형사정책연구 Korean Criminological Review
제32권 제3호(통권 제127호, 2021 · 가을)

최근 독일 정보기관의 정보수집권 확대와 형사정책적 시사점*

– 암호통신감청, 전략적 해외통신감청, 온라인 수색을 중심으로 –

박희영**

국 | 문 | 요 | 약

일반적으로 국가안보와 관련한 업무를 수행하는 기관은 안보와 관련된 정보를 수집하는 기관(정보기관), 안보와 관련된 위험을 방지하는 기관(위험방지기관인 경찰) 그리고 안보와 관련된 범죄를 수사하는 기관(수사기관)으로 구성되어 있다. 이 기관들은 국가안보라는 공동의 임무를 수행한다. 국가안보의 궁극적 목적은 국가보호 및 헌법보호라고 할 수 있다.

지난해 국가정보원법의 개정으로 특히 대공수사권이 경찰로 이관되면서 국가정보원은 이제 국외 정보기관의 역할만 수행하게 되었다. 따라서 국가안보와 관련된 사안에서 앞으로 정보기관, 위험방지기관, 수사기관 사이의 관계를 어떻게 정립해야 하는지 문제가 제기되었다. 이러한 문제 제기는 이 기관들 사이에 분리원칙(Trennungsgebot)과 협력관계를 천명하고 있는 독일의 제도를 비교법적으로 연구할 계기를 제공하였다.

독일에는 3개의 연방정보기관(연방헌법보호청(BfV), 연방정보부(BND), 군정보부(MAD))과 16개의 주정보기관(주헌법보호청)이 존재한다. 이들 정보기관은 분리원칙에 의해서 위험방지 경찰 및 수사기관과 조직, 직무, 권한, 정보에서 분리되어 있다. 하지만 독일의 정보기관은 이러한 분리원칙에도 불구하고 위험방지기관인 경찰 및 수사기관과의 상호협력을 통하여 각자의 역할을 수행함으로써 국가안보에 공동으로 기여하고 있다. 특히 정보교환을 통한 협력관계에서 정보기관은 정보의 수집 및 분석 활동으로 알게 된 위험방지나 범죄수사에 관한 정보를 경찰이나 수사기관으로 전달함으로써 정보기관이 '간접적으로' 형사정책적 기능도 함께 수행하고 있다. 게다가 최근 독일입법자는 암호통신감청, 전략적 해외통신감청, 온라인 수색과 같은 새로운 정보수집권을 정보기관에게 부여함으로써 이러한 기능은 더욱 강화될 것으로 보인다.

이제 한국에도 정보와 수사가 분리되었다. 이러한 분리는 행정부 내의 권력분립이 실현된 것으로 바람직한 방향이라고 여겨진다. 하지만 여러 가지 문제점이 발견된다. 첫째, 정보기관의 정보수집에 관한 규정이 명확하지 않고, 둘째, 정보수집권이 현재의 정보통신기술에 대응하지 못하고 있으며, 셋째, 정보이전과 같은 협력에 관한 규정이 명확하지 않다. 따라서 정보기관과 수사기관이 국가안보에 공동으로 기여하기 어려울뿐 아니라 그리하여 정보기관에게 '간접적' 형사정책기능도 기대하기 어렵다.

* 이 논문은 2020년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2020S1A5A2A01043286).

** 독일 막스플랑크 국제형법연구소 연구원, 법학박사

따라서 국가정보원법에 정보기관의 정보수집권 규정이 명시되어야 하고, 그러한 정보수집권은 정보통신기술의 발전에 맞추어 다양해야 하며, 정보기관과 수사기관 사이의 정보 공유 및 상호협력 관계가 구체화되어야 할 것이다.

DOI : https://doi.org/10.36889/KCR.2021.9.30.3.101.

❖ 주제어 : 정보기관, 분리원칙, 암호통신감청, 전략적 해외통신감청, 온라인 수색, 연방헌법보호청, 연방정보부, 군정보부

Ⅰ. 문제 제기

지난해 국가정보원법의 개정[1]으로 특히 대공수사권이 경찰로 이관되면서 이제 국가정보원은 순수한 정보기관[2]의 역할을 하게 되었다. 국가정보원은 국가안전보장에 관한 업무를 수행한다. 국가안전보장(국가안보)의 궁극적 목적은 국가보호 및 헌법보호라고 할 수 있다. 일반적으로 국가안보와 관련한 업무를 수행하는 기관은 정보를 수집하는 기관(정보기관), 안보와 관련된 위험을 방지하는 기관(위험방지기관인 경찰) 그리고 안보와 관련된 범죄를 수사하는 기관(수사기관: 경찰과 검찰)으로 구성되어 있다. 이번 국가정보원법 개정은 정보기관, 위험방지기관 그리고 수사기관으로 분리된 것으로 볼 수 있다. 형식적으로 보면 독일의 정보기관과 경찰(위험방지기관 및 수사기관)의 분리원칙(Trennungsgebot)의 모습을 띄고 있다.

독일의 경우 정보기관, 위험방지기관, 수사기관이 모여서 국가안보, 나아가서 헌법보호라는 공동의 직무를 수행하고 있다. 이러한 세 개의 기둥이 모여서 국가안보라는 건축물을 구성하고 있다고 하여, 이를 안보건축물(Sicherhietsarchitektur)이라고 표현하고 있다.[3] 이러한 안보관련 기관에 적용되는 개별 법률들을 포괄하는 상위개념으로 안보법(또는 안전법)(Sicherheitsrecht)이라는 개념도 사용되고 있다. 안보건축물은 조직, 직무, 권한 등이 각기 다른 세 기관으로 분리되어 있지만, 안보건축물이 무너지지 않고 지속적으로 유지되기 위해서는 역할이 다른 세 개의 기관이 상호 협력해야 한다는 의미를 내포하고 있다. 상호협력이란 말 속에는 세 개의 기관이 공통적으로 수행하는 기능이 있다. 바로 '정보수집'이다. 정보기관은 국가안보와 관련된 정보를 수집 및 분석하여 국가의 정책결정권자에게 보고한다. 위험방지경찰은 국가안보와 관련된 정보를 수집하여 위험이 발생하지 않도록 사전에 방지하고, 수사기관은 이러한 정보를 수집하여 형사절차에서 증거로 사용한다. 정보수집과 분석을 주요 임무로 하는 정보기관은 성격상 정보활동을

1) 국가정보원법 [시행 2021. 1. 1.] [법률 제17646호, 2020.12.15, 전부개정]

2) 국가정보원법 전부안의 개정 이유서.

3) 독일 안보관련 법률 문헌에서 안보체계(Sicherhietssystem)가 아니라 안보건축물(Sicherhietsarchitektur)이라는 용어를 사용한 것은 세 개의 기둥이 각자 다른 성격을 지니고 있기 때문이다. 여기서 아키텍투어(Architektur)는 건축, 건축물, 건축술, 구성(체), 구조(물) 등 다양하게 번역될 수 있다. 이 글에서는 독일의 전체 안보구조가 성격이 서로 다른 세 개의 기둥으로 떠받치고 있다는 점을 시각적으로 부각시키기 위해서 안보건축(물)이라는 용어를 사용한다.

통해서 위험방지 및 범죄와 관련한 정보를 수집할 개연성이 상당히 높다. 정보기관은 일반적으로 위험방지나 수사기관과 달리 집행권한이 없으므로 기본권 침해의 정도가 낮기 때문에 정보수집의 제한요건이 상대적으로 느슨하고 수집되는 정보의 범위도 훨씬 넓다. 그런데 정보기관은 수집한 정보를 해당 기관에 제공하거나 제공할 수 있다. 안보건축물이 무너지지 않도록 상호 협력해야 하기 때문이다. 상호협력은 이러한 정보의 제공으로 구체화된다. 따라서 상호협력의 핵심은 결국 이러한 정보를 전달하여 공유하는 것이라 할 수 있다. 이러한 상호협력이 가능하기 위해서는 세 개의 기관이 유사한 정보수집권을 가지고 있어야 한다.

독일 정보기관은 이전부터 이러한 유사한 정보수집권을 가지고 있었고, 입법자는 최근 정보기관에게 정보수집권을 확대하기 위해 관련 법률도 개정하였다. 암호통신감청, 온라인 수색, 전략적 해외통신감청 등이 그것이다. 이러한 정보수집권들은 위험정보나 범죄정보를 수집할 개연성이 더욱 높다. 독일 정보기관의 이러한 정보수집권의 확대는 전체 안보건축물의 유지에 기여하기 위한 것이다. 이러한 점에서 우리 정보기관은 안보건축을 유지하기 위해서 어떠한 정보수집권한을 수행하고 있고 다른 기관들과 어떻게 협력하고 있는지 의문이 제기된다. 만일 정보기관이 다른 기관과 형식적으로 분리만 되어있고 정보제공과 같은 실질적인 협력이 이루어지지 않는다면 우리의 전체 안보건축은 부실해질 수 있기 때문이다. 특히 정보기관이 정보활동으로 수집하거나 알게 된 범죄관련 정보를 수사기관에게 제공하는 것은 형사정책적 관점에서 중요한 의미를 가진다.

따라서 이 글은 독일 입법자가 최근 정보기관에게 어느 정도까지 정보수집권을 확대하려고 시도하였고, 현재는 얼마만큼 법제화되어 있는지 검토하고, 이러한 권한확대가 형사정책적으로 어떠한 의미를 가지는지 도출한다. 이러한 검토 결과를 우리 정보기관의 정보수집권과 관련한 법적 상황을 검토하고 개선 방향을 제시하고자 한다.

최근 아프가니스탄 대통령이 해외로 도피하고 탈레반이 무혈입성한 사건을 서방세계의 정보기관들은 사전에 거의 인지하지 못하였다. 정보기관의 역할의 중요성을 일깨워주는 사건으로 판단된다. 따라서 이러한 배경에서 우리 정보기관의 현재의 법적 상황을 검토하는 것은 상당한 의미가 있다고 생각된다.

Ⅱ. 독일 정보기관의 구성, 법적 체계 및 직무

1. 독일 정보기관의 구성

독일의 경우 헌법보호와 관련하여 정보를 수집하는 정보기관, 헌법보호와 관련한 위험방지를 담당하는 경찰 그리고 범죄를 수사하는 수사기관(경찰 및 검찰)이 모여서 하나의 안보건축물(Sicherheitsarchtektur)을 구성하고 있다. 헌법보호임무를 맡고 있는 정보기관은 국내정보를 관할하는 연방헌법보호청(BfV), 국외정보를 관할하는 연방정보부(BND) 그리고 군내의 방첩을 담당하는 군정보부(MAD)로 나뉜다.[4] 또한 16개 주에는 주의 헌법보호임무를 담당하는 각자의 주헌법보호청(LfV)이 존재한다. 따라서 독일에는 3개의 연방정보기관과 16개의 주정보기관이 있다.

2. 독일 정보기관의 법적 체계

정보기관들은 개별 법률에 따라 서로 다른 주무관청의 산하에 설치되어 있다.[5] 연방헌법보호청은 연방헌법보호법(BVerfSchG)에 의해서 연방내무부에 설치되어 있고, 연방정보부는 연방정보부법(BNDG)에 의해서 연방수상청에 그리고 군정보부는 군정보부법(MADG)에 의해서 연방국방부에 설치되어 있다. 그리고 16개 주에 각자의 헌법보호법에 따라 독자적인 기관이 설치되어 있거나 주내무부에 속해 있다. 이러한 법률 중에서 연방헌법보호법이 기본법의 역할을 하고, 다른 법률들은 이 법률의 규정들을 준용하거나 적절하게 관련시키고 있다.

한편 통신비밀을 제한하기 위한 '서신, 우편 및 전기통신의 비밀 제한에 관한 법률'(기본법 제10조법, G10법, 이하 '통신비밀제한법')[6]은 모든 정보기관에게 적용된다. 통신비밀제한법에는 특정 개인을 상대로 하는 일반적 통신감청 외에 불특정 다수를 대상으로 하는 전략적 국제통신감청규정이 포함되어 있다. 후자의 감청은 독일과 외국 사이의

4) Gusy, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, Ⅳ § 1, Rn. 41 ff.

5) Gusy, a.a.O., Ⅳ § 1, Rn. 44 ff.

6) 통신비밀제한법에 대한 전반적인 내용은 다음 문헌 참조: Huber, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 3 Artikel 10-Gesetz.

통신을 감청하는 것으로 연방정보부에게만 적용된다. 통신비밀제한법은 경찰의 위험방지나 수사기관의 범죄수사를 위한 통신감청에는 적용되지 않는다. 위험방지와 범죄수사를 위한 통신감청은 연방 및 주 경찰법과 형사소송법에 각각 별도로 규정되어 있다.

3. 정보기관의 직무

연방 및 주헌법보호청의 직무는 일부 중복되지만 전체 8가지의 헌법적 가치질서에 반하는 시도(Bestrebungen)와 활동에 관한 정보를 수집하고 분석하는 것이다(연방헌법보호법 제3조 제1항). 8가지의 시도와 활동은 자유민주적 기본질서에 반하는 시도, 연방 또는 주의 존립에 반하는 시도, 연방 또는 주의 안전에 반하는 시도[7], 헌법기관의 불법적 침해를 위한 시도, 타국을 위해 안보를 위태롭게 하는 활동, 타국을 위한 정보기관의 활동, 폭력적 시도를 통하여 외교적 이익을 위태롭게 하는 활동, 국제평화에 위배되는 시도 등이다. 헌법적대적 시도란 헌법상 보호이익의 제거 또는 침해를 목적으로 하는 인적단체에서 또는 이를 위해서 정치적으로 목적 및 목표가 정해진 특정된 행동방식을 말한다.[8] 헌법보호청의 가장 중요한 임무는 자유민주적 기본질서[9]에 반하는 활동을 감시하는 것이다.

