

## 인공지능 음성비서를 통한 주거감시의 허용과 입법 방향\*

박희영\*

### 국 | 문 | 요 | 약

스마트 홈(smart home) 환경에서 인공지능 음성비서가 핵심적인 기능을 수행하고 있다. 하지만 음성비서가 주로 개인의 주거에 설치된다는 점에서 사생활의 핵심영역이 침해될 위험이 있다. 서비스 제공자의 인공지능 서버에 저장되어있는 개인의 사생활영역에 관한 디지털 정보가 음성비서를 통해서 기술적으로 쉽게 접근될 수 있기 때문이다. 인터넷과 연결되어있는 음성비서에 접근하게 되면 음성비서 자체에 저장되어있는 데이터는 물론 서비스 제공자의 인공지능서버에 저장되어있는 이용자의 데이터에도 접근이 가능하다(온라인 수색). 또한 음성비서에 설치되어 있는 마이크를 작동하면 주거 내에 있는 사람의 대화나 사람과 음성비서 사이의 대화가 청취되거나 녹음될 수 있고(음성주거감시), 음성비서가 수행하는 전기통신이 감청될 수도 있다(전기통신감청). 이처럼 음성비서를 둘러싸고 수사절차상 다양한 문제가 제기될 수 있다.

이 글은 이러한 다양한 문제 중에서 음성비서를 통한 주거감시가 현행법에서 허용될 수 있는지를 다루었다. 이 글에서 '음성비서를 통한 주거감시'란 수사기관이 음성비서에 비밀리에 접근한 후 마이크를 작동하여 주거 내에서 행해지는 대화를 녹음하거나 청취하는 수사방법으로 이해하였다. 현행 통신비밀보호법의 전기통신감청이나 비공개 대화의 청취 및 녹음에 관한 규정은 이러한 주거감시를 허용하고 있지 않다. 독일 형사소송법은 우리와 달리 암호전기통신감청과 온라인 수색을 통하여 음성비서와 같은 정보기술시스템에 대한 접근을 허용하고 있다. 하지만 이러한 비밀 수사처분도 음성비서를 통한 주거감시를 포섭하기 어려웠다. 그럼에도 불구하고 독일 형사소송법의 음성주거감시와 비밀 온라인 수색 규정의 요건들은 음성비서를 통한 주거감시의 규정이 어떠한 내용을 갖추어야 하는지 그 방향을 제시해 주고 있다. 이를 통해서 음성비서를 통한 주거감시의 요건을 도출할 수 있기 때문이다.

DOI : <https://doi.org/10.36889/KCR.2021.3.31.1.33>.

❖ 주제어 : 인공지능 음성비서, 온라인 수색, 암호통신감청, 주거감시, 주거내 음성감시, 사생활의 핵심영역

\* 이 논문은 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임.  
(NRF-2019S1A5A2A01046918).

\*\* 독일 막스플랑크 국제형법연구소 연구원, 법학박사.

## I. 문제 제기

정보통신기술의 발전으로 우리 사회의 대부분이 디지털화되고 있다. 개인의 사생활영역도 디지털화되어 디지털 데이터로 존재한다. 정보통신기술이 조성한 디지털 환경에서 인공지능(AI)과 연결되어있는 디지털 기기는 데이터의 수집 및 처리에 중요한 역할을 하고 있다. 특히 이러한 디지털 기기가 전통적인 주거에 통합되면서 ‘스마트 홈’(smart home)이라는 새로운 모습의 주거 형태가 탄생하였다. 스마트 홈은 다양한 종류의 스마트 디지털 기기들이 사물인터넷으로 연결되어 이용되고 있다. 스마트 홈에서 핵심적인 기능을 하는 디지털 기기는 디지털 음성비서<sup>1)</sup>라고 할 수 있다. 음성비서는 클라우드를 기반으로 하는 서비스 제공자의 인공지능서버와 연결되어 기존의 사물인터넷 기기들은 물론 스마트 디지털 기기들을 서로 연결하는 인터페이스 역할을 함으로써 현재의 스마트 홈 환경에서 저점 디바이스(허브)가 되고 있기 때문이다.

음성비서와 같은 디지털 기기가 스마트 홈에 통합되어 우리에게 편리함과 다양한 혜택을 주고 있지만,<sup>2)</sup> 음성비서가 주로 개인의 주거나 사무실 또는 자동차에 설치된다는 점에서 사생활의 핵심영역이 침해될 위험이 있다. 인공지능 서버에 디지털 데이터로 보관되어있는 개인의 사생활영역에 관한 정보가 음성비서를 통해서 기술적으로 쉽게 접근될 수 있기 때문이다. 특히 음성비서와 같은 디지털 기기는 이용자와 기기 사이의 상호작용 과정에서 이용자가 자신의 사생활영역을 무의식적으로 지속적으로 기기에 기록하고 저장하여 사생활을 수시로 침해할 수 있는 위험성을 가지고 있다.<sup>3)</sup>

이러한 위험에도 불구하고 사생활 보호 및 보안과 관련한 법적 규제와 정책은 아직

1) 인공지능 가상 비서, 인공지능 개인 비서, 스마트 스피커, 인공지능 스피커 등 다양한 이름으로 불리고 있다. 현재 대표적인 5대 디지털 음성비서로는 삼성의 빅스비(Bixby), 아마존의 알렉사(Alexa), 애플의 시리(Siri), 구글의 어시스턴트(Assistant), 마이크로소프트의 코르타나(Cortana) 등이 언급되고 있다.

2) 예를 들어 취침 명령을 내리면 TV나 조명이 자동으로 꺼지고 침대 매트리스는 취침모드로 전환되고 특정한 요리 명령을 내리면 LG 냉장고 모니터에서 동영상이 재생될 뿐 아니라 영화 관람 명령을 내리면 벽면의 대형 스크린이 내려와서 커튼이 창문을 가리면서 영화를 볼 준비를 해 준다. 이것은 구글의 음성인식 기능을 사용한 한샘과 LG전자가 최근 구글과 합작한 스마트홈 모습이다(한국경제, 2019.2.20. 기사, <https://bit.ly/2IBxq7w>).

3) 이를 ‘프라이버시 로깅’(privacy logging)이라 한다. 심홍진, 인공지능(AI)과 프라이버시의 역할 : AI 음성비서를 중심으로, 정보통신정책연구원, 2018.12. 9.

충분히 마련되어 있지 않다. 게다가 인공지능 디지털 기기 제조사의 데이터 수집 및 사용에 대한 지침도 명확하지 않다. 따라서 클라우드 기반의 인공지능서버와 연결되어 있는 음성비서를 포함한 디지털 기기로 구성되는 스마트 홈 환경은 보안의 취약성으로 말미암아 해커의 공격에 쉽게 노출될 뿐 아니라,<sup>4)</sup> 포괄적 주거감시에도 이용될 위험이 있다. 특히 인터넷과 연결되어있는 음성비서에 접근하게 되면 음성비서 자체에 저장되어 있는 데이터는 물론 서비스 제공자의 인공지능서버에 저장되어있는 이용자의 데이터에도 접근이 가능하며(온라인 수색), 음성비서에 설치되어있는 마이크를 작동하면 주거 내에 있는 사람의 대화나 이용자와 음성비서 사이의 대화가 청취되거나 녹음될 수 있고(주거내 음성감시), 음성비서가 수행하는 전기통신이 감청될 수도 있다(전기통신감청). 나아가서 클라우드 기반의 인공지능서버에 저장되어 있는 데이터를 스트리밍으로 청취할 수도 있다(증거 또는 증인). 이처럼 음성비서를 둘러싸고 수사절차상 다양한 문제가 제기될 수 있다.

이 글은 음성비서가 제기하는 다양한 문제 중 수사기관이 음성비서에 비밀리에 접근한 후 마이크를 작동하여 주거 내에서 행해지는 대화를 녹음하거나 청취하는 ‘주거감시’ 또는 ‘주거내 음성감시(=음성주거감시)’가 현행법에서 허용되는지를 검토한다(Ⅲ.). 음성비서가 주거감시를 위한 기기로 사용되어 헌법상 주거의 불가침 기본권을 침해할 수 있기 때문이다. 만일 현행법이 이러한 주거감시를 허용하지 않는다면, 정보통신기술의 발전에 대응하여 유사한 비밀처분을 이미 도입하고 있는 독일의 법적 논의 상황을 비교법적으로 검토한 다음(Ⅳ.), 음성비서를 통한 주거감시의 입법 방향을 제시해 본다(Ⅴ.). 이러한 논의를 위해서 먼저 음성비서와 관련된 기술적 기능을 간단하게 설명한다(Ⅱ.).

## Ⅱ. 음성비서의 기능과 수사기관의 접근 방법

### 1. 음성비서의 구조 및 기능

인공지능 음성비서는 음성신호를 수집하고 분석하여 음성신호의 맥락에 따라 배치한

4) 사물인터넷으로 연결되어 있는 베이비 모니터, 반려동물용 IP카메라 해킹은 어렵지 않게 발생한다.

다음 이에 응답하는 소프트웨어의 일종이다. 이 소프트웨어는 주로 스마트 스피커나 스마트폰에 설치되어 음성비서의 제작자나 서비스 제공자의 인공지능서버와 연결시켜 준다. 따라서 스마트 스피커에 설치되어있는 음성비서는 음성을 입력하는 마이크, 명령에 따라 반응하는 스피커 그리고 인터넷과 항상 연결을 유지하는 컴퓨터 칩으로 구성된 간단한 시스템이다. 컴퓨터 칩은 항상 인터넷과 연결되어 특정한 명령어를 통해서 활성화 되도록 프로그램되어 있다.<sup>5)</sup>

음성비서의 마이크는 항상 켜져 있고 코드나 명령어에 따라서 주거 내의 음성을 청취하고 녹음할 수 있다. 음성비서는 명령에 반응하기 위해서 클라우드 기반의 서비스 제공자의 인공지능서버와 인터넷을 통하여 항상 접속되어 있다. 음성비서는 사용자가 있는 로컬에서 명령어만 처리한다. 따라서 음성비서가 수집하는 모든 음성정보는 서비스 제공자의 인공지능서버에 저장되고 음성비서 자체에는 이를 작동하기 위해 필요한 일부 정보만 저장된다. 예를 들어 아마존 알렉사의 경우 사용자가 명령을 내리면 이를 인식한 후 아마존의 인공지능서버로 전달한다. 이용자의 명령은 일단 음성데이터로 저장되었다가 이후에 이용자가 접근할 수 있도록 문자로 변환되어 보관된다. 이용자는 또한 자신의 계정으로 인공지능 서버에 접근하여 모든 과정을 스트리밍으로 다시 확인할 수 있다.

