대테러전산자료법의 데이터마이닝 허용 규정에 대한 헌법불합치 결정[1)]

1. 사건개요

(1) 대테러전산자료법상 데이터 확장사용 관련 규정

대테러전산자료(Antiterrordatei)[2)]는 국제적인 테러리즘에 대항하기 위한 연방 및 주의 경찰당국 및 국가정보기관의 결합전산자료(Verbunddatei)이다. 일반적인 경우에 대테러전산자료법[3)] 제5조 제1항 제1호 a목은 권한 있는 행정청의 개인정보 질의에 대해 대테러전산자료 속 식별을 위해 저장된 기초데이터(Grunddaten)[4)]에만 접근을 허용하고 있다. 급박한 상황에서 매우 협의의 조건을 충족하는 경우 외에는 전산자료에 저장된 확장기초데이터(erweiterte Grunddaten)[5)]에 대한 접근은 허용되지 않는다. 2015년 1월 1일에 발효된 개정 대테러전산자료법 제6a조[6)]는 대상적으로 구분될 수 있고, 정해진 기간에

---

1) 2020년 11월 10일자 사건번호 1 BvR 3214/15.

2) 역주: 용어와 관련하여, 'Datei'는 데이터(Daten)가 축적된 자료로서 '전산자료'로 번역하였다. 데이터(Daten)라는 용어는 'Datum(시일)'의 복수(Pluralwort) 형태지만, 전문용어로 쓰일 때에는 대개 연구나 조사의 바탕이 되는 자료를 뜻하며, 이러한 자료를 의미있게 정리하면 정보(Information, Auskunft)가 된다.

3) 정식 명칭은 '연방과 주의 경찰당국 및 정보기관의 표준화된 중앙 대테러전산자료 조직을 위한 법률'(Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern, Antiterrordateigesetz - ATDG).

4) **기초데이터**란 대테러전산자료법 제3조 제1항 제1호 a목에 규정되어 있는 항목을 가리킨다. 이에 따르면 성(姓), 명(名), 개명 전의 이름, 다른 이름, 별칭 관련 인적사항, 이름을 표기하는 다른 방식, 성별, 생년월일, 태어난 장소, 태어난 국가, 현재와 이전의 국적, 현재와 이전의 주소, 신체상의 특이 사항, 언어, 방언 등이 기초데이터에 해당한다.

5) **확장기초데이터**란 대테러전산자료법 제3조 제1항 제1호 b목에 규정되어 있는 항목을 가리킨다. 여기에는 자기 소유 또는 사용하는 원거리통신접속선 및 원거리통신접속장치, 전자우편주소, 은행 계좌, 우편사서함, 자기 명의 또는 사용하는 차량, 가족관계, 소속 민족, 개별 사건에서 국제 테러리즘을 규명하거나 극복하기 위해 필요한 경우 소속 종교에 관한 정보, 형법전 제129a조 제1항과 제2항에 따른 테러 범죄의 준비와 수행에 쓰일 수 있다는 특정한 사실에 기반한 관련 행정청의 인지가 있는 경우에 특수 능력(특히 폭발물이나 무기의 제조나 조작과 관련된 특수 지식 및 숙련도), 학력·직업교육·수행 직업에 관한 사항, 대테러전산자료법 제2조 제1문 제1호와 제2호에서 언급되는 사람들과 만나는 장소 또는 방문한 지역 등이 속한다.

6) **[대테러전산자료법 제6a조 - 프로젝트와 관련된 데이터의 확장사용]**

(1) 관련 연방 행정청은 특정한 개별 사건과 관련된 프로젝트의 범위 내에서 형법전 제129a조, 제129b조, 제211조에 따른 국제 테러 범죄가 시도되고 있다는 인식을 특정 사실이 뒷받침한다면, 그리고 이를 통해 사람들의 신체와 생명 또는 자유에 대한 위험이 임박하고, 개별 사건에서 연관성을

연관되는 과제인 '프로젝트'의 범위 내에서 특정 요건하에 대테러전산자료법 제3조에 따른 전산자료의 확장사용을 가능하게 한다. 대테러전산자료법 제4조에 따라 은폐되어 저장된 데이터는 이러한 이용으로부터 제외된다. 대테러전산자료법 제6a조 제1항 내지 제3항은 특정한 개별 사안과 관련된 프

규명하기 위해 국제적인 테러 움직임에 대한 정보의 수집과 사용이 필요한 때에, 법률상의 과제 이행을 위해 제4조에 따라 은폐되어 저장된 데이터를 제외하고 제3조에 따라 저장된 데이터유형의 데이터를 확장사용할 수 있다.

(2) 관련 연방 행정청은 법률상의 과제 이행을 위해 특정한 개별 사건과 관련된 프로젝트의 범위 내에서 가중범죄인 국제 테러의 소추를 위해 필요한 경우, 개별 사건의 다른 연관성을 규명하기 위해 제4조에 따라 은폐되어 저장된 데이터를 제외하고 제3조에 따라 저장된 데이터유형의 데이터를 확장사용할 수 있다. 국제 테러의 가중 범죄란 형법전 제89a조, 제89b조, 제91조, 제102조, 제129a조, 제211조 또는 제212조의 형사 구성요건을 충족하는 국제 테러 행위이다.