군정보부의 직무는 헌법보호청과 거의 유사하게 규정되어 있다. 따라서 군정보부의 중요 직무는 자유민주적 기본질서와 연방 및 주의 존립과 안전에 반하는 시도 및 안보를 위협하는 정보를 수집하고 분석하는 것이다.

연방정보부의 직무는 독일연방공화국의 외교 및 안보정책상 중요한 외국에 대한 '새로운 정보'(Erkenntnisse, intelligence)[10]를 확보하기 위해 필요한 정보(Informationen)를 수집하고 분석하는 것이다(연방정보부법 제1조 제2항). 외국에 대한 정보수집은 국외뿐만 아니라 국내에서도 수행된다.

---

7) 이러한 '시도'에 대한 법적 개념은 연방헌법보호법 제4조에서 정의하고 있다.

8) Roth, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BVerfSchG § 4 Rn. 6.

9) 자유민주적 기본질서의 개념에 대해서는 명재진, 독일 헌법수호청에 관한 연구, 법과 정책연구 제19집 제1호, 2019, 94면 참조.

10) Erkenntnisse란 정보기관이 일반적인 정보(Informationen)를 수집하고 분석하여 새롭게 알아낸 정보(지식)를 말한다. 영어의 intelligence에 대응하는 개념이다.

독일 정보기관들은 분리원칙에 의해서 경찰과 별도의 조직으로 구성되어 각자의 직무를 수행하고 있지만, 궁극적인 지향점은 헌법보호라는 것을 알 수 있다.

Ⅲ. 독일 정보기관의 정보수집권[11)]

1. 공개 정보수집

정보기관은 자신의 정보를 능동적 또는 수동적 활동을 통해서 수집할 수 있다. 능동적 정보수집은 정보기관을 통해서 정보를 직접 확보하는 것임에 반하여 수동적 정보수집은 제삼자가 정보기관에 정보를 제공하거나 다른 기관의 정보를 이용하는 것이다. 독일 정보기관의 정보수집은 기본법의 역할을 하는 연방헌법보호법의 정보수집과 관련한 규정들을 준용하고 있다.

연방헌법보호법 제8조 제1항에 따르면 "직무 수행을 위해서 필요한 개인정보를 포함하여 정보를 처리할 수 있다". 하지만 제8조 제1항 후반부에서 "적용될 연방개인정보보호법의 규정 또는 이 법률의 다른 특별한 규정에 저촉되지 않는 한"이라는 조건을 달고 있다.[12)] 따라서 이 규정은 정보수집을 위한 특별한 권한규범이 아니다.[13)] 정보기관의 수단을 이용한 정보수집은 동법 제9조와 제8조 제2항에서 특별한 규정들을 두고 있다. 따라서 제8조 제1항이 실제로 적용되는 영역은 공개 정보수집으로 제한된다. 즉 공개 출처(예를 들어 신문, 방송 등)나 공개 조회를 통해서 정보를 수집하는 경우에는 제8조 제1항이 적용된다.

---

11) 독일 정보기관의 구성, 법적 체계 및 직무 등에 관해서는 이미 국내문헌에서 어느 정도 소개되어 있으나 정보수집에 대해서는 현재 거의 소개되어 있지 않다.

12) Brandt, Das Bundesamt für Verfassungsschutz und das strafprozessuale Ermittlungsverfahren, 2015, S. 49.

13) Vgl. BT-Drucksache 11/4306, S. 61.

2. 비밀 정보수집으로서 정보기관수단의 투입

가. 정보기관수단의 개념

연방헌법보호법은 제8조 제2항과 제9조에서 정보기관의 수단을 투입(Einsatz nachrichtendienstlicher Mittel)하여 정보를 수집하는 권한을 부여하고 있다. 제8조 제2항에 따르면 "연방헌법보호청은 비밀리에 정보를 수집하기 위하여 신뢰인(Vertrauensleuten) 및 보증인(Gewährspersonen)의 투입[14], 관찰, 녹화 및 녹음, 위장신분증 및 위장표지와 같은 방법, 대상 및 도구를 이용할 수 있다." 연방헌법보호법이 정보기관의 수단을 언제 투입할 수 있는지는 제9조에서 규정하고 있다. 따라서 제9조와 제8조 제2항은 구성요건과 법적효과의 관계에 있다. 즉 정보기관의 수단을 투입할 요건이 갖추어지면(동법 제9조), 그 투입은 허용된다(동법 제8조 제2항).[15]

정보기관수단의 투입이란 정보기관의 특징을 나타내는 표현이다. 1950년 연방헌법보호청이 설립될 당시 정보기관수단이란 용어는 사용되지 않았다. 1972년 연방헌법보호법의 개정으로 정보기관의 수단을 이용할 권한이 도입되었다.[16] 당시 입법자는 정보기관

14) 정보기관에 일정한 정보를 제공하거나 협력하는 자를 일상적인 언어로 '정보원'이라고 부른다. 이러한 정보원에는 신뢰인(Vertrauensleuten, V-Leute(복수), V-Mann(단수)), 보증인(Gewährspersonen), 정보제공자(Informant) 그리고 이중스파이(Counterman)가 있다. 신뢰인은 '계획적으로 장기간 연방헌법보호청에 협력하는 것이 제3자에게 알려지지 않은 사인'이라고 규정되어 있다(연방헌법보호법 제9b조 제1항 제1문). 따라서 '비밀협력자' 또는 '신뢰할 수 있는 정보원(신뢰정보원)'이라는 번역어가 적합할 수 있다. 신뢰인은 정보기관으로부터 일정한 교육을 받고 투입되며 정보제공활동에 대해서 정기적으로 보수를 받지만 정보기관의 정식요원은 아니다. 실무에서는 극우단체의 구성원을 신뢰인으로 투입하여 그 단체의 정보를 제공받고 있다. 이와 달리 보증인은 교육이나 정기적인 보수를 받지 않지만 연방헌법보호청에 정보를 제공하는 자를 말한다(연방헌법보호법 제8조 제2항). 보증인이 제공하는 정보는 보증할 수 있다는 의미에서 '보증정보원'이라는 표현을 쓸 수 있다. 정보제공자는 개별 사건에서 또는 우연히 정보기관에 정보를 전달하는 자를 말하므로 '우연정보원'이라고 표현할 수 있다. 카운터맨은 외국 정보기관의 요원으로서 독일 정보기관을 위해서 활동하는 이중스파이를 말한다. 정보제공자와 카운터맨은 정보기관법에 규정되어 있지 않다. 정보기관은 보증인, 정보제공자, 카운터맨을 일반규정(특히 연방헌법보호법 제8조 제2항과 제9조 제1항)에 따라 이용할 수 있다(이에 대해 자세한 내용은 박희영/윤해성/김재현/임유석, 독일 온라인 안보정보수집 법제연구, 2021년도 국가보안기술연구소, 위탁연구보고서 2021-147, 제4장 제3절 3. 신분위장요원과 신뢰인 투입 부분 참조).

15) Brandt, a.a.O.(Fn. 12), S.49.

16) BGBl. I 1972 S. 1382.

수단의 개념을 정의할 필요까지는 없다고 보았다.[17] 1990년 연방헌법보호법의 개정 과정에서 정보기관수단의 투입에 관한 새로운 규정이 도입되었고 현재까지 이 체계를 유지하고 있다. 이 당시 입법자는 이 법률에서 정보기관수단을 "비밀리에 정보를 수집하기 위한 방법, 대상 및 수단"이란 표현으로만 정의하고, 구체적인 내용은 직무규정에서 정하려고 하였다. 하지만 의회의 입법과정에서 연방상원의 제안으로 정보기관의 수단의 개별적 사례그룹을 예시적으로 규정하기로 하였다.[18] 그리하여 정보기관수단이란 용어는 법률문언에서 삭제되고 그 대신 "특별한 유형의 데이터수집"으로 규정되었다. 정보기관수단의 투입의 법적 개념을 도입하려는 입법적 시도는 2019년 연방내무부의 '헌법보호법을 조정하기 위한 법률초안'[19]에서 다시 나타났다.[20]

이 법률초안 제9조는 정보기관의 수단을 법적으로 정의하고 있다. 이에 따르면 정보기관수단이란 "비밀 정보수집을 위한 방법, 대상 및 수단"(법률초안 제9조 제1항 제1문)으로 정의하고 정보기관수단을 8가지[21]로 예시적으로 열거하고 있다(법률초안 제9조 제1항 제2문). 법률초안 제9조는 지금까지 실무에서 수행되던 정보기관수단을 체계적으로 정리한 것이다.

하지만 이 조항은 법제화되지 못하였다. 이 법률초안에 들어있던 정보기관수단인 온라인수색과 정보기술시스템 이용 주거 감시의 도입을 연정파트너인 사회민주당(SPD)이 반대함으로써 법률초안 자체가 연방정부의 법률안으로도 채택되지 못했기 때문이다. 비

17) BT-Drucksache VI/3533, S. 5.

18) BT-Drucksache 11/4308, S. 85.

19) Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat : Entwurf eines Gesetzes zur Harmonisierung des Verfassungsschutzrechts. 연방내무부의 '법률초안'은 연정내각을 구성하고 있는 사민당(SPD)과 특히 이 당 소속 연방법무부 장관의 반대로 연방정부의 '법률안'으로 채택되지 못했다.

20) https://bit.ly/3n41qeY(전체 인터넷 주소(URL)는 참고문헌 참조).

21) 1. 위장신분(특히 허구의 이력, 직업 또는 영업 정보), 위장신분증 및 위장표식의 취득, 작성 및 사용. 2. 헌법보호기관의 업무에 협력하거나 기타 도움을 주는 자. 3. 개별 사례에서 또는 경우에 따라서 관찰분야에서 접촉하여 단서를 제공하는 자. 4. 관련자의 보호될 신뢰를 이용하여 인터넷에서의 정보수집. 5. 계획적이고 지속적으로 정보수집을 위해서 투입되는 자를 통한 조사(비밀조사). 여기에는 a. 그 투입이 연방헌법보호청을 위해서 알려지지 않는 자(신뢰인)와 b. 정보요원으로서 장기 부여된 위장신분을 사용하는 자(신분위장요원)가 있다. 6. 관찰. 7. 기술적 수단. 특히 비밀리에 a. 사람, 대상 또는 사건을 광학적 또는 음성적 감시를 위해서 그리고 b. 특히 전송된 내용, 상세한 상황 또는 전송하는 기기에 관한 정보를 확보하기 위한 기술적 신호를 규명하기 위한 기술적 신호. 8. 일시적인 물건의 비밀 점유.

록 법률초안 제9조는 입법되지 않았지만 현행 연방헌법보호법 제8조 제2항에 열거되어 있는 정보기관의 수단을 해석하는데 참고가 될 수 있다. 연방헌법보호법 제8조 제2항에는 정보기관의 수단이 추상적으로 열거되어 있다. 즉 비밀리에 정보를 수집하기 위하여 "신뢰인 및 보증인, 관찰, 녹화 및 녹음, 위장신분증 및 위장표지의 투입"이다. 이러한 열거는 예시에 해당된다. 이 권한 규정은 비밀 정보수집의 기술적 발전에 신속하게 대응하기 위해서 예시규정을 둔 것이다.[22]

나. 정보기관수단의 투입 요건

연방헌법보호청은 제8조 제2항에 예시적으로 열거되어 있는 정보기관의 수단을 곧바로 수행할 수 없다. 제8조 제2항은 권한규범이 아니기 때문이다. 정보기관수단의 허용은 동법 제9조에 규정되어 있다. 다만 통신비밀제한법 제3조에서 예외적으로 규정하고 있다. 또한 전략적 해외통신감청은 연방정보부법에 규정되어 있다.

(1) 일반 요건(연방헌법보호법 제9조 제1항)

입법자는 정보기관수단의 투입 권한과 관련하여 연방헌법보호법 제9조 제1항에서 일반조항을 두고 있다. 이에 따르면 연방헌법보호청은 두 가지 경우에 정보기관의 수단(제8조 제2항의 수단)을 이용하여 정보, 특히 개인정보 등을 수집할 수 있다. 즉 이러한 방법으로 동법 제3조 제1항의 시도나 활동에 관하여 알게 된 정보나 그러한 정보의 조사에 필요한 정보원(Quelle)이 확보될 수 있는 경우이다(제9조 제1항 제1호).

(2) 특별 요건(연방헌법보호법 제9조 제2항과 제4항)

입법자는 기본법 제11조(통신비밀)와 제13조(주거의 불가침)가 보호되는 영역에서 정보기관의 수단을 가능하도록 하기 위해서 연방헌법보호청에게 특별한 권한규정을 부여하고 있다. 주거내 비밀 대화의 도청과 가상기지국의 설치(IMSI-Catcher)가 그것이다. 나아가서 데이터 수집의 특별한 형태로서 신분위장요원과 신뢰인의 투입도 규정하고 있다. 그밖에 정보를 요청할 수 있는 권한도 부여하고 있다. 이에 관해서는 아래의 개별적

22) BT-Drucksache 11/4308, S. 85.

정보수집에서 별도로 검토한다.

3. 개별적 정보수집권

가. 주거 내 비밀 대화 도청

연방헌법보호법 제9조 제2항은 주거 내에서 행해지는 비밀 대화를 기술적 수단을 이용해서 도청할 수 있는 권한을 정보기관에게 허용하고 있다. 이에 따르면 정보기관은 개별적인 경우 현재의 공동 위험의 방지나 개인의 현재 생명의 위험을 방지하기 위하여 불가피하고 법익의 위협에 대한 적합한 경찰의 구조가 적시에 요청될 수 없는 경우에 한해서 주거 내에서의 비공개 대화를 기술적인 수단을 이용하여 비밀리에 청취 및 녹음할 수 있다. 이러한 방법은 녹화 및 녹음을 하기 위해서 비밀리에 기술적인 수단을 사용하는 경우에도 준용된다. 정보기관의 주거 내 비밀 대화는 음성감시뿐 아니라 영상감시도 가능하다. 이 점은 음성감시만 허용하고 있는 형사소송법(제100c조)의 주거 내 감시와 구별된다. 이러한 차이는 주거불가침권을 규정한 기본법 제13조에서 나온다. 기본법 제13조 제3항에서 범죄수사를 위한 주거수색에서는 음성감시만 가능하고, 제13조 제4항에서 위험방지를 위해서는 음성 및 영상 감시에 차이를 두고 있지 않기 때문이다.