음성비서의 기능은 다양하다. 음성비서는 일반적으로 정보 검색, 전화 걸기, 예약 및 주문, 일기예보제공, 기억해야 할 것을 저장하여 상기시켜 주는 일 등을 제공한다. 그뿐만 아니라 음성비서는 이용자와 대화를 한다. 예를 들어 이용자가 음악을 요청하면 이를 검색하여 재생하고(기능적 대화), 고민거리나 상담에 응하게 된다(감성적 대화). 음성비서의 이러한 기능을 통해서 주거 내에서 이루어지는 개인의 사생활의 핵심영역에 관한 대화들이 디지털 데이터로 처리되어 제공자의 인공지능 서버에 보관된다. 따라서 주거에서 범죄가 발생하였고 그곳에 음성비서가 작동하고 있었다면 인공지능서버에 범죄와 관련한 디지털 증거들이 저장되어 있을 개연성이 있다. 이 때문에 수사기관이 이러한 디지털 증거에 관심을 가지는 건 당연하다. 이러한 문제는 이미 미국에서 발생하였다.<sup>6)</sup>

5) Gless, StV 2018, S.671.

6) 살인과 관련한 증거가 아마존 에코의 서버에 저장되어 있는 것으로 간주하여 수사기관과 법원이 관련 데이터의 제출을 요구한 미국의 사건으로는 다음 참조 : State of Arkansas v. James A. Bates, Case No. CR-2016-370-2, <https://regmedia.co.uk/2017/02/23/alexa.pdf>, State of New Hampshire v. Timothy Verrill, Case No. 219-2017-CR-072, <https://www.courts.state.nh.us/caseinfo/pdf/Verrill/110518Verrill-order.pdf>.

## 2. 수사기관의 음성비서에 대한 접근 방법

수사기관은 일반적으로 형사소송법의 공개수사인 압수수색을 통해서 이용자의 음성비서에 접근할 수 있다. 하지만 이용자가 수사기관의 접근을 거부하는 경우(예를 들어 아이디와 비밀번호의 제출 거부) 수사기관은 음성비서 서비스 제공자에게 데이터를 요청하거나 압수수색을 통해서 데이터를 수집할 수 있다. 하지만 서비스 제공자가 해외에 있는 경우에는 국제사법공조를 통해야 한다. 이 방법은 시간이 너무 오래 걸리고, 특히 디지털 데이터는 적시에 수집되어야 하는 특성상 수사기관의 입장에서는 적절한 방법이 아니다.

따라서 이용자나 제공자의 동의를 얻지 못하거나 압수수색이 어려운 경우에는 이용자의 음성비서에 비밀리에 접근해야 한다. 이러한 방법에는 컴퓨터 시스템의 취약점을 이용하는 제로 데이 익스플로이트(Zero Day Exploit)<sup>7)</sup>나 제조자가 필요에 따라 임시로 만들어 놓은 백도어를 이용하거나 원격조정 해킹 프로그램인 감시소프트웨어<sup>8)</sup>를 사용하는 방법이 있을 수 있다. 또한 이용자 몰래 주거에 물리적으로 침입하여 음성비서에 감시소프트웨어를 설치할 수도 있다.<sup>9)</sup> 일단 음성비서에 비밀리에 접근하였다면 마이크를 작동함으로써 음성비서를 통한 주거감시가 가능하다.

## Ⅲ. 현행법상 음성비서를 통한 주거감시의 허용 여부

인공지능 음성비서에 비밀리에 접근하여 마이크를 작동하여 주거 내의 대화를 청취 및 녹음하는 감시행위와 관련하여 검토될 수 있는 규정들은 형사소송법에는 존재하지 않는다. 하지만 통신비밀보호법의 전기통신감청(제5조 이하)과 타인간의 비밀 대화의 청취 및 녹음(제14조 제2항)에 관한 비밀처분이 음성비서를 통한 주거감시를 허용하는지 검토한다.

7) 익스플로이트란 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격을 말한다.

8) 예를 들어 독일의 국가 트로이 목마(Trojaner).

9) 감시소프트웨어의 설치 방법에 대해서는 박희영·이상학, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호(통권 제118호), 2019. 여름, 120-123면.

## 1. 통신비밀보호법의 전기통신감청

감시소프트웨어를 통하여 음성비서에 몰래 접근한 후 마이크를 작동하여 주거 내의 대화를 청취 및 녹음하는 행위가 전기통신감청규정에 포섭될 수 있는지는 감청의 개념과 관련하여 살펴볼 수 있다.

### 가. 전기통신감청의 개념

통신비밀보호법에 따르면 ‘통신’이란 우편물 및 전기통신을 말하고(제2조 제1호), ‘전기통신’이란 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음성·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다(제2조 제3호). 이러한 전기통신의 개념은 전기통신기본법(제2조 제1호)과 전기통신사업법(제2조 제1호)의 기술적인 전기통신의 개념을 따르고 있다. ‘감청’이란 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치 등을 사용하여 통신의 음성·문언·부호·영상을 청취·공독(共讀)하여 그 내용을 지득(知得) 또는 채록(採錄)하거나 전기통신의 송·수신을 방해하는 것을 말한다(제2조 제7호). 감청의 개념에서 ‘당사자의 동의 없이’라는 문언으로 기술적인 전기통신의 범위가 어느 정도 규범적으로 제한된다.

하지만 헌법재판소는 이러한 전기통신의 보호범위를 규범적으로 더욱 제한하고 있다.<sup>10)</sup> 헌법재판소 결정<sup>11)</sup>에 따르면 ‘통신’이란 ‘비공개적이고 쌍방향적인 의사의 교환’을 의미하므로 송신자와 수신자, 즉 당사자를 전제로 한다. 따라서 전기통신도 당사자가 전제되어야 한다. 또한 전기통신감청은 ‘통신이 현재 이루어지고 있는 동안’<sup>12)</sup> 당사자 사이의 통화내용을 엿듣고 이를 청취 또는 녹음하는 것이다. 즉 통신의 내용이 당사자(즉 송신자와 수신자)의 지배영역을 벗어나서 통신사업자의 지배영역에 있는 상태를 말하며 ‘송신 및 수신 완료되기 전’을 의미한다. 따라서 송수신이 완료된 상태에서 통신 내용의 지득 행위는 논리적으로 감청개념에 해당되지 않는다.<sup>13)</sup> 송신과 수신 완료된

10) 통신비밀보호법의 전기통신의 개념에 대한 비판에 대해서는 정배근/이경열, 독일 연방헌법재판소 결정을 통해 바라본 패킷감청 수사의 실질적 통제방안과 통신비밀보호법 신설조문 제12조의2 문제점, 비교형사법연구 제22권 제2호, 2020.7., 117면 참조.

11) 헌법재판소 2001.3.21. 2000헌바25 결정.

12) 대법원 2012. 7. 26. 선고 2011도12407 판결.

전기통신에 대하여 통신비밀보호법이 아닌 형사소송법의 압수, 수색 및 검증 규정이 적용된다. 이러한 집행 사실을 서면으로 통지하도록 한 통신비밀보호법 제9조의 3을 고려하면 이러한 해석이 가능하다.<sup>14)</sup>

이러한 점들을 고려하면 전기통신의 감청이란 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 현재 이루어지고 있는 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다고 할 수 있다.

## 나. 음성비서를 통한 주거감시에 적용

이러한 감청 개념에 따르면 음성비서에 비밀 접근하여 마이크를 작동하여 주거 내에서 행해지는 대화를 청취 및 녹음하는 행위는 감청에 포함하기 어려워 보인다. 우선 통신감청의 대상인 통신은 ‘현재 진행 중인 통신’을 전제로 한다. 따라서 음성비서에 몰래 접근하여 카메라를 작동시키는 행위는 대부분 현재 진행 중인 통신을 전제로 하지 않는다. 즉 현재 진행 중인 통신과 상관없이 주거 내 감시가 수행되기 때문이다.

또한 전기통신감청은 타인의 정보기술시스템에 대한 접근을 전제로 하지 않는다. 음성비서를 통한 주거감시는 일반적으로 세 단계로 수행된다. 감시를 수행하기 위해서는 피처분자의 정보기술시스템(여기서는 음성비서의 스피커)에 비밀리에 침입하여 감시소프트웨어가 설치되어야 하고, 마이크 기능을 활성화하여 감시가 시작되고, 감시의 종료 후 음성비서 기기에 설치된 감시소프트웨어를 제거 내지 삭제해야 한다. 이를 통해서 음성비서를 통한 주거감시는 해당 정보기술시스템에 접근해야 한다. 타인의 정보기술시스템에 접근하는 행위는 그 시스템의 내부를 들여다보게 되므로 통신비밀의 보호를 넘어서 일반적 인격권에서 도출되는 정보자기결정권과 IT 기본권,<sup>15)</sup> 나아가서 주거의 불가침과

13) 조국, 개정 통신비밀보호법의 의의, 한계 및 쟁점: 도청의 합법화인가 도청의 통제인가?, 형사정책연구 제15권 제4호(통권 제60호, 2004 겨울호), 107-108면; 김형준, 현행 통신비밀보호법의 문제점과 개선방안, 형사법연구 제24호(2005 겨울), 217면; 성선제, e-사회에서 테러 및 범죄예방을 위한 감청과 프라이버시의 갈등 조정 방안 연구, 공법연구 제8권 제4호(2007), 176면.

14) 대법원 관례는 수신이 완료된 전자우편의 기록이나 내용을 열어보는 등의 행위 태양은 통법법의 우편물에 대하여 당사자의 동의 없이 개봉하는 등의 행위를 규정한 ‘검열’에 가까운 것이지만, 전자우편의 검열은 통신제한조치 허가 등 위 법에 의한 규율대상에 포함되지 않는다고 보고 있다(대법원 2012. 7. 26. 선고 2011도12407 판결; 대법원 2012. 11. 29., 선고 2010도9007 판결 참조).

같은 기본권을 침해할 가능성이 있다. 하지만 전통적인 전기통신감청은 통신비밀보호만 관련된다. 따라서 타인의 정보기술시스템에 비밀리에 침입하여 소프트웨어를 설치하거나 제거하는 행위는 전통적인 전기통신감청에 포섭되기 어렵다. 물론 감청소프트웨어를 사용하여 데이터 패킷을 가로채는 소위 패킷감청 또는 인터넷회선감청<sup>15)</sup>은 기술적으로 전자장치를 이용한 감청에 포섭시킬 수 있다. 패킷감청이 피처분자의 정보기술시스템에서 수행되는 경우에는 암호통신감청에 해당될 수 있겠지만, 일반적으로 전기통신사업자의 지배영역에서 수행된다. 따라서 인공지능 음성비서를 통한 주거감시는 통신비밀보호법의 전기통신감청에 의해서 허용되지 않는다고 판단된다.

## 2. 통신비밀보호법의 타인의 비밀 대화 청취 및 녹음

### 가. 수사기관의 타인의 비밀 대화 청취 및 녹음

통신비밀보호법 제3조 제1항에 따르면 통신비밀보호법, 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 누구든지 전기통신의 감청과 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 이를 위반하여 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자는 동법 제16조 제1항 제1호에 따라서 처벌된다.

하지만 통신비밀보호법은 수사기관에게 타인간의 비밀 대화를 녹음하거나 청취할 수 있는 권한을 부여하고 있다. 동법 제14조 제1항에 따르면 누구든지 공개되지 아니한 타인간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 없지만, 제

15) IT 기본권은 독일 연방헌법재판소가 노르트라인 베스트팔렌주의 헌법보호법의 비밀 온라인 수색과 관련한 사건(BVerfG, Urteil vom 27. 2. 2008 - 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822-837)에서 새롭게 도입한 기본권으로 ‘정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권’의 줄임말이다. 이에 대해서 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1, 92-123 참조. 우리 헌법상 IT 기본권의 근거에 대해서는 박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호, 2012.9, 161-162면 참조.

