バイエルン憲法擁護法違憲判決（1 BvR 1619/17）について（1）

山　本　真　敬

目次

Ⅰ．序

2022年4月26日、ドイツ連邦憲法裁判所第一法廷は、バイエルン憲法擁護法（Bayerisches Verfassungsschutzgesetz: BayVSG）の定める情報取得権限および情報提供権限の多くのものを、違憲とした（1 BvR 1619/17）[1]。欄外番号が400を超え、「息を呑むほど（atemberaubend）長

1　NJW 2022, S.1583ff.

い」[2]本判決は、憲法擁護庁を含む情報機関の活動のための要件を設定する原則的[3]・指針付与的[4]な判決であるとされている。本稿筆者の見るところ、本件は、情報機関（憲法擁護庁含む）の活動要件が問題となった事案ではあるが、本判決はヨリ広く、治安維持官庁と情報機関（憲法擁護庁を含む）の活動に多段階的な限界設定を行っており、極めて重要な判決であると思われる。

本稿筆者は、本判決について評する機会を得たが[5]、紙幅に厳しい制約があった関係で、長大な判決について詳しく紹介することが叶わなかった。そこで本稿はそれを補い、本判決をできるだけ丁寧に紹介することを目的とする。

Ⅱ．事案の概要

1．バイエルン憲法擁護法の改正動向

バイエルン憲法擁護法（BayVSG）は、2016年7月12日に改正され（BayGVBl. S.145）、憲法擁護庁のデータ・情報取得権能に関して、諜報機関的手段の利用が追加され、また取得したデータ・情報を他の機関に提供する権能も追加された。この改正によるバイエルン憲法擁護法の新編成に

2　*Klaus Ferdinand Gärditz*, Konturen eines allgemeinen Nachrichtendienstverfassungsrechts, Verfassungsblog, vom 2.5.2022（https://verfassungsblog.de/konturen-eines-allgemeinen-nachrichtendienstverfassungsrechts/; PDF: https://intr2dok.vifa-recht.de/receive/mir_mods_00012610, S.1）.

3　*Gärditz*, a. a. O., S.1; *Katein Werner-Kappler*, Neue Eingriffsschwellen der Verfassungsschutzbehörden, NVwZ 2022 Beilage2, S.63.

4　*Markus Ogorek*, Leitlinien für den Verfassungsverbund, NJW 2022, S.1570; vgl. *Friedhelm Hufen*, Teilweise Verfassungswidrigkeit des Bayerischen Verfassungsschutzgesetzes, JuS 2022, S.1182.

5　自治研究誌において、近日中に掲載予定。

より、情報機関、警察官庁、そしてその他の治安維持官庁の協働を改善し、G10法（Artikel 10-Gesetz）および連邦憲法擁護法（BVerfSchG）において規律されているような、連邦に統一的に妥当する法治国家的規準に依拠するとともに[6]、反テロデータファイルⅠ判決（BVerfGE 133, 277）[7]の述べた情報分離原則（informationelles Trennungsprinzip）[8]に対応する形でデータ・情報の提供規定を改正することが改正の目的であった（BayLTDrucks 17/10014, S. 1f.）。

ところが、この改正直前に、連邦刑事庁法判決（BKAG判決）（BVerfGE 141, 220）[9]が下され、バイエルンのラント議会は、同判決に対応するために、2018年6月12日のバイエルン憲法擁護法を改正するための法律（BayGVBl S.382）を成立させた（vgl. BayLTDrucks 17/20763, S. 1）[10]。

6　ドイツにおけるテロ法制の変容とその概観については、渡辺富久子「ドイツにおけるテロ対策法制とその変容」大沢秀介・新井誠・横大道聡編『変容するテロリズムと法』（弘文堂、2017）143頁以下の参照を乞う。

7　本判決については、入井凡乃「情報機関・警察の情報共有と情報自己決定権」ドイツ憲法判例研究会編『ドイツの憲法判例Ⅳ』（信山社、2018）46頁以下参照。

8　情報分離原則の詳細については、上代庸平「安全確保権限の相互協力的行使と情報共有の憲法的課題」大沢ほか編・前掲註6）161頁以下参照。

9　本判決については、石塚壮太郎「テロ防止のための情報収集・利用に対する司法的統制とその限界」大沢ほか編・前掲註6）180頁以下および同「判批」自治研究94巻7号（2018）145頁以下参照。

10　本判決に関わる主な点については以下の通り（BayLTDrucks 17/20763, S.3ff.）。①第8a条（核心領域保護規定）および第8b条（目的拘束規定）の追加。②第9条第1項第1文柱書部に技術的手段の秘密裏の投入のための目的を明示、第9条第1項第1文第3号の文言変更（微修正）、第9条第2項の追加（措置の対象者および場所の限定）。③第10条第1項柱書部の変更（「情報技術システム」の説明追加）、第10条第2項第1文に第3号を追加（核心領域に関するデータの取得禁止規定の追加）、第10条第3項の追加（措置の対象者と方法の限定）。④第11条第3項（第9条および第10条に基づく措置から取得されたデータの利用目的の限定規定）が削除された他、微修正がなされる。⑤第15条第2項第2文（対象となる目的や行為の限定）が削除、

