영행위(제14조 제1항), 촬영물이나 복제물의 반포 등 행위(제14조 제2, 3항)의 법정형이 상향되었으며, 성착취물 소지·구입·저장·시청행위(제14조 제4항)와 성착취물을 이용한 협박·강요행위(제14조의3)를 처벌하는 규정이 신설되었다. 그리고 청소년성보호법 개정을 통해 '아동·청소년성착취물'의 제작·배포·소지·운반·광고 등 행위(제11조 제1-4항)의 법정형 상향되었으며, 해당 성착취물의 구입·시청행위를 처벌하는 규정(제11조 제5항)이 신설되었다.

33) 이때 동법에는 본문의 조치의무 위반자에 대한 과징금 부과 규정이 함께 신설되었다(제22조의6). 참고로 이 조치의무는 원래 (舊) 청소년성보호법 제17조에 규정되어 있어서 '아동·청소년성착취물'만을 대상으로 하였었으나, 2020.6.9.의 개정을 통해 전기통신사업법으로 그 자리를 옮김으로써, 현재에는 모든 디지털 성착취물에 적용된다.

34) 이때의 청소년성보호법 개정을 통해 아동·청소년에 대한 성적 착취를 목적으로 하는 대화·유인·권유행위, 소위 '온라인 그루밍' 행위를 처벌하는 규정도 신설되었다(제15조의2). 동법 제25조의2에 따른 비밀의 수사처분은 – 그 법적 근거가 청소년성보호법에 규정되어 있듯이 – 아동·청소년을 대상으로 하는 동법 제11조와 제15조의2의 행위 및 성폭력처벌법 제14조 제2, 3항의 행위에 대한 증거수집을 위해서만 사용될 수 있다.

한편 텔레그램과 디지털 성착취물에 대한 이러한 대응 논의는 암호화(정보검색방지), 폐쇄성(인증절차), 익명성(임의 IP)을 본질적 성격으로 하는 온라인 플랫폼에서 행해지거나 그것을 이용한 범죄, 소위 '다크넷 범죄'[35]에 대한 대처 필요성으로 확대되고 있다.[36] 다크넷 범죄의 특징인 익명성·폐쇄성을 기술적으로 가능하게 해주는 온라인 플랫폼은 그 성격상 거기에서 공유된 정보는 기본적으로 서버에 보관되지 않거나[37] 기술적으로 운영자도 그 내용을 해독할 수 없도록(종단간암호화)[38] 설계되어 있다. 또한 텔레그램과 같은 폐쇄적인 모바일 메신저의 운영자 및 다크넷 등 온라인 플랫폼의 운영자는 대부분 해외 업체이고 그 서버 또한 해외에 존재하는데, 이 경우 수사기관이 해당 업체로부터 서버에 저장되어 있는 증거자료를 획득하기 위해서는 사법공조 절차를 통해야 하므로 상당한 시간이 필요하고, 이런 절차를 통한다고 하더라도 해당 업체는 거의 협조하지 않는다.[39] 이런 점에서 내란, 외환, 테러 등의 안보 관련 범죄 및 성착취물 제작·배포·거래, 마약·무기 거래, 자금세탁 등의 범죄가 조직적으로[40] 다크넷 범죄의 형태로 행

35) 다크넷 범죄의 대표적인 예가 가상자산을 통한 마약거래이고, 우리나라에서는 2016년에 해당 사건이 처음 공개되었지만 사회적으로 주목을 끌지 못했다(이데일리, "IP추적 어려운 '다크웹', 마약 밀매 루트로 악용", 2017.9.27.자, https://www.edaily.co.kr/news/read?newsId=01656406616064384&mediaCodeNo=257, 2023.7.31. 검색). 다크넷을 통한 거래 중 91%가 마약류 거래라고 한다(중앙일보, "마약사범 역대 최다…10명 중 6명은 '30대 이하' 청년이었다", 2023.7.15.자, https://www.joongang.co.kr/article/25175029#home, 2023.7.31. 검색).

36) 박웅신/이경렬, "다크넷 범죄현상과 형사법적 대응방안", 『형사법의 신동향』 통권 제58호, 대검찰청, 2018.3, 219, 232면 이하; 윤지영(주 30), 47면 이하; 이원상, "다크넷 수사를 위한 수사제도에 대한 소고", 『형사법의 신동향』 통권 제69호, 대검찰청, 2020.12, 343, 357면 이하; 류부곤, "비닉성 온라인 플랫폼을 이용한 범죄에 대한 법적 대응방안", 『경찰학연구』 제21권 제1호, 경찰대학, 2021.3, 29, 31-32면. 텔레그램과 다크넷은 기술적 측면에서 구분되지만, 텔레그램의 '비밀대화방'도 다크넷과 마찬가지로 보안성, 폐쇄성, 익명성을 특징으로 한다.

37) 예를 들어, 텔레그램의 '비밀대화'.

38) 예를 들어, 텔레그램의 '비밀대화', 카카오톡의 '비밀대화', 라인의 'letter sealing'.

39) 윤신명(주 29), 89면. 텔레그램에 대해서는 윤지영(주 30), 46면; SBS 뉴스, "성착취물 범죄 온상된 텔레그램…'n번방 방지법'도 못 잡는다", 2022.9.2.자, https://news.sbs.co.kr/news/endPage.do?news_id=N1006882525, 2023.7.31. 검색: "김승주 고려대 정보보호대학원 교수는 "텔레그램은 지금껏 그 어떤 정부에도 수사 협조를 하지 않아 왔다"며 "텔레그램 정보만으로 피의자 신원을 파악하는 것은 불가능하다"고 짚었습니다." 이에 더해 현재 공개된 텔레그램 회사의 위치 자체가 정확하지 않다고 한다(SBS 뉴스, "[단독] 비밀 조직 같은 텔레그램 … 해외 주소 찾아가 보니", 2023.6.15.자, https://news.sbs.co.kr/news/endPage.do?news_id=N1007230917, 2023.7.31. 검색).

40) '텔레그램 n번방 사건'에서 대법원은 최소한의 통솔체계는 없지만 범죄의 계획과 실행을 용이하게 할 정도의 조직적 구조가 갖추었다는 이유로 형법 제114조의 '범죄집단조직죄'의 성립을 인정하였다(대법원 2021.10.14. 선고 2021도7444 판결).

해지는 경우, 중요한 공익에 대한 침해 또는 다수에 대한 회복 불가능한 피해가 야기될 수 있지만, 수사기관으로서는 그런 범죄에 대한 최초혐의 발견을 위한 내사나 수사 초기의 정보수집조차도 쉽지 않다.

요컨대 지속적으로 개발되고 있는 암호화기술에 기초하여 폐쇄성과 익명성을 특징으로 하는 온라인 플랫폼에서 행해지는 다크넷 범죄에 대한 수사는 공중의 접근 가능성이나 공권력에 의한 진입 및 신원확인 가능성을 특징으로 하는 기존 사이버범죄에 대한 수사와 구분되는 독자적인 특징을 갖는다고 보아야 하고,[41] 다크넷 범죄의 형태로 행해지는 중대한 범죄에 대한 효과적인 형사소추를 위해 – 이미 부분적으로 도입된 잠입수사(신분비공개·위장수사)와 함께 – 온라인 수색의 도입이 엄격한 요건을 전제로 고려될 필요가 있다.[42]

41) 박웅신/이경렬(주 36), 234-235면; 윤지영(주 30), 49-50면; 이원상(주 36), 362면; 류부곤(주 36), 31-32면.

42) 대부분의 연구에 따르면 온라인 수색은 제한된 범죄영역에서만 정당화될 수 있다고 한다: 허황(주 28), 131면 및 류부곤(주 36), 49면: 통신감청 대상 범죄보다 제한된 범위의 범죄; 박웅신/이경렬(주 36), 241면: 다크넷 범죄 중 일부 범죄; 윤지영(주 30), 53-54면: 다크넷 범죄 중 디지털 성착취물 유통이나 마약·무기 거래; 이원상(주 36), 362면: 사이버범죄와 관련된 강력범죄; 이원상(주 30), 200면: 아동·청소년 대상 디지털 성범죄; 윤신명(주 29), 93면: 안보 위기를 야기하는 극히 중대한 범죄; 이와 달리 신중한 입장으로는 박희영(주 3), 180면 및 정대용, "디지털 증거 수집을 위한 온라인 수색의 허용가능성에 관한 연구", 『디지털포렌식연구』 통권 제20호, 한국디지털포렌식학회, 2018.12, 67, 73면. 한편, 일부 문헌에서 언급되고 있는 스마트폰 등 일부 단말기의 비밀번호(잠금장치) 해제의 어려움 및 그 제조업체의 비협조(윤지영(주 30), 47-48면; 윤신명(주 29), 91면)가 온라인 수색의 필요성을 정당화하는지는 의문이다. 왜냐하면, 이는 다크넷 범죄라는 기술적·사회적 현상과 다른 규범적 측면이 고려되어야 하기 때문이다. 피의자가 자기 단말기의 비밀번호를 수사기관에게 제공하지 않는 것은 헌법상 권리인 자기부죄거부특권과 진술거부권에 기초하는 것이다.

Ⅲ. 온라인 수색의 개념: 비밀성과 정보수집의 유형을 기준으로 한 이해

1. 온라인 수색의 일반적 이해

독일에서 온라인 수색은 일반적으로 처분 당사자 모르게, 즉 '비밀로' 그의 '정보기술 시스템에 접근'하여 '거기에 저장된 정보를 수집'하거나 '해당 시스템의 이용을 감시'하는 행위로 이해된다.[43] 소위 '광의의 온라인 수색'.[44] 이는 온라인 수색에 대한 독일의 규정들 및 BVerfG의 판결에 설시된 그에 대한 해석을 통해 알 수 있다. 우선 2008년의 온라인 수색 판결에 따르면 IT-기본권으로 보호되어야 하는 비밀성 보장의 대상은 시스템에 저장된 정보 이외에 정보처리과정에서 생성되는 정보도 포함되며,[45] 심사 대상인 (舊) 2006 VSG NRW 제5조 제2항 제11호 후단에 따른 기술적 비밀접근은 대상 시스템에 저장된 정보의 실시간 수집뿐만 아니라 그 이용의 장기간 감시도 가능하게 한다.[46] 이어서 2016년의 BKAG 판결에 따르면 심사대상이었던 (舊) 2008 BKAG 제20조k 제1항[47]에 따른 온라인 수색을 통해 컴퓨터나 클라우드에 남겨진 정보가 수집되거나 네트워크에서의 당사자 행위가 재구성될 수 있다.[48] 독일 의회는 2017년에 BKAG 판결의 취지에 따라 앞 규정의 문언을 그대로 유지하면서 2017 BKAG 제49조[49]에 국제테

43) 박희영(주 3), 154면; 허황(주 28), 101면.
44) 김재희/박희영(주 27), 17면.
45) *BVerfGE* 120, 274, 314 f. [Rn. 205].
46) *BVerfGE* 120, 274, 323-325 [Rn. 234-237].
47) (舊) 2008 BKAG 제20조k [정보기술시스템에의 비밀침입(Verdeckter Eingriff in informationstechnische Systeme)] ① 다음 각호에 대한 위험이 존재한다는 것이 특정한 사실관계에 의해 정당화되는 경우, BKA는 (처분) 당사자가 알지 못하게 그에 의해 이용되는 정보기술시스템에 침입하여 거기에서 정보를 수집할 수 있다: 1. 사람의 신체·생명·자유, 2. 연방이나 주의 기초나 존립 또는 인간존재의 기초에 영향을 미치는 위협의 대상으로서 공익. 제1문의 처분은 해당 처분이 없다면 가까운 미래에 어떤 침해가 발생한다는 것이 충분한 개연성으로 확인되지 않는 경우에도, 특정한 사실관계가 구체적인 사안에서 제1문에 열거된 법익에 대한 특정인에 의한 긴박한 위험을 드러낸다면 허용된다. 제1문의 처분은 제4조a의 임무수행을 위해 필요하고 그 이외에는 해당 임무수행이 가망이 없거나 현저히 곤란한 경우에만 집행될 수 있다.
② 내지 ⑦ [생략]
48) *BVerfGE* 141, 220, 303 f. [Rn. 209 f.].
49) 2017 BKAG 제49조 [정보기술시스템에의 비밀침입(Verdeckter Eingriff in informationstechnische