기본법 제13조 제4항에 따르면 주거 내 비밀 대화 도청은 법관의 영장이 필요하다. 정보기관의 수단 중에서 '유일하게' 법관의 영장(법관유보)을 요구하고 있다.[23] 지체의 위험이 있는 경우 긴급 주거 내 감시도 가능하다. 하지만 지체없이 법관의 승인을 받아야 한다.

나. 가상 기지국 설치(IMSI-Catcher)

이용대기상태에 있는 휴대전화의 위치정보는 이동통신기술의 특성 때문에 실제로 통신이 행해지지 않더라도 생성된다. 휴대전화와 같은 이동통신기기는 통신이 가능한 상태를 항상 유지하기 위해서 가장 가까운 통신기지국과 자동으로 교신하기 때문이다.[24] 이

23) 다른 정보기관의 수단을 투입하는 경우에는 법관의 영장을 요구하지 않는다.

24) 박희영, 이용대기상태의 휴대전화 위치정보 수사의 허용과 입법방향, 형사정책연구 제31권 제2호 (통권 제122호, 2020· 여름), 75.

러한 상황을 이용한 것이 바로 IMSI-Catcher라는 기기를 이용한 가상 기지국 설치이다.

연방헌법보호법은 제9조 제4항에 이러한 가상기지국을 설치하여 대상자의 대기상태에 있는 휴대전화의 위치정보나 기기번호 및 유심칩카드번호를 수집할 수 있는 권한을 부여하고 있다. 이러한 조치가 허용되기 위해서는 기술적 수단의 투입이 없이는 대기 중의 휴대전화의 위치 조사나 기기 번호 또는 유심칩카드번호의 조사가 불가능하거나 본질적으로 어려워야 한다. 이 조치의 대상자는 동법 제8a조 제3항 제1호와 제2호에서 표시된 사람이다. 데이터의 처리에 대해서는 통신비밀제한법 제4조가 준용된다.

다. 신분위장요원과 신뢰인 투입

연방헌법보호법 제9a조와 제9b조는 신분위장요원(Verdeckter Mitarbeiter)[25]과 신뢰인(Vertrauensleute, V-Leute)을 투입하여 정보를 수집할 수 있는 방법을 규정하고 있다. 연방정보부법(BNDG)은 제5조 제2문에서 이를 준용하고 있다. 이러한 규정들은 '2015년 11월 17일의 헌법보호영역에서 협력을 개선하기 위한 법률' 제1조에 의해서 도입되었다.[26] 도입 동기는 17대 연방의회의 헌법보호기관의 협력과 기능에 관한 포괄적인 조사의 결과였다. 특히 미국 NSA 스캔들에 관한 제2차 조사위원회의 조사 결과[27]와 연방 및 주의 극우테러리즘 위원회(BLKR)[28]의 조사 결과였다. 입법이유에 따르면 비밀리에 인간 자원을 투입하여 계획적이고 체계적으로 정보를 수집하는 것은 자신들의 목적을 비밀리에 수행하는 극우주의자들의 시도를 규명하기 위해서는 필수적인 수단이라고 한다. 이 경우 헌법보호청의 요원인 신분위장요원뿐 아니라 사인인 신뢰인도 투입될 수 있다. 신뢰인은 헌법보호청을 위해서 실제로 상당한 의미가 있다.[29]

---

25) Verdeckte Mitarbeiter는 독일형사소송법 제110a조(신분위장수사관, Verdeckte Ermittler)의 조문 형식을 차용하여 2015년에 규정되었다. 형사소송법에서의 명칭의 번역과 관련한 논의는 민영성/강수경, 독일의 인터넷 비밀수사에 관한 논의와 그 시사점, 국민대학교 법학논총 제31권 제2호, 2018, 362면 각주 4 참조. 아동·청소년의 성보호에 관한 법률 제25조의 2 제2항에서 '신분위장수사'의 법적개념을 정의하고 있으므로 '신분위장수사관'이 적합한 번역어라 생각된다.

26) Gesetzes zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I 2015 S. 1938). 이 법률의 소개에 대해서는 다음 참조: Marschoileck, NJW 2015, 3611-3616.

27) NSU-UA; Abschlussbericht: Bundestagsdrucksache 17/14600.

28) BT-Drucksache 18/4654 S. 18.

29) BT-Drucksache 18/4657 S. 25; Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des

라. 비공공기관에 정보요청권

정보기관은 비공공기관에 대하여 특정한 정보의 제공을 요청할 수 있다. 정보기관은 항공사, 금융기관 등 고객 정보, 조세기본법에 정한 일정한 조세관련 데이터를 요청할 수 있다(연방헌법보호법 제8조 제1항 제1호, 제2호, 제8조 제2항).

통신정보와 관련하여 정보기관은 '전기통신 및 텔레미디어 데이터 보호법'(TTDSG)[30] 제9조 제1항의 임의 보관 트래픽데이터(통신사실확인자료)(동법 제8a조 제1항 제4호)[31]와 텔레미디어 서비스 이용자의 신원확인을 위한 식별표시, 서비스 이용 시간 및 범위, 서비스 이용에 관한 정보(연방헌법보호법 제8a조 제1항 제4호)를 요청할 수 있다. 또한 정보기관은 전기통신사업자에게 전기통신법 제3조 제6호 및 제172조에 의한 가입자정보를 그리고 텔레미디어서비스제공자에게 TTDSG 제2조 제2항 제2호에 의한 가입자정보를 각각 요청할 수 있다(연방헌법보호법 제8d조 제1항). 정보기관은 또한 특정 시점에 부여된 유동 IP주소(제8d조 제2항)뿐 아니라 단말기 또는 이 단말기와 공간적으로 분리되어 있는 저장기기 등에 접근하기 위한 비밀번호와 같은 접근 데이터(제8d조 제3항)도 요청할 수 있다.

정보요청절차와 관련하여 각 정보기관이 연방내무부장관에게 이러한 정보요청을 청구하고 장관이 명령한다. 장관은 명령을 내리기 이전에 G10위원회[32]에 보고하여 정보요

Bundes, BVerfSchG § 9a, Rn. 1.

30) TTDSG는 전기통신법(TKG)과 텔레미디어법(TMG)의 개인정보보호규정을 EU 일반개인정보보호법((EU) 2016/679)과 전자프라이버시지침(2002/58/EC)에 맞도록 조정하기 위해 제정되었다. 현재 전기통신법과 텔레미디어법의 개인정보보호규정과 통신비밀보호규정들이 TTDSG에서 하나로 통합되었다. 이번에 전부 개정된 전기통신법과 새로 제정된 TTDSG는 2021년 12월 1일부터 각각 발효된다.

31) 트래픽데이터(Verkehrsdaten, traffic data)는 우리 통신비밀보호법의 통신사실확인자료에 대응하는 개념이다. 독일 전기통신법(TKG)은 전기통신사업자가 의무적으로 보관해야 하는 트래픽데이터(제113a조 내지 제113c조)와 임의로 보관할 수 있는 트래픽데이터(제96조)를 구분하고 있다. 우리의 통신사실확인자료는 의무적 보관이란 측면에서 전자와 유사하고 종류와 범위의 측면에서 후자와 유사하다. 전기통신법 전부 개정법률에 의해서 제113a조 내지 제113c조의 트래픽데이터는 제175조 내지 제177조로 이전되고, 제96조의 트래픽데이터는 TTDSG 제9조 제1항에서 규정되었다. 하지만 정보기관은 수사기관이나 위험방지기관과 달리 '의무적으로 보관해야 하는 트래픽데이터'는 요청할 수 없다(독일 전기통신법의 트래픽데이터에 관한 자세한 설명은 박희영, 이용대기상태의 위치정보 수사의 허용과 입법방향, 형사정책연구 제31권 제2호(통권 제112호, 2020. 여름), 95면 이하 참조).

32) G10위원회(G10 Kommission)는 통신의 비밀과 관련하여 정보기관을 통제하는 기관이다. G10위원

청의 적법성과 필요성을 심사받아야 한다. 즉 정보요청은 G10위원회의 허가를 받아야 한다. 긴급한 경우 사후에 G10위원회의 심사를 받을 수 있다.

Ⅳ. 최근 도입된 정보기관의 정보수집권

1. 연방내무부의 '헌법보호를 조정하기 위한 법률초안'

연방내무부는 2019년 3월 정보기관의 정보수집권을 확대하기 위한 '헌법보호법을 조정하기 위한 법률초안'을 제안하였다.[33] 이 초안이 공식적으로 발표되기도 전에 언론을 통해서 공개되면서 각계 각층으로부터 많은 비판을 받았다. 이 법률초안의 중요 내용은 연방헌법보호법, 연방정보부법, 통신비밀제한법 등을 개정하여 새로운 정보기관수단을 도입하는 것이다. 이 법률초안은 특히 전기통신법에 의해서 의무적으로 보관해야 되는 통신사실확인자료의 제공요청, 암호통신감청(통신비밀제한법 제11조), 정보기술시스템 침입(온라인 수색), 정보기술시스템 이용 주거내 감시를 허용하고 있다.

현재 정보기관은 전기통신사업자가 의무적으로 저장하여 보관해야 하는 통신사실확인자료(전기통신법 제113a조 내지 제113c조, 2021년부터는 제175조 내지 제177조)는 요청할 수 없고, 임의로 저장하여 보관하는 통신사실확인자료(전기통신법 제96조, 2021년부터는 새로 제정된 TTDG 제9조)만 요청할 수 있다.

법률초안은 암호통신감청과 온라인수색도 허용하였다. 온라인 수색은 정보기술시스템에 침입하여 거기에 있는 데이터를 수집하거나 시스템 이용 현황을 파악하는 것이다.[34] 물론 통신이 진행 중이면 실시간으로 통신정보도 수집될 수 있다. 연방정보부법 개정안은 국내와 해외에 있는 정보기술시스템 침입을 구별하여 각각 규정하고 있었다. 우선 국

회는 전체 10명의 위원으로 구성되며 이 중에서 3명의 위원과 3명의 대리위원은 법관의 자격이 있어야 한다. G10위원회는 법원과 유사한 법적 통제를 행사한다 (G10위원회에 대한 자세한 내용은 박희영/윤해성/김재현/임유석, 앞의 위탁연구보고서 2021-147(각주 14), 제6장 제3절 3. 다. G10위원회의 감독 부분 참조).

33) https://bit.ly/3n41qeY(전체 인터넷 주소(URL)는 참고문헌 참조).

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

내의 정부기술시스템 침입과 관련하여 연방정보부는 당사자 모르게 기술적 수단을 이용하여 '독일국적자', '국내 법인' 또는 '독일에 체류하고 있는 자'의 정보기술시스템에도 침입하여 거기서 처리되는 데이터를 수집할 수 있다(법률초안 제5b조 제1항 제1문). 이와 병행하여 해외에 있는 외국인의 정보기술시스템 침입도 규정하고 있다(법률초안 제5c조).

나아가서 법률초안은 정보기술시스템에 침입하여 거기에 장착되어 있는 카메라나 마이크를 작동시켜서 이 시스템을 사용하고 있는 사람과 주거를 감시하는 정보기술시스템을 이용한 주거내 감시도 도입하고 있다(법률초안 제5d조). 이것은 IT 기본권 뿐아니라 주거의 불가침 기본권까지 제한한다. 암호통신감청이나 온라인수색은 경찰의 위험방지나 수사기관의 범죄수사를 위해서는 허용되고 있지만, 정보기술시스템을 이용한 주거내 감시는 허용하고 있지 않다. 이러한 입법시도는 독일 법에서는 최초로 시도한 것이다.

이 법률초안과 관련하여 연정파트너인 사회민주당(SPD)이 특히 정보기관에게 정보기술시스템에 침입하는 권한을 부여하는 것에 반대하였다. 그리하여 연방내무부 장관과 사회민주당 소속인 연방법무부 장관은 서로 합의하여 암호통신감청(통신비밀제한법 제11조 제1a항과 제1b항)과 해외에 있는 외국인의 정보기술시스템 침입(연방정보부법 제34조)만 도입하기로 하였다. 두 가지 정보수집방법은 2021년 상반기에 법제화되었다. 아래에서 살펴본다.

2. 통신비밀제한법의 암호통신감청(Quellen TKÜ)

앞서 언급한 법률초안은 수정 작업을 거쳐 정부안으로 확정되어 연방의회에 제출되었고[35] 특별한 이견없이 의결되어 2021년 7월 6일부터 발효되었다.[36] 이 법률은 연방헌법보호법(BVerfSchG), 군정보부법(MADG), 연방정보부법(BNDG), 통신비밀제한법(G10) 등의 관련 규정들을 개정하거나 새로운 규정을 도입하고 있다. 오늘날 민주적 법치주의와 자유민주적 기본질서에 대한 중대한 위협이 되고있는 국제테러리즘과 극단주의테러리즘 영역에서의 새로운 도전에 대응하기 위하여 정보기관의 권한을 확대하는 것

35) Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts, BT-Drucksache 19/24785, 27.11.2020.

36) BGBl. I 2021 S. 2280.

