「電信往來資料預先儲存案」判決

德國聯邦憲法法院第一庭2010年3月2日判決
－1 BvR 256, 263, 586/08－

陳顯武、謝建新　譯

10條的基本權利甚微
II.往來資料的儲存暨刑事程序法上的調取規則實質合於比例原則
III.合議庭頒布的暫行命令應予適用
Eichberger法官對於第一庭於2010年3月2日之判決所提之不同意見書

關鍵詞

電信往來資料 (Telekommunikationsverkehrsdaten)
儲備資料儲存 (Vorratsdatenspeicherung)
資訊自決 (informationelle Selbstbestimmung)
歐洲共同體2006/24/指令 (Richtlinie 2006/24/EG)
歐洲共同體法優位 (Vorrang des Gemeinschaftsrechts)
先行裁決程序 (Vorabentscheidungsverfahren)
憲法訴願 (Verfassungsbeschwerde)
受理 (Zulässigkeit)
Solange第二次判決 (Solange II)
通訊自由 (Telekommunikationsfreiheit)
通聯資料 (Verbindungsdaten)
電子郵件(Emails)
妥適性 (Geeignetheit)
必要性 (Erfordlichkeit)
恰當性 (Angemessenheit)
目的達成 (Zielerreichung)
目的促進 (Zielförderung)
合比例性 (Verhältnismäßigkeit)
網際網路協定位址 (IP-Adressen)
不同意見書 (abweichende Meinung)

基本法第1條第1項；基本法第2條第1項；歐洲共同體條約第234條；德國電信法第96條；德國電信法第113條；德國電信法第113b條；德國刑事訴訟法第100g條；關於歐盟運作方式條約第267條；基本法第10條第1項

裁判要旨

1.如歐洲議會和歐洲理事會2006年3月15日的歐洲共同體2006/24/指令（官方公報L105，2006年4月13日，頁54；以下簡稱：歐洲共同體2006/24/指令）所規定，經由私人電信服務業者，對電信往來資料進行六個月預先、不具理由的儲存，並非完全不符合基本法第10條的規定；因此在此並無涉及一種所謂的指令優先。

2.比例原則要求，一個這樣的資料存儲的法律上的形成，對於與儲存聯繫造成的基本權侵犯的特別力道，要適當的考量。基於資料安全，資料

使用，透明度和法律保障觀點而來的充分高度的與規範明確的規則是必須的。

3.聯邦立法者依照基本法第73條第1項第7款，負有將資料安全的確保，以及對可能的資料使用目的規範明確的限制，當作儲存義務的立法規定中不可分的基本部分。與此相反，就有關查詢規定本身，暨透明度規定與法律保障規定的形成權限，則依各依所屬別的事務權限劃分。

4.關於資料安全而言所需要的規定，係以規範明確和有拘束力的情形去達成特別高的安全標準。這件事情無論如何依理由，法律上必須明確，理由在於資訊安全標準應依專業討論的演進，不間斷的納入新的知識和觀點，而不是處於以一般經濟觀點作自由衡量。

5.只有資料的查詢和直接使用，僅有極其重大法益保護任務時，才合乎比例的。在刑事追訴領域，這種資料的查詢和直接使用，以透過特定事實而構成嚴重犯罪的嫌疑為前提。對於危險防範和情報部門的任務的履行，這種資料的查詢和直接使用，只允許有事實足認對於一個人的身體，生命或人身自由的具體危險，以及對於聯邦或一個邦的存續與安全，或是共同的危險等，始被允許。

6.透過電信服務業者提出關於網際網路協定位址擁有人的消息的資料，其間接使用亦不限於為刑事訴追，危險防範以及情報部門的任務的履行等特定的犯罪行為或法益的目錄，方得被允許。就行政不法的追訴，上揭資料的提出，以法律明文所列舉的重大案型為限，方得被允許。

案 由

德國聯邦憲法法院 －1 BvR 256, 263, 586/08－ 以人民的名義，在憲法訴願程序中，

I.1. Prof. Dr. G...先生, 2. Dr. G...先生, 3. K...先生, 4. J...股份有限公司, 以負責人為代表人, 5. U...先生, 6. R...先生, 7. Z...先生, 8. Dr. B...先生, - 訴訟代理權人: Meinhard Starostik 律師，住址如下: Schillstraße 9, 10785 Berlin - 聲明不服電信法第113a條與第113b條，在電信監察和其他秘密偵查措施法修正案的第2條，以及2007年12月21日為轉換歐洲共同體2006/24/指令2006/24/ EG 立法（BGBl I. S. 3198）等方面的文字版本。- 1 BVR 256/08 – II.1. Dr. Dr. h.c. H...先生, 2. Dr. S...先生, 3. L...女士, 4. B...先生, 5. P...女士, 6. K...先生, 7. Dr. L...先生, 8. Dr. W...先生, 9. Prof. Dr. S...先生, 10. S...女士, 11. F...先生, 12. S...先生, 13. V...先生, 14. W...先生, - 訴訟代理權人: Dr. Dr. h.c. Burkhard Hirsch律師，住址如下: Rheinallee 120, 40545 Düsseldorf - 聲明不服電

信監察和其他秘密偵查措施法修正案，以及2007年12月21日為轉換歐洲共同體2006/24/指令2006/24/ EG 立法（BGBl I. S. 3198）等規定 - 1 BVR 263/08 -, III. 1. A...女士, 2. B...女士, 3. B...先生, 4. B...女士, 5. B...女士, 6. B...先生, 7. D...先生, 8. Dr. D...女士, 9. Dr. E...女士, 10. F...先生, 11. G...先生, 12. G...女士, 13. H...女士, 14. H...女士, 15. H...女士, 16. H...先生, 17. H...先生, 18. W...先生, 19. W...先生, 20. T...先生, 21. Dr. T...先生, 22. S...先生, 23. Dr. S...先生, 24. S...女士, 25. S...女士, 26. S...女士, 27. S...女士, 28. P...女士, 29. N...先生, 30. N...先生, 31. M...女士, 32. M...先生, 33. M...女士, 34. L...女士, 35. K...女士, 36. K...先生, 37. K...先生, 38. K...女士, 39. K...女士, 40. Dr. H...先生, 41. H...女士, 42. H...女士, 43. H...女士, - 訴訟代理權人: Prof. Dr. Jens-Peter Schneider，住址如下: Lürmannstraße 10, 49076 Osnabrück - 聲明不服於電信監察和其他秘密偵查措施法修正案，以及2007年12月21日為轉換歐洲共同體2006/24/指令2006/24/EG 立法（BGBl I. S. 3198）中之儲備資料儲存規定 - 1 BVR 586/08 -。

第一審判庭，在以下法官的共同參與下：

院長Papier,
Hohmann-Dennhardt,
Bryde,
Gaier,
Eichberger,
Schluckebier,
Kirchhof,
Masing

於2009年12月15日經言詞辯論判決如下：

裁判主文

1.電信法第113a和第113b條，在電信監察和其他秘密偵查措施法修正案的第2條第6款規定，以及2007年12月21日為轉換歐洲共同體2006/24/指令2006/24/ EG 之立法（BGBl I. S. 3198）等，因牴觸基本法第10條第1項而無效。

2.刑事訴訟法第100g 條第1項第1句，在電信監察法修正案的第2條第6款規定和其他秘密偵查措施，以及2007年12月21日為轉換歐洲共同體2006/24/指令2006/24/ EG 之立法（BGBl I. S. 3198），且依電信法第113a條允許事後調取往來資料的範圍，牴觸基本法第10條第1項而無效。

3.所有基於2008年3月11日於1 BvR 256/08 程序的暫時處分（BGBl I. S. 659）藉由2008年10月28日之裁定（BGBl I. S. 2239）重申且擴及，最近又藉由2009年10月15日的裁定（BGBl I. S. 3704）再重申，提及向公眾開放的電信服務業者，在由官方提出資料查詢申請範圍內，但暫時尚未

依電信法113b條第1句前半段規定，向申請機關傳輸，而已被儲存的電信往來資料，必須立即加以刪除。這些電信往來資料不准再傳輸給申請單位。

4.德意志聯邦共和國應支付憲法訴願人因本件憲法訴願程序而支出的必要費用。

理　由

A 憲法訴願的標的

憲法訴願的標的是電信法（以下簡稱:TKG）和刑事訴訟法（以下簡稱: StPO）的規定，該規定就公開可及的電信服務提供商的六個月內的電信業務資料可以預先性的儲存，並對這些資料的使用。

I.系爭法律規定

系爭規定乃透過電信監察和其他秘密偵查措施法修正案，以及2007年12月21日頒布之歐洲共同體2006/24/指令之轉換立法（BGBl I S. 3198;以下：電信監察法修正案）所增訂或修改，且依上開修正案第16條第1項於2008年1月1日生效。這些規定係歐洲議會和歐洲理事會2006年3月15日的歐洲共同體2006/24/關於由向公眾開放的通訊服務或公共的通訊網絡所生與加工的儲備資料予以儲存的指令之轉換。以及對歐洲共同體2002/58/指令的修正((ABl L 105 vom 13. April 2006, S. 54; 以下：歐洲共同體2002/58/指令)。

1.所有憲法訴願直接聲明不服電信法第113a條與第113b條，其透過電信監察法修正案的第2條第6項增訂於電信法中。所有憲法訴願在第1審判庭 BvR 263/08 與第 1 審判庭 BvR 586/08的訴願程序中，尚進一步直接聲明不服刑事訴訟法第100g條在電信監察法修正案的第2條第6款中的文字版本，就此法官依電信法第113a條允許事後調取已存取的資料。

a)據此電信法第113a條規定，關於所有向公眾開放的電信服務業者提供關於參與一電信連結的連線，電信已經發生的時間，以及傳達出的地點等訊息的往來資料，以六個月加以儲存且保存供國家任務履行。該法，緊接聯邦眾議院，從事於聯邦參議院長久以來提出的要求(參照: BTDrucks 14/9801, S. 8; BRDrucks 755/03 <Beschluss>, S. 33 ff.; BRDrucks 406/1/04; BRDrucks 406/04 <Beschluss>; BRDrucks 723/05 <Beschluss>, S. 1)，該要求於2006年涉及歐洲法層面上與此有關違反的部分。聯邦眾議院要求聯邦政府，同意歐洲共同體2006/24/指令的草案且儘速提出一轉換立法之草案(參照: BTDrucks 16/545, S. 4; 16/690, S. 2; BTPlenarprotokoll 16/19, S. 1430)。聯邦政府據此提出電信監察法修正案的草案(參照: BTDrucks 16/5846)。

電信法第113a條第1項第1句課予向公眾開放的電信服務業者義務，針對於電信法第113a條第2至5項個別列舉就固網電話、網際網路電話與行動電話，簡訊(SMS)，多媒體短信服務(MMS)，與類似訊息，電子郵件收發與網際網路註冊等這些電信往來資料，以六個月的時間範圍去加以儲存。凡從事是項服務，但無需自行供應往來資料的業者，依電信法第113a條第1項第2句規定，必須確保是項資料被儲存，且告知聯邦經濟及科技部轄下聯邦網絡局（Bundesnetzagentur），何人為儲存者。凡從事是項服務，且依電信法第113a條的規定對應儲存資料加以更動者，依電信法第113a條第6項的規定，更負有義務就原始的與被更動的資訊加以儲存。資料於逾儲存期限後，應依電信法第113a條第11項的規定於1個月內被刪除。被點擊網頁的通信與資料的內容，依電信法第113a條第8項的規定不得被加以儲存。就資料安全而言，電信法第113a條第10項指示在電信範圍內必要的注意，且主張訪問資料的管道在此僅保留予特殊授權的人員。

依電信法第113a條的規定，除了儲存之外，就電信服務提供者而言，依照電信法第96條的標準，只要為上揭提到的目的是不可或缺的，尚有對電信往來資料加以儲存而且加以使用的可能性。而在電信連線結束後，只要係為費用的計算和與客戶結算上(電信法第97條第1項第1句)是必需的，就個別通聯證明的建立(電信法第99條第1項第1句)，只要是對電信設施的缺陷和故障等的檢測、限制或排除上是不可或缺的(電信法第100條第1項)，且為回覆起因於對線路所有人脅迫或騷擾來電的訊息(電信法第101條第1項第1句)等，上述這些資料得依照電信法第96條第2項第1句的規定作實質上使用。

電信法第113a條規定如下：

第113a條 資料的儲存義務

(1)凡提供給最終用戶的向公眾開放的電信服務業者，有義務依第2項的標準，就國內或歐盟的其他成員國中，六個月內因利用其服務所生成或被加工之往來資料，加以儲存。凡提供給最終用戶的向公眾開放的電信服務業者，但自身無產生或加工往來資料者，需確保這些資料依第1句的規定被加以儲存，且需依德國聯邦經濟及科技部轄下聯邦網絡局要求，告知儲存這些資料之人。

(2)向公眾開放的電信服務業者儲存以下資料：

1.發話人或受話人的撥號號碼或其他識別碼，以及於的任一額外的連接所涉及的情況下的重新撥打或轉接，

2.依於所處時區(Zeitzone)中之日期和時間分類的連結的開始和結束，

3.於電話服務的範圍內得被利用之不同服務的情形下，被利用之服務的信息，

4.在行動電話服務的情況下還包括：

a)用於發話和受話接線端的國際識別號，

b)用於發話和受話終端的的國際識別號，

c)被用於透過發話和受話接線端於連接開始時的訊號單元(Funkzelle)底標誌，

d)在預付費服務匿名的情況下，依訊號單元的日期，時間和標誌等的服務之首次開通，

5.在網際網路電話服務的情況下，發話和受話接線端的網際網路協定位址。

第1句的規定準用於簡訊、多媒體短信與類似訊息的傳輸;在此依第1句第2項，於報告時，訊息的傳送和接收的時點應予儲存。

(3)電子郵件的服務提供業者儲存以下資料：

1.於消息的發送時，電子郵件信箱的識別號和發送方的網際網路協定位址，以及該消息的每個接收方的電子郵件信箱的標識號，

2.在消息到達電子信箱後，消息的發送方和接收方的電子郵件信箱標識號，以及傳輸消息的電信設施的網際網路協定位址，

3.於訪問電子郵件信箱時，該信箱之標識號暨接收方的網際網路協定位址，

4.前述第1－3號所列的服務的利用，依於所處時區中之日期和時間加以分類。

(4)網際網路服務提供業者儲存以下資料：

1.就網際網路使用分配給客户的網際網路協定位址，

2.用於開通網際網路使用所需的連線的明確標識號，

3.於被分配的網際網路協定位址下的網際網路使用的開始與結束，依於所處時區中之日期和時間加以分類。

(5)在當電話未接或因線路管理員的干預而仍未接通時，則電話服務提供業者亦得依本法第96條第2項所列之目的，就本條所列之往來資料加以保存或記錄的範圍內的這些往來資料亦可依本條的標準被加以儲存。

(6)凡提供電信服務且在此對依本條之標準所儲存的報告加以修改者，負有對於原始的和新的報告以及修改本報告之時點，依於所處時區中之日期和時間加以分類，加以儲存的義務。

(7)凡提供公眾的行動無線通訊業者，負有義務就依本條標準被儲存之訊號單元的標識暨資料，由這些標識其中可得出供應個別訊號單元的訊號天線的地理位置暨該天線的主要放送方向，加以保存。

(8)關於造訪的網站的通信和資料不准以本條為基礎被加以儲存。

(9)依本條第1-7項之規定的資

料的儲存，應以得向提出詢問的有權單位即刻回答的方式達成。

(10)根據本條的規定的義務人，應就關於被儲存往來資料的品質和保護，其在電信範圍內必要的注意，加以顧及。在上揭範圍內，義務人應透過技術的與組織的措施去確保，被儲存資料的造訪只可能係由獲得義務人特別授權之人。

(11)根據本條的規定的義務人，應將這些單以本條為所被儲存的資料，於逾本條第1項所規定期限後1個月內加以或確保刪除。

b)電信法第113b條規定依照電信法第113a條規定被儲存的資料據之准予被使用之目的。這些目的被區分為傳輸到當局，以便其能用之以履行職責，並透過電信服務提供商本身根據電信法第113條用之以發布信息，特別是關於網路連接的所有人的信息。

aa)電信法第113b條第1句前半段規定多項目的，為這些目的，允許電信企業將資料傳輸予機關。這些機關得單方面利用這些資料的要件，應透過聯邦或各邦各自專法中的條款加以規定。電信法第113b條第1句上半段規定，負儲存義務者對於依照電信法第113a條規定單以本條為基礎所被儲存的資料，係專為犯罪行為的訴追(Nr. 1)，公共安全的重大危險的防範(Nr. 2)，以及情報部門的任務的履行(Nr. 3)等，方得將上述資料傳輸予主管單位。

根據電信法第113b條第1句前半段規定而將資料依其請求而傳輸給個別有權責的單位，只有在參考電信法第113a條的規定，而於專法的相關法律規定中明文加以規定且依個案加以編排下，方得作成。

由憲法訴願人於第一審判庭BvR263/08和第一審判庭BvR586/08的程序中所聲明不服的刑事訴訟法第100g條，係為刑事訴追而利用依據電信法第113a條被儲存的資料的專法上的授權基礎。就危險防範與情報部門的任務履行，在這段期間由2008年12月25日的透過聯邦刑警局的防範國際恐怖主義危險法 (Gesetze zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt) (BGBl I S. 3083) 的版本中的聯邦刑警局法(Bundeskriminalamtgesetz;以下: BKAG) 第20m條以及許多不同的邦法上的規定指引於電信法第113a條上且使機關如此追溯依照這些規定被儲存的資料成為可能。

然而允許被儲存的電信往來資料同樣於電信法第113a條生效前已被用於刑事訴追，危險防範或情報部門的任務的履行上。刑事訴訟法第100g條於2001年12月20日的刑事訴訟法修正法案(BGBl I S. 3879; 以下簡稱:舊刑事訴訟法第100a條)第1條的版本就規定，對於具重大犯罪行為之涉嫌或藉助於電信終端設施著手的犯罪行為，

服務供應商基於法官裁定，以提供關於電信連接資料的訊息的義務。同樣的諸如巴伐利亞邦警察任務與權限法(Gesetzes über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei)第34b條第2項第1號於2005年12月24日警察任務法與議會的監督委員會修正法案 (Gesetzes zur Änderung des Polizeiaufgabengesetzes und des Parlamentarischen Kontrollgremiumgesetzes vom 24. Dezember 2005) (GVBl，頁641)版本中(警察任務法(Polizeiaufgabengesetz); 以下簡稱:BayPAG) 授權提取現存的電信連結資料。同樣的，聯邦與各邦就憲法保護事務之合作與聯邦憲法保護局法(Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz) 第8a條第1項第1句第4號(聯邦憲法保護法(Bundesverfassungsschutzgesetz); 以下簡稱: BVerfSchG)，於2007年1月5日反恐法增修法案(Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007) (BGBl I S. 2) 版本中，亦為危險的防範以及情報部門的任務的履行，授權提取現存的電信連線資料。

bb)電信法第113b條第1句後半段原則上雖然不同於在電信法第113b條第1句前半段列舉的目的，而排除將依據電信法第113a條所儲存的資料供與他人使用。但以下方式的例外仍是允許的，即允許服務業者依據電信法第113條提供訊息而使用這些資料。

電信法第113條第1項允許國家機關依據電信法第95條和第111條探詢所謂的顧客資料和基本資料，特別是電話號碼，電信接線標示，以及電信接線所有人的姓名和地址，就此電信法第113b條第1句後半段使服務提供業者對此得告知所謂的「浮動」網際網路協定位址（以下簡稱:IP位址）的所有人的訊息。網際網路協定位址照目前的發展狀況，原則上無法將一個連線確定地被歸類為所謂的「固定」網際網路協定位址，而是各自按照網際網路使用人各自就網際網路的啟用的持續時間被歸類為所謂的「浮動」網際網路協定位址。關於從已經在特定的浮動網際網路協定位址在特定時間使用的電信連線的所有人，因此僅得於當往來資料得被加以使用，就此透露出有哪些連線被於標準時間內相應的網際網路協定位址所指出，此時訊息方得被告知。以上使得電信法第113b條第1句後半段依對於依電信法第113a條被儲存的資料的規定成為可能。

依據通說見解，依據電信法第113條第1項，為查詢回覆浮動的網際網路協定位址的所有人的往來資料於

電信法第113a與第113b條生效前即可被加以使用(參照: 如 LG Stuttgart, Beschluss vom 4. Januar 2005 - 13 Qs 89/04 -, NJW 2005, S. 614 <614 f.>; LG Hamburg, Beschluss vom 23. Juni 2005 - 1 Qs 43/05 -, MMR 2005, S. 711 <712 f.>; Sankol, MMR 2006, S. 361 <365>; a.A. LG Bonn, Beschluss vom 21. Mai 2004 - 31 Qs 65/04 -, DuD 2004, S. 628 <628 f.>; OLG Karlsruhe, Urteil vom 4. Dezember 2008 - 4 U 86/07 -, MMR 2009, S. 412 <413 f.>; Bär, Handbuch zur EDV-Beweissicherung, 2007, S. 148, Rn. 212; Bock, in: Geppert/Piepenbrock/ Schütz/Schuster, Beck'scher Kommentar zum TKG, 3. Aufl. 2006, §113 Rn. 23 f.)。然而在此僅依照電信法第96條被儲存的往來資料得被加以追溯。依據電信法第113條第1項，對浮動的網際網路協定位址所有人的認定的可能性因此取決於，是否這樣的資料於查詢聲請仍被儲存。

對網際網路協定位址所有人的辨識，對著作權保護亦有某種意義在。假如對權利主體而言，對網際網路協定位址加以確定，而將在網際網路中侵害其著作權，則刑事訴追機關透過依據電信法第113條第1項規定申請調閱訊息而得調查個別的連線所有人，依權利主體的看法對這些人，民事法上會優先於刑事行為。雖然2008年6月7日改進智慧財產權落實改善法(Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums vom 7. Juli 2008)(BGBl I S. 1191)第6條第10號版本中著作權法第101條第2項第1句第3號(以下簡稱: UrhG)亦允許在其間於特定要件下就其著作權侵害，對電信服務業者有民事法上訊息請求權。上開訊息依著作權法第101條第9項，基於法官命令亦得方於運用電信往來資料時被加以告知。然而在此追溯依據電信法第113a條被儲存的資料則不在此限。（參見:Frankfurt am Main 邦高等行政法院5月12日2009年的裁定- 11 W 21/09 -,MMR,2009, S. 542 <544> 與其它參考文獻; Hoeren, NJW 2008, S. 3099 <3101>; Bäcker, in: Rensen/Brink, 聯邦憲法法院裁判指示(Linien der Rechtsprechung des Bundesverfassungsgerichts，2009, S. 99<111 f.>，Fn. 49）。

依據電信法第113條第1項第1句的規定，於就犯罪行為或違反行政秩序的訴追，為了公共安全或秩序的危險防範，或為了情報部門的任務的履行等為必要時，必須將訊息告知。

cc)電信法第113b條規定如下：

第113b條 依電信法第113a條被儲存的資料的利用

依電信法第113a條規定的義務人，得將以下依電信法第113a條規

定單獨以儲存義務為基礎的資料

1.犯罪行為的訴追，

2.就對於公共安全而言的重大危險的防範，或

3.為履行聯邦和邦政府，聯邦情報局(Bundesnachrichtendienste)和聯邦軍情局(Militärischer Abschirmdienst)等之憲法保護部門的法定職責。