러의 위험방지를 목적으로 하는 온라인 수색을 입법하였고, 이를 모범으로 하여 StPO 제100조b[50]에 수사목적의 온라인 수색을 입법하였다. 이때 후자의 입법이유서에 따르면, 온라인 수색은 정보기술시스템의 이용을 감시하고 거기에 저장된 내용을 기록할 목적으로 타인의 그 시스템에 비밀로 접근하는 것을 의미한다.[51]

2. 온라인 수색과 비밀성

앞의 이해에 따를 때, 온라인 수색의 개념을 정함에 있어서 1차적으로 기준이 되는 것은 그 집행의 '비밀성'이다. 즉 온라인 수색은 처분 당사자인 처분의 대상이 된 정보기술시스템의 소유자나 점유자 모르게 집행되어야 한다. 따라서 수사기관이 일반 압수수색의 영장을 집행하면서 현장에서 발견된 스마트폰이나 PC를 수색 대상자 앞에서 수색하는 행위 및 발견된 스마트폰 등을 통해 수색 대상자가 이용하는 외부의 서버나 클라우드에 접속하여 수색을 확대하는 행위는 온라인 수색의 개념에 포함되지 않는다. 전자는 오늘날 정보기술 환경에서 일반적인 압수수색의 전형적인 집행방법 중 하나일 뿐이다. 후자는 소위 '원격 압수수색'으로서 일반적인 압수수색에서 그러한 집행방법이 적법한지가

Systeme)] ① 다음 각호에 대한 위험이 존재한다는 것이 특정한 사실관계에 의해 정당화되는 경우, BKA는 (처분) 당사자가 알지 못하게 그에 의해 이용되는 정보기술시스템에 침입하여 거기에서 정보를 수집할 수 있다: 1. 사람의 신체·생명·자유, 2. 연방이나 주의 기초나 존립 또는 인간존재의 기초에 영향을 미치는 위협의 대상으로서 공익. 제1문의 처분은 다음 각호의 경우에만 허용된다: 1. 가까운 미래에 제1문에 열거된 법익에 대한 침해가 최소한 그 유형에 따라 구체화된 방식으로 발생하는 것이 특정한 사실관계에 의해 정당화되는 경우, 2. 가까운 미래에 제1문에 열거된 법익이 침해될 것이라는 점에 대한 구체적인 개연성이 어떤 자의 개별적인 행위에 의해 이유 있는 경우. 제1문의 처분은 제5조의 임무수행을 위해 필요하고 그 이외에는 해당 임무수행이 가망이 없거나 현저히 곤란한 경우에만 집행될 수 있다.
② 내지 ⑧ [생략]

50) StPO 제100조b [온라인 수색(Online-Durchsuchung)] ① 다음 각호가 인정되는 경우에는 (처분) 당사자가 알지 못하더라도 기술적 수단으로 당사자에 의해 이용되는 정보기술시스템에 침입하여 (eingreifen) 거기에서 정보가 수집될 수 있다(온라인 수색): 1. 어떤 자가 정범이나 공범으로서 제2항에 열거된 특별히 중대한 범죄(besonders schwere Straftat)를 범하였다거나 가벌적 미수에서 동 범죄의 실행에 착수했다는 혐의가 특정한 사실관계에 비추어 이유 있고, 2. 해당 범죄행위가 개별적인 경우에도 특별히 중대하다고(besonders schwer) 평가되며, 3. 사실관계의 조사나 공동피의자 거주지의 수사가 다른 방법으로는 지나치게 곤란하거나 가망이 없는 경우.
② 내지 ⑤ [생략]

51) BT-Drs. 18/12785, S. 54 am Anfang.

문제될 수 있으나, 어쨌든 당사자가 알게 행해진다는 점에서 온라인 수색은 아니다. 현재 독일 법제에서 원격 압수수색의 법적 근거는 공개의 압수수색만을 정당화하는 StPO 제100조 제3항 제1문((現) 제2문)[52]이며, 이 규정은 CCC 제19조[53] 제2항의 내용이 2007년의 개정(TKÜG)을 통해 입법화된 것이다.[54] 이런 이유로 독일의 통설과 판례에 따르면 StPO 제100조 제3항은 비밀의 수사처분인 온라인 수색의 법적 근거가 될 수 없다고 한다.[55] 한편 일부 문헌에서는 원격 압수수색을 "작은(kleine) 온라인 수색"이라

52) StPO 제110조 [서류와 정보저장매체의 열람(Durchsicht von Papieren und elektronischen Speichermedien)] ③ 수색 당사자의 정보저장매체에 대한 열람도 제1, 2항의 기준에 따라 허용된다. 이 열람은 해당 저장매체와 공간적으로 떨어져 있지만 그것으로부터 접근될 수 있는 저장매체에까지도 확대될 수 있다; 단, 그렇지 않으면 찾고 있는 데이터의 상실이 우려되는 경우이어야 한다. 수사에 중요할 수 있는 데이터는 확보될 수 있다.

53) CCC 제19조 [저장된 컴퓨터데이터의 수색과 압수(Search and seizure of stored computer data)] ① 각 협약국은 자국의 영토 내에서 다음 각호를 수색하거나 이에 준하는 방법으로 거기에 접속할 권한을 자국의 관할관청에게 부여하기 위한 입법적 조치 및 그 밖의 조치를 취한다: a. 컴퓨터시스템이나 그 일부 및 거기에 저장된 컴퓨터데이터, b. 컴퓨터데이터가 저장될 수 있는 컴퓨터데이터 저장매체.
② (관할)관청이 제1항 a호에 따라 특정한 컴퓨터시스템이나 그 일부를 수색하거나 이에 준하는 방법으로 거기에 접속하여, 찾고 있는 데이터가 해당 협약국의 영토 내의 다른 컴퓨터시스템이나 그 일부에 저장되어 있으며, 해당 데이터가 첫 번째 (컴퓨터)시스템으로부터 적법하게 접속되거나 이용될 수 있다고 추정할 만한 이유가 있는 경우에, 각 협약국은 그 (관할)관청이 수색 또는 이에 준하는 접속을 다른 시스템으로 신속하게 확대할 수 있도록 하기 위한 입법적 조치 및 그 밖의 조치를 취한다.
③ 내지 ⑤ [생략]

54) 반면 우리 형사소송법(이하 "형소법")에는 원격 압수수색을 명확히 포섭할 수 있는 규정이 없다. 다만 대법원은 그러한 집행방법이 법관의 영장 및 형소법 제120조 제1항을 통해 정당화될 수 있다고 한다(대법원 2017.11.29. 2017도9747: "피의자의 이메일 계정에 대한 접근권한에 갈음하여 발부받은 압수·수색영장에 따라 원격지의 저장매체에 적법하게 접속하여 내려받거나 현출된 전자정보를 대상으로 하여 범죄 혐의사실과 관련된 부분에 대하여 압수·수색하는 것은, …… 허용되며, 형소법 제120조 제1항에서 정한 압수·수색영장의 집행에 필요한 처분에 해당한다고 할 것이다. 그리고 이러한 법리는 원격지의 저장매체가 국외에 있는 경우라 하더라도 그 사정만으로 달리 볼 것은 아니다.").

55) BT-Drs. 16/6979, S. 45 am Anfang: 공개 수색이라는 처분의 성격; *Brodowski*, JR 2009, 402, 408; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122 [Tz. a)]; *Köhler* in M-G/*Schmitt*, StPO, § 110 Rn. 6; *Michalke*, StraFo 3/2014, 89, 92; *Wicker*, MMR 2013, 765, 766 [Tz. Ⅲ.]; *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15 u. § 110 Rn. 10. 다만, 외부의 서버나 클라우드가 외국에 위치하는 경우에는 소위 '역외 압수수색'의 허용성이 문제된다. CCC 제19조 제2항의 문언("협약국의 영토 내의")에 따르면 동 규정에 의해서는 역외 압수수색이 정당화되지 않으며(Explanatory Report, Nr. 195), StPO는 주권에 따른 제한으로 독일 내에서만 효력이 있다. 하지만 현실에서 많은 경우 기업이나 ISP의 서버나 클라우드는 외국에 소재한다. 이에 대한 자세한 설명은 지면상

칭했었지만,[56] 2017년의 개정으로 StPO 제100조b가 '온라인 수색'이라는 표제어를 통해 신설된 이후 그런 용어의 사용은 더 이상 타당하지 않아 보인다. 왜냐하면 현재 온라인 수색은 최소한 개념적으로 비밀성을 전제로 한 것이기 때문이다.

이 비밀성이 바로 온라인 수색의 가장 중요한 특징이다. 즉 비밀성 때문에 온라인 수색은 정보기술시스템에 대한 일반적인 압수수색보다 기본권을 훨씬 더 중대하게 침해한다고 평가되며, 그 결과 법치국가 원칙과 비례성 원칙에 따라 법적으로 더 엄격하게 규제되어야 한다.

3. 온라인 수색에서 허용될 수 있는 정보수집의 유형

온라인 수색은 그 개념상 부수처분과 주처분으로 구분된다. 부수처분이란 온라인 수색의 대상이 되는 정보기술시스템에 접근하여 감시소프트웨어[57]를 설치·제거하는 행위로서 주처분의 준비행위에 해당하는 반면, 주처분이란 대상 시스템에서 데이터를 수집하거나 그 이용을 감시하는 행위로서 온라인 수색의 집행행위에 해당한다.[58] 부수처분에서는 대상 시스템에 접근하거나 감시소프트웨어를 설치하는 방법에 따라 침해되는 기본권과 그 허용성이 다를 것이지만, 비례성 원칙과 영장주의를 고려할 때 부수처분에 의한 기본권 침해강도가 주처분의 그것을 초과해서는 안 될 것이다. 만약 부수처분이 주처분보다 강력하게 또는 주처분과 전혀 다른 기본권을 침해한다면, 이는 더 이상 부수처분이 아니며 그것을 위해서는 별도의 법적 근거 및 영장이 요구된다.[59] 반면 주처분의 집행방

생략한다.

56) *Gaede*, StV 2009, 96, 101; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122 [Tz. a)]; *Michalke*, StraFo 3/2014, 89, 91; *Zimmermann*, JA 5/2014, 321, 322 [Fn. 23].

57) 감시소프트웨어 중 대상 시스템에의 접근을 가능하게 하는 프로그램을 속칭 '국가트로이목마(Staatstrojaner)'라 하고, 장기간 감시를 가능하게 하는 프로그램을 원격 포렌식 소프트웨어(Remote Forensic Software)라고 한다(*Derin/Golla*, NJW 2019, 1111).

58) 이에 대한 자세한 설명은 김재희/박희영(주 27), 6면 이하 참고.