(3) 관련 연방 행정청은 법률상의 과제 이행을 위해 특정한 개별 사건과 관련된 프로젝트의 범위 내에서 국제 테러 가중범죄를 예방하기 위해 필요하다면, 그리고 그러한 범죄가 자행될 것이라는 인식을 사실이 뒷받침한다면, 개별 사건의 다른 연관성을 규명하기 위해 제4조에 따라 은폐되어 저장된 데이터를 제외하고 제3조에 따라 저장된 데이터유형의 데이터를 확장사용할 수 있다. 제2항 제2문은 유추 적용된다.

(4) 프로젝트란 대상적으로 구분될 수 있고, 정해진 기간에 연관되는 과제이며, 해당 사건에 관련되는 사람에 대한 위험 또는 임박한 손해, 과제의 목적설정 또는 그 후속효과로 인해 중요성이 강조된다.

(5) 확장사용이란 개인 및 사람들의 집단, 시설, 사물과 대상들 간의 관련성을 생성하고, 중요하지 않은 정보나 인식은 제외하며, 알려진 사실관계에 대한 상세한 정보를 배치하고, 저장된 데이터를 통계학적으로 평가하는 것을 의미한다. 관련 연방 행정청은 이를 위해

1. 음성학적 데이터 또는 불완전한 데이터를 통해서
2. 여러 데이터필드의 검색을 통해서
3. 사람들·시설·기관·사건 간의 연결을 통해서, 또는
4. 검색범주의 시간적 범위를 제한함으로써

데이터를 탐문할 수 있으며, 사람들 간의 공간적 관계 및 다른 관계를 통해 사람들·사람의 집단·시설·사물·사건 간의 연관성을 제시하며 검색의 범주를 중요도에 따라 서열화할 수 있다.

(6) 프로젝트와 관련된 범위 내에서 확장사용에 대한 접근권한은 해당 영역 업무의 직접적인 수탁자에게만 있다. 프로젝트와 관련된 데이터의 확장사용은 최고 2년 이내로 기한을 정해야 한다. 프로젝트와 관련한 데이터의 확장사용 요건이 존속하고 프로젝트에서 얻은 인식으로부터 프로젝트를 지속해야 할 필요성이 도출되는 경우에 기한을 2회에 한하여 각각 최고 1년까지 연장할 수 있다.

(7) 프로젝트와 관련한 데이터 사용은 신청에 기해서만 지시된다. 신청은 행정청장이나 그의 대리를 통해 서면으로 제의되어야 하며 이유를 명기해야 한다. 신청서는 지시에 필요한 모든 사항을 포함하고 있어야 한다. 신청을 제의하는 행정청에 대한 전문감독을 담당하는 연방 최고행정청이 지시를 관할한다. 지시는 서면으로 처리한다. 지시서에는 지시의 이유, 프로젝트와 관련된 데이터의 확장사용에 필요한 제3조에 따른 데이터 종류, 프로젝트와 관련된 데이터의 확장사용의 기능적 범위 및 사용기간을 기재해야 한다. 프로젝트와 관련된 데이터의 확장사용의 기능적 범위는 프로젝트의 목적 달성을 위해 필요한 정도에 국한한다. 지시는 이유를 명기해야 한다. 이유에는 제1항 내지 제3항에서 언급된 요건이 증명되어야 하며, 특히 프로젝트와 관련된 확장사용이 상관관계 규명을 위해 필요하다는 요건이 증명되어야 한다. 지시를 내리는 행정청은 신청서와 지시서를 데이터보호법상 감시목적을 위해서는 2년 동안 보유하며, 적어도 프로젝트와 관련된 확장사용 기간 동안 이를 보유한다.

(8) 제7항에 따라 지시된 확장사용은 G 10 - 위원회(서신·우편·통신의 비밀 제한에 관한 법률 제15조 제1항 내지 제4항)의 동의하에서만 집행될 수 있다. 지체하면 위험할 우려가 있는 경우에는 제7항 제4문상의 관할 행정청이 위원회의 동의 전에 집행을 지시할 수 있다. 위원회가 지시를 허용되지 않거나 불필요한 것이라고 선언하면 제7항 제4문상의 관할 행정청은 이를 지체 없이 취소해야 한다. 이러한 경우에 데이터의 확장사용을 통해 얻게 된 데이터와 인식은 절대적으로 사용이 금지되며 지체 없이 삭제해야 한다.

(9) ~ (11) 생략.

로젝트의 범위 안에서의 확장사용을 국제 테러 계획에 대한 정보의 수집(제1항), 가중범죄인 국제 테러의 소추(제2항 제1문) 또는 가중범죄인 국제 테러의 예방(제3항 제1문)을 위한 것인지에 따라 구분한다.