依其主管當局的要求而加以傳送，只要上揭有於關於電信法第113a條個別的法律規定中被加以規定且傳送依個案被加以規定;就例外情況下為其他目的的查詢回覆，依據電信法第113條規定，義務人不准使用該資料。電信法第113條第1項第4句準用之。

電信法第113條中涉及到電信法第113b條的規定摘要如下：

電信法第113條 條列式的查詢程序

(1)凡提供或參與商業模式的電信服務者，就犯罪行為或違反秩序的訴追，公共安全的重大危險的防範或聯邦或各邦憲法保護機關、聯邦情報局或聯邦軍情局等的法定任務的履行有必要時，於個案中依有權單位請求，應立即向其告知依據第95條和第111條所獲取的資料訊息。關於資料的訊息，藉助這些訊息使終端機或內建於終端機或電源中的儲存裝置的操作受到保護，特別是個人識別密碼(PIN;Personal Identification Number)或個人識別密碼的解鎖碼(PUK; PIN Unlocking Key)，依第1句的義務人，基於依刑事訴訟法第161條第1項第1句、第163條第1句，聯邦或各邦為公共安全與秩序的危險防範的警察法規中的資料調取條款，聯邦憲法保護法 (Bundesverfassungsschutzgesetz)第8條第1項，各邦憲法保護法中相關條文，聯邦情報局法(BND-Gesetz; Bundesnachrichtdienstgesetz)第2條第1項或聯邦軍情局法(MAD-Gesetz; Militärischer Abschirmdienstgesetz) 第4條第1項等法所提出之訊息申請，必須加以告知;對其他公共或非公共單位則不需傳輸這些訊息。調取屬於遠距通訊秘密(Fernmeldegeheimnis的)資料，僅以在與此相關法律規定的要件方得允許。義務人對於其男女客戶與第三人之查詢回覆負有保持沈默義務。

(2)...略。

c)刑事訴訟法第100g條第1項第1句規範為刑事訴追目的而調取電信往來資料。首先，刑事訴追機關得據此如同依舊刑事訴訟法第100g條規定，獲取電信企業基於電信法第96條所儲存的往來資料。此外刑事訴訟法第100g條僅規定依電信法第113a條被預先儲存的資料的獲取。憲法訴願人於程序1 BVR 263/08和1 BVR 586/08中對此聲明不服。

刑事訴訟法第100g條第1項第1句並關連到電信法第113a條在個別中使刑事訴追機關，只要為查清案情或對於嫌疑人所在地的確定有必要，得於

嫌疑人不知情下，調取往來資料。然而就此僅於當一定事實構成懷疑，某人作為犯罪行為之正犯或共犯於個案中有重大意義，特別是對於一項於刑事訴訟法第100a條第2項所列舉之犯罪行為之著手，未遂或有預備行為，或是某人藉助電信作為正犯或共犯著手於犯罪行為。

資料提取於非面臨緊急危害的情況，依據刑事訴訟法第100g條第2項第1句並連結刑事訴訟法第100b條第1項第1句和第2句的規定，僅得透過法官命令為之。是項依據刑事訴訟法第100g條第2項第1句並連結刑事訴訟法第100a條第3項的規定所為的命令，僅得用以針對嫌疑人或個人，其係基於特定事實被認定為有嫌疑或訊息由其傳入或傳出或是此聯繫為嫌疑人所利用的情況下。

針對通過電信手段著手的犯罪行，依據刑事訴訟法第100g條第1項第3句所為的調取往來資料，僅有於查清案情或對於嫌疑人所在地的確定，可能依其他方法無法達成且資料的調取與事務的意義以一種符合比例的關係時，方得被允許。這個限制是立法者因為比例原則而認為是必要的，因為透過與依據電信法第113a條的儲存義務相聯結的往來資料調取的對資料庫的擴大，在整體上是符合干預強度的（參見：BTDrucks 16/5846, S. 52）。

依據刑事訴訟法第100g條第1項第1句所作出的措施，依據刑事訴訟法第101條段第4項第1句應通知對方。受處分人於收到通知後2週內得申請法院審查（刑事訴訟法第101條第7項第2句)。在特定情況下，通知可省略（刑事訴訟法第101條第4項)，而在其它情況下可被推遲（刑事訴訟法第101條第4項)。依據刑事訴訟法第101條第4/5項所為的長期推遲，依刑事訴訟法第101條第4項的規定，除通知之外尚需要法院確認。

刑事訴訟法第100g條規定：

第100g條

(1)有一定事實足認，某人作為正犯或共犯

1.著手於嚴重之犯罪，尤其是第100a條第2項所稱之犯罪，或在未遂可罰之情況下著手實施，或以一犯罪進行預備，或

2.經由電信通訊實施犯罪，

只要為查清案情有必要，得於嫌疑人不知情下，調取往來資料（電信法第96條第1項、第113a條）。在第1句第2款之情形中，僅在查清案情以其他方式可能無望時，方得為此處分。當調取定位資料對查清案情或調查被告所在地有必要時，依據本項規定僅得對未來發生之通信紀錄或同步調取，且僅在第1句第1款之情形中方得為之。

(2) 第100a條第3項及第100b條第1項第1句至第3句、第2項第1句及第4項第1句之規定準用之。不同

於第100b條第2項第2句第2號，在一有重大犯罪行為的案型中有一個時空上充分可確定通訊的標示就滿足，當對案例事實的探究或是偵查嫌疑人的所在地，以其他方式可能會無望時或根本上極困難時。

(3)若調取通信紀錄非在提供公共電信通訊服務者處進行，則通訊過程結束後之調取，依一般規定為之。

(4)依第1項所為的處分，準用第100b條第5項之規定，應每年製作概要提交，其中應載明：

1.就本條第1項執行此等措施之程序數量;

2.就本條第1項，依首次與後續區分的法官命為此等措施之命令數量;

3.依本條第1項第1句第1項與第2項區分的各自以之為基礎的犯罪原因;

4.依本條第1項被詢問的往來資料，自(暫時) 裁定的時點起計可回溯月數的數量;

5.因為被詢問的資料全部或部分已不存在而失敗的措施的數量。

2.歐洲議會和理事會的歐洲共同體2006/24/指令，該指令之轉換係由系爭規定於涉及刑事訴追的範圍內所致力的。該指令係在歐洲議會拒絕一項由法國、愛爾蘭、瑞典和英國等所提出的以在里斯本條約(Vertrag von Lissabon)生效前有效的歐洲聯盟條約(以下簡稱: EUV舊法)中第31條第1項c與第34條第2項b為基礎的關於電信資料儲備儲存的框架決議(參照: Ratsdokument 8958/04 vom 28. April 2004)的草案後(參照: Parlamentsdokument P 6 TA[2005]0348)，由理事會基於歐洲共同體條約第95條，於愛爾蘭和斯洛伐克的投票反對下獲得通過(參照: Ratsdokument 6598/06 ADD 1 vom 27. Februar 2006, S. 4)。

a)該指令繫之於電信往來資料被認為係對於犯罪行為的訴追，特別是對組織犯罪和恐怖主義的領域而言，這是一項極有價值的工具(參照: Erwägungsgründe 7 bis 10 der Richtlinie 2006/24/EG)，且若干會員國針對這樣資料的儲備資料儲存，好像亦有公布彼此間差異極大的法律規定(參照: Erwägungsgrund 5 der Richtlinie 2006/24/EG)。透過上述所創設的法律和技術上的差異影響了電信單一市場(Binnenmarkt)，因為據說電信服務供應商，考慮到地區必須儲存的資料和檔案儲存時間而面臨著不同的要求(參照：Erwägungsgrund 6 der Richtlinie 2006/24/EG)。

b)歐洲共同體2006/24/指令的效力，不但在其與共同體基本權利的兼容性面向上(參照: Klesczewski, in: Festschrift für Gerhard Fezer zum 70. Geburtstag, 2008, S. 19 <24 f.>; Klug/Reif, RDV 2008, S. 89 <91 ff.>;Rusteberg, VBlBW 2007, S. 171

<176>; Westphal, EuZW 2006, S. 555 <558 f.>; Zöller,GA 2007, S. 393 <410 ff.>; Generalanwältin Kokott, Schlussanträge vom 18. Juli2007 - Rs. C-275/06 -, Slg. 2008, I-271 <276>, Rn. 82 - Promusicae -)，而且關聯到歐洲共同體的相關權限基礎面向上，均有疑問(參照：Gitter/Schnabel, MMR 2007, S. 411 <412 f.>;Jenny, CR 2008, S. 282 <285>; Klesczewski, in: Festschrift für Gerhard Fezer zum 70. Geburtstag, 2008, S. 19 <22 ff.>; Klug /Reif, RDV 2008, S. 89 <91>; Leutheusser-Schnarrenberger, ZRP, 2007, S. 9 <11 ff.>; Rusteberg, VBlBW 2007, S. 171 <173 f.>;Westphal, EuZW 2006, S. 555 <557 f.>; Zöller, GA 2007, S. 393 <407 ff.>)。

藉由2009年2月10日的判決，歐洲法院駁回愛爾蘭根據歐共體條約第230條所提的無效之訴，據愛爾蘭方指稱此無效之訴係基於該指令主要目的是簡化刑事訴追，且因此該指令只有在預先假定的歐洲聯盟條約一致決的舊版本的警察和司法合作條款，特別是在第30條，第31條第1項c和第34條第2項b中有考慮到的，方得作為法律依據(參照: Klage vom 6. Juli 2006 - Rs. C-301/06 -, ABl C 237 vom 30. September 2006, S. 5)。歐洲法院對此明確地表示，裁判本身並非以共同體基本權利所受的一些侵害為對象(參見：EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -, Rn. 57)。

c)根據歐洲共同體2006/24/指令第1條第1項，該指令旨在協調各成員國關於向公眾開放的電子通訊服務或公共電信網絡業者，就電信資料的儲備儲存義務的法律規定，以確保該資料係為偵查，確定和訴追嚴重犯罪行為等的，如同每一成員國於其國內法所規定的目的而被提供。為了該指令的採納，議會解釋如下，成員國應就「嚴重犯罪行為(schwere Straftat)」概念的定義，其係2002年6月13日議會關於歐洲逮捕令和成員國之間的移交程序(Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (2002/584/JI) (ABl L 190 vom 18. Juli 2002, S. 1) 的框架決議中第2條第2項中所列舉的犯罪行為，暨藉助電信設備而遂行的犯罪行為，適當地加以注意(參照：Ratsdokument 6598/06 ADD 1, S. 4)。該指令並未就該資料用於危險防範或情報單位加以規定。

根據歐洲共同體2006/24/指令第3條第1項規定，各成員國必須確保在歐洲共同體2006/24/指令第5條中所列舉的資料，在這件事情上，根據歐洲共同體2006/24/指令第6條規定，時間上自通訊可被確定時起以最短六個月且最長兩年資料以儲備的方式被加以儲存。根據歐洲共同體2006/24/指令

第4條第1項規定，各成員國必須確保以儲備的方式被加以儲存的資料僅得於特定案型且依照內國法得被轉交予國內有權機關。對此每一成員國就資料的探訪應遵循符合必要性和合比例的要求的程序和條件加以確定。

根據歐洲共同體2006/24/指令第7條規定，各成員國有義務確保，這些以儲備方式被儲存的資料，有最低度的資訊安全。除此之外，歐洲共同體2002/95/46指令和歐洲共同體2002/58指令的規定仍為有效(參照：Erwägungsgründe 15 und 16 der Richtlinie 2006/24/EG)。根據歐洲共同體2006/24/指令第8條規定，各成員國保障，被儲存的資料及所有其他必要的資料，得立即應有權機關的探詢而轉交之。此外，根據歐洲共同體2006/24/指令第13條規定，各成員國確保對歐洲共同體94/46/指令第三章關於權利救濟(Rechtsbehelfe)、逮捕和處罰的規定加以轉換時亦考慮到歐洲共同體2006/24/指令的資料加工而完整地加以轉換。本指令對此並未規定，何人應負擔資料儲存的費用。

3.此外，刑事訴訟法第100g條亦對歐洲理事會的關於電腦犯罪的公約(Übereinkommen des Europarats über Computerkriminalität)(BGBl II S. 1242; 以下：關於電腦犯罪的公約)有意義(參照：BTDrucks 16/5846, S. 27 f. und 50）。該公約不僅要求各成員國去創設對抗電腦犯罪的刑事實體法，而且亦要求創設特定的刑事程序法的規則。特別是該公約第16條，授權主管機關下令去對往來資料的即時確保。管理這些資料的人必須能被課予義務，對這些資料短期且無損的去確保，以便這些資料得進一步傳送給有權機關 (所謂的快速冰存(Quick Freezing))。然而立法者視相關規定是可被放棄的，因為被冰存的資料基於電信法第113a條無論如何必須被維護(參照：BTDrucks 16/5846, S. 53)。

4.基於憲法訴願人於第一審判庭BvR 256/08程序中的申請，聯邦憲法法院於2008年3月11日以裁定頒布一項暫時命令，令電信法第113b條第1句第2和第3號直至主事實判決前，僅准予有限制地被加以適用(參照：BVerfGE 121 1)。聯邦憲法法院於2008年10月28日決議更進一步將此暫時命令擴張，以致於電信法第113b條第1句第2和3號到主裁判前僅得有限制的被適用(參照：BVerfGE 122, 120)。此外聯邦政府被課予任務，各自就相繼而來多個月的期間就電信法第113a條中規定的資料儲存的實際影響以及暫時命令對刑事訴追的的實際影響報告。聯邦政府就自2008年5月1日至2008年7月31日，2008年8月1日至2009年3月1且以及自2009年3月1日至2009年9月1日提出報告。

II.事實與爭點－憲法訴願人的

主張

1.憲法訴願人於第一審判庭BvR 256/08程序中聲明不服電信法第113a條與第113b條，憲法訴願人抨擊該規定侵害基本法第10條第1項、第12條第1項、第14條第1項、第5條第1項及第3條第1項等。訴願程序與案件編號1 BvR 508/08同樣主張所進行其他34.000個憲法訴願人併案處理。

a)憲法訴願人主張憲法訴願應予受理。

aa)憲法訴願人1至3以及5至8係大學教師，律師，企業經營者，稅捐顧問和註冊會計師，以及調查記者，其於私人或營利上利用不同的電信服務諸如固定電話、行動電話、網際網路入口以及電子郵件信箱。對上述這些人應是無法期待其先在普通法院(Fachgerichten)對電信企業起訴。

女憲法訴願人4為一商業的網路匿名服務發展與推銷軟體。該匿名服務係其與其他獨立的企業合作，在其伺服器上使用她的軟件。該女憲法訴願人自身亦經營一向公眾開放的匿名伺服器。女憲法訴願人之該匿名服務據稱因系爭規定而不再帶來經濟上的利益。且女憲法訴願人亦有客戶流失之虞，因這些客戶因儲備資料儲存而不再信任其仍得維持匿名。事實上，(課予)儲存義務並不亞於職業禁止。儲存義務係現實和直接的牽涉到到女憲法訴願人自身，因為不能指望她承擔行政罰款或刑事訴訟的風險，而不去遵守此儲存義務。

bb)憲法訴願的受理並不排除系爭規定去對歐洲共同體2006/24/指令加以轉換。聯邦立法機構在此超過歐洲共同體2006/24/指令範圍，進一步依電信法第113a條的規定，被存取的資料不僅准許被使用在嚴重犯罪，而且准許被使用在的危險防範和情報部門的任務的履行上。

除此之外，德意志聯邦共和國沒有將歐洲共同體2006/24/指令轉換為國內法的義務。該指令違反歐洲共同體條約第95條規定且侵害共同體成員國人民的基本權利。該指令侵犯依歐洲人權公約第8條所規定私人生活和通信受到尊重的權利且導致對歐洲人權公約第10條所保障的意見表達自由的不合比例的干預。該指令因此不得在德國被加以適用。至少憲法訴願受理，係因為系爭規定，在歐洲法院依歐洲共同體條約第234條(今日:關於歐盟運作方式條約第267條)規定的先行裁決程序範圍內，這些系爭規定的施行被聲請為無效裁判，係以基本法的基本權利為據被加以審查。倘若歐洲法院未視歐洲共同體2006/24/指令為無效，則聯邦憲法法院應宣告歐洲共同體2006/24/指令違反權限而不適用之，並宣告系爭電信法第113a條與113b條無效。

b)本件憲法訴願有理由。在此涉

及儲備資料的儲存，其有違憲之虞。它將首次有可能去確定一個人過去的六個月裡的所有通訊夥伴。對於電訊單元(吾人於其範圍中通話)的儲存，使得動態側寫(Bewegungsprofile)幾乎是完整的。對網際網路協定位址的儲存，使得其後可追蹤之前六個月內的網際網路的使用模式。與此相對不明顯的是儲存在計測上用於辨識度(Aufklärungsquote)或犯罪率(Kriminalitätsrat)上產生的效果。

aa)系爭規定侵害基本法第10條第1項。應被儲存的資料屬於電信秘密的保護範圍之內。網際網路於其被利用為大眾通訊媒介，同樣屬於基本法第10條第1項的保護範圍之內。藉電信法第113a條與第113b條所成立對電信秘密的干預，係不正當的。

(1)對一項合秩序刑事司法的保障，並不能合理化儲備資料儲存(Vorratsdatenspeicherung)。在網絡犯罪領域其首先涉及財產的價值(Vermögenswerte)。至於電信手段也許只是被利用作遂行傳統犯罪的輔助手段，而可能涉及到各方面的法益(Rechtsgüter)。儲備資料儲存就對抗組織犯罪或防止恐怖攻擊上的妥適性被評價為是非常有限。

儲備資料儲存的一般預防上效果也許不需嚴肅地去期待。在刑事訴追的範圍，比起具體危險的防範，輕微的干涉權限較合宜這件事，才是決定性的。避免危及最高法益的危險的防範而獲取的資料，不該被用在處理輕罪上。再次使用僅當於，資料的提取亦為再次使用目的的達成是合比例的情況下，方被允許。目的本身則不在考量之內。刑事訴追機關的延伸調查權限，充其量得略為提升辨識度。這是否會導致犯罪率的下降，是非常值得懷疑的。

就儲備資料儲存對法益保護的妥適性值得懷疑。其雖然阻止通訊過程因此不被探知，因為通訊過程中的事態(Umstände)並未被加以儲存。然而儲備資料的需求多大仍是不明。反正許多的通訊資料係為計費和取證目的而被儲存到六個月長。相比之下，犯罪集團利用匿名的電信如預付費協定(Prepaid-Tarif)或網咖(Internetcafé)這樣的可能性。

(2)快速冰存程序(Quick-Freezing-Verfahren)，即涉及到一個人全部仍被儲存的往來資料的確保，可被考慮作為較儲備資料儲存為溫和的手段。在特殊例外情況下，亦可考慮就特定時點得獲取所有往來資料的儲存的安排(全面冰存(Global Freezing))。

(3)就基本法第10條第1項的干預的強度(力度)係由以下得出，即電信服務業者很可能是對公共開放的，涉及所有的人。儲存行為係在無庸置疑的情況下達成的。單純的可能性，即資料係為了刑事訴追或危險防範目的

而言是有可能需要的這件事，無法證成是項干預。儲備資料儲存使電信與動態側寫的建立成為可能，且擁有大的擴散幅度(Streubreite)。上面這件事在當期待完全保密的電信時，會變得更加重要。

一項對電信連線以地毯式掌握而為全面和隨機的監控，如同其表現於儲備資料儲存，其本身就防範較大的危險上是違憲的。被儲存的資料其後為危險防範或刑事訴追上可能被用上的可能性，是極微不足道的，且其對如此重大的干預無法合理化。儲備資料儲存使對個人形象以前所未有的精確度成為可能。通訊資料在內容上是特別翔實。對電信的進一步事態的掌握比掌握通訊內容並不會較不嚴重。這樣的掌握使完整的個人側寫或行為側寫(Persönlichkeits- und Verhaltensprofile) 成為可能。往來資料提供了很多關於社會關係的資訊。

儲備資料儲存也升高了遭受不公正的調查措施，或無辜的定罪和資料濫用的風險。往來資料得專門針對不受歡迎的人被使用且合於對個人和團體的控制，以及用於經濟間諜活動。只有放棄資料儲存方得以有效地保護免於被濫用。

儲備資料儲存影響到對民主而言不可缺少的通信不受干擾性。人性尊嚴的保護應予顧及，特別是在特別信任關係的範圍中的通訊有一定的尺度。透過對公民的監督而生的損害將無法藉由相關效率獲取來彌補。儲備資料儲存導致反制措施的發展且最終甚至於減少被提供的電信資料的數量。另一方面，漸增的數位化亦於無儲備資料儲存下超過為補足(費率)計算目的被儲存的往來資料的減量。

以上這件事是不合比例的，因為對當事人與社會整體上而言，可預期的利用與是項利用的缺點呈現出明顯的不相稱。法益保護僅於少數案例中被改善。用犯罪程度(Kriminalitätsniveau) 的下降是沒法計算的。考慮到其他涉及個人的資料對於刑事訴追的意義，可以是面對潰堤(Dammbruch) 的威脅。

bb)系爭規定亦侵害基本法第12條第1項。電信法第113a與第113b條以不合比例的方式干涉商業的電信服務業者的職業選擇自由且干涉以信賴為基礎的從業人員的職業自由。

如果客戶的關係可以透過對電信往來資料的運用來被揭示，則會因此揭示到律師與當事人之間的委任關係。儲備資料儲存亦嚇阻專家顧問電信連繫的建立，因為它據此可以被得出進一步關於健康和精神狀態、宗教或財務狀況的結論。記者會面臨失去消息來源的威脅。無可估量的公共利益面臨的是負面的影響。鑑於依賴於職業秘密主體的通訊所作成的程序的數量有限，法益保護的利益 (Belange)

在沒有儲備資料儲存的情況下亦得被確保。

同樣，由服務提供商而言，儲備資料儲存亦違反比例原則的要求。關於應予針對經由這部分的投入成本予以補償的規則，並不存在。在缺乏足夠的報酬償付規定的情況下，同樣，考慮到對儲備資料的管理、加工處理及傳送給有權機關的費用，刖無法期待電信企業的考量。倘若不具備足夠的補償，不應強加予他們去履行作為國家的核心任務的刑事訴追和危險防範的義務。

cc)在到目前為電信服務商使用的設備由於儲備資料儲存而不得被繼續使用的情況下，電信法第113a與第113b條亦是類似於對於基本法第14條第1項的徵收的干預。這在沒有足夠的補償下亦是違反基本法第14條第1項。

dd)其次，電信法第113a與第113b條尚侵害基本法第5條第1項。其侵害意見、資訊與廣電等自由。儲備資料儲存使電信變貴。這會強制去造成對財力不足的公民、企業和組織的限制。此外，供需雙方均不敢觸及特別是批評國家的資料。對資訊自由的影響，與被探查的網頁依據電信法第113a條不得被加以儲存這件事並不牴觸。電信媒體的服務商經常在違反電信媒體法(Telemediengesetz) 而儲存用戶的網際網路協定位址。國家機關在此其實應該要依據電信媒體法第15條第5項聯結到第14條第2項而加以介入。意見、資訊與廣電自由對於自由民主而言係結構性的。鑑於對整體社會的資訊交換及對其極微的利用的影響，儲備資料儲存以不合比例的方式干預了基本法第5條第1項。

ee)電信法第113a條與第113b條在許多方面完全侵害基本法第3條第1項規定的一般平等權。

上面所述首先於僅在對於電信網絡的資訊交換，並非直接在空間上的資訊交換，而達成通訊資料的儲存。考慮到對往來資料高的干預強度，這項差異因此無法特別被合理化，因為於直接在空間上的資料交換範圍中常常有同樣地的也許是其他的證明方法(Beweismittel)。