その後、2022年3月2日には、連邦の新電気通信法（TKG）に対応するための改正、そしてバイエルンのデータ保護法とあわせた改正提案がなされていたが（BayLTDrucks 18/21537）、その改正作業中に、本判決が下されることとなった。

2．関連規定

本件で問題となったバイエルン憲法擁護法の主な規定の概要は、次の通りである。

（1）情報の取得に関する規定

第1に、諜報機関的手段を用いた情報の取得について、第9条は、居住空間を監視するための技術的手段の秘密裏の投入について定めており、その第1項は、連邦またはラントの存立または安全に対する危険（第1号）、人の生命、身体または自由に対する危険（第2号）、特別の公共の利益のためにその保全が要請される物（第3号）に対する切迫した危険の事実に基づく手がかりが存在するときは、秘密裏に技術的手段を用いて盗聴および写真・画像の記録をすることを、ラント当局に授権する旨定める。

第15条第3項第2文（G10法第3b条の準用）が削除。⑥第19a条の追加。⑦第20条第1項第1文第2号c）追加（報告対象追加）の他、微修正。⑧第23条第1項第3文第3号の追加（情報請求権の除外対象の拡大）の他、微修正。⑨第25条第1項第1文（受信者が情報を要求することに関し「事実に基づく手がかり」の語を追加）、同第1文第1号（自由で民主的な基本秩序・公の安全・刑事訴追目的）および第2号の差替え、旧第2号は第3号に、第1a項の挿入、第2項第1文柱書の変更（「受信側が情報を必要としていることの事実に基づく手がかりが存在する場合」の挿入）、同第1文第1号（保護法益の変更）、同第3項第1文第2号の変更（事実に基づく手がかりが存在している旨の限定を追加）、同第1文第3号の変更（同じ）、同第3項に第2文を追加。

第2に、第10条は情報技術システムへの秘密アクセスについて定めており、その第1項は、アクセスデータおよび処理データを取得するため（第1号）、前号に基づく措置を準備するために、特定の識別子（Kennung）および情報技術システムの位置を特定するため（第2号）という目的に限り、情報技術システムに、第9条第1項の定める基準に従って秘密裏に技術的手段を用いてアクセスすることを、ラント当局に授権する旨定める。

第3に、第12条は、携帯通信機器の位置測定について規律している。その第1項は、第3条（任務規定）に含まれる保護利益[11]に対する深刻な危険の発生についての事実に基づく手がかりが存在する場合、電源の入った状態の携帯通信機器の位置を測定するために、または機器番号もしくはカード番号（Kartennummer）の確定のために、技術的手段を投入することを、ラント当局に授権する旨定める。

第4に、第15条は、信書の秘密、郵便の秘密、および電気通信の秘密の保護範囲にある情報の要求について定めており、その第3項は、TKG法（電気通信法）第113a条第2項に基づく義務に際して、同第113c条第2項第2号の下で、同113b条に基づく通信データの情報を取得することをラント当局に授権する旨定める（なお、TKG法第113a条以下は、現行TKG法では175条以下に定めがある）。

11　バイエルン憲法擁護法第3条第1項は、連邦ないしラントの自由で民主的な基本秩序や、その存立もしくは安全に抗する試み、または連邦もしくはラントの憲法上の機関もしくはその構成員の職務遂行を不法に侵害することを目的とする不法な障害を目的とする試み（第1号）、外国権力のために、この法律の妥当領域において、秩序を危険に晒す活動または諜報活動（第2号）、この法律の妥当領域において、武力の行使または武力の行使を目的とする準備行為によってドイツ連邦共和国の外交上の利益を危険に晒す試み（第3号）、この法律の妥当領域において、国際協調主義（基本法第9条第2項）に反する、とりわけ、諸国民が平和のうちに共生すること（基本法第26条第1項）に反する試み（第4号）に関わる様々な情報の取得および評価が、憲法擁護庁の任務である旨定める。

第5に、第18条第1項は、潜入捜査官（Verdeckte Mitarbeiter）、すなわち、自らの職員を、それらに与えられ、長期にわたる作り話（Legende）のもとで、ラント当局が投入することに関して規律している。

第6に、第19条第1項は、嘱託協力者（Vertrauensleuten）、すなわち、計画適合的に、長期間、ラント当局と協力をしていることを第三者が知らない私人（嘱託協力者）を、ラント当局が投入することに関して規律している。