입법자는 대테러전산자료법 제6a조 제5항에서 확장사용의 개념을 정의하고 있다. 이는 개인 및 사람들의 집단, 시설, 사물과 대상들 간의 관련성을 생성하고, 중요하지 않은 정보나 인식은 제외하며, 알려진 사실관계에 대한 상세한 정보를 배치하고, 저장된 데이터를 통계학적으로 평가하는 것을 의미한다(제1문). 관련 연방 행정청은 음성학적 데이터 또는 불완전한 데이터를 통해서나 여러 데이터필드의 검색을 통해서, 사람들・시설・기관・사건 간의 연결을 통해서, 또는 검색범주의 시간적 범위를 제한함으로써 데이터를 탐문할 수 있으며, 사람들 간의 공간적 관계 및 다른 관계를 통해 사람들・사람의 집단・재단・사물・사건 간의 연관성을 제시하며 검색의 범주를 중요도에 따라 서열화할 수 있다(제2문). 이처럼 대테러전산자료법 제6a조는 저장된 데이터베이스의 직접적인 연결로 얻는 자료로부터 새로운 정보를 이끌어 내는 때에 대테러전산자료를 직접적으로 사용하는 것을 허용한다(이른바 '데이터마이닝' [7]).

(2) 이 사건 헌법소원 심판청구 경위

청구인은 대테러전산자료법 제6a조에 대한 헌법소원을 제기하면서 해당 조항을 통해 자신의 개인정보자기결정권(Grundrecht auf informationelle Selbstbestimmung, 기본법 제2조 제1항[8]과 연계한 동법 제1조 제1항[9])이 침해되었다고 주장하였다. 청구인은 자신이 해당 조항의 규율 대상이 될 가능

7) 데이터마이닝이란 '대규모의 데이터 속에서 일정한 패턴을 찾아내는 통계적 기법' 또는 '많은 데이터 가운데 숨겨진 유용한 상관관계를 발견하여 필요한 정보를 추출하고 이용하는 과정' 등으로 설명되고 있다.

8) [기본법 제2조 제1항]
모든 사람은, 다른 사람의 권리를 침해하지 않고 헌법질서나 도덕률에 반하지 않는 한, 자신의 인격을 자유로이 실현할 권리를 갖는다.

9) [기본법 제1조 제1항]
인간의 존엄성은 훼손될 수 없다. 이를 존중하고 보호하는 것은 모든 국가권력의 의무이다.

성이 있으며, 자신이 해당 조항의 규율 대상인지 여부에 대해 전형적으로 알아차릴 수조차 없는데다 자신과 관련된 저장 데이터에 대한 정기적인 문의 또한 현실적으로 불가능하므로 해당 조항이 자신의 기본권을 침해한다고 주장하였다. 청구인은 자신의 사적 또는 공적인 발언 및 정보기관의 입장에서 의심스러울 수 있는 자신과 사회적으로 밀접한 관계를 맺고 있는 사람들로 인해 정보기관이 자신의 대화를 비밀리에 도청하여 이를 통해 얻은 데이터를 저장하고 대테러전산자료에 등록하는 것과 같은 행위를 할 가능성이 있다고 주장하였다. 청구인의 주장에 따르면, 원칙적으로는 그러한 데이터를 수집하거나 인지할 수도 없었던 경찰당국도 대테러전산자료법을 통해 해당 데이터에 접근할 수 있게 되고, 대테러전산자료법 제6a조에 따라 프로젝트와 관련된 데이터의 확장사용까지 가능하게 되었다. 또한 정보기관이 허용되지 않은 정보를 조달할 수 있다는 사실에 대한 자신의 비판적인 발언과 예비적 정보 저장(Vorratsdatenspeicherung)[10]에 반대하는 활동 또는 사회운동단체인 'DigitalCourage[11]' 에 대한 활발한 지지활동으로 인해 자신의 데이터가 수집될 가능성이 존재한다고 주장했다. 이러한 활동 중에 - 가령 집회활동에서 - 극단주의자들과 접촉할 가능성이 있고 정보기관의 눈에 띄어 데이터가 저장될 위험이 있다는 것이다. 나아가 그가 예전에 접촉했던 시리아 사람들이 테러단체인 '이슬람국가(IS)[12]' 의 교전행위와 관련이 있었으므로 대테러전산자료에 그와 관련된 데이터가 저장되어 있을 가능성이 있다고 하였다. 이를 계기로 자신에 관한 데이터가 저장되거나 적어도 그러한 저장을 배제할 수 없으므로 청구인은 자신의 개인정보자기결정권이 침해되었다고 주장하였다.

---

10) 예비적 정보 저장은 중범죄의 예방과 소추를 위한 도구로서, 공적으로 접근 가능한 전자통신서비스의 제공자나 공적 통신네트워크의 운영자로 하여금 계약을 통해 얻게 되는 특정한 데이터를 일반적인 계약상의 데이터 저장 기간보다 훨씬 더 긴 기간 동안 저장하도록 의무지우는 것을 말한다.