以下這件事亦違反基本法第3條第1項，雖然於網際網路中對資料的使用，並非如報紙，書籍和電視般傳統大眾媒體的(資料)使用般被記錄下來。關於電訊網絡的大眾通訊是特別容易產生損失(schadensträchtig)這件事，並沒有可靠的證據。同樣的，儲備資料儲存並不將非通訊的電腦使用掌握進去，亦是不合理的不平等對待。這件事同樣是侵害基本法第3條第1項，因為立法者不合理的對較溫和手段如技術，結構和辨識的預防措施或快速冰存的選擇不予考慮。

同樣是憲法上較無理由的是下列

不平等對待，介於作為電子的資訊交換和對郵政而言作為遠距的，被形構資訊的交換二者間之不平等對待，電信企業相對於郵政企業二者間之不平等對待，對電信服務的需求與其他服務的需求間之不平等對待，以及電信企業與其他企業如銀行，航空公司間之不平等對待。

其次，對於小型電信企業為平等對待實為侵害一般平等權，因為藉此一群典型案例在沒有充份的理由下，實際上蒙受極大的負擔。

最後，為公共目的而對私營電信企業無補償的適用，並未違反基本法第3條第1項之要求。在此並不符合一項具財政功能的特別公課(Sonderabgabe)的要件。危險防犯和刑事犯罪行為的緝拿係一般性的任務，其財務必須由租稅工具加以償付且對此不應強加於相關企業暨其客戶。

2. 憲法訴願人於第1審判庭BvR 263/08程序中除就電信法第113a與第113b條外，只要在涉及依電信法第113a條被儲存的資料的提取上，亦就刑事訴訟法第100g條聲明不服。憲法訴願人控訴侵害基本法第1條第1項，第2條第1項聯結到第1條第1項，第1條第10項以及第19條第2項。

a)憲法訴願人主張憲法訴願應予受理。

aa)憲法訴願人係多位律師，一位大學教師，一位女出版商，一位財政法院院長，一名學生兼國會或邦議會議員。女憲法訴願人3同時是聯邦司法部長。

他們其中每一個需要多個供應商(Provider)。他們於私人，休閒時或是於其政治活動時使用固網，行動電話，網際網路連線以及電子郵件信箱且因此亦受到對他們的電信資料儲存的關連。

bb)儲存本身係透過私人達成，並未與憲法訴願的受理相對立。因為儲存係直接透過電信法第113a條與第113b條的法律規定被加以規定。

cc)對憲法訴願人而言亦無可能期待，在其提起憲法訴願前各自採取正常的法律途徑。

dd)憲法訴願，只要在立法者就歐洲共同體2006/24/指令的轉換上，雖然在留給立法者的轉換空間上容許關注，而違反成員國的憲法時，或是在立法者超出於該指令中的規定範圍外時，便無論如何會受理。這是考慮到儲存目的，合理化資料使用的刑事犯罪行為，捨棄嚴謹的程序規則，以及有使用權限的單位等等這麼回事。

ee)此外，歐洲共同體2006/24/指令係處於越權而違法(ultra vires)的情況且不得在德國落實法律實效。此外，聯邦憲法法院應針對歐洲共同體的法律行為是否侵害基本法第1條，因此在國內法上無法主張效力，完全由聯邦憲法法院決定。一項先行裁決程

序不得向歐洲法院提起。只要聯邦憲法法院不自認有權限就歐洲共同體2006/24/指令的法律效力本身加以裁判，一項先行裁決程序方得向歐洲法院被加以提出。歐洲共同體2006/24/指令係處沒有法律基礎的情況且與共同體基本權利，特別是與歐洲人權公約第8條不符合。

b)憲法訴願人主張憲法訴願應有理由。

aa)歐洲共同體2006/24/指令，雖然其係在歐洲共同體條約第95條的基礎上頒布，並非為單一市場之建立或運作的對象，而是在舊歐洲共同體條約第29條以下意義下的警察與司法合作的措施，係無實效。

bb)依照電信法第113a條與第113b條的儲備資料儲存侵犯人性尊嚴。在一個自由社會中，任何一個使用通訊工具的人不應該被視為潛在的犯罪人或是擾亂者(Störer)。自由社會不應有不尊重秘密通訊的狀況。個人生活實踐的核心範圍，個人於此範圍中免於國家的監視、控制或影響，是必須被加以保存的。國家經由儲備資料儲存取得一項手段，其摧毀市民對自由通訊的信賴而且使得將來的其他的監控成為可能。此係侵犯人性尊嚴暨民主法治國家原則。

cc)電信法第113a條與第113b條以不合比例的方式干涉基本法第2條第1項聯結基本法第1條第1項的資訊自決權。

依據電信法第113a條的儲存以不具理由且一般的方式達成。被儲存的資料使得個人側寫的建立成為可能。手機使用者的所在地得就最近六個月被加以掌握。對於牽涉到私人生活實踐的核心領域的資料，並沒有對消除的預防措施。供應商並不就記錄資料傳輸和標示被傳遞的資料存量負有義務。

電信法第113b條不符合明確性原則(Bestimmtheitsgrundsatz)。刑事犯罪行為的訴追，對於公共安全的重大危險的防範以及情報部門任務的履行僅是總括的稱為使用目的。對干預目的進一步的專殊化於個別專法上的調取規則中達成。因為基本權的干預藉資料的儲存已達成。依據規範明確性的要求，儲存目的必須精確的被確定。因為各邦就調取規則有權限，故資料的使用係完全不可概觀的。

干預鑑於其門檻與可達成的利用無關。儲備資料儲存對於犯罪對抗(Kriminalitätsbekämpfung)的重大成果並不抱期待。

dd)此外，被撤銷的條款在本質上侵害依基本法第10條保障的遠距通信秘密。

ee)歐洲共同體2006/24/指令允許的決策空間，並未依合憲的方式被履行。電信法第113b條在被儲存的資料為大量情報任務的目的可能被提供的

部分，超出了該指令的目的決定。刑事訴訟法第100g條定義得合理化儲備資料的提取的刑事犯罪行為的範圍並不明確。因為何時當一項刑事犯罪行為於個案中是有重大意義的，無法被確認。反而這件事取決於(儘管人們完全視共同體法是重要的)，且就任一將來的權限規範分別的去解釋，是否其目的決定必然歐洲法的方式去立法且是否合於成員國的憲法。刑事訴訟法第100g條允許為任何藉助電信著手的刑事犯罪行為調取通聯資料，因此超出了本指令的目的決定，即防衛恐怖主義的刑事犯罪行為的範圍。

3.憲法訴願人於第一審判庭BvR 586/08的程序中亦針對電信法第113a條和第113b條以及刑事訴訟法第100g條聲明不服。憲法訴願人控訴侵害基本法第10條第1項與第2項並聯結基本法第1條第1項。

a)憲法訴願人主張憲法訴願應予受理。憲法訴願人(德國國會議員和90/綠黨的聯合黨團成員，其中部分以律師或醫師為副業)係自身直接且現實地關連到其自身源於基本法第10條第1項的權利和其資訊自決權。

此規定同樣因為歐洲共同體2006/24/指令加重很大轉換空間的負擔，得在很大範圍內根據德國基本權被加以審查。被強制固定下來的僅有應被儲存的資料範圍與類型，以及至少六個月的儲存期間。轉換空間彷彿係在於關係到儲存與使用目的，有調取權限的單位，調取要件與程序，目的拘束以及對資料安全的要求等。只要成員國於歐洲共同體2002/58/指令第15條第1項的界限內，似乎有針對危險防範與情報部門任務的履行，預先規定為不同於刑事訴追使用目的的其他使用目的，則是項使用目的貌似屬於無限制憲法上的審查。由儲備資料儲存達成的嚴重刑事犯罪行為，其條款取決於成員國。歐洲共同體2006/24/指令第7條確定了最低要求，即對在各國憲法中的繼續達成的資料保護法的要求不加以阻撓。最後，就儲備資料儲存的財務問題並未在本指令中被加以規定。

此外，一項對關於儲備資料儲存規則的完整憲法上的審查，於當歐洲共同體2006/24/指令為無效，歐洲法院確認該指令無效或是當人們就歐洲共同體發布指令的權限的審查，例外的透過聯邦憲法法院來考量時，則是可能的。一項有效性的先行程序得特別由於侵害共同體基本權被支持。

b)憲法訴願人主張憲法訴願亦應有理由。系爭規定侵害基本法第10條第1項。本條保障通訊過程中鄰近狀態的秘密性。因此依據電信法第113a條第2項應被儲存的電信往來資料，蒐集依據電信法第113a條第3項和第4項應被儲存的電子郵件往來資料和網際網路連繫資料等均屬於其保護領域

中。傳統上被歸屬於廣電自由(Rundfunkfreiheit)的大眾通訊亦於網際網路中運行，與此並不相牴觸。個人的通訊亦被傳播，以上就引致基本權保護亦已足夠。

儲備資料儲存的規定干預了基本法第10條的保護範圍。國家干預係藉由依據電信法第113a條規定的往來資料儲存義務而開始。是項國家干預藉由於電信法第113b條中允許將往來資料傳送與國家機關而延續。其他的干預行為如透過主管訊息的機關的資料的利用和使用，以及資料進一步轉移給其他機關或私人。

刑事訴訟法第100g條係完整法條規定，因為本條合於在個案中亦有重大刑事犯罪行為，且具體的指引於刑事訴訟法第100a條第2項明訂的刑事犯罪行為。刑事訴訟法第100g條第1項第2號的規定考慮到刑事訴訟法第100g條第1項第2句是該被較批評的去加以評價。資料調取何時與事物的重要性間成恰當關係，對公民而言無法以被要求的明確性去認識。電信法第113b條的明確性同樣是有問題的。對於危險防範與情報部門的範圍而言下面這件事是無法預見的，亦即被授權的機關准以何種範圍對儲備資料加以調取。

此外，儲備資料儲存侵害比例原則。有效的刑事訴追雖是合法的目的。然而儲備資料儲存的妥適性與必要性不容被否定。快速冰存程序並不同樣夠合適，因為其於當往來資料不或不再存在時則會一無所獲。然而儲備資料儲存是不恰當的。往來資料允許大量追溯溝通或運動行為。基於往來資料的自動利用性，往來資料對於透過情報部門的間歇追捕方法與策略性監察而言是特別的妥適。往來資料提供查明方法且允許對社會，政治或經濟的關係網絡加以重構。完整的個人側寫得被加以建立。無懷疑的儲存與儲存的不同尋常的擴散幅度有特別負擔的作用。此外，加諸於整體社會的行為模式與民主論述上的反作用力，以及濫用憂慮是應被關注的。

刑事訴訟法第100g條超出了為歐洲共同體2006/24/指令的轉換所必要的標準，因為對依據電信法第113a條被儲存資料的調取，一般而言亦得因藉助電信著手的刑事犯罪之故而達成。對於儲備資料的調取，中度的犯罪即已足夠。儲備資料儲存會升高以下的風險，即判定不公平的嫌疑且藉此成為以之為對象擔負的偵查措施。資料調取是秘密達成的。刑事訴訟法第100g條第2項聯結到刑事訴訟法第100b與第101條僅保障持續的，透過有限報告實踐被弱化的法律保障。法官保留的有效性是有爭議的。迄今為止的調取可能大多數是足夠的。於關注替代的偵查方法如快速冰存程序，恰當性審查結果是負面的。

電信法第113b條第1句第2號已允許為公共安全的重大危險而調取不需理由被儲存的資料。情報部門的監視措施係在明顯減低的法律保護可能性上於具體危險的準備階段即達成。對國會（議會）的電信監督的限制並不存在。電信法第113b第1句第1和2號的規定，鑑於其對公民的行為與民主論述的先行效果，是不恰當的。

職業秘密載體並未被分開來加以保護。這件事在醫生與非以刑事辯護為全職的律師上特別有影響。此外，對於服務供應商而言，缺乏資料確保結構指標。這件事隱藏了重大的濫用危險。尤其透過私人為行使如電信法第113b條第1句後半段允許的民事法上請求權所為之資料利用這件事是不恰當的。因為依照這樣的方式僅有連線所有人得被查出，但連線所有人並不強迫地要與網際網路使用人就很大的範圍中去考慮到對未能與者加以追蹤這件事上一致。

依據電信法第113a條第10項，應於電信中顧及必要的注意且應透過技術與組織的措施確保，被儲存的資料僅令獲特別授權之人探訪的義務，並未被更進一步具體化。資料安全並未如此被充分保障。干預的力度並未透過干預的剩餘價值被抵銷。干預正好於組織犯罪與恐怖主義係最低的，因為行為人於此可能籌集的能量，可能是很輕易的破壞儲存的。儲存加諸於民主論述上的反作用力與資料濫用的危險無法完全透過對使用目的的限定來加以減低。

III.相關機關團體的意見

聯邦政府，聯邦行政法院，聯邦法院，聯邦個資保護監察官(Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) 等，並由柏林資料保護和個資保護監察官 (Berliner Beauftragte für Datenschutz und Informationsfreiheit) 以各邦個資保護監察官之名義就憲法訴願提交了他們的意見。

1.聯邦政府視憲法部分訴願應為不予受理，無論如何是不具備理由的。

a)憲法訴願在其僅聲明不服電信法第113a條與第113b條的範圍內不應予受理。

aa)在合於歐洲共同體2006/24/指令的義務規定範圍內，電信法第113a條與第113b條不屬於聯邦憲法法院的審查權限。只要規定的游動空間(Regelungsspielräume) 存在，則聯邦法律上的轉換便指向歐洲共同體2006/24/指令的最低規定標準 (Regelungsminimum)。於此並無一項造成中斷的法律行動，因為其並未涉及歐洲共同體與成員國間的權限分配，而僅是涉及在歐洲聯盟(Europäische Union)內的權限分配。在歐洲的層面上完全有充分的基本權利保護。一項對於人

性尊嚴的侵犯同樣也並不明顯。

bb)憲法訴願人係因為共同體法的優位而沒有提請訴願的權限。電信法第113b條第1句第1號和刑事訴訟法第100g條並未超越透過歐洲共同體2006/24/指令所設定的儲存目的。就嚴重犯罪行為的定義而言，藉助電信設備而遂行的犯罪行為亦需恰當地被加以注意。歐洲共同體2006/24/指令允許儲存目的貫徹於危險防範和情報部門的任務履行的使用上。電信法第113b條第1句第2和3號僅僅其他法律上的使用規定。然而這些規定單純在憲法訴願程序中並不具備指控適格，因為其並未觸及基本權利上的、超出自身透過歐洲共同體2006/24/指令所列出的訴因的關聯性。一項附帶的的訴願只能由授權被儲存的資料作進一步使用的有權規範中得出。電信法第113b條並未包含這樣的規定。在此被規定的目標設定毋寧僅限於可能的資料使用。考慮到由訴願人行使的職業如律師或新聞記者，電信法第113a條與第113b條進一步不具備去規範職業的傾向。於此不觸及基本法第14條。儲存義務並未縮減相關企業的服務權利，而是訂下一項獨立的行為義務。對於意見自由的侵害自始並未發生。依據電信法第113a條的儲存即為無涉於意見的。

cc)女憲法訴願人4於第一審判庭BvR 256/08程序中的憲法訴願因補充性原則(Grundsatz der Subsidiarität)而敗訴。是否法律保障是不可能經由普通法院達成這件事，在此並不清楚。

b）憲法訴願全部無理由。

aa)電信法第113a條在憲法上應是無疑義的。

(1)政府干預基本法第10條的保護領域。然而在此僅涉及私人為使稍後可得獲取的目的而保存特定資料的義務。為此對於被保存的資料，電信法第113a條在類型上將權限規範與國家的使用區分開來。電信法第113a條構成對基本法第10條的中度干預。本條僅導致，對關係人而言，就六個月的資料取消其刪除請求權。被儲存的資料不涉及通訊內容。這些資料僅基於其他合格的權限規範而進入國家的認識範圍。最後，儲存並非以秘密的方式完成。應被加以儲存的資料與儲存的存續期間亦應被明確且完整的加以定義。

電信法第113a條之目的係在於，以現代通訊科技的條件去用以對抗恐怖主義和對抗嚴重犯罪。電信法第113a條係合於這項目的。本條阻止刑事訴訟法第100g條，透過漸增加的一次付費期限內無限使用－協約(Flatrate-Tarif)暨與此相連追溯依據電信法第96條被儲存的資料，以及透過刑事罪犯持續利用網際網路，而失去其基礎。

對往來資料的利用於刑事訴追是

不可或缺的。特別是其得完全就行為時點的線索，嫌犯於犯罪現場附近的停留處，犯罪嫌疑人之前行為與後行為，犯罪嫌疑人彼此間的連繫，逃亡路線的描述以及為偵查其他的犯罪嫌疑人等而被加以取得。特別是就麻醉品犯罪(Betäubungsmittelkriminalität)的訴追而言，定位資料(Standortdaten)是很重要的。往來資料對於起訴被告或是偵查被告的下落的驗證上亦有意義。網際網路中未成年色情演出的傳播的發現於實際上僅得依賴往來資料達成。就特別以企業經營方式從事的犯罪行為而言，溝通行為的認識對於組織結構和連續犯罪事實的發現是至關重要。對資料儲存的妥適性加以反對亦無法顯示出迴避往來資料的可能性。

此外，電信法第113a條是必要的。快速冰存程序並不同樣有實效。該程序僅得確定那些以任何方式被儲存的資料。該程序僅當其涉及關連到存在的事實時才是有意義的。

最後，電信法第113a條是恰當的。(對儲存)的不具理由，自始並未排除儲存的拾為性。不具理由 (加以儲存)的擴散幅度並不論及與此具體相關的負擔。對牽涉個人資料的儲備蒐集並非自動違反憲法的。這些資料係由私人企業依特定目的被加以儲存且直到基於其他權限規範方得由國家所獲知。依據電信法第113a條被加以儲存的資料雖然允許被追溯到關係人的人格，然而只是有限的觸及。這些資料可能並未觸及通訊的內容而且考慮到與其人格相關時，故其不會逾越依據其他規定應被儲存的資料。這些儲存成否總是不確定的。保存資料的義務對德國法律而言，大概較常見是源自於商事法、德國稅捐通則(Abgabenordnung)或是德國金融事業管理法(Kreditwesengesetz)。聯邦憲法法院僅是就詢問要件(Abfragetatbestände)發展憲法上的界線。此外像這樣的儲存亦非不恰當。然而資料調取需限於以合格的方式為之。六個月的儲存期限透過對具體的犯罪行為的訴追的條件被證成。透過電信法第113a條並不會引發寒蟬效應(Einschüchterungseffekt)。決定性的並非是規範相對人(Normadressaten)的主觀感受，而是一個恰當的規範理解。

(2)電信服務提供商因儲存而生的費用既不侵害基本法第12條，也不至於侵害基本法第14條。基本法第14條並未對於企業財產作一般性的保障。但電信法第113a條對於訴願人的企業所牽涉到的既非實體的權利，亦非形成權。去除科技設施所為的報告並非實質上的。同樣職業自由在此亦未被觸及。訴願人想來不至於因無系爭規定而從事其職業。服務商在此僅負擔附加的義務。為顧及公共任務的履行的利用本身並未引起損害請求權

(Entschädigungsanspruch) 。

(3)系爭規定與基本法第3條第1項一致。電信和直接的通訊無法彼此相較。直接的通訊與電子通訊無法以同樣的方式被加以儲存。介於電信和郵政間作不同等對待是合理的。慢速郵件式的溝通比起電信對於犯罪行為的利用較不合適。大型與小型的電信企業不會被平等對待。保障相應的自由權免於不平等的經濟上影響力的並非一般平等權。一項違反平等的特別公課並不成立。

(4)對於資訊安全，係符合憲法上的要求。電信法第109條第1項課予服務提供商採取合理的技術上預防措施，或其他措施，以確保資料的保護，遠距通信秘密和電信和資料處理系統的保護免於員工和第三方未經允許的訪問的保護。依據電信法第109條第1項規定，電信設施的經營者有義務向聯邦網路局提交一項描述為履行資訊安全義務的技術上預防措施，或其他保護措施的安全計畫。且其應應聯邦網絡局之要求而增補與完善。服務供應商依據電信法第113a條第10項規定，應該顧及在電信範圍內必要的注意且就資料的造訪透過特別授權而加以限制。對於遠距通信秘密和資訊保護法上要求的侵害係依電信法第148條受罰金刑或依電信法第149條第1項第16至18號受行政罰金的保障。電信法第115條允許聯邦網絡局去執行資料保護的規則。最後，企業就資料保護與資訊自由將受到聯邦網絡局的管制。

bb)電信法第113b條亦是合憲的。其界定儲存的目的且對之詳細的加以規定。資料的使用指向其他法律規範，就其確定性需要特別的審查。依據電信法第113b條第1句第2點，為危險防範的資料使用，非為迫在眉睫的危險，比起對於電信的內容上的監督上係較小的干預，不合於高層級的法益的門檻。法官保留保在各自的授權規範中被加以規定。為情報任務的履行的資料傳送，依據電信法第113b條第1句第3點不受指摘。在一定限度內，甚至於為情報任務的目的對電信內容作不具理由的管制在過往被裁判為合憲法的（引證：BVerfGE 100，313 <358ff.>）。

cc)刑事訴訟法第100g條亦屬合憲。刑事程序上往來資料的詢問的可能性，以到目前為止的形式是被承認的。因為可能有更多的資料被提供的情形下，所以訪問依據電信法第113a條被儲存的往來資料尚非一項對電信秘密在比較上更密集的干預，鑑於相較對於電信的內容上的監督上為小的力度，於當刑事訴訟法第100g條就資料調取的許可上要求較刑事訴訟法第100a為寬鬆的這件事上是前後一貫的。

只要刑事訴訟法第100g條第1項

第1號聯繫到刑事訴訟法第100a條第2項的犯罪行為所列舉者，且主張一項犯罪行為亦於個案上有重大性，聯邦憲法法院認為上述規定是充分的。刑事訴訟法第100g條第1項第2號同樣是無疑問的。刑事訴追手段的選擇取決於能否徹底掌握出現的犯罪行為的可能性。刑事訴訟法第100g條第1項第2號與刑事訴訟法第100g條第1項第2句可能有將這件事考慮在內，以便其針對借助電信從事的犯罪行為，於缺乏替代的偵查手段與受進一步的比例原則審查下，而提取是項往來資料。儘管刑事司法享有憲法地位，一項對調取可能性的擴大限制於電信的全部範圍中是免於刑事訴追的。刑事訴訟法第100g條亦並未侵犯私人生活形構的核心範圍。倘若除去藉電信往來資料之助去建立溝通側寫與運動側寫的可能性，則刑事訴訟法第100g條就不會以密集的方式侵犯私人生活形構的核心範圍。

