「反恐資料庫」判決

德國聯邦憲法法院第一庭2013年4月24日判決
－1 BvR 1215/07－

謝碩駿　譯

要目

關鍵詞

反恐資料庫(Antiterrordatei)
反恐資料庫法(Antiterrordateigesetz)
資訊區分原則(informationelles Trennungsprinzip)
資訊自主決定權(Recht auf informationelle Selbstbestimmung)
資訊交換(Informationsaustausch)
目的拘束原則(Grundsatz der Zweckbindung)

裁判要旨

1.反恐資料庫作為各不同安全機關為打擊國際恐怖主義而共用之聯合資料庫，因其本質侷限在獲取資訊之前哨站，且明定僅在重大急迫之例外情形下，始可基於有效履行任務之目的而利用該資料，故就其基本架構而言，建置此等資料庫，並未牴觸憲法。

2.使警察機關及情報機關得以進行資訊交換之規定，因資訊自主決定基本權之緣故，應受憲法較高程度要求之拘束。由基本權可以導出資訊區分原則，此一原則對於上開之資訊交換，僅在例外情況下始允許之。

3.諸如反恐資料庫等在各安全機關之間共用的聯合資料庫，鑑於被蒐集資料及其被使用之可能性，必須以充分明確且合乎過度禁止原則之法律規定妥為設計安排。反恐資料庫法並未完全合乎此一要求，詳言之，關於參與機關、被列為與恐怖主義關係密切之人的範圍、聯繫者之併納、對以隱密方式備妥之延伸基本資料之使用、關於安全機關對應儲存資料的具體職權，以及確保有效監督等規定，反恐資料庫法均未達到上開要求。

4.藉由干預書信與通訊秘密及住宅不受侵犯權而獲致之資料，當其不設限地被納入反恐資料庫，即對基本法第10條第1項及第13條第1項造成侵害。

案　由

本案係S先生委託訴訟代理人Maximilian Suermann律師（地址：Brauschweiger Straße 57，12055 Berlin），針對2006年12月22日制定之「聯邦與各邦警察機關及情報機關標準化中央反恐資料庫建置法」（Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern，簡稱「反恐資料庫法」，Antiterrordateigesetz - ATDG）（BGBl I S. 3409）而提起之憲法訴願。聯邦憲法法院第一庭在Kirchhof副院長、Gaier法官、Eichberger法官、Schluckebier法官、Masing法官、Paulus法官、Baer法官、Britz法官的參與下，基於2012年11月6日進行之言詞審理程序，作成本判決。

裁判主文

1.a)2006年12月22日制定之聯邦與各邦警察機關及情報機關標準化中央反恐資料庫建置法（簡稱反恐資料庫法）（Bundesgesetzblatt I Seite 3409）第1條第2項及第2條第1句第3款之規定，牴觸基本法第2條第1項結合第

1條第1項。

b)反恐資料庫法第2條第1句第1款b部分關於支助性組織之支助，以及第2條第1句第2款關於「支持」（Befürworten）之規定，均牴觸基本法第2條第1項結合第1條第1項。

c)反恐資料庫法第5條第1項第2句第1a款，當其規定，在檢索延伸基本資料而出現吻合情況，即得讀取反恐資料庫法第3條第1項第1a款規定之資訊時，牴觸基本法第2條第1項結合第1條第1項。

d)反恐資料庫法第3條第1項第1句第1b款及第10條第1項，因欠缺判決理由要求之補充規定，故在此一範圍內，牴觸基本法第2條第1項結合第1條第1項。

e)除此之外，反恐資料庫法第2條第1句第2款及第10條第1項之規定，應依判決理由之準據作合憲性解釋。

2.反恐資料庫法第2條第1句第1款至第3款、第3條第1項第1款、第5條第1項與第2項及第6條第1項與第2項之規定，因其擴及非依反恐資料庫法第4條隱密儲存且係經由干預電信秘密與住宅不受侵犯基本權所獲致之資料，故在此一範圍內，牴觸基本法第10條第1項及第13條第1項。

3.直至新規定制定前，至遲至2014年12月31日，系爭被宣告牴觸基本法之條文，依以下之指示而繼續適用：除有反恐資料庫法第5條第2項規定之緊急事件外，僅得在如下情況始可利用反恐資料庫，亦即聯繫者（反恐資料庫法第3條第1項第3款）之資料以及藉由干預電信秘密與住宅不受侵犯基本權而獲致之資料不會遭到讀取，且必須確保在檢索延伸基本資料時，若出現吻合情形，僅揭露反恐資料庫法第3條第1項第3款規定之資料；一旦聯繫者之資料以及藉由干預電信秘密與住宅不受侵犯基本權而獲致之資料依此不得被讀取，則此等資料即不得再依反恐資料庫法第5條第2項於緊急事件中利用資料庫之規定而利用之。

4.本件憲法訴願之其他部分，予以駁回。

5.德意志聯邦共和國應償付憲法訴願人因本件憲法訴願程序而支出之必要費用。

理　由

A.事實及爭點

本件憲法訴願之標的為反恐資料庫法之合憲性。

I.事實及系爭規定

憲法訴願人所不服者，乃2006年12月22日制定之聯邦與各邦警察機關及情報機關標準化中央反恐資料庫建置法（簡稱反恐資料庫法），該法係聯邦與各邦警察機關及情報機關共同資料庫建置法（Gesetz zur Errichtung

gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder，簡稱共同資料庫法，Gemeinsame-Dateien-Gesetz）（BGBl I S. 3409）之第1條。反恐資料庫法自2006年12月31日生效以來，尚未進行實質修正。經對本件憲法訴願之提起進行適切理解，可知憲法訴願人係直接針對反恐資料庫法第1條至第6條關於資料儲存及使用之規定表示不服；因此，反恐資料庫法第2條第1句第4款之規定，不在憲法訴願之範圍內。本件憲法訴願之提起，亦間接針對與前揭規定相關之反恐資料庫法第8條至第12條，尤其是涉及個人資料保護法上之責任及審查等規定。

1.透過反恐資料庫法之制定，反恐資料庫，一個供聯邦與各邦警察機關及情報機關打擊國際恐怖主義而建置之聯合資料庫，取得其法律上之依據。該資料庫使參與之警察機關與情報機關間的資訊交換更為容易與迅速，藉此機制，原由個別機關基於打擊國際恐怖主義而獲致與支配使用之特定情報，得被一切參與機關更迅速地發現，且更容易被接近取用。

a)反恐資料庫法第1條首先規定，反恐資料庫作為共用之標準化中央資料庫，設置於聯邦刑事局（Bundeskriminalamt），同時亦規定反恐資料庫之參與機關。依反恐資料庫法第1條第1項之規定，反恐資料庫之參與機關計有：聯邦刑事局、聯邦警察總局（Bundespolizeipräsidium）（反恐資料庫法第1條第1項結合聯邦警察法第58條第1項及聯邦警察機關管轄權命令第1條第3項第1d款）、各邦刑事局（Landeskriminalämter）、聯邦及各邦之憲法保護機關（Verfassungsschutzbehörden des Bundes und der Länder）、軍事情報局（Militärische Abschirmdienst）、聯邦情報局（Bundesnachrichtendienst）以及海關刑事局（Zollkriminalamt）。除上開法定之參與機關外，其他警察執行機關得根據反恐資料庫法第1條第2項結合第12條第2款之規定，在符合一定要件下，成為反恐資料庫之參與機關。依立法理由，此等參與機關，主要係指各邦警察之國家保護機構（BTDrucks 16/2950, S. 14）。依據2010年6月4日之建置命令（Errichtungsanordnung），迄今已有三個邦的警察機構（其位階在邦刑事局的層級以下），對反恐資料庫進行讀取。

b)反恐資料庫法第2條規定，機關對於與何人或何等對象有關之資料，在蒐集後應儲存於反恐資料庫。儲存之要件首先為，事實上顯示警察機關或情報機關掌有之情報，涉及反恐資料庫法第2條第1句第1款至第4款所列之人或對象，且知悉該資料對於調

查或打擊與德意志聯邦共和國相關之國際恐怖主義，具有必要性。依第1款之規定，得被儲存之資料，首先係國際恐怖組織或團體之成員或與其關係特別密切之人。再者，依第2款之規定，個別人士若實施、支助、預備、支持或故意以行為引致非法暴力，而以之作為達到國際取向之政治或宗教利益的工具，則該個別人士之資料亦得被儲存。最後，與第1款及第2款所列之人聯繫者，若其聯繫並非僅屬短暫或偶然型態，且藉由蒐集該聯繫者之資料而得以使調查或打擊國際恐怖主義獲致相關線索，則依第3款之規定，該聯繫者之資料亦成為得被儲存之對象。

c)關於反恐資料庫法第2條第1句第1款至第4款所列之人士與對象之資料，何者應予儲存，規定於反恐資料庫法第3條第1項。該規定將應蒐集之資料，區分成反恐資料庫法第3條第1項第1a款之「基本資料」（Grunddaten）（以下為便於說明起見，亦稱以普通基本資料），以及反恐資料庫法第3條第1項第1b款之「延伸基本資料」（erweiterte Grunddaten）。

一切在反恐資料庫法第2條第1句第1款至第3款所列之人士，其普通基本資料，均應予以儲存。條文又將基本資料本身區分成數種不同與人有關之一般資訊，諸如住址、特殊之身體特徵、語言、方言、證件照片、以及其在反恐資料庫法第2條所列群組之屬性。相較之下，反恐資料庫法第3條第1項第1b款要求，延伸基本資料之儲存對象，僅係反恐資料庫法第2條第1句第1款及第2款所列之人士，以及有事實依據，其對恐怖主義相關活動有所知悉之聯繫者。在反恐資料庫法第3條第1項第1b款的aa至rr細項中，對於延伸基本資料有個別之列舉規定。舉其大要者，例如電信連線及電信終端設備之資訊（aa）、銀行帳號資訊（bb）、族別資訊（gg）、宗教信仰資訊（hh）、與恐怖主義關係重大之能力（ii）、教育背景資訊（jj）、在重要基本設施機構之活動資訊（kk）、暴力傾向之資訊（ll），或為與恐怖主義嫌疑人聚首而造訪之地點或地域之資訊（nn）。

根據立法理由之說明，資料只要依其類型係可能者，應當採取標準化之方式予以儲存。質言之，資料儲存於資料庫時，並非以信手拈來之方式為之，而是透過系統預先設定之指示，擇定資料應如何排列放置於資料庫中。採取此種標準化作法之目的，乃在確保資料庫之檢索能力，並有助於行政管理實務之統一性（BTDrucks 16/2950, S. 17）。在反恐資料庫法第3條第1項第1b款的rr規定下，各參與機關已儲存之特別評註、補充性指示與評價，得被當成自由文字（Freitext）而輸入電腦檢索，這讓原

本未以標準化方式儲存之資料，得進行後續之標準化。

除了基本資料以及延伸基本資料之規定外，反恐資料庫法第3條第1項第3款尚設有儲存輸入資料機關之資訊及其檔案編號之規定，俾利各機關聯繫，以進行進一步之資訊交換。

依反恐資料庫法第4條之規定，在有特別保密之利益或當事人具有特別值得保護之利益時，得對資料採取有限式或隱密式儲存。在採取隱密式儲存時，資料以如下之方式輸入：其他參與機關在查詢時，無從知悉該筆資料之存在，且無法直接讀取已儲存之資料。但其他參與機關之查詢紀錄，將自動傳送至輸入資料機關，從而輸入資料機關得根據法律條文之規定，自行決定是否與查詢機關進行聯繫，以及進行資料之傳輸。此種規定，主要係為保護各該調查機關之資料來源，尤其是當情報機關與外國情報機關共同合作時，對其提供資料來源保護。在立法過程中，當事人之利益則被當成另一獨立之目的而增列於條文中（vgl. BTDrucks 16/3642, S. 6）。

d)反恐資料庫法第5條第1項規定，如何在一般情況下讀取已儲存之資料。依反恐資料庫法第5條第1項第1句之規定，在參與機關打擊或調查國際恐怖主義的任務範圍內，必要時，參與機關得以自動化之程序查詢資料。透過此種不限於依特定姓名而為搜尋之讀取權能，查詢機關得在一切公開及隱密儲存之資料組中，對基本資料與延伸基本資料進行包括自由文字欄位（Freitextfeld）在內之檢索。當查詢機關對人進行查詢，若出現吻合者，查詢機關即得對該基本資料以及輸入資料機關之資訊進行讀取。依反恐資料庫法第5條第1項第3句及第4句之規定，查詢時出現吻合者，僅在輸入資料機關依各該現行傳輸規定對個別之請求案件予以同意時，查詢機關始得讀取延伸基本資料。至於在檢索延伸基本資料時，若出現吻合者，則相符之普通基本資料，不受上開規定之限制，亦得直接傳輸而被查詢機關讀取。

根據反恐資料庫法第6條第1項第1句之規定，查詢機關對於依反恐資料庫法第5條第1項讀取之資料，僅得基於「查驗吻合者是否即為被查詢之人」或「為個別傳輸之請求預作準備與說明理由」之目的，始得使用依反恐資料庫法第5條第1項讀取之資料。

e)依反恐資料庫法第5條第2項第1句之規定，查詢機關得在緊急事件中，直接讀取吻合者之延伸基本資料。此一規定所稱緊急事件之要件為：為防止人的身體、生命、健康發生現時危害，或為防止具重大價值且基於公共利益應予保存之物發生現時危害，有絕對之必要須讀取延伸基本資料，且無法於請求後為及時之資料傳輸

。個案是否該當緊急事件之要件，由查詢機關之首長或首長委任之高階職務公務員決定之。此外，此種讀取應取得輸入資料機關之事後同意；同時，輸入資料機關亦決定得否對該資料為進一步之使用。

當查詢機關在緊急事件中已讀取資料，依反恐資料庫法第6條第2項之規定，僅在與打擊國際恐怖主義具有關聯性，而為防止現時危害有絕對之必要時，始得使用該資料。當聯邦刑事局或各邦刑事局基於請求或在聯邦檢察總長（Generalbundesanwalt）的委託下使用反恐資料庫，依據反恐資料庫法第6條第4項第1句及第2句之規定，得為刑事追訴之目的，而將資料傳輸給聯邦檢察總長；聯邦檢察總長依反恐資料庫法第6條第1項第1句之規定，得使用資料，將資料提供給基於調查或打擊國際恐怖主義之目的，而請求傳輸情報之機關。

反恐資料庫法第7條規定，因應反恐資料庫法第6條第1項第1句所為之請求而傳輸情報，須依各該現行傳輸規定為之。

f)反恐資料庫法第8條對輸入資料機關以及查詢資料機關在個人資料保護法上的責任進行分配。因允許查詢而生之責任，由查詢機關負之；因資料蒐集、資料允許輸入以及資料正確性與現時性而生之責任，由輸入資料機關負之。反恐資料庫法第9條規定，任何基於資料保護審查之目的而讀取資料，均應作成紀錄。依反恐資料庫法第10條之規定，資料保護之審查，由聯邦個人資料保護官以及—依邦法之規定—各邦個人資料保護官為之。

反恐資料庫法第10條第2項規定，對當事人進行訊息告知。此一規定區分公開儲存之資料以及隱密儲存之資料。依反恐資料庫法第10條第2項第1句，關於公開儲存之資料，由聯邦刑事局根據聯邦個人資料保護法（BDSG）第19條之規定，於取得各該個人資料保護責任機關之同意後，對當事人進行告知。相較之下，依反恐資料庫法第10條第2項第2句之規定，關於隱密儲存之資料，其告知則依輸入資料機關之規定辦理。這意味著，當事人知悉被隱密儲存之資料，並非統一由聯邦刑事局告知，而係由各該資料之隱密儲存機關告知當事人。

最後，反恐資料庫法第11條規定資料之更正、刪除以及封鎖等事項；反恐資料庫法第12條則規定，聯邦刑事局應在取得聯邦內政部、聯邦總理府、聯邦國防部、聯邦財政部以及對各參與機關有管轄權之各邦最高機關的同意後，於建置命令中確定何等細節性事項。應在建置命令中確定者，包括反恐資料庫法第1條第2項所稱其他參與之警察執行機關之範圍、依反恐資料庫法第3條第1項儲存之資料之

類型，以及參與機關有權讀取資料之組織單位。

g)依共同資料庫法第5條第2項前半句之規定，反恐資料庫法係限時法，至2017年12月30日失其效力。依共同資料庫法第5條第2項後半句之規定，反恐資料庫法在生效5年之後，應評估其施行成效。

2.2006年12月22日的反恐資料庫法（BGBl I S. 3409），曾透過2008年2月26日的法律（BGBl I S. 215）進行修正，現行條文－與本案相關者－規定如下：

第1條　反恐資料庫

(1)聯邦刑事局、依聯邦警察法第58條第1項訂定之法規命令所規定之聯邦警察機關、各邦刑事局、聯邦與各邦之憲法保護機關、軍事情報局、聯邦情報局，以及海關情報局（參與機關），為履行其「調查或打擊與德意志聯邦共和國相關之國際恐怖主義」法定任務，在聯邦刑事局設置共同使用之標準化中央反恐資料庫（反恐資料庫）。

(2)其他警察執行機關，符合以下情形，經會商聯邦內政部同意，亦有權成為參與機關，參加反恐資料庫之運作：

1.該機關負有「打擊與德意志聯邦共和國相關之國際恐怖主義」之任務，且該任務並非僅是個案性質之特別指派。

2.為履行第1款之任務，該機關有必要讀取反恐資料庫，且經考量當事人值得保護之利益與參與機關之安全利益後，該機關讀取反恐資料庫具有適當性。

第2條　反恐資料庫之內容與儲存義務

當參與機關依據對其適用之法規，掌有警察機關或情報機關之情報，而從該情報可以得知，參與機關已蒐集之資料涉及下列對象，則參與機關即應依第3條第1項之規定，將該資料儲存在反恐資料庫中：

1.符合以下要件之人士

a)加入或支助「刑法第129a條所定並具國際關聯性之恐怖組織，或刑法第129a條結合第129b條第1項第1句所定與德意志聯邦共和國具關聯性之恐怖組織」者。

b)加入或支助「對上述a部分之組織予以支助之團體」者。

2.使用非法暴力，作為「貫徹國際取向之政治或宗教利益」之工具者，或對此種暴力之使用予以支助、預備、支持或故意透過行為引致者。

3.有事實依據證明，與第1a款或第2款所稱之人士並非僅短暫或偶然聯繫，且可期待透過其而獲致關於調查或打擊國際恐怖主義之進一步線索者（聯繫者），或

4.（…略）

以及，知悉該資料對於調查或打

擊與德意志聯邦共和國有關之國際恐怖主義，具有必要性。第1句之規定，僅適用於「參與機關依對其適用之法規得自動化處理」之資料。

第3條　應儲存資料之種類

(1)下列資料，只要存在，即應儲存於反恐資料庫中：

1.下列人士之資料

a)第2條第1句第1款至第3款規定之人士：姓氏、名字、舊名、別名、化名履歷、姓名之不同拼寫方式、性別、生日、出生地、出生國、現今及過去之國籍、現在及過去之住址、特殊之身體特徵、語言、方言、證件照片、與第2條所稱組織團體之關係，以及在其他法律無相反之規定，且對人之識別有必要時，身分識別證件之資訊（基本資料）。

b)第2條第1句第1款及第2款規定之人士，以及有事實依據，其對於計畫或實施第2條第1句第1a款所稱之犯罪行為有所知悉，或對於使用、支助、預備第2條第1句第2款所稱之非法暴力有所知悉之聯繫者，其下列之其他資料類型（延伸基本資料）：

aa)自己所有或由其使用之電信連線及電信終端設備。

bb)電子郵件信箱地址。

cc)銀行帳號。

dd)保險箱。

ee)登記於其名下或由其使用之交通工具。

ff)家庭狀態。

gg)族別。

hh)在個案中為調查或打擊國際恐怖主義而有必要時，關於宗教信仰之資訊。

ii)依參與機關根據特定事實所獲致之情報，對於預備及實施刑法第129a條第1項及第2項之恐怖犯罪行為有所助益之特殊技能，尤其是製造或處理爆裂物或武器之知識與技巧。

jj)中學學歷之資訊、職業資格教育之資訊，以及從事職業之資訊。

kk)有關現在與過去於安全審查法（Sicherheitsüberprüfungsgesetz）第1條第5項所稱之重要生活設施內，或於交通、民生物資供應設備或設施內、公共交通工具內或官方建築內所為活動之資訊。

ll)與人的危險性有關之資訊，尤其是持有武器或暴力傾向之資訊。

mm)車輛或飛行器駕駛執照。

nn)曾與第2條第1句第1款及第2款所稱之人士會面時造訪之地點及地域。

oo)依第2條第1句第3款之規定，與第2條第1句第1a款或第2款所稱之人士有接觸之聯繫者。

pp)第2條第1句第1a或b款規定之具體組織或團體之名稱。

qq)構成情報儲存原因之最終事件發生日。

rr)已儲存於參與機關資料庫，以

事實依據而作成之總結性特殊評語、補充性指示，以及對基本資料與延伸基本資料之評價，當其在個案中依合義務性之裁量被認為實屬必要，且對調查或打擊國際恐怖主義係必不可少者。