11) 독일의 개인정보 보호 및 디지털 권리를 수호하는 사회운동단체.

12) 급진 수니파 무장단체로 이라크와 시리아를 중심으로 세력을 확장했다가 중동은 물론 유럽에서도 테러를 자행하며 전 세계에 공포를 안겼으나, 2017년 7월과 10월에 걸쳐 각각 이라크 모술과 수도인 시리아 락까를 잃으면서 와해됐다. 이후 2019년 3월 시리아민주군(SDF)에 의해 마지막 근거지였던 바구즈까지 상실했다.

2. 결정주문

(1) 대테러전산자료법 제6a조 제2항 제1문[13]은 기본법 제2조 제1항과 연계한 동법 제1조 제1항에 합치되지 아니하므로 무효이다.

(2) 그 밖의 청구는 기각한다.

(3) 독일 연방공화국은 청구인에게 헌법소원심판에 필요한 비용 중 절반을 부담해야 한다.

3. 결정이유

(1) 이 사건 헌법소원은 적법하다. 특히 청구인의 청구인적격이 인정된다. 청구인에 관한 데이터가 전산자료에 저장되어 있을 가능성이 있고, 이러한 데이터의 확장 활용이 가능하다. 데이터의 사용은 전형적으로 비밀리에 이루어지므로 침해적 집행행위가 있을 때까지 기다렸다가 이에 대한 권리보호를 위한 재판상의 방법을 택하도록 기대할 수는 없다. 청구인은 정보공개 요청을 통해서도 그러한 조치가 행해졌는지에 대해 확실히 알 수 없고, 언제든지 새로운 데이터 기록이 저장될 수 있으며 데이터 활용을 위한 프로젝트 또한 언제든지 시작될 수 있으므로 자기관련성과 직접성 및 현재성이 인정된다.

(2) 이 사건 헌법소원은 부분적으로 이유 있다. 대테러전산자료법 제6a조 제2항 제1문은 기본법 제2조 제1항과 연계한 동법 제1조 제1항에서 도출되는 개인정보자기결정권에 위배된다. 대테러전산자료법 제6a조 제1항 내지 제

---

13) **[대테러전산자료법 제6a조 제2항 제1문]**
관련 연방행정청은 법률상의 과제 이행을 위해 특정한 개별 사건과 관련된 프로젝트의 범위 내에서 가중범죄인 국제 테러의 소추를 위해 필요한 경우, 개별 사건의 다른 연관성을 규명하기 위해 제4조에 따라 은폐되어 저장된 데이터를 제외하고 제3조에 따라 저장된 데이터 유형의 데이터를 확장사용할 수 있다.

3항이 행정청에 부여하는 권한은 개인정보자기결정권을 제한한다. 동조 제2항 제1문의 경우 이러한 제한이 비례의 원칙에 위배되어 정당화될 수 없다.

(3) 개인정보자기결정권은 현대의 데이터 처리 요건하에서 정보와 관련된 조치로 인해 발생하는 인격의 위협 및 침해를 고려한다.[14] 인격의 자유로운 발현은 개인정보의 무제한적인 수집과 저장, 사용 및 전달로부터 개인을 보호하는 것을 전제로 한다. 이러한 보호는 기본법 제2조 제1항과 연계한 제1조 제1항으로부터 도출되는 기본권에 포섭된다. 해당 기본권은 원칙적으로 개인이 직접 개인정보의 제공 및 사용에 관해 결정할 수 있도록 함을 보장한다.

대테러전산자료법 제6a조 제1항 내지 제3항은 관련 행정청에 대테러전산자료법 제3조에 따라 저장된 데이터의 프로젝트와 관련된 확장사용을 가능하게 함으로써 기본법 제2조 제1항과 연계한 동법 제1조 제1항에서 도출되는 개인정보자기결정권을 제한한다. 여기서 제한은 이미 분리된 데이터의 확장사용에만 그치지 않고, 확장사용을 가능하게 하는 접속에도 해당한다. 대테러전산자료법 제6a조에 규정된 '프로젝트와 관련된 데이터의 확장사용'은 전형적인 '데이터마이닝'의 사례를 보여준다. 해당 조항이 신설되기 전까지 그러한 확장사용은 허용되지 않았으며, 대테러 데이터의 사용은 위험인물에 대한 정보를 해외 수사기관과 교환하는 경우(Informationsanbahnung)에만 가능하였다. 대테러전산자료법 제5조 제2항과 제6조 제2항에 규정된 급박한 경우(Eilfall)에만 (확장)기초데이터와 확장사용이 작전 업무수행을 위해 허용되었다.

(4) 대테러자료의 범위 내에서 프로젝트와 관련된 데이터의 확장사용은 실체적 측면에서 기본법 제2조 제1항과 연계한 제1조 제1항의 요구를 부분적

14) BVerfGE 65, 1 <42 f.> 참조.