2.聯邦憲法法院認為系爭規定為一對基本法第10條第1項的干預，該干預的正當性是有疑問的。於電信法第113b條第1句中被列舉使用目的被太廣的掌握，以致於在儲存的時點仍未得預見，該資料得依何種目的被加以使用。於此基於侵害禁止為不確定或仍未得確定的目的以儲備方式蒐集與個人有關的資料。基本權限制亦非不缺明顯份量的。儲存義務包含了具高度個人相關，允許明顯的追溯到使用者的人格和個人關係，社會的範域（Umfeld）以及各別溝通內容的方式等的資料。對個人側寫的建立是可能的。資料儲存於刑事程序的案件中得對個人有巨大的影響。資料濫用是可能的。儲存具備極寬廣的效應。儲存的擴散幅度會造成很大的寒蟬效應。另一方面，資料於許多案件中會於未被傳輸與國家單位時就被加以刪除。使用目的不限於對高位階法益的保護。由電信法第113b條第1句第2號無法導出何種法益得對資料使用加以合理化。

3.聯邦最高法院透過第一刑事庭主席與一調查法官指出，就藉助電信著手的刑事犯罪的，使對犯人的確認成為可能的資料，往往於查詢回覆時已被刪除。對使用的內容加以推論於網際網路使用上被排除。緣於一次付費期限內無限使用－契約(Flatrate-Verträgen)的流行性，資料管線(Datenleitung)經常是全天24小時被維持。在此種情形下關於網際網路使用的次數與時間持續的資訊，不再能準確無誤地由被儲存的資料中得出。於電子郵件往來的範圍中，網際網路協定位址的儲存於通聯結束後，於導入儲備資料儲存前僅得於特定要件下得被加以儲存這件事，尤其是必要的。因為網際網路協定位址近年來平均於一至二天後被加以刪除，就財產犯罪行

為或兒童色情犯罪行為進行刑事訴追多半是不可能。對網際網路中的刑事犯罪行為而言，沒有儲備資料儲存就幾乎不存在被發現的風險。一個法外空間將產生。聯邦最高法院院長(Präsident des Bundesgerichtshofs)指出，往來資料似乎只有表徵效用(Indizwirkung)且需要透過其他的偵查結果的支持(Untermauerung)。因此社會行為的範圍並非已是法外空間，因為對社會行為的預防性監督在此尚不被考慮。

4.聯邦個資保護監察官認為依據電信法第113a條的不具理由的資料儲存是違憲的。由不具理由的資料儲存的違憲性繼之認為電信法第113b條的傳輸規定是違憲的。刑事訴訟法第100g條是違憲的，因為使用門檻不適當地被低度定義。同時(系爭)規定亦牴觸歐洲人權公約第8條與第10條。

為儲備資料儲存的授權基礎並未被充分地加以規定。使用目的並未被精確地被限定且僅有限被達成。於恐怖主義與組織犯罪領域中刑事犯罪的訴追並未被持續性地被改善，因為相關的行為人群體有各種去避開儲備資料儲存的可能性。

往來資料一直密集的對溝通行為加以描摹。資料於涉及與職業秘密主體的溝通且因此需要不同的規定時是特別敏感的。對應儲存資料的敏感性因技術的革新而持續增加。往來資料使得對於在運動與溝通行為中的行為方式與利益以及進一步達成的觀察等的追溯成為可能。往來資料反映出關係人的社會網路。對於政黨，工會或公民運動等的歸屬性則會是明確的。（往來資料）與關於談話對象的職業或生意活動的資訊使由往來資料去追溯談話內容成為可能。通聯的時間與次數允許對接觸的密度的推斷。完整的個人圖像與社會份量（Soziogramme）得被加以建立。對於利用現代通信手段的信賴會透過儲備資料儲存持續地受影響。濫用危險必須透過法律的規定儘可能多的被加以排除。但電信法既不課予對依據電信法第113a條被儲存的資料的分離儲存的義務，亦不課予安全的密碼化的義務。該法並未包含關於個別調取的調取理由，調取的紀錄以及紀錄資料的審核等的預先規定。

為刑事訴追的資料利用是遠不恰當的。對儲備資料的調取最多於對嚴重犯罪行為的訴追時可被加以考慮。同樣排除告知(義務) (Benachrichtigung)的諸要件係太不確定且必要的個案權衡則不受保障。此外，排除告知的法院審查並未被完全的事先預見。關於為危險防範與情報部門任務履行所為之對儲備資料的使用造成過低調取門檻的危險。同樣的，電信法第113b條使依據電信法第113條為對隱藏其後的人的偵查而使用依據電信法

第113a條被儲存的網際網路協定位址成為可能這件事是不恰當的，因為這件事對於違反秩序犯的追緝亦是允許的。

5.柏林資料保護和個資保護監察官認為透過電信法第113a與第113b條侵害了遠距通信秘密的本質核心。此外，這些規定違反了禁止就不特定或仍無法確定的目的而為儲備資料儲存的要求。無論如何這些規定使對遠距通信秘密的不合比例的限制成為可能。此外，在這些條文中缺少精確的目標確定。電信法第113條第一句後半段使得被儲存的往來資料的使用，於依據電信法第113條對於查詢回覆予許多秩序機關成為可能。透過私人的資料濫用幾乎沒法被阻止。電信法第113a條第6項阻止使用者藉網際網路中匿名服務之助而維持匿名活動。對特別秘密關係的保護並未被考慮到。鑑於對基本權干預的嚴重度，快速冰存程序必須作為替代方法而被審核。對歐洲共同體2006/24/指令的不干擾基本權的轉換的要求，於當被儲存的資料被允許用於對簡易刑事犯罪行為的訴追以及為低價值保護利益的危險防範時，亦被忽視。刑事訴訟法第100g條係不合比例的。刑事訴訟法第100g條第2項第2句令針對重大意義的刑事犯罪行為，於當在查清案情以其他方式可能無望或極度困難時，一項空間與時間上足夠的特定電信標識便可。藉此是持續的，得以觸及數以千計公民的權利的往來資料調取是可能的。立法者於刑事訴訟法第101條第4與第5項中所創設的免除告知義務的空間，同樣是憲法上有問題的。

6.專業諮詢人員 Prof. Dr. Dr. h.c. Hans-Jörg Albrecht，Constanze Kurz，Prof. Dr. Felix Freiling，Prof. Dr. Andreas Pfitzmann，Prof. Dr. Alexander Roßnagel，Prof. Dr. Christoph Ruland，聯邦個資保護監察官，柏林資料保護和個資保護監察官，德國聯邦司法部於聯邦經濟與科技部(Bundesministerium für Wirtschaft und Technologie)與聯邦內政部(Bundesministerium des Innern)的協助下，於第一審判庭BvR 256/08與BvR 263/08程序中的憲法訴願人以及聯邦資訊經濟，電訊與新媒體協會(Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM))，德國網際網路經濟協會(Verband der deutschen Internetwirtschaft e.V. (eco))，電信與加值服務供應商協會(Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e.V. (VATM)) 等人於法院就科技，事實與法律上的問題表達意見。上述問題涉及電信往來資料，儲備資料儲存義務人，藉電信著手的刑事犯罪行為，依電信法第113條之查詢回覆，確保儲備資料免於無權限調取

以及就這些資料利用的可能法律上形構。聯邦司法部的意見在此係由聯邦網絡局關於聯邦經濟與科技部，聯邦刑事局(Bundeskriminalamt)關於聯邦內政部，聯邦憲法保護局以及女聯邦檢察總長等協作。

7.此外，商業電信用戶協會(Verband der Anwender geschäftlicher Telekommunikatione.V.(TELECOMe.V.))，德國圖書貿易協會(Börsenverein des Deutschen Buchhandels e.V.) 以及聯邦音樂產業協會(Bundesverband Musikindustrie e.V.) 等亦表達其立場。

IV.參與言辭辯論程序者

於言辭辯論程序中表示意見者為：憲法訴願人，聯邦政府，聯邦犯罪局，聯邦網絡局，巴伐利亞邦政府，聯邦個資保護監察官，柏林個資保護監察官，作為專業諮詢人員的 Prof. Dr. Dr. h.c. Hans-Jörg Albrecht，Constanze Kurz，Prof. Dr. Felix Freiling，Prof. Dr. Andreas Pfitzmann，Prof. Dr. Alexander Roßnagel，Prof. Dr. Christoph Ruland，聯邦資訊經濟，電訊與新媒體協會，德國網際網路經濟協會，電信與加值服務供應商協會，德國圖書貿易協會以及聯邦音樂產業協會。

B.憲法訴願程序合法被受理

I.基本權受侵害的可能性

1.憲法訴願人以受理方式控訴違反基本法第10條第1項。他們於私人與商業上利用不同的電信服務如特別是電話服務，電子郵件服務與網際網路，且主張，透過對他們的通聯資料之儲存與預先規定使用，他們的保障電信秘密的基本權係受到侵害。因為基本法第10條第1項亦就電信過程狀態的秘密性加以保護 (參照: BVerfGE 67, 157 <172>; 85, 386 <396>; 120, 274 <307>; stRspr)，透過系爭規定的這樣的侵害是可能的。

系爭規定亦直接，本身與當下的關聯到憲法訴願人。雖然電信法第113a條的儲存義務並非針對作為使用者被關聯到的憲法訴願人，而是針對服務供應商。然而前揭情形係沒有任何判斷自由空間 (參照: BVerfGE 107, 299 <313 f.>) 絕對課予對憲法訴願人的資料的儲存的義務。電信法第113a條於此直接且當下的導致為電信法第113b條中規定的目的而對憲法訴願人的資料的儲存。

因此，關聯到電信法第113b條與刑事訴訟法第100g條上，亦不缺乏直接的當事人適格，因為這些條文直到以進一步執行行為為基方產生實效且仍未確定，目前訴願人的資料是否或多廣的被涉及。若當事人未知悉執行行為，則是項說明足以藉由若干這般措施的可能性被涉及(當事人)。在此特別重要的是，是否是項措施具有擴散幅度且亦偶然地將第三方包含在內

。（參照：BVerfGE 109, 279 <307 f.>; 113, 348 <363>; 120, 378<396 f.>）。其後憲法訴願人將其自身與直按的當事人適格充分地加以說明。鑑於可觀的6個月儲存期間及被掌握資料的大擴散幅度，於依據電信法第113b條與刑事訴訟法第100g條對資料的傳輸與使用亦會牽涉到，沒有就相應措施無法給出理由的個人這件事，並不是不可能的。訴願人必須藉說明對刑事犯罪行為的指責，對於當事人適格自的證明而言並不是必要的（參照：BVerfGE 109, 279 <308>; 113, 348 <363>; 120, 378<396 f.>)）。同樣的憲法訴願人不需就下列事項多說，亦即為公共安全的重大危險負責或就涉及情報部門的任務去採取行動。

2.女憲法訴願人4)於第一審判庭BvR256/08的審判程序中所提之憲法訴願亦考慮到基本法第12條第1項，只在女憲法訴願人針對與儲存義務相繫的技術與財務負擔的範圍內而予以受理。作為一項匿名服務的女服務供應商，其同時亦經營一向公共開放的伺服器，原則上於不受補償或損害賠償規定（Entschädigungs- oder Ausgleichsregeln）拘束下，負有電信法第113a條規定之義務。因為係以止罰金防對該義務之忽視（參照：§ 149 Abs. 1 Nr. 36, Abs. 2 TKG），對該女性供應商而言亦不可被期待，首先，於違背電信法第113a條之規定而不執行且反之去尋求專業法庭的法律救濟（參照：BVerfGE 81, 70 <82>）。女服務供應商對此是透過儲存義務直接，本身且現實的牽涉到她的職業自由。

II. 憲法訴願於轉換歐洲共同體2006/24/指令所被頒布的系爭規定部分應予受理

憲法訴願於轉換歐洲共同體2006/24/指令所被頒布的系爭規定部分並非不予受理。

然而聯邦憲法法院原則上並不行使就關於作為對於德國法院和機關於德意表聯邦共和國的高權領域中的行為所需的基礎的共同體法或現在起的聯盟法的適用性的審判權，而且只有在歐洲共同體（或今日歐洲聯盟），特別是歐洲法院的裁判，普遍的對基本權的有效的，對於由基本法各自作為無條件要求的基本權保護於實質上平等被關注的，特別一般對於基本權的本質形構擔保的救濟加以保障時（參照：BVerfGE 73, 339<387>; 102, 147 <162 f.>），方不依基本法的基本權利標準對本法加以審查。這些原則亦對內國的法律規定，將指令的強制指標轉換至德國法中這件事有適用。不服對歐洲聯盟以此種意義上拘束的法律的適用而提起的憲法訴願，原則上應不予受理。

然而憲法訴願人得於當立法者就聯盟法的轉換有形成自由，亦即透過

聯盟法並未被確定時主張基本法的基本權利（參照：BVerfGE121, 1 <15>）。此外現有的憲法訴願於當系爭規定以有強制性內容的指令規定為依據時方予受理。憲法訴願人以對於歐洲共同體2006/24/指令缺少共同體法上的權限基礎且該指令侵害歐洲基本權保證。這件事作為理由。此外憲法訴願人因此於，沒有以其得直接依此針對聯盟法律的憲法訴願作為向專業法庭的理由，而致力於一項法律案件透過聯邦憲法法院依照關於歐盟運作方式條約第267條（前歐洲共同體條約第234條）以先行裁判程序的途徑移轉案件到歐洲法院以求確認該指令無效，且為對系爭規定依德國基本權的標準加以審查排除障礙。無論如何，依訴願人要求以此種方式依照基本法的基本權標準對系爭規定進行審查的作法自始未被排除。

C.憲法訴願係基本上有無理由的審查

I.本案不必以先行程序移轉予歐洲法院

憲法訴願係實質上受理。系爭規定侵害憲法訴願人基於基本法第10條第1項的基本權利。向歐洲法院移轉的先行裁決程序在此不考慮，因為其並不涉及共同體法的可能優位。基本法的基本權利保障並不排斥對歐洲共同體2006/24/指令的（另一種的形構）轉換。

女憲法訴願人4)於第一審判庭BvR256/08程序中的於其指控侵害基本法第12條第一項的憲法訴願不具理由。

憲法訴願並未就依據關於歐盟運作方式條約第267條以先行程序移轉歐洲法院給予理由。雖然於當就共同體法或聯盟法的解釋或效力上有疑問，要求優先於內國法且聯盟法的轉換原則上不依照基本法的基本權標準被加以審查時，則得特別考慮透過聯邦憲法法院（參照：BVerfGE 37, 271 <282>）的一項相應的先行裁決程序。然而僅於當取決於聯盟法的解釋或效力時，一項這樣的先行裁決程序方得被允許與被要求。前揭於現今並不是這種情形。

歐洲共同體2006/24/指令的效力與可能由此導出的共同體法對德國基本權的優位二者並非重大決定性的。該指令的內容保留予德意志聯邦共和國就由其被規定的電信往來資料儲存中一項廣泛的決定空間。該指令雖就此課予成員國，對向公共開放的電子溝通網絡與溝通服務業者就對實際上所有的電信往來資料就至少6個月儲存，加以規定（歐洲共同體2006/24/指令第1，第3，第5與第6條）。對此這些規定本身實質上限於儲存義務且並未就透過成員國機關的資料的探訪

或使用加以規定。本指令既未就透過有權的國家刑事訴追機關的資料造訪問題，亦未就機關間（參照：EuGH, Urteil vom 10. Februar 2009 - Rs. C-301/06 -,Rn. 83）就這些資料的使用與交換問題作特別的調和。由該指令（歐洲共同體2006/24/指令第7與第13條）的最低要求出發，於成員國同樣需採取對資料安全，透明性與法律保障等的保障的必要措施。

本指令藉前揭內容得於不侵害基本法的基本權的情形下被加以轉換。基本法並未於所有情況下禁止這般的儲存。毋寧是這樣的儲存同樣不取決於共同體法的某些優位，而依基本法的基本權的標準容許性的被加以命令（見以下IV）。因此，依德國基本權的標準對系爭規定的審查並不致於陷入抵觸歐洲共同體2006/24/指令的情況，以致於存在此指令的效力與優位性，並不是重要的。

II. 系爭規定侵害了基本法第10條第1項的規定

1. 基本法第10條第1項係保障藉助電信往來，非形體上的資訊傳送(參照: BVerfGE 106, 28 <35 f.>; 120, 274 <306 f.>)至個別收訊者，保護其免於公權力獲知的電信秘密(參照: BVerfGE 100, 313 <358>; 106, 28 <37>)。是項保護不只包含通訊的內容。毋寧通訊過程更具體的狀態的秘密性亦受保護，特別屬於該通訊過程更具體的狀態的係介於那些人或電信設施間就是否、何時以及多頻繁的開始或嘗試進行電信往來(參照: BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 f.>; 115, 166 <183>; 120, 274 <307>)。

透過基本法第10條第一項的保護不僅對第一次公權力由其中取得通信過程與內容的認識的調取。該保護的保護效果亦及於繫於對受保護的通信過程的掌握以及由所獲取知識的使用的資訊與資料加工過程（參照：BVerfGE 100, 313 <359>）被認為基本權干預的是任何對通信資料的確認、記錄和利用，以及透過公權力對這些資料的內容或其他使用的任何運用（參照：BVerfGE 85, 386 <398>; 100, 313 <366>; 110, 33 <52 f.>）。對於電信資料，其儲存，藉由其他資料的校正，其供其他使用的選取或傳輸與第三方等等之掌握在此均是自身對電信秘密的干預（參照：BVerfGE 100, 313 <366 f.>）。因此對電信企業下令就電信資料加以收集、儲存與傳輸與國家單位等，均個別是對基本法第10條第1項的干預（參照：BVerfGE 107, 299 <313>）。

由基本法第2條第1項聯結基本法第1條第1項導出的資訊自我決定權除基本法第10條外並不適用。基本法第

10條於涉及電信方面包含一項特別的排除一般條款且本身由對於透過遠距通信秘密干預獲取的資料所得出的特殊要求的保障。

不過，就這點而言，聯邦憲法法院自基本法第2條第1項聯結基本法第1條第1項所發展出來的標準，得儘可能地被移轉於基本法第10條的特別保障上（參照：BVerfGE 100, 313 <358 f.>）。

2.a)在電信法第113a條第1項強加於電信服務業者的對電信往來資料的儲存干預電信秘密。這件事首先適用於涉及依據電信法第113a條第2項至第5項暨結合在此依照電信法第113a條第6與第7項的儲存義務。對此，應儲存的報告給出關於，在那些電信設施之間是否、何時、何處以及多頻繁取得或嘗試取得通聯等的訊息。這同樣地適用於依據電信法第113a條第3項電子郵件服務的資料的儲存，該電子郵件的秘密性同樣係透過基本法第10條第1項被保護（參照：BVerfGE 113, 348 <383>; 120, 274 <307>）。電子郵件即令於技術上容易被攔截這件事，亦不改變它們的秘密性格與它們值得保護的性質。依據電信法第113a條第4項的規定對涉及網際網路通路的資料的儲存亦構成對基本法第10條第1項的干預。雖然網際網路通路不只使取得屬於電信秘密的個別通訊成為可能，而且亦使對大眾通訊的參與成為可能。因為，個人與大眾通訊間的區分，在沒有與基本權利的保護功能相背立的，對各別被傳輸的資訊的內容上的聯繫是不可能的，則在對這些作為這樣的網際網路通路所涉及的資料的儲存中，儘管這些資料並未包含關於被造訪的網頁的報告，仍應被視為係一項干預（參照：Gusy, in: v. Mangoldt/Klein/Starck, GG, Bd. 1, 5. Aufl. 2005, Art. 10 Rn. 44; Hermes, in: Dreier, GG, Bd. 1, 2. Aufl. 2004, Art. 10 Rn. 39）。

電信法第113a條的干預品質並不受該條未規定的儲存不是由國家本身，而是由私人服務供應商達成而有疑問。因為這些私人服務供應商僅係作為需要透過國家機關履行任務的輔助人。電信法第113a條課予私人電信企業依據電信法第113b條僅就為刑事訴追、危險防範與情報部門任務履行等目的而透過國家機關的任務履行的資料儲存義務。在這種情形下國家直接於未給予負儲存義務的企業行動空間的情形下，就與儲存相繫的基本權干擾；資料以如下的方式被儲存，即有權限的官方單位的訊息查詢，依據電信法第113a條第9項得立即被履行。依此項要件，對立法者而言資料的儲存在法律上被歸責為對基本法第10條第1項的直接干預。（參照：BverfGE 107, 299 <313 f.>）

b)對基本法第10條第1項的基本

權干預亦處於電信法第113b第1句前半段中的資料傳輸規定中。雖然本條（電信法第113b條）的規定並未允許就依據電信法第113a條被儲存的資料的使用，而是將之移轉於其他法定自行應創設的調取規範上。然而於這些調取規範中有關於資料應就何種目的被使用的基礎的規定。關於這一點這些規定免除電信企業在規定中另外生效的保密義務。資料使用直到於不同規範層級的條文的有層次的交錯連接上取得其全部規定這件事並不改變下面這件事，即使用目的的定義與資料傳輸的允許均係使用規定的一部分且在這範圍內具備干預性格。電信法第113b條涉及到由私人服務供應商方面的資料傳輸這件事，在此亦是不重要的。事先預見的傳輸係基於法律規定且在此直接基於依照基本法第1條第3項受基本權拘束的公權力行為，於個案中預設高權的命令且於機關達成。在這件事上該傳輸於法律上被視為國家的干預。

c)電信法第113b條第1句後半段連結電信法第113條第1項亦是構成對基本法第10條第1項干預的理由。機關據此得依據電信法第95條、第111條向服務供應商主張關於僅於對就依據電信法第113a條第4項被儲存的資料的利用方得由服務供應商加以傳輸的基本資料和客戶資料的訊息。先不論以下的問題，於依據電信法第113條的訊息一般而言，是否與多廣成立對基本法第10條第1項的干預，或者換句話講，是否就這點而言，資訊自決權原則上僅於依據基本法第2條第1項連結基本法基本法第1條第1項是有關的，無論如何需肯定對於依據電信法113b條第1句後半段，第113條第1項的訊息係對基本法第10條第1項的電信秘密的干預。因為在此係規定依據電信法第113a條被儲存且在此透過對基本法第10條第1項的干預而取得的資料的利用。任一對曾以干預基本法第10條第1項的形式所取得的資料的後續使用總是必須依此基本權被衡量（參照：BVerfGE 100, 313 <359>; 110, 33 <68 f.>; 113, 348 <365>）。同樣，於此亦不取決於，此項法律上預先規定的利用並非透過公權力本身，而是（訊息聲請的引入）透過私人供應商而達成。

d)刑事訴訟法第100g條最後亦構成一項對基本法第10條第1項的干預。該干預使得將依據電信法第113a條被儲存的資料由負儲存義務者處傳輸予刑事訴追機關且被其利用一事成為可能。刑事訴訟法第100g條第1項第1句本身以及對此項授權的利用因此作為公權力行為同樣干預基本法第10條第1項的保護範圍。

III. 系爭規定合於基本法第10條第2項第1句的規定

系爭規定於形式觀點看是無疑慮

的。系爭規定合於基本法第10條第2項第1句的法律保留且合於聯邦的權限。

1.對電信秘密的限制依據基本法第10條第2項第一句僅得以法律命令之。首先，在這點而言電信法第113b條與刑事訴訟法第100g條（可能與其他條文共同作用）為涉及個案的，依此成功調取資料的命令的頒布構成法律的基礎。電信法第113a條並未將資料的儲存移交予涉及個案的命令，而是本身直接對之規定這件事，於憲法上是無疑問的。基本法第10條第2項第1句亦不與電信秘密的限制直接透過法律相對立（參照：BVerfGE 85, 386 <396 ff.>）。

