형사정책연구 Korean Criminological Review
제30권 제2호(통권 제118호, 2019・여름)

암호통신감청 및 온라인수색에서 부수처분의 허용과 한계*

박희영**·이상학***

국 | 문 | 요 | 약

정보통신기술의 발전에 따라 나날이 변모하고 있는 중대 범죄에 대처하기 위해서 독일은 온라인수색과 암호통신감청을 형사소송법과 경찰법에 각각 도입하였다. 온라인수색과 암호통신감청을 수행하기 위해서는 우선 감시소프트웨어가 설치되어야 한다. 하지만 이들 규정은 설치방법에 대해서는 아무런 언급을 하지 않고 있다. 따라서 다양한 설치방법들이 주처분에 수반되는 부수처분으로 허용되는지 검토되어야 한다. 검토의 대상은 주거 출입을 통한 방법, 기망을 통하여 착오에 빠진 이용자를 이용하는 방법, IT 보안취약점을 이용하는 방법이다. 이러한 방법들은 추가적인 기본권 침해를 야기할 가능성이 있으므로 부수권한으로 허용될지 상당한 의문이 제기된다. 이러한 부수권한의 입법도 정당화하기에 상당히 제한적으로 보인다.

장래에 우리 입법자도 테러범죄와 같은 중대한 범죄에 대처하기 위해서 온라인수색이나 암호통신감청과 같은 수사방법에 관한 논의가 있을 것으로 예상된다. 특히 헌법재판소가 인터넷회선감청(패킷감청)은 허용될 수 없다고 결정하고 이에 대한 입법을 촉구하였는데, 암호통신감청이 그 대안이 될 수 있다. 온라인수색에 이용되는 감시소프트웨어는 암호통신감청에도 이용될 수 있기 때문에 이들은 동시에 논의되어야 할 것이다. 하지만 온라인수색과 암호통신감청을 수행하기 위한 독일의 부수처분들은 기본권을 추가로 침해할 우려가 있으므로 우리의 도입 논의에서는 보다 엄격한 요건이 필요할 것으로 보인다.

❖ 주제어 : 암호통신감청, 온라인수색, IT기본권, 부수권한, 부수처분, 취약점, 자기부죄금지, 범죄수사적 술책, 기망금지, 고의적 허위정보 유포

---

* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2016S1A5A2A03927806).
** 독일 막스플랑크 국제형법연구소 연구원, 법학박사, 주저자(연구책임자).
*** 대구대학교 DU인재법학부 교수, 법학박사, 교신저자(공동연구자).

Ⅰ. 문제제기

정보통신기술의 발전은 범죄 예방이나 수사 영역에서 다양한 변화를 초래하였다. 유럽 특히 독일에서는 지난 10여년간 무엇보다 전기통신의 감청과 압수 및 수색에서 큰 변화가 있었다. 전통적인 통신감청이 해결하지 못했던 암호화된 통신은 '암호통신감청'으로 해결되었고, 컴퓨터 등 정보기술시스템이나 그 안에 저장되어 있는 데이터를 수색 및 압수하기 위해서 물리적으로 주거에 들어가는 대신 원격으로 접근할 수 있는 '온라인수색'이 등장하였다. 이러한 수사방법은 처음에는 범죄 예방 목적의 경찰법[1]과 정보기관법[2]에 도입되었다가 2017년 8월 형사소송법에 도입되었다.

온라인수색(Online Durchsuchung)이란 국가기관이 원격 통신 감시 소프트웨어와 같은 기술적 수단을 이용하여 이용자의 정보기술시스템에 비밀리에 접근하여 이용자의 시스템 이용을 감시하고 여기에 저장된 내용을 열람하거나 수집하는 것을 말한다.[3] 온라인수색에 사용되는 감시소프트웨어는 인터넷에 연결되어 있는 컴퓨터에 접근하는 것이어서 암호화되기 전 또는 복호화된 후 송신자 또는 수신자의 정보기술시스템에서 암호화된 메신저나 인터넷전화 같은 통신의 내용을 감청할 수 있다. 이러한 방식의 전기통신감청을 암호통신감청(Quellen TKÜ)이라고 한다.[4] 암호통신감청은 테러범과 같은 중대 범죄자가 내용을 암호화하여 통신을 하는 경우 수사기관이 이를 감청하였지만 해독하지 못하면 그 감청은 실패로 끝나게 되는데, 이러한 암호통신으로 인한 수사의 어려움을 해결하기 위해서 등장한 것이다. 일반적인 통신감청은 송신자나 수신자의 지배영역을 떠나서 전기통신사업자의 지배영역

1) 연방범죄수사청법(BKAG)과 각 주 경찰법. 이하 '경찰법'으로 칭한다.

2) 예를 들어 노르트라인 베스트팔렌 주의 헌법보호법(NWVSG)(제5조 제2항 제11호). 하지만 이 조항은 연방헌법재판소로부터 위헌판결을 받았다(BVerfG, 1 BvR 370/07 vom 27.2.2008).

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

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

에 있는 현재 진행 중인 통신을 대상으로 하지만, 암호통신감청은 송신자나 수신자의 지배영역인 통신기기에서 감청이 이루어진다는 점에서 차이가 있다.[5] 따라서 수사기관은 전기통신사업자를 거치지 않고도 암호통신을 직접 감청할 수 있다. 암호통신감청은 기본적으로 온라인수색의 기술적 수단을 이용하기 때문에 '작은' 온라인수색이라고 부른다.

암호통신감청과 온라인수색은 주처분인 감청과 수색을 하기 위해서 반드시 감시소프트웨어의 설치라는 부수처분이 수반되어야 한다. 물론 설치된 소프트웨어를 제거하는 것도 이에 해당된다. 감시소프트웨어는 대상 시스템에 일회의 접근이나 장기간 감시를 가능하게 한다. 대상 시스템에 접근을 가능하게 하는 프로그램을 일상적 용어로 국가트로이목마(Staatstrojaner)라고 부르고, 장기간 시스템 감시를 가능하게 하는 프로그램을 원격 포렌식 소프트웨어(Remote Forensic Software)라고 한다.[6] 감시소프트웨어의 설치와 제거로 대상 시스템에 변경이 가해진다.[7] 그런데 이러한 부수처분을 수행하기 위해서 독자적인 별도의 규정이 필요한지 아니면 부수처분은 주처분에 수반되는 것으로 주처분의 부수권한으로서 허용되는지 문제가 제기된다. 현재 독일의 온라인수색과 암호통신감청에 관한 규정은 이에 관하여 명확하게 언급하고 있지 않다. 필자[8]는 헌법의 기본권 관점에서 암호통신감청의 입법방향을 제시한 연구를 이미 수행하였으나[9] 이 문제는 아직 다루지 않았다. 따라서 이 글은 선행 연구에 이은 후속 연구에 해당된다.

이 글은 온라인수색과 암호통신감청을 수행하기 위한 감시소프트웨어의 설치가 부수권한으로서 허용되는지를 검토한다. 장래에 우리 입법자도 테러범죄와 같은 중대한 범죄에 대처하기 위해서 온라인수색이나 암호통신감청과 같은 수사방법에 관한 논의가 있을 것으로 예상된다. 특히 헌법재판소가 인터넷회선감청(패킷감청)은

5) 암호통신감청에서 독일어 Qullen은 통신의 출처 또는 진원지를 의미하므로 대상자의 통신기기를 말한다. 이러한 통신감청은 암호화된 통신의 내용을 감청한다는 의미에서 암호통신감청이라고 하며 '소스감청'이라고도 번역된다.

6) Derin/Golla, NJW 2019, 111.

7) Freiling/Safferling/Rückert, JR 2018, 9 (18); Heim, NJW-Spezial 2018, 120.

8) 연구책임자.

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

허용될 수 없다고 결정하고 이에 대한 입법을 촉구하였는데, 암호통신감청이 그 대안이 될 수 있기 때문이다.[10] 특히 온라인수색에 이용되는 감시소프트웨어가 암호통신감청에도 이용될 수 있기 때문에 이들은 동시에 논의되어야 한다. 따라서 이러한 부수처분에 관한 문제가 우선적으로 규명될 필요가 있다. 이 글은 우선 독일의 범죄예방과 수사목적의 온라인수색과 암호통신감청이 어떻게 규범화되어 있는지 관련 규정들을 개관하고(Ⅱ) 감시소프트웨어의 다양한 설치방법을 살펴본 후(Ⅲ) 이러한 설치방법이 허용되는지 검토하고(Ⅳ) 우리에게 주는 시사점을 도출한다.