이 주요 목적이다. 특히 입법자는 통신비밀제한법에 '암호통신감청'(Quellen-TKÜ) 권한을 모든 정보기관에게 부여하고 있다.[37]

통신비밀제한법은 제11조 제1a항과 제1b항에서 암호통신감청을 도입하였다. 암호통신감청은 통신의 내용이 송신자의 통신기기에서 송신 전(즉 암호화되기 전에) 그리고 수신자의 통신기기에서 수신된 후 복호화된 후에 기술적 수단(감시소프트웨어)에 의해서 감시 및 기록되는 전기통신감청을 말한다. 암호통신감청은 '현재 진행 중인 암호통신감청'과 '통신 종료 후 암호통신감청'으로 구분된다. 후자는 주로 감청명령이 내려지는 시점에 행해진 전기통신을 대상으로 한다. 따라서 감청 시점에는 통신의 내용이 이미 전기통신사업자의 서버나 대상자의 통신기기에 저장되어 있다. 따라서 통신 종료 후 암호통신감청은 그 성격이 온라인 수색에 해당하므로 '제한적 온라인 수색'이라고도 한다. 이것은 주로 휴대전화에 도착해 있는 메신저의 대화내용을 대상으로 한다. 이런 점에서 통신비밀제한법의 암호통신감청은 형사소송법(제100a조)의 암호통신감청과 유사하다.[38]

암호통신감청은 기본적으로 일반통신감청의 요건을 전제로 한다. 다만 정보기술시스템에 접근하기 때문에 추가요건이 필요하다. 그 요건이 제11조 제1a항과 제1b항에 추가된 것이다. 암호통신감청의 경우 현재 진행 중이거나 감청명령을 받을 당시까지의 통신으로 시간적 제한이 있지만, 일반감청은 과거의 통신내용에도 접근이 가능하다. 감청의 신청권자는 정보기관의 장이며 명령은 연방내무부장관[39]이 내린다. 연방의 모든 정보기관의 명령권한은 내무부장관으로 통일되어 있다. 하지만 감청을 집행하기 위해서 G10위원회의 허가를 받아야 한다. G10위원회는 통신비밀제한과 관련하여 이를 통제하는 기관이다. 법원은 아니지만 수사절차의 영장담당판사와 유사한 기능을 한다. 물론 지체의 위험이 있는 경우 긴급감청도 허용된다. 이번 개정 법률에서 도입되었다.

이러한 암호통신감청은 이제 연방과 주의 헌법보호기관, 연방정보부, 연방군정보부에 모두 적용된다. 앞으로 독일의 모든 정보기관은 제한적 온라인 수색이 포함된 암호통신감청을 수행할 수 있는 권한을 부여받게 된 것이다. 물론 바덴-뷔르텐베르크 주헌법보호청법, 바이에른주헌법보호법(BayVSG), 함부르크헌법보호법(HmbVerfSchG)은 이미

37) 이 법률안은 또한 개인과 관련한 규명원칙들을 강화하고 연방헌법보호청과 연방군정보부의 협력을 개선하고 보안심사법(SÜG)도 조정하고 있다.

38) 연방범죄수사청법(BKAG)은 진행 중인 통신암호감청만 허용하고 있다.

39) 주의 경우 주내무부장관이 관할한다.

진행 중인 암호통신감청을 그리고 함부르크헌법보호법((제8조 제12항 제2문)은 통신 종료 후 암호통신감청에 관한 독자적인 규정을 가지고 있었다. 이제 암호화되어 통신되는 WhatsApp 이나 텔레그램(Telegram)과 같은 메신저 서비스도 감청될 수 있게 되었다.

3. 연방정보부법의 전략적 해외통신감청

가. 전략적 통신감청의 개념과 종류

국내 통신망을 대상으로 하는 통신비밀제한법에 의한 일반통신감청 및 암호통신감청은 감청대상자의 구체적인 혐의나 법적 근거가 있어야 한다(동법 제3조 내지 제4조). 이에 대하여 소위 "전략적 통신감청"(strategische Fernmeldeüberwachung[40])은 특정한 개별 사안을 전제하거나 특정 혐의를 근거로 하는 것이 아니라, 아무런 혐의가 없음에도 불구하고 법률상 규정된 목적을 위하여 일반적으로 정보를 수집하고 이러한 정보를 분석하여 사전에 위험상황을 파악하고 대응하는 정보활동이다. 이러한 전략적 통신감청은 두 가지로 구분된다. 하나는 독일 국경을 넘어서 국내와 외국 사이에 행해지는 통신을 감청하는 국제통신감청(internationale Fernmeldeüberwachung)이고 다른 하나는 독일과는 상관없이 순전히 외국과 외국 사이의 통신을 감청하는 해외통신감청(Ausland-Ausland-Fernmeldeaufklärung)이다. 전자는 통신비밀제한법 제5조 내지 제8조에, 후자는 연방정보부법 제19조 이하[41]에서 규정하고 있다. 두 가지 감청은 그 대상에 차이가 있으므로 기본권 보호의 정도에서도 차이가 있다. 전자의 경우 일반적으로 독일인이 관계되지만 후자의 경우는 독일인이 관여하지 않기 때문이다.

---

40) 우리 통신비밀보호법의 전기통신감청에 대응하는 독일법의 개념은 Telekommunikationsüberwachung (TKÜ)이다. 원격감시(Fernmeldeüberwachung)는 기본법(헌법)에서 사용하는 용어이지만, EU 차원의 전기통신법 개정에 의해서 하위 법령에서는 모두 전자를 사용하고 있다. TKÜ는 전기통신을 감시하고(überwacht) 기록하는(aufgezeichnet) 것이다. 여기서 기록은 감시에 포함된다. '감시와 기록'은 우리의 감청개념에서 통신의 음향, 문언, 부호, 영상을 청취 및 공독하여 그 내용을 지득 또는 채록하는 것에 대응한다. 일반적으로 음향은 청취의 대상이고, 문언, 부호 및 영상은 공독의 대상이다. 이 글에서 TKÜ는 통신감청 또는 통신감시로 표현하다.

41) BGBl. I 2021 S. 772.

나. 전략적 해외통신감청

전략적 해외통신감청은 독일을 통과하는 인터넷 연결지점(internet exchange point)에서 통신사업자가 특정한 기간 특정지역에서 행해진 모든 전기통신의 트래픽을 저장하여 연방정보부의 수집시스템에 전달한 다음 특정한 검색어를 대입하여 원하는 통신의 내용과 트래픽데이터(통신사실확인자료)를 찾아내는 것이다. 예를 들어 아프가니스탄의 탈레반 지도부에 관한 정보를 알고 싶으면 아프가니스탄의 탑레벨 도메인, Taleban, 이미 알고 있는 지도부의 이메일 주소 등을 입력하여 관련되는 통신을 찾아내는 것이다. 이러한 과정은 데이터 수집, 국내 관련 통신의 분리, 트래픽데이터의 분석, 검색어에 따른 내용데이터의 분석, 내용데이터의 수동 분석으로 진행된다. 현재 독일에는 인터넷 연결 지점이 27개 있으며, 그중에서 세계적으로 가장 크고 위치상 중요한 연결지점이 바로 독일 프랑크푸르트 데-킥스(DE-CIX, Deutsche Commercial Internet Exchange)이다.[42] 여기를 지나는 모든 통신트래픽을 통신사업자가 저장하여 연방정보부의 수집시스템으로 전달한다. 수집시스템에서는 데이터의 종류를 분류하고 기술적 관점에서 관련이 없는 데이터를 제거하기 위한 필터링 작업과 분석작업이 자동으로 진행된다. 여기서 데이터트래픽이 기술적으로 처리되므로 사람이 개입하지 않는다. 이어서 해외통신감청에 해당되지 않는 독일 국적자 또는 내국인이 참여한 데이터트래픽을 인식하고 이를 제외할 목적으로 전자적 필터링이 수행된다(소위 DAFIS 필터링). 이를 위해서 다양한 형식기준에 따라서(예를 들어 독일 탑레벨 도메인의 사용 여부) 내국인 관련성 또는 독일인 관련성이 있는지 심사되고 추가로 연방정보부가 운영하고 있는 목록(G 10 - Positivliste)과 내국인 또는 독일인이 속할 수 있는 전기통신의 표시(즉 전화번호 또는 IP주소 등)와 비교된다. 이러한 필터링을 거친 후 남게 되는 트래픽데이터를 저장한다. 수집된 전기통신의 내용들은 사전에 확정되어 있는 검색어와 컴퓨터를 통해서 비교된다. 이를 통해서 알게 된 통신내용이 관련성이 있으면 통신트래픽에서 분리된다. 이렇게 분리된 전기통신의 내용은 연방정보부법 제6조 제2항에 의해서 기술적으로 필요한 임시저장을 넘어서 저장되어 분석된다. 검색어를 통한 내용트래픽의 선정과 저장에 이어서 분석이 행해진다. 이 작업단계에서 핵심은 정보기관과의 관련성을 수동으로 평가하는 것이다. 이 경우 현재 매일 평균 260개의 데이터트래픽이 식별되고 있다고 한다.

42) BVerfG, Urteil vom 19. Mai 2020 - 1 BvR 2835/17, Rn. 17 (https://bit.ly/38HcZQU).

다. 연방정보부법의 전략적 해외통신감청 도입 배경

연방정보부의 전략적 해외 통신감청은 연방정보부법에 구체적으로 명시하지 않고 직무규정에 따라서 수행되다가 2016년 연방정보부법의 개정으로 도입되었다. 그런데 해외통신감청과 관련된 연방정보부법 규정들(제6조, 제7조, 제13조 내지 제15조는)이 기본법 제10조 제1항의 통신의 비밀과 제5조 제1항(표현의 자유)과 일치할 수 없다는 이유로 2020년 5월 9일 연방헌법재판소로부터 위헌판결을 받았다.[43] 또한 개인정보가 처리되는 한, 연방정보부법 제19조 제1항, 제24조 제1항 제1문, 제2항 제1문, 제3항도 마찬가지로 위헌이라고 하였다.[44] 한편 연방헌법재판소는 이 판결에서 외국인도 독일기본권이 적용된다고 최초로 판결하였다.[45]

입법자는 연방헌법재판소가 제시한 기준에 따라 '2021년 4월 19일자 연방헌법재판소와 연방행정법원의 기준을 이행하기 위한 연방정보부법을 개정하기 위한 법률'[46]을 통하여 연방정보부법을 개정함으로써 전략적 해외 통신감청에 관한 규정을 대폭 수정하였다. 개정법 제4장은 기술적 정보활동을 두 가지로 구분하여 규정하고 있다. 기술적 정보활동의 핵심 내용인 전략적 해외 통신감시와 개인의 정보기술시스템에 침입하는 특별한 유형의 기술적 정보활동이 그것이다. 전략적 해외통신감청과 관련한 연방정보부법 개정안은 2021년 3월 26일 연방의회에서 의결되었고, 2022년 1월 1일부터 발효된다.[47]

라. 명령요건

연방정보부는 연방정부의 정책 보고를 위해서 또는 국제적 의미가 있는 외국으로부터 임박한 위험을 조기 인식하기 위해서 필요한 경우 직무 수행을 위해서 기술적 수단을 이용하여 외국에 있는 외국인의 개인과 관련된 통신내용데이터를 사전에 명령을 받은 전략적 해외통신감청을 근거로 처리할 수 있다(전략적 해외통신감청)(연방정보부법 제19

43) BVerfG, Urteil vom 19. Mai 2020 - 1 BvR 2835/17.

44) BT-Drucksache 19/26103, S.1.

45) 이 판결을 소개하고 있는 국내문헌으로는 정문식·정호경, 정보기관의 해외통신정보활동에 대한 헌법적 한계 - 독일연방정보원법(BNDG) 위헌결정에 나타난 위헌심사기준과 내용을 중심으로 -, 공법연구 제49집 제3호, 2021, 137-167면.

46) BGBl. I 2021 S. 771.

47) BGBl. I 2021 S. 796.

조 제1항). 이러한 전략적 통신감청은 통신감청의 목적, 통신감청의 주제, 대상 지역, 기간을 명시하여 전략적 해외통신감청의 범위를 제한하고 있다(제2항). 전략적 해외통신감청은 독일연방공화국의 외교 및 안보 정책에 의미가 있는 외국에 관한 정보(Informationen)를 확보하여 연방정부의 정책결정자에게 보고하기 위한 것이다. 이러한 감청은 연방수상청이 그 규명을 연방정보부에 위임한 경우에만 허용된다(제3항).

전략적 해외통신감청의 명령권자는 연방정보부이다(제23조). 하지만 집행이전에 독립통제위원회(Unabhängige Kontrollrat)로부터 이 명령의 정당성을 심사받아야 한다. 독립통제위원회는 기존의 전략적 해외통신감청에 대한 통제기관이었던 독립위원회를 개정법에서 독립통제위원회로 조직을 개편한 것이다. 독립통제위원회는 '법원유사통제기관'과 '행정통제기관'으로 구성된다. 전자가 독립통제위원회의 핵심기관이고, 후자는 전자의 지원기관이다. 법원유사통제기관은 6명으로 구성되는데, 그 자격은 임명되기 전 연방(민형사)대법원(BGH)과 연방행정대법원의 대법관으로 활동한 자여야 한다. 법원유사통제기관의 구성원으로 임명되면 법관의 자격은 정지된다. 이와 같이 대법관 자격을 요구한 것은 전략적 해외통신감청에 대한 통제를 보다 강화하기 위한 것이다.[48] 이러한 감청명령은 독립통제위원회로부터 명령의 정당성을 확인받지 못하면 효력을 상실한다. 지체의 위험이 있는 경우 독립통제위원회 산하의 '법원유사통제기관'의 한 명의 구성원을 통해서 정당성의 임시심사가 행해질 수 있다. 전략적 해외통신감청은 규명목적이 좌절되거나 본질적으로 어려운 경우에만 가능하다(제4항).