으로 충족하지 않는다. 데이터를 직접 전산자료에 등록하지 않은 행정청이 해당 데이터를 확장사용할 수 있도록 하는 형태의 기본권 제한은 이에 대한 한계를 대테러전산자료법 제6a조 제2항에서 규정하지 않았으므로 비례의 원칙에 위배된다. 확장사용을 대테러전산자료법 제6a조 제4항상의 프로젝트의 범위 내에서만 허용한다는 규정을 통해서는 개인정보자기결정권에 대한 제한을 비례적으로 보장할 수 없다. 동조 제7항의 감독 규정이나 제8항의 통제 규정을 통해서도 실체적 요청을 대체할 수는 없다.

1) 대테러전산자료법 제6a조는 테러리즘에 효과적으로 대항한다는 정당한 목적을 추구하며, 이 목적을 위해 적합하고 필요한 수단이다. 그렇지만 해당 규정 제2항 제1문은 좁은 의미의 비례의 원칙에 부합하지 않는다. 이미 존재하는 데이터목록을 해당 데이터를 직접 수집하지 않은 행정청에서 확장사용 하는 것은 좁은 의미의 비례원칙에서 데이터 신규 수집 가정 원칙(Grundsatz der hypothetischen Datenneuerhebung)[15]의 범주에 따라 이루어진다.[16]

2) 입법자가 이미 축적된 전산자료를 활용하도록 한다면 이에 대한 사용 규정이 비례의 원칙에 부합하도록 형성되어야 한다. 입법자는 이러한 전용(Weiterverwendung)을 충분히 중대한 법적 보호대상[17]과 충분한 제한의 한계[18]에 기속시켜야 한다.[19] 데이터를 처음 수집할 당시의 제한이 중할수록 해당하는 법적 근거 내에서 데이터 사용의 요건과 그 범위는 더 협소하게 제한되어야 한다. 개별 제한의 계기와 목적, 범위 및 이에 상응하는 제한의

15) 기본권을 제한하는 감시와 수사조치를 통해 얻은 데이터를 법익 보호나 범죄의 수사 등 변경된 목적을 위해 사용하는 경우 새로운 사용은 해당 데이터를 기존과 유사하게 중한 수단을 통해 신규 수집하는 것이 헌법상 정당화될 수 있는지 여부에 달려있다는 원칙(연방헌법재판소 2016. 4. 20. 판결 - 1 BvR 966/09, 1 BvR 1140/09).

16) BVerfGE 141, 220 <327 f. Rn. 287> 참조.

17) BVerfGE 141, 220 <279 f. Rn. 106 ff.>.

18) BVerfGE 141, 220 <271 ff. Rn. 109 ff.>.

19) 최근의 사례로 2020. 5. 27. 연방헌법재판소 제1재판부 결정 - 1 BvR 1873/13, 1 BvR 2618/13 - , Rn. 130 참조.

한계가 영역별 특징을 고려하여 입법자에 의해 적확하게 확정되어야 하고, 규범이 명백하게 규정되어야 한다.[20]

3) 입법자는 새로운 목적을 위해 데이터를 사용하는 경우나 다른 기관이 데이터를 사용하는 때에 데이터 수집 제한의 경중이 반영될 수 있도록 해야 한다.[21] 수행 과제로 인해 상대적으로 덜 엄격한 요구를 적용받는 행정청이 더 엄격한 요건을 적용받는 다른 행정청에 데이터를 전달하는 방법을 통해 데이터의 수집과 저장 및 처리와 관련된 헌법상 요건을 무력화해서는 안 될 것이다.[22] 따라서 데이터 신규 수집 가정의 원칙에 따라 해당 데이터를 변경된 목적을 위해 새로 수집하는 것이 헌법적 기준에 합치되는지 여부가 결정적이다.[23]

(5) 경찰당국과 정보기관 간에 데이터를 교환할 수 있도록 하는 규정은 특별한 헌법적 요청하에 있다(‘정보 분리의 원칙’, informationelles Trennungsprinzip).[24] 경찰당국과 안보청이 정보기관의 정보를 사용할 수 있도록 하는 규정에는 강화된 헌법적 요청이 적용된다.

1) 범죄를 예방하고 저지하며 소추하는 과제 및 공공의 안전과 질서에 대한 위험을 방지해야 하는 과제를 이행하는 경찰당국과 안보청은 작전책임(operative Verantwortung)[25]을 지며, 개인에 대해 필요한 경우에는 강제적인 조치를 관철시킬 권한을 갖고 있다. 따라서 이러한 권한은 협소하고 정확하

---

20) BVerfGE 125, 260 <328>; 2020. 5. 27. 연방헌법재판소 제1재판부 결정 - 1 BvR 1873/13, 1 BvR 2618/13 - , Rn. 133 참조.

21) BVerfGE 100, 313 <389 f.>; 109, 279 <377>; 120, 351 <369>; 130, 1 <33 f.>; 133, 277 <372 f. Rn. 225>; 141, 220 <326 f. Rn. 284> 참조.

22) BVerfGE 133, 277 <323 f. Rn. 114>.