Ⅱ. 암호통신감청과 온라인수색에 관한 독일의 관련 규정들

1. 연방범죄수사청법(BKAG)

예방목적의 암호통신감청과 온라인수색은 연방범죄수사청법(이하 'BKAG')과 각 주 경찰법에 규정되어 있다. 여기서는 테러범죄와 관련하여 이러한 처분을 두고 있는 BKAG의 규정들을 살펴본다. 연방헌법재판소는 2016년 4월 20일 BKAG의

10) 암호통신감청과 패킷감청은 그 개념이나 기본권 침해의 정도면에서 차이가 있는데, 전자가 후자의 대안이 될 수 있는지 의문이 제기될 수 있다. 양자는 통신감청이란 개념을 전제로 하고 있다는 점에서 동일하지만 그 방법에 차이가 있다. 암호통신감청은 대상자의 통신기기에 침입한다는 면에서 일반감청보다 침해의 강도가 높지만, 통신이 암호화되기 전에 해당 통신만 가로채고 기본적으로 대상자의 통신기기에 있는 데이터에는 침입하지 않는다(물론 독일의 경우 통신 종료 후 감청도 허용하고 있지만, 이것은 어디까지나 예외에 해당된다). 암호통신감청은 대상 통신이 전자메일인지 스카이프와 같은 비밀 음성통신인지 아니면 메신저인지 특정된다. 이에 대하여 패킷감청은 해당 통신회선을 통과하는 모든 패킷이 일단 그 대상이 된다. 즉 쌍방통신이 아닌 소위 '1인통신'(인터넷 검색, 쇼핑, 영화관람이나 음악감상 등)이나 통신비밀보호법의 대화감청으로 보기 어려운 '사람과 인공지능 음성비서와의 대화'도 그 대상이 된다. 감청은 기본적으로 '송수신자의 의사소통'을 전제로 하고 있다는 점에서 패킷감청은 전통적인 감청의 범위를 훨씬 벗어날뿐 아니라 기본권 침해의 정도도 암호통신감청보다 높다고 생각된다. 따라서 암호통신의 문제를 해결할 수 없고 기본권 침해의 정도가 높은 패킷감청을 입법할 필요가 없으며 암호통신감청이 그 대안이 될 수 있다고 본다. 이에 대해서는 다음 기회에 상세하게 다룬다(일반통신감청, 패킷감청, 암호통신감청, 온라인 수색의 구분에 대해서는 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018 ·여름), 28-31 참조)

국제테러의 위험을 방지하기 위한 비밀 감시처분규정들에 대한 헌법불합치 판결에서 개정 방향에 필요한 기준들을 제시하였다.[11] 이러한 기준들에 따라서 BKAG는 '2017년 6월 1일 연방범죄수사청법의 새로운 체계화를 위한 법률'에 의해서 전부 개정되어 2018년 5월 25일부터 발효되었다.[12]

가. 온라인수색[13]

BKAG는 제49조에서 온라인수색을 규정하고 있다.[14] 동조 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 것이 특정한 사실로부터 정당화되는 경우 당사자 모르게 기술적인 수단을 통해서 당사자가 이용하고 있는 정보기술 시스템에 침입하여 거기에 있는 데이터를 수집할 수 있다(제1항 제1문). 동조 제2항은 또한 데이터 수집을 위해서 반드시 필요한 경우에만 정보기술시스템에 변경이 가해지고, 이 변경은 처분의 종료 시 기술적으로 가능한 한 자동으로 복구되도록 해야 한다(제2항 제1문)고 규정하고 있다. 나아가서 사용된 수단은 현재의 기술 수준에서 무권한 이용으로부터 보호되어야 하며(제2항 제2문), 복제된 데이터는 현재의 기술 수준에 의해서 변경, 무권한 삭제, 무권한 인지로부터 보호되어야 한다고 규정하고 있다(제2항 제3문).

---

11) BVerfG Urteil vom 20. April 2016 - 1 BvR 966/09. 이 판결을 다루고 있는 문헌으로는 이상학, 테러방지 수권규정과 기본권침해의 한계 – 독일연방수사청법의 테러방지권한에 대한 연방헌법재판소의 판결(2016.4.20.) 검토를 중심으로, 공법학연구 제17권 제3호, 제109-134면; 정문식, 테러방지 감시조치에 대한 위헌심사기준 – 독일연방헌법재판소 연방사법경찰청법(BKAG) 결정을 중심으로, 법과 정책연구, 제18권 제2호, 2018, 6. 3-43면; 홍선기/강문찬, 테러방지법상 국정원 정보수집권한에 대한 개정논의 – 최근 독일 연방헌법재판소의 판결과의 비교검토, 법과 정책연구 제17권 제3호, 2017.9.

12) Bundesgesetzblatt 2017 Teil I Nr. 33, 08.06.2017 S. 1354.

13) 온라인수색에 관한 최근 독일의 법제동향에 대해서는 박희영, 국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향, 최신외국법제정보 2019 제1호, 한국법제연구원, 55-73.

14) 동법 제49조는 정보기술시스템의 비밀 침입(Verdeckter Eingriff in informationstechnische Systeme)이라고 표제어를 사용하고 있으나 형사소송법 제100b조는 온라인수색(Onlinedurchsuchung)이라는 표제어를 사용하고 있다.

나. 암호통신감청

BKAG 제51조 제1항은 일반통신감청을, 제2항은 암호통신감청을 각각 규정하고 있다. 제2항에 따르면 전기통신의 감청은 위험의 방지 또는 범죄의 예방이 다른 방법으로는 가망이 없거나 본질적으로 어렵고, 기술적인 조치를 통해서 오로지 현재 진행 중인 전기통신만 감청되는 것이 확보되고, 특히 암호화되지 않은 방식으로도 전기통신의 감청을 가능하도록 하기 위해서 정보기술시스템의 침입이 필요한 경우에 당사자 모르게 당사자가 이용하고 있는 정보기술시스템에 기술적인 수단으로 침입하는 방법으로 수행될 수 있다고 규정하고 있다. 그리고 온라인수색 제49조 제2항을 준용하고 있다.

2. 형사소송법

범죄수사목적의 온라인수색과 암호통신감청은 형사소송법에 규정되어 있다. 앞서 언급한 BKAG 대한 연방헌법재판소의 판결이 제시한 기준에 따라서 '2017년 8월 17일 효율적이고 실무에 적합한 형사절차의 구성에 관한 법률'[15]에 의하여 형사소송법이 개정되어 2017년 8월 24일부터 발효되었다.[16] 개정 법률의 핵심 내용은 형사소송법에 암호통신감청과 온라인수색을 도입하는 것이었다. BKAG 대한 연방헌법재판소의 판결이 제시한 기준을 따르고 있기 때문에 BKAG의 규정 내용과 거의 유사하게 입법되어 있다. 다만 기존 형사소송법의 조문 체계에 맞추다보니 암호통신감청이 온라인수색보다 앞에 규정되어 있다.

가. 암호통신감청

BKAG의 통신감청의 규정방식과 같이 일반통신감청과 암호통신감청을 구분하고

15) Bundesgesetzblatt 2017 Teil I Nr. 58, 23.08.2017 S. 3202.

16) 입법이유에 대해서는 김성룡, 독일 형사소송법 최근 개정의 형사정책적 시사 – 수사절차를 중심으로 -, 형사정책 제29권 제3호, 2017.12; 허 황, 최근 개정된 독일 형사소송법 제100조b의 온라인수색과 제100조a의 소스통신감청에 관한 연구, 형사법의 신동향 통권 제58호, 대검찰청, 2018.3 참조.

있다. 일반통신감청은 제100a조 제1항 제1문에서, 암호통신감청은 제100a조 제1항 제2문과 제3문에서 두 가지로 구분하여 각각 규정하고 있다.

일반통신감청은 '중대한 범죄'[17]를 정범 또는 공범으로서 행하였거나 미수가 처벌되는 사례에서 실행에 착수하였거나 다른 범죄행위를 통해 예비하였다는 혐의를 뒷받침하는 특정한 사실이 있고, 범행이 개별적인 경우에도 중대하며, 사실관계의 조사나 피의자의 소재지에 대한 수사가 다른 방법으로는 현저히 어렵거나 가망이 없을 것으로 예상되는 경우에 당사자가 모르더라도 수행될 수 있다.

이에 대해 암호통신감청은 특히 암호화되지 않은 형태로 감청이 가능하도록 하기 위해서 필요한 경우, 기술적 수단을 이용하여 당사자가 이용하고 있는 정보기술시스템에 침입하는 방법으로도 수행될 수 있다('현재 진행 중인 전기통신'). 또한 통신 진행 중에도 공중전기통신망에서 암호화된 형태로 감시되고 기록될 수 있었던 경우에는 당사자의 정보기술시스템에 저장되어 있는 통신의 내용과 상황(내역)도 감시되고 기록될 수 있다('통신 종료 후' 감청). '현재 진행 중인 전기통신' 감청은 전형적인 암호통신감청이고, '통신 종료 후' 감청은 특히 메신저 서비스 등에 적용되는 특별한 암호통신감청이다. 즉 메신저의 송수신이 종료되었더라도 만일 이것이 전송 중일 때도 감청이 가능하였던 것이라면 해당 시스템에 보관되어 있는 메신저에도 접근할 수 있다는 것이다. 이것은 감청영장을 발부받은 시점부터 감시소프트웨어를 설치하여 집행하기까지 행해진 통신을 대상으로 한다.

동조 제5항은 암호통신감청에서 기술적으로 확보되어야 할 내용을 규정하고 있다. 첫째, 암호통신감청의 대상은 현재 진행 중인 전기통신이어야 하고, 감청명령의 시점부터 진행 중인 전송과정 동안에도 공중전기통신망에서 감시되고 기록될 수 있었던 통신의 내용 및 상황만이 감시되고 기록될 수 있어야 한다. 둘째, 정보기술시스템에서는 오로지 데이터 수집을 위해서 불가결한 경우에만 변경이 가능하다. 셋째, 변경된 것은 처분의 종료 시 기술적으로 가능한 한 자동적으로 복구되어야 한다. 또한 설치된 수단은 현재의 기술 수준에 의해서 무권한 이용으로부터 보호되어야 한다. 복제한 데이터도 기술의 수준에 의해서 변경, 무권한 삭제 및 무권한 인식으로부터 보호되어야 한다.

17) 제100a조 제2항에 열거되어 있다.

나. 온라인수색

제100b조 제1항은 온라인수색의 개념을 '기술적 수단을 이용하여 당사자가 이용하는 정보기술시스템에 침입하여 이 시스템에서 데이터를 수집하는 것'으로 정의하고 있다. 이러한 온라인수색은 당사자가 모르더라도 특정한 사실이, 누군가가 정범 또는 공범으로 특별한 중범죄[18]를 범했거나 가벌적 미수 사례에서 미수를 범하였다는 혐의를 뒷받침하는 경우, 범죄행위가 개별적으로도 특별히 중대한 비중을 가지는 경우, 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로 본질적으로 어려울 수 있거나 가망이 없을 수 있는 경우에 수행된다. 온라인수색은 또한 암호통신감청의 기술적 확보 조항(제100a조 제5항)을 준용하고 있다.