연방정보부법의 전략적 해외통신감청에 대해서는 통신비밀제한법의 G10위원회가 아니라 연방정보부법의 독립통제위원회가 통제한다. 이에 대해 통신비밀제한법의 전략적 국제통신감청의 경우에는 연방정보부가 신청하고 연방내무부가 명령을 내리며 집행 이전에 G10위원회의 동의를 받아야 한다(통신비밀제한법 제15조 제6항).[49]

48) 독립통제위원회에 대해서는 박희영/윤해성/김재현/임유석, 앞의 위탁연구보고서(각주 14), 제6장 제3절 3. 라. 연방정보부법의 독립통제위원회 부분 참조.

49) 독일 정보기관의 규범적 통제의 헌법적 근거는 기본법 제45d조이다. 이에 따르면 연방의회가 연방정보기관의 활동을 통제하기 위해서 위원회를 설치하도록 규정하고 있다. 이에 근거하여 통제위원회법(PKGrG)이 제정되었다. 이 법률에 의해서 연방정보기관의 모든 조치와 활동을 포괄적으로 심사하는 의회통제위원회가 설치되었다. 한편 통신비밀과 관련한 통제기관으로는 통신비밀제한법(G10법)에 의하여 G10위원회가 설치되어 있고, 연방정보부의 전략적 해외통신감청과 관련한 통제기관으로는 독립통제위원회가 설치되어 있다(자세한 내용은 박희영/윤해성/김재현/임유석, 앞의 위탁연구보고서(각주 14), 제6장 제3절 3. 가. 독일 연방정보기관의 규범적 통제 체계 참조).

4. 연방정보부법의 외국인의 정보기술시스템 침입

가. 도입배경

외국인의 정보기술시스템 침입은 앞서 언급한 전략적 해외통신감청과 함께 연방정보부법에 규정되었다. 해외에 있는 외국인의 정보기술시스템 침입은 연방정보부의 직무 수행을 위해서 불가피하기 때문에 실무에서 이전부터 수행되고 있었다. 따라서 이를 도입한 것은 연방정보부의 활동영역을 확대하기보다는 앞서 언급한 연방헌법재판소의 전략적 해외통신감청의 위헌판결을 이행한 것이다.[50]

연방헌법재판소는 이 판결에서 해외에 있는 외국인에 대한 해외 통신감시조치를 기본법 제10조(통신비밀)의 제한으로 판단하였고 그 결과 상세한 권한 규정을 요구하였다. 이에 따라 연방정보부가 이미 수행하고 있는 해외에 있는 외국인의 정보기술시스템 침입의 경우 법적 근거가 문제되었다. 그리하여 이러한 조치를 위한 특별한 권한 규범이 마련되어야 했다. 따라서 이번 개정 법률을 통해서 외국인의 정보기술시스템 침입에 대한 법적 근거가 마련되어 연방정보부는 이러한 조치를 위한 법적안정성과 법적명확성을 확보하게 된 것이다.[51]

입법이유에 따르면 정보기술시스템 침입은 다른 정보기관 수단과 비교하여 정확한 정보를 확보할 가능성이 있다고 한다. 따라서 이러한 침입은 외교정책 및 안보정책상 문제와 관련한 특별히 중요한 정보를 수집하고 위험을 조기 인식하여 연방정부에 공급할 수 있다고 한다. 연방정부가 전략적으로 외교 및 안보정책상 결정을 하는데 이러한 정보는 매우 중요하다고 한다. 따라서 이러한 수단의 투입은 정당한 목적에 기여하고, 이러한 종류의 정보는 일반적으로 더 경미한 수단을 통해서는 확보될 수 없다고 한다. 나아가서 해외에 있는 외국인의 정보기술 시스템 침입 권한은 엄격한 의미에서도 비례적이라고 한다.

정보기술시스템 침입 권한은 일반적으로 IT기본권의 제한이다. 연방헌법재판소는 국내 사안의 위험방지에서 IT 기본권이 제한되는 경우 그 제한요건을 높게 설정하였다. 하지만 연방헌법재판소는 2020년 5월 19일 판결에서 개별적 기본권의 보호는 국내와

50) BT-Drucksache 19/26103, S. 94.

51) BT-Drucksache 19/26103, S. 94.

국외에서 구분될 수 있다는 점을 확인하였다. 따라서 정보기술시스템 접근을 통한 해외 정보활동의 사례에서 제한의 요건은 국내의 경우와 비교하여 낮아질 수 있다고 한다.[52)]

이러한 권한은 진행 중인 전기통신 외에 정보기술시스템에 저장되어있는 통신데이터 및 기타 데이터도 포함한다. 이들 데이터의 분석은 연방정보부의 직무수행을 위해서 반드시 필요하다고 한다. 특히 해외의 군사적 IT 네트워크에 저장되어 있는 기록에 접근하는 경우에 명백하다고 한다.

나. 요건

외국에 있는 외국인의 정보기술시스템 침입은 전략적 해외통신감청과 달리 불특정 다수의 통신을 대상으로 하지 않고 특정되거나 특정될 수 있는 자를 대상으로 한다. 따라서 이 조치의 대상자는 자연인은 물론 법인도 포함된다. 예를 들어 정보기관에게 특별히 이익이 되는 개인, 테러 단체 및 이의 구성원 및 후원자, 대량살상무기의 확산과 관계가 있는 기업 등이 포함된다.

이러한 정보기술시스템 침입은 두 가지 목적으로 수행된다. 첫째 연방정부에 대한 정책보고와 둘째 국제적 의미가 있는 외국으로부터의 임박한 위험의 조기 인식을 위해서다(연방정보부법 제34조 제1항). 연방정부에 대한 정책보호의 경우 이러한 침입을 통해서 독일의 외교 및 안보 정책에 중대한 의미가 있는 정보를 확보할 수 있다는 사실상 근거가 있어야 한다(동법 제2항). 임박한 위험의 조기인식은 이러한 조치로 연방수상청이 규명을 위임한 정보를 확보할 수 있다는 사실이 정당화되고, 이를 통하여 독일연방공화국의 외교안보정책상 중대한 의미를 가지는 사례들에서 특정한 위험(연방정보부법 제19조 제4항)에 관한 새로운 정보가 확보될 경우에만 허용된다(동법 제3항). 또한 이러한 조치는 연방정보부의 직무수행을 위해서 필요하고 그렇게 하지 않으면 직무수행이 가망이 없거나 본질적으로 어려울 수 있는 경우에만 수행될 수 있다(제34조 제1항 제2문).

명령절차는 전략적 해외통신감청과 동일하다. 즉 연방정보부가 명령을 내리고 독립통제위원회의 정당성 심사를 받아야 한다. 지체의 위험의 경우에도 마찬가지다.

52) BT-Drucksache 19/26103, S. 95.

5. 소결

독일 정보기관의 정보수집권은 법률에 명확하게 규정되어 있고 정보수집권이 다양하여 광범위하게 정보를 수집할 수 있는 환경을 조성하고 있다. 이렇게 수집된 정보는 분석되어 국가정책결정자에게 보고된다. 정보기관이 직무 수행과 관련하여 정보를 수집하고 분석하는 과정에서 위험방지나 범죄수사에 해당되는 정보나 활동을 발견할 수 있다. 정보기관의 직무의 상당수가 이와 관련된다. 하지만 정보기관은 위험방지나 범죄수사를 할 수 있는 집행권을 가지고 있지 않다. 정보기관과 경찰 사이에 분리원칙이 적용되기 때문이다. 하지만 협력관계를 통하여 이 문제를 해결하고 있다. 한편 정보기관의 정보수집권은 위험방지를 위한 경찰법이나 범죄수사를 위한 형사소송법에 이미 도입되어 있다. 이것이 분리원칙과 협력관계에서 어떤 의미를 가지는지 아래에서 검토한다.

Ⅴ. 정보기관과 수사기관의 분리원칙 및 협력

1. 분리원칙

정보기관과 경찰의 분리원칙(Trennungsgebot)이란 정보기관의 정보활동에서 경찰권한이 배제되어야 하고, 경찰권은 정보업무를 포함해서는 안 된다는 것을 의미한다. 이러한 분리원칙은 1949년 4월 14일 연합군 군정관들이 제헌위원회에 보낸 연방경찰권에 관한 서신에서 비롯되었다.[53] 이것을 소위 '경찰서신(Polizeibrief)'이라고 한다.[54] 경찰서신 제2항에 따르면 "연방정부는 자신을 대상으로 국가전복을 꾀하는 활동에 관한 정보를 수집하고 배포하는 기관을 설립할 수 있지만, 이 기관은 어떠한 경찰권한도 가져서는 안된다". 이러한 분리원칙을 규정한 경찰서신 제2항은 1950년 9월 27일 연방헌법보호법(BVerfSchG)에서 처음으로 법제화되었다.[55] 그 후 연방정보부법과 군정보부법에

53) http://www.verfassungen.de/de49/grundgesetz-schreiben49-3.htm(2021.8.25 방문).

54) 경찰서신의 한글번역본은 박병욱, 독일 나찌시대 제국안전중앙청(Relchssicherheitshauptamt)의 긴 그림자, 경찰법연구 제11권 제2호, 2013, 255면.

55) BGBl. I 1950 S. 682.

도 동일한 내용이 규정되었다.[56]

정보기관과 경찰의 분리에서 두 가지 본질적인 요소는 이들의 권한과 조직이다. 여기에서 두 조직의 분리는 상이한 권한에 기인한다고 할 수 있다. 이러한 조직의 구분으로 서로 다른 임무가 부여된다. 정보의 분리는 독자적인 분리원칙의 내용이라기보다는 권한의 분리로부터 도출되는 내용이라고 할 수 있다.[57] 1970년대 말 정보의 분리가 법적으로 거론되었을 때의 문제는 정보기관과 경찰의 정보에 대한 협력이 정보자기결정권과 그와 연계된 정보보호의 배경에서 허용되는가였다.[58] 하지만 이후 법률은 명시적으로 정보기관이 자신에게 권한이 없는 조치를 경찰에 공무협조(Amtshilfe)의 방식으로 요청하여서는 안 된다고 규정하였다.[59] 그럼에도 불구하고 안보정책상의 이유로 정보교환을 요구하는 경우에는 입법자는 정보전달을 가능하도록 규정하고 있으며(연방헌법보호법 제17조 이하), 경찰의 권한범위 내에서 정보를 수집하는 것이 헌법보호를 위한 것이면 분리원칙의 대상이 되지 않는다고 하였다.[60]

이러한 분리원칙이 헌법적 지위를 가지는가에 대해서는 견해가 대립되고 있다.[61] 특히 독일기본법은 분리원칙의 개념과 내용을 명시적으로 규정하고 있지 않아서 그 지위에 관한 논란이 제기되고 있다. 연방헌법재판소는 지금까지 분리원칙의 헌법상 지위에 대해 명확하게 언급하고 있지 않지만, 기본적으로 헌법적 지위를 인정한다고 볼 수 있는 입장을 제시하고 있다.[62] 헌법재판소에 따르면 "법치국가원리, 연방국가원리, 기본권의 보호는 특정한 기관들을 서로 통합하고 이들을 헌법상의 지위와 일치될 수 없는 직무와 관련시키는 것을 금지한다. 그래서 헌법보호 또는 정보업무의 목적을 위한 중앙관청들은 -

56) 연방정보부법 제1조 제1항 제2문 및 제2조 제3항, 군정보부법 제1조 제4항 및 제4조 제1항.

57) 분리원칙에 대한 자세한 설명은 손미숙, "독일의 테러 대응 법제 및 체계", 「테러 예방 및 대응을 위한 수사의 실효성 및 예측의 효율성 확보 방안」, 한국형사정책연구원, 2016, 104-114면 참조. 이에 대해서 분리원칙의 내용을 5가지로 구분하는 견해에 따르면 기능, 조직, 권한, 정보 외에 인적 분리를 추가하고 있다(Gusy, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BNDG § 1 Rn. 14.).

58) Singer, Das Trennungsgebot - Teil 1 -, Die Kriminalpolizei 2006, S. 88.

59) 연방헌법보호법 제8조 제3항 제2문, 연방정보부법 제2조 제3항 제2문, 군정보부법 제4조 제2항 제2문.

60) Singer, a.a.O.(Fn.58), S. 89.

61) 이러한 논의에 관한 문헌은 Brandt, a.a.O.(Fn. 12) S. 325 Fn. 385 참조.

62) 분리원칙의 헌법적 위상에 관한 자세한 소개는 박병욱, 앞의 논문(각주 54), 258면 이하.

다른 종류의 직무와 권한을 고려하여 - 집행경찰과 병합되어서는 안 된다."[63]고 하였다.

하지만 이와 같은 분리원칙은 기관들 사이의 '협력'을 방해하지는 않는다. 특히 테러가 빈번하게 발생하고 있는 상황에서 테러상황에 대응하기 위해 양 기관의 협력은 필요하다. 분리원칙의 완화가 고려될 수 있는 것은 반테러데이터베이스법(Antiterrordateigesetz, ATDG)[64]이다. 이 법률은 2006년 제정되었으나 2013년 4월 24일 헌법재판소의 일부 위헌 판결로 인해 2014년 12월 18일 개정되어, 2015년 1월 1일 다시 발효되었다.[65][66] 연방범죄수사청, 연방경찰, 주범죄수사청, 연방과 주의 헌법보호청, 군정보부, 연방정보부 그리고 조세범죄수사청은 독일연방공화국과 관련한 국제 테러리즘의 규명(Aufklärung) 또는 대응(Bekämpfung)을 위한 각자의 법적 임무를 수행하기 위해서 연방범죄수사청에 표준화된 공동의 중앙반테러데이터베이스(Antiterrordatei, ATD)를 설치하여 운영한다. 여기서 테러리즘의 규명은 정보기관의 직무이고, 테러리즘의 대응은 위험방지를 위한 경찰의 직무이다. 즉 '규명'이란 정보를 수집하고 분석하여 새롭게 얻어낸 정보(Erkenntnisse, intelligence)를 정책결정자에게 제공하는 정보활동이므로 작전상 권한을 행사하는 것이 아니다. 이에 반해서 '대응'이란 작전권한을 실제로 행사하는 경찰의 집행활동이다. 이 법률 역시 정보기관과 경찰의 분리원칙이 엄격하게 유지되지 않는 것으로 평가된다.[67]

2. 정보 전달을 통한 협력

가. 수집된 개인정보의 목적변경 및 다른 기관 제공

정보기관은 개인정보의 수집은 물론 이를 보관하거나 원래 수집목적과 다른 목적으로 이용하거나 다른 기관으로 전달할 수도 있다. 이러한 개인정보의 처리는 모두 침해에 해

63) BVerfG, Beschluss vom 28. 01. 1998 - 2 BvF 3/92 -, Rn. 87 (https://bit.ly/3tdrwxc).