2.（…略）

3.第1款及第2款各該情報資料持有機關之資訊，以及該資料之檔案編號或其他業務文件存查編號，以及各該資料作為機密文件尚存之機密等級。

(2)倘依據其他法規之規定，應予儲存之資料應標記者，於資料儲存在反恐資料庫時，亦應維持該標記。

第4條　有限儲存及隱密儲存

(1)於特別保密利益或當事人特別值得保護之利益的例外要求下，參與機關對於第3條第1項第1b款規定之延伸基本資料，得全部或一部不予儲存（有限儲存），或對於第2條規定人士之資料、組織、團體、財團、企業、物、銀行帳號、住址、電信連線、電信終端設備、網頁或電子郵件信箱地址，得以其他參與機關在查詢時，無從知悉該資料之儲存，且無法對該儲存之資料進行讀取之方式輸入（隱密儲存）。是否採取有限儲存及隱密儲存，由各該機關首長或首長委任之高階職務公務員決定之。

(2)當被查詢之資料係以隱密方式儲存，輸入資料機關即藉由查詢資料之傳輸而自動得知該查詢，並應立即與查詢機關聯繫，以釐清是否得依第7條之規定傳輸情報。輸入資料機關僅在保密利益依個案情況亦屬重大時，始得不與查詢機關聯繫。依第2句所為之決定，應於文件中敘明其重要理由。已傳輸之查詢資料以及第3句規定之文件，應至遲於隱密儲存資料須刪除時，予以刪除或銷毀。

第5條　資料之讀取

(1)參與機關於履行各該調查與打擊國際恐怖主義之任務有必要時，得以自動化之程序使用儲存於反恐資料庫之資料。在出現吻合者時，查詢機關得：

1.

a)若查詢對象為人，讀取與該人士相關之已儲存基本資料，或

b)若查詢對象為第2條第1句第4款規定之組織、團體、財團、企業、物、銀行帳號、住址、電信連線、電信終端設備、網頁或電子郵件信箱地址，讀取該已儲存之資料，以及

2.讀取第3條第1項第3款之資料。

查詢機關於輸入資料機關在個案中應其請求而給予同意時，得在出現吻合者之情況下，讀取與人相關之已儲存延伸基本資料。輸入資料機關是否作成同意請求之決定，依現行各該傳輸規定。

(2)基於一定之事實，為防止個

人身體、生命、健康發生現時危害，或為防止具重大價值且基於公共利益應予保存之物發生現時危害，讀取延伸基本資料乃絕對必要，且無法及時應請求而同意為資料傳輸時（緊急事件），查詢機關得在出現吻合者之情況下，直接讀取延伸基本資料。是否發生緊急事件，由查詢機關之首長或首長委任之高階職務公務員決定之。此一決定及其理由，應清楚敘明於文件中。資料之讀取應在依照第3句所為之決定指示下記錄之。讀取後，查詢機關應立即請求輸入資料機關為事後同意。若輸入資料機關拒絕事後同意，查詢機關即不得繼續使用該資料。查詢機關應立即將資料刪除，或依第11條第3項之規定封鎖該資料。當資料已傳輸給第三人，查詢機關應立即指示該第三人不得繼續使用該資料。

(3)在參與機關內，僅被專屬授權者始得讀取反恐資料庫。

(4)查詢機關在為任何查詢時，查詢之目的與急迫性應敘明記載於文件中且應具備可辨識性。

第6條　資料之進一步使用

(1)查詢機關對於已讀取之資料，僅得為審查吻合者是否即為被查詢之人士或第2條第1句第4款所列之資訊，以及為履行其各該調查或打擊國際恐怖主義之任務，因應請求而傳輸情報，始可使用之。將資料供作其他目的使用，僅在下列情形，始得被認為係為履行其各該調查或打擊國際恐怖主義之任務，而受允許：

1.為追訴特別重大之犯罪，或為防止個人身體、生命、健康及自由遭受危害，具有必要性，以及

2.輸入資料機關同意使用時。

(2)在緊急事件中，查詢機關僅於與打擊國際恐怖主義具有關聯性，而為防止第5條第2項第1句之現時危害不可或缺時，始得使用已讀取之資料。

(3)依第1項第1句或第2項使用資料時，應標記該資料。資料經傳輸後，接收資料者應維持該標記；依第3條第2項所為之標記，亦同。

(4)當聯邦刑事局或各邦刑事局因應請求，或在聯邦檢察總長的委託下，使用反恐資料庫時，得為刑事追訴之目的，將已讀取之資料傳輸給聯邦檢察總長；聯邦檢察總長因應依第1項第1句所為之請求，得使用該資料。刑事訴訟法第487條第3項準用之。

第7條　情報之傳輸

各參與機關間因應他機關依第6條第1項第1句之請求，而為情報傳輸，依各該現行傳輸規定辦理。

第8條　個人資料保護法之責任

(1)輸入資料機關對儲存於反恐資料庫之資料，負有個人資料保護法上之責任，尤其是對資料蒐集之合法性、對資料輸入之容許性以及對資料

正確性與現時性之責任。輸入資料機關必須可得被辨識。查詢之提出是否合法之責任，由查詢機關負之。

(2)僅有輸入資料機關始得對資料進行修改、更正、封鎖或刪除。

(3)若任何機關認為其他機關輸入之資料不正確，應立即通知輸入資料機關，輸入資料機關應立即審查此項通知，並於必要時即刻更正該資料。

第9條　紀錄、技術性及組織性之措施

(1)聯邦刑事局對於任何基於以審查為目的而為之資料讀取，應記錄讀取之時間、能確認已讀取資料列（Datensätze）之資訊、對資料讀取應負責之機關，以及第5條第4項規定之讀取目的。紀錄之資料，僅在知悉該資料對於資料審查、資料保全、確保資料處理設備正常運行，或對機密文件提出閱覽證明之目的有必要時，始得予以使用。專為第1句之目的而儲存之紀錄資料，應在18個月後予以刪除。

(2)聯邦刑事局應採取聯邦個人資料保護法第9條規定之必要技術性及組織性措施。

第10條　個人資料保護法之審查與告知當事人

(1)聯邦個人資料保護暨資訊自由官（Bundesbeauftragte für den datenschutz und die Informations-freiheit）依聯邦個人資料保護法第24條第1項之規定，審查個人資料保護之實施。各邦機關對資料輸入及查詢進行個人資料保護法之審查，悉依各邦個人資料保護法之規定為之。

(2)關於非隱密儲存之資料，由聯邦刑事局取得依第8條第1項第1句負有個人資料保護法之責任且依現行法規範對告知之容許性進行審查的機關同意後，依聯邦個人資料保護法第19條之規定告知當事人。關於隱密儲存資料之告知，依輸入資料機關應適用之法規範為之。

第11條　資料之更正、刪除與封鎖

(1)錯誤之資料，應予更正。

(2)個人資料，當其不得被儲存，或知悉該資料對於調查或打擊國際恐怖主義已不再必要時，即應刪除。個人資料至遲應於與該資料相關之情報顯示，依參與機關應適用之各該現行法規範，該資料應予刪除時，予以刪除。

(3)若有理由認為，刪除資料將損害當事人值得保護之利益，得以封鎖取代刪除。被封鎖之資料，僅能基於資料不被刪除之目的，始得被調取與使用；若為保護具有特別高度價值之法益而絕對必要，且若不調取及使用該資料，則事實之調查將不可指望或顯有困難，或當事人已同意時，亦得調取及使用被封鎖之資料。

(4)輸入資料機關依情報資料適用之期限，於個案處理時，審查個人資料是否應予更正或刪除。

第12條　建置命令

聯邦刑事局應會同參與機關訂定建置共同資料庫之命令，以確定下列事項之細節：

1.本法所稱與德意志聯邦共和國相關之國際恐怖主義範圍。

2.第1條第2項規定之其他參與之警察執行機關。

3.第3條第1項規定之應儲存資料種類。

4.應儲存資料之輸入。

5.參與機關有讀取權之組織單位。

6.查詢目的之區分及其急迫性。

7.紀錄。

建置命令必須獲得聯邦內政部、聯邦總理府、聯邦國防部、聯邦財政部、以及對各邦參與機關有管轄權之邦最高機關之同意。建置命令訂定前，應聽取個人資料保護暨資訊自由官之意見。

第13條　基本權之限制

書信、郵件與通訊秘密基本權（基本法第10條）以及住宅不受侵犯基本權（基本法第13條）得依本法規定限制之。

3.創設反恐資料庫，最初之思考，可溯源自聯邦眾議院第15屆任期。當時聯邦參議院基於下薩克森邦、巴伐利亞邦、薩爾蘭邦、圖林根邦之提案，而提出「為監控與打擊伊斯蘭極端主義及恐怖主義而建置德國安全機關共同資料庫法草案」（Entwurf eines Gesetzes zur Errichtung einer gemeinsamen Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus）（反恐資料庫法）（BTDrucks 15/4413）。依據該草案之規定，參與之警察機關及情報機關，應將與伊斯蘭極端主義與恐怖主義具有關聯性之人士或事件的一切資料，建置於該共同資料庫中（BTDrucks 15/4413, S. 8）。當時的聯邦政府，則與此不同，而較偏向於建置索引資料庫，亦即僅為發現進一步情報所必要之資料，建置一套電子式資料發現地憑據（BTDrucks 15/4413, S. 9）。惟這兩種建議，在第15屆任期中，均未能被實現。

2006年8月，在柯布倫茲（Koblenz）以及多特蒙特（Dortmund）發生意圖襲擊火車未遂事件，聯邦政府於此一事件後提出聯邦與各邦警察機關及情報機關共同資料庫建置法草案（共同資料庫法），該草案第1條亦包含聯邦與各邦警察機關及情報機關標準化中央反恐資料庫建置法（反恐資料庫法）（BTDrucks 16/2950, S. 5），並且在內政委員會聽取專家意見後（Innenausschussprotokoll Nr. 16/24

），微調其內容而通過。根據草案之立法理由，此部法律係為共同資料庫創設法源依據，使警察機關與情報機關間的資訊交換更有效率，讓現有的共同合作模式更臻完善，並減少傳輸之錯誤（BTDrucks 16/2950, S. 12）。依反恐資料庫法第1條第1項之規定，反恐資料庫之設置目的，乃在協助參與機關履行調查與打擊國際恐怖主義之任務，主要作法是，使用「調查」此一概念簡要說明情報機關之任務，以及藉由「打擊」此一概念簡要說明警察機關之任務。反恐資料庫法第2條係規定反恐資料庫之內容。能被參與機關基於知悉之目的而儲存於資料庫者，僅限於參與機關依其適用之法規範而已掌有之資料；反恐資料庫法並未為參與機關蒐集資料創設額外之法律依據（BTDrucks 16/2950, S. 15）。透過反恐資料庫法第2條第1句第2款之規定，殘暴及準備實施暴力之個別行為人，尤其是本身被認為係「仇恨鼓吹者」（Hassprediger），亦被納入反恐資料庫法之規範範圍（vgl. BTDrucks 16/2950, S 15）。

反恐資料庫法第3條第1項規定，關於第2條提及之人士與對象，其何種資料類型應予儲存。第3條第1項第1a款規定之基本資料，可用來辨識被查詢之人。延伸基本資料除可用來辨識被查詢之人外，亦得用以作成（作為專業初步評價之）準確危害預測。與基本資料不同的是，延伸基本資料原則上僅能被檢索，然而在出現吻合情況時，經詢問儲存機關後，亦得依據專業法律之規定，將延伸基本資料揭露予查詢機關。應予輸入之資料－在儘可能的範圍內－應當依據系統方面之預先設定，以標準化之形式儲存。透過自由文字欄位，在標準化之資訊外，得輸入個人之評註、指示與評價，藉此使得與恐怖主義相關但未透過目錄以標準化方式納入之資訊，亦得以因此被納入。然而，原則上應履行之標準化義務，不得藉此方式規避之（BTDrucks 16/2950, S. 17）。

依共同資料庫法第5條第1項之規定，反恐資料庫法於2006年12月31日生效。

4.在參與機關之實務上，反恐資料庫作為標準化資料庫此一特性，影響反恐資料庫之操作及使用。標準化意指，並非一切依反恐資料庫法第3條第1項應予儲存之資訊，得信手拈來地輸入資料庫內，而是在目錄中提供資訊之特定類型選項，亦即所謂的目錄值（Katalogwerte），輸入資料機關則從中選擇資料之輸入位置。依聯邦政府之說明，以自由文字輸入之可能性，僅限於反恐資料庫法第3條第1項規定之資訊中，不能就特定目錄值予以標準化者。此種資訊，在基本資料的範圍內，包括街道、門牌號碼、郵遞區號以及地方之資訊，而在延伸

基本資料的範圍內，則包括例如電話號碼、電信終端設備之機器號碼，或交通工具識別號碼、汽車之車牌與發照地，以及必然地包括反恐資料庫法第3條第1項第1b款rr的自由文字欄位。標準化之實施，係在輸入介面內，以所謂「下拉式選單」（Pull-Down Menüs）之形式，透過專為提供輸入資料機關選擇所設之目錄值列表而為之。反恐資料庫法第3條第1項之何種資料類型出現於目錄上，且何種資料類型作為被註記資料之目錄值而得以在各該目錄中被選擇，原則上係由聯邦刑事局依反恐資料庫法第3條第1項，以及進一步依反恐資料庫法第12條第1句第3款規定，於建置命令之具體化內容，以目錄編輯工作確定之，並記錄於目錄手冊中，而該目錄手冊就如同建置命令本身一樣，被界定為「密件－僅供勤務使用」（VS－Nur für den Dienstgebrauch）。應與此區別者，乃「封閉式」（geschlossen）與「學習式」（lernend）目錄。當使用「封閉式」目錄時，可能的目錄值係以不可更改的方式予以確定。例如反恐資料庫法第3條第1項第1b款ee規定之被人使用的交通工具資料，在「交通工具類型」目錄中，應從不可更改的「貨車、小型汽車、巴士、飛機、摩拖車、火車、特殊交通工具、自行車、四輪摩拖車」選單中作選擇。要在選單內容以外為其他登載，即屬不可能。欲對目錄進行修改，僅能由聯邦刑事局以目錄編輯工作之方式為之。當目錄編輯者將目錄值預先設定之選項，供作使用者選擇時之建議，就此而言，「學習式」目錄即近似「封閉式」目錄。但除此之外，使用者尚可基於為進一步登載之目的，而對目錄予以補充。該進一步之登載，後續亦得由其他使用者當作目錄值，於選擇時加以利用。此一額外之登載，並不以聯邦刑事局之同意為必要。例如在輸入反恐資料庫法第3條第1項第1b款aa所定電信終端設備之資訊時，得由使用者在目錄中輸入電信終端設備之新興類型，此應當有其必要，因為應予儲存之人會使用迄今尚未寫入目錄之新型態電信終端設備。

利用參與機關源頭資料庫之資料存量，經常可在部分自動化之程序中填充反恐資料庫。首先，在源頭資料庫內之現有資料組，由各該參與機關依其對反恐資料庫之重要性，以手工專業審查方式進行審核，並於可能時為適當之標記。繼之，從被標記之資料組中產生所謂的輸出資料庫，而來自源頭資料庫之資料類型，只有在反恐資料庫中已有相應之類型者，始被納入輸出資料庫。反恐資料庫之資料類型，若為源頭資料庫所無或在具體之資料組內空無一物者，則該資料類型於反恐資料庫中，將繼續保持空無一物之狀態。考量到標準化目錄之因

素，故在此亦會針對源頭資料庫之所有目錄值與反恐資料庫預設之目錄值是否一致進行審核。若出現用語不一致之情形，即進行改寫，例如將Fernsprecher改寫為Telefon。接著，再將輸出資料庫傳送給聯邦刑事局，由聯邦刑事局輸入反恐資料庫內。

5.關於反恐資料庫，有不同的個人資料保護官對各參與機關進行審查。聯邦刑事局、聯邦憲法保護局以及聯邦情報局所為之資料處理，由聯邦個人資料保護暨資訊自由官審查之。聯邦個人資料保護暨資訊自由官曾就聯繫者延伸基本資料之儲存，提出根本性疑慮，並批評指出，聯邦刑事局對於源頭資料庫之資料，曾未經個案審查即在反恐資料庫法第3條第1項第1b款rr之自由文字欄位中遭到傳輸。聯邦刑事局因此修正了自由文字欄位的填充程序（BTDrucks 16/12600, S. 51 f.）。至於聯邦憲法保護局，則除了對於反恐資料庫之填充，尤其是自由文字欄位填充的問題外，其對於取之於隱密性電信監察之資料，亦遭認定具有標記之缺失。由於聯邦憲法保護局允諾立即改善被認定之缺失，故對其提出之形式上指責即告止歇（BTDrucks 17/5200, S. 83 f.）。因反恐資料庫之故，邦機關亦受到審查，諸如在巴登符騰堡邦，該邦刑事局（國家保護部門）以及該邦憲法保護局，即接受為期數日之登門審查。與若干資料組有關之缺失，因邦個人資料保護官曾提出指責，而使該資料組遭到刪除或修正（Landtag von Baden-Württemberg, LTDrucks 14/2050, S. 12, 14 ff.）。其他進一步之審查，由邦個人資料保護官為之。

II.憲法訴願人之主張

憲法訴願人認為，其受基本法第2條第1項結合第1條第1項保障之資訊自主決定基本權，以及受基本法第10條、第13條與第19條第4項保障之基本權，被系爭規定侵害。

1.憲法訴願人主張，其被系爭規定直接影響。儘管反恐資料庫法的條文尚需有實際之執行行為，亦即將憲法訴願人之資料置入反恐資料庫內。但因憲法訴願人不會被告知其資料遭置入反恐資料庫內，以致憲法訴願人無法提起有效司法審查。不過，憲法訴願人得依反恐資料庫法第10條第2項之規定請求告知，並在情況可能時提起訴訟。惟此一權利救濟之可能性顯有未足。蓋即便其於某日被告知未被納入反恐資料庫內，然翌日卻可能出現完全不同之發展。此外，這種涉及隱密儲存資訊之請求，須向30個以上之不同機關提出。

由於憲法保護機關有義務將蒐集之資料儲存於反恐資料庫內，因此憲法訴願人擔心，與其相關之資料會在其無從得知的情況下，被納入反恐資料庫。由於憲法保護機關有權以情報

機關手段秘密蒐集資訊，故憲法訴願人作為素行良好之人，有可能在從事合法行為時－例如基於匿名之指示－成為情報機關程度強烈措施之行使對象。而且，憲法訴願人無從知悉某些人士是否與恐怖主義有何瓜葛，但卻可能被視為是這些人的聯繫者，而遭誤認能為調查國際恐怖主義提供進一步之線索。

2.透過反恐資料庫，一切參與機關得讀取由憲法保護機關儲存之資料，尤其亦包括本身不得蒐集該資訊，且若無反恐資料庫即無從獲悉該資訊之警察機關。藉由反恐資料庫法之存在，警察機關與情報機關區分之誡命，已部分地遭到揚棄。此一區分誡命在憲法上之位階，係從基本法第87條第1項第2句推導而出；其可謂法治國原則與基本權保障之展現。警察機關與情報機關相互區分之誡命，其目的乃在防止，因警察機關取得基於現行規定不得自行蒐集之資料，而淘空法律對警察機關干預職權之規定。

3.反恐資料庫法之規定，對憲法訴願人之資訊自主決定權造成侵害。這些規定並不明確，且不符合比例原則。依據反恐資料庫法之規定，人們若－在不確定的根據事實下－被認為是非法暴力的支持者，則其資料也會被納入反恐資料庫，此處所稱之暴力，並非僅限於典型的恐怖暴力，而是各種微小暴力即為已足；至於何謂「支持」，仍無明確之答案。對資料之儲存而言，只要有內在的「根據」，即可謂合於要件。因此，反恐資料庫法第2條第1句第2款之規定，與明確性要求不符。

反恐資料庫法第2條第1句第3款關於聯繫者之特別規定，太過不明確。由於無須自己對恐怖活動有認識，即可被認定為是聯繫者，當事人的範圍因基於「雙重揣測」，而被不合比例地擴展開來。如素行良好之人，只要有－不確定的－「根據」認為其與他人有所聯繫，而又有－可能同樣不確定之－「根據」，顯示該他人有恐怖行為方式，或「支持暴力」，則該素行良好之人的資料，亦將被納入反恐資料庫。從聯繫者身上可以獲取「進一步線索」之必要期待，實際上並無法發揮限制受波及者範圍之功能。

反恐資料庫法第3條第1項第1a款對於基本資料之規定，不符合比例原則，亦太過不明確。當「延伸基本資料」依據反恐資料庫法第3條第1項第1b款被納入反恐資料庫，基本權遭受的干預也就隨之增強。延伸基本資料所勾勒者，乃廣泛之人格輪廓。反恐資料庫法第5條第2項，在發生緊急事件時，所有參與機關得讀取延伸基本資料之規定，不符比例原則，因為該規定對此種資料之重要性並未給予適當之評價，且只需任何人之健康遭受威脅，即可合理化對延伸基本資料之