59) 감시소프트웨어 설치 방법으로는 백도어(back door)를 이용하는 방법, 물리적인 접근방법, 원격의 접근방법이 고려될 수 있다(박희영, "암호통신감청 및 온라인수색에서 부수처분의 허용과 한계", 『형사정책연구』 제30권 제2호, 한국형사법무정책연구원, 2019.6, 1, 8면 이하). 하지만 독일의 온라인 수색 수권규정들에는 감시소프트웨어 설치 방법에 대해 아무런 언급이 없다. 다만 StPO 제100조b 제1항 제1문– 및 제100조a 제1항 제2문 –의 문언("기술적 수단으로[mit technischen Mitteln]") 때문에 수사상 온라인 수색에서는 부수처분이 주거의 불가침을 침해하는 방식으로 행해

법은 구체화될 필요가 있다. 왜냐하면 온라인 수색의 수권규정 형성에 전제가 되는 그 기본권 침해강도는 주처분에 속하는 개별적인 정보수집의 유형 및 수집되는 정보의 양과 질(다양성)에 좌우될 것이기 때문이다. 주처분은 그 개념에 따라 크게 2가지 유형으로 구분된다: '정보기술시스템에 저장된 정보의 수집' 및 '시스템 이용자의 사용행위에 대한 감시'.

첫 번째 유형인 대상 시스템에 저장된 정보의 수집은 온라인 수색의 가장 전형적인 집행방법이며,[60] 여기에는 앞에서 언급된 원격 압수수색이 비밀리에 행해지는 경우, 즉 대상 시스템에서 그것과 네트워크로 연결된 외부의 컴퓨터(예를 들어, ISP의 서버나 클라우드)에 비밀리에 접근하여 정보를 수집하는 것도 포함된다.[61] 한편 '통신원감청(Quellen-TKÜ)'[62]이 본 유형에 포함되는지가 문제된다. 통신원감청은 암호화 기술의 발달로 전송 중인 통신을 대상으로 하는 기존의 통신감청이 무력해지자 이에 대처하기 위해 송신자나 수신자의 통신기기에서 암호화나 복호화 과정 중에 있는, 즉 암호화되어 있지 않은 통신내용을 수집하는 행위이다. 그 개념에서 알 수 있듯이 통신원감청은 기술적으로 집행방법의 측면에서 온라인 수색과 구분되지 않지만, 통신감청을 대체하기 위한 처분이라는 점에서 그 대상이 – 영장 발부 시점 이후에 전송된 – 통신내용으로 제한된다. 이런 이유로 독일 의회는 2017년의 StPO 개정에서 온라인 수색과 함께 통신원감청도 도입하였지만, 그것을 – 온라인 수색이 아닌 – 통신감청의 한 유형으로 정당화시켰다.[63]

질 수는 없고(*Köhler* in M-G/Schmitt, § 100a Rn. 14d; *Roggan*, StV 2017, 821, 822; *Singelnstein/Derin*, NJW 2017, 2646, 2647 m.w.N.), 기술적 수단이나 수사상 간계를 통해서만 행해질 수 있다고 한다(BT-Drs. 18/12785, S. 52; *Roggan*, a.a.O.; *Singelnstein/Derin*, a.a.O.). 한편 2017년의 StPO 개정의 입법이유서에 따르면 백도어를 이용한 감시소프트웨어의 설치는 허용되지 않는다고 하며(BT-Drs. 18/12785, S. 48 f.), 한 유력한 견해에 따르면, 원격의 접근방법 중에서 IT-보안취약점을 이용한 접근도 정보기술시스템의 보안과 관련된 국가의 보호의무를 고려할 때 타당하지 않다고 한다(*Blechschmitt*, MMR 2018, 361, 365; 박희영, 앞의 논문, 23-24면).

60) 이때 삭제된 정보의 수집이 문제될 수 있다. 이용자의 단순 삭제 후 '휴지통'에 아직 존재하는 정보는 온라인 수색의 대상이라 할 것이나, 완전 삭제되어 그 수집을 위해서는 특수한 복구프로그램을 이용해야 하는 경우라면 온라인 수색의 범위를 벗어난 것이다(김재희/박희영(주 27), 93면).

61) *BVerfGE* 120, 274, 314 [Rn. 203] u. 324 [Rn. 235]; *BVerfGE* 141, 220, 303 f. [Rn. 209 f.]. 이때 역외 압수수색이 허용되는가가 문제되는데, 이에 대한 논의는 지면상 생략한다.

62) 통신원감청이란 통신내용이 통신의 출처(Quellen)인 통신기기에서 암호화되기 전이나 복호화된 후에 감청(TKÜ)된다는 의미이다. 문헌에 따라 '암호통신감청'(박희영(주 28)) 또는 '소스통신감청'(허황(주 28))으로 번역된다.

63) 통신감청은 일반적으로 ISP의 협력을 통해 집행되지만, 통신원감청은 수사기관이 독자적으로 집행

StPO 제100조a 제1항 제2, 3문 및 제5, 6항.[64] 따라서 독일에서 통신원감청은 통신감청의 기능적 등가물(funktionale Äquivalenz)로 여겨진다.[65] 이에 반해, 영국 법원은 수사기관이 온라인 수색 영장을 통해 마약거래 등 범죄에 이용된 암호통신네트워크에 비밀리에 침입하여 범죄 관련 정보를 수집한 EncroChat 사건에서 송신기와 발신기에서 암호화·복호화 과정에 있는 정보는– 전송 중이 아닌 – 저장되어 있는 정보이기에 – 통신감청이 아닌 – 온라인 수색의 대상이 된다고 판결하였다.[66] 온라인 수색과 통신감청은 명확히 구분되는 처분이고 통신원감청은 암호화기술을 회피하기 위한 통신감청의 대체물이라는 점에서, 독일과 같이 통신원감청과 온라인 수색은 개념상 구분된다고 보는 것이 타당하고, 통신원감청은 통신감청으로 수집될 수 있는 정보만을 그 대상으로 해야 한

한다. 이점과 통신원감청이 집행방법의 측면에서 온라인 수색과 차이가 없다는 점을 모두 고려할 때, 통신원감청에 대한 절차법적 안전장치는 일반적인 통신감청보다는 온라인 수색에 대한 그것과 동일해야 할 것이다.

64) StPO 제100조a [전기통신감청(Telekommunikationsüberwachung)] ① 다음의 경우가 인정되는 경우에는 당사자가 알지 못하더라도 전기통신을 감청·기록(녹음)할 수 있다: 1. 어떤 자가 정범이나 공범으로서 제2항에 열거된 중대한 범죄(schwere Straftat)를 범하였다는 혐의, 가벌적 미수에서 동 (중대한) 범죄의 실행에 착수했다는 혐의, 또는 다른 범죄행위를 통해서 이 (중대한) 범죄를 예비하였다는 혐의가 특정한 사실관계에 비추어 이유 있고, 2. 그 범죄행위가 개별적인 경우에도 중대하다고 평가되며, 3. 사실관계의 조사나 피의자 거주지의 수사가 다른 방법으로는 가망이 없거나 현저히 곤란한 경우. (제1항의) 전기통신의 감청·기록은, 특히 암호화되지 않은 방식으로(in unverschlüsselter Form) 감청·기록을 가능하게 하기 위해, 필요한 경우에는 기술적 수단으로 당사자에 의해 이용되는 정보기술시스템에 침입하는 방식으로도 행해질 수 있다. 당사자의 정보기술시스템에 저장된 통신의 내용과 상황이 공공 전기통신망에서 진행 중인 전송과정 동안에도 암호화된 방식으로 감청되고 기록될 수 있다면 감청되고 기록될 수 있다.

② 내지 ④ [생략]

⑤ 제1항 제2, 3문에 따른 처분에서는 다음 사항이 기술적으로 확보되어야 한다: 1. 다음 사항만이 감청되고 기록될 수 있다는 점: a) 진행 중인 전기통신(제1항 제2문)이나, b) 제100조e 제1항에 따른 명령 시점부터 공공 전기통신망에서 진행 중인 전송과정 동안에도 감청되고 기록될 수 있는 통신의 내용과 상황(제1항 제3문), 2. 정보기술시스템에서 정보수집을 위해 불가피한 변경(만이 행해진다는 점, 3. (제2호에 따라) 행해진 변경이 처분의 종료 시에, 기술적으로 가능하다면, 자동적으로 복귀된다는 점. 투입된 수단은 기술수준에 따라 무권한 이용으로부터 보호되어야 한다. 복제된 정보는 기술수준에 따라 변경, 무권한 삭제, 무권한 인식으로부터 보호되어야 한다.

⑥ 매 기술적 수단의 투입에 있어서 다음 사항이 기록되어야 한다: 1. 기술적 수단의 명칭과 투입된 시점, 2. 정보기술시스템의 식별정보와 거기에서 행해진 일시적이지 않은 변경, 3. 수집된 정보의 확인을 가능하게 하는 정보, 4. 처분을 집행하는 조직단위.

65) BT-Drs. 18/12785, S. 50 f. 한편 *Sieber* 교수는 '통신원감청'을 '작은 온라인-수색'이라 칭한다 (*Sieber*, 69. DJT 2012, C 105).

66) 김재희/박희영(주 27), 80 및 83면.

다. 또한 통신원감청만이 필요한 사안에서 수사기관이 통신감청의 수권규정보다 더 엄격한 (또는 엄격하게 형성될) 온라인 수색의 수권규정에 따라야 한다면, 이것은 효과적인 형사소추의 이익에 반하다고 할 것이다. 다만, 통신원감청과 온라인 수색은 기술적으로 동일한 방식으로 집행되기에 통신원감청이 집행 중에 – 더 중대한 처분인 – 온라인 수색이 되지 않도록 기술적으로 보장하는 것이 의문시된다면, 통신원감청을 통신감청의 수권규정에 따라 허용하는 것은 타당하지 않을 수 있다.[67]

두 번째 유형인 시스템 이용자의 그 사용행위에 대한 감시에서 사용행위의 예로는 우선 처분 대상자가 시스템에서 행하는 이메일이나 메신저 작성행위, 문서소프트웨어을 이용한 문서 작성행위, 온라인 포탈에서의 검색행위나 콘텐츠 이용행위, 인터넷뱅킹 등의 금융거래행위, 위치정보가 연동된 애플리케이션 이용행위 등이 생각될 수 있다. 이외에 수사기관은 시스템 사용행위를 감시하면서 키로깅(key logging)이나 스크린샷(screen shot)을 통해 대상 시스템의 PW(잠금장치)뿐만 아니라 이용자의 서비스 계정의 ID와 PW(접속보안코드)도 획득할 수 있다.[68] 여기서 문제되는 것은 수사기관이 온라인 수색을 통해 획득한 처분 대상자의 서비스 계정의 ID와 PW를 가지고 대상 시스템이 아닌 자기의 정보기술시스템에서 그 계정에 접속하여 정보를 수집하는 것이 허용되는지 및 이런 집행방법도 온라인 수색의 개념에 속하는지이다. 한 문헌에 따르면 현재 우리나라 실무에서 이러한 수사방법이 활용되고 있다고 한다.[69] 우선 이러한 방식의 정보수집은 더 이상 처분 대상 시스템으로부터 정보를 수집하는 것이 아니므로, 개념상 온라인 수색에 속하지 않으며, IT-기본권에 대한 침해도 아니다. 나아가 온라인 수색은 대상 시스템에 설치된 감시소프트웨어를 통한 기술적 통제 및 사전·사후의 법원에 의한 통제에 의해 정당화되는 것인데, 위와 같은 정보수집은 대상 시스템을 벗어나서 행해지는 것으로서

67) *BVerfGE* 120, 274, 309 [Rn. 190]: 통신원감청이 온라인 수색이 되지 않는다는 점이 기술적 안전장치와 법적 기준을 통해 확보되어야 한다. 이런 점에서 현재 통신원감청을 합법화시킨 독일의 수권규정(StPO 제100조a 제1항 제2, 3문)에 대해서는 그 합헌성에 의문이 있다. 물론 동 규정의 제5항 제2, 3문은 "기술수준에 따라(nach dem Stand der Technik)"라는 문언으로 최신의 기술적 조치를 취할 것을 요구하지만, 이것이 통신원감청이 온라인 수색이 되지 못하도록 보장한다는 의미는 아니다. 아직 감시소프트웨어 중에서 그런 제한이 가능하다는 보고는 없다.