3. 소결

예방목적 및 수사목적의 암호통신감청과 온라인수색에 관한 규정들은 공통적으로 '기술적 수단을 통한 정보기술시스템의 침입'이라는 법문언을 사용하고 있다. 하지만 주처분인 암호통신감청과 온라인수색이 수행되기 위해서 정보기술시스템에 감시소프트웨어가 설치되어 있어야 하는데, 이러한 설치방법에 대해서는 명확하게 언급되어 있지 않다.

Ⅲ. 감시소프트웨어의 설치 방법

온라인수색과 암호통신감청을 수행하기 위해서는 우선 대상 IT 시스템에 감시소프트웨어가 설치되어야 하고 처분이 종료된 이후에는 설치된 감시소프트웨어를 제거해야 한다. 법적으로 중요한 의미를 가지는 것은 설치 방법이다. 감시소프트웨어를 설치한다는 의미는 일반적으로 악성코드로 대상시스템을 감염시키는 것이다. 여기에는 다양한 방법이 고려될 수 있다.

18) 제100b조 제2항에 열거되어 있다. 자세한 내용은 박희영, 앞의 글 참조.

1. IT 시스템 제작 시 백도어를 이용하는 방법

IT 시스템 제작자는 일반적으로 이후에 업데이트나 복구 작업에 대비하여 이에 상응한 기능을 해당 시스템에 설정해 두거나 백도어(backdoor)을 설치해 놓는다. 백도어란 시스템 설계자가 이후에 다양한 목적으로 해당 시스템에 접근하기 위해서 의도적으로 만들어 놓은 비밀통로이다. IT 시스템 제작자가 공장 출고 시 이러한 백도어를 만들어 놓고 이를 통하여 감시소프트웨어가 설치될 수 있는 IT 시스템을 이용자에게 제공할 수 있다. 물론 이 방법은 IT 시스템 제작자와 수사 및 보안기관 사이의 협력을 요구한다. 하지만 이러한 설치 방법이 성공할 수 있을 지는 여전히 의문이 남아 있다.[19] 독일에서는 보안기관을 위해서 IT 시스템에 백도어를 설치할 의무를 제조자에게 부여하는 방안이 논의된 적이 있었다. 하지만 이 방법은 암호통신감청이나 온라인수색과는 관련이 없었다. 무엇보다 독일 입법자는 형사소송법 개정 이유에서 백도어를 통해서는 온라인수색이나 암호통신감청이 수행되어서는 안 된다는 점을 명백하게 밝히고 있다.[20]

2. 물리적인 접근 방법

물리적인 접근 방법은 가령 수사관이 비밀리에 대상자의 주거에 들어가서 그 곳에 있는 컴퓨터에 감시소프트웨어를 설치하는 것이다. 예를 들어 비밀 수사관이 인터넷 기사로 위장하여 IT 시스템이 있는 공간에 접근하는 것이다. 주거 외부에서는 수사기관이나 보안기관이 출입국 시 세관통제나 기타 교통 통제 처분과 관련하여 일시적으로 모바일 기기에 접근할 수도 있다. 마지막으로 제삼자가 고의 없이 행위하는 도구로서 물리적인 침입을 하게 하는 것을 생각해 볼 수 있다. 예를 들어 회사의 동료가 판촉물로 받은 USB 칩으로 대상 컴퓨터를 감염시키는 경우이다.

---

19) Freiling/Safferling/Rückert, JR 2018, 9 (18).

20) BT-Drs. 18/12785, 53.

3. 원격 접근 방법

인터넷을 통한 원격접근의 경우로는 국가트로이목마나 원격 포렌식 소프트웨어를 통해서 해당 시스템에 접근하여 설치하는 방법이 고려될 수 있다. 우선 IT 시스템의 보안취약점을 이용할 수 있다. 보안취약점(vulnerability)이란 소프트웨어나 정보시스템 상에 존재하는 보안상의 결함으로서 프로그램을 본래의 기능과 다르게 작동하게 하거나 허용된 권한을 초과하여 사용할 수 있게 하거나 의도하지 않은 오류를 발생하게 할 수 있는 조건들을 말한다. 보안취약점은 타인의 컴퓨터에 악성코드를 설치하는 데에 많이 악용되고 있다.[21] 또한 수사기관 및 보안기관이 소프트웨어 제작자나 전기통신사업자에게 해당 IT 시스템에 대한 접근을 가능하도록 강제하는 것이다. 가령 정기적인 소프트웨어 업데이트를 통해서 비밀리에 설치하는 것을 생각해 볼 수 있다. 끝으로 시스템 이용자를 조종하여 설치하게 하는 방법이 고려될 수 있다. 여기에는 다양한 방법들이 있을 수 있다. 감시소프트웨어는 감염된 첨부파일을 이메일과 함께 이용자에게 송신하여 설치될 수도 있다. 가령 피싱 방법으로 행해질 수도 있다. 다만, 이 경우에는 이용자가 첨부파일을 개봉해야만 설치가 가능하다.[22] 이러한 방법의 경우 당사자가 첨부파일이 있는 메일을 열람하도록 유도하기 위해서 수사기관이나 보안기관이 사인(예컨대 가족구성원)이나 다른 국가기관(예컨대 국세청)으로 사칭할 수 있다.

---

21) 보안취약점에 의해 악성코드에 감염되는 대표적인 사례는 악성코드가 포함된 웹사이트를 방문하는 경우, 악성코드가 포함된 이메일을 열람 하는 경우, 악성코드가 포함된 동영상이나 문서파일을 열어보는 경우, 악성코드에 감염된 PC가 내 PC와 같은 네트워크에 속해 있는 경우 등이다. 그리고 보안취약점과 상관없이 악성코드에 감염되는 대표 사례로는 악성 실행파일을 직접 실행하는 경우, 악성 Active X 설치 안내에 동의하는 경우, 프로그램 설치 시 악성 제휴프로그램 설치에 '동의'를 체크하는 경우, 이미 설치된 악성 프로그램이 또 다른 악성코드를 자동으로 설치하는 경우, 윈도우의 '이동식미디어 자동실행'옵션을 켜둔 상태에서 악성코드에 감염된 이동식 저장장치를 PC에 연결하는 경우 (USB메모리, MP3플레이어, CD등) 등이 있다 (https://www.estsecurity.com/securityCenter/commonSense/view/23).

22) BeckOK Polizeirecht Baden-Württemberg/v. der Grün, 12. Ed. 2018, § 23 b PolG BaWü Rn. 37.

4. 소결

이상에서 처분 대상자의 IT 시스템에 감시소프트웨어를 설치하는 다양한 방법이 있음을 살펴보았다. 이들 중 특히 IT 시스템 제작 시 백도어를 이용하는 방법은 허용되지 않는다고 생각된다. 아래에서는 온라인수색과 암호통신감청을 수행하기 위한 부수처분이 법적으로 허용되는지 특히 문제가 될 수 있는 세 가지 설치 방법을 검토한다. 이들은 주거 출입을 통한 접근, 착오에 빠진 이용자를 통한 접근, IT 보안 취약점을 이용한 접근 등이다.

Ⅵ. 부수처분의 허용 기준과 그 한계

1. 부수처분의 허용 기준

온라인수색과 암호통신감청을 수행하기 위한 사전처분인 감시소프트웨어의 설치는 도그마틱상 형사절차에서 비밀 처분의 수행으로 발생하는 전형적인 부수처분으로서 법적으로 허용되는 부수권한(Annexkompetenz)에 속하는지 문제가 된다. 우선 학설과 판례가 인정하고 있는 형사소송법상 부수처분의 허용 기준을 살펴본다.

부수권한이란 형사절차상 적법한 조치의 수행과 관련하여 발생하는 부수처분이 법률에 명시적으로 규정되어 있지 않더라도 피의자 또는 제3자의 권리를 침해할 수 있도록 허용하는 권한을 말한다. 부수권한을 인정하는 배경은, 입법자가 수권규정을 만들 때에 전형적인 또는 필요한 모든 부수처분을 개별적으로 규정하지 않는다는데 있다. 그리하여 허용되는 주처분의 수행에 전형적으로 수반되는 추가적인 침해는 허용되는 부수처분으로 본다. 만일 이를 허용하지 않게 되면 법률상 규정된 주처분이 수행될 수 없거나 불완전하게 수행될 수 있어서 주처분의 목적을 달성할 수 없게 된다.[23] 따라서 법원이 명령한 주처분의 수행에 필요한 사전처분의 허용여부는 주

23) BGH Ermittlungsrichter, Beschluss vom 20.3.2003 – 1 BGS 107/03, Rn. 6 ff.; BGH, Urteil vom 24.1.2001 - 3 StR 324/00, Rn. 18.

처분의 수행을 위한 수권규정의 해석에 달려있다.[24] 판례와 학설이 인정하고 있는 부수권한의 예로는 위치추적기를 자동차에 부착(주처분)하기 위해서 몰래 차문을 여는 행위(부수처분)[25], 피의자가 주거수색에 반항하고 있는 경우 주거수색(주처분)을 위해서 문을 강제로 개방하는 행위(부수처분)[26]등이 있다.

부수권한을 인정하기 위한 요건은 비례성원칙과 전형성 표지의 두 가지다.[27] 비례성원칙에 따르면 기본권을 침해하는 국가의 모든 처분은 정당한 목적을 추구하고 이러한 목적을 달성하기 위해서 필요하고 적합하며 적정해야 한다. 부수권한의 허용 여부를 판단하기 위해서 부수처분의 기본권 침해의 정도가 주처분의 정도를 넘어서는 안 된다. 부수처분의 침해의 정도가 주처분과 같거나 넘어서는 경우 입법자는 기본권 침해를 근거로 이 처분에 대한 새로운 수권 근거를 마련해야 한다. 그렇지 않은 경우 국가의 침해행위의 중요한 부분이 입법자에 의해서 규제되지 않을 뿐 아니라[28] 기본법상 법률유보가 우회될 위험이 존재할 수 있다.