第7に、第19a条は、長期間継続する監視（Observation）について定めている。第1項は、基本法第13条および憲法第106条第3項（住居の不可侵）の保護範囲外で、それが著しい意義を有する試みまたは活動の解明のために必要である場合、或る人物を、48時間を超えて連続的に監視する（beobachten）、または1週間のうち3日以上、秘密裏に、公然と発せられたわけではない言葉を盗聴し記録する（第1号）、写真および画像記録を作成する（第2号）という技術的手段をも用いて計画的に監視することを、ラント当局に授権する旨定めている。

第8に、以上の情報取得に関して、第8a条で核心領域の保護のための定めが置かれている。

（2）取得した情報の他機関への提供に関する規定

第1に、第25条では、取得した情報の他機関への提供について規律されている。第1項は、情報の提供を受ける側の機関が、そのデータ・情報を、第3条に含まれる法益の保護の目的のため、またはさもなくば公衆の安全の目的のため（第1号）、刑事訴追、刑の執行、行刑、そして恩赦手続の目的のため（第2号）、その他のラント当局に割り当てられた任務の実現のため―ただしその際、ラント当局は、自由で民主的な基本秩序の保護、または公衆の安全もしくは外交上の利害の観点をも評価しなければならない―（第3号）に必要であるということの事実に基づく手がかりが存在する場合には、国内の公的機関に提供することを、ラント当局に授権する旨

定める。

第1a項は、EU構成国の公的機関および公的でない機関への提供（第1号）、EU構成国の国家間および超国家的機関への提供（第2号）、シェンゲン協定の諸規定を、シェンゲン協定の国内法化（umsetzen）、適用および発展に関するEUの連合協定に基づいて適用する国家の公的機関への提供（第3号）に、第1項を準用する。

第2項は、諜報機関的手段を用いて取得した情報を、検察庁、AO（租税通則法）第386条第1項に基づく税務官庁、警察、脱税調査を委託されたラント財務官庁の機関、税関警察およびその他の関税に関する機関に対して、これらが連邦警察法に基づく任務を遵守する限りで、連邦またはラントの存立または安全の保護、または個人の生命、身体、健康、自由または性的自己決定の保護もしくはその保全が特別の公的利益のために要請されている物の保護のため（第1号）、著しい意義を有する犯罪の予防、その他の防止、または訴追のため（第2号）、提供された側が情報を自らの権限によっても同じ方法で取得し得る場合（第3号）に、情報を提供される者が情報を必要とするということの事実に基づく手がかりが存在する場合のみ、提供することを授権する。

第3項は、駐留軍の機関（第1号）、外国の公的機関ならびに超国家機関および国家間機関（第2号）、公的でない機関（第3号）に、一定の条件の下で、ラント当局に情報の提供を授権する旨定める。

第2に、第8b条は、目的拘束について定めており、その第2項は、居住空間の監視のために技術的手段を秘密裏に投入することにより、または情報技術システムへの秘密のアクセスにより獲得された個人関連データを再処理することを、第9条第1項第1文の事項的な前提条件が存在する場合（第1号）、刑事訴訟法第100b条第2項の意味での犯罪の実行の切迫した危険があるという事実に基づく手がかりが存在する場合（第2号）、その解明のために、刑事訴訟法の対応する権能に基づいて措置が命じられ得る犯罪の訴追に当該データが役立つ限りで、犯罪の訴追を行う場合（第3号）

に限定して許容し、さらに第9条に基づく措置から得られた個人関連データで、写真または画像記録の作成によって獲得されたものについては、刑事訴追の目的のために再処理することは許されないと定める。

そして同第3項は、BayVSG第15条第2項および第3項ならびに第16条第1項に基づく措置によって獲得された個人関連データは、G10法第4条の準用によってのみ、再処理することが許されるとする。

3．異議申立人とその主張

異議申立人は、ラントの憲法擁護庁により監視され、その憲法擁護報告書においても言及されている組織の構成員であって、かつ部分的には積極的に活動を担っている者である。異議申立人は、2017年7月に提起した憲法異議（法律憲法異議）において、バイエルン憲法擁護法において規律されている様々なデータ取得権能および提供権能について、基本法第1条第1項、第3条第1項、第10条第1項、第13条第1項および第19条第4項と結び付いた第2条第1項の基本権が侵害されていると主張した（その後のバイエルン憲法擁護法の法改正に応じた主張の追加および取下げがある）。

すなわち、異議申立人によれば、侵害の閾値は、侵害が重大になればなるほどヨリ厳しい要件が据えられるべきで、特に強度の高い侵害措置に際しては、情報機関への授権と警察法上の授権の要件（侵害の閾値）は収斂する。しかしBayVSGでは、①居住空間の監視（第9条）およびオンライン監視（第10条）を実施する権能は、その目標が切迫した危険（dringende Gefahr）を阻止することに限定されていないので、違憲である。②BayVSG第12条に基づく携帯電話の位置測定は、まさにそれが長い期間続き、行動プロファイル（Bewegungsprofil）を作成され得る場合には高い強度の侵害になり得るにもかかわらず、これらは侵害の閾値が不足している。③BayVSG第19条の秘密裏に行動する人物の投入および同19a条の監視についての侵害の閾値は、極めて低い。④BayVSG第25条に基づく