讀取。

此外，依反恐資料庫法第3條第1項第1b款rr之規定，將僅基於「根據」而作成之評語、總結、評價及指示，當成額外之自由文字納入反恐資料庫，此亦違反比例原則且太過不明確。由於缺乏實質上之限制，因此一切類型之其他資訊，在漫無邊際的範圍內，均可能被納入反恐資料庫中；而自由文字之儲存，事先難以估量。

由於反恐資料庫法本身並無資料刪除之條文，而僅指出輸入資料機關之適用規定，故牴觸明確性要求。輸入資料機關之適用規定，散見於反恐資料庫法並未提及之諸多法律條文中。在發生封鎖或刪除之情況時，被參與機關所獲悉並予以儲存之資料將如何處理，亦不明確。

4.在住宅內實施「大監聽」（großer Lauschangriff）而取得之資料，也被納入反恐資料庫，這違反了基本法第13條。反恐資料庫法第3條第2項在未遵守基本權要求門檻的情況下，允許對基本法第13條作如是之侵害。反恐資料庫法賦予憲法保護機關及情報機關，享有藉由反恐資料庫而為資料傳輸的廣泛干預可能性，導致憲法訴願人之私人通訊行為及通訊內容，會被其他機關以不合比例原則之方式獲悉，因此基本法第10條之書信及電信秘密亦遭受侵害。

5.憲法訴願人依基本法第19條第4項享有之對公權力行為提起司法救濟基本權，亦遭到侵害。各項措普遍以隱密方式進行，剝奪憲法訴願人請求司法審查的機會。而其他得代替司法救濟途徑的審查，亦付之闕如。

III.相關機關之意見

對本件憲法訴願提出意見之機關，計有：聯邦政府、聯邦個人資料保護暨資訊自由官、什勒斯維希-霍爾斯坦邦個人資料保護獨立中心、柏林個人資料保護暨資訊自由官，以及巴登符騰堡邦個人資料保護暨資訊自由官。

1.聯邦政府認為，本件憲法訴願不合法，縱使程序合法，亦屬無理由。

a)由於憲法訴願人並未透過反恐資料庫法而直接、自身及現時地受有不利益，故本件憲法訴願並不合法。憲法訴願人並未說明其資料被存入反恐資料庫之事實。憲法訴願人在提起本件憲法訴願前，並未依據反恐資料庫法第10條第2項之規定，為證明其確屬資料遭儲存之當事人，而向聯邦刑事局以及在可能的情況下，向其他參與機關要求告知其資料是否被儲存在反恐資料庫內。必要時，須向38個參與機關要求告知資訊，此種耗費實屬高估。若憲法訴願人就是否具備訴願權能所為之闡述，無法排除「民眾憲法訴願」（Popularverfassungsbeschwerde）之疑慮，則憲法訴願人所

為之說明即過於模糊。同時，本件憲法訴願究竟欲具體地指責哪些規定，並不清楚，故本案欠缺充分明確之訴願標的。

b)縱使程序合法，本件憲法訴願無論如何亦屬無理由。

aa)聯邦對於制定反恐資料庫法之立法權，原則上係從基本法第73條第1項第10a至c款導出；在涉及聯邦情報局及軍事情報局的部分，聯邦之立法權可從基本法第73條第1項第1款導出，而關於海關刑事局以及聯邦警察的部分，則可從基本法第73條第1項第5款導出聯邦之立法權。至於在聯邦刑事局創設中央資料庫，亦可歸屬於基本法第87條第1項第2句所規定建置中央機構之職權。

bb)從基本法中能否導出警察機關與憲法保護機關在組織及職權上應相互區分之誡命，似仍存有疑問，因為憲法保護機關與警察機關之任務及活動領域並不會相互摻雜混合在一起。對基本法而言，在情報機關與警察機關之間的資訊協助，似乎並無嚴格之要求。反恐資料庫法並未造成不受控制的資料流動。其僅是讓各機關彼此間之相互聯繫，以及依其他法律規定而為之資訊流動成為可能。反恐資料庫法中重要的資訊傳輸規定，並未包含新的資訊流動範圍。

cc)反恐資料庫法並未侵害資訊自主決定基本權。資料之儲存、提取及其進一步之使用，均屬合理。

將資料儲存在反恐資料庫內，充其量僅構成輕微的基本權干預，或僅輕微強化原本資料蒐集與使用造成的基本權干預。僅有依各該專業法律規定本來即可蒐集之資料，始能儲存於反恐資料庫內。充實反恐資料庫，本身並未變更資料儲存之目的，對儲存於反恐資料庫內之資料進行使用，侷限於非常特殊的國際恐怖主義危害領域。對於已儲存之資訊予以標準化，其產生之影響亦屬有限。普通基本資料所包含者，基本上係與人有關而寓有便利資訊交換目的之資訊，至於延伸基本資料，則除此之外尚寓有於緊急事件中，獲取對某人之第一印象及其危害性之目的。

認為受牽連族群過廣而欠缺明確性，此種想法不具說服力。反恐資料庫法第2條第1句第2款的暴力概念，比刑法典的以強制力而為物理上之強暴更為嚴格。暴力支持者的變體，主要係指所謂的仇恨鼓吹者，且要求必須從外觀上可以認識到，其贊成使用暴力。要認定依反恐資料庫法第2條第1句第3款應予儲存之聯繫者，尚須適用其他標準，例如進行預防性之電話監聽時，因為反恐資料庫法的條文，僅係將依其他法律規定已合法儲存之人納入反恐資料庫，而不涉及新的資料蒐集。所謂必要之事實根據所要求者，恆為嫌疑之事實基礎。將資料

儲存於反恐資料庫法第3條第1項第1b款rr規定的自由文字欄位，係對資料輸入標準化所為之調校措施，而且藉由資料必須展露出其與法律定義之資料在內容上的直接關係，亦可限縮自由文字欄位之資料儲存。就連廣泛的資訊總額，也受有限制。

僅在為調查或打擊國際恐怖主義有必要時，始得檢索反恐資料庫，從而，檢索反恐資料庫所造成的干預程度，也就有一定之侷限。反恐資料庫之使用，不得基於與其他資料庫進行自動調準之目的。檢索後若出現吻合情形，原則上僅會為識別某人之目的而使普通基本資料遭到讀取，並且，對此種資料進行使用，僅限於用來調準吻合者，以及僅限於提出請求調查之單位使用。反恐資料庫法僅係用來使各參與機關彼此之間就已被調查之人能進行相互聯繫；至於用來找出「嫌疑人」，則為此部法律所不許。基於調查之請求而交付延伸基本資料，須依具決定性之專業法律傳輸規定為之。

在發生緊急事件時，亦得讀取延伸基本資料，而且為了防止反恐資料庫法第5條第2項規定之危害，得使用延伸基本資料，這確實是反恐資料庫法引致之嚴重干預。然而，延伸基本資料的資訊內容，亦受有限制。依反恐資料庫法第5條第2項的規定，僅在非常態的緊急情況下，始得讀取延伸基本資料。當此一規定以具重大價值之物為據，則具重大價值之物所指為何，乃透過物的經濟與公共價值而告確定：反恐資料庫法第5條2項之目的，係在保障諸如橋樑、機關、基本設施等公物。反恐資料庫法第5條第2項，對於發生緊急事件時，得讀取延伸基本資料，亦設有特殊之程序法上保障制度。事實上，反恐資料庫法第5條第2項之規定，迄今僅被動用過一次。

反恐資料庫法引致之基本權干預，應屬合理。打擊恐怖主義，乃是一項具有最高位階的憲法任務。建置反恐資料庫，使各參與機關能藉由資訊交換更臻完善，讓調查及打擊國際恐怖主義變得更為容易，因此，建置反恐資料庫對於其目的之達成，具有適當性。為了讓警察機關及情報機關能快速獲致有關國際恐怖主義及其支持者之情報，對於調查及打擊國際恐怖主義的盤根錯節網絡而言，反恐資料庫法亦具有必要性。又，反恐資料庫法亦合乎狹義比例原則。在為整體之衡量時，干預之嚴重程度與合理化事由之重要性，二者非不相稱。

dd)儲存於反恐資料庫內的資料，可能亦得藉由干預基本法第10條及第13條之方式而獲得，因此反恐資料庫法第13條顯然會對這兩項基本權造成限制。用這樣的資料來充實反恐資料庫，對基本權之限制確屬十分重大

，但並非不合比例原則。資料的新使用目的，受有充分之限制，而反恐資料庫法第3條第2項規定之標記義務，可確保資料使用之關聯性不致逸失。雖然反恐資料庫法第5條第1項並未將資料之查詢，限制於僅依資料傳輸之規定，始能傳輸藉由干預基本法第10條及第13條而獲得之資料。但在出現吻合情形時，只有普通基本資料才會被傳輸至查詢機關。此外，受基本法第10條或第13條特別保障之資料，本身被當成吻合者資料而遭到揭露之情形，也可以透過以下之方法予以避免：依據反恐資料庫法第4條第1項之合憲性解釋，各機關必須以隱密之方式，儲存藉由干預基本法第10條或第13條而得來之基本資料。

依反恐資料庫法第5條第2項，受到特別保護之資料得在緊急事件範圍內被讀取，於結論上合乎比例原則，因為此項得讀取延伸基本資料之規定，乃在使具體的警察危害防止配置更為簡易，其目的非在廣泛勾勒人格輪廓。

ee)由於被載入反恐資料庫內的當事人並未欠缺權利救濟之機會，因此反恐資料庫法也符合基本法第19條第4項的權利救濟保障。儘管參與機關不會主動依職權通知當事人，但當事人得依反恐資料庫法第10條第2項之規定請求告知，若未獲同意並可透過行政訴訟予以貫徹。此一權利救濟可能性之安排，可藉由行政任務之類型以及載入反恐資料庫之輕微干預程度而合理化。

ff)反恐資料庫法第10條第1項於各該管轄權範圍內，授權聯邦個人資料保護暨資訊自由官以及各邦個人資料保護官，審查反恐資料庫之個人資料保護事宜。個人資料保護官所為之審查，並不因為其審查權僅能在各該公法團體內實施，而有所不全。聯邦個人資料保護官若對一切的資料庫使用事件均享有審查權，將使聯邦個人資料保護官從而得對邦機關進行審查，這會產生憲法上之問題。至於各邦個人資料保護官讀取記錄資料，則在位於Wiesbaden的聯邦刑事局為之。

gg)在事實的方面，聯邦政府則為以下之陳述：被資料儲存所牽連者，大部分是在外國生活而姓名之寫法並不恆常清楚之人。在2012年8月，一共有17,101筆關於人的資料組被儲存在反恐資料庫內，其中約有920筆為雙重命名或雙重儲存，因此約有16,180位不同人士遭資料儲存所波及。在這些人士中，有2,888人住在國內，而有14,213人住在國外。這些人士中，之所以住在國外者為數眾多，這可歸因於聯邦情報局的參與。資料被依反恐資料庫法第4條第1項第1句而隱密儲存者，一共有2,833人。參與機關對於把不知情恐怖活動的聯繫者資料納入反恐資料庫中，抱持非常

審慎保留的態度。反恐資料庫在2012年8月僅有141筆大部分係由各邦警察機關輸入之聯繫者的資料組。

現有的資料組幾乎沒有延伸基本資料之登載。僅44%的資料組係完全由延伸基本資料充實。又，幾乎沒有任何一個資料組含有近乎全然的延伸基本資料組。94%以上的資料登載並未包含自由文字欄位資訊，其理由在於，聯邦情報局的源頭資料欠缺可對比的欄位。自由文字欄位限於2000個字元，亦即較A4頁所載規格文字更少。自由文字欄位之登載，通常非常簡短，經常僅包含一個字，大多介於15至55個字元。在反恐資料庫法第3條第1項第1b款rr規定的自由文字欄位中，僅有三分之一的個人資料組超過100個字元。

從2007年3月起至2007年秋季止，每星期通常有1,200個查詢，總計約350,000個查詢被記錄下來。這顯示了，反恐資料庫被當成「特別電話簿」而非供作共同的資料源頭調準目的使用。在這段期間，查詢延伸基本資料者，其比例不到1%。在通常的情況下，對於機關而言，直接與儲存機關聯繫，會比請求告知延伸基本資料更有意義，因為延伸之基本資料僅在特殊情況下，始能基於首要與快速危害預測功能而被傳輸。在查詢延伸基本資料時，大約有三分之一或四分之一的比例，其讀取延伸基本資料的請求會遭到拒絕。

為了能理性地對查詢結果設限，目前系統所確保的是，查詢時若出現200個以上的吻合者，系統在技術上即不呈現查詢結果。經查詢而列出吻合情況者，其數量平均約4至5筆。在反恐資料庫法第5條第2項的緊急事件規定範圍內，對延伸基本資料進行讀取，至2012年8月為止僅發生過一次。該次延伸基本資料之讀取，係邦刑事局讀取聯邦憲法保護局之資料組。

在紀錄伺服器裡，一共儲存了大約7,700,000筆資料組；每一筆資料組所反映者，乃經由反恐資料庫內之活動而引發的各該資料庫資料往來。

2.聯邦個人資料保護暨資訊自由官對於反恐資料庫法表達疑慮。警察機關與情報機關的資訊共同合作，應遵守區分誡命保留（Vorbehalt des Trennungsgebots）原則。當參與之警察機關在緊急事件中得以直接讀取情報機關儲存之延伸基本資料，即與上開原則不符。關於規範清楚性要求（Gebot der Normenklarheit）之疑慮，係存在於：反恐資料庫法第1條第2項、反恐資料庫法第2條第1句第2款的「支持」此一構成要件要素、反恐資料庫法第2條第1句第3款的聯繫者規定（就該規定而言，被儲存的聯繫者與未被儲存之短暫或偶然的日常聯繫，二者界限不明），以及反恐資料庫法第3條第1項第1b款rr的自由文字欄

位。對於自由文字予以儲存，在和其他被儲存之資料綜合觀察下，廣泛的人格輪廓即被勾勒而出。反恐資料庫法第10條第2項第2句之規定，指望當事人向反恐資料庫之參與機關請求告知，並在可能的情況下對其提起訴訟，這樣的規定並未對有效權利保護提供保障；反恐資料庫法應規定者，乃課予參與機關告知義務。

聯邦個人資料保護暨資訊自由官進一步指出，其與各邦個人資料保護官的管轄權劃分，可能會產生不受查驗的空間。由於資料庫係由聯邦機關掌理，因此聯邦個人資料保護暨資訊自由官應讀取一切紀錄資料，此亦包括涉及邦機關讀取資料之資料。以對基本法第10條基本權限制法（Artikel-10-Gesetz）為據而採取之措施，其蒐集到的資料，恐也會出現查驗漏洞。此外，讀取紀錄伺服器僅能在伺服器所在地為之，這也造成查驗上之困難。

3.什勒斯維希-霍爾斯坦邦個人資料保護獨立中心以及柏林個人資料保護暨資訊自由官共同提出意見。其認為，本件憲法訴願之提起合法且有理由。反恐資料庫法不但不符規範清楚性與明確性原則，亦違反比例原則，並且對資訊自主決定基本權以及基本法第10條與第13條造成侵害。而反恐資料庫法是否符合區分誡命，亦同樣存有疑義。

反恐資料庫法第2條第1句第1款至第3款包含之當事人範圍，過於廣泛。對於將人納入當事人範圍而言，欠缺充分的嫌疑程度；第2款的暴力概念並未充分地侷限在暴力的恐怖形式；第3款的聯繫者，則有鑑於應予蒐集資料之敏感性，從許多方面來看，其範圍都未作充分之限制。依反恐資料庫法第3條第1項第1b款hh而儲存宗教信仰資料，因具有烙印化之危險，故干預程度特別強烈，且是否合於基本法第4條第1項，亦有疑問。資料讀取的規定，也與資料蒐集原本之目的欠缺充分的連結。一切參與機關，可以在沒有干預門檻的情況下，讀取普通基本資料。於發生緊急事件時讀取資料，其要件上的門檻同樣亦非甚高；而反恐資料庫法第6條第1項也有可疑之處。藉由「刪除、剔除之審查期限、封鎖、更正以及告知」而為程序法上之保全，並不足以達成憲法上之要求。對於隱密儲存時的共同告知程序，其規定付之闕如。最後，邦個人資料保護官在實施查驗時，亦即關於紀錄資料之讀取，會和聯邦個人資料保護暨資訊自由官一樣遭遇相似的困難。

4.巴登符騰堡邦個人資料保護官提出之報告，則為其在2007年（vgl. hierzu Landtag von Baden-Württemberg, LTDrucks 14/2050, S. 12 ff.）以及2012年至邦刑事局以及邦憲法保護

局進行之查驗。關於暴力的概念，以及應受非難的「支持」與受基本權保障的意見表達，二者界限如何劃定，均存有問題。在進行查驗時，聯繫者之規定顯得過於不明確。對於機關而言，評價現行的聯繫行為強度，以及查驗資料儲存是否合於可期待從聯繫者身上獲致調查及打擊恐怖主義之進一步線索此一要件，乃困難之事。對邦個人資料保護官而言，不能以電子方式讀取紀錄資料，這也造成查驗之困難。除此之外，巴登符騰堡邦參與機關之資料儲存，則無可指責之處。

IV.參與言詞審理程序者

聯邦憲法法院在2012年11月6日舉行言詞審理程序，各種法律見解在言詞審理程序中已獲得表達與深入闡述。於言詞審理程序中表示意見者為：憲法訴願人、以聯邦眾議院成員身分出席之Clemens Binninger議員、聯邦政府、聯邦刑事局、聯邦憲法保護局、聯邦情報局、聯邦個人資料保護暨資訊自由官、巴登符騰堡邦個人資料保護官、巴伐利亞邦個人資料保護官、柏林個人資料保護暨資訊自由官，以及巴登符騰堡邦刑事局。德國人權研究院（Deutsche Institut für Menschenrechte）、人本聯盟（Humanistische Union）以及混亂電腦俱樂部（Chaos Computer Club）以專家身分提出意見。

B.憲法訴願程序合法

本件憲法訴願之提起合法。

I.基本權遭受侵害之可能性

憲法訴願人所指責者，乃資訊自主決定基本權（基本法第2條第1項結合第1條第1項）、通信及電信秘密自由（基本法第10條第1項）、住宅不受侵犯（基本法第13條第1項），以及與這些基本權相結合之權利保護（基本法第19條第4項）受到侵害。

憲法訴願人陳述其資訊自主決定基本權有遭到侵害之可能，其主張，系爭條文有相當之蓋然性規定了儲存及使用與其相關之個人資料事宜，且這些規定太過不明確，規範之範圍亦不合比例地過於廣泛。由於相關資料可能涉及藉由干預基本法第10條第1項或第13條第1項而取得之資料，故憲法訴願人亦得主張這些基本權遭到侵害。憲法訴願人指責，資訊之儲存及使用僅以不充分之方式，附加以達成權利保護為目的之資訊權，就此而言，這些基本權結合基本法第19條4項遭到侵害，憲法訴願人同時也充分指責之。

II.直接、自身及現時之利害關係

憲法訴願人與系爭規定之間，具有直接、自身及現時之利害關係。

1.憲法訴願人就本件憲法訴願並未欠缺必要之直接利害關係。雖然在法律之規定，無須進一步之執行行為，即干預憲法訴願人之權利時，憲法訴願人始與法律規定之間具有直接利

害關係。若法律要貫徹施行，就法律必要性而言，或是僅依據事實上之國家實務運作而言，必須具備特殊的、被執行單位意志所影響的執行行為，則憲法訴願人原則上於提起憲法訴願之前，應對該執行行為提出權利救濟且已窮盡救濟途徑（BVerfGE 1, 97 <101 ff.>; 109, 279 <306>; stRspr）。然而，當憲法訴願人因為無從知悉相關之執行措施，而不可能提起訴訟時，則憲法訴願人即與該法律規定之間具有直接利害關係。在此種情況下，憲法訴願人直接針對法律規定提起憲法訴願，一如無中介之執行行為，而針對法律提起基本權訴願（vgl. BVerfGE 30, 1 <16 f.>; 113, 348 <362 f.>; 120, 378 <394>; stRspr）。本案即是如此。原則上，憲法訴願人對於其資料依系爭規定而被儲存或被使用，均無法獲致可信賴之資訊。

上述之情形，並不因為憲法訴願人得依反恐資料庫法第10條第2項之規定請求告知有關資料被儲存之情形，並針對資料儲存續向法院提起訴訟，而有所改變。因為憲法訴願人透過此種途徑，只能針對在特定之時間，其個人資料事實上被儲存提起訴訟，但對於其無法施加影響力或未請求告知，而隨時可能發生之資料儲存，即難以－與其權利保護之請求相符地－提起訴訟予以防禦。針對授權採取隱密措施之法律直接提起憲法訴願，通常僅在以下情形始不得為之：透過國家之積極告知義務，在法律上可確保當事人在日後能被告知（so in BVerfG Beschluss der 1. Kammer des Ersten Senats vom 25. April 2001 - 1 BvR 1104/92 -, NVwZ 2001, S. 1261 <1262 f.>）。反恐資料庫法並未設有此種告知義務之規定。