2.聯邦有立法權限。電信法第113a與第113b條可於基本法第73條第1項第7號中取得其權限基礎，刑事訴訟法第100g條可於基本法第74條第1項第1號與基本法第72條第1項取得權限基礎。

然而，基本法第73條第1項第7號僅直接授權與電信設施的設置與藉電信設備之助的資訊傳輸等之技術面相的規定。直接針對電信利用的內容或方式（參照：BVerfGE 113, 348 <368>; 114, 371 <385>），且預先規定例如針對刑事訴追或危險防範任務為資訊獲取目的所為的電信監察等的規定並未包含於規範之中。這樣的規定係考慮到立法權限而於各自的，以監聽達成其目的的法律領域中加以規定（參照：BVerfGE 113, 348 <368>）。

然而，電信法第113a與第113b條係作為在此需聯繫的資料保護法上規定的部分，根據事物關聯而由電信法的立法權限共同訂定。雖缺乏明顯的權限分配，資料保護的法律原則上屬於各邦的權限之中。然而，依據事物關聯對於資料保護法的聯邦法律上的權限，於聯邦就對分派給其立法的材料於並無資料保護法上的規定對之共同加以規定，於合理方式無法制定時(參照: BVerfGE 3, 407 <421>; 98, 265 <299>; 106, 62 <115>; 110, 33 <48>; stRspr; zum Datenschutzrecht vgl. Simitis, in: Simitis, BDSG, 6. Aufl. 2006, § 1 Rn. 4)成立。對於電信法第113a和第113b條而言，上面所述便是這種情形。電信法第113a和第113b條與電信法就資料保護的規定有關且以資訊傳輸的技術上條件的規定為起點，就涉及電信服務的提供所產生或加工的資料上各別應注意的要求去加以規範。對此，電信法第113a和第113b條直接依賴於屬於電信立法材料範圍的事實。因為介於技術上的傳輸過程與藉此產生的資料間的這項緊密的關聯，關於資料使用的必要資料保護法上規定僅於整體上得透過關於(制定)傳輸過程規定有權限的聯邦立法者加以制定。否則，對於資料處理規則的技術與

資料處理法上規定上，由於矛盾而生瓦解的危險將可能產生。除電信法第113a條與第113b條的規定以及電信法第88條以下關於遠距通信秘密的規定之外，亦包含與此相應的規定。電信法亦於第91至第107條中包含對資料保護完整的，領域專門的規定，這些規定權限上的合法性迄今(大體上明顯的)並未嚴肅的被質疑。

聯邦依範圍得基於此授權基礎制定對資料使用的合於基本權規定為必要的法規。特別是立法者得創設必要的條款，以便於電信法第113a條中規定的資料儲存與將資料傳輸予刑事追訴與危險防範機關以及情報部門，暨該資料為依據電信法第113條的訊息查詢的使用等滿足基本法第10條第1項的基本權利上的要求。對基本法第10條第1項的干預係以該干預目的是領域專門的、精確的及規範明確的被加以規定(參照: BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 115, 320 <365>; 118, 168 <187 f.>)。無疑的，與此有關的聯邦的立法權限僅及於依照資料保護法上觀點暨與此關聯的憲法上要求所被命令的權限範圍內。聯邦就資料調取的授權本身因此無法依據基本法第73條第1項第7號的規定。聯邦對此需要自己的權限名義或是聯邦必須在此就決定權委由各邦。

電信法第113a與第113b條作為原則出發的考量。這二個條文僅限於，透過儲存義務與傳輸規則去為國家對資料的調取去創造要件。反之，對這些要件的履行委由自身資料調取的規則，在無損於就聯邦是否在這種情形下實質的對使用目的作充分的限定的（見以下C V 5與VI 3 b）實質問題情形下，無需於權限法律上對此提出異議。

IV.對電信秘密的干預的實質合憲性繫於合法的共同目的及是否合乎比例原則

對電信秘密之干預是實質合憲的，倘若其屬合法的公益目的，此外尚合乎比例原則(參照: BverfGE 100, 313<359>)，也就是對目的的達成是妥適的、必要的且恰當的(參照: BVerfGE 109, 279 <335 ff.>; 115, 320 <345>; 118, 168 <193>; 120, 274 <318 f.>; stRspr)。

為了在刑事追訴、危險防範及情報部門的任務履行領域內，如其在電信法第113a條113b條所規定的，而設有門檻的使用，而對電信往來資料六個月，不具理由(anlasslos)的儲存，並非自身地就完全不符合基本法第10條的規定。立法者能以此規定來達成合法的目的；為了目地之達成，此種儲存被依比例原則的原意是妥適的且是必要的。又依狹義的比例原則而言，此種儲存亦非從一開始即欠缺證成可能性的能力(Rechtfertigungsunfähigkeit)。在對特別在顧及特別重要性而

依此而來的干預有充分考量的立法形成下，一項不具理由的對電信往來資料的儲存，並非如聯邦憲法法院裁判(參照: BVerfGE 65, 1 <46 f.>; 115, 320 <350>; 118, 168 <187>) 意義下對儲備資料 (Daten auf Vorrat)予以儲存地嚴格禁止。

1.刑事追訴、危險防範及情報部門的任務履行地有效性是合法目的，基本上能夠合理化一項電信祕密的干預(參照: BVerfGE 100, 313<373,383 f.>; 107,299<316>; 109,279<336>; 115,320<345>)，電信往來資料應該預先地，不具理由地被保存的。此外，一個毀棄基本法第10條第1項的自由原則本身的不合法的目的設定，並不因電信往來資料應該預先地不具理由地被保存就已出現。基本法第10條第12項並不禁止所有的資料地預先的保存及儲存本身，而是保障免於這種不合於比例關係的資料蒐集之形成，尤其應免於漫無目的的設定的蒐集情況。嚴格被禁止的僅是為了不確定的目的或尚不明的目的所做的個人相關的儲備資料予以儲存(參照: BverfGE 65,1 <46>;100,313<360>)。然而，一種預先的不具理由的資料儲存僅為有例外狀況始是允許的。此種允許狀況必須遵循嚴格的要求，不論是基於許可的理由亦或基於許可的形成，尤其是與先前預見的使用目的的關聯性而言。

2.一種電信往來資料預先的不具理由的儲存而至後來因相關理由而傳輸到主管刑事追訴或危險防範的機關，或者是情報部門的任務的履行機關，是立法者可以認為對目的達成是妥適的方法。藉此方法，使此外無法釐清的可能性出現或基於電信在眾多的犯罪行為準備及實行犯行，也日益增加的重要性，起了有效的釐清的可能性。至於被立法者制定的規定是否能做到，去對所有電信連線無漏洞的加以重建，則是無關緊要的。於此亦也適用於下列情況，若一種如此的資料儲存並不能確保所有電信連線皆可信地被提供聯結的業者(Anschlussnehmen)所能處置的，即像罪犯(犯罪集團)能夠利用無線熱點(Hotspot)、網咖、外國的網際網路通話服務或以假造名義登錄的預付費用手機來規避儲存，則此亦不能阻擋此種規定的妥適性，這規定並不需求規定的目的在每個個案事實上皆被達成，而僅要求其有助於目的達成即可(參照: BVerfGE 63, 88 <115>; 67, 157 <175>; 96, 10 <23>; 103, 293 <307>)。

3.立法者可以判斷，電信往來資料六個月的儲存亦是有必要性的，與之較不侵害性的方法，其也能同樣達成案情釐清的措施，並沒有被見到。一種相較之下同樣有效的釐清可能性，並不存在於所謂的快速冰凍程序，其代替一概不具理由的電信資料儲存

，僅在個案且是在某時間點才開始，規制其儲存即大約因對一特定的犯罪行為嫌疑有對其具體的理由存在為起始時間點。這樣一種程序僅能對在儲存規制之前時間的資料，只要其還存在，一加以掌握，反正是不能如連續儲存的有效果，概連續儲存保存在最後六個月完整的資料存續狀態的原貌。

4.電信往來資料六個月的儲存以在電信法113a條範圍內的情形，並非自始即不符狹義的比例原則。

a)畢竟在這種儲存是關於一種特別嚴重的干預，且是以一種至今法秩序不熟悉的廣泛擴散影響:即實際上，在整整六個月的期間所有公民的全部電信往來資料皆被掌握，不論是否有與一可歸責而可非難的行為或一僅僅是抽象的危險性相連結。儲存在此關係到日常行為，且是在日常生活上相互之間基本的在現代世界的社會生活中的參與不再可以捨棄的日常行為。基本上，電信上無任何形式原則上例外儲存。雖然規定在結果留有個別的漏洞，以防止毫無例外的每個電信連線能夠個人化式地被重建，如在無線熱線使用的某些狀態下，無法窺視的私人網路伺服器或歐體以外之外國服務業者，然而一種一般性的迴避可能性並無對公民開啟此種效果。再有甚者，立法者嘗試基本上如此來掌握所有的電信連線，以致使用者能夠最大可能地地毯式的被偵查到。

這些電信往來資料的訴說力(Aussagekraft)是廣泛的，愈依由被涉及者方面的電信服務使用，就促使由資料本身且當然地能更進一步的做為繼續偵查的連結點來使用，將深入獲得每位公民所處社會環境及個別的行為的風貌。雖然，電信往來資料儲存，如其在電信法第113a條所見，僅是通聯資料(時間點、持續、參與的連結及在行動電話通話地點)的確定，而不包含電信的內容。然而，由這些資料在全面地且自動化的篩選可導致直到私密領域充分的內容的回推被撈出來。電信交談的接受者(他的特定職業團體的歸屬、制度或利益團體或由其提供之貢獻)、資料、時間及通話地點允許，倘若它們在一段長的期間被觀察著，經由組合而對那些人對社會或政治歸屬及個人的偏好、傾向、弱點的詳細陳述皆可由其通聯資料所篩選出來。因此，在此方面，就沒有秘密保護。依賴電信及未來以更增強的密度的使用，這樣一種的儲存，實際上有可能對每個公民構作出有說服力的個人人格特徵及動態側寫。若涉及群體及社團，則資料超出此處之外，還可以在某些情況下，揭開其內在影響結構及決策過程。

這種（目的外）使用基本都受許可或在特定情況下應可以如此使用地儲存，的確會造成極其嚴重的干預。

與一個如經常被規定的資料使用的立法形成無關的是大幅的提升公民的風險，暴露於更多的偵查，而本身無需為此給出理由，也是此處要衡量的有力力道(Gewicht)。對於不利的時間點，在一特定的訊號單元 (發話地點)下或與特定人有所接觸而使之在更大的範圍暴露於偵查(Ermittlung)及陷入澄清說明的壓力，就已滿足其力道，同樣也與此種資料蒐集相連結的濫用可能性亦產生更嚴厲的負擔的效應。這種情形尤其常出現，因為有多數不同的私人服務業者，而電信往來資料即儲存在他們手上。基於負有儲存的義務人的數目的觀點可以接觸到及必須接觸到這此資料的人的數量已相當大。因為儲存義務也包括較小的服務業者，免於濫用的安全無視於立法者所有可能且必要的嚴格要求，在考量他們的承擔能力時，也會碰到結構性的界線。這種侷限更強烈透過資料管理的要求，及資料到機關傳輸預設高標準的技術管控及高品質的軟體，由此必然地系統偏誤的危險及操控的危機透過有興趣的管理者連接起來。此外，電信往來資料的儲存有特別重要的力道還經由它本身及儲存資料預見的使用對被涉及者而言，直接地並不被查覺。然而，同時它們掌握在秘密期待下進行的連結。循此，不具理由的電信往來資料的儲存，有利於造成一種被監視的迷惘的威脅感出現，亦即在眾多領域侵害基本權不受干擾的感受。

b)雖然有巨大的廣泛擴散影響及與此而來相連結的干預力道，立法者如電信法113a條所預見，導入六個月的儲存義務，在憲法上並非自始即是被禁止的。然而，依照於聯邦憲法法院向來的見解，對國家而言，為了不確定的目的或尚不明的目的，所做的個人相關的儲備資料地儲存，是被嚴格禁止的(參照: BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>)。在對電信往來資料預先的，不具理由的儲存的情況而言，其並非關係到一開始即在任何狀況下皆禁止的資料蒐集形式。倘若它是為特定目的而為之，則此種儲存，在於立法者關照到其與干預合宜的法律的形成內(詳見以下V部分)，則其亦能滿足狹義比例原則的要求。

aa)在此首先要合乎標準的即是電信往來資料的儲存不直接經由國家，而是透過私人服務業者的義務來實行。由此而來，資料在儲存本身還未被統整，而是分散式般地存在眾多的個別企業裡，而無法當作整體提供國家來處分。國家尤其是，概經過適當的規定及技術上防患措施的安全維護的限制，並無法直接接觸這些資料。由國家方面的資料查詢(Abruf)僅在第二步驟且還要是按照法律較詳細設立的判準的具體理由。在立法形成下，

對查詢及對儲存資料的繼續使用的法律授權規定，能在此安全確保儲存不被用於不確定的目的或尚不明確的目的。所以在這種儲存義務的立法裡能夠且必須被確保，一個事實上認識及使用的資料要以明確規範的形式且限制以下列的方式來實行，即更進一步的資料掌握的力道與資料的查詢及事實上的使用僅限於資料蒐集毫無條件的必要部分。儲存與查詢結構性地分離同時促進資料使用的透明及控制，此乃是經由立法的形成來較詳細的確定保護之。

bb)六個月的電信往來資料的儲存並不以經由自身出發，即已牴觸基本法第10條第1項作為秘密通訊原則。它既不侵害人性尊嚴(基本法第1條第1項)，也非其核心內容(基本法第19條第2項)。雖然它有極度廣泛的影響，它還是實際上有所限制的。因為電信的內容是自外於往來資料儲存的限制之外。同時儲存的持續基於範圍即被儲存資料陳述的能力非常長，還是在比例原則衡量的上限內可以有證成說服力之內。在儲存期限述及每個公民，能相信他們資料(只要他人不是經由重要理由，例外般的被查詢)將被刪除且無人能再重建複製之。

cc)六個月的電信往來資料的儲存本身並不是一項標準，而是對公民通訊與行動的全面掌握。較多的是，被儲存還是以有現存在的方式來連結現代世界通信的特別重要性，且對與電信結合的特殊危險可能性來回應。新型態的電信方法以一種與其他通訊形式不可比擬的方式來超越時間與空間且基本上排除其公開性的感受。它們同時以此方式，減輕了隱藏的通訊與犯罪行為者的行動，並促使分散各地的較少眾的群體，集結及有效地集體運作。經由實際地無抵抗的通訊，使知識、行動準備及犯罪能量的結合成為可能，而對危險防範及刑事追訴產生新的挑戰。一些犯罪行為直接借助新科技而得逞。而且在現有科技相互溝通的電腦及電腦網路的相連結，這些行動更是不易被察覺。同時它們(如約略經由攻擊電信的第三者)也發展成新型態的危險。因此，正是電信連線的重建是對有效的刑事追訴及危險防範有特別重要性。

此外，基於電信資料缺乏公共可感知性 (öffentliche Wahrnehmbarkeit)，也沒有社會記憶性（gesellschaftliches Gedächtnis），不像在其他領域，過去的行動在偶然的回憶的基礎上還可以重建:電信資料或者被刪除而完全遺失，或者將被儲存而一直可以完全來存取。因此，立法者可以，對多遠刪除或儲存這種資料的問題的決定時，做出利益衡平及在此國家的任務接受的關聯加以考量。在此，立法者亦得將下列納入的契約形成的擴散(如一次付費期限內無限使用

(Flatrate))的增加，在嚴守對契約清算不必要的電信往來資料，及刪除義務的效力下，降低儲存者資料的可處理性。如此一來，也可以使預先的電信往來資料的儲存得到現代電信的特殊性有一特別看待的理由。

反過來，電信往來資料的儲存並沒有要求，即要立法達到一個最大可能性的地毯式的覆蓋的預先的將所有刑事追訴或危險預防有用的資料皆儲存。這種立法，不必論及使用規定的形成，可能一開始就不符合憲法。預先的、不具理由的電信往來資料儲存，在憲法上無疑慮，或許要以儲存是例外的情形為前提。其不可以導致與公民實際上其他所有行動，重建可能收回的現存檔案再相組合。所以，一般來說，一種這樣的儲存的證成，說服力的標準，在於儲存不直接經由國家的單位接手，其也不涉電信內容，且商業的服務業者基本上也禁止由客戶提出的網際網路方面的儲存。所以電信往來資料的儲存的引進，並不能當作是更多的預先的不具理由的資料蒐集的模範，而是要強迫立法者在新的儲存義務或有權儲存的考慮中，觀點不同的已有在公民資料蒐集做出較大的讓步。公民的自由感受決不允許全盤的被掌握被登錄，此乃屬於聯邦德國的憲法認同性(關於基本法上的認同性保留，參照: BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 - 2 BvE 2/08u.a. -,juris, Rn. 240)，聯邦德國在歐洲及國際的共同關係中，必須促進認同性的維護。經由一種預先的、不具理由的電信往來資料的儲存，將使未來更多的不具理由的資料蒐集的游動空間。

dd)總結而言，也經由歐盟的途徑大大的降低六個月電信往來資料的儲存在由立法者在電信法第113a第1項第1至8句所預見的範圍內，在當時的情況下，並非一開始即不合乎比例原則。然而，要其憲法上無疑慮性的前提，即是儲存及資料的使用的立法形成，恰當地要顧及一種這樣的儲存的特別(干預)力道。

V.電信法第113a條所規定的預防性往來資料儲存建構要合於憲法上特別的要求

如同其於電信法第113a條中所規定的一項預防性的電信往來資料儲存的建構，歸屬於憲法上特別的要求，特別是關於資料安全、資料使用範圍、透明度(Transparenz) 以及法律保障。僅在當涉及與此相關、充分、完全且規範清楚的規定時，基於這樣的儲存的干涉方合於狹義比例原則。

1.對電信往來資料以電信法113a條規定範圍的儲存，需要對資料安全特別高標準的法定保障。

考慮到藉這般儲存所達的資料存量(Datenbestände) 的範圍和潛在訴說力，資料安全對於系爭規定的合比例

性有重大意義。這件事特別成立，因為資料係被處於經濟條件與成本壓力下運作且對資料安全確保僅有有限興趣的私人服務供應商所儲存。私人服務供應商原則上是私用取向且不受特別的官方義務所拘束。同時違法調取資料的危險又大，因為關於資料多面的表現力，對最極端的行動者(Akteure)會是有吸引力的。 因要要求一項對電信資料保存以超過一般憲法上要求的標準之特別高的安全標準。這般對資料安全的要求不但就資料保存，而且就資料的傳送亦成立；這同樣要求對資料刪除的保障的有效確保。

於本程序言詞辯論中的陳述以及書面意見中，由專家鑑定人一方所展現出為提升資料安全的制度面廣泛的光譜。於此被列舉的，例如對於依據電信法第113a條所儲存的資料存於實體上分離且與網際網路離線的計算機(physisch getrennte und vom Internet entkoppelte Rechnern)上的分離儲存，將鎖鑰分開保管的非對稱密碼學的鎖碼(eine asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel)，為造訪資料去預先規定的二人視野相對原則(Vier-Augen-Prinzip)兼備以進步的程序為開啟鎖鑰的真實性確認 (Authentifizierung)，對造訪資料與資料刪除的安全變更的紀錄(die revisionssichere Protokollierung)以及自動化的錯誤校正程序與說明程序(automatisiertes Fehlerkorrektur- und Plausibilitätsverfahren) 的啟用等。被指出作為對這般技術取向的制度補充的還有創造對於資料侵害的資訊義務，一項無過失責任的導入或針對無體的損害的損害賠償請求權的強化，以求創造對有效資料保護的安置(Implementierung)的誘因。

憲法並未詳細規定，於個案中被要求何種安全標準。然而結果上一項標準必須被加以確保，其專門關注於透過一預防性電信往來資料儲存而創造的資料存量的特殊性，於安全上確保一特別高的標準。在這種情況下必須確保，這項標準（如回到單一立法的法律圖像上如科技的狀態（參照：Heibey, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 575, Rn. 19, S. 598, Rn. 145; Tinnefeld/Ehrmann/ Gerling, Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 628），指向專業討論的發展狀態且持續採納新的知識與觀點。與此相應的必須去規定，負儲存義務的企業（例如基於每隔一定時間需加以更新的安全構想）在這點上需能複查的調整其作法。由有疑問的資料存量由得出的危險潛力，並不允許成文的安全要求服務於藉一般經濟觀點的自由裁量下。當立法者無例外的規定對電信往來資料平面覆蓋

的儲存，則相關供應商不只就其儲存義務，而且就資料安全的合作要求得履行這件事，是屬於必要的要件。以專家證人的意見原則上很容易以當今討論的狀態為起點，即必須對於資料的分離儲存，對於一項高要求的鎖碼(Verschlüsselung)，對於一項運用例如二人視野相對原則(Vier-Augen-Prinzip) 以及安全變更的紀錄(revisionssichere Protokollierung)的安全(資料)造訪機制等去加以確保，以求對資料的安全於憲法上充分的去保障。

法律規定對一如此特別高的安全標準以合格的方式，依其理由，規範明確且拘束性的去加以規定是必要的。因此，立法者可自由決定，對現存標準作技術上的具體化一事，委由監督機關。然而。立法者需對此確保，就涉及的保護措施的方式與標準，不得於各別的電信供應商手中而不受控制。需被設定的要求不是透過不同的技術規章(可能依不同的規範領域劃分等級)，就是以一般普遍的方式被加以規定且其後以透明化的方式，透過有拘束力的裁決去加以具體化。進一步對於公共性，於包含獨立資料保護受託人的透明性管制下是憲法上所要求的(參照: BVerfGE 65,1<46>)，以及公平的對於侵害資料安全賦予適當的力度評價的處罰體系。

2.電信往來資料的儲存，如於電信法第113a條所規定的，進一步預設就使用這些資料的法律規定。就這些使用規則的合比例的形構本身，不只是就成立干預的規定的合憲性作決定，而且基於合憲性而駁回像這樣的儲存。依聯邦憲法法院的裁判，對資料使用的限制與使用範圍於相關法律基礎中的要件，在越被嚴格限制，則於儲存而造成的干預越應該被評價得更重。個別干預以及相應的干預門檻的理由，目的與範圍應透過立法者以領域專業，精細且規範明確地加以規範(參照: BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 166<191>; 115, 320 <365>; 118, 168 <186 f.>)

實際上對所有電信往來資料，透過不置理由、體系性的儲存所獲得的資料存量的使用，依此歸屬於特別高的要求。特別是於此資料存量於憲法上非以如同對電信往來資料運用同樣的範圍被允許。這些電信往來資料係服務商依電信法第96條規定，靠個別經營與契約狀態(部分是受客戶影響的)被准予儲存的。考慮到就六個月體系性預防性被調取的往來資料的非證明性，完整性以及藉此提升的表現力，這些資料的調取有不同大小的重力力度。因為，對這些資料的利用得深入私人生活的追溯，且在此情況下，詳細的個人與運動側寫，使得，不是能很快由此出發，原則上對這些資料的追溯原則上較(依據舊法的調取

，參照: BVerfGE 107,299 <322>)涉及內容的電信監察較低的重力力度評價成為可能。而且對這些資料的利用，僅於其致力於特別高層級的公共福祉利益上時，始得被視為合比例性的。