提供権能も、それが諜報機関的手段によって取得されたデータに関する限り、部分的に、憲法上の要件を充たしていない。⑤BayVSG第12条、同第18条、同第19条および同第19a条に基づく措置には、独立した機関による事前の統制が欠けている等、主張した。

Ⅲ．判旨

1．憲法異議の適法性（Rn.92ff.）

連邦憲法裁判所は、基本法第93条第1項第4a号および連邦憲法裁判所法第90条第1項に基づき、公権力の行為による基本権または基本権類似の権利の侵害の可能性に関して、自らの、直接的かつ現在の制約（Betroffenheit）について判断し（Rn.103ff.）、結論として、上記の各規定に対する憲法異議を適法とし、その他の規定に対する憲法異議は不適法とした（Rn.144ff.）。

2．判断枠組み

連邦憲法裁判所は次いで、判断枠組みを以下のように述べる。

（1）合憲性の審査尺度（Rn.148ff.）

まず判決は、判断枠組みの総論として、本件で審査の中心となるのは比例原則、特にその狭義の比例性（相当性）審査であるとする（Rn.148）。判決は、基本法がたたかう民主制を採用していることから、自由で民主的な基本秩序を保護するための自由権制約を、正当な目的に奉仕するものとしたうえで（Rn.150）、争われている諸規範が、この目的を達成するために、適合的かつ必要的であるとする（Rn.151）。

（2）警察の権能に対する情報機関の権能の特殊性（Rn.153ff.）

そして判決は、憲法擁護庁を含む情報機関の監視措置に対する憲法上の要件の狭義の比例性を判断するために論を進めるが、まず、先例を引用・参照しつつ、次のように警察官庁の権能と情報機関の権能の差異とその帰結について述べる。

> 警察官庁および刑事訴追官庁の任務は、犯罪を予防し、防止し、訴追することならびに公の安全および秩序に対するその他の危険を防禦することであるが、この任務は、（措置を）実施する責任（operative Verantwortung）および個人に対して必要とあれば強制力をも伴った形で措置を貫徹する権能（「強制力のある措置に接続する権能（operative Anschlussbefugnissen）」）によって特徴付けられる。これに対して、憲法擁護庁は、具体的危険（konkrete Gefahren）の前段階（Vorfeld）で潜在的な危険のある試みを一般的に監視し予備的解明を行うものの、強制力を伴った具体的な危険防禦措置または刑事訴追措置を貫徹するという上記の警察上の強制権能を有していない点で警察官庁から区別される（Rn.154）。

この差異が、憲法擁護庁の権限発動要件を、警察官庁の権限発動要件よりも緩和することを正当化するという。

> 憲法擁護庁の監視措置は、（治安維持官庁のようには）強制措置との接続がないことからして、制約の重大性が原則として減じられており、それゆえその発動要件を修正することが正当化される（Rn.159）。具体的危険の前段階で憲法敵対的な試みを解明するというその任務の特殊性を考慮すると（Rn.162）、警察的な具体的危険という要件は、一般的な要件としては憲法擁護庁の任務の特色には対応していない（Rn.163）。憲法擁護庁の監視措置について、個別事例において、一定の、情報機関による監視が必要な行為または集団の解明を目的とすることを要件とすることは、原則として、警察上の措置に向けられた具体的危険という要件の憲法適

合的な対応物なのである（Rn.164）。

しかし、判決によれば、憲法擁護庁の上記監視の必要性については、監視措置の制約の強度に応じて、その要件が強化され得る（この点について詳細は後述）。

> 憲法擁護庁の措置であっても、その都度の制約の強度および追求される目的に照らして、制約の比例性を確保する要件に拘束することが必要となる。（憲法擁護庁の）制約の強度の高い措置は、充分な根拠に基づくものであり、充分に重要な法的利益（hinreichend gewichtige Rechtsgütern）に奉仕するものでなければならない（Rn.160, 164）。

このように判決は、警察や刑事訴追機関といった治安維持官庁と、憲法擁護庁といった情報機関の権能の差異に着目し、強制権能を有する前者についてはその活動につき具体的危険を前提すること、これに対して強制権能を有しない後者については具体的危険の前段階での活動が許容される、すなわちその活動要件に具体的危険の存在が必要とされない、という区別をひとまず行う。

（3）データ取得の狭義の比例性（Rn.174ff.）

①情報機関のデータ・情報取得の一般的要件

それでは、憲法擁護庁を含む情報機関がデータ・情報を取得するための要件は、具体的には何か。判決は次のように述べる。

> 憲法擁護官庁の措置は、第1に、憲法擁護に特殊な解明の必要性（verfassungsschutzspezifischer Aufklärungsbedarf）が充分に存在していなければ、狭義の意味において比例的とはいえない（Rn.181）。監視が必要であることおよび措置が解明のために要請されることの双方に充分な根拠が必要であるところ（Rn.182）、前者については充分な事実に基づく手がかりが存在しなければならず、後者については制約が深刻になれば