68) *BVerfGE* 120, 274, 324 [Rn. 236]; 김재희/박희영(주 27), 11면.

69) 정대용/김기범/권헌영/이상진, "디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 – 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로", 『법조』 통권 제720호, 2016.12, 법조협회, 133, 146면.

그에 대한 통제의 흠결로 오남용의 위험성이 크다. 따라서 위와 같은 집행방법이 허용되기 위해서는 온라인 수색과 별개로 수사기관이 이용할 정보기술시스템의 명칭과 접속될 계정의 명칭 및 접속 시작과 종료의 시점, 접속 횟수와 기간, 획득된 정보 등이 기재된 별도의 영장 및 이에 대한 법원의 사후 통제가 필요하다고 할 것이다. 다만 그 법적 근거로서 공개의 집행을 전제로 하는 압수수색 일반규정이 고려될 수는 없다.[70]

4. 소결

지금까지 검토한 바를 토대로 한다면, 온라인 수색이란 기본적으로 처분 대상자 모르게 그의 '정보기술시스템에 접근하여 감시소프트웨어를 설치'한 후 '거기에 저장된 정보를 수집'하거나 '해당 시스템의 이용을 감시'하는 행위를 의미하며, 정보수집 행위는 대상 시스템으로부터 외부의 컴퓨터까지 확대될 수 있고, 감시행위를 통해 처분 대상자가 입력한 문자, 특히 ID와 PW가 수집될 수 있다. 이때 장기간 행해지는 온라인 수색은 사실상 통신감청을 포함하는 처분이 될 것이다. 하지만 앞에서 검토하였듯이 통신원감청은 온라인 수색이 아닌 통신감청에 속한다고 해야 하고, 수사기관이 온라인 수색을 통해 획득된 처분 당사자의 서비스 계정 ID와 PW를 가지고 자신의 정보기술시스템에서 정보를 수집하는 것은 온라인 수색의 개념에 속하지 않는다고 보아야 한다.

온라인 수색의 개념을 위와 같이 이해하고, 일상의 생활영역에서 PC와 스마트폰 및 메신저나 이메일의 이용이 필수적인 오늘날의 정보기술 환경을 고려한다면, 온라인 수색은 인격탐구를 상당한 정도로 가능하게 한다. 이때 온라인 수색의 기본권 침해성을 특별히 증대시키는 가장 중요한 요인은 바로 그 집행의 비밀성이다. 온라인 수색 판결에 따르면 "기술적 비밀침입이 정보기술시스템 이용의 장기간 감시와 (거기에 저장된) 정보의

70) 이러한 처분은 사실상 통신감청이나 패킷감청과 동일한 효과를 야기한다는 점에서 일반적인 압수수색이라 보기 힘들다. 물론 위 처분을 일반적인 압수수색의 한 집행방법이라고 보면서 형소법 제107조 제3항 단서와 제122조 단서에 따라 처분 당사자에 대한 통지를 생략할 수 있다고 해석할 수도 있지만, 이는 해당 처분의 강력한 기본권 침해성을 고려할 때 법치국가 원칙과 비례성 원칙에 반하는 해석이다. 동일한 고민 아래 최근 해당 처분을 통신감청에 준하는 처분으로 취급하는 독일의 입법태도를 참고할 필요가 있다. 이에 대한 자세한 설명은 박중욱, "제3자 보관 정보의 압수수색 과정보주체에 대한 통지 – 강제처분의 공개성/비밀성에 대한 독일 논의를 참고하여 –", 『원광법학』 제38권 제3호, 원광대학교 법학연구소, 2022.9, 51면 참고.

실시간 수집을 가능하게 하는 경우, 기본권 침해의 비중은 특별히 중대하다. 이러한 유형의 (비밀)접근을 통해 획득될 수 있는 데이터베이스(에 있는 정보)의 범위와 다양성은 1회의 개별적인 정보수집의 경우보다 훨씬 크다. …… 본 (비밀)접근의 침해강도는 그 비밀성에 의해서도 정해진다. 법치국가에서 국가기관의 침해처분의 비밀성은 예외적인 것이며, (이를 위해서는) 특별한 정당화가 필요하다."[71]

요컨대 온라인 수색은 테러나 디지털 성착취와 같은 중대한 범죄 및 다크넷 범죄에 대한 효과적인 형사법적 대응의 측면에서 보면 필요하고 적합한 수단이지만, 그에 의해 야기될 수 있는 인격의 본질적인 부분에 대한 침해 가능성을 고려한다면 그 적용영역은 엄격히 제한되어야 할 것이고 그에 대한 절차법적 통제는 충분히 효과적이어야 할 것이다. 온라인 수색의 정당화는 비례성 원칙에 따른 그 수권규정의 법적 형성에 달려 있다. 이때 특히 동 처분은 예외적인 비밀의 수사처분이라는 점에서 그로 인한 과도한 기본권 침해의 방지를 보장할 수 있을 정도의 절차법적 안전장치가 요구된다.[72]

Ⅳ. 독일 연방헌법재판소 판결에 따른 온라인 수색의 허용요건

1. 2008년의 온라인 수색 판결

가. 처분요건과 절차법적 안전장치

온라인 수색 판결에서 BVerfG는 IT-기본권 또한 예방과 수사를 위해 제한될 수 있다고 전제한 후, 온라인 수색은 비례성 원칙에 따를 때 국가의 기반·존립과 같은 국가의 안전 및 생명·신체·자유와 같은 개인의 안전을 보장하기 위해 적합하고 필요한 수단이지만,[73] 그 수권규정에는 협의의 비례성 원칙(전체적 이익형량)에 따라 그것의 강력한

71) *BVerfGE* 120, 274, 323-325 [Rn. 234-238]. 처분 당사자가 국가의 처분을 그 집행 전에 아는 경우, 그는 처음부터 법적으로 처분의 위법성을 다툴 수 있고, 실질적으로 처분의 진행을 감독할 수 있다.

72) 이원상(주 30), 200면: "초점은 온라인수색이 폭주하지 않고 목적을 이룰 수 있도록 균형 있게 설계되고, 감시·통제할 수 있는 충분한 장치를 고려하여 규정하는 것으로 옮겨진다."

73) *BVerfGE* 120, 274, 315-321 [Rn. 207-225].

기본권 침해강도를 상쇄할 수 있는 처분요건 및 절차법적 안전장치가 형성될 것을 요구한다.[74] 우선 처분요건으로는 '매우 중요한 법익(überragend wichtige Rechtsgüter)에 대한 구체적인 위험/혐의(konkrete(r) Gefahr/Tatverdcht)가 존재한다는 점이 최소한 실질적인 근거(tatsächliche Anhaltspunkte)로 이유 있을 것'이 요구되며, 국가의 기반·존립과 같은 국가의 안전과 생명·신체·자유와 같은 개인의 안전 및 공적 연금제도의 핵심기능 등이 그러한 법익으로 고려될 수 있다.[75] 다음으로 절차법적 안전장치는 처분 당사자의 이익을 보장하기에 적합한 '법적 안전장치(gesetzliche Vorkehrungen)'이어야 하는데, 이런 안전장치로는 특히 법관유보(영장주의), 즉 독립된 기관에 의한 예방적 통제가 요구된다. 이와 관련하여 법관은 처분 명령서에 그 적법성을 자세히 심사한 후 처분의 이유까지 명확히 밝힐 필요가 있다.[76]

나. 사적 생활형성의 핵심영역 보호를 위한 절차법적 안전장치

이어서 BVerfG는 온라인 수색의 대상이 되는 정보기술시스템에는 불가침의 '사적 생활형성의 핵심영역(Kernbereich privater Lebensgestaltung)'[77]에 속할 수 있는 개인정보가 존재할 가능성이 높고, 거기에 비밀로 접근하여 정보를 포괄적으로 획득하는 것은 다른 (비밀의) 감시처분에 비하여 위 핵심영역에 속하는 정보가 수집될 위험이 높으므로, 이에 대처하기 위한 특별한 절차법적 안전장치가 필요하다는 점을 강조한다.[78] 그리고 이를 위해 온라인 수색의 수권규정에는 핵심영역과 관련된 정보가 가능한 한 처분 집행

74) *BVerfGE* 120, 274, 321 ff. [Rn. 207 ff.].
75) *BVerfGE* 120, 274, 326 ff. [Rn. 243 ff.].
76) *BVerfGE* 120, 274, 331 f. [Rn. 257-259].
77) BVerfG는 독일연방공화국(Bundesrepublik Deutschland: BRD) 초기의 판결부터 지금까지 지속적으로 기본법(Grundgesetz: GG)의 '각 기본권 규정과 결부된 제1조 제1항'에 근거하여 시민에게는 '사적 생활형성의 불가침의 핵심영역', 즉 공권력으로부터 벗어나 절대적으로 보호되는 영역이 인정되고, 따라서 그러한 영역에 속하는 개인정보는 절대적으로 보호되어야 한다는 점을 강조한다(*BVerfGE* 6, 32, 41; 27, 1, 6; 80, 367, 373; 109, 279, 313; 113, 348, 390; 120, 274, 335; 124, 43, 69 m.w.N.). 사적 생활형성의 핵심영역 보호는 기본적으로 헌법적 차원의 인격권 보호의 한 내용이다. 다만 독일의 입법자는 2017년 개정에서 온라인 수색 판결과 BKAG 판결의 취지를 반영하여 StPO 제100조d를 신설함으로써 동 핵심영역 보호를 위한 처분의 집행 단계에서의 절차법적 조치를 구체적으로 규정되었다.
78) *BVerfGE* 120, 274, 335-337 [Rn. 271-275].

의 앞선 단계에서 보호되도록 보장하는 규정이 포함되어야 한다. 이와 관련하여 온라인 수색 판결에 따르면, 핵심영역 관련성 판단은 2단계로 구분될 필요가 있다: 소위 '2단계 보호구상(zweistufiges Schutzkonzept)'. 이에 따르면 핵심영역 관련성이 '정보의 수집 전이나 수집 중의 단계'에서 드러나는 경우라면 즉시 처분의 집행이 개시되지 않거나 중단되어야 하고(이미 수집된 정보는 폐기), '정보의 수집 후 열람(분석·활용)의 단계'에서 드러난 경우라면 즉시 해당 정보는 삭제되거나 사용이 배제되어야 한다.[79] 물론 BVerfG는 이러한 구상에서 첫 번째 단계에서 핵심영역 관련성이 드러나는 경우는 거의 없기 때문에 두 번째 단계에서의 보호가 중요하고, 바로 여기서 수집된 정보의 열람 과정에서 당사자의 이익이 충분히 고려될 수 있는 절차가 법적으로 형성될 것을 요구한다.[80] 이때 그러한 절차가 무엇을 의미하는지는 온라인 수색 판결에 명확히 드러나 있지 않지만, 동 판결이 참조한 BVerfG의 2004.3.3. 판결(소위 '주거감청 판결')[81]에 따르면 '법관유보'를 의미한다. 이에 대해서는 단락을 나눠 좀 더 자세히 검토할 필요가 있다.

주거감청(Akustische Wohnraumüberwachung)[82]이란 주거 내에서 비공개로 행해진 발언을 당사자 모르게 기술적 수단으로 감청·기록(녹음)하는 처분이다(StPO 제100조c 제1항).[83] 이 처분은 그 도입이 논의되던 당시 독일에서 가장 강력한 기본권 침해강도를 갖는 수사처분으로 평가되었고, 이 때문에 – 온라인 수색이 도입되던 시점에서와 같이 – 사적 생활형성의 핵심영역 보호가 문제되었다. 온라인 수색 판결에서 핵심영역 보호와 관련하여 자세히 설시된 앞 단락의 내용은 이미 주거감청 판결에서 자세히 설시

79) *BVerfGE* 120, 274, 337-339 [Rn. 276-283].