資料的利用因此僅得於法益保護相當重要的任務，方得被加以考慮。亦即，對相當重要法益有威脅的刑事犯罪行為的追緝，或是對這樣的法益的危險的防範。

a)在刑事追訴上，由此產生資料的調取至少預設重罪行為嫌疑的特定事實。那些刑法構成要件應被包含在內，應由立法者最終藉資料儲存義務去確定，對立法者而言，在此的判斷空間。立法者要不是追溯現有的目錄，就是設立自身的目錄，例如涉及電信往來資料對之有重大意義的刑事犯罪行為，去加以掌握。是否具有刑事犯罪行為嚴重性，必須在刑法規範(尤其是透過刑罰範圍)中找到一項客觀的表述(參照: BVerfGE 109, 279 <343 ff., insbesondere 347 f.>)。相反的，一項一般條款或僅是指引有重大意義的刑事犯罪行為是不足的。

除就相應的刑事犯罪行為目錄的抽象確定之外，立法者須確保，就預防性被儲存的電信往來資料的追溯，僅於當於個案中，被追訴的刑事犯罪行為具重大意義且資料的運用係和比例時，方得允許。

b)就危險防範而言，對有疑問的資料必須同樣方式有效的加以限制。資料使用應致力於犯罪行為的阻止，而對關於對關於特定刑事犯罪目錄啟動資料提取(參照: BVerfGE 121, 1 <26>; zu Straftaten von erheblicher Bedeutung vgl. BVerfGE 107, 299 <322>; zu besonders schweren Straftaten im Sinne von Art. 13 Abs. 3 GG vgl. BVerfGE 109, 279 <346>)，並不是合適的立法技術。是項技術係針對法益危害程度的要求而取得明確性，且於當刑事構成要件本身亦就預備行為和單純危及法益而加以處罰時，則導致不確定性。應取而代之的是法律上直接相關的法益，應就其保護去合理化資料使用，以及對此法益危害的強度等在此作為干預門檻而加以達成。一項如此的規則合於作為法益保護的危險防範的特性，且就直接聯繫於應合理化基本權干預的標準目的加以保障。

介於就資料儲存與資料使用的干預的力度與一項有效的危險防範重要性的力度二者間的衡量導致，對預防性被儲存的電信往來資料的調取僅於為防範個人身體、生命或自由為聯邦或各邦的生存或安全的危害或是共同的危險的防範等情形下方得被准許（參照：BVerfGE 122, 120 <141 ff.>)。關於這一點法定的授權基礎必須主張對於需保護的法益的具體危險至少有一實際上的支撐點。這個必要性導致

，推測或一般經驗法則並不足以正當化對資料的調取。毋寧是支持對具體危險的預測的特定事實必須得加以確定。於以下的範圍需要藉此於個案中成立充分的可能性成立，於可預見的期間，不具國家干預，對於規範的保護利益透過特定之人所造成的事實基礎，合議庭就這方面的說明在此準用於對線上搜索的要求（參照：BVerfGE 120, 274 <328 f.>）。具體的危險係透過以下3個標準被加以確定：個案，危險於損害中突然的變化的時間上的接近以及涉及作為肇事者的個人。然而對預防性被儲存的資料的調取，於當即使特定事實於個案中指出對於相當重要的法益的危險，仍未能藉充分的可能性確定，危險即將到來時，則是正當的。這些事實必須一方面依據至少就其種類具體的與時間上可見的事件允許推得出結論，另一方面基於特定的人參與其中，就這些人的辨識於措施施加且得全神貫注其上時會更清楚。與此相反，對基本權干預的力度於當實際上的干預原因對於規範的保護利益而言，於個案中仍未得見之具體危險的前階段中仍極度欠缺時，並未被作出充分的考量。

c)憲法上針對危險防範的資料使用上的要求，係就所有對藉由預防性目的的干預授權而適用，這些目的亦適用於就透過情報任務單位的資料使用。因為透過對所有在這些案件中的關係人所干預的影響是一樣的，就這些要求並不存在與機關有關的，如警察機關與其他從事預防性任務的機關(如憲法保護機關)間的差異。警察機關與憲法保護機關有不同的任務與權限，且於結果上作出不同的干預深度這件事，對於干預覆蓋性全面且長期被儲存的電信往來資料的使用的力度比重而言，基本上是不重要的 (參照: BVerfGE 120, 274 <329 f.>)。雖然，在憲法前不同有預防性任務機關的授權，是有差異性的(參照: BVerfGE 100, 313 <383>; 120, 274 <330>)。然而，立法者將個別從事預備階段辨識的安全機關的權限的規定，令之受由比例原則導出的憲法規定的拘束上(參照: BVerfGE 120, 274 <330 f.>)。如今此等作法導致，不只考慮到受保護的法益，而且考慮到要顧及的干預門檻，均應對資料使用設定更高的要求。

何以上述這項要求不應用於情報部門的任務履行上，是沒有理由的。雖然，情報部門的任務限於為蒐集資訊報告政府。這件事對於個別公民而言，除被監視的風險外，並無與此相繫的風險時，降低了其干預的力度，同時在此亦減低對這樣的干預的合法性的力度比重，因為僅透過單純政府的資訊無法對法益侵害加以阻止。這件事(阻止法益侵害)只有透過負責危險防範的機關，其資料使用的憲法上

的限制，不應在準備階段透過其他的使用權限而產生，的結果取向的措施方有可能。此外，一項這樣的干預對於公民的特別的負擔效果，基於，不只這樣各別的對電信祕密的干預，原則上是秘密進行，而且實際上情報任務的全部活動也是秘密達成的。該任務就預防性覆蓋或被儲存電信往來資料使用的權限，此不能受控制被監督的感覺以特別的方式去升高且將持續的寒蟬效應延伸至自由體驗中。

本合議庭承認，由情報單位那邊對預防性儲存的電信往來資料的使用，在很多案例中是不應予以考慮的。然而上面這件事是以其任務做為準備階段辨識(Vorfelsanfklarung)的方式，而且不具憲法上容忍的，由比例原則得出，去減少以現在出現的方式的干預的要件的理由(參照: BVerfGE 120, 274 <331>)。

d)將資料使用限制於特定目的，必須亦確保與程序上附加資料運用依其調取與傳輸予聲請機關。於此法律上必須去確保，該資料於傳輸後立即得被加以使用，且如該資料就調取目的而言並不重要時，應立即被加以刪除(參照: BVerfGE 100, 313 <387 f.>)。此外，下面這件是必須去預見，該資料於對於固定目的不再是必要時被刪除，且對此要寫入紀錄(參照: BVerfGE 100, 313 <362>; 113, 29 <58>)。

電信往來資料並不透過國家機關取得其內容而喪失其源自基本法第10條的保障。基本權的要求明晰的目的拘束，因此涉及到將資料與資訊轉傳予其他單位。這件事並不排除目的變更。然而，目的變更需要自身的法律基礎，其餘它這邊合於憲法上的要求(參照: BVerfGE 100, 313 <360>; 109, 279 <375 f.>)。將被傳遞的電信往來資料，進一步轉傳於其他單位只能於法律上對此規定，於使任務的落實的達成，且為此落實對這些資料的提取或許是直接允許的情況下方得達成(參照: BVerfGE 100, 313 <389 f.>; 109, 279 <375 f.>; 110, 33 <73>)。上面這些必須由受傳的單位去紀錄(參照: BVerfGE 100, 313 <395 f.>)。在此是項目的拘束僅在於依掌握而認清，在此涉及預先不置原因被儲存的資料。立法者依此就這些資料需就標示義務加以規定(參照: BVerfGE 100, 313 <360 f.>)。

e)憲法上的界限完全得鑑於被調取的資料範圍而得出。故由比例原則觀點，於不同的查詢行為間可形成各種層級步驟。例如其是否僅涉及個別的電信連線，於傳輸時可僅由一訊號單元於特定時間中提取且僅基於個人間的溝通(可能限於特定時間內或特定的溝通形式)與接斷線定位資料或者換句話講，是否該步驟由一人資料的完整傳輸而藉此盡可能建立詳細的

運動或個人側寫。同樣關注於干預力度而區分，是否於資料傳輸時從中過濾，藉此為保護特殊的信賴關係而將特定的電信連線加以挑出。

考慮到原則上已依現有標準，為了預先被儲存的電信往來資料的使用有適用的高門檻，立法者在就資料使用範圍的進一步仍有形成空間。特別對立法者而言是自由的，這樣的比例原則考量，在個案中留予就決定資料調取命令審查的職權法官。

然而，作為比例原則審查結果的憲法上的要求是，至少對於基於特別指向秘密性的緊密團體的電信連線，去預見基本的傳輸禁止。在此應被設想的大概是人、機關和組織等在社會或教會領域中連繫的連結，這些連結原則上維持匿名的通話，完全獲大部分是電話上的諮詢，且是提供以心靈或社會上急迫性，且本身或其他同事對此要遵從保密義務。

3.進一步，一項預防性、不具理由的電信往來資料儲存暨(資料)的使用，僅於當立法者就資料使用的透明性，以及對有效法律保護與有效制裁的確保，創設了完整的預防措施時，方是合比例的。

a)對透明性的要求，屬於對於透過一項就獲取的資料如此地儲存的於憲法上無疑問的使用的要件。資料的使用大體上必須儘可能公開達成，否則其原則上至少需要對相關人的事後告知。如果上述情形於例外情況下不發生，即就未告知需要法官裁定。

aa)此外，一項對所有電信往來資料關於六個目的預防性，不具理由的儲存因此是相當重大的干預，因為是項儲存引致持續被監視的感覺;是項儲存允許以不可預見的方式，在未顧及資料對於公民是直接可感受且明顯的，深入的觀察私人生活。個人並不知，關於他有哪些國家機關知道什麼，但是知道，機關關於他能得知許多且極度個人化的東西。

立法者必須就依此得包含資料儲存的廣泛性的威脅，透過有效的透明性規則去防堵。針對關係人就資料調取或利用的資訊的規定一般屬於基本權資料保護的基礎制度(參照: BVerfGE 100, 313 <361>; 109, 279 <363 f.>; 118, 168 <207 f.>; 120, 351 <361 f.>) 。對於預先不置的電信往來資料儲存的廣泛和各種有表現力的資料存量的使用因此需設置高的要求。是項要求一方面有如下的任務，就由對資料的實際上重要性的不知得出的威脅性去加以削弱，去對抗不確定的推測且對關係人創造就這些措施去公開討論的可能性。另一方面，這樣的要求亦因基本法第10條第1項的有效法律救濟的要求連結基本法第19條第4項而被加以導出。在不知情的情況下，嫌疑人既無法就機關的不合比例的資料調取，亦無法就某些權利如

刪除、報告或補償等加以主張(參照: BVerfGE 100, 313 <361>; 109, 279 <363>; 118, 168 <207 f.>; 120, 351 <361>)。

bb)對涉及個人的資料的調取和利用的公開性原則，亦屬於透明性的要求。

於嫌疑人不知情下對資料的使用僅於當調取資料所致力的偵查的目的於別種方法無法實現時，方是憲法所允許的。立法者對此種作法原則上就危險防範與情報任務的履行是可接受。反之，於刑事訴追的範圍內，對資料的公開調取與利用亦在考慮之內。（參照：§ 33 Abs. 3 und 4 StPO）於偵查措施在其他情況下，部分係於嫌疑犯知情且以其當下被執行（參照：zum Beispiel §§ 102, 103, 106 StPO）。反之，關係人面臨其資料被詢問或傳輸時原則上應被告知。對資料的秘密使用僅有當其於個案中係必要的且法官下令時方得被預先規定。

只要對資料的秘密使用達成，立法者有義務就最少事後報告義務加以規定。上面這件事需保障，直接涉及到資料詢問（無論是作為嫌疑人，警察義務人或第三人），至少於原則上事後告知。立法者得於衡量憲法上保護的第三人法益規定例外。然而其應限於絕對必要性上（參照：BVerfGE 109, 279 <364>）。告知義務（的例外）關聯到刑事訴追例如當認識到干預電信秘密導致錯失刑事訴追的目的，當告知（義務）於未對一個人的身體與生命的危害而發生或是當刑事訴追的重大利益，如因為透過未能取得進一步成果的措施的告知而似乎加深基本權干預（參照：BVerfGE 100, 313 <361>; 109, 279 <364 ff.>）而與一個關係人對立等等例外是可設想的。如果有強制性，排除事後告知的理由，則此事需被法官加以確認且隔一定時間加以審查（參照：BVerfGE 109, 279 <367 f.>）。以相應的方式，考慮到危險防範或情報部門任務的目的的資料使用，亦需要告知義務的形構。

反之，對於其電信往來資料僅偶然被共同掌握且這件事並未處於機關行為的焦點下的人，可比較的嚴格的告知義務是憲法上不要求的像這樣的參與，得於電信往來資料的運用上於大範圍內於毋需對其資料的短期認識而留下蹤跡，或必須對關係人有結果，而給出。反而，一項報告得於個案中對於關係人加深干預（參照：BVerfGE 109, 279 <365>; BVerfGK 9, 62 <81>）。於這些案例中，一項告發得於當關係人僅受措施不明顯的干擾且認為其對報告無興趣時，則原則上不會發生。對於此衡量決定並不需要法院的證明。

b)對電信往來資料的預防性儲存暨該資料的使用二者的合比例上形構

進一步要求對一項有效的法律保護暨合適的制裁二者的保障。

aa)就有效法律保護的保障而言，對這些資料的詢問與傳輸原則上必須被置於法官保留之下。

依照聯邦憲法法院的裁判，就導致重大基本權干預的偵查措施，於憲法上得被要求一項透過獨立審級的預防性控制。上面這件事特別是當基本權干預係秘密成就且對於相對人而言無法直接感知的（參照：BVerfGE 120, 274 <331>）。對於電信往來資料的詢問與傳輸會是這種情形。鑑於在此的干預的力度，立法者的遊戲空間限縮於以下的範圍，即這樣的措施原則上需置於法官命令保留之下。法官得基於其人與事上的獨立性且其完全受法律拘束的情況下，於個案中作最好與最安全的維護關係人的權利（參照：BVerfGE 77, 1 <51>; 103, 142 <151>; 120, 274 <332>)。依照基本法第10條第2項第2句，就情報任務干預電信自由的管制係一項例外。於此得透過人民代表構成的機關或輔助機關的控制（同樣的特別關聯到各別措施）以取代預防性法官控制的地位（參照：BVerfGE 30, 1 <21>）。

立法者將就預防性法官控制的要求以特別和規範明確的形式與對法院命令內容與說理上的嚴格要求二者聯繫在一起（參照：BVerfGE 109, 279 <358 f.>）。於此同時導出就被請求對法院而言，直到行使有效的控制（參照：BVerfGE 103, 142 <160 f.>)。係被允許的資料的詢問的充分實質的說理與界定的必要性，直到在此基礎上，下令的法院得且必須就是否被申請的資料使用合於法定要件，自我負責地作出判決。對干預要件，特別是包含法律的干預門檻的仔細審查亦屬於此。法院的命令裁定必須內容豐富的被說理。此外，應被傳輸的資料，依比例原則的標準應充分的選取且以明確的方式被標示出來（參照：BVerfGE 103, 142 <151>)，以便服務供應商毋需自行作實質審查。上面這件事應僅基於明確的資料傳輸命令被課予義務與授權。

同樣的，資料基於命令而由對電信企業負義務之第三方過濾出來且加以傳輸，亦即未讓機關直接提取資料，這樣亦是屬於對控制的有效性。以這種方式，資料的使用係移轉到不同行動者的共同作用且藉此被包含於相互管制的決定結構中。

bb)為對資料使用的持續管制的法律保護（救濟）程序的開啟亦是因憲法之故而被要求。只要相對人面對措施的貫徹並無機會，本人於法庭上對於對他的電信往來資料的使用去加以防護，則應對相對人持續的開啟法院控制。

cc)最後，一項合理的建置，應是對於權利侵害規定有效的制裁。倘

若對電信秘密的嚴重侵害卻沒有制裁的結果，形同使人格權保護非基於實體因素而受到侵害，然而人格權的保護，在基本法第10條第1項中卻有特別保護的建構(Ausprägung)，（Vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 11. November 2009 - 1 BvR 2853/08 -, juris, Rn. 21; BGHZ 128, 1 <15>)，此與國家應保護人格權的義務相左，亦與儘可能促使個人發展其人格之意旨背道而馳(參照：BVerfGE 35, 202 <220 f.>; 63, 131 <142 f.>; 96, 56 <64>），且違背國家保護個人人格權免於受到第三人危害之義務。(參照：BVerfGE 73, 118 <210>; 97, 125 <146>; 99, 185 <194 f.>; BVerfGK 6, 144<146>）。對電信秘密的嚴重侵害，於當下不法被取得的資料進一步不受阻擾准予被使用或是不造成實質損害的不法資料使用，也沒有對相對人平復的補償時，特別會是這樣的情況。

然而，立法者關於這一點有一項廣的形成空間。此外，立法者得特別觀察，相應的規則於刑事訴訟法或成文責任法的一般體系中得適應到何種程度。立法者就這點而言亦得考量，於人格權的嚴重分割上依成文的法律規定已不僅於衡量（參照：BVerfGE 34, 238<248 ff.>; 80, 367 <375 f.>; 113, 29 <61>; BVerfGK 9, 174 <196>; BGHSt 34, 397<401>; 52, 110 <116>）基礎的禁止利用，而且非實體損害的責任得被建立（參照：BVerfGE 34, 269 <282, 285 f.>; BVerfGK 6, 144 <146 f.>; BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 11. November 2009 - 1 BvR 2853/08 -, juris, Rn. 21; BGHZ 128, 1 <12>）。對於就這一點有關的，是否需要其他規則的判斷，因此並不會阻礙立法者，首先去觀察，是否常存於對在此有疑問的資料的無權獲取或使用中的人格權侵害的特別嚴重性，已基於文法由裁判以憲法要求的方式被加以考量。

4.對於服務供應商，利用現存的資料下所應提供的特定網際網路協定位址的連線所有人，以機關對服務供應商的訊息請求權的形式而預防性被儲存的資料，只對這些資料的間接使用而言，憲法上的標準較不嚴格。無賴於有限的法益或刑法目錄而創設這般的訊息請求權，整體而言比起對電信往來資料的探詢和使用，本身是進一步允許的。

a)預防性被儲存的電信往來資料於針對所有人可確定的網際網路協定位址，針對這些位址的調查，必須被加以動用，由憲法的原因，不需被給出於其他情況下就這些資料的使用成立的嚴格要件。

在此一方面，機關本身對於預先應儲存的資料並未有認知這件事，是

有意義的。機關於這般訊息請求權範圍內調取的並非預先不置理由被儲存的資料本身，而是僅取得針對由服務供應商對資料追索而得的特定連線所有人的涉及個人的信息。在這情況下這些資料的表現力是極度受限的：對預先被儲存資料的使用僅得到關於於網際網路中以已知，另一方面多少已被告知的網際網路協定位址註冊的連線所有人的訊息。一項這般的訊息依其形式結構仍有與查詢電話所有人某程度的類似性。是項訊息的認識價值是逐條逐項的。向長時間或個人側寫與運動側寫的建立的體系性的探問，僅基於這般訊息的基礎係沒法被實現的。

另一方面具決定性的即是，就這種消息僅是資料中從一開始即保有的一小部分被使用而已，單單這種消息的儲存可以是在明顯的較低的前提來被立法規定。單純的這種必要的網際網路連線(Internetzugang)的資料的消息，而用來對浮動的網際網路協定位址之確認的儲存，與所有的電信連線資料幾乎完整的儲存存比較起來，其有著一個明顯較無負擔的力道。由這此觀點上共伴效應導出如下的結論，為了往後的使用而預先被儲存的電信往來資料在其他方面所要求的嚴格的立法規定，對這種消息並不需同等嚴格的適用。

b)然而官方對網際網路協定位址的確認的消息請求提出的理由也有重要的力道。立法者基於此點，而對網際網路電信條件加以干預且限制其匿名性的範圍，在上述所說的基礎上，再與網際網路連線資料較廣泛的系統性的儲存的連結(接)就可以確定網際網路使用者的身分。只要私人，其自認在網際網路受有損害，而將相應地網際網路協定位址登錄並自首，或同樣只要機關自己偵查網際網路協定位址，則這些確定的上網用戶即可被有序般地列出，且在其後存在的通訊過程皆以極顯著的或然率可以被個別化的身分確認。

網際網路協定位址，對上網連接用戶的歸屬確認，對由被涉及者的觀點而來也有重要性，雖然其與電話號碼的確認有某種相似性，但卻仍不相同的。電話號碼做為持續的被給予的標示而使用者來相互交換，以致對用戶的詢問的可能性也不用涉及詢問到具體的電信溝通行為。與此相反地，對動態網際網路協定，位址連結同仁的消息的詢問自身，即同時必然地含有事情(由)及網際網路協定位址與誰連接及在特定的時間被使用的資訊。此外，更有甚者，電話號碼後無疑問能立刻被印出，但就私人的網際網路協定位址，當時的使用下的情況，基本上能在僅是匿名性的服務的隱藏性中就可以進行。同樣地，就網際網路協定用戶可能的個人身分的關聯性的

詢問也是不同於電話號碼用戶的詢問:已經由接觸範圍來說，網際網路方面的即時的呼收使用所提供的資訊皆比電話號碼的查尋有透漏更多的訊息。一個網際網路上接觸的接收訊息也有與電話不同的內容重要性:因為網際網路的內容並不同於電話談話中的內容。是電子上被固定下來且長時間還可以再被呼叫的，同樣的情況，促使網路通訊可以更多方且可信的方式被重建，由此，何種課題是彼此相互溝通的被設入於網路是較易重建者。網際網路協定位址的個人化之確認做為"網際網路電信號碼"同時給出溝通內容的消息。在電話通話適用的外在通聯資料及通話內容的區別，在網際網路上即被解消了，而無區別了。

假如一個特定的網際網路方面的造訪者經由對網際網路協定位址的個人身份的被確認，則我們即不僅知道，他與誰有接觸，也可在一般情況下知道接觸的內容。

當然，反過來也存在一個對下列可能的高度興趣，即網際網路上電信連線對法益保護或法秩序的維護可歸給各行其事的行動者。基於網際網路對日常生活中最大不同領域及過程中日益增長的重要性，同時各式各樣的犯罪行為及侵權透過網路利用的危險也同時提升。在一個法治國家中，網際網路也不允許形成法的自由空間。因此，網際網路互動而生的有此力道的侵權而歸責於個人的可能性，構成了立法者合法的規範任務。電信往來資料必須被使用到的這種情況，也結果上不會產生新的原則性的疑慮，倘若就從服務業者方面在現行的科技條件下，即準此，網際網路協定位址大部分僅為了及時的位置(「浮動的」)而被給予，而為了相應的消息來篩選往來資料的情況而言之。同樣地，立法者能針對可信賴的網址的歸屬的確保而規定服務業者，在特定的期間就相關的資料的保存，有時或就被保存資料再進一步的被回取的課以義務，立法者在此有立法的形成空間。

c)與此相符的，立法者可以也在與對犯罪行為或危險防範及情報部門的任務的履行無關的限制的法益目錄，或犯罪行為目錄外，在一般專法上干預授權的基礎允許這種消息之確認。(參照Bock in: Geppert/Piepenbrock/Schutz/Schuster, Beckscher Kommentar zum TKG, 3. Aufl., 2006, §113 Rn. 7; Granlich, in: Arudt/Fetzer/Scherer, TKG, 2008, §113 Rn. 8)。然而，基於干預的門檻要確保即是消息不可毫無目的的獲得，而是僅以充分的案情開端的懷疑的理由，或一個在個案關聯的事實基礎上具體危險才可以有結果。同樣地，一種在事實上有憑有據的具體危險的要求或對情報部門的任務及負責所有危險防範確保公共安全及公共秩序的主管機關，消息獲得才可