부수권한을 인정하기 위한 두 번째 요건인 전형성 표지는 부수처분이 전형적으로 주처분에 수반되어야 한다는 것을 의미한다.[29] 즉 부수처분은 주처분의 수행과 반드시 결부되어야 한다. 또한 비례성원칙과 전형성 표지는 동시에 존재해야 한다. 한편 형사소송법상 부수처분의 허용 기준은 예방적 영역에서도 적용될 수 있다.[30]

2. 주거 출입을 통한 설치

지금까지 독일의 문헌과 실무는 온라인수색과 암호통신감청의 부수처분이 허용되는지의 문제를 주로 IT 시스템의 물리적인 접근과 관련하여 논의하였다. 특히 이

24) Schlegel, Normative Grenzen für internetbasierte Ermittlungsmethoden, 2019, 88-89.
25) BGH Urteil vom 24.01.2001 - 3 StR 324/00.
26) SK-StPO/Rudolphi, 5. Aufl. 2016, vor § 94 Rn. 32.
27) LG Hamburg, MMR 2011, 693 (694); Schneider, NStZ 1999, 388. 박희영, 암호통신감청의 허용 여부, LG Hamburg, Beschluss vom 13.9.2010 - 608 Qs 17/10, 최신독일판례연구, 로앤비(www.lawnb.com), 2017.8, 1-8.
28) AG Hamburg, Beschl. v. 28.08.2009 - StV 2009, 636 (637).
29) Schneider, NStZ 1999, 388 (388).
30) Schneider, NStZ 1999, 388.

와 관련하여 수사기관이 필요한 소프트웨어를 설치하기 위해서 '비밀리에' 주거에 출입할 수 있는지가 핵심이었다.[31)]

공중이 접근할 수 있거나(예컨대 공공 장소의 컴퓨터) 권리자의 동의를 받은 경우(예컨대 인터넷 카페)에는 대상 시스템에 직접 접근하는 것은 문제가 되지 않는다. 또한 접근 권리자의 동의를 얻기 위해서 범죄수사적 술책을 사용하는 것(예컨대 수사기관이 인터넷 관리 기사로 위장하는 경우)은 비례성원칙을 고려하더라도 기본적으로 허용된다.[32)]

하지만 이에 반해서 물리적인 전달이나 포렌식 소프트웨어를 설치하기 위해서 주거자의 동의 없이 비밀리에 주거에 출입하는 것이 허용되는지가 문제이다. 그 동안 이와 관련하여 상당한 논쟁이 있었다.[33)] 우선 암호통신감청의 경우에는 주거출입이 허용되지 않지만, 온라인수색의 경우에는 가능하다는 견해가 있다.[34)] 암호통신감청은 기술적으로 허용되는 기본법 제10조의 특수한 형태의 통신비밀침해라는 헌법재판소의 판결[35)]을 근거로 하고 있다. 통신감청은 송수신자의 지배영역이 주거가 아니라 전기통신사업자의 지배영역인 통신공간에서 행해지기 때문인 것으로 보인다. 하지만 온라인수색은 주거침입을 전제로 하는 음성주거감시(제100c조)에 근거하고 있고 그 요건도 이에 준하기 때문에 온라인수색을 위해서 타인의 주거에 비밀리에 침입하는 것은 허용될 수 있다고 한다.

이에 대해서 온라인수색 명령만으로는 정보기술시스템에 침입할 목적으로 당사자의 주거에 비밀리에 출입할 수 없다는 견해가 있다.[36)] 이것은 부수권한을 정당화할 수 없다고 한다. 비밀 주거 침입은 독자적인 기본권 침해에 해당되어 온라인수색

---

31) Vgl. Soiné, NStZ 2018, 497 (501).

32) BT-Drs. 18/12785, 52; Singelnstein/Derin NJW 2017, 2646; Soiné NStZ 2010, 596 (600).

33) 출입에 찬성하는 견해 : Bär in Anm. zu AG Bayreuth MMR 2010, 266 (268); Graf in BeckOK StPO Rn. 107 f.; Günther in MüKoStPO § 100a Rn. 224. 출입에 반대하는 견해 : LG Hamburg MMR 2008, 423; Singelnstein, NStZ 2012, 593 (598); Sankol, CR 2008, 13; Buermeyer, StV 2013, 470; Gercke, StraFo 2014, 94; Hierament, StraFo 2015, 365 (371); Roggan, NJW 2015, 1995 (1997).

34) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100b, Rn. 6.

35) BVerfG NJW 2008, 822, Rn. 190.

36) Soiné, NStZ 2018, 497, 501; BT-Dr. 18/12785, S. 52; BeckOK StPO/Graf 28. Ed., § 100 a Rn. 109.

을 위해 필요한 단순한 부수처분이 아니라고 한다. 게다가 감시소프트웨어는 기본법 제13조 제1항의 주거의 불가침을 통해서 보호되는 영역의 외부에서도 설치할 가능성이 존재한다고 한다. 이것은 주거 외부에서 이동성 정보기술시스템에 물리적으로 접근함으로써 또는 주거의 내외부에서 이 기기에 네트워크기반의 원격 접근을 통해서도 행해진다. 따라서 비밀 주거 침입이 가능하기 위해서는 온라인수색(제100b조) 외에 추가로 음성주거감시(제100c조)의 명령도 함께 받아야 한다고 한다.[37)]

생각컨대 앞서 언급한 부수처분의 기준인 전형성 표지와 비례성원칙을 온라인수색과 암호통신감청에 적용해 보면, 주거 출입은 이러한 처분에 전형적이지 않다는 점을 확인할 수 있다. 이미 설명한 바와 같이, 대상 시스템에 감시소프트웨어를 설치하는 다양한 방법이 존재하기 때문이다. 주거 출입은 IT 시스템에 접근을 개방하는 다양한 방법 중의 하나이다. 비례성원칙과 관련하여 주거출입은 기본권 제13조의 주거의 불가침 기본권에 위배될 수 있다.[38)] 주거출입은 해당 시스템 자체의 감염 외에도 현저한 독자적인 비중을 가지기 때문이다. 주거출입은 이미 공간적인 사생활영역의 보호범위를 침범한다. 따라서 주거출입은 부수처분으로써 전형적이지도 경미하지도 않기 때문에, 온라인수색이나 암호통신감청을 위한 규정되지 않은 부수처분으로서 허용될 수 없다.[39)]

또한 주거출입은 강제수사에 해당될 수 있기 때문에 경찰법이나 형사소송법의 수사의 일반조항에 의해서 뒷받침될 수 없다. 마찬가지 이유로 주거수색도 현장에 있는 IT 시스템에 감시소프트웨어를 설치하기 위한 근거로 인정될 수 없다.[40)] 수색은

37) Soiné, NStZ 2018, 497, 501; SSW-StPO/Eschelbach 3. Aufl., § 100 b Rn. 27.

38) 인터넷으로 연결된 주거에 있는 컴퓨터에 정보수집 소프트웨어를 잠입시켜 감시카메라 내지 감청장치를 작동하여 정보를 수집하는 것도 주거의 사생활 침해에 해당된다. 이에 대해서는 이상학, 사이버정보활동의 기본원칙과 한계, 법학연구, 2014.5, 407면 참조.

39) Roggan, NJW 2009, 257 (260); Schenke in Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2014, § 20 k BKAG aF Rn. 15; Soiné, NVwZ 2012, 1585 (1588 f.); Tinnefeld, ZD 2012, 451 (454); BeckOK Polizeirecht Baden-Württemberg/v. der Grün, § 23 b PolG BaWü Rn. 37 (예방 영역); Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 100 a Rn. 14 d; Roggan, StV 2017, 821 (822); Singelnstein/Derin, NJW 2017, 2646 (2647); Soiné, NStZ 2018, 497 (501) (수사영역).

40) Soiné, NStZ 2018, 497, 501.

당사자가 그 근거와 집행을 알아야 한다는 공개적인 성격을 가진다. 온라인수색과 암호통신감청은 비밀리에 수행되는 처분이기 때문에 공개처분으로 수행되는 것은 모순이다.[41] 따라서 주거 출입을 통해서 감시소프트웨어를 설치하는 것은 부수권한으로 인정되기 어렵다고 본다. 현재 경찰단계에서 주거 출입을 통한 설치 방법이 논의되고 있는데[42], 이러한 논의는 현재 부수권한으로 인정될 수 없다는 점을 증명하고 있다.

3. 이용자를 기망하여 설치하는 방법

수사개시의 일반조항(형사소송법 제161조와 제163조)에 의해서 수사기관은 수사절차를 자유롭게 형성할 수 있고 범죄를 규명하기 위해서 허용되는 적합하고 필요한 모든 처분을 할 수 있다.[43] 수사전략과 기법의 정당한 사용을 위한 재량권은 수사기관에게 부여되어 있다.[44] 수사전략의 관점에서 예를들어 피의자가 알지 못하게 수사를 개시하는 것은 허용되고 합목적적일 수 있다.[45] 이러한 배경에서 이용자를 기망하여 감시소프트웨어를 설치하게 하는 방법이 허용될 수 있는지 문제가 된다.

이용자를 속여서 즉 이용자를 기망하여 착오에 빠트린 상태에서 감시소프트웨어를 설치하는 모든 방법이 여기에 속한다. 예를 들어 수사기관이 감시소프트웨어가 첨부된 가짜 이메일을 이용자에게 전송하여 이를 열람하게 함으로써 시스템에 자동으로 설치되도록 하는 방법이다. 이 경우 이용자의 이메일 주소가 먼저 수집되어 있어야 한다. 이메일 주소의 수집은 온라인수색과 암호통신감청 권한에 규정되어 있지 않는 부수처분으로 간주될 수 있다. 예방 목적의 온라인수색의 경우 바이에른 주와 라인란트-팔츠 주 경찰법은 이러한 처분을 준비하기 위해 필요한 데이터를 수

41) Derin/Golla, NJW 2019, 1111, 1113.