2.憲法訴願人就本件憲法訴願具有自身及現時之利害關係。

當藉由系爭法律之執行始生具體損害，而當事人因通常對執行行為無從知悉，則只要憲法訴願人主張，其基本權遭以系爭法規範為據之措施干預，具有相當之蓋然性，則憲法訴願人具有自身及現時利害關係之可能性，即已具足（vgl. BVerfGE 122, 63 <81 f.>; 125, 260 <305>; stRspr）。憲法訴願人對利害關係得否主張之可能性，會影響基本權干預蓋然性之要求程度。因此，某一措施之對象是否在構成要件上緊縮範圍，抑或該措施之對象範圍廣泛且第三人亦可能意外受牽連，此一因素即具有重要性。憲法訴願人欲證明具有自身現時利害關係，無須主張到：自己乃是犯罪行為人或是可能對公共安全造成危害之人（vgl. BVerfGE 109, 279 <308>; 113, 348 <363>; 120, 378 <396>）。

憲法訴願人所為之主張，已合於上開要求。雖然憲法訴願人對於其受資料儲存波及之特殊蓋然性，僅能為

有限之描述。其所主張者，基本上僅是其與可能親近恐怖主義之人有所聯繫。但是，由於被儲存於反恐資料庫而可能遭到掌握之人士範圍廣泛，因此憲法訴願人所為之說明，已屬充足。依反恐資料庫法第2條第1句之規定，資料遭到儲存之人，並非只有恐怖主義嫌疑者及其援助者，而是範圍廣泛地從僅屬恐怖主義周圍之人，至單純之聯繫者－精確地說，乃對其所為之聯繫與恐怖主義間之關係毫不知情之聯繫者－，均包括在內。

C.無須向歐洲法院提起事先裁判程序

本件憲法訴願，無須依歐盟運作方式條約（AEUV）第267條之規定，向歐洲法院（Europäischer Gerichtshof）提起事先裁判程序（Vorabentscheidungsverfahren），以釐清歐盟法上之基本權保障，對不同安全機關在共同資料庫所為如同反恐資料庫之資料交換，其保障之射程範圍何在。即便考慮到歐盟基本權利憲章（Grundrechtecharta - EuGRCh）第8條設有個人資料保護基本權利之規定，亦同。理由在於，歐盟基本權利憲章並不適用於待決之本案。因系爭規定並非透過歐盟法而產生，故應以基本法之基本權規定予以衡酌（vgl. BVerfGE 118, 79 <95>; 121, 1 <15>; 125 260 <306 f.>; 129, 78 <90 f.>）。因此，本案亦與歐盟成員國執行歐盟法，受歐盟基本權利憲章拘束（歐盟基本權利憲章第51條第1項第1句）無涉。

然而，系爭規定使資料得基於打擊國際恐怖主義之目的而相互交換，這有一部分亦涉及歐盟法之規範領域。歐盟對於歐盟運作方式條約第16條之個人資料保護，享有自身之規範權限。就此，例如1995年10月24日由歐洲議會（Europäisches Parlament）與歐盟理事會（Rat der Europäischen Union）制頒之自然人於資料處理時之保護及資料自由往來之保護指令（95/46/EG）（Abl. L 281 vom 23. November 1995, S. 31 ff. －個人資料保護指令），確立了原則上對私人及公務機關均一體適用之資料處理基本要求。相應地，歐盟法對於與抵禦恐怖主義有關之事務，亦設有不同之權限及法律基礎。尤其是2005年9月20日歐盟理事會制頒之關於資訊交換與涉及共同合作之恐怖犯罪決議（2005/671/JI）第2條規定，歐盟成員國應依內國法之規定，將其刑事追訴機關針對恐怖犯罪實施之刑事偵查結果，傳輸至歐盟刑事司法共同合作組織（Eurojust）、歐洲警察署（Europol）以及其他歐盟成員國。因此，反恐資料庫法以及藉由反恐資料庫法所欲追求之安全機關共同合作效率化，亦與歐盟法有關，並在經由反恐資料庫法規定之資訊交換而獲致進一步之結果時，亦直接在歐盟法之報

告義務範圍內發生作用。依2001年12月27日歐盟理事會制頒之2580/2001號歐洲共同體規章（Verordnung）（ABl. L 344 vom 28. Dezember 2001, S. 70 ff.），各歐盟成員國為打擊恐怖主義負有對特定人士及組織頒布限制性措施之義務，此亦同樣存有與歐盟法之連結點。此外，可能透過反恐資料庫而在諸多歐盟法之法律關係上獲致之有效共同合作結果，亦得以且應該屬於司法共同合作之範疇。

反恐資料庫法以及安全機關與情報機關依反恐資料庫法而為之行為，並非歐盟基本權利憲章第51條第1項第1句規定之執行歐盟法，這雖然沒有疑義且－另亦根據歐洲法院之清楚明白行為判決（Acte-claire-Rechtsprechung）（EuGH, Urteil vom 6. Oktober 1982, Rs. C-283/81, C.I.L.F.I.T., Slg. 1982, S. 3415 Rn. 16 ff.）揭示的標準－無須再進一步澄清。對於歐盟個人資料保護指令而言，從95/46/EG指令第3條第2項之規定可知，個人資料處理涉及公共安全、國家安全以及國家在刑事法領域內之行為者，顯然即排除在歐盟個人資料保護指令適用範圍之外。另外，反恐資料庫之建置與擴編，亦非透過歐盟法而決定。尤其是，在歐盟法中，並無任何條文規定德意志聯邦共和國必須或不得建置這樣的資料庫，或對此預為相關內容之規定。反恐資料庫法所追求者，毋寧乃是內國之特定目的，該目的僅能間接影響歐盟法上法律關係之成立，尚不足以依歐盟法上之基本權利保護標準進行審查（vgl. EuGH, Urteil vom 18. Dezember 1997, C-309/96, Annibaldi, Slg. 1997, S. I-7493 Rn. 22）。因此，歐盟基本權利之適用性，一開始即被排除。直接由歐盟基本權利憲章第51條第2項以及歐盟條約第6條第1項之文義可以得知，歐盟基本權利憲章既未將歐盟法之適用領域擴張至歐盟管轄權範圍之外，亦未替歐盟創設新任務，也未變更歐盟諸條約確立之管轄權與任務（vgl. auch EuGH, Urteil vom 15. November 2011, C-256/11, Dereci u.a., Rn. 71; EuGH, Urteil vom 8. November 2012, C-40/11, Iida, Rn. 78; EuGH, Urteil vom 27. November 2012, C-370/12, Pringle, Rn. 179 f.）。

據此，對於在本件憲法訴願中所提－而僅關乎德國基本權－之問題而言，歐洲法院並非基本法第101條第1項規定之法定法官（Gesetzlicher Richter）。從歐洲法院在Åkerberg Fransson案件的裁判（EuGH, Urteil vom 26. Februar 2013, C-617/10）中，亦應得出相同結論。在聯邦憲法法院與歐洲法院合作共存的意義下（vgl. BVerfGE 126, 286 <307>），此一裁判不能被評價為顯係越權行為（Ultra-vires-Akt），或被解讀為，以使

藉由基本法建置之憲法秩序同一性遭受質疑（vgl. BVerfGE 89, 155 <188>; 123, 267 <353 f.>; 125, 260 <324>; 126, 286 <302 ff.>; 129, 78 <100>）之方式，危及內國基本權之保障與貫徹（基本法第23條第1項第1句）。就此而言，此一裁判不能作如下之理解與適用：某一規定涉及歐盟法之純粹抽象適用領域，或在歐盟法之純粹抽象適用領域中發生單純之事實上作用，由該規定之事務關聯性，即足以導出歐盟成員國須受歐盟基本權利憲章之歐盟基本權利拘束。歐洲法院在此一裁判中毋寧亦指出，歐盟基本權利憲章規定之歐洲基本權利，僅在受歐盟法規範之事件中，而非在此領域之外有其適用（EuGH, Urteil vom 26. Februar 2013, C-617/10, Rn. 19）。

D.對憲法訴願有無理由之審查

本件憲法訴願，部分有理由。

I.受干預之基本權

系爭規定對資訊自主決定權（基本法第2條第1項結合第1條第1項）、書信及電信秘密自由（基本法第10條第1項）、住宅不受侵犯權（基本法第13條第1項）之保障範圍造成干預。

1.反恐資料庫法第1條至第6條所規定者，乃個人資料之儲存及使用，因此觸及資訊自主決定權之保障範圍。倘被儲存或被使用之資料係藉由干預基本法第10條第1項或第13條第1項而得來，則該資料之進一步使用亦應以這些基本權作為衡量標準（vgl. BVerfGE 125, 260 <313>; stRspr）。

2.這些基本權被上開條文所干預。首先，構成干預之處在於，反恐資料庫法第1條至第4條規定之儲存義務，使出自不同來源之資料有所匯集。這並不受資料係已由他方蒐集之資料所影響，因為資料乃是為使其他機關能如同資料蒐集機關一樣基於其目的進行支配使用，而依據特有之標準予以匯集與整理。其他構成干預之處尚有：依反恐資料庫法第5條至第6條以檢索形式呈現之資料使用、依反恐資料庫法第5條第1項第1句與第2句及第6條第1項第1句於出現吻合情況時，得讀取普通基本資料、依反恐資料庫法第5條第2項與第6條第2項於出現緊急事件時，亦得讀取延伸基本資料。

II.系爭規定具備形式合憲性

系爭規定在形式上合憲。尤其，聯邦權限之界限未遭僭越。

1.反恐資料庫法規定聯邦刑事局、各邦刑事局、聯邦憲法保護局、各邦憲法保護機關以及其他警察執行機關之資訊交換，就此而言，聯邦得以基本法第73條第1項第10a至c款關於機關共同合作事項之立法權為依據。共同合作，乃合作之長期持續形式，包含在各自之職權範圍內經常性之相互告知與答覆、相互商議以及相互支援與提供協助，並得建置功能性與組織性之聯絡管道、共同之組織以及共

同之資訊系統（vgl. Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 231 <Apr. 2010>）。反恐資料庫法規定之共同合作，亦屬之。

不同警察機關間之之共同合作權限，並不侷限於刑事追訴。基本法第73條第1項第10款之規定，可能導致聯邦與各邦在履行事後抑制性與事前預防性任務時，鬆動聯邦體制之管轄權界限。基本法第73條第1項第10a款之「刑事警察」（Kriminalpolizei）概念，並未排除聯邦得規定以防止犯罪為目的而為之共同合作，蓋此一概念之目的僅在將聯邦立法權侷限於與重要暴力犯罪有關之事項（Uhle, in: Maunz/Dürig, GG, Art. 73 Rn. 239 ff. <Apr. 2010>; Heintzen, in: v. Mangoldt/Klein/Starck, GG, Bd. 2, 6. Aufl. 2010, Art. 73 Rn. 114; Stettner, in: Dreier, GG, Bd. 2, 2. Aufl. 2006, Art. 73 Rn. 43; Werthebach/Droste, in: Bonner Kommentar, Bd. 9, Art. 73 Nr. 10 Rn. 109, 118 ff. <Dez. 1998>）。

反恐資料庫法對於警察機關與憲法保護機關共同合作之規定，雖兼具專業及跨專業之性質，但此並無礙於回歸適用基本法第73條第1項第10款。基本法第73條第1項第10款亦允許如此之跨專業規定。這不僅係對旨在超越聯邦體制之權限界限，而一般性地使不同安全機關彼此共同合作具有效率之基本法第73條第1項第10款作功能性之理解，亦貼近基本法第73條第1項第10款原來尚未以字母分成不同部分之版本。該文本同樣不能作狹隘之理解。1972年對此一條文進行修正時，並無就此方面賦予規範不同意義之目的（vgl. BTDrucks VI/1479）。

2.當反恐資料庫法第1條第1項將聯邦情報局、軍事情報局、海關刑事局以及聯邦警察當作另外的機關而納入規範，其可在基本法第73條第1項第1款及第5款尋得權限基礎。

將聯邦情報局納入規範範圍之權限，來自聯邦依基本法第73條第1項第1款享有之外交關係規範權。然而，就此劃歸聯邦之權限，係透過立法權之分配而形塑，且因基本法此一權限規定係與涉外事件相關，故其並未授權立法者得將以預防、防止或追訴犯罪本身為目的之職權賦予聯邦情報局（vgl. BVerfGE 100, 313 <368 ff.>）。毋寧，為了能從基本法第73條第1項第1款規定之立法權限中找到立法依據，法律之規定與適用，必須具備涉及海外情報工作以及為聯邦政府提供政治資訊之關聯性（vgl. BVerfGE 100, 313 <370 f.>）。不過，聯邦情報局參與反恐資料庫，則與此要求相符。就此而言，與上開要求相符之處首先在於，反恐資料庫法第5條及第6條使聯邦情報局得以讀取儲存於反恐資料庫之資料。依此規定，僅基於各查詢機關之各該任務始得讀取資料；因

此，聯邦情報局並未被賦予逾越防止國際恐怖主義犯罪目的外的、一般性的權限。與上開要求相符者亦包括，聯邦情報局將其資料輸入資料庫而使其他機關得以接近使用。反恐資料庫法並未創設不在基本法第73條第1項第1款範圍內之新資料蒐集權，其僅是連結為履行自身任務所蒐集之各該資料，並且規定其他機關僅能為履行任務始得接近使用該資料。為其他任務主體作如此具目的變更性之資訊提供，其範圍之規定，依事務之關聯性，係各該資料蒐集權限，以及與此相關的資料保護權限之一部（vgl. BVerfGE 125, 260 <314 f.>）。立法者並未藉此將聯邦情報局改造成前置的警察機關。

相應地，聯邦對於軍事情報局之參與，得以基本法第73條第1項第1款之（國防）為依據，並且對於聯邦警察與海關刑事局之參與，得以基本法第73條第1項第5款之規定（海關及邊界防衛）為依據。系爭規定得據此讓這些機關讀取資料以及將其資料寫入反恐資料庫內。

相較之下，反恐資料庫之其他參與機關得直接讀取上開聯邦機關輸入之資料，此種規定不能以基本法第73條第1項第1款及第5款為依據。毋寧，反恐資料庫法第5條第1項及第2項之規定，在對資料使用作事務最適之理解下，係以各該資料讀取機關各自之資料保護規定為要件，在可能情況下，係在邦之層級（vgl. BVerfGE 125, 260 <315>; 130, 151 <193>）。

3.對於掌理作為聯合資料庫之反恐資料庫而言，是否額外地須有聯邦行政權限，此一問題可置之不論。因為，這樣的權限，對由聯邦刑事局掌理之反恐資料庫而言，至少可從基本法第87條第1項第2句之職權（建置警察資訊及訊息事務中央單位）導出。

Ⅲ.反恐資料庫之基本架構合憲

透過系爭規定而建置之反恐資料庫，在基本架構的部分，符合基本法第2條第1項結合第1條第1項之資訊自主決定權。此種資料庫，其設置之目的係在調查與打擊國際恐怖主義範圍內作為資訊獲取之前哨，並在緊急事件中防止危害發生，原則上並非當然與比例原則相違。然而，其進一步之規範形塑，在個別規定的部分，亦須合於比例原則之要求。

1.反恐資料庫所追求之目的正當。其特別是要讓安全機關能夠迅速且容易知悉，其他安全機關是否掌有特定人士涉及國際恐怖主義之重要資訊。因此，其所意欲者，乃中介提供預備性基礎資訊，該預備性基礎資訊讓這些機關能更迅速順利地與其他機關進行資訊交換，且在緊急事件中亦得進行初步行為主導性之危害評估。立法者欲追求之目的，並非對所有安全機關掌有之個人資料作一般性之交換

，或解構其彼此間之任何資訊界限；若立法者真以此作為追求之目的，將會對目的拘束原則（Grundsatz der Zweckbindung）本身造成破壞，並從而立即不被允許。立法者所意欲並創設者，毋寧僅是有限度地使資訊交換更為容易，而此資訊交換，並未使專業法上有限度個別傳輸規定之基本標準受到影響，且在事務上侷限於打擊國際恐怖主義。雖然，「恐怖主義」之概念本身並不清楚。但是，從反恐資料庫法第2條第1句第1a款（其係何人應被儲存在資料庫內之核心規定）可以得知，反恐資料庫法係依循刑法第129a條之規定，並將「恐怖主義」理解為：以恐嚇民眾、敵對國家或國際組織之基本架構為目的，而有具體定義之重大犯罪。對此，在憲法上並無疑慮。

2.系爭規定對於達成上開目的，亦具有適當性與必要性。藉由反恐資料庫法第1條至第4條規定之儲存義務，基本資料之庫存因而產生，其供參與機關在反恐資料庫法第5條第1項及第6條第1項第1句之規範範圍內，使用於進一步之資訊查詢準備工作，並依反恐資料庫法第5條第2項及第6條第2項之規定，在特別緊急事件中提供參與機關有關防止特殊危害之資訊。除此之外，並無其他同樣能有效達成上開目的，且確保造成較小侵害的手段。

3.反恐資料庫法在基本架構的部分，亦與狹義比例原則相符。

狹義比例性之誡命，其要求立法者對基本權所為之限制，在整體衡量下，不得與基本權限制之合理化事由顯然輕重失衡。在規範之干預程度與立法者欲追求之目的間，以及在個人利益與公眾利益間，應取得適當之衡平（vgl. BVerfGE 100, 313 <375 f.>; 113, 348 <382>; 120, 378 <428>; stRspr）。

系爭規定造成之干預程度重大(a)。然而，與干預之基本權相對立者，乃重要之公共利益(b)。在進行權衡後，反恐資料庫之建置及其性質並未引發基本上之憲法疑慮；但是，對於資料庫之進一步形塑而言，則需要清楚且具有充分限制的規制，包含有效查驗資料庫使用之規定(c)。

a)由系爭規定所創設之資訊交換，影響力實屬重大。這樣的評價，從對此具有決定性而不能單獨觀察之基本權干預共同作用，可以導出：應被置於資料庫之資料，其重大程度與容許性之範圍，主要係依據資料庫之目的及性質而定，反之亦同，資料使用的重大程度，主要係取決於儲存義務之範圍。為數眾多且任務高度殊異之安全機關間，得以透過資料庫交換資訊，尤其尚包括情報機關與警察機關間之資訊交換，此乃使基本權干預程度加劇之關鍵因素(aa)。然而基本權

干預的嚴重程度，可透過以下因素而減輕：將儲存客體侷限於已蒐集之資料、將資料庫建置成以資訊獲取前哨為重點之聯合資料庫，以及將資料庫之建置目的侷限在調查與打擊國際恐怖主義(bb)。

aa)反恐資料庫使為數眾多且部分顯然擁有不同任務與職權之安全機關彼此間得交換資訊，此一因素升高了反恐資料庫的干預程度。就此尤其重要的是，反恐資料庫使情報機關與警察機關彼此間亦得進行資訊交換。

(1)不同機關各該被授予之蒐集與處理資料職權，其涉及個人資料之部分，係依機關之特殊任務而設計，並藉此受有限制。與此相應者，乃基於憲法之緣故，資料之使用必須遵循目的之拘束，且不得逕自傳輸給其他機關。對個人資料保護而言，依專業及聯邦體制之角度而區分各安全機關，亦因此形成了特別的基本權面向。不同安全機關間的資訊不得廣泛且自由地交換，這並非此等機關不符事務組織之展現，而是憲法藉由個人資料保護法上之目的拘束原則，基本上所預設且所意欲者。

然而，憲法上之資料目的拘束原則，若透過比基本權保護之利益更為重要之公共利益，可以取得合理化之事由，則並不排除可由立法者進行目的變更（vgl. BVerfGE 100, 313 <360>; 109, 279 <375 f.>; 110, 33 <69>）。對於評價不同機關間之資訊交換是否合乎比例，主要取決於不同的資訊關聯間是否具有可相提並論性。任務履行之任務、職權及類型越是殊異，則相應資料之交換也就越屬重大。因此，對於此等目的變更之合憲性判斷，特別重要的是，資料傳輸或輸入機關在蒐集資料時所受之拘束，以及查詢機關蒐集資料時所受之拘束，二者間之契合程度如何。據此，若從動用特定調查方法應受基本權限制的角度觀之，按照相應之法律依據，若資訊不得基於變更後之目的本身而被蒐集，或不得以該型態或方式被蒐集，則目的變更即非法之所許（vgl. BVerfGE 109, 279 <377>; 120, 351 <369>）。與此相應地，聯邦憲法法院一再作成裁判指出，要將藉由干預電信秘密自由而取得之資料作其他使用，僅在基於對原本之資料蒐集而言，亦屬合理之目的時，始屬合憲（vgl. BVerfGE 100, 313 <360, 389>; 109, 279 <375 f.>; 110, 33 <73>）。若資料係藉由干預資訊自主決定權而取得時，上開原則亦適用於資料處理之目的變更。憲法上對於資料蒐集、儲存及處理之要件，不得因以下情形而遭到破壞：因其任務緣故而適用較寬鬆要求之機關，以傳輸之途徑，將資料傳給應適用較嚴格要求之機關。

(2)依上所述，將情報機關與警察機關之資料合而為一，具有高度之

重要性，原則上應謹守憲法之嚴格界限。理由在於，警察機關與情報機關擁有顯然相互殊異之任務。相應地，關於任務履行之公開性，以及關於資料之蒐集，警察機關與情報機關有根本上之不同要求。