16) 헌법재판소는 이러한 패킷감청은 헌법에 합치하지 않는다고 결정하였고(헌법재판소 2018. 8. 30. 선고 2016헌마263 결정) 이에 따라 통신비밀보호법 제12조의2가 신설되었다. 이 조항의 문제점에 대해서는 정배근/이경열, 독일 연방헌법재판소 결정을 통해 바라본 패킷감청 수사의 실질적 통제방안과 통신비밀보호법 신설조문 제12조의2 문제점, 비교형사법연구 제22권 제2호, 115면 이하 참조.

14조 제2항에 따르면 전기통신제한조치에 적용되는 규정들을 준용하여 타인의 비밀 대화를 녹음하거나 청취할 수 있는 예외를 허용하고 있다. 이 예외조항에 따라 수사기관은 공개되지 아니한 타인간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 있다. 녹음의 경우는 그 수단이 당연히 전제되므로 이것이 명시되어 있지 않지만, 청취의 경우는 전자장치 또는 기계적 수단이 이용되어야 한다. 따라서 예를 들어 창밖에서 귀를 대고 방안의 대화를 엿듣는 것은 청취에 포함되지 않는다.

한편 동법 제14조 제1항은 타인간의 대화 행해지는 장소를 구분하고 있지 않다. 즉 대화의 감시 장소가 주거 내인지 주거 외인지 구분하고 있지 않다. 주거 내에서의 대화의 녹음 및 청취는 사생활의 자유뿐 아니라 주거의 자유도 침해할 수 있다. 따라서 입법론적으로 주거내외를 구분하는 것이 적합하다. 하지만 제14조 제1항은 주거내 대화와 주거외 대화를 구분하지 않기 때문에 해석론으로는 모두 포함하는 것으로 볼 수 있다. 따라서 동법 제14조 제2항에 따르면 주거 내에서 행해지는 타인간의 비밀대화도 전자장치나 기계적 수단을 통해서 녹음하거나 청취할 수 있다.

#### 나. 음성비서를 통한 주거감시에 적용

우선 음성비서에 감시소프트웨어를 설치하는 것이 주처분인 대화의 녹음과 청취의 부수처분으로서 허용될 수 있는가이다.<sup>17)</sup> 통비법 제14조 제2항에 따르면 통신제한조치의 대상인 범죄의 경우 수사기관은 공개되지 아니한 타인간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 있다. 이 경우 통신제한조치에 관한 규정이 준용된다. 이러한 대화감시의 집행은 제9조 제1항에 따라서 이를 청구한 검사나 사법경찰관이 행한다. 하지만 구체적인 집행방법이 언급되어 있지 않다.<sup>18)</sup> 즉 수사기관이 주거 내의 피의자의 비밀대화를 녹음하거나 청취하기 위해서는 전자장치나 기계적 수단을 주거 내에 설치할 수 있는지 그리고 이를 설치하기 위해서 주거 내에 출입할 수 있는지(예를 들어 전기 수리공으로 위장하여)와 같은 부수처분에 대하여는 규정하고 있지 않다. 하지만 이러한 부수처분은 허용되어야 한다. 왜냐하면 이것이 허용되지 않는다면 제14

17) 부수처분의 허용 기준과 그 한계에 대해서는 박희영/이상학, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호(통권 제118호), 2019. 여름, 123-136면.

18) 이 점은 전기통신감청의 경우에도 마찬가지이다.

조 제2항은 수사실무에서 실효성이 크지 않기 때문이다. 즉 주거외부에서 전자장치나 기계적 수단을 이용하여 주거 내의 대화를 녹음하거나 청취하는 것은 현대의 주거구조의 측면에서 상당한 어려움이 있기 때문이다.

둘째, 전자장치 또는 기계적 수단의 이용이 음성비서에 감시소프트웨어를 설치하는 방법을 포섭할 수 있는지 문제가 된다. 음성비서에 감시소프트웨어를 설치하여 접근하는 방법은 피처분자의 정보기술시스템에 접근하는 것이므로 IT 기본권을 침해하게 된다. 하지만 전자장치 또는 기계적 수단은 피처분자의 소유가 아니라 수사기관의 소유에 속하고 이를 이용하는 행위는 다른 기본권을 추가로 침해하지 않는다. 그렇다면 전자장치 또는 기계적 수단의 이용을 음성비서에 감시소프트웨어를 설치하는 방법으로 유추 적용할 수 있는지 문제가 될 수도 있다. 우리 대법원 판례<sup>19)</sup>와 통설적 견해<sup>20)</sup>에 따르면 “형사소송법에서는 원칙적으로 피고인에게 불리한 유추가 금지되지 않는다”고 보고 있다. 하지만 유추적용으로 기본권을 침해하는 결과를 야기한 경우에는 유추적용은 허용되지 않는다고 보아야 한다.<sup>21)</sup>

셋째, 제14조 제2항은 대화의 청취 및 녹음만을 언급하고 있다. 여기서 대화란 적어도 두 사람의 의사 교환을 전제로 하므로 사람과 반려동물 사이의 대화, 독백, 노래 부르기, 흥얼거림, 소음, 신음소리<sup>22)</sup> 등은 여기에 포함되지 않는다. 따라서 이용자가 음성비서와 나누는 대화가 이 조항에서 말하는 대화인지도 의문이다. 만일 이 조항에 포섭된다고 하더라도 음성비서는 그 성능에 따라서 일정한 범위의 주거 내에서 행해지는 모든 음성이 감시될 수 있으므로 그 대상이 대화를 훨씬 넘어선다.

넷째, 제14조 제2항은 또한 영상감시는 언급하고 있지 않다. 통비법의 정의 규정(제2조 제3호)에 따르면 전자적 방식에 의하여 영상을 송수신하는 것도 전기통신에 포함된다. 따라서 화상통신으로 전달되는 영상도 전기통신의 감청대상이 될 수 있다. 예를 들어 카카오톡의 화상채팅이 감청되는 경우를 고려해 보면 스마트폰의 카메라의 촬영범위에

19) 대법원 2002.5.17. 선고 2001도53 결정.

20) 최석훈, 형사소송과 유추금지, 형사정책연구 제14권(2003 여름호), 348면.

21) 같은 취지로는 최석훈, 형사소송과 유추금지, 형사정책연구 제14권(2003 여름호), 348면.

22) 한편 대화비밀침해죄에서 ‘신음소리’가 ‘대화’에 해당되는지의 사건에서 법원은 신음소리는 문리 해석상 ‘대화’에 해당한다고 보기 어려울 뿐 아니라, 이 법규정의 입법목적에 비추어 이를 유추해석하거나 헌법 제17조 사생활의 비밀과 자유보호 규정에 의하여 증거능력을 인정할 수 없다고 판시한 바 있다(서울서부지법 2007. 9. 19., 선고 2007고단270 판결).

들어있는 영상이 감시될 수 있다. 이러한 해석에 따르면 통신감청은 부분적으로 영상감시도 포함하는 것으로 볼 수 있다. 일반적으로 음성비서에는 카메라가 설치되어 있지 않지만, 휴대전화에 장착되어 있는 음성비서는 카메라를 작동시킬 수 있으므로 영상감시가 가능하다. 따라서 제14조 제2항의 예외조항이 영상감시를 언급하고 있지 않기 때문에, 이 부분에서는 전기통신감청규정이 준용될 수 없다.

이러한 점들을 고려하면 제14조 제2항의 예외조항은 음성비서를 통한 주거감시에는 적용될 수 없는 것으로 판단된다.

### 3. 소결

음성비서에 몰래 접근하여 마이크를 작동하여 대화를 청취 및 녹음하여 주거를 감시하는 것은 통신비밀보호법의 전기통신감청이나 타인의 대화 비밀 침해금지의 예외 조항에 의해서 허용될 수 없다.

## IV. 독일법에 따른 음성비서를 통한 주거감시의 허용 여부

### 1. 개관

독일에서도 최근 음성비서와 관련하여 활발하게 논의가 진행되고 있다. 음성비서를 통한 주거감시와 관련하여 논의되고 있는 규정들은 형사소송법의 암호통신감청(제100a조), 온라인 수색(제100b조)<sup>23)</sup> 그리고 주거 내 음성감시(제100c조)이다. 이들은 모두 비밀감시처분이며, 앞의 두 가지는 2017년 형사소송법 개정을 통하여 도입되었으며,<sup>24)</sup> 현재 우리는 이러한 비밀감시처분을 두고 있지 않다.

23) 암호통신감청과 온라인 수색 등의 구별에 대해서는 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018. 여름호), 28-31면 참조.

24) BGBl. 2017 I, 3202.

## 2. 전기통신감청(제100a조)

독일 형사소송법은 제100a조에서 전기통신감청을 크게 세 가지로 유형으로 구분하고 있다. 전통적인 일반통신감청(제100a조 제1항 제1문), 통신 진행 중의 암호통신감청(제100a조 제1항 제2문), 통신 종료 후의 암호통신감청(제100a조 제1항 제3문)<sup>25)</sup>이 그것이다.

### 가. 전통적인 전기통신감청

형사소송법 제100a조 제1항 제1문에 따르면 특정한 사실로부터 어떤 사람이 정범 또는 공범으로서 중대한 범죄(제2항의 목록범죄)를 범했거나 미수를 범했거나 어떤 범죄를 예비하였다는 혐의가 뒷받침되고(제1호), 범행이 개별적으로도 중대한 비중이 있고<sup>26)</sup>(제2호), 사실관계의 조사나 피의자의 소재지 파악이 다른 방법으로는 본질적으로 어렵거나 기망이 없는 경우(제3호) 당사자가 모르더라도 전기통신이 감시되고 기록될 수 있다.

감시(Überwachung)란 사실관계를 규명하기 위한 수단으로써 전기통신데이터를 지득하여 이후에 이를 증거목적으로 사용하는 것이고, 기록(Aufzeichnung)은 이러한 데이터를 어떤 형태로 고정하는 것을 의미한다. 감시와 기록은 서로 다른 의미의 내용을 가지고 있지만, 기록은 목적론적으로 해석하는 경우 독자적인 의미를 갖지 않는다.<sup>27)</sup> 기록은 증거로 제출하기 위한 수단이므로 감시의 요소에 포함되기 때문이다. 이러한 감시 및 기록은 우리 통신비밀보호법의 감청개념의 지득 또는 채록에 대응하는 것으로 보인다.

한편, 형사소송법은 전기통신의 개념을 별도로 규정하고 있지 않다. 연방대법원은 전기통신의 개념을 전기통신법(TKG)의 개념(제3조 제22호)에 근거하여 해석하고 있다.<sup>28)</sup>

25) 통신이 종료된 후의 암호통신감청(제100a조 제1항 제3문)은 제100b조의 온라인 수색과 비교하여 ‘작은 온라인 수색’이라고도 한다(민영성/강수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 국민대학교 법학연구소, 법학논총 제31권 제2호, 379).