42) 2018년 6월 제89차 주법무부장관 콘퍼런스에서 암호통신감청과 온라인수색을 위한 주거출입권에 관한 규정을 보완해야 한다고 결의한 바 있다(89. Konferenz der Justizministerinnnen und Justizminister 2018, Beschluss zu TOP II 8 – Ergänzung der Regelungen zur Quellen-TKÜ und zur Online-Durchsuchung um ein Betretungsrecht). (https://bit.ly/2HZAA1k).

43) BVerfG NStZ 1996, 45.

44) Meyer-Goßner, § 163 Rn 47.

45) Meyer-Goßner, § 161 Rn 8.

집할 수 있도록 규정하고 있다.[46] 하지만 이메일을 전송하여 감시소프트웨어를 설치할 수 있는지에 대해서는 아무런 규정이 존재하지 않는다. 이와 같이 이용자를 기망하여 착오에 빠트려서 감시소프트웨어를 설치하는 방법이 정당화될 수 있는지 검토한다.

가. 형사소송법의 독자적인 평가 기준

이용자를 기망하여 감시소프트웨어를 설치하게 하는 방법은 형사소송법의 기망금지와 관련이 있다. 즉 형사소송법은 기망을 금지하는 특별한 기준들을 인정하고 있다. 아래에서는 일반적인 부수처분의 허용기준보다는 형사절차에서 피의자의 기망에 대해 특별한 기준들을 중심으로 검토한다. 형사소송법은 기본적으로 피의자가 착오에 빠지는 것을 금지하지 않지만, 피의자의 기망은 기본적으로 허용하지 않는다.[47] 특히 형소법은 제136a조에서 피의자 신문 시 기망을 금지하고 있다. 이 외에 형사소송법은 피의자 및 피고인에게 자기부죄금지원칙과 공정한 재판을 받을 권리를 인정하여 수사활동의 한계를 정하는 기준으로 삼고 있다.[48]

1) 피의자 신문 시 기망금지 및 범죄수사적 술책의 허용 여부

독일 형사소송법은 제136a조[49]에서 금지되는 신문방법을 규정하고 있으며 그 중 하나가 기망을 통한 피의자 신문의 금지이다. 피의자의 동의와 상관없이 기망금지는 인정되지 않으며 이를 위반하여 얻은 진술은 증거로 사용할 수 없다.[50]

---

46) Art. 45 II 1 Nr. 1 BayPAG; § 31 c III 1 RhPfPOG.

47) Müller/Römer, NStZ 2012, 543 (545); aA Nowrousian, NStZ 2015, 625.

48) Vgl. MüKoStPO/Hauschild, 2014, § 108 Rn. 7; Soiné, NStZ 2010, 596.

49) 제136a조 (금지되는 신문방법; 증거 사용의 금지) (1) 피의자의 의사결정과 의사표현의 자유는 가혹행위, 피로하게 함, 신체의 침해, 약물 투여, 학대, 기망 또는 최면으로써 침해해서는 안 된다. 강제는 형사절차법이 허용하는 한도에서만 적용할 수 있다. 형사절차법 규정에서 허용하지 않는 조치를 수반한 위협과 법률에서 규정하지 않은 이익의 약속은 금지된다. (2) 피의자의 기억력이나 사고력을 침해하는 조치는 허용되지 않는다. (3) 제1항과 제2항의 금지는 피의자의 동의와 상관없이 적용된다. 이런 금지를 위반해 얻은 진술은 설령 피의자가 증거 사용에 동의하더라도 증거로 사용할 수 없다.

50) 우리 형사소송법은 독일과 같이 금지되는 신문방법을 직접 규정하고 있지 않지만, 경찰청 범죄수사

하지만 수사기관의 증거수집에서도 기망이 금지되는 것은 아니다. 현재 독일의 지배적 견해는 형소법 제136a조의 기망금지는 기본적으로 수사절차에서 피의자 신문에만 적용되고, 증거수집에는 일반적으로 적용되지 않는다.[51] 이러한 배경에서 증거수집에서 금지되는 기망과 허용되는 기망의 구분이 오랫동안 논의되어 왔다. 허용되는 기망을 '범죄수사적 술책'(kriminalistischen List)이라고 부른다. 술책이란 원래 총명, 재능, 지식, 학식 등을 도덕적으로 중립적인 의미로 이해되었으나 시간이 지나면서 부정적인 의미로 변용되었다. 새로운 견해에 따르면 술책은 부정적으로 자신의 이익을 획득하기 위해서 기망을 이용하는 능력을 의미한다.[52] 이러한 술책의 성격을 규정짓는 중요한 구성요소는 상대방을 착오에 빠지게 하는 것이다. 술책이 도덕적으로 부정적인 이미지를 주는 것은 특히 그 비밀성에 있다.[53] 형사소송법은 범죄수사적 술책의 개념을 정의하고 있지는 않다. 하지만 이러한 정의 규정이 없다고 해서 가령 피의자 신문 금지와 같이 허용되지 않는다는 것을 의미하지 않는다.

따라서 예를 들어 수사기관의 위탁으로 활동하는 신분위장수사관(VE)은 위장신분으로 법률행위에 참여할 수 있고(형소법 제110a조 제2항 제2문), 비공개수사관(Noep)(형소법 제163조)과 비경찰정보원(VP)[54](노르트라인 붸스트팔렌 주 경찰법 제19조)는 자신의 실제 신분으로 상대방을 기망할 수도 있다. 비밀처분인 통신감청

규칙 제56조에서 피의자를 조사할 때 고문, 폭행, 협박, 신체구속의 부당한 장기화 그 밖에 진술의 임의성에 관하여 의심을 받을 만한 방법을 사용해서는 안 된다고 규정하고(제1항) 있고, 경찰관은 조사를 할 때에는 희망하는 진술을 상대자에게 시사하는 등의 방법으로 진술을 유도하거나 진술의 대가로 이익을 제공할 것을 약속하거나 그 밖에 진술의 진실성을 잃게 할 염려가 있는 방법을 취하여서는 아니된다(제2항)고 규정하고 있다. 물론 피의자 신문의 방법이 적법한 절차에 따르지 않고 수집한 증거는 증거로 할 수 없기 때문에(형사소송법 제309조) 위법한 피의자의 신문은 어느 정도 통제가 가능하다. 이러한 점에서 독일과 한국은 '기망을 통한 피의자 신문'을 규범적으로 금지하고 있는 것으로 보인다.

51) BGHSt 33, 217 (224) = NJW 1986, 390; BGHSt 34, 365 (369) = NJW 1987, 2524; BGHSt 52, 11 (15) = NJW 2007, 3138; Meyer-Goßner/Schmitt, § 136 a Rn. 4; LG Hannover StV 1986, 521; MüKoStPO/Schuhr, 2014, § 136 a Rn. 73 ff.

52) Prasch, Die List in der Vernehmung und Befragung des Beschuldigten, 2003, S. 2ff., 24f.

53) Soiné, Kriminalistische List im Ermittlungsverfahren, NStZ 2010, 596), 597.

54) 비경찰정보원(V-Person:VP/V-Mann/V-Leute)은 수사기관의 직원이 아니라 특정한 사안이나 인물에 대한 정보를 취득할 목적으로 수사기관으로부터 위탁받은 사인을 말한다. 이에 대한 자세한 내용은 이상학, 테러방지 수권규정과 기본권침해의 한계, 공법학연구 제17권 제3호, 116면 참조.

의 경우도 통신의 상대방이 감청사실을 알고 있는 경우에도 기본적으로 허용된다. 형사소송법 개정 이유도 감시소프트웨어를 설치할 목적으로 범죄수사적 술책을 통해서 당사자의 정보기술시스템에 대한 접근이 가능하다고 언급하고 있다.[55]

하지만 범죄수사적 술책의 한계를 벗어나서 적극적이고 의도적으로 허위정보를 피의자에게 제공하는 것은 일반적으로 금지된다.[56] 이러한 기준에 따르면 피의자를 적극적인 기망을 통하여 착오에 빠지게 하여 IT시스템에 침입하는 것은 허용되지 않는다고 본다.

2) 자기부죄금지원칙

자기부죄금지원칙(Der nemo tenetur Grundsatz)도 형사절차에서 기망 가능성의 한계가 된다. 자기부죄금지원칙이란 '스스로에게 불이익한 진술과 행동을 하도록 강요할 수 없다'는 원칙으로[57] 법치국가적 형사절차의 기본원칙에 속한다.

이 원칙은 독일의 경우 기본법 제2조 제1항과 제1조에 의해서 보장되는 인간의 존엄성 존중권과 자유로운 인격의 발현권을 통해서 헌법상 보장되고 있고 유럽인권협약(EMRK) 제6조에 의해서 보장되는 공정한 재판을 받을 권리의 핵심영역에 속한다. 이러한 헌법상 기본권은 형소법 제55조(증인의 답변거부권), 제136조 제1항(피의자의 진술거부), 제136a조 제1항과 제3항(금지된 피의자 신문방법), 제163a조 제3항(검찰에 출석한 피의자의 진술거부), 제243조 제4항에서 구체화되어 있다.[58]

자기부죄금지원칙에 관한 법규범들은 주로 피의자나 피고인의 진술을 대상으로 규정되어 있지만 여기에 한정되지 않고 '행위'에도 적용된다. 따라서 피고인은 자신

55) BT-Drs. 18/12785, 52.

56) Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 662, 669 f.; MüKoStPO/Schuhr, 2014, § 136 a Rn. 43.

57) 자기부죄강요금지원칙, 자기부죄거부특권 등으로 번역되기도 한다. 자기부죄금지원칙의 의미에 대해서는 홍영기, Nemo tenetur-원칙, 고려법학 제66호 2012년 9월, 고려대학교 법학연구원, 305-338 참조.

58) 우리 헌법도 제12조 제2항에서 형사책임에 관하여 자신에게 불이익한 진술을 강요당하지 아니한다고 하여 자기부죄금지원칙을 천명하고 있고 헌법재판소도 이를 확인하고 있다. 나아가서 형사소송법 제244조의 3(피의자의 진술거부권 등의 고지)와 제283조의 2(피고인의 진술거부권)에서 이를 구체화하고 있다(홍영기, 앞의 논문, 307).