(aa)情報機關的任務為，在危害情狀尚未發生前，即採取調查措施。其對於資料之存取，旨在同時追求類型殊異且甚為廣泛之目的，諸如防止國內敵視憲法之行動、防止外國之情報組織在國內之活動、防止對「外交利益」之整體領域造成危害之暴力行動，或防止敵對國際和解之思維或敵對國際和平共同生活之行動（vgl. § 3 Abs. 1 BVerfSchG, § 1 Abs. 2 BNDG, § 1 Abs. 1 MADG sowie § 1 Abs. 1 i.V.m. § 3 Abs. 1 und § 5 Abs. 1 G 10）。情報機關必須就各種活動之危害可能性一般地予以注意並洞察之，而無關乎是否出現具體危害（BVerfGE 122, 120 <145>）。

相應於此種涉及前危害階段（Vorfeld）之任務多樣性，情報機關擁有廣泛的資訊蒐集職權，其具體之行為領域並無特別之定義，且各該應配置之手段亦缺乏詳細之安排。就憲法保護機關而言，其握有諸如運用線民與消息權威人士、觀察、記錄照片聲音、使用掩護身分之證件與牌照等隱密蒐集資訊之方法與工具（vgl. § 8 Abs. 2 BVerfSchG; § 6 Abs. 1 LVSG Baden-Württemberg）。依據對基本法第10條基本權限制法第5條之規定，聯邦情報局得基於資訊蒐集之目的，在特定情況下，透過策略性監控之工具，依特定之搜尋概念對國際電子通訊關係進行過濾（BVerfGE 100, 313 <368 ff.> zur Vorgängervorschrift des § 3 Abs. 1 G 10 a.F.）。儘管此處與程序標的無涉之憲法要求仍有諸多不同，但這些職權卻反映出情報機關任務的廣泛性，且彰顯出較低的干預門檻。此外，情報機關蒐集資料，原則上以隱密方式為之。資料蒐集公開原則對情報機關並不適用，且情報機關對當事人亦不負公開透明與告知義務。個人權利救濟之可能性，也從而相應降低。甚至，個人權利救濟部分係被政治審查所取代（vgl. Art. 10 Abs. 2 Satz 2 GG）。

為對治與衡平此一資訊蒐集職權之廣泛性，調查之目的即受有限制。儘管在不同情報機關間還會再作進一步之細分，但情報機關蒐集資訊之目的，本質上終究侷限於：為了能對安全情況作出政治上之預測，而就足以動搖國家整體之基本危害，予以監控並提出告知。其目的並不在於策略性地防止危害，而是提供政治上之資訊。因此，聯邦情報機關活動之任務，並非打擊犯罪本身，而是一般性地取得對德國外交及安全政策具重要性之外國情報。以情況報告、分析及告知

之形式，聯邦政府得及時獲悉危害情況，並－在政治上－予以解決（vgl. BVerfGE 100, 313 <371>）。與此相應地，憲法保護機關之調查，並非直接以預防或防止具體犯罪，或準備相對應之策略性措施為目的。憲法保護機關之任務，亦侷限於對政治上應負責之國家組織或公眾，負起告知義務（vgl. BVerfGE 130, 151 <206>）。

情報機關此一侷限在政治上前危害階段調查之任務，亦反映出其職權受有限制：其並無警察職權，且亦不得透過職務協助之途徑，請求警察機關採取情報機關不得採取之措施（vgl. § 8 Abs. 3 BVerfSchG, § 2 Abs. 3 BNDG, § 4 Abs. 2 MADG, § 3 Abs. 4 des Hessischen Gesetzes über das Landesamt für Verfassungsschutz [VerfSchutzG HE]）。在請求傳輸資料時，能被傳輸者，原則上僅限於被請求之機關已知，或能從一般可得接近之來源取得的資料（vgl. etwa § 17 Abs. 1 BVerfSchG – auch i.V.m. § 8 Abs. 3 Satz 2 BNDG und § 10 Abs. 4 MADG -, § 8 Abs. 2 Satz 2 VerfSchutzG HE, § 19 Abs. 1 i.V.m. § 7 Abs. 2 Satz 1 HmbVerfSchG）。

(bb)警察及安全機關之任務與職權，則與此有根本上之差異。警察及安全機關所負之義務為，預防、防止與追訴犯罪，以及防止公共安全與公共秩序之其他危害。其任務係由策略性的責任，以及特別係由對個人在必要時亦採取強制措施之職權形塑而成。就此而言，其任務在法律上受到不同之限制，並且透過實體與程序法上各種不同層次之規定，從而享有行為職權。儘管警察與安全機關的某些任務也在前危害階段，但原則上僅基於具體之事由，始賦予警察與安全機關得行使對個人之職權；其要件通常為：有犯罪嫌疑或危害之線索存在。這樣的任務輪廓，亦與警察及安全機關的資訊蒐集與處理職權相應相符。由於警察及安全機關的資訊蒐集與處理職權，畢竟係為強制措施預作準備，且會干預個人之自由，在法律本質上會比情報機關的資訊蒐集與處理職權更為嚴格及精確，並且在諸多方面相互區隔。相應地，此種與資料相關的職權，乃是－在許多個別之層次－，以諸如危害或犯罪嫌疑等具體線索作為要件。若立法者例外地允許在無任何線索的情況下，預防性地或是僅基於防範危害或犯罪發生之目的而蒐集資料，則必須具備特別之合理化事由，並符合憲法上較高的要求（vgl. BVerfGE 125, 260 <318 ff., 325 ff.>）。

與此相應地，原則上，警察以公開之方式採取行動，且主要係基於公開原則而處理資料。雖然警察機關任務之履行，在顯著的範圍內是以首先對當事人隱密進行調查作為前提。但

是，藉此僅有特定的、在有具體嫌疑時始得採取的調查措施或調查階段，受到隱密為之的保障，而此種調查措施並不使警察執行職務原則上之公開性受到影響。就此而言，尤其調查之資料在對個人採取伴隨之措施時－例如起訴或作成警察處分時－，即被揭露並使當事人獲得對此採取相關作為之機會。調查本身，如果可能的話，亦係以公開方式進行。在刑事程序中，對此之適例有：被告諸多之聽審、閱覽卷宗及防禦權、住宅搜索之公開實施（vgl. § 106 StPO）、使用預防性儲存資料之規定（vgl. BVerfGE 125, 260 <353>），以及在刑事程序之控訴，最終原則上應採取公開及言詞審理。與此相對地，運用臥底偵查者（§§ 110a ff. StPO）及藉助科技工具隱密蒐集資料（(§§ 100a ff. StPO），乃屬例外情形，且在符合特定條件下始受允許。與此相應地，警察同樣在危害防止領域內適用資料公開蒐集原則（vgl. § 21 Abs. 3 BPolG; § 19 Abs. 1 PolG Baden-Württemberg; Art. 30 Abs. 3 BayPAG）。

因此，法秩序採取如下區分：警察機關原則上公開執行職務，被要求進行策略性之任務履行，並受詳細之法律基礎指示，而情報機關原則上隱密執行職務，侷限在前危害階段為蒐集政治上之資訊，而進行監控與調查，並因此較無分殊化之法律基礎。至於秘密警察，在法秩序中未見規定。

(cc)基於上開區分原則，法律之規定若授權警察機關與情報機關得交換資訊，應符合較高之憲法要求。就此而言，從資訊自主決定基本權可以導出資訊區分原則。依據此一原則，情報機關與警察機關間，原則上不得交換資訊。要對資料區分予以限制，僅在例外情況下始受允許。若限制資料區分係基於策略性任務履行之目的，即構成特別嚴重之干預。為可能的策略性行動而在情報機關與警察機關間進行資訊交換，因此原則上必須以追求卓越之公益為目標，且該公益必須對如同情報機關使用資訊般在寬鬆條件下存取資訊，能予以合理化。這必須藉由充分具體及加重之干預門檻，且該門檻係以明確之法律規定為基礎，而予以確保；就此而言，獲取資訊之門檻亦不得遭到破壞。

bb)然而，反恐資料庫被形塑成本質上侷限在資訊獲取之前哨，且規定僅在急迫之例外情形，始可基於策略性履行任務之目的而為資料使用之聯合資料庫，其對基本權的干預程度因此降低。

(1)系爭規定將反恐資料庫形塑成如下的工具設備：－除反恐資料庫法第5條第2項及第6條第2項規定之緊急事件外－，並非直接為各該機關履行任務，尤其並非為策略性之目的而設，其僅供作進一步資料傳輸之基礎

。反恐資料庫雖然本身直接讓各參與機關得交換資料，其允許對一切基本資料進行檢索，且同意查詢機關得依反恐資料庫法第5條第1項第1句及第2句之規定，讀取反恐資料庫法第3條第1項第1a款的普通基本資料。但是，反恐資料庫法第6條第1項第1句規定，查詢機關對於該資料之使用，其目的僅限於審核該資料是否屬於被搜尋之人士，或為履行各該機關之任務而請求傳輸情報。所以，如此取得之資訊，原則上僅能基於以下之目的方得使用：為了決定是否以及應向何機關查詢進一步之資訊，以及為了替此種個別之傳輸請求提出更好之理由。與此相對地，要在緊急事件中基於請求而傳輸源自專業機關掌有之資料庫的資料，以及藉此亦為了達到策略性任務履行之目的，則各該相關之專業法律即屬重要。因此，關於反恐資料庫法第3條第1項第1a款的普通基本資料，反恐資料庫所允許者，並非為履行任務而交換資訊本身，其僅是對此預作準備而已。這更是適用於反恐資料庫法第3條第1項第1b款的延伸基本資料，各機關依據反恐資料庫法第5條第1項第4款，原則上僅能按照專業法律之傳輸規定讀取延伸基本資料。

因此，反恐資料庫法主要係以資料傳輸在專業法律上之基礎為據，並從中遵循法治國的界限。在此可以得出的結論是，無疑地，除了反恐資料庫法第5條第2項及第6條第2項外，對於調查及打擊恐怖主義而言，為直接使用資料而交換資料，僅在合於個別傳輸規定的法律要件下始得為之。其所採取者，乃是在前危害階段對於資訊獲取之前哨而言少量的，尤其是侷限於必要性標準的要求，而這些要求則是透過參照資料傳輸時不同之界限而來。然而，這些要求必須達到憲法上之要求，且至少對於情報機關與警察機關間之資料傳遞而言，不能以諸如任務履行之必要性或公共安全之維護等可相提並論的低門檻要件即為已足。

(2)反恐資料庫之功能，原則上侷限在供作資訊獲取之前哨，這明顯地降低了其對基本權干預的程度；然而，就算僅具此一功能，反恐資料庫對於基本權干預的程度仍屬重大。理由在於：雖然基於策略性任務履行之目的而使用資料，僅在其他資料傳輸規定允許時始得為之，但在履行此一任務之前的階段，反恐資料庫本身已造成機關情報間的直接交換。反恐資料庫允許查詢機關在出現吻合情況時，依反恐資料庫法第5條第1項第1句及第2句之規定，得一般性地讀取反恐資料庫法第3條第1項第1a款作為清楚資訊的基本資料，並且亦得檢索反恐資料庫法第3條第1項第1b款的延伸基本資料，但就此在出現吻合情況時，被傳遞者僅有資訊掌理機關之資訊

發現處證明，以及相符之普通基本資料而已。作為資訊獲取前哨的工具，反恐資料庫藉此使得專業法律上的資料交換更為容易，並且讓現有之個別傳輸規定實質上擁有改變性之影響力。這樣的影響力，將個別傳輸規定置於另外的、尚未將資訊予以告知前的場域，並使得情報在「原本不能或不可能」的情況下進行交換。因此，反恐資料庫成了這些專業法律上資料交換的前沿構成部分。

將資料納入這樣的資料庫內，會對當事人造成顯著不利之影響。被納入資料庫之人，應可預期，因查詢而被歸類到恐怖主義的範疇內，並且—藉由資料被納入反恐資料庫內，而更為容易的進一步傳輸請求—，將遭受隨之而來的不利益措施。如此的歸類結果，應該顯著可見，並且使個人處於對此一歸類無所知悉，且實際上不可能對之防禦的困難境地。資料交替地透過各該具體背景被記錄在資料庫內，且部分係以機關在本質上並不確定的單純預測及主觀評估為據，從而加深了干預之重大性。藉此，人民終究在對此本身無可歸責之理由的情況下，遭受顯著不利影響。不利益之措施原則上不能以系爭規定為據直接使用資料，而是結合了其他規定，方對資料使用造成間接效果，但這並未改變反恐資料庫升高了此種措施的機率。

(3)當反恐資料庫允許情報機關與警察機關間，得在緊急事件中交換資訊，且同時得直接為防止特殊危害與策略性之目的而使用資料，反恐資料庫即具備特別嚴重之干預程度。

b)反恐資料庫之建置，原則上符合禁止過度原則。對於當事人權利之干預重大程度而言，與其相對立之法益，乃如下之公共利益：為調查及打擊國際恐怖主義，而讓不同安全機關間進行有目的之資訊交換，並使其在重要之緊急事件中為防止危害而作成精確評估。

立法者得認為，為了調查與打擊國際恐怖主義之任務，建置一個旨在目的性資訊交換之中央聯合資料庫，乃高度重要之事。蓋鑑於履行此一任務之機關為數眾多，確保在這些機關間能成功地交換情報，實具特殊之重要性。現今，依據建置命令之規定，有超過60個以上的機關及警察機構參與反恐資料庫。姑且不論組織分殊化的詳細範圍應如何界定方屬適當，至少在聯邦國及權力分立原則下，為調查及打擊恐怖主義而生的資訊問題，即無法完全在組織層級予以解決。

為有效調查與打擊國際恐怖主義，當立法者認為個別傳輸條款尚不足以作為資訊交換之基礎時，得建置以資訊獲取之前哨為目的之協調性聯合資料庫，例如本案之反恐資料庫。對於以國際組織化之方式進行，且目的

在散布驚懼不安的恐怖犯罪予以防範及追訴，乃國家主管機關之特殊挑戰。由於此種犯罪特別難以掌握，且目標人士經常以高度神秘的方式行事，故安全機關要能以特殊之方式成功有效地履行任務，必須讓某一機關掌有之重要資訊，亦能被他機關接近使用，且透過匯集及調校源自混亂個別情報的不同資訊，而成為富含意義的資訊及狀況情景。顯而易見地，具備特殊架構之資料庫，若其內容包含被各機關關注人士之基本輪廓以及向哪些機關可取得哪些人士資料之證明，可根本改善任務之履行。同樣可接受之設想，尚有：各機關在急迫緊急事件中，為能作出初步之危害評估，以及藉此採取進一步之適當措施，應得直接使用其他機關之特定資訊。

在考慮此種資料庫的意義時，不應被忽視者，乃為民主自由秩序有效打擊恐怖主義具有高度重要性。具備恐怖主義特徵之犯罪，例如反恐資料庫法所規定者（見前述D. III. 1.），其目的在動搖國民整體，並就此包括以將他人肆無忌憚地當成工具之方式，攻擊第三人之身體與生命。其所針對者，乃憲法秩序之支柱以及國民整體。這樣的攻擊，在本國憲法秩序要求下，不能被視為是戰爭或無庸重視法治國要求的例外狀態，而應該將其視為犯罪並透過法治國之方法予以打擊。反之，與此相應地，在比例性考量的法治國範圍內打擊恐怖主義，應被認為具有高度重要性（vgl. BVerfGE 115, 320 <357 f.>）。

c)鑑於其間存在相互對立之利益，將反恐資料庫的基本架構廣泛視為資訊獲取前哨之工具，以及緊急事件危害評估之行為導引資訊來源，並無憲法上之疑慮。然而，資料庫之規定，僅在以下情況，始符合狹義比例性原則：關於應蒐集之資料及其使用可能性的規範必須明確，且就此以充分有限的方式予以安排設計，並置入及注意遵守加重之審查要求（BVerfGE 125, 260 <325>）。

aa)在憲法上不應受到指責者，首先為就基本架構而言，立法者將反恐資料庫建置為資訊獲取前哨之聯合資料庫。於此一資料庫中，關於可能與國際恐怖主義親近之特定人士，其具識別性之基本資料應予納入，而參與機關得基於資訊獲取前哨之目的使用之，在出發點上並非不符合比例原則。由於其僅係為法律上有限之個別傳輸預作準備，故透過打擊恐怖主義之任務，即可合理化此種情報機關與警察機關之資訊匯集。同樣沒有深切疑慮者，乃反之在資料庫中，於具識別性之基本資料外，尚儲存進一步在內容上富含意義的所謂延伸基本資料。這些－由於具有高度之人格重要性，故參與機關原則上不得將之作為清楚資訊，但也許會供隱密搜尋之目的

而使用之一資料，其功能也同樣在於，使資訊能依專業法律之規定進行有目的性之交換，並藉由有效打擊恐怖主義之目的，從而基本上能被合理化。

然而，詳盡清楚地對資訊交換予以規範，且須有充足之設限，此乃設計資料庫所必須。這對於參與機關之規定、應納入資料庫之人士及其資料，以及使用該資料之進一步規定，亦有適用。亦應受到確保者，尚包括有效之查驗（見下述D. IV.）。

bb)由於防止恐怖攻擊具有重大意義，所以立法者意欲在此之外，藉由反恐資料庫，提供讓各機關於緊急事件中亦能作成初步行為導引性危害評估之資料來源，也同樣不應受到指責。然而，在這種情況下進行資訊交換，並非僅係以專業法律為據而創設出資訊蒐集之前哨，且亦直接有助於策略性目的之實現，故為特別嚴重之干預。惟其並不當然牴觸禁止過度原則。然具關鍵性的是，法定之干預門檻，關於急迫性與受威脅之法益，係以顧及此等特殊干預程度之方式，而作有限度之設計安排（見下述D. IV. 4. d）。

IV.反恐資料庫法之個別規定違憲

由這些原則出發，系爭規定從諸多角度觀之，並未達到反恐資料庫之設計應充分明確且符合禁止過度原則之要求。因此，系爭規定侵害了資訊自主決定權。

1.反恐資料庫法第1條第2項關於其他警察執行機關參與反恐資料庫之規定，不符明確性之要求。

a)明確性原則旨在確保，統治權與行政權能於法律中找到調控性與受有限制之行為標準，且法院能對之實施有效法律審查。此外，規範之明確性與清晰性，亦使受影響之人民能為可能之侵益措施預作準備（vgl. BVerfGE 110, 33 <52 ff.>; 113, 348 <375 ff.>; 120, 378 <407 f.>）。立法者只要對採取之時機、目的及範圍自為規定，則其可依基本法第80條第1項，將這些標準之詳細規定授權行政機關透過法規命令定之。惟就此同樣涉及之實質意義法律基礎，不僅在行政內部對行政機關具有拘束力，其作為外部法，亦得拘束人民與法院。明確性之要求與基本權之法律保留具有密切關係，依據基本權之法律保留，對基本權之干預僅能透過法律或以法律為基礎而為之。藉此可得確保的是：首先，基本權干預之範圍，其根本之觀點能在議會程序中公開地於兼任與非兼任政府官員之議員的參與下受到討論；再者，其進一步之一般抽象精確規定，由行政權依據基本法第80條第1項，以可得認識之方式予以明示，而被當成議會決定之具體化；復次，就此具有決定性之規範，能以對任何人均具有拘束力之方式，且透過簽

署與頒布而以可得認識之方式對外公告。法律保留之民主與法治國功能，在此相互交融。法律規定應適用何種程度之明確性要求，取決於該規定或以該規定為基礎而造成之基本權干預強度如何。

依據這些標準，參與反恐資料庫之機關，應直接透過法律，或以法律為據而透過法規命令確定之。哪些機關應將其資料存入資料庫，哪些機關有權讀取資料庫之資料，均關鍵性地決定了資料庫的範圍與內容，以及對資料為進一步使用的程度。在此所涉及者，乃須具備清晰性及明確性，而對外發生效力之規定的規範要素。尤其，讓任何其他警察執行機關加入反恐資料庫法的資訊集團，加深對於情報機關與警察機關資訊區分的突破。情報機關與警察機關間的資訊交換，使連結反恐資料庫法的基本權干預，其嚴重性因而升高（D. III. 3. a) aa）。突破情報機關與警察機關之資訊區分，而讓其他警察執行機關參與反恐資料庫，此等規定，亦於組織法上實現了前述之情形。有關參與機關之規定，因此成為反恐資料庫對基本權之特殊危險潛能的核心。

b)反恐資料庫法第1條第2項本身，以及結合反恐資料庫法第12條規定之建置命令，均未達到其他警察執行機關參與反恐資料庫之法律規定應有的特殊要求。

aa)在反恐資料庫法第1條第2項中，並無充分明確使參與機關得直接從中確定的法律規定。明確性之要求，雖然原則上並未排除立法者僅以一般抽象之方式，－依資料庫之類型與物件－規定有權讀取資料庫之機關。若可直接從法律中充分明確地推斷出參與機關之範圍，則雖未清楚舉出具體之機關，亦無大礙（vgl. BVerfGE 130, 151 <199, 203>）。然而，現行之規定並非如此。反恐資料庫法第1條第2項對於參與機關之規定，僅以廣泛且價值開放之標準為依據。其所指示者，乃他方面之任務分派以及必要性與相當性之觀點，而後者使參與機關最終係為安全政策之有利考量而確定。就此而言，一如由其規範關聯性可得知，該條文亦未被立法者理解為：該條文應當對參與機關自為終局之規定。毋寧，從反恐資料庫法第12條第2款要求透過建置命令而確定參與機關，以及從反恐資料庫法第1條第2項與第12條－非無矛盾地－要求會商、會同、同意，可以得知，立法者所意欲者，並非透過這些條文直接親自確定參與機關之範圍，而是讓參與機關的範圍依照行政權決定之專業標準而確定之。這可以從依據建置命令之現況，僅有三個邦的其他警察執行機關參與反恐資料庫，而獲得證明。無論如何，著眼於反恐資料庫之干預程度，參與機關之範圍如此開放，並未