なるほど監視の必要性が高くなければならない（Rn.183）。連邦憲法擁護法第4条についての理解を諜報機関的手段による憲法擁護庁の監視措置の制約の閾値とすることには憲法上疑念はなく、その際、合法な活動を行う集団についての認識を獲得するために諜報機関的手段の投入権能を認めても、憲法上問題がない（Rn.186）。

第2に、監視措置は、個別事例において、特定の、情報機関による監視の必要な行動または集団を解明するために要請されなければならず、監視措置がその解明にいかなる意味で寄与するのかについて、充分な事実に基づく手がかり（tätsachliche Anhaltspunkte）（連邦憲法擁護法第4条参照）に依拠して根拠付けられなければならない（Rn.181f., 206ff.）。監視の必要がある試みについて、特定の集団が自由で民主的な基本秩序に敵対し得るのではないかという漠然とした疑念・推定・推測・仮説に基づいてではなく、それについて憲法擁護庁がその都度の監視の開始に際して知っていた、具体的かつ充分に濃縮された状況という形式において憲法敵対的な試みであるとの疑念を根拠付けるに適合的な事実がなければ、措置は行い得ない（Rn.188f.）。

第3に、情報機関の解明措置は、試みに間接的に関与するだけの者に対してはヨリ僅かな手段のみが許され、オンライン監視および居住空間の監視という特に侵害の度合いの高い措置は、第三者に対して直接行うことは許されない。情報技術システムへのアクセスおよび居住空間の監視は、目標人物としては、危険に責任を有する者にのみ、直接向けることが許される（Rn.209ff.）。

このように判決は、①情報機関が監視を行う要件として、個別事例において、特定の、情報機関による監視の必要性および解明の必要性がある試みが存在し、そしてその際、この解明の必要性が事実に基づく手がかりにより根拠付けられなければならないこと、②措置が間接的関与者に対するものである場合には制約はヨリ僅かなものでなければならないこと、（そ

して、後述のとおり、③重大な制約を伴う措置には、独立した機関による事前統制が必要であること〔Rn.215ff.〕）という要件を示す。

そして、形式面についても、立法者は監視の必要性の基準を、充分に確定し規範の明確性を伴ってその都度法律で規律しなければならず、憲法擁護官庁を含めて行政を統御し限界付ける尺度を定め、監視の必要性や成果の程度に比例した監視の必要性や監視措置の基準を自ら法律で定めなければならない、と判決はあわせて指摘する（Rn.199ff.）。

②措置の制約の強度に応じた要件の強化

それでは次に、判決が繰り返し留保を付している、措置の制約の強度に応じて要件が強化され得るとは、具体的にはどのような意味であろうか。

憲法擁護庁の秘密裏の監視措置は、常に特別に高度のランクの法益の保護に奉仕するところ、その監視措置に対する比例原則の厳格さは、その都度の制約の重大性により異なる（Rn.174f.）。例えば、オンライン監視や情報技術システムへの秘密裏のアクセスのように、憲法擁護庁の措置それ自体が重大な制約となり、その後の措置による制約がむしろ些細と思わせるような程度となる場合、強制権能との接続がなくとも、それが人格の最も広範囲の把握（weitestgehende Erfassung der Persönlichkeit）を許容するものであるから、警察による措置と同じ（く具体的危険という）要件が必要である（Rn.166, 168）。また、このことは、基本法13条4項からして、憲法擁護庁の聴覚的・視覚的な居住空間の監視にも妥当し（Rn.169）、それは具体的危険を超えて切迫した危険（dringende Gefahr）を防禦するためにのみ許容される（Rn.177）。

さらに、人格の特別に広範囲の把握が問題となる措置の際には、核心領域保護の要件が必要となるが、そのような措置だけでなく、典型的に私的領分に深く侵入し、それなりの蓋然性で最高度に機密性の高い状況を把握し得るその他の手段が用いられる際にも、核心保護の要件が必要となる（Rn.167）。

そして、憲法擁護庁の監視権能が、このように具体的危険の防禦のためにのみ容認されている場合、憲法擁護庁自身は強制権能は利用できないので、具体的危険が生じた場合には、その防禦のために情報を強制権能を持つ官庁に提供しなければならない。しかし、この提供がそれ自体として基本権侵害となるため（Rn.179）、このような監視措置は原則として治安維持官庁が自ら行わなければならない。治安維持官庁による監視措置が適合的でないか、時宜を逸している場合に限り、例外的に憲法擁護庁による補充的なオンライン監視または居住空間の監視が、憲法上許容され得る（Rn.180）。