適用。相關的消息請求的法律上及事實上的基礎，必須以公文般的按件被製作。與資料儲存相反的，為這種消息而請求法官保留並不需被預見。

同時，應不允許一般的且毫無限制也在每個秩序罰的訴追或阻止使用這些訊息。對網際網路匿名性的廢止，至少需要造成一個法益的侵害，而此法益是法秩序也是特別地衡諸一重大的力道而加以保護的。這種情況並不完全排除秩序罰的訴追或防止相互配合消息，但其必須是，也在個案上，與有特別重大的秩序罰有關才可以，且必須由立法者明示般的列舉出來。

同樣的針對網際網路協定位址的確認上去放棄透明性原則(詳見上面CV 3)也是沒有理由的。在一般情況，由匿名的使用網際網路的想法出發，而被涉及者，原則上有權知道，事件及何種理由這種匿名性被取消，與此相配合地立法者無論如何要預見告知義務，倘若經此告知，消息目的並不會立即被妨害或此外第三者極大的利益或被涉及者自身不會成為阻擋的絆腳石。依相關的法律上規定的標準可例外的處理外，一旦有一個告知，則對告知要被確認的理由即需公文般的按件被製作。至於，不需告知要得到法官的證實，則在此並不需要，此乃與資料儲存即使用相反的。

5.憲法上要求的資料安全的確保，以及符合比例原則，要求的資料使用目的規範明確的限制是儲存義務的立法規定中不可分的基本部分，且因此將此義務的承擔歸屬於聯邦立法者。與此相反，就有關制定查詢規定本身的責任，暨透明度規應與法律保障規定的立法形成則各依所屬的事務權限劃分。

a)只要是與服務業者對電信往來資料預先的不具理由的儲存的義務，相關的資訊安全應規定的問題，則其聯邦依照基本法第73條第1項第7款當作儲存義務及與此法律上相連結的效果的直接的基本部分來立法施行。除了被儲存資料的安全規定外，此立法也包括資料傳輸的安全規定及此處信賴關係保護的確保(見上面: ＣＶ1及CV２e)。

更有甚者，一種合乎憲法上要求的充分精準的資料使用目的的確保，其乃是伴隨儲存而來的亦歸屬於聯邦來立法。此事的理由在於，資料儲存及使用目的在不可揚棄般的憲法上的相關聯，其一直是合乎如聯邦憲法法院所確立的裁判:資料從一開始僅能為了確定的、特別領域的、精確的且規範明確般設定的目的而被儲存，以致在儲存時以充分的被確保，資料僅僅是用於這些可以證立資料儲存重力(力道)的目的。一個儲存不能僅是當作此種儲存而抽象的被證立，而是僅是當它是為了充分的有力的具體稱呼

的目的而存在，始足當之(參照: BVerfGE 65, 1 <46>; 118, 168 <187 f.>) 。與此相反，獨立於這種目的規定，而建造儲備資料泳池也是不被允許的。其利用留待各依事後不同國家層級的需要，及政治裁量來行使。在這種情形裡可能儲存的合憲性，在儲存時會存在的干預的時間點尚無法被斷定，欠缺充分的可預見性及有限制性的目的。且其射程對公民既非可預見性，亦非依比例原則的標準可被限制。此種資料儲存及使用目的實質的結合當作在干預及證立合法的標準，連帶亦不允許在聯邦與邦的共同一致的配合中被打破。這種聯結的確保的權限歸屬於聯邦，乃基於基本法第73條第1項第7款源自於事物的彼此相關聯(見上面: C Ⅲ 2)。

屬於聯邦聯結儲存自身，被觸及的規定包括對資料使用嚴格前提的設定，為了刑事訴追的目的，危險防範或經由情報部門任務的危險預防，按照上述所發展的標準來立法。對資料更廣的使用，尤其是以標示義務或紀錄義務形式所生必要的目的拘束的遵守的規定，亦屬於聯邦立法規定範圍。

b)與此相反，儲存義務的立法規定並不直接促使聯邦，就資料在聯邦所設定的目的框架內，事實上是否與多久允許被回蒐調取一事負責任。資料查訊本身規定的施行，其規定資料查訊本身基本上不再是聯邦事務，而是依照一般的立法權限。準此，授權資料查詢，不能立足於基本法第73條第1項第7款，而是在各依所屬的權限規範的基礎上來立法，這此權限立法各為與其資料使用所追求的任務而規定之(參照: BVerfGE 113, 348 <368>; 114, 371 <385>)。在危險防範即情報部門的任務的履行的領域內，其對此立法的權限大部分是屬於邦的權限與憲法上命令式的使用目的限制的確保，其因為資料保護法上干預與證立合法相牽扯，而必須一體的與儲存同時加以規定不同;除在查詢授權外，對資料使用的立法形成的持續的憲法要求的維護，如特別地對被涉及者事後告知的規定，及有效的法律保障的確保皆留待邦後續的立法行為來完成。因此，這此規定的合憲性的責任則直接歸屬各邦自己。

VI. 系爭規定於依據電信法第113a條提取往來資料的範圍內牴觸基本法第10條第1項的規定

系爭規定並不符合上開要求。雖然電信法第113a條因比並未牴觸基本法第10條第1項的保護電信秘密的基本權利，因為儲存義務的範圍依照電信法第113a條第1項第1至7、11號自始彷彿是不合比例的。然而資料安全，資料使用目的和透明性，以及法律保護的規定並不合於憲法的要求。對

此整體而言缺少對規定的合於比例原則的形構。電信法第113a條與第113b條及刑事訴訟法第100g條，於允許提取依據電信法第113a條所儲存的資料的範圍內，因此牴觸基本法第10條第1項。

1.電信法第113a條並非因其範圍即屬違憲。立法者得就刑事訴追和危險預防的有效化由其規定的，依本條第1項第1至7號所及差不多所有往來資料擴延至向公眾開放的電信服務業者的儲存義務，仍屬妥適，必要及合乎狹義比例的(參照上述: C IV)。儘管因(儲存義務)的範圍，本規定自已經被掌握的資料的範圍起仍是充分受限的。電話交談，電報與電子郵件的內容如電信法第113a條第8項所明示，不得多於在網際網路中與使用人接觸的網頁或服務供應商而被加以儲存。同樣立法者依電信法第113a 條第1項和第11項藉由六個月和與此相關的一個月刪除期限確定了一憲法上仍容許的儲存期間長度。同樣就現今時點並未確定該規定與其他條款共同作用下造成或導致為對公民的每一活動儘可能的重建而創設一普遍完整的資料庫。資料保護法另外進一步貫徹的原則對於，立法者原則上藉以尋求阻止資料庫產生的資料省減以及大量的刪除義務的效力，在此是有意義的。對此評判決定性的是特別如電信法第11條以下課予服務供應商依照電信媒體法原則上就非於計算上必要的資料刪除的義務(參照: 電信媒體法第13條第4項第2號) 且反於私有經濟上的原因而去阻止，網際網路使用於內容上在一般商業資料庫中被確定且藉此是維持在可被重建的狀態。電信法第113a條無法被掌握為一為刑事訴追和危險預防的目的的普遍公共資料照顧的表達，而是儘管其(範圍)廣泛的，試著考慮對現代電訊就刑事訴追和危險防範的特別挑戰的受限的例外。

2.此外，對於像這般的資料庫所要求的憲法上的保障上而言，缺少特別高的安全標準。電信法第113a條第10項在此僅規定尚不確定的義務，透過技術與組織上的措施去確保，得已經儲存資料加以調取對有得到授權的人是完全可能的。而且在其他方面僅依照在電信領域內一般必要的注意。於此缺少一項依據電信法113a條就廣泛與明確的資料庫的安全考量考慮特別高要求的條文。實質上與此相關電信法第88與109條並未保障這般特別高的安全標準，而是對安全標準允許合於較寬適用範圍的多種相對化。上面這件事尤其是成立在電信法第109條中。故依據電信法第109條第1項，有針對每一服務供應商，為保護遠距通信秘密和電信與資料加工系統，免於不法的(資料)提取的適當的技術防護措施或其他措施去加以規範。對於適當性的規定則規定於電信法第109

條第2項第4句中(參照: Klesczewski, in: Säcker, Berliner Kom-mentar zum TKG, 2. Aufl. 2009, § 109 Rn. 12)。其後於當對此必要的技術與經濟上費用(Aufwand) 與保護權利的意義間以適當的方式呈現。因此由於前揭所發展出的標準出發，針對依據電信法第113a條所儲存資料的保護的特殊要求其實保障並不充分。對於「恰當的技術防護措施或其他措施(angemessene technische Vorkehrungen oder sonstige Maßnahmen)」的法律規定的標準僅要求就技術發展的地步去加以「關注(berücksichtigen)」 (參照: 電信法第109條第2項第2句; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 109 Rn. 13)，且於個案中就一般經濟權衡(Wirtschaftlichkeitserwägungen) 維持不確定的方式對安全要求加以相對化。此外對於是項標準更仔細的具體化則讓與個別的，必須於其方面在競爭和價格壓力的條件下，去提供服務的電信服務供應商。

這些要求的具體化亦無法以法律命令型式或透過監督機構的執行而加以確保。特別是電信法第110條並不保障具足夠安全標準的效力。雖然在依此規範需創造的低度立法的立法結果(參照電信法第110條第2與第3項)的範圍內，有共同就資料安全的見解加以考慮。然而此項 (主要係透過技術上的目標設定而被決定的) 規範既不包含內容上的標準，亦不涉及其他資料安全的見解。此外，於電信法第113a條的儲存義務生效二年後，一項新法對電信監察秩序(Telekommunikationsüberwachungsverordnung) 的調整並不成功。同樣的就轉換電信監察措施與往來資料的查詢申請的法律手段的技術性指令(Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten (TR-TKÜV) (於2009年12月依據電信法第110條第3項第3句的規定於聯邦網絡局的網頁上出版(參照: Bundesnetzagentur, Amtsblatt 2009, S. 4706)，依照電信法第110條第3 項規定於此項調整後一年始生效力 (Inhaltsangabe 1 <Regelungsbereich> TRTKÜV; Teil B 1 <Grundsätzliches> TR-TKÜV)。

電信法第109條第3項亦不保障全面的資料安全。雖然該規範規定，電信設施的經營者為安全受託人且需向聯邦網絡局提交安全構想。此構想於當以之為基礎的「存有(Gegebenheiten)」有變更，適應以及更新時亦同。然而一項特別高的安全標準並非可信賴的被保障。因此本條只針對設施營運人，而非所有的電信法第113a條的亦涉及其他服務商的規範相對人。此外，電信法第109條第3項實質上

僅指引電信法第109條第1與第2項的不充分的要求。同樣的，安全標準持續的和可控制的適應於科技發展的狀態並未以充分規範明確的形式被加以確保。是否電信法第109條第3項第4句要求就保護設施的科技發展的適應上且自身法律上持續發展的安全標準，並不甚清楚。無論如何就對安全構想分期發展的義務上缺少使得有效控制成為可能的義務。

在電信法中缺少充分的安全標準，亦無法藉由聯邦資料保護法第9條連結有關附件而加以彌補。本規範於無損於其部分抽象的高標準的情況下，本就是補充性的被適用(參照: Fetzer, in: Arndt/Fetzer/Scherer, TKG, 2008, vor § 91 Rn. 10; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 91 Rn. 15)，以使一般性的以完全專門和可靠的方式，去考慮到依據電信法第113a應加以儲存的資料對特別高的安全標準加以確保。

整體而言，對於應依據電信法第113a條被儲存的資料而言，不但一項特別高的安全標準無法以有拘束力與規範明確的方式被加以保障。被專業咨詢人員與本程序中認定為所提及機制的核心要素的儲存(分離儲存，非對稱密碼學的鎖碼 (asymmetrische Verschlüsselung)，為開啟鎖鑰的真實性確認之二人視野相對原則兼備以進步的程序，對造訪資料與資料刪除的安全變更的紀錄)無法被貫徹式的加以規定，亦無法強加他們去保障一項具可比較的安全程度安全設施。在此亦缺少平復的處罰體系。就侵害資料安全並不比侵害儲存義務有較輕的比重。對於不注意儲存義務的罰金範圍是明顯的較侵害資訊安全的罰金範圍為廣(參照： 電信法第149條第2項第1句聯結電信法第149條第1項第36與第38號)。對憲法上資料蒐集安全的要求，如同透過電信法第113a條所創設的是項安全，不符合有效的法律狀態。

3.依據電信法第1136條第1句前半規定的對資料的傳輸與利用的規定，並不符合憲法的要求。

a)首先，為刑事訴追的資料使用規定，並不合於由比例原則所發展出的標準。

aa)電信法第113b條第1句第1號聯結到刑事訴訟法第100g條，並不合於特別嚴的要件，依此要件得用到僅依據電信法第113a條被儲存的資料。雖然立法者藉此條文規定了一項於共同作用中分化的，而且依照基本法第74條第1項第1號與第72號第1項作成的為刑事訴追的資料使用的目的決定。立法者仍然就資料的使用，滿足了類似的要求，如同這些迄今為電信資料提取適用的要求，這些電信往來資料得被服務供應商得依其營業和契約上需要的標準以有限的範圍內，且對

個人透過契約內容依據電信法第96條，部分可免除的，就這些資料加以儲存。上揭對於特別重的，基於電信法第113a條的預防性，不置理由與體系性資料儲存的干預並未作充分的考量。

刑事訴訟法第100g條第1項第1句第1號並未確保，普遍而且於個案中僅針對嚴重的刑事犯罪行為，得為調取相應資料的理由，反面是（獨立於全部的列舉規定）具重大意義的一般的刑事犯罪行為便足夠。何況，刑事訴訟法第100g條第1項第1句第2號，第2句是落在憲法的標準之後，以便此犯罪行為不依賴於其重度，而對任一藉電信而著手的刑事犯罪行為，依據在比例原則審查範圍內的一般衡量的標準而作為資料調取可能的導火線。藉此規定，依據電信法第113a條被儲存的資料實際上於所有的刑事構成要件是可使用的。（資料）的使用，藉此考慮到電信於日常生活中變動的意義，而失去其例外特性。立法者在此不再限於為了訴追嚴重犯罪行為，而是遠遠超出（且在此亦超出歐洲法上規定的資料儲存的目標設定，其亦於其方面僅限於，在不顧及危險預防的情況下，嚴重犯罪行為的訴追）。雖然這些資料的使用在直接就藉助電信而著手的犯罪行為的訴追上是極有用的，以致於對其限制會使（犯罪行為）的辨識於若干案例中變得困難或受阻礙。於此基於基本法第10條第1項保障及與此相繫的比例原則的要求的本質，即並非每一就刑事訴追極有用的且於個案中亦是必要的措施，是合憲的。反之，在於此決定性的要求的後果中，同樣於較不重要的刑事犯罪領域內，電信並不全然是成為法外空間：依據電信法第113條第1項之查詢，立法者得（同樣對依電信法第113a條被儲存的資料的間接利用）為了所有刑事犯罪的辨識而就此查詢加以規定（見前揭: ＣＶ４ｃ）。因此，同樣的依據刑事訴訟法第100g條在其他方面（資料）溯及，是比依電信法第113a條被儲存的電信往來資料來得可能。

bb)刑事訴訟法第100g條進一步於其就資料提取於嫌疑人不知情的情況下，亦得允許這件事，係不合憲法上的要求(刑事訴訟法第100g條第1項第1句)。憲法上對資料使用的透明性的要求，對祕密調取依據電信法第113a條僅於當是項調取依據壓倒性的法律上近乎具體的理由是必要且法官命令的，方得允許。

cc)告知義務的形成，在每一方面均不合於上面被發展出的標準。不過就被規定的這樣的告知義務的範圍而言，並未有憲法上的疑問。刑事訴訟法第101條第1、4和5項是與聯邦憲法法院的判決(參照: BVerfGE 109, 279 <363 ff.>)一致下有差異的規定，

其對關係人事後告知的原則，於憲法上可承擔的，與在個案中例外的對立的重大利益取得平衡。因此，同樣特別是不應加以指責的是，嫌疑人於其身上不涉及資料調取，其無論如何，依據刑事訴訟法第101條第4項第4句的規定，不是，而是僅依一項衡量的標準被告知。在這個衡量的範圍內，得且必須就間接的關係人的利益充分的加以考量。

反之，法官就個案管制的規定於其中報告並未發生係不充分的。刑事訴訟法第101條第6項認為一項法院命令僅是依據刑事訴訟法第101條第5項的對告知的免除，而非依據刑事訴訟法第101條第4項的目的。上面的看法，為就依據電信法第113a條被儲存的資料的透明使用的報告的高的價值並未作充分的考量。只在直接對往來資料的資料詢問係牽涉到特定的人時，則對此人的事後報告只得依相應的採納理由的法院管制加以免除。在一些案例中，缺乏這樣的管制。在這些案例中，告知應依據刑事訴訟法第101條第4項第3句的規定因為關係人重大的利益而被加以排除。

dd)反之，對資料調取和資料利用的法院管制本身，以合於憲法要求的方式被保障。就依據電信法第113a條被儲存的資料的提取，依據刑事訴訟法第100g條第2項第1句，第100b條第1項第1句的規定，需要法官命令。法官命令並非授權機關去直接取得資料，而是課予服務供應商義務，將這些資料於自身的中間步驟，依命令的標準取加以篩選與傳輸。進一步依據刑事訴訟法第101條第1項、第7項第2至4句的規定，有可能，事後導致法院對措施的合法性的審查。整體而言，這些條文並未保障有效的法律保障這件事，並是不清楚的。

然而，就法官命令的形式要求的法律規定並未完全規範清楚的被訂定。刑事訴訟法第100g條第2項連結到刑事訴訟法第100b條第2項僅規定裁判形式的最低要求；此外依據刑事訴訟法第34條，一般告知義務於裁判時亦有適用。立法者應於新法考量，是否或許實質上有益，將嚴格的要求透過新增一特別且有區分的條文，授權法官命令(參照: BVerfGE 103, 142 <151>; 107, 299 <325>; 109, 279 <358 f.>)的補充性說理。無論如何於法律上必須去確保，應傳送的資料的範圍於命令中充分地選擇以合於比例原則的方式且對服務供應商明確的加以描述。

b)系爭規定關於為危險防範與情報部門任務，依電信法第113a條所儲存的資料調取與利用，亦不合於憲法上的要求。電信法第113a條第1句第2與第3號依其條文結構不滿足就對使用目的充分的界定的要求。聯邦立法者於此僅以一般化的方式，在不具體

明定使用目的下，去描述應使資料提取可能的任務領域。立法者毋寧將該使用目的之具體化其後留予立法，特別是各邦的立法者。在此立法者並不貼近立法者就憲法上對使用目的界定的要求的責任。當立法者規定電信往來資料的儲存，使其同時負有義務，就該規定憲法上合理的必要的使用目的和干涉門檻以及為保障目的建構所必要的後果規定等有拘束力的加以固定。電信法第113b條前半句中並未包含這般固定。毋寧是透過服務業者就所有電信往來資料預防性儲存的義務且同時就透過警察和情報任務於依近他們全部任務範圍內，交付資料以建立各種且無限公開使用的資料庫，對此（僅限透過粗略的目的設定）各自基於立法者於聯邦與各邦中自己的決定得被調取。這般依其目的設定公開的資料庫的備妥，提升了介於儲存與儲存目的間的必要關聯，且不合於憲法(見前揭：ＣＶ5 a) 。

反之，於電信法第113b條中並未包含針對告知義務過度的規定或為危險防範和情報部門的任務履行的目的而使用依據電信法第113a條儲存的資料的案例中的法院的控制，這件事是不應被指摘的。雖然這樣的規定在憲法上是不可捨棄的。但聯邦立法者得將此項與資料調取一致的規定委由各別專法且可能地透過各邦法律。

b)對依據電信法第113a條儲存的資料的容許利用，未就傳輸對信賴關係的保護加以規定時是不合比例的。至少對於一個狹窄的圈子中，基於隱密性的電信連線，這樣的保護原則上是被要求的(參見上述ＣＶ２e最後)。

4.最後，電信法第113b條第1句後半段，其就服務供應商依據電信法第113a條規定的查詢加以規定，於各方面不合於比例原則的要求。

然而，依據上面所發展出的標準，下面這件事沒有憲法上的疑慮，即立法者於電信法第113b條後半段針對關於特定的，對於機關而言已知的網際網路位址的連線所有人的查詢並未設定極端嚴格，對於依據電信法第113a條被儲存的資料的直接調取應被加以注意的要件。下面這件事因此亦是無可爭論的，即依據電信法第113b條第1句後半段聯結電信法第113條第1項的規定，這樣的查詢於沒有事前法官的命令，對於所有種類的刑事犯罪行為的訴追和一般對危險防犯和情報部門任務是許可的。然而此規定關於必要的干預門檻並不是相當清楚的。然而就合憲解釋可以如下的方式被理解，亦即電信法第113條第1項指引各別專法上的干預基礎且至少就資料的調取預設依據刑事訴訟法第161與第163條規定一充分的初始懷疑或是警察的一般條款意義下的具體危險(參照: Bock, in: Geppert/Piepenbrock/Schütz/Schuster, Beck'scher Kommentar

zum TKG, 3. Aufl. 2006, § 113 Rn. 7; Graulich, in: Arndt/Fetzer/Scherer, TKG, 2008, § 113 Rn. 8)。具體危險的干預門檻如同對於情報部門的查詢要求般，必須由本條中依合憲解釋方式被推導出來。

同樣地以合憲解釋的途徑，可能遭遇遇到一項對本條迴避刑事訴訟法第100g條的某種濫用。電信法第113b條第一句後半段連結電信法第113條第1項b條就合憲的理解上並不就機關對於其電信連線未為機關所知之連線所有人的公開調取，加以授權。反而允許機關相應的其在法律解釋中表明的目的方向僅得就其事前已知的網際網路位址提出查詢(參照: BTDrucks 16/6979, S. 46)。立法者想要在必要的新法範圍內審查，是否其看到法律上加以澄清的理由。然而電信法第113b條第1句後半段聯結電信法第113條第1項的違憲性在此並無法被確定。

然而由比例原則觀點下，電信法第113b條第1句後半段聯結電信法第113條第1項，於當本條一般而言認為就違反秩序的追查便足以為這般的詢問，是太過廣泛。雖然對立法者而言，依前面發展出的標準原則上並不禁止，於特別重要的案型中同於秩序罰法的領域內就這樣的詢問加以規定(見如上:C V 4 c)。然而此需要現行法中缺乏的，規範清楚的特別規定。此外，電信法第113b條第 1 句後半段聯結電信法第113條第一項，亦於當其中缺乏對關係人的報告的規定時，是違憲的。依據電信法第113條第1項第4句，查詢義務人面對關係人有義務保持沈默。同樣的由查詢申請的方面，機關的報告係絕不受保障。前揭不合於憲法上對依據電信法第113a條被儲存的資料透明化使用的要求(見以上:C V 3 a)。

5.總結而言，資料安全的法律上規定，或是依據電信法第113b條第1句第1號聯結刑事訴訟法第100g條，電信法第113b條第1句第2與第3號以及電信法第113b條第1句後半段等條文均不符合憲法上的要求。同時對於依據電信法第113a條規定的儲存義務亦缺乏憲法上可承擔的合理化。整體而言，系爭規定於結果上不符合基本法第10條第1項的規定。