達到憲法之要求。

bb)參與機關之充分明確規定，亦無法從反恐資料庫法第1條第2項結合反恐資料庫法第12條第2款之建置命令而得出。雖然，委由行政機關對參與機關作成終局確定，並無原則上之疑慮。但是，有鑑於反恐資料庫參與機關之規定對基本權具有特殊重要性，故建置命令尚不足以確定參與機關，蓋建置命令作為純粹之行政規則，對當事人及法院均無法律上之拘束效力，且在法律形式上亦未經簽署與發布。若立法者意欲讓行政權決定參與機關，則依基本法第80條第1項之規定，在此應採取法規命令之形式。

2.對被資料庫掌握人士範圍予以確定之規定，並非從任何角度觀之均符合憲法之要求。這些規定中的若干條文，違反明確性原則與禁止過度原則。其他條文則須作緊縮性之合憲性解釋。

a)反恐資料庫法第2條第1項第1a款並無可受批評質疑之處。此一規定係在指示蒐集可能加入或資助恐怖組織之人士的資料，並從而包括有效防止恐怖主義之焦點人士。此一規定所連結之刑法規範，係將可罰行為遠遠提前至法益侵害前之階段，且就此有「事實依據」－如果有的話，也僅係對支助行為－即為已足，藉此，此一規定雖然讓行政機關享有主觀評估之廣泛空間，並創設出無法衡量性的廣大領域。但是，除了緊急事件外，反恐資料庫僅作為資訊獲取之前哨，且應當在此範圍內使嫌疑與危害狀態之不確定評估於調查前之階段即能被摒棄或證立，在此一框架內，反恐資料庫如此之設計安排尚可被容忍。在適當之解釋下，這些構成要件要素至少充分確定，資料之儲存不能單純僅以臆測為據。尤其是，事實依據須能回溯連結至具體情報，且支助之概念－亦從主觀要件來看－應與其在刑法第129a條第5項第1句之意義作相同理解（vgl. BTDrucks 16/2950, S. 15）。最後，在個案中對於資料儲存之合比例性存有疑義時，反恐資料庫法第2條第1句結尾對於儲存義務作一般性限制之條款能發揮修正之功能，蓋依其規定，獲悉資料，必須對調查或打擊與德國相關之國際恐怖主義具有必要性，始得為之。雖然，此一條款因具有開放性，而無法治癒一開始本身即不明確或原則上太過廣泛之儲存義務。但是，如現行規定所示，只要應予儲存之資料原則上能妥為確定，則此一條款對讓典型之個案獲致憲法上有力之解答，即屬適當。

b)反恐資料庫法第2條第1句第1b款，其在支助恐怖組織的觀點下，擴張被反恐資料庫掌握人士的範圍，部分與禁止過度原則不符而違憲。

aa)當條文包含歸屬於對恐怖組織提供支助之團體的人士，在此範圍

內，條文並不存有疑慮。對於合比例性的評價而言，並不區分支助行為係以個人或集體方式為之。與此相應地，儲存這些人士之資料，乃一如依據反恐資料庫法第2條第1句第1a款（後半段）儲存支助恐怖組織者之資料，以相同之方式為之而合乎比例。

bb)相對於此，條文亦包含對支助性組織僅提供支助之人士，則被反恐資料庫掌握人士的範圍即再次擴張。在此一條文中，並未要求與恐怖主義間須具備主觀聯繫。依其文句以及未偏離文義之意義，此一條文規定之儲存義務，亦涉及以下人士：該人士遠在危害前階段，以及可能對恐怖主義之關聯性毫不知情的情況下，支助由其眼中看來並無犯罪嫌疑之團體，例如支助清真寺團體之幼兒園，然該團體卻被行政機關認為涉嫌資助恐怖組織。將恐怖組織的最廣泛影響範圍予以納入，這樣的規範開放性，牴觸規範明確性原則，並與禁止過度原則不符。當有事實足證，該支助係有意贊助此等團體所為之恐怖主義支助性活動，雖然立法者可自行決定，將純粹對具支助性團體提供支助列為儲存資料之理由。但是，立法者對此若有必要，應以符合規範明確性原則之方式載明於條文中。從反恐資料庫法第2條第1句第1b款的文義看來，無法得知是否有此一意思。有鑑於反恐資料庫之運作方式通常不為當事人所知，且亦不受法官審查，對此不得存有任何不明確性。所以，在此亦不能作合憲性解釋。

c)反恐資料庫法第2條第1句第2款與憲法未盡相符。將可能與恐怖主義親近之個人包含在內的條文，其連結一連串多義及可能廣義之法律概念。關於非法暴力以及故意引致此種暴力之概念，由於在本庭中票數相同，故不能確認其違憲；依本庭四位法官所持與判決結論相同（聯邦憲法法院法第15條第4項第3句）之見解，這些概念之使用，只要未過度將其他意義附加在概念上，即與基本法相符（aa）。依本庭其他四位法官所持不同於判決結論（聯邦憲法法院法第15條第4項第3句）之見解，應就此進一步宣告此一條文違憲（bb）。相較之下，依本庭一致之見解，此一條文意義下的單純支持暴力，尚不能使人被納入反恐資料庫。此一條文就此牴觸禁止過度原則而違憲（cc）。

aa)(1)此一條文主要係配合非法暴力之概念。雖然，在法秩序的其他部分為此一概念附加了相當廣泛的意義，而該廣泛意義對作為把當事人界定成與恐怖主義親近者的前哨而言，太不清楚，以致於不能以合乎比例原則之方式限制當事人之範圍，且在憲法上亦無法忍受對當事人之資料進行儲存。聯邦憲法法院在憲法上不予指責地肯認：刑事法院針對封鎖行動就

強制罪構成要件（刑法第240條）進行評價時認為，藉由將綁著人的金屬鎖鍊固定在入口門柱上，而施展體力，已構成暴力之使用，理由在於，此一鎖鍊固定手段，讓抗議活動有了使第三人屈服於抗議活動者意志的超乎心理強制力（vgl. BVerfGE 104, 92 <102>）。然而，依據安全機關在言詞審理時之陳述，實務上係以嚴格方式理解非法暴力之概念。在此處應受審查的法律範圍內，對非法暴力概念作刑法強制罪構成要件意義下的廣義解釋，恐與法律之文義及目的不符。相應於反恐資料庫對抗恐怖犯罪行為之目的，非法暴力概念毋寧應理解為：僅包含直接針對生命及身體，或透過使用有害公眾之方法而為之暴力。在這樣的解釋下，透過反恐資料庫法第2條第1句第2款之暴力概念而被掌握的人士範圍，其合比例性即無憲法上之疑慮。

(2)另外，依據反恐資料庫法第2條第1句第2款之規定，被納入規範者，不但包括使用、支助及預備暴力之人士，亦及於僅係支持或透過其行為故意引致暴力之人士。若刑法用語意義下的間接故意（Eventualvorsatz）被認為亦足以該當故意引致暴力，則上開規定即創造出不合比例的廣泛干預可能性。若故意引致暴力在此附加之意義為僅包含意圖引致暴力，即未違反比例原則。

bb)依據本庭其他四位法官所持與判決結論不同（聯邦憲法法院法第15條第4項第3句）之見解，反恐資料庫法第2條第1句第2款由於欠缺明確性且射程範圍過於廣泛，應全部被宣告為違憲。即便將非法暴力以及故意引致之概念作不同於刑法一般眾所周知概念性的狹義解釋，亦無法避免上開條文被宣告違憲之命運。如此使用合憲性解釋，可謂前後矛盾，且解消了個人資料保護法上的明確性要求。

(1)一如與判決結論相同之本庭法官所見，此一條文之關鍵性標記具有多重意義，且在法秩序之其他部分－亦即在對法學慣用之概念而言，具基礎性的刑法領域－以在反恐資料庫的關聯性下不符比例原則及禁止過度原則之方式，被廣泛理解。此一條文即是如此一般性地使用非法暴力之概念。按照被採用的刑法定義，對此只要在道路上設置有形之障礙，即為已足（vgl. BVerfGE 104, 92 <101 f.>; BVerfGK 18, 365 <369>）。依此－在具有相應之主題關聯性時－，以鎖鍊固定之手段實施單純的封鎖行動，即會被納入反恐資料庫中。另一個額外擴張之處在於，對於資料儲存而言，只要故意引致暴力即為已足。依據通行的刑法故意理論，若當事人認識到，其發表之圖文會－即使不符其意願，亦同－促使第三人為暴力行為，即合於故意引致暴力之概念。如此之解

釋，亦未違背原意：蓋其與文義及一般眾所周知且在規範本身指向應參照刑法規範之關聯性下，應採取的刑法解釋原則相承。從安全機關的角度看來，如此之解釋亦顯得具有意義且引人注目：此等解釋，使從恐怖主義純粹外環又再次廣泛向外延伸而出之人士圈，一開始原則上就被資料庫之適用範圍所涵蓋。此等解釋，恐怕要動用反恐資料庫法第2條最後的分離條款（salvatorische Klausel）後，才能依相當主觀之標準而受有限制，蓋依該分離條款之規定，僅在獲悉資料對履行任務係屬必要時，始得儲存資料。

(2)在此不考慮使用深入細緻的合憲性解釋。

(a)就反恐資料庫法第2條第1句第2款之規定，不考慮採取合憲性解釋，因為「非法暴力」此一居於規範核心之概念，係被立法者有意廣泛且開放性選用。在立法過程中，暴力概念模糊且射程範圍過廣，遭到明顯的批評（BTPlenarprotokoll 16/71, S. 7100; BT Innenausschuss, Protokoll Nr. 16/24, S. 55; A-Drucks 16(4)131 D, S. 10; A-Drucks 16(4)131 J, S. 10），並且，為限制此一概念，甚至還提出嚴格之相反建議，依該建議，仿照刑法第129a條第2項之規定，非法暴力僅在以下情形始得作為資料儲存之開端：「若對此可確定，人民遭到顯著方式之恐嚇、機關或國際組織遭到非法脅迫、抑或國家或國際組織之政治、憲法、經濟或社會基本結構遭到排除或顯著侵害，以及人的行為對國家或國際組織具有顯著損害之危險」（vgl. BTDrucks 16/3642, S. 14 f.）。因此，有嘗試將暴力概念以近似國際或歐洲為打擊恐怖主義而設之規定般予以設限者（vgl. Rahmenbeschluss des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung, ABl. L 164/3 vom 22. Juni 2002, Art. 1; Entwurf einer Allgemeinen Konvention zum internationalen Terrorismus, in: Measures to eliminate international terrorism, Report of the Working Group vom 3. November 2010, UN Doc. A/C.6/65/L.10.）。然而，立法者對此卻有意識地決定不予理會－其顯然有意給予安全機關寬廣的自由空間。如此之決定，不能以合憲性解釋之途徑予以改正。

(b)同樣基於原則上之考量，合憲性解釋在此應予排除。當法律之干預基礎以上述方式採取開放性之措辭，且以眾所周知的概念定義作為基礎時，未背離本意地採取如此之廣義解釋，則此一法律規定作為資料處理之基礎，如其現行所指涉者，並不符合規範清晰性原則與比例原則。規範清晰性原則之目的，不偏不倚即在於，要求立法者就基本權干預之要件自為

充分清楚且足以確保禁止過度原則之決定。若立法者未盡此一要求，則聯邦憲法法院不能透過合憲性解釋治癒此一瑕疵。動用合憲性解釋－藉此，理應可以限制任何空白授權－，將使個人資料保護法上對於明確性之要求及其標準實質上被解消。這必然會造成前後矛盾之現象：哪些開放性的法律概念得採取合憲性解釋，哪些卻又不能採取合憲性解釋，幾乎欠缺可得理解的界限。目前的規定也是如此：為何反恐資料庫法第2條第1句第2款的「暴力」，以及「故意引致」之概念，應當採取合憲性之嚴格解釋，而同一條文中的「支持」，或反恐資料庫法第2條第1句第1b款「對支助性之團體予以支助」概念，卻相反地不採合憲性之嚴格解釋，並無具說服力之理由。

上述意見，不能以法秩序亦使用其他的不確定法律概念，以及規範總是需要解釋等理由而反駁之；而與此相應地，暴力概念在不同的關聯性下，具有不同的意義，這也不能作為反對之託辭。理由在於：明確性之要求以及法律基礎充分清晰之界限，依各事務領域與規範關聯性而有所不同。根據聯邦憲法法院向來之裁判，在個人資料保護法的領域，明確性及規範清晰性之要求程度特別高（vgl. BVerfGE 65, 1 <46>; 118, 168 <187>; 120, 378 <408>），對於尚在調查前之階段即規制安全機關間資料交換的反恐資料庫而言，尤其應適用這樣的高度要求。這是因為，不同於諸如透過行政處分（其乃行政機關對個別人民採取之措施，並附記理由，且在個案中得受法院審查）而執行法律，依反恐資料庫法所為之資料處理係在人民不能直接察覺的情況下進行。其為非形式化之行為，並不對當事人附記理由，且通常也無法受到法院審查。干預基礎之某種程度的不明確性，可在兩相對立的交互影響作用中，並透過按部就班的解釋規則發展而被具體化，相異於此，此處資料處理之界限必須對當事人而言可信任地，而對安全機關而言盡可能地，以本身可得認識之方式直接從法律規定中得出。

此種基本權上個人資料保護的加重明確性要求，並非植基於對安全機關的高度不信任。毋寧，這些要求正可為安全機關履行任務尚未形式化或僅微量形式化之階段（在此一階段，資料處理往往扮演重要角色），確保其具有清楚明確之條件（這些條件盡可能地明確指引機關履行其高要求之任務，並且亦減輕所受之質疑）。

(c)本案亦不能以尊重立法者為由，而作出合憲性解釋。誠然，立法者透過反恐資料庫法所實現者，乃高要求且分殊化的規範計畫，而此一規範計畫之特色，在許多方面係透過法治國之節制，以及認真致力於確保適

當個人資料保護所彰顯。但是，對轉化此一規範計畫的具體條文進行憲法上之評判，不能以立法者在政策上努力之整體評價為準據。法院的任務毋寧在於，讓憲法上之標準與此無涉地詳盡發揮作用，並確保在總體利益中具基礎性之法治國性格，不會藉由開放的個別規定而再度離散。毋寧，尊重立法者，其要求的反倒是，法院慮及個人資料保護法上要求之特有限制，而宣告條文違憲：與其將從規範目的觀之，或許可想而知，但卻顯非立法者所欲之規定－至少暫時地－透過解釋，認為係立法者之意思而予以尊重，倒不如以維護立法者權限之方式，而將重要的界限劃定任務退回給立法者。這對於立法者而言，也看不出來基於專業或其他規範條件之理由而有特別困難之處。

cc)支持暴力此一要素，射程範圍特別廣泛。立法者在此採取的，僅係內在態度，而該內在態度無須表現出支助暴力之行為。此一要素之使用與憲法不符，本條文因此違憲。此一標準的射程範圍原則上太過廣泛，亦無法透過合憲性解釋之途徑予以排除。雖然立法理由所舉之例，僅有仇恨鼓吹者（當其在公然鼓吹仇恨及暴力的情況下，將其納入資料庫中，於憲法上並無原則性之疑慮）。但是，原則上涵蓋範圍廣泛的文義，並不侷限於此。毋寧，此一文義容易讓人理解為，端視其相應之態度如何。就此而言，按照文義，由事實上之根據可推斷出支持暴力，即為已足。此一標準，直接針對內心信念，並從而觀察個人不受支配的內心領域，與如此之標準連接，對於自由權（尤其是信仰及意見自由）的行使而言，將足以發生恫嚇效力。法律在此讓主觀之信念本身成為標準，並以個人僅能有限支配且透過守法行為無法影響之標準作為基礎。依據如此之標準，將人們納入反恐資料庫中，並不符合禁止過度原則。就此點而言，反恐資料庫法第2條第1句第2款違憲。

d)反恐資料庫法第2條第1句第3款亦屬違憲。此一規定將聯繫者納入，不符合明確性原則及禁止過度原則。

反恐資料庫法第2條第1句第3款規定，與前兩款規定之人士單純聯繫者，亦應被納入反恐資料庫內。法律將這些聯繫者當作自成一類群組，參與機關透過相同方式得接近使用其資料，一如使用其他被納入資料庫之人的資料。應被納入資料庫者，尚包括對涉及恐怖主義之主要人士毫不知情的聯繫者－雖然就此僅止於聯繫者之普通基本資料（反恐資料庫法第3條第1項第1a句）。若聯繫者對涉及恐怖主義之主要人士知情，則除此之外，其延伸基本資料亦應納入資料庫中（反恐資料庫法第3條第1項第1b句）。

將聯繫者當作自成一類之群組而納入亦包含清楚資訊的資料交換範圍中，此等規定並不符合明確性之要求。哪些人事實上應納入資料庫中，就其依據而言無法預見。即便立法者排除僅係短暫或偶然聯繫者，但規範除此之外所包含者，則為與條文第1款及第2款列舉人士之整體社會生活領域有關之人－包括與其私領域有關之人，以及在職業上與商務上有所聯繫之人。顯然地，一切以此為據，而在考慮範圍內之人，並非都應當被納入反恐資料庫中。在言詞審理時已指出的是，現今事實上被包含之聯繫者人數微少，且關於「非居心叵測」之聯繫者僅有141人被掌握而已。一開始定義過於寬鬆的群組，毋寧依據反恐資料庫法第2條第1句最後結尾條款之規定（依此據此一結尾條款，獲悉相關資料必須對防止恐怖主義具有必要性），再度廣泛地受有限制。但是，機關卻未能獲得充分明確之標準。毋寧，確定何等資料應予儲存，最終仍委諸機關之自由評估。

由於可能透過規定而被涵蓋的人士範圍幾乎不可預見，故其違反禁止過度原則。然而，在憲法上，並未原則性地禁止將聯繫者之資料納入反恐資料庫中。不在條文第1款及第2款範圍內，從而本身並非恐怖活動潛在支助者，此等人士若能有助取得與恐怖主義接近之主要人物資訊，則通常依資料庫之目的，此等人士即成為受到關注之人。法律之設計，亦以此為導向。就此而言，可能的設計諸如：將聯繫者及其少數基本資料包含在內，且將這些資料－如同現行反恐資料庫法第3條第1項第1b款oo之規定－當成與恐怖主義接近之主要人物的相關資訊，而以僅能隱密檢索之方式儲存。無論如何，透過以主要人物為目標之查詢，可以查詢到聯繫者，並且也能依據聯繫者之姓名本身而進行隱密檢索（但此一隱密檢索在出現吻合情況時，僅會顯示掌有該資訊之機關以及該資訊之檔案編號）（亦參見後述D. IV. 4. c）。這樣的規定，儘管可能被涵蓋的人士範圍廣泛，但由於其干預程度明顯降低，故似合於明確性之要求，蓋明確性之要求，亦端視有疑問之基本權干預其干預程度如何（vgl. BVerfGE 59, 104 <114>; 86, 288 <311>; 117, 71 <111>）。這無關乎所涉之聯繫者，是否對恐怖主義相關之主要人物知情。

3.反恐資料庫法第3條第1項第1a及b款關於被蒐集資料範圍之規定，在憲法上不應受到非難。然而，就反恐資料庫法第3條第1項第1b款而言，需有（在規範中已部分含有之）補充性規定，而要求行政機關為進一步之具體化。

a)反恐資料庫法第3條第1項第1款a部分之基本資料規定，在憲法上

不應受到批評非難。

然而，這些資料的範圍以及陳述力，非常顯著。由於透過這些資料，不僅現今之資訊，就連先前之名字、住址、國籍、證件照片均會被掌握，故其能使當事人部分之生活途徑可得辨識。此外，條文包含了敏感性資料。尤其是特殊身體特徵之資料，即屬於此等資料。雖然依據適切之理解，僅有藉助鑑識措施方得確定的外部特徵始應被通曉，但具高度屬人性之特徵卻從而遭到掌握。相類似者，尚有應儲存於資料庫中，依據事件而涉及出身原籍的資訊。雖然條文並未區別性地以及可能帶有標籤意味地連結特定之出身原籍，而係對所有被掌握人士的相應資訊一視同仁地予以規定。但就此而言，這些資訊並非無關緊要。