最後に、居住空間の監視や長期間の監視などの制約の度合いの高い監視措置については、憲法擁護庁の措置の要件が順守されているか否かについて、原則として、例えば、裁判官の命令の形式におけるような、独立した機関による事前の統制を行う仕組みを、立法者は詳細かつ明確に法律上設けていなければならない（Rn.213ff.）。

このように、憲法擁護庁による人格の最も広範囲の把握に至り得る措置については、治安維持官庁と同じ具体的危険の存在が措置の要件となり、居住空間の監視については、具体的危険を超えて切迫した危険の存在が措置の要件となる。また、具体的危険を防禦するための憲法擁護庁の権能は、治安維持官庁による措置の補充的なものでなければならず、核心領域保護や、独立した事前統制といった更なる要件も課せられることになる。

なお、本判決は、このような制約の重大性に伴う要件の加重を、治安維持官庁に関しても前提としている。

秘密裏の監視を行うための警察官庁の権能は、背後に控える強制権能と接続し得ることから、比例原則や具体的危険の概念について厳格な要件に拘束される。すなわち、警察官庁の活動領域では、制約の強度が高い秘密裏の監視措置によって取得されたデータは、特に重要な法益（besonders gewichtige Rechtsgüter）に対する危険が個別事例において

充分に具体的に予見可能であって、かつ措置の名宛人が合理的な第三者（verständige Dritten）の目から見て客観的な状況に基づくと巻き込まれることになる場合に限り、原則として比例的である。また、具体的危険という伝統的な警察上の概念は、個別事例において客観的に予期されるべき出来事が妨げられることなく経過した際に、予見可能な時間内に、充分な蓋然性をもって、警察上の保護利益の侵害に至る事態を前提としている。あるいは、充分に具体化された危険はまた、被害に至る因果関係がなお充分な蓋然性をもって予期されていない場合には、個別事例において既に一定の事実が抜きんでて重要な法益（überragend wichtiges Rechtsgut）に差し迫った危険（drohende Gefahr）を指示する限りで、存在し得る（Rn.158）。

③小括

判示を整理しておこう。まず、警察および刑事訴追機関をはじめとする治安維持官庁は、具体的危険の存在を前提に活動し得るのに対して、憲法擁護庁を含む情報機関は、具体的危険の前段階で、個別事例において、特定の、情報機関による監視の必要性および解明の必要性がある試みが存在し、そしてその際、この解明の必要性が事実に基づく手がかりにより根拠付けられれば、活動をなし得る。ただし、措置については、試みに間接的に関与する第三者の権利制約は局限しなければならず、また法律において、監視の必要性や基準を明確に定めなければならない。

もっとも、情報機関の措置であっても、措置の制約の強度に応じて要件が強化され得る。例えば、人格の最も広範囲の把握に至り得る措置については、情報機関の措置であっても、治安維持官庁と同じ具体的危険（居住空間の監視やオンライン監視の場合はさらに、切迫した危険）の存在が措置の要件となり、その他にも、補充性、核心領域保護、独立機関の事前統制といった要件がさらに課される。

このように本判決は、情報機関の一般的な措置、情報機関の制約の度合

いの高い措置、治安維持官庁の一般的措置、治安維持官庁の制約の度合いの高い措置といった形で、措置の侵害の度合いに応じた段階的な要件設定を行ったのである。

（4）更なる利用と提供の狭義の意味における比例性（Rn.225ff.）

次に判決は、取得したデータ・情報の利用や提供について議論する。判決は、目的拘束（もともとの取得目的の枠内で更にデータを利用する）と、目的変更（もともとの取得目的と異なる目的で更にデータを利用する場合）を区別し（Rn.225）、他の官庁へのデータの提供は目的変更の下位分類であるとする（Rn.226）。

判決は、まず目的拘束について、データを取得した官庁が当該データを更に利用することは、もともとの取得目的での利用を立法者が許可している場合、その利用に正当化根拠は必要ないが（Rn.227）、居住空間の監視およびオンライン監視から得られたデータは、その利用につき取得の要件と同じく切迫した危険か具体化された危険がある場合にのみ利用可能であるとして、ここでも制約の重大性と要件の高さを連動させている（Rn.228）。

他方で、目的変更について判決は、立法者は目的変更を認めることができるとしつつ、取得したデータを他官庁に提供することにつき、高い要件を設定する。個人関連データの提供は、それ自体が独自の基本権侵害を構成するので、データ提供のための法律上の授権も、個別事例における提供措置も、比例性の要請を充たさなければならないところ（Rn.230）、狭義の比例性の判断の出発点は、これまでの判例においても議論されてきた「仮想的なデータ新規取得（hypothetische Datenneuerhebung）」の基準であるとする。

> 憲法擁護庁の監視措置から得られた情報は、強制権能を有する他の官庁に容易に提供されてはならない（「情報分離原則（informationelles Trennungsprinzip）」）。憲法擁護庁が秘密裏の監視措置によって得た情報