64) 일부 국내 문헌에서는 반테러'데이터'법으로 번역하고 있으나 법문의 Datei는 데이터가 아니라 데이터베이스, 데이터뱅크, 데이터파일을 의미한다. 따라서 반테러데이터베이스법이 정확한 표현이다.

65) Arzt, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, ATDG § 1 Rn. 1 f.

66) Data mining을 규정하고 있는 이 법률 제6a조는 2020년 11월 10일 헌법재판소로부터 위헌으로 결정되었다(BVerfG, Beschluss vom 10. November 2020 - 1 BvR 3214/15 -) (http://www.bverfg.de/e/rs20201110_1bvr321415.html).

67) Arzt, a.a.O.(Fn. 65), ATDG § 1 Rn. 29 ff.

당된다. 이러한 침해의 위험성 때문에 연방헌법재판소는 이와 관련하여 원칙을 정해두고 있다.

연방헌법재판소는 2012년 1월 24일 전기통신가입자데이터의 저장 및 처리에 관한 규정의 일부 위헌에 대한 결정(Beschluss)[68]에서 다양한 국가기관 사이의 개인정보 전달의 경우 필요한 법적 토대에 대하여 기본적으로 다음과 같이 상술하였다.[69] 국가기관을 통하여 개인정보를 취급할 권한을 부여하는 규정들은 일반적으로 다양하고 서로 체계적인 기본권 제한을 근거지운다. 이 경우 우선 데이터의 수집, 저장 및 이용은 구분되어야 한다.[70] 따라서 연방정보부가 자신의 목적을 위해서 전기통신감청에서 확보한 개인정보를 다른 국가기관으로 전달하는 것은, 이러한 전달이 그 목적을 위해서 필요하고, 목적변경의 요구사항이 준수되고 법률상 이전요건이 비례성원칙을 충족해야 한다[71]고 하였다.

이러한 목적변경에 대한 비례성원칙의 요구사항은 2016년 4월 20일 헌법재판소 판결(Urteil)에서 제시한 '가정적 데이터 수집 원칙'(Grundsatz der hypothetischen Datenneuerhebung)에 맞추어야 한다. 이에 따르면 우선 데이터의 새로운 이용은 법익의 보호에 기여하거나 그 이용을 비교가능한 비중이 있는 수단으로 헌법상 정당화할 수 있는 비중을 가진 범죄의 규명에 기여해야 한다.[72] 또한 국가의 직무수행을 위한 데이터 교환 규정은 다음을 구별해야 한다. 즉 데이터를 제공하는 기관의 데이터 전달과 데이터를 요청하는 기관의 데이터 호출의 구별이다. 데이터 교환은 각자의 법적 근거를 필요로 하는 조회와 전달의 제한에 의해서 수행된다. 이와 관련하여 헌법재판소는 소위 '이중문이론'(Doppeltür)을 개발하였다. 입법자는 데이터를 전달하는 문뿐만 아니라 이를 조회하는 문도 함께 개방해야 한다는 것이다. 이중문과 같이 두 개의 법적 근거가 함께 존재

68) BVerfG, Beschluss vom 24. Januar 2012 - 1 BvR 1299/05 - (https://bit.ly/3kXUeOK).

69) Greßmann, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, IV § 3 Nachrichtendienste und Strafverfolgung, 2017, Rn.10.

70) BVerG, Beschluss vom 14. Juli 1999 - 1 BvR 2226/94, Rn. 184 ff.) (https://bit.ly/3tdJiQQ); BVerfG, Beschluss des Ersten Senats vom 04. April 2006 - 1 BvR 518/02 -, Rn. 73f. (https://bit.ly/3kX4mYa); BVerfG, Urteil des Ersten Senats vom 11. März 2008 - 1 BvR 2074/05 -, Rn. 70ff. (https://bit.ly/3zNgrVZ); BVerfG, Urteil vom 02. März 2010 - 1 BvR 256/08, Rn. 190 (https://bit.ly/2YhtHV1).

71) 목적변경에 대한 연방헌법재판소 판결에 대해서는 다음 판결 참조: BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn.156ff., Rn.202 (https://bit.ly/3jJM1yn).

72) BVerfG NJW 2016,1781; BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 -, 결정요지 2. c) (https://bit.ly/3DQQgQE).

하는 경우에만 개인정보의 교환이 비로소 법적으로 허용된다는 것이다.[73]

나. 자발적 보고의무

정보기관은 다른 국가기관의 요청이 없더라도 데이터를 이전할 권한이 있다. 이를 자발적 전달(Spontanübermittlung)이라고도 한다. 예를 들어 연방헌법보호청은 연방헌법보호법 제19조 제1항에서 정보기관의 수단에 의해서 수집한 개인정보를 다른 국가기관으로 전달할 수 있다. 여기에 열거되어 있는 국가기관은 검찰, 경찰, 세관 등이다. 이러한 전달은 정보기관의 직무 수행(제1호), 조세관련 직무 수행(제1항 제1호), 중요한 의미의 범죄의 방지(제3호) 그리고 중요한 의미의 범죄의 소추(제4호)를 위해서 필요해야 한다. 군정보부법은 제11조 제1항 제1문에서 그리고 연방정보부법은 제24조 제1항에서 연방헌법보호법 제19조를 각각 준용하고 있다.

통신비밀제한법에 의해서도 수집된 데이터의 전달은 동법 제4조 제4항에서 독자적인 법적 토대가 규정되어 있다. 이에 따르면 연방 및 주 헌법보호청, 연방정보부, 연방군정보부는 동법 제3조 제1항과 제1a항의 목록에 열거된 범죄의 방지나 규명을 위해서, 이러한 범죄의 소추를 위해서, 위헌정당에 대한 조치의 집행을 위해서 통신감청으로 수집된 특정 데이터를 전달할 수 있다.

연방정보부도 통신비밀제한법 제5조의 전략적 국제통신감청과 관련하여 수집된 데이터를 추가로 전달할 가능성을 가진다. 동법 제7조 제4항 제1문과 관련한 제2문에 의해서 거기에 언급된 특정한 범죄의 혐의가 있는 경우 형사소추기관으로 데이터를 전달할 수 있다. 또한 연방정보부는 제8조 제6항 제1문과 제2문에 의해서 특정한 위험방지와 범죄소추를 위해서 위험방지기관이나 소추기관에 전달할 수 있다.

이에 대해서 연방의 모든 행정관청 및 공법상 연방의 직할법인은 정보기관의 직무와 관련하여 알게 된 정보를 자발적으로 보고해야 한다(연방헌법보호법 제18조 제1항). 특히 검찰과 경찰 등은 헌법보호기관의 직무 수행을 위해서 전달이 필요하다는 사실상 근거가 있는 경우, 자신이 알게 된 제3조 제1항의 시도나 활동에 관한 개인정보를 포함한 모든 정보를 연방 및 주헌법보호기관에 자발적으로 보고해야 한다(제18조 제1b항). 연방정보부법(제23조)와 군정보부법(제10조)에도 공공기관이나 검찰 및 경찰의 자발적 보고

73) Greßmann, a.a.O.(Fn. 69), IV § 3 Nachrichtendienste und Strafverfolgung, Rn.10.

의무가 규정되어 있다.

다. 의무적 전달

정보기관은 특정한 범죄의 경우에는 의무적으로 관련 데이터를 전달해야 한다. 자발적 전달의 경우 법률 규정은 재량의 여지를 허용하지만 특정한 범죄의 경우에는 법률상 전달 의무가 존재한다. 연방헌법보호법 제20조는 연방헌법보호청을 통하여 국가보호 및 헌법보호 사안에서 형사소추기관 및 보안기관에 정보의 전달을 규정하고 있다. 이에 따르면 연방헌법보호청은 국가보호에 관한 범죄의 저지 및 소추에 필요하다는 사실상 근거가 있는 때에는 자신이 알게 된 개인정보 및 다른 정보를 경찰 및 검찰에 전달해야 한다. 연방정보부의 경우 제24조 제3항에서 군정보부는 제11조 제2항에서 의해서 국가보호 및 헌법보호 사안과 관련하여 개인정보를 포함한 정보를 검찰과 경찰에 전달해야 한다.

라. 정보 요청

자발적 보고의무나 의무적 전달 외에 정보기관은 직무수행을 위해서 필요한 경우 관련 정보를 연방의 모든 관청, 공법상 직할 법인, 검찰, 경찰 등에 요청할 수도 있다(연방헌법보호법 제17조 제1항과 제3항, 연방정보부법 제23조, 군정보부법 제10조 제2항).

이에 대하여 검찰은 형사소송법 제160조에 의해서 정보기관을 포함한 모든 국가기관에 정보제공을 요청할 수 있다. 법률상 관청의 정보제공을 제한하지 않는 이상 국가기관은 검찰에 이러한 정보를 제공할 의무가 있다.

마. 전달 금지

자발적 보고의무, 의무적 전달, 정보 요청의 경우라 하더라도 모든 정보가 전달되는 것은 아니다. 일정한 경우에는 전달이 금지되어 있다. 그러한 사례로는 첫째, 정보의 종류와 이의 수집을 고려했을 때 당사자의 보호가치 있는 이익이 전달에 따른 공익보다 현저히 높다고 전달 담당부서가 인지한 경우, 둘째, 더 중대한 안전에 관한 이익이 전달 금지를 요구하는 경우, 셋째, 직업상 또는 공무상 비밀준수의무 등으로 다른 법률에서 전달을 금지하고 있는 경우이다(연방헌법보호법 제23조). 한편 미성년자의 개인정보를

포함한 정보도 전달해서는 안 된다(동법 제24조).

3. 소결

독일 정보기관은 분리원칙에 의하여 조직, 직무, 권한, 정보가 분리되어 있지만, 협력관계에 의해서 정보가 상호전달됨으로써 사실상 정보가 공유되고 있다. 이러한 정보의 공유는 정보기관과 수사기관 사이에 유사한 정보수집권이 부여되어 있음을 전제로 한다. 독일의 위험방지기관인 경찰이나 범죄수사기관은 이미 정보기관에게 부여되어 있는 정보수집권을 대부분 가지고 있다. 이번에 정보기관에게 부여된 암호통신감청이나 온라인 수색과 같은 비밀정보수집권한도 이미 경찰이나 수사기관에게 허용되어 있다. 다만 전략적 통신감청은 정보기관의 성격에서 나오는 특별한 정보수집권이기 때문에 경찰이나 수사기관에게는 허용되지 않는다.

이번에 정보기관에게 허용된 암호통신감청, 온라인 수색, 전략적 해외통신감청은 기존의 정보기관의 일반통신감청과 전략적 국제통신감청과 함께 범죄와 관련된 정보를 발견할 개연성이 상당히 높다. 이러한 정보들이 수사기관으로 전달되면 수사기관의 범죄대응능력이 전체적으로 상승할 것으로 보인다. 이런 점에서 정보기관의 협력은 수사기관의 범죄수사에 중요한 기여를 함으로써 '간접적'으로 형사정책기능을 수행하고 있다고 평가할 수 있다. 이것은 정보기관과 수사기관이 분리되어 있더라도 협력관계를 통해서 안보건축물을 함께 유지할 수 있다는 것을 의미한다. 이러한 평가는 지난해 정보와 수사를 분리한 우리 국가정보원법 개정에 시사하는 바가 상당히 크다. 그렇다면 국정원법의 개정으로 안보건축물이 유지될 수 있도록 충분한 정보수집권이 보장되어 있는지 그리고 협력관계가 어떻게 작동하고 있는지 검토한다.

Ⅵ. 국가정보원의 정보수집권과 수사기관의 협력

1. 국가정보원의 직무

국가정보원은 국가안전보장 업무를 수행한다. 이러한 업무수행을 위해서 국가정보원법은 제4조에서 국가정보원의 6가지 직무를 규정하고 있다. 그중에서 이 글의 연구 대상인 국정원의 정보활동은 제4조 제1항에서 5가지로 구분하고 있다. 첫째, 국외 및 북한에 관한 정보, 둘째, 방첩(산업경제정보 유출, 해외연계 경제질서 교란 및 방위산업침해에 대한 방첩을 포함), 대테러, 국제범죄조직에 관한 정보, 셋째, 형법 중 내란의 죄, 외환의 죄, 군형법 중 반란의 죄, 암호 부정사용의 죄, 군사기밀 보호법에 규정된 죄에 관한 정보, 넷째, 국가보안법에 규정된 죄와 관련되고 반국가단체와 연계되거나 연계가 의심되는 안보침해행위에 관한 정보, 다섯째, 국제 및 국가배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보 등[74]이다.

개정 전 국정원법의 직무범위가 예시적 열거인지 한정적 열거인지 실무와 학계에서는 논란이 있었다. 특히 개정 전 제3조의 제1항 제1호의 국내보안정보와 관련하여 실제 재판에서 문제가 되었다.[75] 이러한 논란은 개정 국정원법에서 국내보안정보수집이 국정원의 직무범위에서 배제됨으로써 입법적으로 해결되었다. 나아가서 입법자는 국정원법 개정 이유에서 제4조에 열거된 직무를 국가정보원의 직무로 명확히 함으로써 한정적 열거임을 분명히 하였다. 이러한 한정적 열거규정은 독일 정보기관의 직무와 비교할 때 상당히 제한적이다.