80) *BVerfGE* 120, 274, 339 [Rn. 283].

81) *BVerfGE* 109, 279 = NJW 2004, 999. 이 판결의 심사대상은 1998년의 개정(아래 각주 83 참고)으로 신설된 주거감청의 수권규정인 (舊) StPO 제100조c 제1항 제3호이다.

82) 주거감청은 독일에서 '대감청(Großer Lauschangriff)'이라고도 한다. 참고로 '소감청(Kleiner Lauschangriff)'은 StPO 제100조f에 규정된 '주거 외 감청(Akustische Überwachung außerhalb von Wohnraum)'을 의미한다. 주거 외 감청은 1992.7.15.의 불법마약거래·조직범죄퇴치법(OrgKG vom 15. Juli 1992, BGBl. I S. 1302, 1992.9.22. 발효)을 통해 (舊) 제100조c 제1항 제1문 제2호에 처음 도입되었다.

83) 주거감청은 1998.5.9.의 강화된 조직범죄퇴치법(OrgKVerb vom 4. Mai 1998, BGBl. I S. 845, 1998.5.9. 발효)을 통해 (舊) StPO 제100조c 제1항 제3호에 처음 도입되었다. 독일 의회는 StPO에 주거감청을 도입하기에 앞서 그 위헌성을 제거하고 헌법적 근거를 마련하기 위해 GG 제13조(주거의 불가침)에 제3항 내지 재6항을 새롭게 추가하였다(Gesetz zur Änderung des GG (Artikel 13) vom 26. März 1998, BGBl. I S. 610, 1998.4.1. 발효). 여기서 제3항은 수사목적 주거감청의 헌법적 근거이다.

되었던 내용이다.[84] 특히 BVerfG는 이 판결에서 사적 생활형성의 핵심영역 보호의 2단계 보호구상에서 가장 중요한 부분이라고 여겨지는 두 번째 단계에서의 열람된 정보의 핵심영역 관련성에 대한 판단을 형사소추관청 이외에 당사자의 이익도 고려하는 독립된 기관, 즉 법원도 내릴 수 있어야 한다고 설시하면서, 법원이 (수사절차 종료 후인) 공판준비절차가 돼서야 비로소 핵심영역 관련성 판단을 내릴 수 있도록 하는 것은, 관련성 판단이 실질적으로 사용가능성에 대한 판단이라는 점을 고려할 때, 핵심영역 보호와 모순되며, 수사과정에서 그 관련성이 명확하지 않다면 수사기관은 법원에 그에 대한 판단을 구할 의무가 있고, 입법자는 이런 내용을 법률에 명확히 규정해야 한다고 설시하였다.[85]

요컨대 원칙적으로 즉시 삭제되고 사용이 금지되어야 하는 핵심영역에 속하는 정보가 수사과정에서 발견된 경우, 수사기관은 실무상 – 거의 – 언제나 그 관련성을 부정할 것이기 때문에, 관련성의 종국적 판단권자인 법원이 수사절차의 종료 후가 아닌 수사절차 중에 그 판단을 위해 개입하는 것이 타당하고, 이때 법원의 개입은 사실상 수사기관의 청구에 달려 있기 때문에 법률을 통해 수사기관에게는 청구의무가 부과되어야 한다는 것이다.

2. 2016년의 BKAG 판결

가. 기존 판례의 확인

BKAG 판결의 심사대상은 앞에서 언급하였듯이 2008년의 개정을 통해 도입된 BKAG 제3절a에 속하는 여러 수사·감시처분의 수권규정이고, 여기에는 정보제출요구, 압수수색, 신원확인조치 등의 공개의 처분부터 온라인 수색, 통신감청, 주거감청과 주거 외 감청 등 비밀의 수사처분까지 포괄적으로 규정되어 있다. 하지만 동 판결에서 BVerfG는 사적 영역을 깊게 침해하는 처분, 즉 통신감청, 교신데이터 수집, 온라인 수

84) *BVerfGE* 109, 279, 311-324 [Rn. 113-152] und 328-335 [Rn. 169-196].

85) *BVerfGE* 109, 279, 333 f. [Rn. 190-194]. 한편 사적 생활형성의 핵심영역에 속하는 정보는 헌법상의 요청에 따라 – 법률상 규정이 없더라도 – 그 사용이 금지되고 삭제되어야 하지만, 그것을 보장할 절차법적 규제가 없어서 기본권 보호에 흠결이 발생하고 기본권을 위태롭게 한다면, 입법자는 헌법상 기준을 실현하기 위해 입법권을 행사할 수 있다(a.a.O. 334 f. [Rn. 195 f.]).

색, 주거감청 등을 위주로 헌법소원을 심사하였다. 이때 BVerfG는 협의의 비례성 심사를 함에 있어서 각 처분의 헌법적 허용요건을 심사한 기존의 판결들을 적극적으로 인용하여 설시하면서, 온라인 수색을 주거감청과 유사한 정도의 기본권 침해강도를 갖는 처분으로 평가하였다.[86)]

BVerfG는 이 판결에서도 특별히 강력한 침해강도의 감시처분(besonders eingriffsintensiven Überwachungsmaßnahmen)에 대해서는 사적 생활형성의 핵심영역에 대한 '특별한 보호'를 요구한다. 즉 핵심영역 보호는 모든 감시처분에서 요구되지만, 전형적으로 핵심영역과 관련된 정보를 수집하는 감시처분의 경우에는, 핵심영역을 효과적으로 보호하기 위한 독자적인 규정이 요구되며, BVerfG의 설시에 따르면 이러한 감시처분으로 통신감청, 주거감청, 온라인 수색이 있다.[87)] 다만 핵심영역 보호를 위한 절차법적 안전장치의 기본적인 내용인 2단계 보호구상은 위 주거감청 판결 및 온라인 수색 판결과 동일하지만, 핵심영역 관련성 판단과 관련하여 통신감청의 경우에는 그것이 반드시 외부의 독립된 기관에 의해 행해질 필요는 없지만, 주거감청과 온라인 수색은 그렇지 않다.[88)]

나. 비밀의 강제처분에 대한 추가의 안전장치

한편 BKAG 판결에서 BVerfG는 사적 영역을 깊게 침해하는 비밀의 (감시)수사처분, 즉 '비밀의 강제처분'에 대해서는 증대된 절차법적 안전장치가 요구된다고 하며 그 유형과 내용에 대해 자세히 설시한다. 이 부분의 내용은 BKAG 판결에서 처음 설시된 것이 아니라 2010년의 VDS 판결에서 처음 설시된 이후 2011년의 TKÜG 판결 및 2013년

86) *BVerfGE* 141, 220, 303 [Rn. 210 a.E.]: IT-기본권 침해의 비중은 주거의 불가침 침해의 그것과 유사하다.

87) *BVerfGE* 141, 220, 277 f. [Rn. 123].

88) *BVerfGE* 141, 220, 279 [Rn. 129]. 그 결과 BVerfG는 심사대상이자 온라인 수색의 수권규정이었던 (舊) BKAG 제20조k에서 사적 생활형성의 핵심영역의 보호를 위한 규정이었던 제7항은 위 요청을 부분적으로 충족하지 못한다고 판시하였다(a.a.O. 307 ff. [Rn. 221 ff.]). 특히 동 제7항 제3, 4문("획득된 정보는 제5문에 따라 명령한 법원의 지휘 아래 지체 없이 BKA의 정보보호관 및 법관 자격을 가진 1인을 포함한 2인의 BKA 공무원에 의해 핵심영역 관련 내용이 열람되어야 한다. 정보보호관은 이러한 행위를 집행할 때 독립적이며(weisungsfrei), 이로 인해 불이익을 받을 수 없다(BKAG 제4조f 제3항)")이 위헌이라고 지적되었다(a.a.O. 308 f. [Rn. 223-225]).

의 대테러데이터베이스법(Antiterrordateigesetz: ATDG) (부분)위헌 판결에서 재확인된 내용이다.

BVerfG의 판결에 따르면 시민의 개인정보가 국가에 의해 비밀로 수집되는 경우에는 (협의의) 비례성 원칙 및 기본권과 재판청구권에 근거하여 절차법적 안전장치로서 투명성, 개별적인 권리보호, 감독적 통제가 요구된다고 한다.[89] 우선 정보 수집·처리의 투명성 요청(Anforderung an Transparenz)에 따라 국가에 의한 정보의 취급은 민주적 담론과 결부되어야 하므로, 비밀로 행해지는 국가의 처분에서 당사자는 가능하다면 사후에라도 그 집행에 대해 통지받아야 하고 이에 기초하여 개별적인 권리보호의 기회를 가질 수 있어야 한다.[90] 즉, 투명성 요청에 따라 국가의 사적 영역을 깊게 침해하는 정보수집이 그 목적 달성을 위해 비밀로 행해지는 경우, 입법자는 기본권과 재판청구권의 보장을 위해 최소한 사후에는 처분 당사자가 그 집행에 대해 통지받도록 하는 '사후 통지(nachträgliche Benachrichtigung)'[91]에 관한 규정 및 통지받은 당사자가 합리적인 방식으로 처분에 대해 이의제기할 수 있는 '법원에 의한 적법성 통제(eine gerichtliche Rechtmäßigkeitskontrolle)'[92]에 관한 규정을 입법해야 한다. 이때 사후 통지는 헌법상 보호되는 제3자의 법익을 위해 이익형량에 따라 예외적으로 배제될 수 있지만, 이러한 예외는 무조건 필요한 경우로 제한되어야 하며, 형사소추와 관련하여 그러한 예로는 (사후) 통지로 인하여 처분의 목적이 무위가 되는 경우, 개인의 신체·생명에 대한 위험이

89) *BVerfGE* 141, 220, 282 [Rn. 134].

90) *BVerfGE* 141, 220, 282 [Rn. 135]. 이로써 처분 당사자는 국가감시의 막연한 위협에 대처할 수 있다(a.a.O.).

91) *BVerfGE* 141, 220, 282 f. [Rn. 136]. 비밀의 수사처분에 대한 사후 통지에 대해 VDS 판결에는 더 자세한 법리가 다음과 같이 기술되어 있다. 투명성 요청에 따라 국가에 의한 (사적 영역을 깊게 침해하는) 개인정보의 수집·이용은 공개가 원칙이고, 당사자 모르는 이용은 위험방지나 정보기관의 임무수행과 같이 그렇지 않으면 정보수집의 목적이 무위가 되는 경우에 원칙적으로 허용되지만, 형사상 압수수색의 경우에는 StPO에 따를 때 공개가 원칙이다(StPO 제33조 제3, 4항, 제106조). 따라서 당사자는 원칙적으로 처분에 앞서 통지를 받아야 하고, 정보의 비밀 이용은 개별적으로 필요하고 법관의 명령이 있는 경우에만 고려될 수 있다(*BVerfGE* 125, 260, 335 f. [Rn. 243]). 중대한 기본권 침해를 야기하는 수사처분에 대해서는 헌법상 독립된 기관에 의한 사전적 통제, 즉 법관유보가 요구되며, 이는 특히 해당 처분이 비밀로 행해지는 경우에 그렇다(a.a.O. 337 [Rn. 248]). 다만, 이러한 서술에서 StPO에 따른 압수수색 부분은 우리 법제와 일치하지 않을 수 있다. 왜냐하면 형소법 제106조 제4항, 제107조 제3항 단서, 제118조 단서, 제122조 단서에 따르면 압수수색이 당사자 모르게 집행될 수도 있기 때문이다.

92) *BVerfGE* 141, 220, 283 f. [Rn. 138]. 이 부분은 우리 법제의 준항고를 의미한다(형소법 제417조).