を提供することが許されるのは、仮に、当該情報を提供される側の官庁において、当該情報を提供される側の官庁が自ら当該情報を取得するとした場合に、その取得のための要件を充たしている場合に限られる（「仮想的なデータ新規取得」の基準）（Rn.170）。

この仮想的なデータ新規取得の基準は、情報機関によるデータの提供にも妥当するところ（Rn.232）、いかなる官庁にデータが提供されるかにより、提供の要件が変わる。重要なのは、憲法擁護官庁による治安維持官庁への提供に対する提供の閾値としては、少なくとも一般的に具体的危険が存在しなければならず（Rn.245）、居住空間の監視に関しては、切迫した危険（基本法第13条第4項参照）が存在しなければならない、ということである（Rn.248）。

このような要件を設けない限り、憲法擁護庁が強制権能と接続していないという事情が無意味になってしまい、提供先（提供される側）官庁が、憲法擁護庁から得た情報を用いて、強制権能を行使し得ることになるからである（Rn.171）。

それでは、情報機関から治安維持官庁へのデータ提供の具体的な要件とは何か。判決は次のように敷衍し、特に高い価値を有する法益の保護のためにのみ、許容されるという。

情報機関が、警察または刑事訴追官庁のような強制権能を有する官庁にデータを提供する場合、そうでない場合と比してヨリ厳格な要件が提供につき妥当し（Rn.234f.）、提供するためには、抜きん出た（herausragend）公的利益が存在しなければならず、特に高い価値を有する法益（besonders hochwertige Rechtsgüter）の保護のためにのみ認められる（Rn.236f.）。そして、「特に高い価値を有する法益」とは、人間の生命、身体および自由ならびに連邦またはラントの存立または安全、そしてその保全が公的利益のために要請される、重要な価値を有する物の保護である（Rn.243）。

それ自体は侵害の度合いがヨリ僅かな監視措置から得た情報であっても、特に高い価値を有する法益のためにのみ、提供することが許される（Rn.238）。情報機関は、具体的危険の前段階で広く取得した豊富なデータから自らの認識を得て、そこから重要な情報を獲得しまた転送するために、相互にかつ他の機関の認識と結び付け、自らの認識を濾過するのであって（Rn.239）、データを取得する広範な権能を有している。それゆえ侵害の重大性が僅かな措置であれば、憲法擁護庁は、憲法擁護に特殊な監視の必要性が単に存在するだけで、措置が許容され得る（Rn.240）。警察官庁に対してこのような権能を認めることは許されないし、憲法擁護庁による幅広いデータの取得、評価、解明を行うための権能も、憲法擁護が奉仕する特別に高い法益に限って、憲法上正当化され得る（Rn.241）。

情報機関によって最初に取得されたデータの提供について、治安維持官庁による最初の取得と同じ要件を課さないとすれば、強制権能を有する官庁が、取得の要件が低い官庁を通じて自らが取得できない情報を提供させることができ、「裏をかく」ことに至るので、許されない（Rn.248）。

刑事訴追のための提供についての規律に対する憲法上の要件も、同じく仮想的なデータの新規取得の基準によるとされ（Rn.249）、特に重大な犯罪の訴追のためにのみ、提供が許容されるという。

著しい犯罪（erheblicher Straftat）、重大な犯罪（schwerer Straftat）、特に重大な犯罪（besonders schweren Straftaten）という犯罪の重大性の区分でいえば、憲法擁護庁が取得したデータの提供は、抜きんでた公的利益の保護のためにのみなされ、そしてそれゆえ特に重大な犯罪の訴追のためにのみ考慮される（Rn.251）。情報機関により最初に取得されたデータを刑事訴追のために提供するための閾値として立法者が要求しなければならないのは、一定の、嫌疑を根拠付ける事実が存在すること、すなわち、その点について具体的かつ或る程度の範囲で濃密化された状

況が嫌疑に対する事実の根拠（Tatsachenbasis）として存在しなければならないということである（Rn.252）。

さらに、情報機関によって取得されたデータをその他の機関に提供する場合も、それが一般データ保護法上の目的拘束原則のあらわれであるがゆえに、仮想的なデータの新規取得の基準が妥当し、提供は特に重要な法益に奉仕しなければならない（Rn.254, 255ff.）。ただし、提供の閾値は、秩序維持または刑事訴追目的での提供のように提供される側の官庁が強制的権限を有する場合と異なり、その侵害の重大性によっては、低下し得るという（Rn.254, 257ff.）。

最後に、情報機関が取得したデータを外国の官庁に提供する場合も、原則として仮想的なデータの新規取得の基準に従い、憲法擁護官庁による外国への情報を提供は抜きんでた公的利益の保護のために、具体的な危険が存在する場合にのみ許容される（Rn.261）。さらに、この提供は、提供される側の国家において、データ保護法上適切かつ基本的な人権の保障と両立し得る形で提供されたデータを取り扱うこと、そしてドイツ国家の側でこの点について適切に確認することを、前提とすると判決は述べる（Rn.264ff.）。