74) 제4조 제3항에서 사이버안보와 관련하여 직무수행에 필요한 사항은 대통령으로 정한다고 하여, 사이버 안보업무규정에서 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보의 수집, 작성, 배포 업무를 규정하고 있다.

75) 서울중앙지방법원 2009.5.29. 선고 2008가합40668 판결; 서울고등법원 2010.2.10. 선고 2009나60819 판결; 대법원 2010.5.27. 선고 2010다21894 판결. 이에 대한 자세한 내용은 김호정, 정보기관의 정보수집 활동과 '개인정보 자기결정권', 외법논집 제39권 제1호, 2015. 2, 169-186.

2. 정보기관의 정보수집권[76]

가. 일반적 정보수집권

국정원은 위에서 언급한 5가지 직무 분야에 해당되는 정보를 수집, 작성, 배포할 수 있다. 여기의 정보에는 직무와 관련성이 인정된다면 개인정보를 비롯한 사물관련 정보, 사건, 사고 등 모든 정보가 해당된다. 하지만 직무와 관련성이 없는 정보수집은 금지된다. 이러한 금지는 개정 국정원법 제3조 제2항에서 명시하고 있기 때문이다.

국가기관이 특히 개인정보를 수집하는 경우에는 일반적으로 개인정보보호법이 적용될 수 있다. 하지만 개인정보보호법은 국가안보와 관련하여 정보 분석을 목적으로 처리되는 개인정보에 대해서는 그 적용을 배제하고 있다(제58조 제항 제2호). 즉 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공이 요청되는 개인정보에 대해서 개인정보보호법 제3장부터 제7장까지[77]를 적용하지 않는다.

테러분자의 추적, 간첩 색출, 국가전복 기도 방지, 국가기밀 누출방지 등 국가안보를 위한 정보·수사기관들의 정보 수집, 분석 및 관리 업무는 비밀리에 수행되어야 하므로 국가안보를 목적으로 하는 개인정보 수집·제공 행위 등에 대해서는 이 법의 일부를 적용에서 배제하고 있다. 따라서 국가안보와 관련하여 정보 분석을 목적으로 처리되는 개인정보에 대해서는 정보주체의 동의가 필요하지 않다. 이러한 의미에서 국가정보원법은 개인정보보호법의 특별법이라 할 수 있다.

국가정보원법 제3장이 개인정보의 처리에 관한 규정이다. 국가안보와 관련된 정보 분석은 그 자체가 이용에 해당된다. 개인정보의 수집은 이용을 전제로 하고 있으므로 안보관련 정보 분석을 위해서 수집 또는 제공에는 이용이 포함된다.[78]

하지만 개인정보보호법의 관련 규정들이 적용되지 않는다 하더라도 국가정보원법에 규정되어 있지 않는 방법으로 개인정보를 수집하는 것은 제58조 제1항 제2호로는 허용

76) 국가정보원의 개인정보처리에 대해서는 선행연구가 거의 발견되지 않는다. 따라서 일반적인 법리와 필자의 개인적인 견해를 중심으로 분석한다.

77) 제3장은 개인정보의 처리, 제4장은 개인정보의 안전한 관리, 제5장은 정보주체의 권리 보장, 제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례, 제7장 개인정보 분쟁조정위원회에 관한 규정들이다.

78) 개인보호위원회 결정 제2019-04-044호 참조.

되지 않는다고 보아야 한다. 적용 배제 규정인 제58조 제1항 제2호는 일반규정으로 이해되기 때문이다. 따라서 개인정보를 처리하는 수권규정이 필요하다. 이러한 결론은 국정원법의 관련 규정을 고려하면 도출될 수 있다. 즉 국정원의 운영원칙과 관련한 국정원법 제3조 제1항의 "국민의 자유와 권리 보호", 제2항의 "정보의 수집 목적에 적합한 정보 수집" 그리고 제14조의 불법 감청 및 불법위치추적 등의 금지에서 도출될 수 있다.

나. 개별적 정보수집권

그런데 국정원이 이러한 직무를 수행하기 위한 구체적인 수권규정은 국가정보원법에 구체적으로 명시되어 있지 않다. 국정원법은 오히려 국정원의 직무와 관련하여 직무수행의 원칙, 범위, 절차 등은 국정원의 '정보활동기본지침'에 정하도록 하고 있다(국가정보원법 제1조 제2항). 이것은 법률이 아니라 일종의 직무규정이다. 독일 정보기관이 과거에 수권규정없이 정보를 수집해 온 관행과 유사하다. 국가정보원장은 이러한 정보활동기본지침을 국회정보위원회에 보고한다(국가정보원법 제1조 제2항). 따라서 국정원의 정보수집활동은 국정원 직원과 국회정보위원회 소속의 국회의원만이 알 수 있다.

이러한 입법 태도는 현재 정보기관의 정보수집권한을 법률에 명시하고 있는 독일의 법제와 완전히 다르다. 이러한 입법 태도가 법치국가원리에 합치하는지는 의문이다. 국가정보원이 비밀리에 정보를 수집하는 활동은 기본적으로 개인정보자기결정권이나 사생활의 비밀, 통신의 비밀 나아가서 주거의 불가침도 침해할 수 있기 때문이다. 물론 국회정보위원회가 정보활동기본지침에 위법하거나 부당한 사항이 있다고 인정되면 이를 시정이나 보완을 요구할 수 있고, 원장은 특별한 사유가 없으면 그 요구에 따라야 한다(국가정보원법 제1조 제2항 제2문). 하지만 이러한 시정 및 보완 요구가 국민의 기본권 침해를 정당화할 수 있는지 의문이다.

하지만 구체적인 수권규정이 불비되어 있음에도 불구하고 국가정보원법의 일부 규정을 통해서 몇 가지 정보수집방법을 도출할 수 있다. 여기에는 국정원법에 직접 규정하고 있는 것과 다른 법률에 규정되어 있는 것으로 나누어 볼 수 있다. 우선 국정원법에 직접 규정하고 있는 것은 협조를 통한 정보수집이다. 국정원법 제5조에 따르면 국정원은 국가기관 등에 정보를 요청할 수 있다. 국가기관이나 그 밖의 기관 또는 단체에 사실의 조회 및 확인, 자료의 제출 등 필요한 협조 또는 지원을 요청할 수 있고, 이 경우 요청을 받은

국가기관 등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다(제5조 제1항).[79] 또한 일정한 직무수행을 위하여 필요한 경우 현장조사, 문서열람, 시료채취, 자료제출 요구 및 진술요청 등의 방식으로 조사할 수도 있다(제5항 제2항). 이러한 정보수집은 비밀리에 수행되는 정보기관의 수단이라기 보다 공개적인 정보수집에 가깝다.

국정원법에 직접 규정한 것은 아니지만 반대로 해석하면 직접 규정한 것으로 볼 여지가 있는 정보수집방법이 있다. 국정원법 제14조에서 불법 감청 및 불법위치추적 등의 금지를 규정하고 있기 때문이다. 이에 따르면 통신비밀보호법, 위치정보의 보호 및 이용 등에 관한 법률, 형사소송법 또는 군사법원법 등에서 정한 적법절차에 따르지 않고는 우편물의 검열, 전기통신의 감청 또는 공개되지 아니한 타인간의 대화를 녹음 및 청취하거나 위치정보 또는 통신사실확인자료를 수집할 수 있다고 규정하고 있다. 따라서 이러한 법률에 정한 적법절차에 따르면 이러한 정보수집활동이 가능하다.

다른 법률에 규정된 정보수집권한으로는 테러방지법 제9조(테러위험인물에 대한 정보수집 등)와 전기통신사업법 제83조 제3항의 통신자료 요청이다. 우선 테러방지법 제9조에 따르면 국가정보원장은 테러위험인물에 대하여 출입국, 금융거래 및 통신이용 등 관련 정보를 수집할 수 있다. 이 경우 출입국, 금융거래 및 통신이용 등 관련 정보의 수집은 출입국관리법, 관세법, 특정 금융거래정보의 보고 및 이용 등에 관한 법률, 통신비밀보호법의 절차에 따른다(제1항). 이러한 정보 수집 및 분석의 결과 국가정보원장은 테러에 이용되었거나 이용될 가능성이 있는 금융거래에 대하여 지급정지 등의 조치를 취하도록 금융위원회 위원장에게 요청할 수 있다(제2항). 또한 국가정보원장은 테러위험인물에 대한 개인정보와 위치정보를 개인정보처리자와 개인위치정보사업자 및 사물위치정보사업자에게 요구할 수 있다(제3항). 나아가서 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 추적을 할 수도 있다(제4항).

전기통신사업법 제83조 제3항에 의해서 통신자료를 요청할 수도 있다. 여기에는 이용자의 성명, 이용자의 주민등록번호, 이용자의 주소, 이용자의 전화번호, 이용자의 아이디(컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호를 말한다), 이용자의 가입일 또는 해지일이 열거되어 있다.

79) 이것은 형사소송법(제199조 제2항)의 공무소 등 공사단체에 대한 조회와 유사하다.

다. 소결

정보수집권한이 국가정보원법에 체계적이고 명확하게 규정되어 있지 않고 산발적으로 흩어져 있다. 이러한 정보수집권한에서 국가정보원이 범죄와 관련된 정보를 수집할 가능성이 예상될 수 있는 경우로는 우편물의 검열, 전기통신의 감청, 공개되지 아니한 타인간의 대화의 녹음 및 청취 또는 금융거래정보의 수집으로 보인다. 하지만 실제로 전기통신의 감청을 제외하면 가능성은 그리 높아보이지 않는다. 그리고 국가안보를 위한 통신제한조치는 일반통신감청보다 까다롭다. 고등법원 수석판사의 허가나 대통령의 승인을 요구하고 있기 때문이다. 독일의 경우 통신비밀제한법에 의한 일반감청이나 암호통신감청 그리고 전략적 국제통신감청은 해당 정보기관이 신청하고 내부무장관이 명령하며 G10 위원회의 동의를 받아 집행한다. 연방정보부법의 전략적 해외통신감청이나 정보기술시스템 침입의 경우 연방정보부가 명령하고 독립통제위원회의 허락을 받는다. 우리처럼 법관이나 대통령의 승인을 받지 않는다.

무엇보다도 독일이 도입하고 있는 암호통신감청, 온라인수색, 전략적 통신감청과 같은 정보통신기술의 발전에 대응하는 비밀정보수집권한이 도입되어 있지 않다. 또한 신분위장요원이나 신뢰인과 같은 정보원을 활용할 수 있는 권한도 명시되어 있지 않다. 따라서 독일 정보기관의 정보수집권한과 비교할 때 정보수집권한의 종류가 상당히 부족하고 게다가 법률 규정도 명확하지 않다.

3. 정보기관과 수사기관의 협력

국가정보원법에는 국정원과 다른 공공기관 사이의 협력에 관한 명시적인 일반규정은 존재하지 않는다. 개인정보보호법 제58조 제1항 제2호의 적용 배제 규정이 적용되더라도 구체적인 협력 규정이 필요하다. 하지만 형사정책적 관점에서 의미를 가질 수 있는 협력에 관한 것으로 볼 수 있는 것은 수사기관과의 공조체계 구축 및 상호 협력(제5조 제3항)과 수집된 정보의 직무 외 사용금지(제3조 제2항)이다.

우선 제5조 제3항에 따르면 제4조 제1항 제1호 나목부터 라목까지의 직무수행과 관련하여 국정원은 각급 수사기관과 정보 공조체계를 구축하고, 국정원과 각급 수사기관은 상호 협력하여야 한다고 규정하고 있다. 2024년부터 적용될 개정 국정원법에는 다목과

라목으로 제한된다. 나목은 방첩, 대테러, 국제범죄조직에 관한 정보이고, 다목은 형법의 내란의 죄와 외환의 죄, 군형법의 반란의 죄, 암호부정사용의 죄, 그리고 군사기밀보호법에 규정된 죄에 관한 정보이다. 라목은 국가보안법에 규정된 죄와 관련되고 반국가단체와 연계되거나 연계가 의심되는 안보침해행위에 관한 정보이다. 이러한 공조체계 및 협력에는 국외 및 북한에 관한 정보와 국제 및 국가 배후 해킹조직 등 사이버안보 및 위성자산 등 안보 관련 우주 정보는 제외되어 있다. 이들은 수사기관과 직접 관련이 없기 때문인 것으로 보인다.

수사기관과의 공조체계 구축 및 협력에 관한 제5조 제3항은 이번 국가정보원법 개정으로 도입된 것으로 정보와 수사의 분리란 관점에서 중요한 의미를 가진다. 그런데 국정원이 구축해야 할 정보공조체계가 무엇인지, 각급 수사기관이 상호협력해야 할 내용이 무엇인지에 대하여 법문언상으로는 쉽게 알 수 없다. 다만 국정원의 운영원칙에 관한 제3조 제2항에서 유추해 볼 수 있다. 이에 따르면 국정원은 수집된 정보를 직무 외의 용도로 사용해서는 안 된다고 규정하고 있다. 여기서 직무와 관련하여 수집된 정보는 사용할 수 있다는 해석이 논리적으로 나온다. 국정원이 이 규정에 의해서 범죄에 관한 정보를 제공할 수 있는 것으로 볼 수 있다. 따라서 제한적 범위에서 국정원이 수집한 정보를 수사기관으로 이전할 수 있다.