발생하는 경우, 통지가 (오히려) 당사자의 우월한 이익과 충돌하는 경우가 생각될 수 있다.[93] 다만, 이때 BVerfG는 사후 통지의 예외적인 배제의 이유가 명확히 존재함을 법관이 확인하고 일정한 간격으로 심사할 것을 요구한다.[94] 다음으로 '효과적인 감독적 통제(wirksame aufsichtliche Kontrolle)'란 입법부와 행정부 차원에서의 통제, 즉 수사(·정보)기관에 대한 의회의 통제와 기관 내의 통제를 의미한다. BVerfG의 설시에 따르면 사적 영역을 깊게 침해하는 비밀의 (감시)수사처분에서는 전술한 통지를 통한 개별적인 권리보호가 매우 제한적으로만 확보될 것이기에 감독적 통제에 더 큰 중요성이 부여된다.[95]

BVerfG는 이외에 사적 영역을 깊게 침해하는 비밀의 수사처분의 집행(현황)이 의회와 공중에게 정기적으로 보고되어 공개적 토론으로 이어짐으로써, 그것이 민주적 통제 아래 놓일 것을 요구한다.[96]

끝으로 BVerfG는 정보자기결정권 판결 이래로 국가에 의한 개인정보의 사용은 그 목적에 제한되고, 그 사용이 종료된 후에는 사용이 더 이상 불가능하도록 보장될 것을 강조한다. 따라서 사적 영역을 깊게 침해하는 비밀의 (감시)수사처분에서도 사용이 종료된 정보는 삭제되어야 하고, 이에 대한 투명성 보장을 위해 그것은 기록되어야 한다.[97]

3. 수사목적 온라인 수색의 수권규정: StPO 제100조b, d, e, 제101조, 제101조b[98]

우선 처분요건과 관련하여 가장 중요한 부분인 대상 범죄는 '특별히 중대한 범죄'로 제한되어 있고(StPO 제100조b 제1항 제1호), 그 범위는 제2항에 열거되어 있다: 소위 '범죄목록(Straftatenkatalog)'.[99] 목록에 열거된 범죄로는 내란·외환 등, 범죄단체·테러

93) *BVerfGE* 125, 260, 336 [Rn. 244]; 141, 220, 283 [Rn. 136].
94) *BVerfGE* 125, 260, 336 [Rn. 244]; 141, 220, 283 [Rn. 136 a.E.].
95) *BVerfGE* 133, 277, 366 f. [Rn. 207]; 141, 220, 282 u. 284 [Rn. 135 a.E. u. 140].
96) *BVerfGE* 141, 220, 285 [Rn. 142 f.].
97) *BVerfGE* 141, 220, 285 f. [Rn. 144].
98) 각 규정의 전체 내용은 독일법연구회(譯), 독일 형사소송법, 사법발전재단, 2018 참고.
99) 원칙적으로 모든 수사상 (강제)처분은 모든 유형의 범죄에 적용된다. 하지만 독일의 입법자는 새로운 유형의 수사처분이 그 강력한 기본권 침해성 때문에 문제될 때, 협의의 비례성 원칙에 근거하여 그 적용범죄를 대상 범죄의 제한을 통해 축소하고 있다. 이에 따라 현재 StPO의 강제처분 중 강력

단체 조직, 화폐·유가증권 위조, 아동 음란물 배포·취득·소지, 자금세탁, 증뢰·수뢰, 탈세, 난민법 및 외국인체류법 위반행위, 마약 유통·거래·수입, 전쟁무기통제법·국제형법(집단학살 등)·무기법 위반행위 등이 있다. 앞에서 검토한 온라인 수색의 강력한 기본권 침해성을 고려할 때, 증뢰·수뢰와 탈세 등의 범죄에까지 동 처분이 적용되어야 하는지는 의문이다.

다음으로 절차법적 안전장치와 관련하여 온라인 수색은 법원의 강력한 통제 아래 있다고 할 수 있다. 이는 기본적으로 BVerfG가 온라인 수색 판결과 BKAG 판결을 통해 요구한 사항들이다. 우선 사적 생활형성의 핵심영역 보호와 관련하여 BVerfG가 요구한 내용은 StPO 제100조d에 전부 반영되어 있다. 특히 2단계 보호구상에서 두 번째 단계에서의 핵심영역 관련성 판단에 대한 규제가 동조 제3항 제2, 3문에 명시되어 있다. 이어서 StPO 제100조e에 따르면 법원은 온라인 수색의 처분절차에 – 주거감청에서와 마찬가지로 – 다층적으로 개입한다. 즉 법원은 혐의의 근거가 되는 특정한 사실관계 및 처분의 필요성과 비례성에 관한 주요 고려사항이 기재된 명령서를 통해서만 온라인 수색을 명령할 수 있고(법관유보, 동조 제3, 4항), 수사기관은 그 집행의 종료 시에 처분의 결과뿐만 아니라 (집행)과정도 법원에 보고해야 한다(동조 제5항 제2, 3문). 이외에 사후

한 기본권 침해성을 가지는 특정 처분의 적용범위는 '범죄의 비중(중요성)(das Gewicht der Straftaten)'에 비례하여 3단계로 구분한다: 중요한 의미의 범죄(Straftaten von erheblicher Bedeutung), 중대한 범죄(schwere Straftaten), 특별히 중대한 범죄(besonders schwere Straftaten). '중요한 의미의 범죄'는 1992년의 OrgKG를 통해 처음 도입되었고(각주 82 참고), 최소한 중급의 범죄영역에 속하고, 법적 평화를 민감하게 교란하며, 법적 안정성에 대한 시민의 감정을 현저히 침해하기에 적합한 범죄를 의미한다(*BVerfGE* 103, 21, 34; 107, 299, 322; 109, 279, 344 [Rn. 228]; 112, 304, 305 f. [Rn. 48]; 124, 43, 64 [Rn. 73]; *LG Mannheim* StV 2001, 266; *Schmitt* in M-G/Schmitt, § 81g Rn. 7a). 동 개념에 대해서는 그 불명확성과 불특정성 때문에 일부에서 위헌의 우려가 제기되지만(*Rieß*, GA 2004, 623, 624), BVerfG는 동 개념의 사용이 헌법상 문제되지 않는다고 한다. 현재 StPO 제81조g(DNA-동일성 확인), 제98조a(자동화된 비교조사), 제100조h 제1항 제2호(기술적 수단의 투입), 제110조a(비밀수사관), 제163조f(장기감시) 등에서 사용되고 있다. '중대한 범죄'는 1968년에 StPO 제100조a에 통신감청이 신설되면서 도입된 개념이며(Gesetz zu Artikel 10 GG vom 13. August 1968, BGBl I S. 949), 통신감청의 강력한 기본권 침해성을 고려하여 그 적용범위를 열거된 범죄로 제한한다. 현재 통신감청 이외에 StPO 제100조f(주거 외 감청), 제100조g 제1항(실시간 교신데이터 수집), 제100조i(IMSI-Catcher) 등에서 사용되고 있다. '특별히 중대한 범죄'는 1998년에 주거감청이 신설될 때(각주 83 참고) StPO에 도입되었으며, 통신감청이나 주거 외 감청보다 더 강력한 주거감청의 기본권 침해성 때문에 그 대상이 되는 범죄가 더 제한적으로 열거되어 있다. 현재 이 개념은 주거감청 이외에 StPO 제100조b(온라인 수색), 제100조g 제2항(예방적 교신데이터 수집)의 규정에서만 사용되고 있다.

통지 및 법원의 적법성 통제에 대해서는 비밀의 처분에 대한 절차규정인 StPO 제101조가 그대로 적용된다. 사후 통지와 관련하여 가장 중요한 부분은 동 통지의 예외적인 유예와 배제의 사유 및 그 판단권자인데, 이것에 대해 BVerfG는 이미 주거감청 판결에서 자세히 설시하였고, 동 재판소의 요청사항은 StPO 제101조 제4항 내지 제6항에 기반영되어 있었다. 여기서 핵심이 되는 내용은 통지의 유예·배제 사유가 법률이 명확히 규정되어 있다는 점과, 최초의 통지유예는 수사기관의 판단에 의해 가능하지만 그 계속적 유예 및 최종적 배제를 위해서는 법원의 승인 필요하다는 점이다.

Ⅴ. 수사목적 온라인 수색의 도입을 위한 입법론적 검토사항

1. 개념 및 처분요건과 절차법적 안전장치

이미 언급하였듯이 현재 우리나라에서 온라인 수색의 개념은 독일에서의 같이 처분당사자 모르게 그의 '정보기술시스템에 접근'하여 '거기에 저장된 정보를 수집'하거나 '해당 시스템의 이용을 감시'하는 행위로 이해되고 있다. 이때 '정보기술시스템을 이용한 외부환경의 감시'도 온라인 수색의 주처분에 속하는 집행방법에 포함될 수 있는지 또는 그래야 하는지가 문제될 수 있다. 이러한 집행의 구체적인 예로는 수사기관이 대상 시스템에 내장된 카메라나 마이크 등을 작동시켜 그 시스템이 있는 장소(예를 들어, 주거, 사무실, 자동차 내)를 감시하거나 감청하는 것이다. 미국과 영국에서는 이러한 집행행위도 온라인 수색의 개념에 속한다고 본다: 소위 '최광의의 온라인 수색'.[100] 하지만 이러한 이해는 타당하지 않다고 생각된다. 오늘날의 정보기술 환경을 고려할 때 이러한 유형의 집행도 온라인 수색으로서 허용된다고 한다면, 온라인 수색의 영장(법관명령)은 사실상 거의 모든 유형의 처분이 비밀로 집행될 수 있게 하는 만능키가 될 것이기 때문이다. 온라인 수색의 수권규정을 통해 그것이 허용되는 범죄가 제한적일지라도 그러한 해석은 수사권의 과도한 확대이다. 정보통신 기술의 발전과 그것이 우리에게 끼치는 영향을 고려할 때 온라인 수색은 지속적으로 여러 유형의 처분으로 전용될 가능성이 매우

100) 김재희/박희영(주 27), 28 및 73면

높다. 기본권 보호와 효과적인 통제의 측면에서 온라인 수색의 개념을 제한적으로 볼 필요가 있다.[101]

온라인 수색의 처분요건과 관련해서는 비례성 원칙에 따라 최소한 통신제한조치(통신감청) 규정인 통비법 제5조 제1항의 요건보다 더 엄격해야 한다.[102] 무엇보다 대상 범죄의 목록이 매우 제한적이어야 한다. 현재 통신감청이 허용되는 범죄 중 형법상의 협박죄나 재산범죄, 군형법상의 지휘권 남용이나 항명 등의 죄 등에 온라인 수색이 사용되는 것은 과도하다고 할 것이다. 온라인 수색은 기본적으로 법익의 측면에서는 국가의 안전 및 생명·신체·자유 등 개인의 안전을 위해, 범죄 형태의 측면에서는 다크넷 범죄의 형태에 대한 대처로서만 사용되어야 한다.