26) 통신감청의 대상범죄는 추상적으로도(즉 형벌 위하 때문), 구체적으로도 특별한 비중이 있어야 한다. 이 경우 법률에 언급되어 있는 덜 중대한 사례도 고려될 수 있다. 판례에 따르면 피해법익의 보호필요성, 일방공중이 위협받는 정도, 범행의 방법, 피해자의 수 및 손해의 규모 등은 특별한 비중의 지표로서 언급되고 있다(KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100a Rn. 28).

27) MüKoStPO/Günther, 1. Aufl. 2014, StPO § 100a Rn. 86.

28) MüKoStPO/Günther, 1. Aufl. 2014, StPO § 100a Rn. 29 m.w.N.

이에 따르면 전기통신은 “전기통신설비를 통하여 신호의 송신, 전달, 및 수신 기술적 과정”으로 정의하고 있다. 이에 대하여 연방헌법재판소는 형사소송법 제100a조의 전기통신의 개념을 전기통신법의 개념을 따르지 않고 있다. 즉 연방헌법재판소는 “기본법 제10조 제1항의 통신비밀은 발전에 개방되어 있고 새로운 전달기술을 포섭해야 하므로,<sup>29)</sup> 이에 상응하게 해석되어야 한다”고 한다. 즉 “기본법 제10조 제1항은 전기통신법의 순수한 기술적 전기통신개념을 따르는 게 아니라, 통신과정에서 제삼자의 개입으로부터 기본권 향유자의 보호필요성과 관련지어야 한다”고 하였다.<sup>30)</sup> 이 경우 전달매체와 무관하게 항상 정보전달의 과정만 포함된다<sup>31)</sup>고 한다. 따라서 전기통신의 범위는 신호의 송신에서 수신되기까지의 범위로 제한된다<sup>32)</sup>고 한다.

이러한 개념에 따르면 스마트 홈 기기에서 음성 및 영상 신호를 낚아채는 것은 기본적으로 전통적인 전기통신감청(제100a조 제1항 제1문)을 통해서 허용될 수 있다. 이 경우 오로지 현재 진행 중인 전기통신과정만이 포섭된다.<sup>33)</sup> 하지만 이러한 전기통신감청은 타인의 정보기술시스템에는 침입하지는 않는다. 따라서 제100a조 제1항 제1문은 음성비서를 통한 주거감시를 허용하는 법적 근거가 될 수 없다.

#### 나. 현재 진행 중인 통신의 암호통신감청

통신의 내용이 암호화되어 전송되는 경우 그 통신을 감청하더라도 암호를 해독할 수 없거나 해독에 많은 시간이 필요하다면 전통적인 전기통신감청은 감청의 목적을 달성하기 어렵다. 이러한 암호통신의 문제를 해결하기 위해 도입된 것이 바로 제100a조 제1항 제2문의 소위 ‘암호통신감청’(Quellen TKÜ)이다.<sup>34)</sup> 이에 따르면 전기통신의 감시와 기록이 특히 암호화되지 않는 방식으로 감시와 기록이 될 수 있도록 필요한 경우 기술적

29) BVerfG NJW 1978, 313; 2006, 976 (978).

30) BVerfG Beschl. v. 6.7.2016 - 2 BvR 1454/13, BeckRS 2016, 50705; BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 18; KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100a Rn. 4.

31) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100a Rn. 16.

32) BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 21.

33) Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 9.

34) 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018. 여름호), 27.

수단을 이용하여 당사자가 이용하고 있는 정보기술시스템에서 침입하는 방법으로도 수행될 수 있다. 따라서 암호통신감청은 통신의 내용이 암호로 전달되는 경우 암호화되기 직전에 송신자의 정보기술시스템에서 또는 복호화 된 직후 수신자의 정보기술시스템에서 감청이 수행될 수 있다. 따라서 전통적인 전기통신감청은 송수신자의 지배영역을 벗어나서 전기통신사업자의 지배영역에서 수행되지만, 암호통신감청은 송수신자의 지배영역인 정보기술시스템(예를 들어 컴퓨터, 휴대전화와 같은 통신기기 등)에서 수행된다.<sup>35)</sup> 따라서 암호통신감청의 경우 송수신자의 정보기술시스템에 비밀리에 접근해야 한다. 이러한 접근은 감시소프트웨어(예를 들어 국가트로이목마(Staatstrojaner) 또는 연방트로이목마(Bundestrojaner))를 통해서 수행된다.<sup>36)</sup> 이러한 암호통신감청은 항상 전통적인 전기통신감청의 요건이 존재해야 한다.<sup>37)</sup>

연방헌법재판소는 이러한 암호통신감청도 헌법상 기본적으로 허용될 수 있다고 구 연방법죄수사청법(BKAG) 제201조에 대한 일부 위헌판결에서 이미 확인하였다.<sup>38)</sup> 이에 따르면 제100a조 제1항 제2문의 암호통신감청의 경우 수사기관이 감시소프트웨어를 통해서 당사자의 정보기술시스템에 침입하기 때문에 통신의 비밀(기본법 제10조) 외에 추가적으로 일반적 인격권(기본법 제1조 제1항과 관련한 제2조 제1항)에서 도출되는 IT 기본권도 제한된다고 하였다.<sup>39)</sup>

음성비서는 피처분자가 이용하고 있는 정보기술시스템에 포함될 수 있다. 또한 제100a조 제1항 제2문은 '현재 진행 중인 전기통신'만을 대상으로 마이크에서 음성 신호를 가로채는 등 필요한 기술적 처분을 수행할 수 있다.<sup>40)</sup> 하지만 음성비서를 통한 주거 감시는 현재 진행 중인 전기통신만을 그 대상으로 하지 않는다.

35) Quellen TKÜ(Telekommunikationsüberwachung)에서 Quelle(크벨레)는 사전적으로 원천, 기원, 출처, 소식통, 원산지 등 다양한 의미를 가진다. 여기서 Quelle는 처분대상자의 '정보기술시스템'을 말한다. Quellen TKÜ가 '암호통신'을 감청하기 위해서 등장한 것이므로 그 기능에 착안하여 '암호통신감청'으로 번역하였다. 개별 국가의 법조항이 거의 일치하는 경우는 드물기 때문에 그 기능에 착안하여 연구하는 기능적 비교법학방법론에 따랐다.

36) 민영성/강수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 국민대학교 법학연구소, 법학논총 제31권 제2호, 372면.

37) Freiling/Safferling/Rückert, JR 2018, 9, 10.

38) BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09, NJW 2016, 1781, Rn.227.

39) BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 110.

40) BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 112.

#### 다. 통신 종료 후 암호통신감청

일반적으로 법원으로부터 암호통신감청명령을 받는 시점과 실제로 감청을 수행하는 시점에는 차이가 있다. 따라서 법원의 명령을 받은 시점부터 실제 감청이 수행된 시점 사이에 이루어진 전기통신을 소급하여 감청할 수 있는지 문제가 된다. 특히 이러한 통신이 암호로 행해졌으나 처분 대상자의 정보기술시스템에서 암호화되지 않은 상태로 남아 있는 경우 이에 접근할 수 있는 지이다. 이러한 데이터에 접근할 수 있도록 허용한 것이 바로 형사소송법 제100a조 제1항 제3문의 ‘통신 종료 후 암호통신감청’이다.<sup>41)</sup> 따라서 이 감청이 허용되기 위해서는 명령 당시 해당 통신의 내용이 암호화되어 송수신되었어야 한다.

이러한 감청에 따르면 음성입력 및 키보드 입력 외에 저장되어 있는 통신과 함께 사진 및 영상 데이터도 암호통신감청을 통해서 수집될 수 있다.<sup>42)</sup> 제100a조 제1항 제3문을 통해서 저장되어 있는 내용은 오로지 “진행 중인 전송과정 중에도 이것이 공중전기통신망에서 암호화된 형태로 감시 및 기록될 수 있었던 경우”에만 수집될 수 있다.<sup>43)</sup> 따라서 이러한 감청은 통신과 무관한 다른 데이터를 수집해서는 안 된다.<sup>44)</sup> 하지만 음성비서는 일반적으로 주거에서 행해지는 모든 내용이 전기통신을 통해서 전달되도록 특정되어 있지 않고 전기통신의 방법으로 데이터를 전달하는 것은 단지 선택적이다.

따라서 암호통신감청은 진행 중인 전기통신과정에만 관련되기 때문에 대상기기의 마이크를 작동시킬 기술적 가능성을 포함하고 있는 음성비서를 통한 감시는 형소법 제100a조에 의해서는 허용될 수 없다.<sup>45)</sup> 암호통신감청은 정보기술시스템에 접근하기 위해서 감시소프트웨어를 이용하여야 한다는 점에서 음성비서를 통한 주거감시의 그것과 동일하지만,<sup>46)</sup> 현재 진행 중인 암호통신감청을 전제로 하고 있다는 점에서 차이가 있다. 따라서 제100a조는 음성비서를 통한 주거감시에 적합한 수권근거가 될 수 없다.<sup>47)</sup>

41) 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(통권 제114호, 2018. 여름호), 37면.

42) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100a Rn. 44.

43) Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 10.

44) BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 115.

45) Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 11.

46) Freiling/Safferling/Rückert, JR 2018, 9, 10.

### 3. 온라인 수색(제100b조)

#### 가. 내용 개관

형사소송법 제100b조에 따르면 다음 세 가지 요건이 존재하는 경우 당사자가 모르더라도 기술적 수단을 통하여 당사자가 이용하고 있는 정보기술시스템에 침입하여 거기에 있는 데이터가 수집될 수 있다(온라인 수색). 첫째, 특정한 사실로부터 누군가가 정범 또는 공범으로서 제100b조 제2항에 열거된 특별히 중대한 범죄를 범하였거나 미수를 범하였다는 혐의를 뒷받침하는 경우, 둘째, 범행이 개별적인 경우에도 특별히 중대한 비중이 있고, 셋째, 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로 본질적으로 어렵거나 가망이 없는 경우이다.

온라인 수색은 기술적 수단을 이용하여 정보기술시스템에 접근하여 그 시스템에서 데이터를 수색하는 것이다. 입법자는 기술적 수단(technische Mittel)의 개념을 정의하지 않았다. 입법이유에 따르면 대상시스템을 침입하는 감시소프트웨어의 사용만이 언급되어 있다.<sup>48)</sup> 하지만 기술적 수단의 개념은 이 규정의 목적을 달성하는 모든 기술적 응용 소프트웨어를 포함하는 것으로 보아야 한다.<sup>49)</sup> 정보기술시스템의 개념은 넓게 해석되고 있다.<sup>50)</sup> 따라서 전통적인 PC 외에 마이크로프로세서에 의해서 조정되는 모든 기기, 즉 모바일폰(스마트폰), 서버 및 라우터, 음성비서 등 스마트 홈 기기도 정보기술시스템에 포함된다.<sup>51)</sup>

제100b조의 요건이 존재하는 한 기본적으로 기술적 수단으로 피치분자가 이용하고 있는 정보기술시스템에 침입할 수 있고 거기서 데이터가 수집될 수 있다. 게다가 새로 수신되는 통신의 내용뿐 아니라 IT 시스템에 저장되어 있는 내용이나 사람의 시스템 이용행태도 감시될 수 있다.<sup>52)</sup> 그러한 점에서 당사자가 스마트 홈 기기를 통해서 음성 또는 영상을 생성하는 한, 이것은 제100b조에 의해서 기본적으로 파악된다. 하지만 문제는

47) Rüscher, NSTZ 2018, 687, 689.