儘管如此，此一規定仍合於禁止過度原則。關於資料之規定，具有充分之明確性，且整體看來其範圍亦合乎比例。藉由此一規定所建構者，乃－限於可能與恐怖主義親近之人士（見上述D. IV. 2.）－對當事人進行更精確辨識之基本輪廓，而此一基本輪廓雖然具有陳述力，但終究侷限於外在參數。基於打擊恐怖主義之意義，這在將情報機關之資料予以納入的情況下，於憲法上亦不應受到非難。就此應再次被考慮的是，資料並非受到重新之探查，資料庫之目的並非調查性地建構關於基本資料之全然輪廓，而僅是匯集個別機關已掌有之資料。然而，資料之儲存，就結果而言，絕大部分可能也會將終究已經證明，與恐怖主義無關之人士牽涉在內。但這對於讓機關得匯集可能關乎恐怖活動之資料的資料庫而言，乃不可避免之事。由於可能被恐怖暴力行為威脅的法益位階崇高，也由於國際恐怖活動之結構若干部分相當難以查明（見上述D. III. 3. b），因此藉由匯集反恐資料庫法第3條第1項第1a款規定之基本資料，將打擊恐怖主義作如此之提前，並非法治國所不許。

b)依反恐資料庫法第3條第1項第1b款應予儲存之延伸基本資料（對參與機關而言，原則上僅供隱密檢索，且在發生緊急事件時供作清楚資訊使用），其範圍在憲法上亦未受到與禁止過度原則有關之批評。然而，立法者必須確保，對於適用重要之具體化規定而言，那些透過行政權進一步予以一般抽象之具體化後，始能得知其內容輪廓的構成要件要素，能以可理解的方式載明並對外發布。

aa)反恐資料庫法第3條第1項第1b款aa至ff、jj、ll、mm、oo、pp以及qq，並無憲法上之疑慮。

(1)依此條文而被置於反恐資料庫中的特徵要素，立法者已為足夠明確之規定，且無庸透過行政權而為一般抽象之具體化中間措施。儲存義務

之範圍直接可得認識，且其適用能直接了當被監督機關或法院審查檢驗。無關緊要的是，特徵要素有部分係透過電腦程式以標準化之形式儲存。機關內部之標準規定，就其意義而言，即係透過解釋性行政規則而為之規定。無論如何，機關在適用反恐資料庫法第3條第1項第1b款rr之規定，亦得補充現有之標準，即是如此。

(2)根據此一條文而應予蒐集之特徵要素，在對其範圍及陳述內容進行觀察後，可認為與禁止過度原則相符。

然而，這些資料可能的陳述力，指涉廣泛。透過電信連線、電信終端設備、電子郵件地址以及銀行帳戶，實際上所有現代通訊方法與所有大宗金融交易之座標圖均遭掌握；同時，對使用之交通工具予以儲存，亦從而讓私人之行動遭到觀察。此等資料，乃個人通訊大部分之基礎資料。這些資料所連結者，此外尚有教育背景資訊、個人工作能力資訊，以及得對個人生平進行觀察之個人事態。結合不同之資訊，尤其是結合普通基本資料，得以匯集與當事人有關，且能易於將其連結至通緝令之詳細陳述。這具有特別之重要性，因為在基於不同蒐集關聯性而產生之資料庫中，情報機關之資料與警察機關之資料亦被融匯於一爐（見上述D. III. 3. a) aa）。

反之，在此亦應考量的是，條文所規定者，並非新資料之蒐集，而僅是個別機關已有資料之匯集。尤其，與此一干預嚴重程度所相對者，乃有效調查及打擊國際恐怖主義此一非常重要之公益（見上述D. III. 3. b）。由於恐怖犯罪對於個人專屬法益以及整體法秩序造成極為高度之危害，故對這些資料進行匯集式之儲存，若與立法者欲追求之目的作整體衡量，符合禁止過度原則。

此等立法目的，首先係讓這些資料在個案中，能為行為導引性之初步危害評估，而供作清楚資訊使用。只要立法者意欲藉此讓警察在發生特別緊急之危害情況時，得採取相關措施—且限制僅在此等重要緊急事件中，始得使用資料（如反恐資料庫法第5條第2項，見後述D. IV. 4. d）—，則將這些由不同機構掌有之資料作匯集式之儲備，在憲法上即得阻卻違憲。

此等立法目的，亦包括其他透過這些資料之儲存而欲追求之目的，也就是以資訊儲存之前哨為目的而隱密使用資料。這是因為，正由於透過這些資料而可能採取的調查措施，就內容而言相當廣泛，所以此等資料能在本質上較成功地創設出為防止危害而為之調查，且儲備此等資料亦具有重要之公共利益。因為資料侷限於與恐怖主義親近人士之範圍以及已遭蒐集之資料，故就資料之儲備，原則上不應予以非難。對延伸基本資料而言，

重要的是，其僅基於資訊儲存前哨之目的，而以隱密方式儲備給機關，供作清楚資訊使用，且僅依專業法律之規定始得傳輸。雖然，這根本未影響其干預之程度。就算是以隱密方式儲備，也能在原先的關聯性之外，透過不同資料彼此間以及與其他資訊間之調校，而使資料可能被利用，並可產生藉以讓該資料在專業法律上可能且得以傳輸的新情報（見上述D. III. 3. a) bb) [2]）。但是，資料之儲備僅能隱密為之，藉此卻明顯降低了資料儲存之干預程度。這是因為，以隱密方式儲備資料時—若資料使用系統採用一致性之設計（見下述D. IV. 4. c）—，即能確保，從事調查之機關透過查詢尚不能直接得知資料本身，而必須依據專業法律之傳輸條款及其各自不同的干預門檻與要件，始能知悉資料之內容。所以，由此資料而得出之個人資訊，充其量係從吻合者之資訊推斷而出，但並非出自於該資料之傳輸本身。以此等方式，侷限於為交換資料預作準備，而隱密使用資料，在此一目的下，對資料進行匯集式之儲存，亦得包括在此容有疑義之延伸基本資料。

bb)反恐資料庫法第3條第1項第1b款gg、hh、ii、kk、nn規定之特徵要素儲存，亦屬合憲。但是，對於這些特徵要素，立法者必須確保，對其使用具必要性之具體化規定，應由行政機關載明並對外發布。

(1)這些條文符合明確性之要求。

然而，這些規定特別需要被具體化，且此係因為這些規定對於人民而言，尚不能終局性地從中得知，哪些資訊事實上會被納入資料庫中。諸如預備及實施恐怖犯罪之技能、在公共官方建築所為之活動、與恐怖主義親近者會面之地點及地域，其光譜範圍特別廣泛。在族別以及宗教信仰之歸屬此一項目下，有哪些資訊應當被納入，由於有各種不同之具體化可能性，故難以單純從規範中評估。依立法者之理解，何等資料應納入資料庫，其精確之認定尚非終局性地見諸法律規定本身，而須待安全機關進一步予以一般抽象之具體化後（安全機關所為之具體化，首先應透過反恐資料庫法第12條第3項之建置命令，並繼之應在標準化之電腦程式中，確定哪些資料應納入資料庫），始告確立（vgl. BTDrucks 16/2950, S. 17）。姑且不論反恐資料庫法第3條第1項所設計者，乃嚴格之儲存義務，立法者透過此等規定，顯然無意終局性地確定，一切被本項所提及之特徵要素涵攝的資訊，均被應納入資料庫中。毋寧，對此應當由行政機關決定之。

儘管有這樣的開放性及具體化之需求，但條文在資料庫的整體關聯性上，仍符合規範清晰性及明確性原則

。明確性原則並非一開始即排斥不確定法律概念之使用（BVerfGE 118, 168 <188>）。但立法者應確保，其條文應明確到考量規範目的，依據應受規範之生活事實的特性，而有被領會的可能（BVerfGE 78, 205 <212>; vgl. auch BVerfGE 110, 370 <396>; 117, 71 <111>）。必要的是：依法學方法之規則而解釋所涉規範，不確定法律概念藉此得以被充分具體化，且其模糊性亦不至於廣泛到國家部門經規範授權而得為之行為，其可預見性及可受司法審查性遭到危害之地步（vgl. BVerfGE 21, 73 <79 f.>; 118, 168 <188>; 120, 274 <316>; stRspr）。

反恐資料庫主要係針對不同安全機關之資訊獲取前哨而設，其目的乃在讓其他機關更易於蒐集分散而不確定之有效打擊恐怖主義相關情報，在此一關聯性下，不能要求法律對應予儲存之資料為詳盡之規定。在哪一方面詳盡地規定對調查而言係屬重要，此一問題與機關之認識情況間具有緊密之交互作用，可能會透過突發事件而短時間有所改變，然後必須順利地使其具有實用價值。對重要標準作終局性之限定，就此而言，僅以特殊專業之認識及現時之評估為據，始屬可能。在這樣的情況下，當立法者對應予儲存之資料以尚須具體化之開放方式描述，且規定適用時其具體化之階層式程序（在此程序中，事實上應儲存於資料庫之資訊，依據專業之標準予以詳盡闡明並設有限制），從明確性的角度觀之，即不應受到非難。此等具體化工作，並非立法者本身被強制賦予之任務，即便其含有對重要意義之一般抽象確認。毋寧，在實施權力分立的國家中，將這樣的具體化工作託付給行政權，並無法治國之疑慮。就此重要的是，立法者當前對行政機關並無空白授權，而僅係以尚待具體化之方式，描述構成要件要素。應予儲存之資料，其視角及目標方向，在法律上係以如下之方式，被立法者包含實事地表述且附有適例及判斷之視角：其作為由行政權進行具體化之基礎，具有陳述力，且對此蘊含了清楚的指導方針及界限。而就此應考慮者，乃此僅關乎如下資料範圍之具體化：應置於資料庫且輸入機關已掌有之個人資料，該個人資料所涉及之人，係被視為可能與恐怖主義親近者，且就此應由立法者親自充分有限度地予以規定（見上述D. IV. 2.）。

(2)要衡平這些條文的開放性及具體化之需求，立法者應確保，對在個案中適用此等規定而言具有最終決定性而由安全機關所為之具體化及標準化規定，能以可得理解的方式載明並公布。

由於在實際適用時，法定構成要件要素可得認識之意義，其能直接從法律本身探知者相當有限，故必須透

過行政權以可得理解之方式予以具體化及標準化。在此應被評價之條文，其不確定性須透過行政權特殊具體化與透明化之要求而予以衡平，因為現有資料庫之運用原則上並不被當事人所知，而不確定法律概念之具體化，也就也無法透過行政處分及法院審查之交互影響作用而進行。由於欠缺行政法院之審查，要對不確定職權規範作必要限制，其主要機制也就付之闕如。為衡平此一特殊性，立法者必須確保，對於在個案中運用反恐資料庫之重要規定及標準，應由行政權以一般抽象之形式予以確認且可靠地載明之（vgl. SächsVerfGH, Urteil vom 10. Juli 2003 - Vf. 43-II-00 -, juris, Rn. 193 ff.），並以應由立法者進一步確定之方式，對外發布。此等確認、載明及發布，一方面旨在限制授與行政權之職權，而藉此預防對法條作漫無邊際及胡亂之適用（vgl. SächsVerfGH, a.a.O., Rn. 198）。另一方面，亦藉以確保充分之審查水準。將行政權確認之標準載明及發布，讓個人資料保護官得以審查：行政權是否遵循理性之標準而（依立法者之設想，有層次地）適用條文？是否以法律之意義及目的為依歸？

現今之法律狀態，非無限制地合於上開要求。然而，依據當今實務，有疑義之不確定法律概念，其具體化及標準化，係藉由－被納入重要電腦程式中的－應予儲存特徵要素目錄而為之。對此，聯邦政府向本庭提出一份「目錄指南手冊」（Katalog-Manual），其載明在個案中對於適用反恐資料庫法第3條第1項第1b款而言，重要之規定及標準。在該指南手冊中，特徵要素係透過預先設定之輸入選項－這些選項之詳細評價，並非本案程序之標的－而被限制性地詳細闡明，且在實務上，規定應如何適用及其意義為何，亦以可得理解之方式對外發布。

然而，從形式面觀之，卻存有憲法上之疑慮。對於反恐資料庫法第3條第1項第1b款不確定法律概念之具體化，反恐資料庫法並未規定充分明確之載明及發布義務。哪些資料應被納入反恐資料庫，應當透過資訊科技上經過整理及標準化之目錄而予以具體化，這無法直接從法律規定中得出答案，而必須回歸相關資料後始能得知。但是，反恐資料庫法第12條第3款卻規定，關於依反恐資料庫法第3條第1項應儲存資料之細節，以建置命令確認之。不過，這－至少依據實務上對此規範之理解－不應被解讀為係適用上最終決定性之確認，一如其從目錄指南手冊可以明顯看出，其僅係在中間層級之具體化而已（該具體化現今從許多特徵要素觀之，稍微逾越了法律文義範圍）。相對地，在指南手冊中載明之規定，並未被理解為

是建置命令之一部。但無論如何，不管是直接對於指南手冊而言，或是對於建置命令本身而言，均欠缺對外發布之規定。毋寧，這兩者被當成「密件－僅供勤務使用」（Verschlusssache - Nur für den Dienstgebrauch）來處理。

是故，現今之法律狀態並不符合法治國家之形塑要求。若立法者意欲維持反恐資料庫法第3條第1項第1b款gg、hh、ii、kk、nn之不確定法律概念，必須設有補充規定，以確保這些特徵要素由立法者預先規定之具體化，能透過安全機關以可得認識之方式載明及對外發布。

(3)根據反恐資料庫法第3條第1項第1b款gg、hh、ii、kk、nn之規定應納入資料庫內的特徵要素，依其內容觀之，符合禁止過度原則。儘管就此涉及者，乃－尤其與其他應予儲存之特徵要素相連結－可能會揭露高度屬人事況之資料。但是，有鑑於資料庫之功能受有限制，且防止恐怖主義具有重要性（參照上述D. III. 3. a) bb), b），立法者所為者，仍在其享有之立法形成空間內。

這對於反恐資料庫法第3條第1項第1b款gg、hh規定之族別及宗教歸屬特徵要素而言，亦有適用。然而，將此等特徵要素納入，須適用特別之憲法要求，因為對其而言，依基本法第3條第3項之規定，存有憲法上特別之歧視保護，且宗教之歸屬此外亦受基本法第140條、威瑪憲法第136條第3項對於揭露之特別保護。相應地，這些資料也被認為具有特別敏感性（(vgl. § 3 Abs. 9, § 28 Abs. 6 bis 9 BDSG, Art. 8 Abs. 1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Art. 6 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 [BGBl 1985 II S. 539]）。由於有效防止恐怖主義具有重要性，故將此等資料亦納入反恐資料庫中，這樣的考量並非自始即應被排除。惟基於憲法的緣故，這樣的考量必須審慎為之。透過以下的思維，始能考慮將此等資料納入：要將相應之資料納入，不得逾越該資料僅供身分辨識之意義。

cc)反恐資料庫法第3條第1項第1b款rr規定之自由文字欄位，亦符合禁止過度原則。就此所涉及者，並非空白授權讓任何其他資訊一個又一個被填入資料庫內，而是為通常不能透過資料輸入之標準化及目錄化予以描述的指示及評價，開啟一扇大門。其－一如從法條文義可知－與法律定義之基本資料或延伸基本資料相關，且

內容亦受此拘束。作為單純之補充，本條文亦未允許諸如將整個檔案置於資料庫內，而是有限度地－依現今實務，在技術上設有2000字元之限制－以逐點說明之方式，將相關資料輸入。在這樣的理解下，本條文並無憲法上之疑慮。

4.至於資料使用之規定，則並非從任何角度觀之，均符合禁止過度原則。

a)然而，查詢及使用反恐資料庫法第3條第1項第1a款之普通基本資料，其規定在憲法上並無疑慮。

aa)反恐資料庫法第5條第1項第1句及第2句讓參與機關得將這些資料當成清楚資訊而直接讀取。對此，機關不但能著手進行涉及姓名之查詢，其所為之查詢，也會涉及個別或多數於反恐資料庫法第3條第1項第1a款列舉之資訊，從而得辨識對機關而言尚不熟悉人士的身分。在出現吻合情況時，即可對當事人被儲存之普通基本資料的各該整體部分進行讀取。就此而言，反恐資料庫法第5條第1項第1句並未設有加重之干預門檻。對於查詢而言，只要為履行各該調查或打擊國際恐怖主義之任務而有必要，即為已足。反恐資料庫法對於－反恐資料庫法本身未作規定，而僅以之作為要件的（見上述D. II. 2.）－參與機關讀取職權，亦未要求較高之侵害門檻；其出發點顯然在於，低門檻之一般性資料蒐集職權亦已足夠。

藉此，參與機關得在廣泛的範圍內，查詢及檢索基本資料。然而，這並不表示，此一職權不受限制。界限尤其在於，反恐資料庫法第5條所允許者，僅係個別查詢，而非多點查詢、集中查詢或透過資料欄位之連結而對人與人之間的關聯性進行廣泛之調查。因此，條文係以具備具體之調查理由作為前提要件。任何查詢，均須合於必要性之要件，而此一要件在個案中實質上應受審查。此外，依現今條文之安排，其並未授權自動化之照片辨識以及相類功能之運用，或是以不完全之資料進行查詢（所謂「萬用字元」）。

bb)儘管資料讀取之可能性相當廣泛，尤其是藉由有限干預門檻之放棄採取，但該規定卻合乎比例原則。對此具決定性者，乃使用之規定。依據反恐資料庫法第6條第1項第1句之規定，要使用傳輸之資料，其目的必須是為辨識對調查至關重要之人士，或為準備向掌有資訊之機關請求個別傳輸，始得為之。在此之外的傳輸或行為主導性資訊，機關不得從這些資料中取用。機關得在其他步驟中，依專業法律之規定，而請求取用該資訊。對資料為其他目的之進一步使用，僅在獲得掌有該資訊之機關同意後，始得為之，亦即在適當之理解下，僅依據專業法律之規定始得為之。就反

恐資料庫法第3條第1a項之普通基本資料而言，在先行階段採取此等受有限制之資訊交換，基於防止恐怖主義之重大意義，從比例原則的角度觀之，不應予以非難。在此範圍內，反恐資料庫法第5條第1項第1句及第2句與第6條第1項第1句合憲。

b)透過反恐資料庫法第5條第1項第1句及第3句之規定，得以檢索反恐資料庫法第3條第1項第1b款之延伸基本資料，此等檢索在以姓名為檢索條件的實施範圍內，亦合乎禁止過度原則。

反恐資料庫法第5條第1項第1句允許查詢一切儲存於反恐資料庫之資料，因此亦包括對延伸資本資料之檢索。當依據姓名查詢某人而在延伸基本資料中得出吻合者，機關依據反恐資料庫法第5條第1項第3句之規定卻不能接近使用該延伸基本資料本身，而僅能獲知吻合之訊息，以及相關資訊由哪一個機關在哪一個檔案編號下掌有之指示。要讀取延伸基本資料，必須在依專業法律之規定而為個別請求後，透過資訊掌有機關之開通，始屬可能（反恐資料庫法第5條第1項第3句及第4句）。因此，對反恐資料庫法第3條第1項第1b款之延伸基本資料進行檢索，仍保有隱密之性質。將延伸基本資料當成清楚資訊而傳輸，此乃獨立且稍後才會發生的法律行為，必須依據各該專業法律對資料個別傳輸之合憲要件，始得為之。對延伸基本資料作如此隱密之使用，雖然射程範圍廣泛，但在憲法上應無疑慮。

c)相反地，授權得以特徵要素作為檢索條件而檢索延伸基本資料，此等授權違反禁止過度原則，其不但使查詢機關在出現吻合情況時能找到後續資訊之所在地，更讓查詢機關得以直接接近使用反恐資料庫法第3條第1項第1a款之普通基本資料。就此，反恐資料庫法第5條第1項第2句第1a款違憲。

反恐資料庫法第3條第1項第1b款之延伸基本資料，其內容廣泛，且含有高度個人專屬性以及對於當事人生平具有描述性之資訊（見上述D. IV. 3. b) aa) [2]）。因此，從比例原則的角度觀之，要讀取這樣的資訊，相較於讀取反恐資料庫法第3條第1項第1a款之普通基本資料而言，顯然應受較多之限制。所以立法者親自規定，原則上僅能對這些資料為隱密檢索，且必須在合於專業法律之傳輸規定時，始得將這些資料當成清楚資訊而傳輸之。然而，由於一旦在檢索這些資料時出現吻合情況，立法者讓普通基本資料得同時被當成清楚資訊而受讀取，因此，對於以特徵要素為檢索條件進行之檢索而言，亦即對於「反向查詢」而言，上開限制在本質上即被立法者廣泛地解消。與延伸基本資料有關之吻合訊息，連結了普通基本資料

之個人化資訊後，被查詢之延伸基本資料也就成為可歸屬於特定個人之資料，且得被當成個人資訊使用。因此，機關得藉由查詢個別或多數之特徵要素－例如查詢經常造訪特定會面地，且具有特定宗教信仰或教育背景之人士（參照反恐資料庫法第3條第1項第1b款hh, jj, nn）－而實施檢索，並在出現吻合情況時不僅獲悉何機關掌有該資訊，亦可得知所有與被查詢特徵要素吻合之人士其姓名、住址以及其他在反恐資料庫法第3條第1項第1a款列舉之一切資訊。