절차법적 안전장치와 관련해서는 비밀성에 따른 처분 당사자의 자기 방어 기회의 박탈을 상쇄할 정도의 법적 보장책이 요구된다. 그리고 이 보장책은 앞의 BVerfG 판결들에서 보았듯이 독립된 기관인 법원의 다층적 개입으로 달성될 수 있다. 형사절차에서의 증거확보와 관련된 법리의 측면에서 볼 때 독일 법제의 사적 생활형성의 핵심영역 보호 및 형사절차에서의 핵심영역 관련성 있는 정보의 배제는 우리 법제의 무관정보의 배제 및 위법수집증거배제의 법칙에 상응한다고 볼 수 있다. 즉, – 독일의 통설과 판례에 따를 때 – 위법한 절차로 획득된 증거의 사용금지가 자명하지 않은 독일 법제에서도 사적 생활형성의 핵심 영역에 속하는 정보는 원칙적으로 증거사용금지로 이어지는데, 이는 우리 법제에서 사건과 관련성 없는 정보가 위법수집증거배제의 법칙에 따라 원칙적으로 그 사용이 배제되어야 한다는 점과 일치한다. 이런 점을 고려한다면, 온라인 수색으로 획득된 정보는 전부 그 집행의 종료 후 즉시 영장을 발부한 법관의 심사 아래 놓일 필요가 있다. 헌재 결정[103]과 2020.3.24.의 개정으로 신설된 통비법 제12조의2는 이미 패킷감청에 대해 이러한 통제를 가능하도록 하고 있다. 한편 비밀의 수사처분에서 기본권 및 재판청구권에 기초한 주관적인 권리보호(준항고)의 실효적인 보장을 위해서는 그 전제가 되는 사후 통지가 너무 늦게, 즉 수사 종료 후에야 비로소 이루어지거나 또는 수사기관의 독단으로 그것이 유예·배제되어서는 안된다. 물론 비밀의 수사처분(대표적인 예로 통

101) 한편 독일 법제로 본다면 이러한 집행으로 침해되는 기본권은 주거의 불가침이기 때문에 (*BVerfGE* 120, 274, 309 f. [Rn. 192 f.]), 그 집행을 위해서는 주거감청 영장이 필요할 것이다.
102) 허황(주 28), 131면; 윤지영(주 30), 53면; 류부곤(주 36), 49면; 이원상(주 30), 200면 이하.
103) 헌재 2018.8.30. 2016헌마263, 판례집 30-2, 481.

신감청)을 통해 획득된 증거의 사용가능성 및 통지의 유예나 배제의 판단에 있어, 해당 처분의 종료 직후, 아직 수사절차가 진행 중임에도 법관이 개입하는 것은 실무상 수사기관에게 부담이 될 수 있다. 하지만 – 최소한[104] – 개인의 내밀한 정보까지 포괄적으로 수집되는 온라인 수색과 같은 수사행위는 기본권 보호를 위해 강력히 통제될 필요가 있고, 이러한 통제의 역할은 1차적으로 처분을 명령하거나 허가한 법원이 맡을 수밖에 없다. 그리고 이런 경우에 있어 법원의 개입은 수사를 방해하는 것이 아니라, 처분 당사자의 기본권에 근거한 법적 이익에 대한 불법적 침해를 방지하여 수사의 적법성을 유지하는데 있다고 보는 것이 오히려 더 합리적이다. 요컨대 온라인 수색을 통해 획득된 정보의 관련성 및 사후 통지의 유예나 배제의 판단을 수사단계에서 경찰 및 수사기관으로서의 성격이 매우 강한 검찰에게만 맡겨 놓는 것은 타당하지 않다. 신뢰할 수 있는 적법성 통제가 필요하다. BVerfG가 설시하였듯이 비밀의 수사처분에 의한 막연한 위협은 효과적인 투명성 규제를 통해 완화되어야 한다.[105]

한편 기술적으로 해킹인 온라인 수색의 집행은 대상 정보기술시스템에 설치된 감시소프트웨어에 의존할 수밖에 없다. 하지만 규범적으로 온라인 수색이 적법하기 위해서는 그 집행이 앞 Ⅲ.에서 검토한 개념 범위를 초과하거나 법원에 의해 명령·유보된 범위를 위반해서는 안 된다. 이런 점에서 온라인 수색의 적법성은 부분적이지만 감시소프트웨어의 기술적 수준에 달려 있다고 할 수 있다. 이러한 기술적 수준이 명확히 보장된다면 온라인 수색에 대한 적법성 통제는 한층 투명하고 객관적으로 신뢰할 수 있을 것이다. 하지만 그 기술적 수준에 의문이 제기됨에도 효과적인 형사소추를 위해 온라인 수색이 도입되는 경우, 그에 대한 통제는 앞 단락에서 검토된 법원의 적극적 개입이 가장 유효한 듯하다.

---

104) 통비법에 따르면 통신감청의 정보주체에 대한 통지는 공소 관련 처분을 한 날로부터 30일 이내에 하도록 되어 있다(제9조의2). 심지어 이는 공개의 처분임을 전제로 하는 압수수색에서 수사기관이 전기통신사업자가 보관하는 정보를 획득한 후에도 마찬가지이다(동법 제9조의3). 이러한 규정은 전술한 BVerfG 판결의 기준에 따르면 위헌적이다. 이에 대한 자세한 내용은 박중욱, "통신비밀보호법 통지규정의 문제점과 개선방향 - 한국과 독일의 헌법재판소 결정 내용을 중심으로", 『형사법의 신동향』 통권 제68호, 대검찰청, 2020.9, 97면 참고.

105) *BVerfGE* 125, 260, 335 [Rn. 242].

2. 온라인 수색 수권규정의 법체계적 지위: 처분요건과 절차법적 안전장치의 측면에서

온라인 수색을 도입하는 수권규정이 형소법에 위치해야 하는지, 아니면 통비법이나 개별 법령에 위치해야 하는지가 문제된다. 이 쟁점은 일차적으로 온라인 수색의 법적 성격을 통신감청과의 관계에서 어떻게 구성할 것인지의 문제이지만 근본적으로는 사적 영역을 깊게 침해하는 비밀의 수사처분을 어떻게 통합적으로 규제할 것인지와 관련이 있다.

우선 통신원감청의 개념에서 검토하였듯이 온라인 수색과 통신감청은 개념상 구분되는 처분이다. 수집되는 정보의 상태 및 그 양과 질이 다르며, 침해되는 기본권도 다르다. 무엇보다 대법원은 통비법 제2조 제3호(전기통신)와 제7호(감청)에 근거하여 동법에 따른 통신감청의 개념에 집행의 동시성과 현재성을 요구하여, 전송과정이 종료된 전기통신의 내용을 지득하는 행위는 통신감청이 아니라고 한다.[106] 이런 점을 고려하면 통비법의 제목과 정의 규정 등을 전체적으로 개정하지 않는 한, 통비법에 온라인 수색을 규정하는 것은 법체계적으로 타당하지 않아 보인다.

반면 형소법 제106조 이하의 규정에 따른 압수수색은 당사자 알게 행해지는 것이 원칙이지만, 형소법 제106조 제4항과 제107조 제3항 단서 및 제118조 단서, 제122조 단서에 따르면 압수수색은 예외적으로 당사자 모르게 집행될 수 있다. 그렇다면 형소법의 압수수색 규정이 비밀의 수사처분인 온라인 수색을 정당화할 수 있는가? 절대 그렇지 않다. 물론 형소법 제123조와 제129조의 적용도 문제되지만, 근본적으로 그렇게 해석하는 것은 헌법상 원칙인 법치국가 원칙과 비례성 원칙에 반한다. 무엇보다 그것은 헌법의 최우선 가치인 국가의 기본권 보호의무를 국민적 합의 없이 사법기관의 판단, 즉 검찰의 승인 또는 법관의 영장으로 방기하는 것과 같다. 헌법에 합치하는 법률을 통한 규제가 필요한 부분이다.

정보기술을 포함한 과학기술의 급속한 발전 및 과학기술이 수사기법에 주는 영향을 고려할 때 독일에서와 같이 형소법에 사적 영역을 깊게 침해하는 비밀의 수사처분을 법체계적으로 입법하는 것이 타당하다.[107] 따라서 통비법의 형사절차법 관련 내용 및 최근

106) 대법원 2012.10.25. 선고 2012도4644; 대법원 2016.10.13. 선고 2016도8137 등.

입법된 청소년성보호법의 신분비공개수사와 신분위장수사 관련 내용도 형소법에 통합적으로 규정하는 것이 타당하다.

Ⅵ. 글을 마치며

온라인 수색은 기본적으로 국가에 의한 해킹이고, 이러한 수사방법은 오늘날의 정보기술 환경을 고려할 때 시민의 기본권을 심각하게 침해하고 국가의 기본권 보호의무를 극도로 축소시킬 수 있다. 하지만 텔레그램이나 다크넷 등의 온라인 플랫폼을 이용한 테러나 조직범죄 등의 안보범죄 및 디지털 성착취물이나 마약의 유통·거래·소지 등의 범죄에 대한 수사에서 기존의 사이버범죄에 대한 수사방법은 한계가 가진다. 즉 암호화기술에 기반하여 폐쇄성과 익명성을 특징으로 하는 온라인 플랫폼에서 행해지는 범죄는 주로 국가의 기반·존립과 같은 국가의 안전 및 생명·신체·자유와 같은 개인의 안전을 침해하지만, 그에 대처해야 하는 국가가 사용할 수 있는 방법은 제한적이다. 이런 점을 고려할 때, 온라인 수색이라는 수사방법이 그 자체로서 위헌적이거나 무조건 금지되어야 하는 것은 아니라 할 것이다. 이 모든 것을 고려할 때, 온라인 수색의 수권규정은 국가의 기본권 보호의무 및 법치국가 원칙과 비례성 원칙에 따라 그 강력한 기본권 침해강도에 상응하도록 엄격하게 형성되어야 한다.

온라인 수색은 비례성 원칙에 따라 통비법의 통신감청보다 더 엄격한 요건 아래에서 허용되어야 한다. 우선 처분요건의 측면에서 온라인 수색은 통신감청보다 더 제한된 범위의 중대한 범죄에 대한 충분한 혐의가 있다고 인정되는 경우에만 보충적으로 허용되어야 한다. 다음으로 절차적 통제의 측면에서 그것은 세부적인 집행방법이 기재된 법관의 영장에 의해서만 명령될 수 있고, 그 집행의 비밀성과 수집되는 정보의 광범위함을 고려할 때 처분의 집행 종료 후 수집된 정보의 관련성 및 사후 통지에 대한 판단에 법원의 개입이 요구된다. 수집된 정보의 관련성 통제에는 현행 통비법상의 패킷감청 통제규정(제12조의2)에 상응하는 통제가 고려될 수 있겠지만, 사후 통지는 그렇지 않다. 현행 통비법상의 사후 통지 규정은 처분 당사자의 기본권 보호에 기여하지 못한다. 온라인 수색

107) 김재희/박희영(주 27), 142면.

에서 사후 통지는 처분의 종료 후 즉시 행해지는 것을 원칙으로 하여, 그 유예와 배제의 사유가 법률에 명확히 규정될 필요가 있고, 이러한 예외의 판단은 종국적으로 수사기관이 아닌 법원이 내려야 한다.

법치국가의 형사사법은 국가 형벌권의 유효한 실현과 사법 정형적인 절차에 따른 기본권 보호라는 상반되지만 동위에 놓인 두 가치가 이익형량될 것을 요구한다.[108] 정보기술의 발전에 따라 법익보호를 위해 수사기관의 능력이 변화된 기술여건에 발맞추어 강화될 필요가 있듯이, 기본권 보호를 위해 강력한 수사행위는 법치국가 원칙에 따라 엄격하게 통제되어야 한다.[109] 법치국가에서는 수사방법과 형사소추전략의 최신화뿐만 아니라 그것에 상응하는 수권규범의 법치국가적 업데이트가 동시에 요구된다.

108) *Roxin/Schünemann,* § 1 Rn. 7. 적법절차의 유지가 책임 있는 자의 유죄판결과 법적 평화의 재건보다 덜 중요하지 않다(a.a.O. Rn. 2).

109) 박중욱, "독일 형사소송법에서 개인정보수집을 위한 법적 근거의 변천과정과 법치국가 원칙", 『형사법의 신동향』 통권 제60호, 대검찰청, 2018.9, 320, 328-331면. 수사절차에서 법치국가적 통제가 없다면, 그것은 순수한 경찰국가이다(*Schünemann*, ZStW 114 (2002), 1, 17 f.).

참고문헌

[국내문헌]

김재희/박희영, 온라인 수색 활동의 적법성 검토 및 도입방안 연구, 2022년도 경찰청 정책연구용역 결과보고서, 경찰청/성결대학교, 2022. 12.