48) BT-Drs. 18/12785, S.46.

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

50) Haller/Conzen Das Strafverfahren, 8. Aufl. 2018, Rn. 1253.

51) KK-StPO/Bruns, 8. Aufl. 2019, § 100b Rn. 4.

52) KK-StPO/Bruns, 8. Aufl. 2019, § 100b Rn. 5.

제100b조가 마이크나 카메라와 같은 다른 센서시스템에 대한 접근도 허용하는지이다.

## 나. 마이크 및 카메라의 작동 여부

온라인 수색 규정이 수사기관에게 네트워크로 연결되어 있는 시스템의 마이크와 카메라를 작동시켜 음성 및 영상 신호를 수집할 권한도 부여하고 있는 것으로 이해될 수 있는지에 대해서는 아직 판례는 존재하지 않고, 문헌의 견해는 나뉘어 있다.<sup>53)</sup>

일부 견해에 따르면<sup>54)</sup> 제100b조는 이를 제한한다는 문언이 명시적으로 없으므로 수사기관은 기본적으로 피처분자를 탐지하기 위해서 네트워크로 연결된 시스템을 적극적으로 이용할 권한이 있다고 주장한다.

이에 대해서 지배적인 견해<sup>55)</sup>는 제100b조는 비공개 대화를 감시하기 위해서 정보기술시스템의 마이크 및 카메라에 대한 접근 권한을 부여하지 않는다고 한다.

생각건대 제100b조에서 명시적인 언급이 없다고 해서 타인의 정보기술시스템의 마이크와 카메라를 적극적으로 작동할 수 있고 그리하여 당사자의 주거의 탐지도 포섭될 수 있다는 견해는 설득력이 없어 보인다.

첫째, 제100b조의 문언에 따르면 당사자가 이용하고 있는 정보기술시스템에 침입하여 거기에서 데이터가 수집될 수 있다고 규정되어 있기 때문이다. 제100b조 제1항은 온라인 수색의 법적 개념을 “기술적 수단을 이용하여 당사자가 이용하는 정보기술시스템에 침입하여 거기에서 데이터를 수집하는 것”으로 정의하고 있다. ‘거기에서 데이터가 수집

53) SSW-StPO/Eschelbach, StPO, 3. Aufl. 2018, § 100 c Rn. 5. 이에 반해서 음성비서나 스마트 가전 기기와 같이 네트워크로 연결된 기기가 켜고 끄는 기능이 자동화되어 있거나 프로그램되어 조정되거나 인터넷검색이나 전화걸기만 하는 경우에는 제100b조의 정보기술시스템에 포함되지 않는다는 견해로는 BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a Rn. 9a 참조.

54) Beukelmann, NJW-Spezial 2017, 440; Buermeyer, „Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur ‚Formulierungshilfe‘ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, AusschussDrucksache 18(6)334, im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 31. Mai 2017“, S. 4; SSW-StPO/Eschelbach, StPO, 3. Aufl. 2018, § 100b Rn. 4.

55) Singelstein/Derin, NJW 2017, 2646, 2647; Roggan, StV 2017, 821, 826; Soiné, NStZ 2018, 497, 502; Gercke, in: Gercke/Julius/Temming/Zöller, StPO, 6. Auflage 2019, § 100b Rn. 11; Rüscher, NStZ 2018, 687, 692; Großmann, JA 2019, 241, 244; Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 18.

된다’는 법문언에서 ‘거기’란 정보기술시스템만을 의미한다. 이에 대해서 “‘이것으로’ 데이터가 수집된다”는 것을 의미하지 않는다.<sup>56)</sup> 따라서 이러한 법문언에 따르면 이 규범의 적용범위는 정보기술시스템에 존재하는 데이터로 제한된다<sup>57)</sup>고 보는 것이 타당하다. 그리고 감시소프트웨어를 작동하여 침입하는 것과 데이터 수집은 구별되어야 한다. 마이크나 카메라와 같이 개별 기기에 연결되어 있는 센서의 이용은 정보기술시스템의 침입이 아니라 데이터의 수집이라 보아야하기 때문이다.

둘째, 제100b조(온라인 수색)와 제100c조(음성주거감시)의 법문언을 비교해 보면, 제100b조의 경우 데이터의 수집은 수사기관이 접근한 정보기술시스템에서만 가능하다는 점이 분명하다. 제100b조의 표제어는 ‘온라인 수색’임에 반하여, 제100c조는 ‘주거내 음성감시’로 되어 있다. 따라서 온라인 수색으로 당사자의 주거 수색은 가능하지 않고 정보기술시스템의 수색만이 기술적 수단을 통하여 가능하다.<sup>58)</sup>

셋째, 제100b조의 입법이유에서도 주거공간을 수색할 수 없음이 명확하다. 입법이유에 따르면 “온라인 수색과 관련하여 정보기술시스템의 비밀 침입의 경우, (...) 시스템의 이용이 포괄적으로 감시되고 저장매체가 읽혀질 수 있다”.<sup>59)</sup> 즉 명백하게 시스템 이용의 감시가 해당되고 당사자의 주거 이용의 감시나 주거 감시가 아니다. 따라서 당사자 또는 제삼자가 해당 시스템을 이용하는 경우에만, 수사기관은 제100b조에 따라서 그 시스템에 접근하여 데이터를 수집할 수 있다. 또한 입법이유는 제100b조와 관련하여 IT 기본권의 제한에 대한 연방헌법재판소의 판례를 상세하게 언급하고 있지만, 제100c조가 근거로 하고 있는 기본법 제13조는 언급하지 않았다.<sup>60)</sup> 이러한 입법자의 의사에 따르면 제100b조는 주거감시를 위해서는 적용될 수 없다는 점이 명확해 보인다. 따라서 제100b조의 문언 상 오로지 정보기술시스템에만 적용되고 이와 독립된 대화나 주거는 아니다.<sup>61)</sup>

결론적으로 제100b조는 정보기술시스템의 이용과 무관한 당사자를 탐지하기 위해서

56) Singelstein/Derin, NJW 2017, 2646, 2647.

57) Rüscher, NSZ 2018, 687, 691.

58) Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 18.

59) BT-Drs. 18/12785 vom 20.06.2017, S. 47.

60) BT-Drs. 18/12785 vom 20.06.2017, S. 47 f.

61) BT-Drs. 18/12785 vom 20.06.2017, S. 47 f.

수사기관에게 스마트 홈 기기의 마이크나 카메라를 적극적으로 조정하는 권한을 부여하지 않았다고 판단된다. 오히려 당사자의 시스템 이용에서 생성되는 데이터만이 수동적으로<sup>62)</sup> 수집될 수 있다. 따라서 온라인 수색에 관한 제100b조는 정보기술시스템과 연결되어 있는 마이크와 카메라의 이용을 허용하지 않으므로 음성비서를 통한 주거감시에 적용될 수 없다.

#### 4. 주거 내 음성감시(제100c조)

##### 가. 내용 개관

형사소송법 제100c조는 주거 내 음성감시를 규정하고 있다. 이러한 주거 내 음성감시가 가능하기 위해서는 우선 다음 네 가지 요건이 존재해야 한다. 첫째, 특정한 사실로부터 누군가가 정범 또는 공범으로서 제100b조 제2항에 열거되어 있는 ‘특별히 중한 범죄’를 범했거나 처벌되는 미수를 범했다는 혐의를 뒷받침해야 한다(제1항 제1호). 둘째, 범행이 개별적으로도 특별히 비중이 있어야 한다(제1항 제2호). 셋째, 사실상의 근거에 의해서 감시를 통해서 사실관계의 조사를 위해서 또는 공동피의자의 소재지 파악을 위해서 의미가 있는 피의자의 발언이 수집된다는 것이 인정될 수 있어야 한다(제1항 제3호). 넷째, 사실관계의 조사나 공동피의자의 소재지 파악이 다른 방법으로는 현저하게 어렵거나 가망이 없어야 한다(제1항 제4호). 이러한 요건이 존재하는 경우 당사자가 모르더라도 주거에서 비공개로 행해지는 대화를 기술적 수단으로 청취(Abhören) 하고 기록(Aufzeichnen) 할 수 있다. 주거 내 음성감시는 주거 내에서의 대화를 감시하는 것이므로 기본적으로 주거 내에 도청기와 같은 기술적 수단이 설치되는 것을 전제로 한다. 따라서 이를 위해서 주거에 몰래 출입하는 것은 부수처분으로 허용된다.<sup>63)</sup> 또한 주거 외에서 도청장치를 이용하여 주거 내의 대화를 감시하는 것도 허용된다. 하지만 영상감시는 허용되지 않는다.<sup>64)</sup>

62) Soiné, NStZ 2018, 497, 502.

63) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100c Rn. 4.

64) 이에 대해서 국제테러의 위험방지를 위한 연방범죄수사청법(BKAG) 제46조는 영상감시도 허용하고 있다.

## 나. 음성비서를 통한 주거감시에 적용

주거 내 비공개 대화의 청취와 기록이 당사자의 음성비서를 통하여 허용되는지 문제와 관련하여 결정적인 것은 음성비서가 제100c조 제1항의 기술적 수단으로 간주될 수 있는가이다.

입법자는 주거 내 음성감시처분을 이행하기 위한 구체적인 수단을 언급하고 있지 않다. 이는 이러한 처분이 새로운 기술적 발전에 개방적으로 적용될 수 있기 위해서다.<sup>65)</sup> 따라서 형소법 제100c조의 음성주거감시의 의미와 목적을 고려하면 스마트 홈 기기를 이용하여 주거감시를 할 수 있을 것으로 보인다. 하지만 제100c조는 제100a조 및 제100b조와 달리 타인의 정보기술시스템에 침입하여 데이터를 수집하기 위한 명시적인 권한을 언급하고 있지 않다.<sup>66)</sup> 연방헌법재판소에 따르면 정보기술시스템의 비밀 침입과 관련되는 처분은 IT 기본권의 제한이다. IT 기본권은, 개별 통신과정이나 저장되어 있는 데이터만을 대상으로 하지 않고 정보기술시스템의 접근을 전체적으로 방지한다. 따라서 IT 기본권은 일반적 인격권에서 도출되는 독자적인 기본권으로서 국가의 접근으로부터 기본권 향유자의 개인생활 및 사생활을 보호한다.<sup>67)</sup> 따라서 제100c조는 형사소추기관이 스마트 홈 기기 당사자의 주거를 감시할 목적으로 마이크나 카메라에 접근할 권한을 부여하지 않는다<sup>68)</sup>고 보아야 한다.