（5）規範の明確性（Normenklarheit）および確定性（Bestimmtheit）（Rn.272ff.）

判決は、情報機関の措置、特に秘密裏の監視措置のための法律上の授権を行う規範は、充分に明確であり確定（特定）されなければならないとする。

統御し限界付ける行為尺度を政府および行政が法律において見出すことそして裁判所が効果的な法的統制を行い得ること（確定性）、規律の内容が理解できること、特に規律によって市民が負担となる措置に備え得ること（明確性）が重要となるところ、見通しのきかない参照の連続は、

基本権の要請と両立し得ない（Rn.272）。原則として、秘密裏のデータ取得および処理を行うための授権の確定性および規範明確性に対しては、とりわけ厳格な要件が据えられなければならない（Rn.273）。憲法擁護庁を含む情報機関にも上記のことは例外なく妥当する（Rn.274）。

（6）核心領域保護（Rn.275ff.）

判決はさらに、基本権制約の度合いの高い監視措置については、治安維持官庁による措置であれ情報機関による措置であれ、私的な生活形成の核心領域を保護するための特別な要件が生ずるという（Rn.275）。

この核心領域の保護は、比例原則に基づく衡量によって相対化することが許されず、データの取得ならびにデータの評価および利用の2つのレヴェルで顧慮される。前者につき、核心領域に属する情報をも故意によらずに把握してしまうことを可能な限り排除する予防措置がなされなければならず、後者につき、にもかかわらず避けられない私的な生活形成の核心領域への侵入の効果を厳格に最小限化しなければならない（Rn.277）。

まず、特に深く私的領分に侵入し得る居住空間の監視については、核心領域保護の要請は具体的には次の通りとなる。

まず取得に関して、私的空間において特別に人格的な信頼関係がある人となされた会話は私的な生活領域の核心領域にあり、監視することは許されない、という推定が妥当する。それに対応して、そのような会話が想定されるべき空間については、自動的に行われる長期的監視も排除される。特定の会話について、それが直接的に犯罪に関連していること―これはまた、その会話が高度に人格的な内容を伴ってなされている場合も存在する―を示しているか、あるいはその会話におよそ高度に内密な性格が欠けているということの具体的な根拠が存在する限りでは、この推定は反証され得る（Rn.280）。この推定ルールによれば、私的な生活形

成の核心領域に監視措置が侵入する蓋然性が存在する場合、会話が直接的に犯罪に関連するかおよそ高度に内密な性格を欠いているときを除き、この措置は断念されなければならない（Rn.281）。他方、評価・利用に関して、監視の成果について独立した立場からの精査がなされなければならない（Rn.282）。

評価のレヴェルでは、核心領域の保護に資する精査に際して、官庁自身による（更なる）把握がされるという事態が、許されない（Rn.283）。

他方で、情報技術システムへの秘密アクセスは、同じく、核心領域のための特別な予防措置が必要であるが、取得されたデータから高度に内密なデータの選別が問題となるので、評価および利用の段階に焦点が当たり、その限りで取得のレヴェルでは要件が若干低下する（Rn.284f.）。核心領域に関係するデータが、データ取得の前またはデータ取得に際して分離され得ない場合には、情報技術システムへのアクセスも許容されるが、この場合に決定的な重要なのが、核心領域に関連する情報を官庁によるその把握と利用の前にフィルタリングする、独立した機関による精査である（Rn.286）。

（7）監視措置の協働作用（Rn.287f.）

判決は、さまざまな監視措置の協働作用について、現代的、とりわけ関係者に秘密でなされる捜査手法の投入は「加算的（additiv）」[12]な基本権侵害に内在する危険の潜在的可能性をも考慮しなければならないとする。憲法擁護庁の権能について判決は、個別事例でのさまざまな監視措置の投入について比例原則での審査を行う際に、措置の付加的効果による侵害を顧慮しなければならないとする（Rn.287f.）。

12　基本権侵害の「加算」につき、小山剛「監視と委縮」憲法研究6号（2020）111頁以下を参照。

（8）手続的要件（Rn.289f.）

以上のような実体的統制に加えて、憲法擁護庁に対しては、狭義の意味における比例原則から、既に述べた独立した事前の統制に加えて、監視権能の内容形成に対する手続的要件も生ずる。すなわち、通知義務（Benachrichtigungspflicht）および情報閲覧請求権（Auskunftsrecht）ならびに報告義務（Berichtspflicht）が原則として規律されなければならず、秘密裏の監視措置については、それを効果的に監督統制する機関を設けなければならない（Rn.289f.）。

〔附記〕本研究は、JSPS科研費21K13187の助成を受けたものです。