如此廣泛地使用資料，並未充分考量到延伸基本資料內容的涵蓋範圍。姑且不論個別之延伸基本資料（諸如電信連線）被歸屬到普通基本資料，是否合理，在與特徵要素相關之檢索範圍內，得個別推斷出一切延伸基本資料之廣泛資訊內容，此等可能性即與禁止過度原則不符。當立法者在此範圍內要求將資料置於資料庫，則這些資料只可在獲取資訊之前哨的範圍內，基於能指出資料所在地之目的而被使用。相應地，資料使用之規定應被設計成：當延伸基本資料亦可被檢索時，能被揭露者，僅有檔案編號及掌有資訊之機關，而不及於相關聯之普通基本資料。

d)相對於此，依反恐資料庫法第5條第2項及第6條第2項之規定而在緊急事件中使用延伸基本資料，則－亦非反向查詢之情形（見前述c）－無憲法上之疑慮。

雖然就此所涉及者，乃對匯集於反恐資料庫裡之資料而言，最廣泛之使用可能性。理由在於，除了普通基本資料被讀取之外，延伸基本資料亦額外被當成清楚資訊而遭到讀取，並且就此而言，不僅可為準備進一步之傳輸請求而使用資料，尚可－在行為主導性之危害評估的意義下－為危害防止本身而使用資料（反恐資料庫法第6條第2項）。由此所產生的結果是，特別因為與上開情形相結合，而使情報機關與警察機關間之資訊區分原則受到抑制，從而出現特別嚴重之干預程度（見前述D. III. 3. a) aa), bb) [3]）。

但是，為合理化權利之干預，對資料作如此之使用，其允許要件已受充分嚴格地規定。讀取及使用資料，僅為保護特別重要之法益，亦即為保護人的身體、生命、健康或自由，始得為之。就這些規範的關聯性而言，對健康造成損害，顯然僅指具有持續效果之嚴重健康傷害。只要條文除此之外亦規定保護具重大價值之物，則立法者係在闡明，此一規定所要保護者，並非財產權或物之價值，而是基於公共利益應予維護之物（反恐資料庫法第5條第2項第1句）。在防止恐怖主義的關聯性下，係指諸如重要之基礎設施，或其他對國民整體具有直接

意義之設備。載於條文中者，尚包含干預之高度門檻。要達到此一門檻，必須係為保護法益不受現時之危害，而該危害不能僅以事實上之線索為據，尚須透過特定之事實而存在。就此，資料之讀取及使用，僅在絕對必要且不能及時透過請求而傳輸資料時，始得為之。此外，讀取資料受到程序法上之保全。對資料為擴大之使用，係進一步在各該資訊管理機關的同意保留下，－一如從規範關聯性可輕易得知－依各該專業法律之規定而決定可否為之。因此，總體而言，法條之要求嚴格；相應地，在迄今之實務，此一條文亦係首次被適用。如此之規定，在憲法上並無疑義。其符合禁止過度原則，且亦能通過資訊區分原則之檢驗。

5.比例原則對於公開透明、個人權利保護以及監督性之查驗等，亦有所要求。透過資料庫之目的及運作方式，反恐資料庫法對於資訊交換之公開透明，僅能為有限範圍之確保，並從而使當事人僅能獲得有限的權利救濟可能性；對反恐資料庫法之適用進行查驗，基本上係透過個人資料保護官之監督而為之。若對於監督作有效安排，已注意憲法上之規定，即與憲法相符。

a)為履行機關之任務而儲存及使用個人資料時，立法者在比例原則的角度下，亦應注意公開透明、權利保護以及監督性查驗（(vgl. BVerfGE 125, 260 <325 ff.>）。

資料處理之公開透明，有助於信賴與法安定性之存在，並將資料往來融入民主思辯中。同時，資料處理之公開透明，使人民得以有所應對。此外，對於當事人而言，資料處理之公開透明乃有效權利保護之要件。資料處理之公開透明使個人知悉與其有關之資料處理，藉此，個人得以－在必要時，亦由法院－檢驗相應措施之合法性，並主張可能之刪除、更正及賠償權利（vgl. BVerfGE 100, 313 <361>; 109, 279 <363>; 118, 168 <207 f.>; 120, 351 <361>; 125, 260 <335>; stRspr）。

監督性查驗，係在客觀法上佐助透過法院而為之主觀權利性審查。其目的在於－除行政上之目的外－整體確保行政之合法性，並包括保護當事人之主觀權利。對監督性查驗之要求，亦屬於資料處理合比例性安排的要件之一（vgl. BVerfGE 100, 313 <361> unter Verweis auf BVerfGE 30, 1 <23 f., 30 f.>; 65, 1 <46>; 67, 157 <185>），這考慮到了以下的情形：在儲存及處理資料時，會涉及當事人經常無法直接察覺之干預，且此等干預對自由造成危害之重要性，常常僅間接或至遲在與其他措施產生共同作用後，始生效果。因此，干預資訊自主決定權，若未輔以充分有效之監督

法上的查驗機制，即亦不符比例原則。主觀權利性之審查越是難以確保，則監督性之查驗就越重要。

b)反恐資料庫法對於公開透明之創設以及個人權利保護之確保，其規定為數稀少。基本上，其僅滿足於肯認受告知權，而此等受告知權之有效性，在內容上及程序上均受有限制。但是，由於此一資料庫之功能及作用方式的緣故，反恐資料庫法不應受到非難。

aa)依聯邦個人資料保護法享有之受告知請求權，被反恐資料庫法當成確保公開透明的重要工具而規定之（反恐資料庫法第10條第2項）。然而，此一請求權有其界限，且有部分僅在顯著之程序花費下始能實現。但是，有鑑於反恐資料庫法的功能運作，其合乎憲法上之要求。

(1)反恐資料庫法第10條第2項原則上所保障之請求權，乃係請求告知資料庫內是否有請求權人之資料。此一請求權，參照聯邦個人資料保護法第19條之規定，以及依據資料責任機關各該應適用之法規範所形成的告知界限，受有限制。因此，若告知會對資訊掌理機關履行任務造成危害（vgl. § 19 Abs. 4 Nr. 1 BDSG; § 15 Abs. 2 Nr. 1 BVerfSchG; Art. 48 Abs. 2 Nr. 1 BayPAG），或可能使憲法保護機關之情報狀況受到查探（vgl. etwa § 15 Abs. 2 Nr. 2 BVerfSchG; Art. 11 Abs. 3 Nr. 2 BayVSG; § 14 Abs. 2 Nr. 2 VSG NRW），即不予告知。對反恐資料庫而言，其前提在於，這些非屬否決之例外情形具有重要性，且受告知請求權顯然得受其限制。因此，受告知權並非不夠充足。對告知義務予以限制，要件在於，其有益於相對立之重大利益，且法定豁免構成要件能確保所涉之利益全面地且在個案中彼此相互歸屬（vgl. BVerfGE 120, 351 <364 f.>）。對反恐資料庫而言，從憲法中亦未能導出進一步之受告知權。

(2)對於反恐資料庫法第4條規定之資料隱密儲存而言，主張受告知請求權，關乎顯著之程序花費。與對其他資料不同的是，反恐資料庫法第10條第2項在此規定之受告知請求權，並非統一向聯邦刑事局主張，而僅係對個別的資料掌理機關主張之。因此如有必要時，得向將資料儲存在反恐資料庫的一切機關申請告知。儘管如此之程序實屬遲緩，但此一規定在憲法上仍尚能忍受。其乃如下決定之必然結果與不利面：為當事人之利益，而決定將特定資料隱密地列為僅完全隱密被置於資料庫之資料，且不被任何機關－包括聯邦刑事局－所知悉。資料是否有必要為如此之保密，乃立法者原則上本於其責任與憲法上可得接受之決定。若立法者基於保密之理由，以此種方式讓機關間的資訊交換變得困難，則被告知請求權相應地變

得困難，亦屬可忍受之事。課予聯邦刑事局包裹式的告知義務（此等義務恐怕終究無法排除個別局部告知義務的遲緩），立法者對此並不負有立法義務。

(3)因此總體而言，被告知請求權之設計，在憲法上可被接受。其所保障者，當然僅係對個人而言公開透明的最低標準。但是，基於反恐資料庫之目的及運作方式，這在憲法上應被容忍。

bb)此外，反恐資料庫法對於資料使用之公開原則、法官保留，以及除其他法律規定之告知義務外的法定事後告知義務，均未設有規定。因此，其揚棄了讓個人資料保護之規制合乎比例性的重要確保機制。但是，基於反恐資料庫之目的，這在憲法上仍應屬合理。蓋反恐資料庫之目的，乃在防止國際恐怖主義的範圍內，為進一步之調查預作準備，而作為資訊之前哨。顯而易見的是，此等調查原則上得不依循公開原則。而法官保留，在反恐資料庫的框架內，亦非適當之（可能是憲法要求的）手段。由於反恐資料庫法第5條第1項規定之職權並未在法律上詳為精細形塑，再加上反恐資料庫法第5條第2項規定之讀取時的決定緊急必要性，法官的審查保留恐怕大多不可行。同樣地，忽視特別之告知義務，在憲法上應可被接受。告知義務僅在以下的情況，始對資料庫之功能運作方式不構成實質妨礙，而被考慮：人們終局性地被排除在資料庫之外。然而，與就此而生的花費相較，使用此等受有限制之告知義務，實在太微不足道，以致於其從比例原則的角度觀之非屬必要。

c)資料處理之透明公開性以及個人權利保護之可能性，透過反恐資料庫法僅能受到相當有限之確保，是故，有效之監督性查驗其意義也就愈行重大。比例原則因此在法律的層次與行政實務的層次，對於此一查驗之有效形塑，有其提高之要求。

aa)有效監督之確保，其要件首先係在聯邦以及各邦之層級賦予設置之監督主管機關－例如依現行法之個人資料保護官－有效職權。此外，將資料現狀之讀取與變更完全記錄，亦屬必要。就此，應透過技術上及組織上之措施，確保資料得以實際可評價之方式，為個人資料保護官所用，並且紀錄應包含被列為須受查驗事件的充足資訊。

著眼於反恐資料庫之性質乃聯邦與各邦跨域之聯合資料庫，應注意的是，不能因為聯邦體制之管轄權不明確，而使對反恐資料庫之有效查驗，劣於資料交換之成效。這並非意謂，讓聯邦個人資料保護官亦得廣泛地讀取涉及邦機關儲存及下載資料之紀錄資料。毋寧，對此紀錄資料之查驗，乃各邦個人資料保護官之職責。然而

，反恐資料庫作為聯合資料庫，相應之下，應使個人資料保護官共同合作，且彼此在行使職權時，透過權限授與（Delegation）或授權，以諸如職務協助之方式相互支援。同樣應予確保者，乃不同監督主管機關在合作時，依據對基本法第10條基本權限制法規定之措施而蒐集之資料－在（亦得由聯邦情報局充實之）資料庫中，其乃具有特殊意義之資料－，須實質有效受到保障。當立法者規定安全機關間的資訊合作，其亦應規定有利於資料保護的查驗性合作。

由於監督性查驗對於被弱化設計的個人權利保護而言具有衡平功能，故其正常之實施具有特殊之意義，且此等查驗應以適當之時間間隔－該時間間隔不得逾一定之最高限度，例如每兩年一次－實施之。此乃設計監督性查驗時，應注意之處。

bb)擔保有效監督性查驗能符合憲法要求，乃立法者及行政機關共同之職責。

立法者在反恐資料庫法第8條規定了資料處理之責任，在反恐資料庫法第5條第4項及第9條規定了對資料庫進行一切讀取之殊異與廣泛的紀錄，在反恐資料庫法第10條第1項規定了與聯邦體制之權限分配有關，在事務上並無設限，透過聯邦與各邦個人資料保護官而為之監督。這些規定乃有效查驗（該查驗本質上合於憲法之要求）之基礎。依反恐資料庫法第10條第1項結合聯邦個人資料保護法第24條第4項第4句之規定，在特殊的、嚴格操作的例外情況下，告知或閱覽可能遭到拒絕，這並不會影響上開職權的有效性。然而，關於對固定週期性義務查驗之要求，卻缺乏足夠的法律規定。就此而言，立法者負有增補義務。

此外，立法者首先得相信，這些規定在作好合作準備的機關實務上能被有效地付諸實施。但立法者對此必須觀察，就此是否出現須由法律闡明或須實施爭議解決機制，例如擴大訴訟權能（vgl. Sächs. OVG, Beschluss vom 25. September 1998 - 3 S 379/98 - , NJW 1999, S. 2832; weitergehend Art. 76 Abs. 2 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [Datenschutz-Grundverordnung] vom 25. Januar 2012, KOM[2012] 11 endgültig）」之衝突。

d)為確保透明公開及查驗，最終有必要由法律規定報告義務。

由於依反恐資料庫法而為之資料儲存與資料使用，相當程度地讓當事人無從察覺且並不透明公開，而被告知權亦僅有限地產生對向影響力，再

加上有效之法院審查並不具充分可能性，因此在法律上應確保的是，聯邦刑事局定期向國會及公眾報告反恐資料庫之資料現有儲量及使用情形。為使透過反恐資料庫而為之資料交換能受到公開討論，並接受民主檢驗與審查，此一報告乃屬必要，且其內容必須豐富不流於空洞。

6.關於反恐資料庫法第11條第2項及第4項規定之刪除條款，其合憲性並無憲法上之疑慮。資料儲存持續時間之最高限度，悉依專業法律規定各該儲存在資料庫內資料之刪除期限，這根據反恐資料庫作為聯合資料庫此一構想，乃顯可理解之事，且無論如何在憲法上均屬有理而可被接受。

V.牴觸基本法第10條第1項及第13條第1項

系爭規定將藉由干預電信秘密自由或住宅不受侵犯基本權而取得之資料納入反恐資料庫，在此範圍內，牴觸基本法第10條第1項及第13條第1項。

1.資料之蒐集，其對基本法第10條第1項及第13條第1項之基本權造成干預者，由於該等基本權特殊之保護內容，原則上應適用特別嚴格之要求。此一提高之要求，依據聯邦憲法法院之裁判，在對藉此取得之資料為傳輸及目的變更時，亦繼續發生影響力。對此，例如在刑事訴訟措施的範圍內透過住宅監聽而取得之資料，其傳輸之門檻，即不得低於在進行危害防止時相應干預措施的門檻要求，理由在於：基本權對動用特定之資料蒐集方法所加諸之限制，不得藉由目的變更而遭到規避（vgl. BVerfGE 109, 279 <377 f.>; vgl. auch BVerfGE 100, 313 <389 f., 394>）。同樣地，僅於特別嚴格條件下始得下載之電信資料，只有在如下之情形，始得傳輸給另一其他部門：該其他部門為履行某一任務，且因履行該任務而亦得直接讀取該資料時（vgl. BVerfGE 125, 260 <333>; ähnlich bereits BVerfGE 100, 313 <389 f.>; 109, 279 <375 f.>; 110, 33 <73 f.>）。與此相應地，因對基本法第10條第1項或第13條第1項造成重大干預而取得之資料，應予標記。此等資料之可辨識性，應當得以確保該資料在可能傳輸給其他部門後，其使用之特殊界限仍能被遵守。

2.將藉由干預基本法第10條第1項及第13條第1項而取得之資料亦全然且不設限地納入反恐資料庫中，並不符合上開要求；此外，亦及於藉由干預－憲法訴願人未主張之－保障資訊科技系統機密性與完整性之基本權（基本法第2條第1項結合第1條第1項）（vgl. BVerfGE 120, 274 <302 f.>）而取得之資料。此等資料通常僅在嚴格的規定下始能蒐集，並以高度之干預門檻作為要件，例如：加重之危害情狀或加重之犯罪嫌疑、特別重要之

法益遭受危害或追訴特別重大之犯罪。屬於此類資料者，尤其是藉由電信監察、住宅監聽或策略性限制措施（參照「對基本法第10條基本權限制法」第5條以下）而取得，且若有必要時係以對基本法第10條基本權限制法為據之資訊。這些資料－例如在採取監聽措施時，設法探悉得知之特殊身體特徵或少數方言－，透過被置於反恐資料庫，對許多機關而言係直接作為事先資訊而得以接近，且以檢索為目的而被支配使用，這些機關得僅藉此辨識人別，且決定其是否意欲為個別之傳輸請求（參照反恐資料庫法第6條第1項第1句）。就此，這些資訊與已出現或具體存在之恐怖行為無關，其為了調查措施而遠在可掌握之危害情狀（對於該危害情狀而言，嚴重干預電信秘密或住宅不受侵犯性而蒐集資料，難謂正當合理）尚未發生前即被支配使用。即便假設性之資料新蒐集，其憲法上之容許性標準對於評價傳遞已蒐集之資料而言，並不千篇一律具有決定性意義，但現行將藉由干預基本法第10條第1項及第13條第1項而取得之資料全然且不作區分地予以納入，在為總體衡量時，即與禁止過度原則不符。

3.就此而言，聯邦政府在言詞審理程序中主張，上開資料依反恐資料庫法第4條之規定，尚仍以隱密方式儲存，然而此一主張並未構成任何改變。從反恐資料庫法並不能導出如此之限制。反恐資料庫法第3條第2項明顯提及應標記之資料，由此毋寧可知，此等資料原則上亦應當為反恐資料庫法之規定所涵蓋。相應地，根據聯邦政府之說明，迄今實務就此點而言無論如何均非一致。對此，在憲法上可被接受者，乃以合於明確性原則之形式而清楚確定此等資料之處理的規定。

然而，此等資料始終依反恐資料庫法第4條以隱密方式儲存之規定，從比例原則的角度觀之，與憲法相符。其所保障者，乃相應之資訊僅依據專業法律之傳輸規定（這些傳輸規定的功能在於，確保憲法要求之加重干預門檻以及充分重要之法益保護），始可接近使用。由於此一途徑在言詞審理程序中被聯邦政府與安全機關之一切出席代理人認為洵屬適當，故無庸再審查是否亦有其他途徑－例如將此等資料置於諸如為延伸基本資料而設之使用規定下（見上述D. IV. 4. c）－為憲法所許。

E.單純違憲確認宣告

I.系爭違憲規定得有條件繼續適用

系爭規定部分違憲，但其造成之結果，並非對其為無效之宣告，而僅係確認其牴觸基本法之規定。該等規定得繼續適用，惟須依以下指示為之：僅在不得讀取反恐資料庫法第2條第1句第3款之聯繫者資料，以及不得

讀取藉由干預電信秘密與住宅不受侵犯基本權而獲得之資料，且確保在檢索延伸基本資料時若出現吻合情況，僅能揭露反恐資料庫法第3條第1項第3款，而非第3條第1項第1a款之資訊的範圍內，始得在反恐資料庫法第5條第2項規定之緊急情況外使用反恐資料庫。只要聯繫者資料以及藉由干預電信秘密與住宅不受侵犯基本權而獲得之資料不得被讀取，則此等資料亦不得再依反恐資料庫法第5條第2項所定緊急情況之資料庫使用而被使用之。

對違憲之規定作單純違憲宣告並使其在一定期限內繼續被適用，此種宣告模式在以下情形可被考慮：若宣告系爭規定立即失效，恐造成重大公益失其基礎，且在權衡相關基本權後，過渡期間之干預應可被接受（BVerfGE 109, 190 <235 f.>）。本案即是此種情形。反恐資料庫被立法者以清楚之理由，視為係對有效防止恐怖主義之重要改進。就此，反恐資料庫以及透過反恐資料庫而運作之資訊交換，其基本設計被立法者為不同之形塑，且原則上合憲。由於系爭規定之違憲性基本上僅涉及立法形塑之個別問題，而此等個別問題造成之不利影響，得透過條文暫時適用之限制性指示予以減緩，因此基於反恐資料庫對防止國際恐怖主義之重要性，在為整體權衡後可得出如下結論：系爭規定得暫時繼續適用。

不過，作為暫時繼續適用之要件，在此之前，不得讀取反恐資料庫法第2條第1句第3款之聯繫者資料，並且應確保，在檢索延伸基本資料以及藉由干預電信秘密與住宅不受侵犯基本權而獲得之資料時，若出現吻合情況，僅反恐資料庫法第3條第1項第3款之資訊，而非反恐資料庫法第3條第1項第1a款之資訊遭到揭露。反恐資料庫法第5條第2項之緊急情況規定，得不受上開應遵循之指示限制而繼續適用，俾使針對此等急迫危害不致出現保護漏洞。然而，一旦這些資料不得基於反恐資料庫法第5條第1項之暫時使用目的而讀取之，則其亦不得在反恐資料庫法第5條第2項的範圍內遭到讀取。理由在於：只要憲法上不當備置之資料能被篩選並予以封鎖，則在緊急情況下，亦無任何理由得被讀取。

立法者被賦予充裕的期限，此一充裕期限使立法者得以檢視，是否在反恐資料庫法新規定的關聯性下，其他法律的規定以及（可能的話）個別安全機關資料傳輸條款宜予修正，並與反恐資料庫法之條文作連結。

II. 費用償付

本判決之作成，在C部分獲得一致通過，除此之外則部分存有反對意見。費用償付之決定，悉依聯邦憲法法院法第34a條第2項及第3項之規定

。

法官：Kirchhof　Gaier　Eichberger
Schluckebier　Masing　Paulus
Baer　Britz