또한 제100c조의 기술적 수단은 수사기관에게 속한다. 주거감시를 위해서 침입하는 음성비서는 처분 대상자의 정보기술시스템이다. 비록 제100c조의 기술적 수단이 물리적인 기기가 아니라 거기에 설치되는 수사기관의 소프트웨어라고 하더라도, 이러한 수단을 통해서 곧바로 주거에서의 대화를 기록하는 것은 가능하지 않다.<sup>69)</sup> 음성비서를 이용한 주거감시는 주거의 불가침(기본법 제13조)의 제한 외에도 소프트웨어의 설치 또는 조장을 통해서 IT 기본권의 제한도 발생한다.

65) MüKoStPO/Günther 2014, § 100 c Rn. 50; SSW-StPO/Eschelbach, StPO, 3. Aufl. 2018, § 100 c Rn. 3.

66) Vgl. SSW-StPO/Eschelbach, StPO, 3. Aufl. 2018, § 100c Rn. 5.

67) Blechschmitt, MMR 2018, 361, 365.

68) Blechschmitt, MMR 2018, 361, 365; SSW-StPO/Eschelbach, StPO, 3. Aufl. 2018, § 100c Rn. 5.

69) Rüscher, NSZ 2018, 687, 690.

따라서 음성비서를 이용한 주거감시는 입법자가 제100c조의 음성주거감시를 도입할 때 의도했던 기본권 제한의 정도를 넘어선다. 따라서 제100c조는 음성비서를 통한 주거감시를 정당화할 수 없다.

## 5. 소결 및 시사점

이상에서 독일 형사소송법의 전기통신감청, 온라인 수색, 음성주거감시에 관한 비밀 처분은 음성비서를 통한 주거감시를 위한 권한 규정으로 볼 수 없다. 하지만 음성주거감시와 온라인 수색을 동시에 이용하는 경우에는 주거감시가 가능할 수 있어 보인다. 온라인 수색의 경우 정보기술시스템에 접근하는 것은 허용되고 카메라를 작동하여 주거를 감시하는 것은 허용되지 않지만, 음성주거감시의 경우 마이크를 작동하여 주거를 감시하는 것은 허용되고 정보기술시스템에 접근하는 것은 허용되지 않는다. 그 때문에 각 처분에서 허용되는 온라인 수색의 정보기술시스템 침입과 음성주거감시의 마이크 작동을 동시에 이용하는 방법이 고려될 수 있다.

독일 연방헌법재판소의 확립된 판례에 따르면 여러 비밀수사방법을 동시에 사용하는 것은, 당사자의 인격프로필을 포괄적으로 작성하게 하는 “총체적 감시”(Totalüberwachung)로 이어지지 않고 그 처분들이 전체적으로 비례성을 갖추고 있는 한 가능하다고 한다.<sup>70)</sup>

하지만 음성비서를 통한 주거감시의 경우는 법적으로 허용되는 다수의 개별 처분의 결합이 아니라, 새로운 침입수단을 창설하기 위해 다수의 침입 권한이 결합되어 있다.<sup>71)</sup> 따라서 기술적으로 가능한 새로운 수사처분을 창설하기 위해서 형사소송법 내부에서 제한 권한의 개별적 요소의 결합은 허용되지 않는다. 이것은 독일 헌법(기본법) 제20조 제3항의 기본권 제한을 위한 법률유보원칙에 반하고, 형사소송법의 기본권 제한 규범의 명확성원칙과 구성요건의 특정성원칙에도 반하기 때문이다.<sup>72)</sup> 따라서 형사소송법 제100b조와 제100c조의 수권근거들의 결합은 배제되어야 한다.

독일에서 2017년 형사소송법 개정을 통하여 수사기관의 제한 권한은 온라인 수색과

70) BVerfGE 109, 279, 323; BVerfGE 112, 304, 309 ff.; BGHSt 46, 266, 277 f.

71) BGHSt 51, 211, 218 f.

72) BVerfGE 112, 304, 315 ff.; BVerfGE 115, 166, 187 ff.; BGHSt 51, 211, 218 f.

암호통신감청으로 상당히 확대되었지만, 음성비서를 통한 주거감시는 아직 포섭하지 못하는 것으로 판단된다. 하지만 독일의 법적 상황의 검토는 우리에게 시사하는 바가 크다. 암호통신감청이나 온라인 수색의 경우 음성비서와 같은 정보기술시스템에 접근하여 그 이후의 통신감청이나 데이터의 수색을 규범적으로 이미 허용하고 있으므로 정보기술시스템의 접근을 전제로 하는 음성비서를 통한 주거감시의 요건들이 어떻게 규범화되어야 하는지를 알 수 있기 때문이다.

## V. 음성비서를 통한 주거감시의 입법 방향

### 1. 입법 필요성

정보통신기술의 발전으로 오늘날 음성비서와 같은 스마트 홈 기기들은 대부분 통신기능을 가지고 있다. 통신기능을 가진 기기들이 인터넷과 같은 정보통신망에 연결되면 제삼자가 온라인에서 접근할 수 있고 그 방법은 다양하다. 이러한 접근이 정당화되지 않는 한 정보통신망법의 통신망침입죄에 해당될 수 있다. 하지만 오늘날 스마트 폰과 같이 정보통신기기를 사용하지 않고서는 일상생활이 어렵다. 이러한 통신환경에서 정보통신망에 연결되어 있는 정보기술시스템에 수사기관이 접근하는 것은 피할 수 없는 현실이 되었고, 앞으로 인공지능기기가 사물인터넷으로 연결되는 초연결사회에서는 더욱 확대될 것이다.

따라서 테러범죄와 같은 중대한 범죄에 대응하기 위해서 증거수집이나 사실관계의 확인을 위해서 그리고 이들 범죄의 혐의를 받고 있는 자의 감시 및 관찰을 위해서 음성비서에 대한 접근은 불가피한 수사가 될 수 있으므로 이를 수사기관에 허용할 필요가 있을 것으로 보인다. 초연결사회에서 발생하는 범죄에 대응하기 위해서는 이에 상응하는 수사방법이 마련되어야 한다. 아날로그 수사방법은 이러한 범죄에 대응하기 어렵다. 특히 현재 형사소송법이나 통신비밀보호법은 비교법적으로 보면 비밀처분과는 상당한 거리가 있고 초연결사회에서는 제대로 대응하기 어려운 아날로그 수사방법으로 구성되어 있다. 범죄로부터 국가와 국민을 보호해야 될 국가의 의무는 수사기관과 범죄자의 무기대응의

원칙이 전제되어야 한다. 따라서 디지털화된 수사기관의 음성비서에 대한 접근은 범죄수사라는 국가의 정당한 목적에 해당되고 이러한 목적을 달성하기 위해서 필요하고 적합한 수단이 될 수 있다. 이러한 수단이 균형성의 원칙을 충족할 수 있도록 그 요건에서 마련되어야 할 것이다.

## 2. 관련 기본권

음성비서를 통한 주거감시는 기본적으로 음성비서에 대한 접근을 전제로 한다. 이러한 접근이 가능하기 위해서는 감시소프트웨어가 대상 음성비서에 설치되어야 한다. 음성비서에 대한 접근은 IT 기본권을 침해하게 된다.<sup>73)</sup> 설치된 감시소프트웨어를 통해서 음성비서에 접근한 다음 마이크 기능을 작동하여 주거를 감시하는 것은 주거의 불가침을 침해할 수 있다. 나아가서 마이크를 통하여 대상자와 음성비서 사이에 주고받는 대화를 청취하거나 기록하는 경우에는 공개되지 않은 대화비밀이 침해될 수 있고, 음성비서가 수행하는 전기통신행위를 감시하는 경우에는 (암호)전기통신감청이 될 수 있다.

수사기관의 음성비서에 대한 접근은 주거 내 대화감청, 통신감청, 시스템이용감시, 데이터수집이 모두 가능할 수 있다. 따라서 이러한 접근은 기존의 수사처분이 예정하지 못한 포괄감시에 해당될 수 있으므로 수사기관이 이에 접근하는 경우 남용의 위험성이 상당히 높다. 이러한 접근은 국민의 사생활 보호와 침해, 주거의 불가침, 통신비밀보호, 정보자기결정권, IT 기본권 등을 심각하게 침해할 우려가 있다. 따라서 수사기관이 음성비서에 접근하기 위한 권한 규정은 범죄수사를 위해서 적합하고 필요하며 상당성이 있는 엄격한 요건을 갖춘 법률에 근거해야 한다.

## 3. 입법의 기본 방향

형사소송법이나 통신비밀보호법은 독일과 같이 정보기술시스템에 접근을 허용하는 수권 규정을 두고 있지 않다. 따라서 음성비서를 통한 주거감시를 허용하는 규정을 도입

73) IT 기본권의 헌법적 근거에 대해서는 박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호(2012. 9), 161면.

하기 위해서는 비교법적으로 검토한 독일의 법적 상황을 입법자료로 참고할 수 있을 것이다.

### 가. 음성비서를 통한 주거감시의 기본권 제한의 정도

독일의 법적 상황을 보면 암호통신감청과 온라인 수색은 기본적으로 정보기술시스템의 접근이 전제되어 있다. 따라서 음성비서와 같은 정보기술시스템에 접근하여 전기통신을 감청하거나 그 안에 있는 데이터를 수집하는 것은 암호통신감청과 온라인 수색의 요건이 참고될 수 있다. 기본권 제한의 정도는 온라인 수색이 암호통신감청보다 더 높다.

온라인 수색과 주거내 음성감시는 독일 형사소송법의 수사절차상 기본권 제한의 정도가 가장 높은 비밀강제처분이다. 음성비서를 통한 주거감시는 음성비서에 대한 접근과 마이크의 작동이라는 두 단계의 과정이 필요하므로 온라인 수색과 주거 내 음성감시의 기본권 제한의 정도와 다르지 않다. 따라서 현재 우리 통신비밀보호법의 통신제한조치나 이를 준용하고 있는 비공개 대화의 청취 및 녹음보다는 더 엄격한 요건이 필요하다.

### 나. 실체적 요건

온라인 수색과 주거 내 음성감시의 대상 범죄는 형사소송법 제100b조 제2항에서 한정적으로 열거되어 있는 ‘특별히 중대한 범죄’이다.<sup>74)</sup> 피처분자가 이들 범죄의 정범 또는 공범으로서 기수나 미수를 범하였다는 혐의가 있어야 하고, 특별히 중대한 범죄는 추상적으로도 구체적으로도 특별히 중대한 비중이 있어야 한다. 독일 형사소송법은 범죄유형을 그 비중에 따라서 세 가지로 구분하고 있다. 중요한 의미가 있는 범죄(*Straftat von erheblicher Bedeutung*), 중한 범죄, 특별히 중한 범죄(*besonders schwere Straftat*)가 그것이다. 중요한 의미의 범죄는 헌법재판소와 지배적인 견해에 따르면 법적 평화를 민감하게 교란시키고 국민의 법적안전성에 대한 느낌을 현저하게 침해하기에 적합한 중간정도<sup>75)</sup>의 범죄영역에 속하는 범죄를 말한다.<sup>76)</sup> 중한범죄는 특히 전기통신감청의 대상범

74) 형사소송법 제100b조 제2항은 특별히 중대한 범죄를 7개의 개별범률(형법, 난민절차법, 외국인체류법, 마약류법, 전쟁무기통제에 관한 법률, 국제형법, 무기법)에서 선별하여 규정하고 있다.