의 유죄판단에 근거가 될 진술이나 행위를 해야 할 의무가 없다.

이러한 점에서 적극적인 기망을 통해서 착오에 빠진 피의자가 감시소프트웨어를 자신의 IT 시스템에 설치하게 하여 자신이 생산한 증거방법을 수사기관이 확보하도록 하는 것은 자기부죄금지와 관련하여 정당화될 수 있는지 의문이다. 왜냐하면 피의자는 기본법에서 보장하고 있는 무결성을 신뢰하고 있기 때문이다.

3) 공정한 재판을 받을 권리

공정한 재판을 받을 권리는 기본법의 법치국가원칙과 자유권에 뿌리를 두고 있다. 이 권리는 인간이 국가의 소송절차에서 단순한 객체로 취급되는 것을 금지하고[59], 국가에게 구체적이고 공정한 절차를 두도록 의무를 부과한다.[60] 이러한 공정한 재판을 받을 권리도 형사절차에서 기망의 허용을 제한한다. 이 원칙은 강요를 통한 자기부죄의 야기뿐 아니라 피의자를 자신에 대한 도구로서 수단시하는 자기부죄의 야기를 금지한다.[61] 기망을 통해서 피의자가 자신에게 불리한 증거를 생산하도록 협력하게 하는 것은 피의자가 자기부죄에 관한 자유로운 판단과 절차의 객체가 아닌 주체로서의 역할을 효과적으로 인식할 수 없게 하거나 그럴 가능성을 감소시킨다. 연방대법원은 수사절차에서 투입된 비경찰정보원(VP)이 범죄적성이 없는 사람을 범죄를 실행하도록 유도한 경우에는 공정한 재판을 받을 권리가 침해된다고 인정하였다.[62] 따라서 온라인수색 및 암호통신감청의 전단계에서 피의자를 기망으로 착오에 빠지게 하여 감시소프트웨어를 설치토록 하는 것은 공정한 재판을 받을 권리에 의해서도 그 정당성에 의문이 제기된다.

나. 일반적인 평가 기준

형사소송법 평가 기준은 예방적 영역에 그대로 적용될 수는 없다. 물론 경찰법상 절차에서도 공정한 재판을 받을 권리에 따라 기망의 가능성이 제한된다.[63] 또한 연

59) BVerfGE 57, 250, 274f.; BVerfG NJW 2004, 999.
60) BVerfGE 38, 105, 111.
61) Vgl. MüKoStPO/Gaede, 2018, Art. 6 EMRK Rn. 319.
62) BGHSt 45, 321, 335; 47, 44.

방경찰법(BPolG)이나 각 주 경찰법(바이에른주, 니더작센주, 작센주 등)은 특히 직무질문, 출석요구 및 신문을 위한 개별 규정에서 형소법 제136a조를 준용하여[64] 당사자의 신문 시 기망을 금지하고 있다.

개별적인 경우 기망을 허용하기 위한 다른 평가 기준은 기본권에서도 직접 도출된다. 국가기관이 진실하지 않은 내용을 제공할 목적으로 통신하는 행위는 적어도 당사자의 일반적인 행위의 자유를 침해하는 적극적인 허위정보(Desinformation)[65]의 유포에 해당될 수 있다.[66] 국가기관이 개인정보를 수집할 목적으로 통신상대방의 신분이나 동기에 대한 보호가치가 있는 신뢰를 이용하는 경우에는 이 기본권 주체와 통신을 하면서 자신의 신분을 기망하는 것은 정보자기결정권을 침해하는 근거가 된다.[67] 이러한 정보자기결정권 침해가 IT 시스템의 침입에 기여한다면 그 침해의 강도는 훨씬 높다. 따라서 정보자기결정권 침해를 동반하게 되는 IT 시스템의 침입은 침해의 강도가 더 높은 기본권 침해를 준비하는 것이다.[68] 또한 적극적인 기망을 통해서 조종자에 대한 당사자의 신뢰가 커지면 커질수록 침해의 강도는 더욱 높아진다.

다. 소결

적극적인 기망으로 착오에 빠진 이용자에게 발생하는 권리 침해는 형사소송법의 특별한 평가 기준과 경찰법 및 헌법에 근거한 일반적 평가 기준에 의해서도 경미하지 않아 보인다. 따라서 이러한 이용자의 권리침해는 온라인수색과 암호통신감청의 부수권한이나 경찰법상 일반조항에 의해서도 정당화되기 어려워 보인다. 물론 낮은

63) Vgl. BVerfGE 38, 105 (111) = NJW 1975, 103.

64) Vgl. § 22 IV 1 BPolG; Art. 15 IV BayPAG; § 12 IV 2 NdsSOG; § 18 IX SächsPolG.

65) Desinformation(영, disinformation)은 국가기관(정보기관이나 군대 등), 정당이나 단체, 로비스트, 개인 등이 특정한 목적을 가지고 고의적으로 유포하는 잘못된 정보 또는 부정확한 정보를 말하며 고의성이 없는 오보(misinformation)와 구별된다. 이것은 주로 국민 기망, 여론조작, 반대세력의 혼란을 목적으로 한다.

66) Ingold, Desinformationsrecht, 2011, 26 f., 41 ff.; Schmalenbach, NVwZ 2005, 1357.

67) BVerfGE 120, 274 (345) = NJW 2008, 822. BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, Rn.310.(https://bit.ly/2VTdeQi)

68) Derin/Golla, NJW 2019, 1111, 1114.

정도의 착오에 빠지게 하는 것은 앞서 살펴본 부수권한의 허용기준이나 형사소송법 및 경찰법의 일반조항에 의해서 여전히 허용될 수 있다고 본다.

4. IT 보안취약점을 이용하여 설치하는 방법

시스템 침입은 IT 보안취약점의 이용과 밀접한 관련이 있다. 온라인수색과 암호통신감청 권한은 기술적 수단에 의한 정보기술시스템의 침입을 허용한다. 권한규정의 의미와 목적 그리고 입법자의 의사에 따르면 이러한 처분을 이행할 목적으로 필요한 소프트웨어를 통하여 시스템에 침입하는 것도 여기의 침입에 포함된다.[69] 하지만 수사기관이 이러한 침입을 위해서 대상 시스템에 있는 보안취약점을 이용할 수 있는지에 관해서 권한 규정은 아무런 언급을 하지 않고 있다. 따라서 보안취약점이 이미 존재하고 있는 경우 온라인수색과 암호통신감청 권한에 의해서 이 취약점을 통한 접근과 이용은 정당화될 수 있다고 주장할 수 있다. 연방정부도 의회의 대정부질문에 대한 답변에서 이러한 가능성을 배제하지 않았다.[70]

하지만 이러한 관점은 '정보기술시스템의 기밀성 및 무결성 보장에 관한 기본권'(이하 'IT 기본권')과 관련하여 문제가 제기된다. IT 기본권이란 개인이 자신의 인격 발현을 위해서 IT 시스템을 이용함으로써 발생하는 인격의 위태화를 보호하고 IT 시스템의 기밀성과 무결성을 보장함으로써 일반적 인격권의 결함을 보충하는 기본권이다.[71] 이 기본권은 타인의 IT 시스템에 비밀리에 접근하여 거기에 저장된 데이터를 열람하거나 시스템의 이용 상황을 감시하는 행위를 금지하고 있다. 따라서 IT 보안취약점을 이용하여 설치하는 방법은 IT 기본권의 관점에서 그 허용여부를 직접 검토할 수 있다.

IT 기본권은 방어권의 구성에서 개인의 보호뿐 아니라 기본권 보장의 의미도 함

69) Vgl. BT-Drs. 18/12785, 51.

70) BT-Drs.18/13413 (https://bit.ly/2wtCiCO).

71) 박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 160-164. 특히 IT 기본권의 헌법적 근거에 대해서는 161면 참조. IT 기본권은 온라인수색에 관한 위헌판결에서 독일헌법재판소가 처음으로 창설한 것이다. 이에 대해서 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 인터넷법률 통권 제45호(2009. 1), 92-123면 참조.

께 가지고 있다. 즉 IT 기본권은 정보기술시스템의 기밀성과 무결성을 '보장'한다고 표현하고 있다.[72] 이로부터 IT 보안에 대한 국가의 보호의무가 도출된다.[73] 따라서 수사기관이 감시처분을 수행하기 위해서 IT 보안취약점을 개방해 놓는 것이 국가의 보호의무와 일치하는지 문제가 된다. 이러한 배경에서 이미 알려져 있는 보안취약점이 아직 처리되지 못하고 이용되는 경우에는 문제가 덜 심각할 수 있다. 하지만 특히 국가기관이 IT 시스템의 제작자와 이용자가 아직 알지 못하는 보안취약점을 찾아서 이용하는 사례의 경우 문제는 더욱 심각해진다.

연방헌법재판소는 IT 기본권을 창설한 계기가 되었던 2008년 온라인수색 판결에서 IT 보안취약점을 개방해 놓는 이익과 일반적 IT 보안의 이익 사이에 목적충돌을 언급한 바 있다.[74] 연방헌법재판소는 지금까지 알려지지 않은 운영시스템의 보안상의 결함이 침입에 이용된다면, 성공한 접근의 공익과 정보기술시스템의 중대한 보안의 이익 사이에 목적충돌을 야기할 수 있다고 하였다. 그리하여 수사기관이 그러한 보안상의 결함을 제거하는 조치를 하지 않거나 심지어 그 결함이 알려지지 않도록 적극적으로 노력하게 될 위험이 있다고 하였다. 따라서 시민들은 높은 수준의 정보기술의 보안을 위해 국가가 가능한 노력해야 한다고 신뢰하고 있는데, 그러한 목적 충돌은 시민들의 이러한 신뢰를 침해할 수도 있다고 지적하였다.[75]

그 동안 연방정부는 보호의무의 관점에서 항상 IT 보안을 장려하고 보호하고 있음을 천명해 왔다. 특히 연방내무부는 2016년 독일의 사이버안전전략에서 국가의 직무는 자유와 안전을 보장하는 것이며 이는 사이버 공간에도 적용되어야 하므로 국가는 사이버 공간에서 발생하는 위협으로부터 시민을 보호해야 한다고 밝히고 있다.[76]

---

72) Hoffmann-Riem, JZ 2008, 1009 (1019).