23) BVerfGE 125, 260 <333>; 133, 277 <373 ff. Rn. 225 f,>; 141, 220 <327 ff. Rn. 287 ff.>; 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 216 참조.

24) BVerfGE 133, 277 <329 Rn. 123>; 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 218 f. 참조.

25) 주로 테러 범죄의 방지를 위해 전략적으로 대응해야 하는 임무를 의미한다.

게 규정되어야 한다. 데이터의 처리는 원칙적으로 범죄 혐의나 위험과 같은 구체적인 계기를 근거로 요한다.[26]

2) 반면에 정보기관은 주로 정책 결정권자에게 정보를 제공하는 역할을 수행한다. 정책에 대한 선제적 해명이라는 과제에 상응하여 정보기관은 광범위하며 제한의 한계에 거의 구애받지 않는 데이터 수집 권한을 갖는다.[27] 이처럼 광범위한 데이터 수집 권한은 정보기관에게 선제적 해명 과제를 넘어서는 작전책임이 주어지지 않는다는 점을 통해 상쇄된다.[28] 그렇지만 정보기관의 과제가 필연적으로 정책에 대한 선제적 해명에만 국한되지는 않는다. 연방정보기관은 국제적 차원에서 다수의 해외로부터의 임박한 위험에 대한 조기발견 과제[29]를 수행하고 있으며, 위험의 조기발견에 대한 정보를 경찰당국과 안보청에 전달하는 업무[30] 또한 수행하고 있다. 이를 통해 정보기관과 경찰당국 간의 간극이 좁혀질 수 있다. 하지만 정보기관에 위험의 조기 감지를 위해 비교적 광범위한 데이터 수집 권한이 주어지며, 이에 반해 작전 수행은 할 수 없다는 사실에는 변함이 없다.

3) 수행 과제의 차이로부터 도출되는 데이터의 수집 및 처리에 관한 특수한 요청이 무력화될 위험은 정보기관의 정보를 경찰당국과 안보청이 사용할 수 있도록 하는 규정에 더 높은 헌법상 요청을 부과할 것을 요구한다. 즉, 뚜렷한 공공의 이익과 충분히 구체적이고 적합한 제한의 한계가 요구된다.[31]

---

26) BVerfGE 133, 277 <327 f. Rn. 120> 참조.

27) BVerfGE 133, 277 <325 f. Rn. 117>; 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 150 ff. 참조.

28) BVerfGE 133, 277 <326 f. Rn. 118 f.> 참조.

29) 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 128 참조.

30) 연방정보기관법 제24조 이하, 연방헌법청법 제19조, 군사대응정보법 제11조 참조.

31) BVerfGE 133, 277 <329 Rn. 123>; 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 218 f. 참조.

(6) 데이터 신규수집 가정 원칙에 따라 권한 형성에 있어서 어떤 요청이 법익보호와 제한의 한계에 대해 개별적으로 요구되는지는, 구체적인 부담 작용에 따른다. 대테러전산자료법 제6a조 제5항에 따라 결합전산자료를 정보기관과 경찰당국이 공동으로 확장사용하는 것에는 동법 제5조에 따른 단순사용에 비해 더 높은 부담이 작용한다.

1) 이러한 이유로 대테러전산자료를 위험방지의 목적으로 확장사용한다면 최소한 충분히 구체적인 위험이 발생할 수 있다는 사실상의 근거가 있어야 한다. 정보평가를 확장사용하기 위해서는 개별 사례에서 정보기관의 관찰을 요하는 특정한 행동이나 집단적인 움직임이 필요하다. 즉, 적어도 구체적이고 예견 가능한 사건이 있어야 한다. 범죄의 소추를 위한 확장사용에는 특정하고 사실을 기반으로 하는 혐의가 있어야 한다. 해당 혐의는 구체적이고 확고한 정황에 따른 사실을 바탕으로 해야 한다.[32]

2) 대테러전산자료법 제6a조 제2항 제1문은 위의 요구를 충족시키지 아니한다. 물론 해당 규정은 특히 중대한 법익 보호를 위해서만 확장사용을 허용하고 있다. 그렇지만 대테러전산자료법 제6a조 제2항 제1문에 따른 권한에는 충분히 적합한 제한의 한계가 부재하다. 대테러전산자료법 제6a조 제2항 제1문은 "개별 사건의 다른 연관성(weitere Zusammenhänge des Einzelfalls)"을 규명하기 위한 요건으로 "개별 사건에서 필요한 경우(im Einzelfall erforderlich)"라면 인정하고 있다. 해당 조항은 범죄소추를 목적으로 하는 확장사용에서 요구되는 기초적 사실이 형사소송법상의 초기 혐의(Anfangsverdacht)와 구분되며, 더 확고한 혐의를 요구한다는 점을 규범적으로 명백하게 규정하지 않고 있다. 대테러전산자료법 제6a조 제4항에 규정된 특정 프로젝트에 대한 기속을 통해서도 동조 제2항 제1문의 요건의 헌법상 미비점을 개선할 수는 없다. 제4항에서도 충분한 제한의 한계가 규정되어 있

32) 2020. 5. 19. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 222 참조.