75) 일반적으로 범죄는 그 비중에 따라서 다시 4단계로 나눌 수 있다. 단순범죄(*einfache Kriminalität*), 중간범죄(*mittlere Kriminalität*), 중한범죄(*schwere Kriminalität*), 특별히 중한 범죄(*besonders*

죄(제100a조)를 통해서 구체화되고 있으며 일반적으로 형벌의 상한이 5년 이하인 범죄를 말한다. 특별히 중한 범죄는 형벌의 하한이 5년 이상인 범죄를 말한다.<sup>77)</sup> 음성비서를 통한 주거감시도 적어도 특별히 중한 범죄를 대상으로 해야 한다.

독일의 온라인 수색과 주거 내 음성감시는 엄격한 보충성 조항을 두고 있다. 온라인 수색의 경우 사실관계의 조사나 피의자의 소재지 수사가 다른 방법으로는 본질적으로 어렵거나 가망이 없어야 한다. ‘본질적인 어려움’이란 다른 수사처분의 경우 시간이 많이 소요되거나 신속한 수사에 필요하고 충분한 정보수집이 기대될 수 없는 경우를 말하고, ‘가망 없음’이란 다른 수사처분이 이용될 수 없거나 성공할 수 없는 경우를 말한다.<sup>78)</sup>

주거 내 음성감시의 경우에는 그 밖에 공동피의자의 소재지 파악을 위해서 피의자의 진술이 포착될 수 있어야 하고 공동피의자의 소재지 파악이 다른 방법으로는 현저히 어렵거나 가망이 없어야 한다.<sup>79)</sup> 이것은 기본법 제13조에서 규정하고 있는 가장 엄격한 보충성 조항(ultima-ratio-Klausel)이다. 온라인 수색의 ‘본질적으로 어려움’이나 주거 내 음성감시의 ‘현저히 어려움’의 경우 후자가 보충성의 강도가 더 높지만, 수사실무에서는 차이가 그리 크지 않다.<sup>80)</sup> 이처럼 온라인 수색이나 주거 내 음성감시가 형사소송법의 비밀처분에서 가장 엄격한 보충성원칙을 요구하고 있는 것은 다른 강제처분으로는 더 이상 소용이 없을 때 이 강제처분이 마지막 수단으로 사용될 수 있다는 것을 의미한다.<sup>81)</sup> 따라서 음성비서를 통한 주거감시에도 이러한 정도의 보충성원칙이 필요하다.

온라인 수색은 정보기술시스템의 접근을 전제로 하므로 이와 관련하여 기술적으로 확

schwere Kriminalität)이다.

76) 예를 들면 제98a조 제1항, 제100g조 제1항 제1호, 제100h조 제1항, 제100i조 제1항, 제110a조 제1항, 제163e조 제1항, 제163f조 제1항이다.

77) 윤해성·최호진·박희영·이권일, 영장주의의 현대적 한계와 개선방안에 관한 연구, 2020.12. 한국형사정책연구원, 242면.

78) BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100b Rn. 16.

79) 형사소송법은 보충성원칙을 단계화하고 있다. 즉 처분이 필요한 경우, 성공할 가망이 적거나 어려운 경우, 성공할 가망이 현저히 적거나 어려운 경우, 가망이 없거나 본질적으로 어려운 경우이다(윤해성·최호진·박희영·이권일, 영장주의의 현대적 한계와 개선방안에 관한 연구, 2020.12. 한국형사정책연구원, 243면).

80) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100c Rn. 15.

81) KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100c Rn. 14.

보되어야 할 내용(제100b조 제4항 및 제100a조 제5항)<sup>82)</sup>과 기술적 수단의 투입 시 기록되어야 할 사항(제100조 제4항 및 제100a조 제6항)<sup>83)</sup>을 규정하고 있다. 이러한 규정들은 음성비서를 통한 주거감시에도 필요하다.

#### 다. 절차적 요건

온라인 수색과 주거 내 음성감시에서 명령의 신청권자는 검사이고 명령을 내리는 자는 검찰청 소재지를 관할하는 지방법원 합의부이다(제100e조 제2항). 지체의 위험이 있는 경우에는 재판장이 명령을 내릴 수 있으나 3일 이내에 형사합의부의 승인을 받아야 한다. 따라서 전기통신감청과 달리 검사의 긴급명령권은 허용되지 않는다. 명령권한은 최대 1개월이며 기존의 수사결과를 고려하여 명령의 요건이 존속하는 한도에서 연장이 가능하고 매번 1개월 이내로 허용된다. 명령의 기간이 총 6개월로 연장되었으면 추가 연장에 관해서는 고등법원이 재판한다. 명령의 요건이 더 이상 존재하지 않으면 그 명령에 근거한 조치는 지체 없이 종료해야 한다(제100e조 제5항). 명령 법원에는 조치의 종료 후에 그 결과를 알려야 한다. 제100b조와 제100c조에 따른 조치에서는 명령 법원에 조치의 경과도 알려야 한다. 명령의 요건이 더 이상 존재하지 않는 경우, 이미 검찰이 조치를 중단하지 않으면 법원은 그 중단을 명해야 한다. 이러한 절차에 관한 규정들은 음성비서를 통한 주거감시에도 적용할 수 있다.

한편 온라인 수색과 주거 내 음성감시로 취득한 개인정보를 다른 목적으로 사용할 수 있는지 문제가 될 수 있다. 이와 관련하여 형사소송법 제100e조 제6항에 따르면 온라인 수색과 주거 내 음성감시가 명령될 수 있는 다른 범죄를 수사하거나 그러한 범죄의 혐의

82) 첫째, 데이터 수집을 위해서 불가피한 경우에만 침입한 정보기술시스템에 변경을 가할 수 있다. 둘째, 처분의 종료 후 그 변경은 기술적으로 가능한 한 자동으로 복구되어야 한다. 셋째, 투입된 수단은 현재의 기술 수준에 상응하게 무단 사용으로부터 보호해야 한다. 넷째, 복제된 데이터는 현재의 기술 수준에 따라서 변경, 무단 삭제, 무단 지득으로부터 보호되어야 한다. 다섯째, 음성비서를 통해서 청취 및 기록된 내용은 현재의 기술 수준에 따라서 변경, 무단 삭제, 무단 지득으로부터 보호되어야 한다.

83) 첫째, 기술적 수단의 명칭과 그 투입 시점, 둘째, 정보기술 시스템의 식별 표시와 그 시스템에 대하여 단지 일시적이지 않게 변경된 사항, 셋째, 수집된 데이터의 확인을 가능하게 하는 표시, 넷째, 그 조치를 실행한 조직 등이다. 음성비서를 통한 주거감시도 정보기술시스템에 접근해야 하므로 이러한 기술적 보호조항과 기록에 관한 규정이 필요하다.

를 받는 자의 소재지를 파악하기 위한 경우, 그리고 생명, 신체, 자유나 국가의 안전과 존립 등에 대한 급박한 위협을 방지하기 위한 경우에는 당사자의 동의 없이 그러한 개인 정보를 사용할 수 있다. 나아가서 경찰법에 근거하여 수집된 개인정보도 온라인 수색이나 주거 내 음성감시가 명령될 수 있는 범죄의 수사나 그러한 범죄의 혐의를 받는 사람의 소재지 파악을 위한 경우에도 당사자의 동의 없이 사용될 수 있다.

우리 통신비밀보호법 제12조는 통신제한조치로 취득한 자료의 사용제한을 규정하고 있다. 이에 따르면 특히 전기통신의 내용은 통신제한조치의 대상 범죄나 이와 관련되는 범죄를 수사 및 소추하거나 그 범죄를 예방하기 위하여 사용할 수 있다. 제14조 제2항은 제12조를 준용하고 있으므로 제14조 제2항의 비공개 타인 간의 대화의 녹음 또는 청취로 확보한 대화내용도 사용할 수 있다. 따라서 음성비서를 통한 주거감시의 경우 독일 형소법 제100e조 제6항과 통비법 제12조 및 제14조 제2항을 고려하여 도출할 수 있을 것이다.

마지막으로 피처분자는 당해 처분에 대한 통지를 받아야 하며 처분에 대해 이의를 제기할 수 있어야 한다(제101조 제4항 이하). 음성비서를 통한 주거감시는 기본권 침해의 강도가 아주 높은 비밀처분이기 때문에 통지와 이의제기권은 반드시 필요하다.

#### 라. 사생활의 핵심영역의 보호와 증언거부권자의 보호

독일 형사소송법은 전기통신감청, 온라인 수색, 주거 내 음성감시의 경우 증거금지를 통하여 사생활의 핵심영역을 보호하고 있다(제100d조). 이러한 처분으로 사생활의 핵심영역에 관한 데이터가 수집되거나 사용되어서는 안 된다(증거수집 및 증거사용 금지, 제100d조 제1항과 제2항). 따라서 사생활의 핵심영역에 관한 내용이 수집된 경우 지체없이 삭제되어야 하고 수집과 삭제는 기록되어야 한다. 특히 제100b조의 온라인 수색의 경우에는 가능하다면 사생활의 핵심영역에 관한 데이터가 수집되지 않도록 기술적으로 확보해야 한다. 또한 온라인 수색으로 사생활의 핵심영역에 관한 데이터가 수집된 경우 지체없이 삭제하거나 이의 사용이나 삭제에 대해서 명령 법원에 재판을 청구할 수 있다. 제100c조의 음성주거감시의 경우에는 사생활의 핵심영역에 관한 발언이 수집되는 않는다는 사실상 근거가 있어야 한다(제100d조 제4항). 주거감시 중에 사생활의 핵심영역에 관한 표현이 수집되는 근거가 있는 경우 감시를 지체없이 정지해야 한다. 주거감시의 요

건이 존재하는 경우에만 이를 속행할 수 있다. 검찰은 이러한 조치나 속행에 의심이 있는 경우 이에 관하여 지체없이 법원에 재판을 청구해야 한다.

우리 통신비밀보호법은 전기통신감청의 경우 불법감청에 의하여 지득 또는 채록한 전기통신의 내용은 재판에서 증거로 사용할 수 없도록 하고 있다. 제14조 제2항의 준용 규정에 따라 비밀대화의 청취 및 녹음(제14조 제2항의 준용)에도 동일하다. 이러한 방식의 사용금지는 불법 수집을 간접적으로 통제할 수 있다. 하지만 수집 자체를 직접 금지하지 않는 경우에는 다른 방법으로 우회할 수 가능성이 있으므로 바람직하지 않다. 나아가서 정보기술시스템에 접근하는 음성비서를 통한 주거감시는 기본권 침해의 정도가 전기통신감청보다 높기 때문에 수집단계부터 금지될 필요가 있다.