류부곤, “비닉성 온라인 플랫폼을 이용한 범죄에 대한 법적 대응방안”, 『경찰학연구』 제21권 제1호, 경찰대학, 2021. 3., 29면.

박웅신/이경렬, “다크넷 범죄현상과 형사법적 대응방안”, 『형사법의 신동향』 통권 제58호, 대검찰청, 2018. 3., 219면.

박중욱, “독일 형사소송법에서 개인정보수집을 위한 법적 근거의 변천과정과 법치국가원칙”, 『형사법의 신동향』 통권 제60호, 대검찰청, 2018. 9., 320면.

박중욱, “통신비밀보호법 통지규정의 문제점과 개선방향 - 한국과 독일의 헌법재판소 결정 내용을 중심으로”, 『형사법의 신동향』 통권 제68호, 대검찰청, 2020. 9., 97면.

박중욱, “제3자 보관 정보의 압수수색과정보주체에 대한 통지 - 강제처분의 공개성/비밀성에 대한 독일 논의를 참고하여 -”, 『원광법학』 제38권 제3호, 원광대학교 법학연구소, 2022. 9., 51면

박희영, “독일에 있어서 경찰에 의한 ‘예방적’ 온라인 수색의 위헌여부”, 『경찰학연구』 제9권 제2호, 경찰대학, 2009. 8., 185면.

박희영, “예방 및 수사목적의 온라인 비밀 수색의 허용과 한계”, 『원광법학』 제28권 제3호, 원광대학교 법학연구소, 2012. 9., 153면.

박희영, “수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계”, 『형사정책연구』 제29권 제2호, 한국형사법무정책연구원, 2018. 6., 26면.

박희영, “유럽에서 온라인수색과 암호통신망 EncroChat 사건”, 『형사법의 신동향』 통권 제78호, 대검찰청, 2023. 3., 36면.

박희영/홍선기, “독일 정보기관의 공법 체계 및 경찰과의 분리원칙”, 『법학논집』 제26권 제3호, 이화여자대학교 법학연구소, 2022. 3., 235면.

윤신명, “텔레그램 등 익명·비대면 공간에서의 조직범죄 수사절차와 한계”, 『4차산업혁

명에 있어서 정보화 시대의 당면 과제』, 4차산업혁명융합법학회/한국형사소송법학회 2022년 하계 학술대회 자료집, 63면.

윤지영, "디지털 성범죄 대응을 위한 수사법제 개선 방안 - 온라인 수색과 잠입수사 법제화를 중심으로", 『형사정책』 제32권 제2호, 한국형사정책학회, 2020. 7., 41면.

이원상, "온라인 수색(Online-Durchsuchung)에 대한 고찰 - 독일의 새로운 논의를 중심으로", 『형사법연구』 제20권 제4호, 한국형사법학회, 2008. 12., 335면.

이원상, "다크넷 수사를 위한 수사제도에 대한 소고", 『형사법의 신동향』 통권 제69호, 대검찰청, 2020. 12., 343면.

이원상, "온라인수색의 도입 필요성과 한계 - 아동·청소년 대상 디지털 성범죄를 대상으로", 『비교형사법연구』 제24권 제2호, 한국비교형사법학회, 2022. 7., 183면.

전윤정, "'n번방' 사건으로 본 디지털 성범죄 규제현황과 개선과제", 『이화젠더법학』 제13권 제3호, 이화여자대학교 젠더법학연구소, 2021. 12., 1면.

정대용, "디지털 증거 수집을 위한 온라인 수색의 허용가능성에 관한 연구", 『디지털포렌식연구』 통권 제20호, 한국디지털포렌식학회, 2018. 12., 67면.

정대용/김기범/권헌영/이상진, "디지털 증거의 역외 압수수색에 관한 쟁점과 입법론 - 계정 접속을 통한 해외서버의 원격 압수수색을 중심으로", 『법조』 통권 제720호, 법조협회, 2016. 12., 133면.

허황, "최근 개정된 독일 형사소송법 제100조b의 온라인 수색(Online-Durch- suchung)과 제100조a의 소스통신감청(Quellen-TKÜ)에 관한 연구", 『형사법의 신동향』 통권 제58호, 대검찰청, 2018. 3., 94면.

SBS 뉴스, "성착취물 범죄 온상 된 텔레그램…'n번방 방지법'도 못 잡는다", 2022. 9. 2.자, https://news.sbs.co.kr/news/endPage.do?news_id=N1006882525, 2023. 7. 31. 검색.

SBS 뉴스, "비밀 조직 같은 텔레그램 … 해외 주소 찾아가 보니", 2023. 6. 15.자, https://news.sbs.co.kr/news/endPage.do?news_id=N1007230917, 2023. 7. 31. 검색.

이데일리, "IP추적 어려운 '다크웹', 마약 밀매 루트로 악용", 2017. 9. 27.자,

https://www.edaily.co.kr/news/read?newsId=01656406616064384&mediaCodeNo=257, 2023. 7. 31. 검색.

중앙일보, "마약사범 역대 최다…10명 중 6명은 '30대 이하' 청년이었다", 2023. 7. 15.자, https://www.joongang.co.kr/article/25175029#home, 2023. 7. 31. 검색.

한국일보, "경찰, '실시간 감시' 온라인 수색 도입 검토... 기본권 침해 우려도", 2022. 4. 29.자, https://m.hankookilbo.com/News/Read/A2022041509320001942, 2023. 7. 31. 검색

[외국문헌]

Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG, Nebengesetze und ergänzende Bestimmungen, 62. Auflage, C.H. Beck, München 2019. (인용: *작성자* in M-G/Schmitt, StPO, § ... Rn. ...)

Roxin, Claus/Schünemann, Bernd, Strafverfahrensrecht, 29. Auflage, C.H. Beck, Mün-chen 2017. (인용: *Roxin/Schünemann*, § ... Rn. ...)

Sieber, Ulich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C.H. Beck, München 2012. (인용: *Sieber*, 69. DJT 2012, C ...)

Sieber, Ulrich/*Mühlen*, Nicolas von zur/*Tropina*, Tatiana, Access to Telecommunication Data in Criminal Justice, 2021.

Wolter, Jürgen (Hrsg.), SK-StPO, 5. Auflage, Carl Heymanns, Köln 2016. (인용: *작성자*, SK-StPO, § ... Rn. ...)

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter - Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, S. 361.

Brodowski, Dominik, Strafprozessualer Zugriff auf E-Mail-Kommunikation - zugleich Besprechung zu BVerfG, Beschl. vom 16.6.2009 - 2 BvR 902/06 sowie zu BGH, Beschl. vom 31.3.2009 - 1 StR 76/09 -, JR 10/2009, S.

402.

Brodowski, Dominik/Eisenmenger, Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden - Sachliche und zeitliche Reichweiter der „kleinen On-line- Durchsuchung“ nach § 110 Abs. 3 StPO, ZD 3/2014, S. 119.

Dalby, Jakob, Das neue Auskunftsverfahren nach § 113 TKG - Zeitdruck macht Gesetze - Eine Beurteilung der Änderung des manuellen Auskunftsverfahrens und der Neu-schaffung des § 100j StPO, CR 6/2013, S. 361.

Derin, Benjamin/*Golla*, Sebastian J., Der Staat als Manipulant und Saboteur der IT-Sicherheit? - Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung“ und Quellen-TKÜ. NJW 2019, S. 1111.

Gaede, Karsten, Der grundrechtliche Schutz gespeicherter EMails beim Provider und ihre weltweite strafprozessuale Überwachung, StV 2009, S. 96.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, S. 1035.

Hofmann, Manfred, Die Online-Durchsuchung - staatliches „Hacken” oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121.

Kudlich, Hans, Strafverfolgung im Internet: Bestandsaufnahme und aktuelle Probleme - Zur 34. Strafrechtslehrertagung 2011 in Leipzig, GA 2011, S. 193.

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042.

Michalke, Reinhart, Durchsuchung und Beschlagnahme - Verfassungsrecht im Alltag, StraFo 3/2014, S. 89.

Rieß, Peter, Die »Straftat von erheblicher Bedeutung« als Eingriffsvoraussetzung - Versuch einer Inhaltsbestimmung, GA 2004, S. 623.

Roggan, Fredrik, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung:

Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, S. 821.

Schünemann, Bernd, Wohin treibt der deutsche Strafprozess?, ZStW 114 (2002), S. 1.

Singelnstein, Tobias/Derin, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens - Was aus der StPO-Reform geworden ist, NJW 2017, S. 2646.

Wicker, Magda, Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765.

Zimmermann, Till, Der strafprozessuale Zugriff auf E-Mails, JA 5/2014, S. 321.

Zulässigkeitsvoraussetzungen der strafprozessualen Online-Durchsuchung

Überprüfung in gesetzgeberischer Hinsicht unter Bezugnahme auf deutsche Diskussionen

Joongwook Park*

Bei der Online-Suche handelt es sich im Grunde genommen um Hacking durch den Staat, und diese Untersuchungsmethode kann angesichts der heutigen IT-Umgebung die Grundrechte der Bürger ernsthaft verletzen und die staatliche Pflicht zum Schutz von Grundrechten erheblich einschränken. Bei der Aufklärung von Staatsschutzdelikt wie Terrorismus und organisierter Kriminalität sowie von Straftaten wie der Verbreitung, dem Handel und dem Besitz von sexueller Ausbeutung/Erpressung oder Drogen über Online-Plattformen wie Telegram oder Darknet stoßen die bestehenden Methoden der Cyberkriminalität jedoch an ihre Grenzen. Die neuen Online-Plattformen basiert auf Verschlüsselungstechnologie und zeichnet sich durch Geschlossenheit und Anonymität aus, die Methoden, die der Staat dagegen einsetzen können, sind jedoch sehr begrenzt. Vor diesem Hintergrund ist die Online-Durchsuchung nicht an sich verfassungswidrig und sollte bedingungslos verboten werden. Aus alledem sollte die Ermächtigungsnorm zur Online-Durchsuchung strikt nach der staatlichen Pflicht zum Schutz von Grundrechten und den Grundsätzen der Rechtsstaatlichkeit und der Verhältnismäßigkeit so ausgestaltet werden, dass sie dem schwerwiegenden Grundrechtsverstoß entspricht.

Eine rechtsstaatliche Strafrechtspflege fordert, dass die wirksame Verwirklichung des staatlichen Strafanspruchs und der Grundrechtsschutz nach einem justizförmigen

* Expert Researcher(Dr. jur.), The Institute of Comparative Law and Legal Culture, Dongguk University

Verfahren, die beide gegensätzliche, aber gleichrangig gestellte Werte darstellen, abgewogen werden. Wie nach dem Fortschritt der IT zum Schutz der Rechtsgüter eine Anpassung der Fähigkeit der Ermittlungsbehörde an veränderte technische Gegebenheiten von Bedeutung ist, ist ebenfalls zum Schutz der Grundrechte auch eine Kontrollierung der Ermittlungshandlungen gestützt auf das Rechtsstaatsprinzip von Bedeutung. Sowohl die Modernisierung der Ermittlungsmethoden und der Strafverfolgungsstrategien als auch die rechtsstaatliche Aktualisierung der dementsprechenden Ermächtigungsgrundlagen ist zugleich geboten.

❖ Schlagwörter: Straftaten im Darknet, Online-Durchsuchung, Quellen-TKÜ, IT-Grundrecht, Verhältnismäßigkeit, Transparenz, Heimlichkeit der Ermittlungsmaßnahme, verfahrensrechtliche Vorkehrungen, Benachrichtigung

❖ Key words: darknet crimes, online search, Quellen-TKÜ, the fundamental right to IT, proportionality, Transparency, confidentiality of investigative measure, procedural safeguards, notification

투고일 : 8월 28일 / 심사일 : 9월 22일 / 게재확정일 : 9월 30일