지 않기 때문이다. 결과적으로 대테러전산자료법 제6a조 제2항 제1문은 기본법 제2조 제1항과 연계한 동법 제1조 제1항에서 도출되는 개인정보자기결정권을 침해하였다.

(7) 이에 반해 대테러전산자료법 제6a조 제1항과 제3항은 헌법에 합치한다. 대테러전산자료법 제6a조 제7항과 제8항에 규정된 감시적 통제에 대한 요청 또한 비례의 원칙에 합치한다.

1) 대테러전산자료법 제6a조 제1항은 국제 테러계획에 관한 정보의 수집과 활용을 위해 헌법상의 요청에 부합하도록 해석해야 한다는 특정한 요건하에서 은폐되어 저장되지 않은 대테러 데이터에 대한 접근을 연방 행정청(특히 정보기관)에게 허가하고 있으므로 헌법에 합치한다. 해당 조항은 이 규정을 정보를 수집하지만 직접 작전수행을 하지 않는 행정청, 특히 정보기관이나 중앙기관으로서 연방범죄수사국에게만 적용할 수 있음을 충분히 확실하고 규범적으로 명확하게 규율하고 있다. 해당 조항은 또한 구체적인 제한의 한계를 명시하고 있다. 이에 따르면 개별 사건에서 연관성을 규명하기 위해 국제적인 테러 움직임에 대한 정보의 수집과 사용이 필요한 때에, 형법전 제129a조, 제129b조, 제211조에 따른 국제 테러 범죄가 시도되고 있다는 인식을 특정 사실이 뒷받침하고 이를 통해 사람들의 신체와 생명 또는 자유에 대한 위험이 임박하였다면 대테러전산자료법 제6a조 제5항상의 확장사용이 가능하다.

2) 반면에 대테러전산자료법 제6a조 제2항 제1문에는 이와 같은 제한의 한계 내지 협의의 한계에 관한 규정이 부재하다. 대테러전산자료법 제6a조 제2항은 진압과제 수행을 위한 규정이다. 이에 따라 관련 범죄소추 행정청이 적용범위에 해당되며 정보기관은 적용범위에서 배제된다. 범죄소추 행정청으로 하여금 정보기관이 대테러전산자료에 수집한 데이터를 확장사용할 가능

성을 열어주게 되면 제한의 한계는 더 제약적이어야 한다. 혐의를 뒷받침하는 사실보다 더 분명한 형태의 제한의 한계가 필요하다. 그러나 대테러전산자료법 제6a조 제2항에는 그러한 내용이 포함되어 있지 않다.

3) 대테러전산자료법 제6a조 제3항은 헌법합치적 해석에 의해 결과적으로 비례의 원칙에 부합하는 것으로 보인다. 해당 규정은 정보기관이 대테러전산자료에 저장한 데이터를 국제 테러의 가중범죄 방지를 목적으로 확장사용을 할 수 있는 경찰당국을 대상으로 한다. 이 경우에도 더 제약적인 제한의 한계가 필요하다. 대테러전산자료법 제6a조 제3항은 국제 테러의 가중범죄를 방지하기 위해 그러한 범죄가 자행될 것이라는 인식을 사실이 뒷받침하는 경우에만 행정청이 대테러자료를 확장사용할 수 있도록 하고 있다. 대테러전산자료법 제6a조 제3항상의 구성요건인 '개별 사건의 다른 연관성을 규명'하는 것은 규범의 명확성 원칙에 따라 헌법합치적인 해석을 통해 다음과 같이 이해되어야 한다. 즉, 행정청이 적어도 구체적이고 예견 가능한 사건을 인지하였거나 특정 인물의 개별 행동이 그가 예측 가능한 시점에 테러범죄를 자행할 것이라는 구체적인 개연성을 뒷받침한다면 전산자료의 확장사용이 허용되는 것으로 이해되어야 한다.[33]

4) 대테러전산자료법 제6a조 제7항과 제8항에 규정된 감독기관의 통제는 개인정보자기결정권의 영역에서 준수되어야 하는 비례의 원칙의 기준에 부합한다. 여기서는 행정상의 통제와 법원과 유사한 법적 통제가 상호 보완하고 있다.[34] 특히 급박한 경우에는 사전적인 법적 통제가 항상 필요한 것은 아니다.[35] 따라서 감독기관의 통제(제7항)와 원칙적으로 사전적 통제이자 지체의 위험이 있는 경우에는 사후 동의로 대체 가능한 G - 10 위원회[36]의 법

33) BVerfGE 141, 220 <272 f. Rn. 112, 290 f. Rn. 164>; 2020. 5. 27. 연방헌법재판소 제1재판부 결정 - 1 BvR 1873/13, 1 BvR 2618/13 Rn. 226) 참조.

34) BVerfGE 133, 277 <369 Rn. 213>; 2020. 5. 20. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 274 참조.