한편 온라인 수색과 주거 내 음성감시 처분은 증언거부권이 인정되는 업무상 비밀 준수자에게는 적용되지 않는다(제100b조 제5항). 우리 통신비밀보호법의 전기통신감청이나 비밀대화감시의 경우 피처분자를 제한하는 규정이 존재하지 않는다. 이러한 사생활의 핵심영역의 보호와 업무상 비밀 준수자의 증언거부권도 음성비서를 통한 주거감시에서 고려되어야 한다.

## Ⅵ. 결론 및 함께 논의되어야 할 문제들

이 글은 음성비서가 제기할 수 있는 다양한 문제 중에서 수사기관이 음성비서에 비밀리에 접근한 후 마이크를 작동하여 주거 내에서 행해지는 대화를 녹음하거나 청취하는 주거감시가 현행법에서 허용되는지를 검토하였다. 우리 통신비밀보호법의 전기통신감청이나 타인의 대화비밀 침해금지의 예외조항은 이러한 주거감시를 허용하지 않는다. 우리와 달리 정보기술시스템에 접근할 수 있는 비밀 수사처분을 도입하고 있는 독일 형사소송법의 전기통신감청과 온라인 수색이나 음성주거감시에 관한 비밀 처분도 이러한 음성비서를 통한 주거감시를 위한 수권 규정으로 보기 어렵다. 하지만 독일의 검토는 우리에게 시사하는 바가 크다. 암호통신감청이나 온라인 수색의 경우 음성비서와 같은 정보기술시스템에 접근하여 그 이후의 통신감청이나 데이터의 수색을 규범적으로 이미 허용하고 있으므로 정보기술시스템에 접근을 전제로 하는 음성비서를 통한 주거감시의 요건들이

어떻게 규범화되어야 하는지를 알 수 있기 때문이다. 따라서 이상의 논의들을 고려하면 음성비서를 통한 주거감시를 위한 규정을 도출할 수 있을 것으로 보인다.

음성비서를 통한 주거감시에 관한 논의는 이것만으로 끝나지 않는다. 즉 동시에 논의되어야 할 다른 문제들이 서로 관련되어 있기 때문이다. 우선 음성비서를 통한 주거감시에 관한 규정은 통신이 가능한 다른 스마트 홈 기기나 사물인터넷 기기에도 전용될 수 있는지이다. 특히 카메라가 장착된 기기의 경우에는 실시간으로 영상감시를 할 수 있으므로 음성감시보다 기본권 침해의 강도가 훨씬 높을 것으로 예상된다. 그런 점에서 독일 기본법은 제13조 제3항에서 수사목적의 주거 내 음성감시의 경우에는 음성감시만 허용하고 영상감시는 허용하고 있지 않다. 하지만 기본법 제13조 제4항에서 경찰의 위험방지를 위한 감시의 경우에는 이러한 제한을 하고 있지 않다. 그리하여 국제테러의 위험방지를 위한 연방범죄수사청법(BKAG) 제46조나 대부분의 주경찰법<sup>84)</sup>에는 영상감시도 허용하고 있다. 따라서 우리 입법자가 수사절차에서 영상감시를 허용할 수 있는지는 기본권 차원에서 심도있게 논의되어야 할 것이다.

또한 음성비서나 다른 스마트 홈 기기가 주거에 있지 않고 주거 바깥에 있는 경우에는 어떠한 요건에서 감시가 허용될 수 있는지도 문제가 될 수 있다. 독일 형사소송법은 주거 내 감시(제100c조)와 주거 외 감시(제100f조)를 명확히 구분하고 있다. 우리 통신비밀보호법은 제14조 제2항 예외조항에서 이를 구분하고 있지 않다. 음성비서를 통한 주거감시의 규정을 논의할 경우 이 조항도 함께 다루어야 할 것이다.

음성비서를 통한 주거감시에서 음성비서에 접근하는 경우 이용자와 음성비서 사이의 대화가 감시될 수 있고 음성비서가 명령에 따라 수행하는 전기통신이 감청될 수 있다. 대화나 전기통신은 사람인 상대방을 전제로 한다. 따라서 이러한 경우 전기통신감청이나 비공개 타인간의 대화의 감청에 해당하는지 문제가 된다. 나아가서 음성비서에 접근하는 경우 수사기관은 음성비서 제공자의 클라우드 서버에 저장되어 있는 이용자의 데이터에 접근할 수 있다. 따라서 음성비서를 통한 주거감시에 관한 논의는 (암호)통신감청이나 온라인 수색에 관한 논의도 함께 진행되어야 함을 의미한다.

마지막으로 이러한 비밀처분들은 기본적으로 정보기술시스템에 대한 접근을 전제로 한다. 이에 접근하기 위해서는 현재 독일 실무에서는 다양한 방법들이 이용되고 있다.

84) 예를 들어 바덴주 경찰법 제50조, 바이에른주 경찰법 제41조 등.

하지만 특히 수사기관이 정보기술시스템의 보안상 취약점을 이용할 수 있는지는 아직 명확하지 않다. 이것은 IT 보안에 대한 국가의 보호의무와 관련되기 때문이다.<sup>85)</sup> 따라서 수사기관의 보안상 취약점의 이용과 국가의 보호 의무를 어떻게 조화시킬 것인지도 함께 논의되어야 할 것이다.

---

85) 박희영·이상학, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호(통권 제118호), 2019. 여름, 134면.

## 참고문헌

- 김형준, 현행 통신비밀보호법의 문제점과 개선방안, 형사법연구 제24호(2005. 겨울).
- 민영성/강수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 국민대학교 법학연구소, 법학논총 제31권 제2호, 372면.
- 박희영, 수사 목적의 암호통신감청(Quellen TKÜ)의 허용과 한계, 형사정책연구 제29권 제2호(2018. 여름호).
- 박희영, 예방 및 수사목적의 온라인 비밀 수색의 허용과 한계, 원광법학 제28권 제3호 (2012. 9).
- 박희영, 독일 연방헌법재판소의 정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권, 법무부, 인터넷법률 통권 제45호, 2009. 1.
- 박희영·이상학, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호(2019. 여름호).
- 성선제, e-사회에서 테러 및 범죄예방을 위한 감청과 프라이버시의 갈등 조정 방안 연구, 공법연구, 제8권 제4호(2007).
- 심홍진, 인공지능(AI)과 프라이버시의 역설 : AI 음성비서를 중심으로, 정보통신정책연구원, 2018.12.
- 윤해성·최호진·박희영·이권일, 영장주의의 현대적 한계와 개선방안에 관한 연구, 2020.12. 한국형사정책연구원.
- 정배근/이경열, 독일 연방헌법재판소 결정을 통해 바라본 패킷감청 수사의 실질적 통제 방안과 통신비밀보호법 신설조문 제12조의2 문제점, 비교형사법연구 제22권 제2호, 2020.7.
- 조국, 개정 통신비밀보호법의 의의, 한계 및 쟁점: 도청의 합법화인가 도청의 통제인가?, 형사정책연구 제15권 제4호(2004 겨울호).
- 최석윤, 형사소송과 유추금지, 형사정책연구 제14권 제2호(2003 여름호).
- Beukelmann, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, S.440.
- Blechschnitt, Lisa, Strafverfolgung im digitalen Zeitalter, Auswirkungen des

stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, 361-366.

Buermeyer, Ulf, „Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur ‚Formulierungshilfe‘ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, AusschussDrucksache 18(6)334, im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags am 31. Mai 2017“, S. 4.

BeckOK StPO/Graf, 38. Ed. 1.10.2020, StPO § 100a, § 100b.

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, in: Gercke/Julius/Temming/Zöllner, StPO, 6. Auflage 2019, § 100b Rn. 11.

Gless, Sabine, Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter, StV 2018, 671-678.

Großmann, Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, JA 2019, 241-248.

Haller/Conzen Das Strafverfahren, 8. Aufl. 2018, Rn. 1253.

KK-StPO/Bruns, 8. Aufl. 2019, StPO § 100a, § 100b, § 100c.

MüKoStPO/Günther 2014, § 100a. § 100c.

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

Rüscher, Daniel, Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, 687-692.

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

NJW 2017, 2646)

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

SSW-StPO/Eschelbach, 3. Aufl. 2018, § 100b, § 100 c.

Wissenschaftliche Dienste, Zugriff auf vernetzte Geräte zum Zweck der Strafverfolgung, Strafverfahrensrechtliche Rahmenbedingungen, Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S. 9. (zit.; Deutsche Bundestag, WD 7 - 3000 - 119/19. 19. August 2019, S.).

State of Arkansas v. James A. Bates, Case No. CR-2016-370-2, <https://regmedia.co.uk/2017/02/23/alex.pdf>)

State of New Hampshire v. Timothy Verrill, Case No. 219-2017-CR-072, <https://www.courts.state.nh.us/caseinfo/pdf/Verrill/110518Verrill-order.pdf>).

BGBI. 2017 I, 3202.

## Allowance and Legislative Direction for Private Premises Surveillance through Intelligent Virtual Assistant\*

Park, Hee-Young\*\*

In a smart home environment, an intelligent virtual assistant (Digitale Sprachassistenten) is playing a key function. Since the virtual assistant is mainly installed in individual residences, there is a risk of invading key areas of privacy. This is because digital information about an individual's private life area stored in an artificial intelligence server of a service provider can be easily accessed technically through the assistant. When accessing the virtual assistant connected to the Internet, it is possible to access the data stored in the assistant itself as well as the user's data stored in the service provider's artificial intelligence server (Covert remote search of information technology systems, Online-Durchsuchung). When the microphone installed in the assistant is operated, private conversations in the residence or conversations between users and the assistant can be heard or recorded (Acoustic surveillance of private premises, Akustische Wohnraumüberwachung), and telecommunications performed by the assistant may be intercepted (Telecommunications surveillance, Telekommunikationsüberwachung, TKÜ). In this way, various issues can be raised in criminal proceedings surrounding the voice secretary.

Among these various issues, this article has dealt with whether in-home voice surveillance can be permitted under the current law.

In this article, Private Premises Surveillance through Intelligent Virtual Assistant

---

\* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5A2A01046918).

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

is understood as housing surveillance in which an investigative agency secretly approaches the Assistant and then operates a microphone to record or listen to conversations in the home. The current regulations on telecommunications monitoring in the Communications Secret Protection Act do not allow such residential monitoring. The German Criminal Procedure Act, unlike ours, allows access to information technology systems through confidential measures such as cryptographic telecommunication interception, online search, and voice surveillance in residences. However, even these secret investigations do not allow voice surveillance in the residence through voice secretaries. However, the requirements of the in-house voice surveillance and online search regulations of the German Criminal Procedure Act provide a direction for what the regulations for residential surveillance through voice assistants should have. Through this, it is expected that the requirements for residential monitoring through voice assistants can be derived.

- ❖ key words: intelligent virtual assistant(Digitale Sprachassistenten), Covert remote search of information technology systems(Online-Durchsuchung), Telecommunications surveillance(Telekommunikationsüberwachung, TKÜ), Source Telecommunications surveillance(Telecommunications surveillance at the source, Quellen TKÜ), Acoustic surveillance of private premises(Akustische Wohnraumüberwachung), Core area of private conduct of life(Kernbereich privater Lebensgestaltung)