73) Becker, NVwZ 2015, 1335 (1339 f.); Hoffman-Riem, JZ 2008, 1009 (1013 f.); Kutscha, NJW 2008, 1042 (1044); Roßnagel/Schnabel, NJW 2008, 3534 (3535); Sachs/Krings, JuS 2008, 482 (486).

74) BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07.

75) BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07, Rn.241.

76) 우리 정부도 사이버위협에 대응하여 사이버 공간에서 국민이 안전하고 자유롭게 활동할 수 있도록 보장하기 위하여 '국가사이버안보전략'을 2019년 4월 3일 발표하였다. 이 전략은 국민을 위한 사이버안보의 3대 기본원칙으로 국민의 기본권 보장, 법치주의에 기반을 둔 안보활동의 전개, 국민의 참여를 보장하는 투명한 사이버 안보의 실현을 천명하고 있다. 국가사이버안보전략은 특히 국민의

이러한 배경에서 국가기관이 온라인수색이나 암호통신감청과 같은 처분을 가능하도록 하기 위해서 보안취약점을 계속 유지하는 것은 IT 보안에 대한 이러한 국가의 노력들과 모순된다.[77] 보안취약점의 유지 이용은 IT 보안의 일반적인 위협을 의미할 수 있다. 현재 정보기술의 취약점을 제삼자가 이용하지 않도록 통제할 가능성이 알려져 있지 않기 때문에[78] 그러한 위협(threat)은 구체적 위험(risk)으로 발전될 개연성이 있다.[79] IT 보안의 취약점을 의도적으로 알게 됨으로써 어떠한 손해가 발생할 수 있는지는 지난 2017년 5월 발생한 WannaCry 사건이 잘 보여주고 있다. 악성프로그램 WannaCry는 전세계적으로 짧은 시간에 대규모 손해를 야기하였고 여기에는 국가기간통신망(정보통신기반시설)도 포함되었다.[80] 그밖에도 미국의 정보기관 NSA가 수년간 보안취약점을 알고 있었지만 제작자나 국민에게 통지하지 않고 이를 토대로 침입소프트웨어를 개발하였다는 사실도 보안취약점의 위험성을 잘 말해 주고 있다.

최근 IT 보안 연구는, 취약점을 체계적으로 발견하여 제거하는 것이 전적으로 가능하다는 것을 보여준다.[81] 그리고 국가가 전체 취약점을 항상 해결할 수는 없다 하더라도 적어도 국가에게 IT 보안을 최적화할 의무가 있다. 따라서 국가가 보안취약점을 장기간 개방해 놓고 이를 알리지 않거나 해결하지 않고 방치하는 경우 야기되는 IT 보안의 침해는 기본적으로 IT 기본권의 보호의무와 일치할 수 없다.

IT 보안에 대한 이익이 헌법을 통해서 보호되는 다른 권리와 이익형량을 통해서 후순위로 물러나야 하는 사례들만 헌법적으로 정당화될 수 있다. 하지만 이를 위해

기본권 보장과 법치주의에 기반을 둔 안보활동을 적시하고 있으므로 비록 법적 규범력을 갖지는 않지만 국가차원의 사이버안보 정책의 최상위 지침서로 사이버위협에 대응하는 국가의 기본 방향이라는 점에서 상당한 의미를 가진다(청와대 국가안보실, 국가 사이버안보전략). (https://bit.ly/2wrSZ1A)

77) 동일한 견해로는 다음 참조 : Blechschmitt, MMR 2018, 361 (365); Heim, NJW-Spezial 2018, 120.

78) Pohlmann/Riedel, DuD 2018, 37 (43).

79) IT 보안 연구에서 위협은 위험을 일으킬 소지가 다분한 요소를 말하며, 위험은 위협 요소가 일으킬 수 있는 피해를 의미한다.

80) Vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2018, 13.

81) Stock/Pellegrino/Li/Backes/Rossow, Proceedings of the 25th Annual Symposium on Network and Distributed System Security (NDSS '18), 2018(https://publications.cispa.saarland/1190/).

서 적어도 법적인 기본조건이 필요하다. 현재 국가기관의 보안취약점의 취급에 관한 검토할 말한 기준이 마련되어 있지 않기 때문이다. 그 기준은 발견된 보안취약점이 어떤 상황에서 비밀로 유지될 수 있는지 그리고 언제 공개되어야 하는지를 규정하는 것이어야 한다. 이에 상응한 기준들은 기본적으로 보안취약점과 이로부터 나오는 위험의 비중 그리고 이를 이용하려는 국가 목적의 비중에 초점을 두어야 한다.[82] 장래 이에 상응한 기준을 마련하는 경우 IT 보안의 이익이 항상 다른 보안이익보다 후순위로 물러나야 한다는 일반적인 가정은 유지될 수 없다. 왜냐하면 IT 보안은 다른 중요한 법익의 보호와 연결되어 있다는 점에 유의해야 하기 때문이다. 예를 들어 국가기간통신망을 위한 IT 보안의 보장(예컨데 원자력발전소)은 생명 및 신체의 안전성 보호를 위해서 필요하다.[83] 또한 IT 보안은 가령 학술연구의 자유, 표현의 자유, 직업의 자유과 같은 다른 기본권을 행사하기 위한 조건이 된다.[84]

따라서 현재의 상황에 따르면 온라인수색과 암호통신감청을 수행하기 위해서 IT 보안취약점을 제거하지 않고 의도적으로 개방해 놓는 것은 IT 기본권에서 도출되는 국가의 보호의무와 기본적으로 일치하기 어렵다고 판단된다. 결국 IT 보안취약점을 이용하는 방법은 기본권 차원에서나 형사소송법의 부수처분의 허용기준에 의하더라도 정당화될 수 없다고 본다.

V. 결론 및 시사점

1. 결론

온라인수색과 암호통신감청을 수행하기 위해서는 감시소프트웨어가 우선 설치되어야 한다. 하지만 권한 규정들은 이의 설치방법에 대해서는 아무런 언급을 하지

82) 이러한 제안에 대해서는 Herpig, Schwachstellen-Management für mehr Sicherheit, 2018 (https://bit.ly/2HLEEnl).

83) Wischmeyer, Die Verwaltung 50 (2017), 155 (162).

84) 이러한 쟁점에 대해서는 이상학, 사이버정보활동의 기본원칙과 한계, 법학연구, 2014.5.30., 411-415면 참조.

않고 있다. 따라서 다양한 설치방법들이 주처분에 수반되는 부수권한으로 허용되는지 검토하였다. 검토의 대상으로 삼은 주거 출입을 통한 방법, 기망을 통하여 착오에 빠진 이용자를 이용하는 방법, IT 보안취약점을 이용하는 방법들의 해석론은 기본권 차원에서 이를 정당화하기에 상당한 의문이 제기되는 것으로 판단된다.

입법론적으로도 이러한 부수처분이 정당화될 가능성도 상당히 제한적인 것으로 보인다. 앞서 언급한 바와 같이 현재 주거 출입을 통한 방법은 경찰단계에서 논의되고 있다.[85] 하지만 주거 출입 방법은 주거의 불가침이라는 기본권 침해를 추가로 야기하기 때문에 입법론적으로 특히 헌법상 요청을 충족해야 할 것이다.[86]

이용자를 적극적으로 기망하여 착오에 빠지게 한 다음 정보기술시스템에 접근하게 하는 것은 주거 출입보다 더 정당화하기 어려워 보인다. 속이는 행위와 허위정보 유포를 위한 법적 근거를 만드는 것은 국가의 정보 활동에 대한 신뢰를 일반적으로 흔들기에 충분하다. 따라서 국가질서의 근본토대가 위험에 처하게 될 수 있다. 모든 국민이 이메일에 첨부된 감시소프트웨어를 우려해야 한다면, 이것은 또한 전자정부의 구상에 따른 행정과도 부합하기 어려울 수 있다.

마지막으로 IT 보안취약점을 방치해 두는 것도 마찬가지로 정당화되기 어려워 보인다. 현재 이를 위한 적합한 규정이 존재하지 않는다. 이를 허용하는 규정들은 엄격한 한계 내에서만 IT 기본권과 일치할 수 있을 것이다. 따라서 IT 취약점의 획득 및 보존, 비밀유지, 방치를 위한 기준이 마련되어야 하고 그것은 구속력이 있어야 할 것이다. 국가의 IT 보안취약점 취급에 관한 구체적인 규정은 IT 보안법의 추가적인 발전과 함께 고려되어야 할 것이다.

2. 시사점

현재 우리는 독일과 같이 온라인수색이나 암호통신감청과 같은 비밀처분을 범죄예방이나 수사목적으로 두고 있지 않다. 정보통신기술의 발전에 따라서 범죄의 수법도 나날이 발전하고 있으므로 수사기관이나 예방기관도 이에 걸맞는 비밀처분이

85) 앞의 각주 42) 참조.

86) Vgl. Soiné, NStZ 2018, 497 (501).