35) BVerfGE 133, 277 <369 Rn. 213>; 2020. 5. 20. 연방헌법재판소 제1재판부 판결 - 1 BvR 2835/17 - , Rn. 254 참조.

적 통제(제8항)로 구분되는 통제절차는 헌법상 문제가 없다. 그러나 이러한 통제만으로는 대테러전산자료법 제6a조 제2항에 따른 확장사용에서 부재한 실체적 범주의 제약을 대체할 수 없다. 프로젝트의 한계 및 제한 권한을 준수하는 것은 실체적 규정을 통해서만 통제될 수 있기 때문이다.[37]

4. 결정의 의의

이 사건 헌법소원심판의 청구인은 평소 개인정보 보호 및 디지털 권리 등을 수호하는 사회운동단체의 활동을 지지해오던 사람으로, 대테러전산자료법상 데이터 확장사용에 관한 조항으로 인해 자신에 관한 개인정보가 수집될 가능성이 있음을 주장하며 해당 조항의 위헌성을 다투었다. 이에 대해 연방헌법재판소는 "데이터의 사용이 전형적으로 비밀리에 이루어지므로 침해적 집행행위가 있을 때까지 기다렸다가 권리구제를 받을 것을 기대할 수 없다"는 이유로 적법요건을 인정하여 본안판단에 나아갔다[38].

본안판단과 관련하여서는 행정청이 대테러자료를 확장사용할 수 있는 요건과 관련한 규정이 문제되었다. 연방헌법재판소는 가중범죄인 국제 테러의 '소추'를 위해 필요한 경우 데이터 확장사용을 규정한 대테러전산자료법 제6a조 제2항의 적용대상이 국민에 대하여 강제력을 행사할 수 있는 경찰당국임을 감안할 때, 데이터 확장사용을 허용하기 위한 요건으로 '형사소송법

36) 독일 기본법 제10조에 따른 서신·우편·통신의 비밀을 보장받을 권리를 제한하는 연방 정보기관의 조치에 대해 독립적이고 어떠한 지시에도 얽매이지 않는 기관으로서 해당 조치의 필요성과 허용 여부를 직권으로 조사하는 위원회.

37) 이와 관련하여 BVerfGE 110, 33 <67 f.>; 120, 274 <331> 참조.

38) 우리나라에서는 다양한 사회적 활동에 참여해온 사람들이 '국민보호와 공공안전을 위한 테러방지법'상 정보 수집에 관한 조항 등의 위헌성을 다툰 적이 있었는데, 헌법재판소는 '국가정보원장이 청구인들을 테러위험인물로 지정하지 않았고, 청구인들을 상대로 정보수집 등 조항에 근거한 각종 조치를 위한 적도 없으므로, (...) 청구인들의 주장은 막연한 권리침해의 가능성 내지 우려를 표명한 것에 불과하다'고 하며 헌법소원심판청구의 자기관련성을 부정한바 있다(헌재 2018. 8. 30. 2016헌마442). 독일의 대테러전산자료법과 우리나라의 '국민보호와 공공안전을 위한 테러방지법'의 구조와 내용에 차이가 있어 단순 비교는 어렵겠지만, 적법요건에 대한 관점에 있어서의 차이를 엿볼 수 있다.

상 초기 혐의보다 더 높은 혐의가 있음이 구체적인 사실에 근거하여 뒷받침되는 경우' 등과 같은 더 엄격한 규정이 존재하여야 함에도 불구하고, 해당 규정은 이와 같은 요건을 규정하고 있지 않으므로 헌법에 합치되지 않는다고 결정하였다.

이 결정은 독일 연방헌법재판소가 2020년 5월 27일에 선고한 제2차 기본데이터[39] 결정(Bestandsdatenauskunft Ⅱ)[40]의 연장선상에 있다. 해당 결정에서 연방헌법재판소는 여러 연방 법률에서 기본데이터를 제공할 수 있도록 하는 규정이 헌법에 위배된다고 판시하였다. 이를 통해 보안청이 통신회사로부터 고객의 전화연결 정보나 특정 시점에 할당된 아이피 주소를 알 수 있게 되어 그러한 서비스를 이용하는 고객의 개인정보자기결정권 및 통신의 비밀보장이 침해될 수 있기 때문이라는 취지이다. 범죄 소추와 예방을 위해 이러한 기본데이터를 제공하는 것 자체는 헌법상 허용되지만, 그 허용 범위가 너무 넓어서 입법자가 비례의 원칙에 상응하는 법적인 근거를 마련해야 할 의무가 있다고 한 것이다. 이처럼 개인정보에 대해 개별 상황에 따라 기존 보호 범위보다 더 두터운 보호가 요구된다고 보는 연방헌법재판소의 태도가 이 결정에서도 반영된 것으로 보인다.

39) 기본데이터란 원거리통신서비스제공자와 계약을 체결하거나 계약을 이행하면서 계약의 상대방이 제공하는 이름, 주소, 생일 및 계약의 내용과 같은 데이터를 의미한다.

40) 1 BvR 1873/13, 1 BvR 2618/13.