한편 국정원이 국가안보와 관련한 정보 분석의 목적으로 개인정보를 수집하거나 제공을 요청하는 경우에는 제3장의 개인정보의 처리에 관한 규정들이 적용되지 않는다. 따라서 다른 기관으로 정보를 이전하는 것도 이 조항에 의해서 가능할 수 있다. 여기서 이전은 제3자 제공을 의미한다. 하지만 개인정보의 이전도 자기정보통제권의 보호범위에 포함되기 때문에 이를 제한하는 수권규정이 필요하다.

이에 반해서 정보기관과 위험방지기관인 경찰 사이의 공조체계나 협력에 대해서는 구체적인 규정이나 시행령도 존재하지 않는다.[80] 공조체계나 협력에 대한 구체적인 내용은 아마도 정보활동기본지침에 규정될 것으로 예상된다. 이 경우 공공기관, 검찰이나 경찰이 정보기관 관련 정보를 자발적으로 보고하는 규정과 이와 반대로 정보기관이 검찰이

80) 이것은 국가정보원법의 문제라기 보다는 위험방지와 관련한 경찰의 수권규정이 우리 경찰법이나 경찰관직무집행법에 구체적으로 갖추어지지 않았기 때문으로 보인다. 독일의 위험방지와 관련한 경찰법 규정들은 범죄수사에 관한 형사소송법의 수권규정들과 거의 유사하게 규정되어 있다. 이에 반해 우리 경찰법은 위험방지와 관련한 구체적 수권규정이 제대로 규정되어 있지 않다.

나 경찰에 정보를 제공하는 것이 포함되어야 할 것이다. 정보활동기본지침은 공개되지 않는다. 앞서 언급하였듯이 이러한 비밀주의는 현대의 법치국가에서 허용되기 어렵다. 따라서 독일과 같이 법률에 명시적으로 규정되어야 한다.

Ⅶ. 형사정책적 관점에서 개선방안

국가정보원법의 개정으로 정보와 수사가 형식적으로 분리되었지만 정보수집권이 정보통신기술의 발전에 대응하지 못하고 있고 각자의 기능이 협력관계에 있지 않기 때문에 이러한 법적 상황은 국가의 전체 안보건축을 유지하는데 충분하지 않다. 따라서 정보기관에게 '간접적' 형사정책기능을 기대하기 어렵다고 판단된다. 정보와 수사의 분리원칙에 입각하여 상호협력을 통하여 안보건축물을 공동으로 유지해야 한다는 전제에서 각자의 직무를 수행하되 정보교환을 통해서 상호협력하는 시스템이 마련되어야 한다. 그런 의미에서 몇 가지 개선방안을 제시한다.

1. 정보수집권 규정의 명시

국가정보원이 정보를 어떻게 수집하고 있는지 국민들은 아무도 모른다. 국가정보원법은 정보수집권에 대해 명시적으로 규정하지 않고 국정원의 '정보활동기본지침'에서 정해지기 때문이다. 앞서 언급했듯이 이러한 태도는 법치국가원리에 합치하는지 의문이다. 국가정보원법 제8조에서 조직 등의 비공개를 규정하고 있지만, 이것이 정보수집권의 비공개를 의미하지는 않는다. 조직 등의 비공개는 또한 예외적인 경우이다. 국가정보원이 비밀리에 정보를 수집하는 활동은 기본적으로 개인정보자기결정권이나 사생활의 비밀, 통신의 비밀 나아가서 주거의 불가침도 침해할 수 있기 때문이다. 국가정보원이 이제는 국외정보만 수집한다고 해서 국민의 기본권 침해와 관련이 없다고 주장할 수도 있다. 하지만 이러한 주장은 오늘날 일상생활이 국내에 한정되어 있지 않고 인터넷과 같은 정보통신기술을 통해서 전세계를 대상으로 영위되고 있다는 환경을 고려하지 못한 것이다. 나아가서 독일연방헌법재판소가 외국인에게도 독일기본법의 기본권이 적용될 수 있다고

천명한 점을 환기할 필요가 있다. 따라서 정보수집권을 명확하게 규정해야 한다. 그리고 다른 법률에 간접적으로 규정되어 있는 정보수집권도 국가정보원법에서 명시할 필요가 있다. 이에 대해서 남북한의 대치 상황 등을 이유로 정보수집권을 명시적으로 규정하는 것에 반대하는 견해가 제시될 수도 있다. 하지만 앞서 검토한 바와 같이 정보수집권이 산발적으로 이미 규정되어 있다는 점에서 이러한 견해는 설득력이 떨어진다.

2. 정보통신기술의 발전에 대응하는 정보수집권의 도입

현재 국가정보원의 정보수집권은 독일과 비교할 때 상당히 부족하다. 특히 그 속성이 비밀리에 수행될 정보기관의 수단이 충분하게 규정되어 있지 않다. 국가안전보장과 관련된 범죄나 테러범죄에 대응하기 위해서는 발전된 정보통신기술을 활용할 수 있어야 한다. 이미 테러범죄자들은 이러한 정보통신기술을 이용하여 은밀하게 헌법질서에 반하는 시도나 활동을 하고 있는데 아날로그 방식의 정보수집권한으로는 이에 대응할 수가 없다. 이러한 점에서 최근 독일 정보기관에게 부여된 암호통신감청, 온라인 수색, 전략적 해외통신감청 등 비밀정보기관의 수단을 도입할 필요가 있다. 정보기관의 정보수집권 확대는 수집한 데이터를 수사기관으로 이전하는 상호협력과 밀접한 관계가 있다.

3. 정보의 전달 및 상호협력 관계의 구체화

국정원법의 개정을 통해서 정보와 수사가 분리되었지만, 정보기관과 수사기관의 협력관계가 구체적으로 규정되어 있지 않다. 이러한 협력관계는 특히 정보의 상호 전달로 구체화될 수 있다. 따라서 정보기관에게 충분한 정보수집권을 보장하여 수집 및 분석과정에서 위험방지나 범죄행위에 관한 정보나 활동을 발견한 경우 경찰이나 수사기관으로 전달할 수 있어야 한다. 이와 반대로 공공기관이나 경찰 및 수사기관도 임박한 위험이나 범죄에 해당되지 않는 시점의 정보기관직무와 관련된 정보를 알게 된 경우 즉시 보고하도록 하는 규정을 도입해야 한다. 이것은 국가의 안보건축물을 공동으로 떠받치고 있는 세 개의 기둥이 해야 할 각자의 역할에 해당하기 때문이다. 국가의 안보건축물이 유지될 수 있도록 충분한 정보수집권이 보장되어 협력관계가 작동될 수 있어야 한다.

또한 협력관계에서 정보의 요청 시 가정적 정보 이전 원칙에 따라야 한다. 정보수집의 요건이 동일하거나 유사한 정보의 경우에만 사용이 가능해야 한다. 예를 들어 공개수집으로 가능한 정보를 통신감청으로 수집한 정보와 동일시 할 수 없기 때문이다. 이러한 문제는 구체적으로 형사절차의 관점에서 증거사용금지와 관련이 될 수 있다.

Ⅷ. 맺음말

국가정보원법의 개정으로 정보와 수사가 분리되어 독일 정보기관의 외양을 갖추고 있다. 비교법적 분석을 통하여 독일의 정보기관은 분리원칙에 따라 직무를 수행하고 있지만 위험방지기관인 경찰 및 범죄수사기관과의 상호 협력을 통하여 각자의 역할을 수행함으로써 국가안보에 공동으로 기여하고 있음을 알 수 있다. 특히 정보교환을 통한 협력관계에서 정보기관은 정보의 수집 및 분석 활동으로 알게 된 위범방지나 범죄수사에 관한 정보를 경찰이나 수사기관에 전달함으로써 정보기관이 '간접적으로' 형사정책적 기능도 함께 수행하고 있다고 판단된다. 최근 정보기관에게 정보수집권이 확대됨으로써 이러한 기능은 더욱 강화될 것으로 보인다.

하지만 우리의 경우 특히 정보와 수사가 분리되었지만, 정보기관의 정보수집이 명확하게 규정되어 있지 못하고 게다가 정보수집권한도 현재의 정보통신기술에 대응하기 어려울 뿐 아니라 정보이전과 같은 협력에 관한 규정이 명확하지 않다. 따라서 정보기관과 수사기관이 국가안보에 공동으로 기여하기 어려운 구조로 되어 있고 그리하여 정보기관에게 '간접적' 형사정책기능도 기대하기 어렵다고 판단된다.

따라서 국가정보원법에 정보수집권 규정이 명시되어야 하고, 정보통신기술의 발전에 대응하는 정보수집권이 도입되어야 하며, 정보의 전달 및 상호협력 관계가 구체화되어야 할 것이다. 그리고 국가정보원법의 개정으로 현재 국내정보기관이 부재하다. 이러한 연구결과는 앞으로 존재하게 될 국내정보기관에게도 그대로 적용될 수 있을 것이다.

참고문헌

김호정, 정보기관의 정보수집 활동과 '개인정보 자기결정권', 외법논집 제39권 제1호, 2015.

명재진, 독일 헌법수호청에 관한 연구, 법과 정책연구 제19집 제1호, 2019.

민영성/강수경, "독일의 인터넷 비밀수사에 관한 논의와 그 시사점", 국민대학교「법학논총」제31권 제2호, 2018.

박병욱, 독일 나찌시대 제국안전중앙청(Relchssicherheitshauptamt)의 긴 그림자, 경찰법연구 제11권 제2호, 2013.

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

박희영, 이용대기상태의 위치정보 수사의 허용과 입법방향, 형사정책연구 제31권 제2호(통권 제112호, 2020. 여름).

박희영/윤해성/김재현/임유석, 독일 온라인 안보정보수집 법제연구, 2021년도 국가보안기술연구소, 위탁연구보고서 2021-147.

손미숙, "독일의 테러 대응 법제 및 체계",「테러 예방 및 대응을 위한 수사의 실효성 및 예측의 효율성 확보 방안」, 한국형사정책연구원, 2016.

정문식/정호경, 정보기관의 해외통신정보활동에 대한 헌법적 한계 - 독일연방정보원법(BNDG) 위헌결정에 나타난 위헌심사기준과 내용을 중심으로 -, 공법연구 제49집 제3호,

Arzt, Clemens, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, ATDG § 1 Rn. 29 ff., 2019.

Brandt, Karsten, Das Bundesamt für Verfassungsschutz und das strafprozessuale Ermittlungsverfahren, Die Mitwirkung des Bundesamtes für Verfassungsschutz in strafprozessualen Ermittlungsverfahren vor dem Hintergrund des sog. Trennungsgebots, Berlin 2015.

Graulich, Kurt, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes,

BVerfSchG § 9a, 2019.

Greßmann, Michael, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, IV § 3 Nachrichtendienste und Strafverfolgung, 2017.

Gusy, Christoph, in: Dietrich/Eiffler, Handbuch des Rechts der Nachrichtendienste, Ⅳ § 1, 2017.

Gusy, Christoph, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BNDG § 1, 2019.

Huber, Bertold, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, Artikel 10-Gesetz § 3, 2019.

Marschoileck, Dietmar, Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, NJW 2015, 3611-3616.

Roth, Wolfgang, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, BVerfSchG § 4 Rn. 7, 2019.

Singer, Jens, Das Trennungsgebot - Teil 1 -, Die Kriminalpolizei 2006.

인터넷사이트

https://netzpolitik.org/2019/wir-veroeffentlichen-den-gesetzentwurf-seehofer-will-staatstrojaner-fuer-den-verfassungsschutz/#Referentenentwurf-Bundesverfassungsschutzgesetz (2021.8.25 방문)(인용: https://bit.ly/3n41qeY).

Expansion of information collection rights of German intelligence services and implications for criminal policy*

- Focusing on Online-Durchsuchung, Quellen-TKÜ, and Ausland-Ausland-TKÜ -

Park, Hee-young**

In general, state authorities that perform tasks related to national security are three: intelligence agencies, risk prevention agencies, and investigation agencies. The ultimate goal of national security is national protection and constitutional protection.

With the revision of the National Intelligence Service Act last year, especially the anti-communist investigation authority was transferred to the police, the National Intelligence Service (NSA) now plays only the role of a pure foreign intelligence agency. Therefore, the question of how to establish the relationship between these three agencies in the future in matters related to national security has been raised. Raising these issues provides a starting point for comparative legal research on the german system that follows the principle of the separation of police and intelligence (Trennungsgebot) and cooperative relationship among these agencies.

The german intelligence services (BfV, BND, MAD and 16 State Office for the Protection of the Constitution) are separated from the police in their organization, duties, authority and information by the separation principle. However, despite this separation principle, german intelligence agencies are contributing to national security jointly by performing their respective roles through mutual cooperation with other agencies. In particular, in cooperative relationships through data sharing, intelligence agencies are also performing criminal policy functions ‘indirectly’ by

* This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2020S1A5A2A01043286).

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

providing information learned through information activities to the police or investigation agencies. In addition, these functions are expected to be further strengthened with the introduction of new information-gathering rights such as the online search (Online-Durchsuchung) and source telecommunications surveillance (Quellen-TKÜ) and the strategic surveillance of foreign telecommunications (Ausland-Ausland-Telekommunikationsüberwachung).

Now in Korea, intelligence and police are separated. This separation is considered to be a desirable direction as the separation of powers within the executive branch has been realized. However, several problems are found. Therefore, the regulation on the information collection right of intelligence agencies should be specified in the National Intelligence Service Act, such information collection right should vary according to the development of information and communication technology, and information sharing and mutual cooperation relationship between intelligence and investigative authorities should be materialized.

❖ key words: intelligence services(Nachrichtendienste), the principle of the separation of police and intelligence (Trennungsgebot), online search(Online-Durchsuchung), source telecommunications surveillance(Quellen-TKÜ), strategic surveillance of foreign telecommunications(Ausland-Ausland-Telekommunikationsüberwachung), BfV, BND, MAD

투고일 : 9월 6일 / 심사일 : 9월 30일 / 게재확정일 : 9월 30일