필요하다. 따라서 이러한 종류의 비밀처분의 도입에 관한 논의가 요구된다. 필자는 이미 선행연구를 통하여 암호통신감청의 헌법적 정당성을 도출하고 현행 통신비밀보호법은 암호통신감청을 포섭할 수 없으므로 그 입법 방향과 한계를 제시하였다.[87] 이러한 논의는 기본적으로 온라인수색에도 전용할 수 있다고 본다. 암호통신감청과 온라인수색은 그 기원이 같고 기능도 거의 유사하기 때문이다.[88]

그런데 현재 독일의 온라인수색과 암호통신감청을 수행하기 위한 부수처분을 검토한 결과 주거 출입을 통한 방법, 기망을 통하여 착오에 빠진 이용자를 이용하는 방법, IT 보안취약점을 이용하는 방법들은 기본권 차원에서 이를 정당화하기 어려운 점이 발견되었다. 이들을 제외한 다른 부수처분들은 형사소송법상 수사의 일반조항이나 경찰법상 경찰활동의 일반조항 그리고 기본권 차원에서도 허용된다. 예를 들어 물리적인 접근 방법으로서 수사기관이나 보안기관이 출입국 시 세관통제나 기타 교통 통제 처분과 관련하여 대상자의 모바일 기기에 접근하는 방법, 고의 없는 제삼자를 도구로 이용하여 물리적으로 침입하게 하는 방법(예를 들어 회사의 동료가 판촉물로 받은 USB 칩으로 대상 컴퓨터를 감염시키는 경우) 등이 있다. 또한 원격 접근 방법으로는 수사기관이나 보안기관이 소프트웨어제작자나 전기통신사업자의 협력을 통하여 해당 IT 시스템에 접근하는 방법, 감시소프트웨어에 감염된 첨부파일을 이메일과 함께 대상자에게 송신하여 설치하는 방법, IT보안취약점을 이용하는 방법을 제외한 국가트로이목마나 원격 포렌식 소프트웨어를 통해서 설치하는 방법 등이 있다. 하지만 이러한 방법만으로는 암호통신감청이나 온라인수색의 목적을 달성하기에는 사실상 상당히 미흡하다. 특히 국가트로이목마나 원격 포렌식 소프트웨어를 통해서 해당 시스템에 접근하여 설치하는 방법은 IT 시스템의 보안취약점을 이용하는 방법이 대부분이기 때문이다. 하지만 부수처분이 주처분에 버금가거나 다른 기본권을 침해하게 되는 경우에는 이에 상응한 수권규정이 필요하다. 앞서 언급한 주거 출입을 통한 방법, 기망을 통하여 착오에 빠진 이용자를 이용하는 방법, IT 보안취약점을 이용하는 방법들이 여기에 해당되는 것으로 보인다.

따라서 우리의 도입 논의에서는 추가적인 기본권 침해가 예상되는 부수처분에 대

87) 박희영, 앞의 논문, 형사정책연구 제29권 제2호(통권 제114호, 2018 ·여름), 42-53 참조.
88) 온라인 수색의 입법 방향에 대한 상세한 논의는 다음 기회로 미룬다.

해서는 비례성원칙을 고려한 보다 엄격한 요건이 필요하다. 이글에서 검토한 헌법상 기본권을 고려한 부수처분들과 기준들은 범죄수사나 범죄예방에 모두 적용될 수 있으므로 개별 수권 규정의 요건을 정하는데 참조할 수 있을 것이다.

참고문헌

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

박희영, 국가의 합법적인 해킹행위로서 온라인 수색에 관한 독일 법제 동향, 최신외국법제정보 2019 제1호, 한국법제연구원, 55-73.

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

박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018 ·여름), 28-31.

박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 160-164.

이상학, 테러방지 수권규정과 기본권침해의 한계 - 독일연방수사청법의 테러방지 권한에 대한 연방헌법재판소의 판결(2016.4.20.) 검토를 중심으로, 공법학연구 제17권 제3호, 109-134.

이상학, 사이버정보활동의 기본원칙과 한계, 법학연구, 2014.5, 407.

정문식, 테러방지 감시조치에 대한 위헌심사기준 - 독일연방헌법재판소 연방사법경찰청법(BKAG) 결정을 중심으로, 법과 정책연구, 제18권 제2호, 2018, 6. 3-43.

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

홍선기/강문찬, 테러방지법상 국정원 정보수집권한에 대한 개정논의 - 최근 독일 연방헌법재판소의 판결과의 비교검토, 법과 정책연구 제17권 제3호, 2017.9.

홍영기, Nemo tenetur-원칙, 고려법학 제66호 2012년 9월, 고려대학교 법학연구원, 305-338.

Bär, Wolfgang, in Anmerkung zu AG Bayreuth MMR 2010, 266 (268)

Becker, Florian, Grundrechtliche Grenzen staatlicher Überwachung zur

Gefahrenabwehr, NVwZ 2015, 1335-1340.

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter, Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, 361- 366.

Buermeyer, Ulf, Zum Begriff der "laufenden Kommunikation" bei der Quellen-Telekommunikationsuberwachung ("Quellen-TKU"), StV 2013, S. 470.

Derin, Benjamin/Golla, Sebastian, Der Staat als Manipulant und Saboteur der IT-Sicherheit?, Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung“ und Quellen-TKÜ, NJW 2019, 1111-1116.

Freiling, Felix/Safferling, Christoph/Rückert, Christian, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9－22.

Gercke, Björn Überwachung der Telekommunikation － von der Ausnahme zur Regel,

Heim, Maximilian, Staatstrojaner im Einsatz, NJW-Spezial, 2018, 120.

Hiéramente, Mayeul, Telekommunikationsüberwachung und Cloud Computing, StraFo 9/2015, S. 365-374.

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009-1022.

Kutscha, Martin, Das „Computer-Grundrecht“ ― eine Erfolgsgeschichte?, DuD 2012, 391 (394).

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042-1044.

Müller, Wolfgang/Römer, Sebastian, Legendierte Kontrollen - Die gezielte Suche nach dem Zufallsfund, NStZ 2012, 543-547.

Nowrousian, Bijan, Darf der Beschuldigte im Ermittlungsverfahren getäuscht

werden? - Zur grundsätzlichen Zulässigkeit aktiver Täuschung im Ermittlungsverfahren, NStZ 2015, Heft 11, 625-628.

Pohlmann, Norbert/ Riedel, Rene, Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen, DuD 2018, 37-44. (zit.: Pohlmann/Riedel, DuD 2018, 37)

Roggan, Frederik Die „Technikoffenheit“ von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen. Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, NJW 2015, 1995-1999.(zit.: Roggan, NJW 2015, 1995)

Roggan, Frederik, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, 821-829.

Roggan, Fredrik, Das neue BKA-Gesetz - Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, NJW 2009, 257-262.

Roßnagel, Alexander/Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534-3538.

Sachs, Michael/Krings, Thomas, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, JuS 2008, 481-486. (zit.: Sachs/Krings, JuS 2008, 481)

Sankol, Barry Überwachung der Internet-Telefonie: Ein Schatten im Lichte der §§100a ff. StPO, CR 2008, 13-18. (zit.: Sankol, CR 2008, 13)

Schmalenbach, Kirsten, Wenn der Staat lügt: Desinformation im demokratischen Rechtsstaat NVwZ 2005, Heft 12, 1357-1361.

Schneider, Hartmut, Zur Zulässigkeit strafprozessualer Begleitmaßnahmen im Zusammenhang mit dem Abhören des nicht öffentlich gesprochenen Wortes, NStZ, 1999, 388-391. (zit.: Schneider, NStZ 1999, 388)

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer

Ermittlungsmaßnahmen - Telekommunikation, Web 2.0., Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593-606. (zit.: Singelnstein, NStZ 2012, 593).

Singelnstein, Tobias/ Derin, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. Was aus der StPO-Reform geworden ist, NJW 2017, 2646-2652. (zit.: Singelnstein/Derin, NJW 2017, 2646)

Soiné, Michael, Die strafprozessuale Online-Durchsuchung, NStZ 2018, Heft 9, 497-504.

Soiné, Michael, Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder NVwZ 2012, 1585-1589.

Soiné, Michael, Kriminalistische List im Ermittlungsverfahren, NStZ 2010, Heft 11, 596-602.

Tinnefeld, Die "Staatstrojaner" aus verfassungsrechtlicher Sicht - Gedanken zum ... Landesbeauftragten für den Datenschutz, ZD 2012, 451 (454).

The Admissibility and Limitations of Accompanying Measures to Quellen TKÜ and Online-Durchsuchung*

Park, Hee-young**·Lee, Sang-hak***

As the development of information and communication technology has led to the development of crime techniques day by day, investigative agencies and preventive agencies need to dispose of them appropriately. To this end, Germany introduced the online search(Online-Durchsuchung) and source telecommunications surveillance(Quellen-TKÜ) to the criminal procedure law and police law respectively.

Surveillance software must be installed to perform Online-Durchsuchung and Quellen-TKÜ. However, the regulations do not mention how to install them. Therefore, various installation methods should be examined. The focus of the examination is on how to use residential access, how to manipulate users who are misled by deception, and how to use IT security vulnerabilities. The interpretation of these regulations seems to raise considerable questions to justify them at the basic level. Legislative theories, it seems that the possibility of justifying these dispositions is also very limited. And the possibility of justifying the legislation of subsidiary disposal appears to be limited.

In the future, koreanr legislators are also expected to discuss on-line search or cryptographic communication eavesdropping in response to serious crimes such as terrorist crimes. In particular, the Korean Constitutional Court ruled that so-called packet inspection could not be allowed and urged legislation thereon. Quellen-TKÜ

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2016S1A5A2A03927806).

** Researcher, Max Planck Institute for Foreign and International Criminal Law, Germany, PhD in Law.

*** Professor, Daegu University, PhD in Law, Corresponding Author.

could be its alternative. These will have to be discussed at the same time as Online-Durchsuchung and Quellen-TKÜ use the same monitoring software.

However, preliminary disposition to carry out Online-Durchsuchung and Quellen-TKÜ may infringe fundamental rights. Therefore, in our introduction discussions, it seems that more stringent requirements are needed for the disposal of these.

❖ key words: online search(Online-Durchsuchung), source telecommunications surveillance(Quellen-TKÜ), IT vulnerabilities(IT-Sicherheitslücken), IT-Grundrecht, Der nemo tenetur Grundsatz, Annexkompetenz, Begleitmassnahme, kriminalistischen List, Täuschungsverbot, Desinformation

투고일 : 5월 31일 / 심사일 : 6월 24일 / 게재확정일 : 6월 24일