VII.本案涉及基本法第12條第1項之職業自由並無違憲

與此相反，鑑於基本法第12條第1項在這個程序中必須對之去做成裁判的系爭規定，並無造成憲法上的疑問。女憲法訴願人4於第一審判庭BvR 256/08的程序中，其職業自由並未透過有系爭規定以及與此相關聯的財政上的負擔而受到侵害。

1.儲存義務的課予，至少於女憲法訴願人本身亦經營一向公眾開放的匿名伺服器(Anonymisierungsserver)時牽涉到她，構成對她的職業自由的

一項侵害。本身作為營業的女服務供給者得主張基於基本法第12條第1項的職業自由。本條亦於客觀上有對職業規範的傾向。儲存義務係針對如是向公眾開放的電信服務原則上係有償向終端使用者提供(參照: 電信法第113a條第1項第24號)，且藉此典型方式完全為營利目的(Erwerbszweck)的服務供應商。

就干涉而言是涉及一個職業行使規定。儲存義務被規定於電信法第113a條中且本身對電信服務供應構成技術標準的傳送義務被規定於電信法第113b條第1句前半段中。反之則缺少儲存義務相對於匿名服務作為職業選擇規定加以運作的要求，因為一項徹底的匿名不得再被提供。雖然當不但一項職業從事在法律上係受限時，而且亦於當對一項職業有意義的行使在事實上是成為不可能時(參照: BVerfGE 30, 292 <313>)，則一項職業選擇規定是被顧及的。然而依據電信法第113a條第6項規定的儲存義務並不導致，匿名服務於原則上不再得被營運。匿名服務得繼續於網際網路中，不可能透過私人辨識網際網路協定位址而瀏攬的情況下，提供其服務。匿名服務藉此使擁有一靜態的(且因此開放的) 網際網路協定位址的使用者隱藏其身分且保護其他使用者免於駭客或其他非法調取成為可能。

匿名性(Anonymität)僅在相對國家機關且僅於當資料調取依照就對於依據電信法第113a條被儲存的往來資料的直接使用的嚴格的要件，於例外情況下是允許時方被撤銷。依此僅有客戶於客戶的匿名利益係針對這般偵查特別重大案例的機關時而受到妨礙。透過上述匿名服務的提供在整體而言是不會失效的。

2.透過儲存義務的強加而成立的干預，在憲法上是有理由的。此項干預既不是關於技術上費用上，亦不是關於與此相繫的財政負擔上不合比例。

對於職業行使自由的干預需透過共同福祉(Gemeinwohl)上充分的理由方是合理的(參照: BVerfGE 94, 372 <390>; 101, 331 <347>; 121, 317 <346>)。原則上普遍福祉(Allgemeinwohl)的合理理由就此已足。(參照: BVerfGE 7, 377 <405 f.>; 16, 286 <297>; 81, 156 <189>; stRspr)。比例原則的要求同樣在此成立，亦即干預需為干預目的的達成而言是適當，必要且狹義合比例的。這些要件在此均具備。

a)儲存與傳送義務本身亦有助於刑事訴追，危險防範及情報任務的目標設定，而對職業自由的干預係正當的。這些義務受普遍福祉的合理理由支持，合於為一般公共利益的促進。一項較少進行干預，但同樣有效率且就公共部門(die öffentliche Hand) 而

言價格便宜的規定，並不明顯。因為電信往來資料自電信領域的私有化起不再發生在國家，國家在它那方面不再處於直接儲存的地位。將所有連線資料移轉予國家，以使其自行接手儲存這件事，已因與此相繫的風險不但就電信秘密的保護，而且對資料的安全與完整性皆不加以考慮了。同樣就透過費用負擔或費用義務的強加對職業活動的影響的必要性並不因此放下，因為相關任務以租稅手段的財務可能是輕微的手段 (參照: BVerfGE 81, 156 <193 f.>; 109, 64 <86>)。輕微的手段並非那種僅推遲費用負擔的手段(參照: BVerfGE 103, 172 <183 f.>; 109, 64 <86>)。

b)對儲存義務的課予典型地對相關的服務供應商而言不會加上過度負擔的。

aa)儲存義務超出許可的界限並非透過要求資料供給者交出的技術費用。因為相關的資料供給者，其必須於電信市場中活動，其本來於電信資料掌握，儲存知加工的範圍裡必須顯示有較高技術掌握的尺度。小型企業亦必須在這個領域內有這些能力。此外無論如何，大部分依照電信法第113a條被儲存的資料總是由相關的電信企業暫時為自己的目的加以儲存。為資料安全的確保的徹底組織上的要求並非始自電信法第113a條的儲存義務，而是早獨立於相關企業所提供的服務的對象之外。對此，依據電信法第113a 條的特別義務的課予，在技術－組織面向上並非不合比例。

bb)儲存義務涉及企業透過依據電信法113a條的儲存義務與此相繫的後續義務如資料安全的確保所生的財務負擔並非不合比例。因此上述也不是特別不可期待的，因為彷彿藉此不得將國家任務委託予私人企業。一項對「國家任務(Staatsaufgaben)」與「私人任務(private Aufgaben)」的概念區分，與原則上為公共福祉目的從事服務，而由私人自行負擔不容許的後果這件事無法由憲法中得出。毋寧立法者就將公共利益之確保義務課予於私人在其職業行使的範圍上這方面有較寬的形成空間 (參照：BVerfGE 109, 64 <85>)。立法者原則上得就為公共福祉利益的，作為商業活動的後果有需法律規定的維護之負擔與手段，去強加於合適的市場行動者上，以求與此相繫的費用以此種方式整合進市場和市場價格中。立法者於此不限於令私人僅於，當其職業活動得解決直接危險或其職業活動就這些危險直接正中犯人時，方得從事。毋寧介於職業活動與被強加的義務間的一個層級式的準事務與準責任機制即已足夠。(參照：BVerfGE 95, 173 <187>)。

此後，針對儲存義務所生的費用負擔並沒有基本的考量。立法者以此方式將與儲存相繫的成本依照電信部

門的私有化全部轉移到市場中。故如電信企業為獲利而得利用這些電信科技的新機會，其必須償付與電信相聯結的新安全風險的圍牆的費用，且以此代價工作。對企業強加的責任與由其提供的服務有緊密的關聯，且如此的責任僅得由其本人履行。在此亦非強加於個別的服務提供者為個案上的特別犧牲者，而是以一般形式就電信服務的提供去形構空間條件。這個作法於當企業原則上要負擔所生成本時，於憲法上是無可指摘。單純牽涉公共利益的目標設定不要求，為此就費用填補去加以規定(vgl. BVerfGE 30, 292 <311>)。一項法律以如下方式，即私人於行使其職業時被強加義務且經常牽涉相當多人時，去規範職業行使，該法於當不可期待加負擔與個別關係人時並不因此已是不合比例，而是直到當該法在一較大群關係人上侵犯了過度禁止原則時(參照: BVerfGE 30, 292 <316>)，該法方為不合比例。費用負擔以此種方式有致命的效果，在實質上是既不被表現在外，也不被認知的。

就此不需再進一步審查，是否就特別的案例群體(參照: BVerfGE 30, 292 <327>)或由比例原則觀點的特殊狀況下要規定嚴厲規則(Härteregelungen)。因為自女憲法訴願人4於第1審判庭BvR 256/08審判程序中提出的主張中是毫無所得。特別是她於涉及匿名服務時針對一項超出在其他電信企業的匿名服務的負擔，既不為己，亦不為其他服務提供商，為這般服務充分合理的透過具體的支付來加以償付。但僅於這樣條件下，於匿名服務的行使上確定超越立法者的形成空間。只要立法者的考量僅透過推測和強調被質疑的情形下，聯邦憲法法院無法就這個問題進行探究(參照: BVerfGE 114, 196 <248>)。

關於可能的剩餘費用負擔，歸屬於依照電信法第113b條第1句第1號聯結刑事訴訟法第100g條規定，而被立法者規定為一補償規定(vgl. § 23 Abs. 1 Justizvergütungs- und –entschädigungsgesetz)的傳送義務，原則上沒有疑慮。在此規定的損害賠償請求權並非本程序的客體。

VIII. 對系爭規定無再更進一步的主張

此外在諸基本權利中，於基本權利的侵害已受理指控的範圍內，針對系爭規定沒有進一步的主張。

IX. 系爭規定於確定基本權侵害的情況下被宣告為無效

因基本法第10條第1項電信秘密的基本權被侵害，故電信法第113a條與第113b條以及刑事訴訟法第100g條第1項第1句等規定，在其後得依據電信法第113a條規定提取往來資料的範圍內，應屬無效。系爭規範因此於確定基本權侵害的情況下應予宣告無效

(參照：聯邦憲法法院法第95條第1項第1句與第95條第3項第1句)。此外，依據2008年3月11日與2008年10月28日所頒布的暫行命令，由服務供應商於訊息聲請的範圍內所提取，但暫時不得被傳送到聲請機關，而是被儲存的電信往來資料，必須立即被刪除。其不准再被傳送到聲請單位。

關於費用報銷的決定是基於聯邦憲法法院法第34a條第2項的規定。

本裁判係就歐洲法上的問題，形式合憲性以及原則上預防性的電信往來資料儲存與憲法的合致性，而於結果上作成的一致決。對電信法第113a條與第113b條的評判係結果上以7比1票決為違憲，且就進一步實體法上問題於特別投票達成6比2票決結果。

(系爭) 規定依據聯邦憲法法院法第95條第3項第1句被宣告為無效且不只是被宣告為與基本法牴觸。合議庭對此以4比4票決作成決定。(系爭) 規定依此亦不得進一步於有限的範圍內被加以適用，而是維持被宣告無效的規定的結果。

法官：
Papier
Hohmann-Dennhardt
Bryde
Gaier
Eichberger
Schluckebier
Kirchhof
Masing

Schluckebier法官對於第一庭於2010年3月2日之判決所提之不同意見書

- 1 BvR 256/08 -
- 1 BvR 263/08 -
- 1 BvR 586/08 -

本席根據以下提綱式的考量，對於本判決的結論及大部分的說理部分難以贊同。

本法庭認為對往來資料的儲存係對於基本法第10條的基本權利的一項特別嚴重的干預的效果。根據本席之見解，雖然可賦予這樣的干預特別的力度，然而相較於涉及內容的監察措施，其顯示出相當少的力度(就此以下 I)。本席進一步認為，考慮到立法者追尋的目的，亦即對於在個案中有重要意義、或對於藉助於電信而行使以致於很難釐清的犯罪行為的釐清(Aufklärung)，往來資料的儲存暨刑事程序法上的調取規則構成有限的干預，這看法在憲法上原則是合理的。以上述為基之條文，根據本席之見解，對於狹義合比例性原則的審查，特別是恰當性與期待可能性的審查(Angemessenheits- und Zumutbarkeitsprüfung)，實質上站得住腳 (就此以下 II)。於上述，於被儲存與被傳送的電信往來資料的資訊安全的確保就只有內容上的要求;這一點本席與合

議庭多數見解一致，故於以下不再論及。就法律效果請求上可能是基於合議庭多數對於系爭規定無效的評價，在本席看來也沒有不同的看法，這也準用於由合議庭頒布的至有新法生效前的暫行命令應予適用(就此以下 III)。

I.往來資料的儲存干預基本法第10條的基本權利甚微

合議庭多數認為對電信服務業者往來資料以六個月儲存是對基本法第10條第1項的一項特別嚴重的干預。本席對此並不贊同。

電信秘密係保護通信過程的內容及更進一步的狀態，使*免於透過公權力的識別 (vor einer Kenntnisnahme durch die öffentliche Gewalt)* (參照: BVerfGE 100, 313 <358>; 106, 28 <37>; 107, 299 <312 f.>)。如果我們認為私人服務業者之儲存義務(電信法第113a條)已構成干預基本權，係因服務商是「國家的助手(Hilfsperson des Staates)」 且該通信資料的儲存係歸責於國家規定，則就干預強度的評價而言，以下情況便有特殊意義，亦即對往來資料的某種藉由國家單位的存取，完全保留在私人服務商的領域。這些往來資料處於締約雙方的手中，就這些締約雙方而言，提供於這種契約締結時預設的基本信賴，其首先對因經營和計算理由而觸及的資料，自始作嚴格保密的處理且確保對這些資料的保護。如果資料安全是依科技上可能最適的水平被保障，則欠缺對積極干預的寒蟬效應或(如同本判決所述)「持續被監看的感覺(Gefühls des ständigen Überwachtwerdens)」以及「迷惘的威脅(diffuse Bedrohlichkeit)」等接納的每一客觀的基礎。此外儲存並非被秘密的，而係基於被頒布的法律所達成的。儲存的對象並非電信過程的*內容(Inhalt)*。只要能允許以往來資料在有限的範圍內逆推回這樣的內容或甚至對運動圖像或社會側寫的重建成為可能的，則其將觸及相應調取規則的合比例性問題以及法律適用層次上合比例性要求等問題。像如此在個案中於有相對重要理由下得達成的密集干預式的利用，並不會合理化下面這些事，是項利用作為全部中的例外情況，在儲存的力度上被賦予決定性意義，且不受限的以這些理由為基礎。

合議庭早於其2003年3月12日之判決(BVerfGE 107, 299 <322>)就涉及電話交談的電信連線資料的*供應(Herausgabe)*而指出，干預的力度(在此透過調取) 係低於對涉及電訊內容的電話監聽，然而無疑是大的。雖然考慮到儲存義務的擴散效果與此效果的預防性(Vorsorglichkeit) 而給出此一特殊的案情形成。然而就干預的力度而言，對這一般特別嚴重的干預仍應去維持一經驗上的距離，如同就聲

音的住居監規或是資訊科技系統的線上搜索(Online-Durchsuchung)，同樣及於*透過國家機關的直接掌握 (durch unmittelbaren Zugriff staatlicher Organe)* 提取電信的內容監察和利用，且此外(不同於在此) 就這些嚴重干預以特別的方式而產生的風險，即牽涉私人生活形塑的絕對嚴格被保護的核心範圍。對所有電信接觸的往來資料的掌握，在私人服務提供商不具識別而透過公權力，且在嚴格實質要件下特別規定的資料(於法律適用的層次上規範化透過受命法官審查且嚴格限制) 於程序，安全的措施(例如依刑事訴訟法第100g條所規定的調取)之下的聲請的可能性，是項掌握相反的由涉及個人的基本權利主體的觀點並沒有如這般重力度的基本權干預，以致似乎得被合理化為，將該干預評價為「特別嚴重(besonders schwer)」且藉此歸類為對基本權的最大可想像的干預之一。其後基於被私人服務供應商的儲存的干預，被認為是特別有力度的。上述的差異在系爭規定的適當性審查上取得進一步的意義。

II.往來資料的儲存暨刑事程序法上的調取規則實質合於比例原則

關於為刑事訴追目的的儲存義務與往來資料調取的系爭規定是（不同於合議庭多數的見解）並非不適當的；其對當事人而言亦係可期待的也因此是狹義上符合比例原則。

1.這些規定符合源自比例原則的恰當性與期待可能性的要求。基於介於對基本法第10條第1項干預的重度與能證成此干預合法理由之重力二者間之整體衡量推導出立法者已維持由上揭要求得出的界限。

狹義比例原則要求干預的強度，在整體衡量上不得超出與能證成此干預合法理由的重力的比例(參照: BVerfGE 90, 145 <173>; 92, 277 <327>; 109, 279 <349 ff.>; 115, 320 <345>)在介於國家為的法益保護義務與個人為維護憲法保障權利之利益二者間之緊張關係中，立法者的任務是以抽象的方式去達成相衝突利益間的平衡(vgl. BVerfGE 109, 279 <350>; 115, 320 <346>)。給立法者對此（合議庭多數在方法上專有名詞式的論及）的是考量與形成空間。

就系爭規定的適當性的憲法上意見而言，必須在出發點上考量，基本權利並不窮盡於防衛國家的干預。根據其客觀－法律上的面向得出國家的義務保護市民免於騷擾。此項保護義務連繫到以下任務，採取合適的手段以避免對法益的侵害，儘可能釐清侵害，就侵害歸責且重建法律和平(參照: Jutta Limbach, AnwBl 2002, S. 454）。在此意義上對市民暨其基本權利，以及共同體根基的保護之確保和如重大犯罪行為的識別般的阻止，同時

算是透過市民的和平共同生活與基本權利無異議的行使的要件。有效的識別犯罪行為與有實效的危險防範本身並非對市民自由的威脅，對此不許漫無標準和限制。它們二者是在合適性與期待可能性的範圍內被要求，以求在需要它們的同時去確保基本權利及保障個人的法益。市民在法治國家中必須如同基於*對抗(gegen)*國家的保護般*透過(durch)*國家有效的保護自身。（參照: Di Fabio, NJW 2008, S. 421 <422>)與此相對，聯邦憲法法院將國家描述為憲法上被構作的和平與秩序力量且由國家對其市民加以保障的安全被承認為憲法價值，國家與其他處於同等位階且不可捨棄，因為國家這個制度亦得由此導出其合理性(參照: BVerfGE 49, 24 <56 f.>; 115, 320 <346>)。

就透過立法者而相衝突利益的平衡而言，立法者創設了對於犯罪行為的辨識與危險防範的法律上基礎，總是應關注，對個人而言於其共同體關聯性與共同體拘束性上期待某程度的影響，這些影響是致力於對其他市民的法益保護與基本權保護，但亦致力於對自身的保護(參照: BVerfGE 4, 7 <15>; 33, 303 <334>; 50, 166 <175>)。同樣考慮到以上情形，必須給予立法者就其有義務的（利益）平衡一個形成空間，以便其一方面保障基本權載體的自由權，但另一方面創設這方面法律上的空間條件，其使市民的基本權與法益免於被侵害的客觀保護及以合適與可期待的手段有效的辨識犯罪行為等成為可能。

2.立法者將電信往來資料儲存為期六個月的意義，使用目的規定以及刑事訴訟程序上的調取規定等維持在其基於憲法而達成的形成空間中。由系爭規定出發的影響對於關連到往來資料儲存的電信使用者而言是考慮到需保障的基本權與法益並非不適當與不可期待；對透過犯罪行為被侵害的個別與一般法益保障的立法者的力度，以及於常常幾乎不留痕跡的電子通訊可能性遠遠超越建立的時代，就相應危險的防範二者，立於需達成平衡的相反的一方。合議庭多數原則上亦如是者，然而其關注在此觀點上僅對規定的合適性與必要性問題之見解上，就此並未明白的處理，真正對關連到的重要性「彼此相關」的適當性審查。

a)對立法者而言「自由與安全(Freiheit und Sicherheit)」的緊張關係中，就介於在議論中的法益與利益間的抽象平衡所初步達成的形成空間(參照: BVerfGE 109, 279 <350>; 115, 320<346>)係透過規定對象的特性與規則應規制的現實性二者共同形塑。因此規定的目的和實效亦應於適當性與期待可能性的判斷上被顧及。

立法者藉由電信監察與其他秘密

偵查措施法修正案，以及對歐洲共同體2006/24指令的轉換對刑事程序秘密偵查方法的體系作了基本的修正。立法者藉此以相當仔細的方式依賴取得的鑑定書如法學中充分的討論，檢察與警察實務的實務報告（參照: Gesetzentwurf BTDrucks 16/5846, S. 1）。在議會程序中達成一個專家證人的詳細的聽證(參照: die Protokolle der 73. und 74. Sitzung des Rechtsausschusses des Deutschen Bundestages, 16. Wahlperiode, am 19. und 21. September 2007)。努力的部分總是將迄那時為止聯邦憲法法院的判決加以轉換。該法律係最後以高度多數表決通過(參照：Plenarprotokoll des Deutschen Bundestages, 16. Wahlperiode, 124. Sitzung am 9. November 2007, S. 13009 (D); siehe auch die Einbringungsrede von Bundesjustizministerin Brigitte Zypries, a.a.O., Plenarprotokoll S. 12994 f.)。立法者當時欲將新的科技發展考慮進來，因為它針對特別難以偵防的犯罪，交易與經濟犯罪，以及利用現代通訊技術遂行的犯罪行為等的辨識(參照: Gesetzentwurf BTDrucks 16/5846, S. 2)，而對目前在此討論中的規定，立法者有將大的效果加以考量。在此進一步被闡明的目的是，對於一個實效、法治國家的刑事司法的必然的需求加以考量，其任務在於，在其中就其法律上的界限中去創造正義與法律和平。這個目標原則上預設了就必要事實辨識的可偵查性(a.a.O. S. 22)。在此立法者亦由下出發，電信往來資料因為科技的演進在費率上（完全不同於過往時代，當時電話的通聯資料仍可提供許多月）在法官為訊息提供的命令生效前或是其僅就一相應的聲請所必要的資訊事先已被提供的情況下，常常是要不是根本未被儲存，就是已被刪除(a.a.O. S. 27)。眾所周知，犯罪行為本身在透過或在網際網路中，就在進行。與犯罪存在相聯繫的社會現實在電信的不同分枝的範圍中建構自身。當立法者對此反應到，依其評估僅在當相應的往來資料歸屬於特定期間內的保護與儲存義務時，該義務由立法者強制予服務提供者，該必要性方可能是有效的，故這件事原則上並非不適當且對於基本權主體涉及其資料時亦是可預見的。法秩序亦如其他領域如（在可能不直接與此相較的情況下）在住民登記義務(Einwohnermeldepflichten)或透過銀行的所謂存摺資料(Kontostammdaten)的保留中(參照：dazu § 24c KWG; BVerfGE 118, 168)亦認識到這樣的先前防範。

由立法者所選取的方式並未傾斜這件事，亦於聯邦網路局於2008/2009年指出近年來的語音和其他的資料通信的不同入口的數量的活動報告之中得到證實。本報告令人印象深刻

的陳列出鑑於連線數量不尋常的增長率，尤其是在網際網路中互動的語言和資料總量。本報告闡明，近年來人們的通訊行為有基礎性的改變（參照：同上如頁38關於數位用戶迴路連線(DSL-Anschlüssen)，行動網路使用者的發展，頁50；頁53就在行動電話中的語言總量以及就一次付費期限內無限使用－計算的增長率，頁59關於企業連線的往來總量）。

在這種情況下，對立法者而言，為保護法益持有人的目的，將犯罪行為的被害人，考慮到對其可預見的手段的實效且適應於變動中的情況（透過對資料供應商義務，於其領域內將往來資料就某種程度的期間加以保護和掌握），此事基本上是不致於失敗的。國家機關伴隨技術進步的腳步亦並非僅得被當作各種犯罪偵防方法的競技場的完善者，而進一步補充有效的傳統偵查手段，而是完全在傳統通訊型式的背景下移轉到數位信息往來的加工處理與儲存，針對有效的刑事訴追與危險防範而言，不只是在嚴重犯罪，而且在個案中有重大意義或藉助電信從事的但在沒有掌握往來資料極難釐清，犯罪行為的辨識的範圍內，對往來資料提供六個月，依立法者無爭議的考慮是有重大意義的(參照：BVerfGE 115, 166 <192 ff.>; siehe auch BVerfG, 1. Kammer des Zweiten Senats, Besch-luss vom 22. August 2006 - 2 BvR 1345/03 -, NJW 2007, S. 351 <355>)。

同樣合議庭多數相應地承認，對電子或數位通訊工具及其傳播漸增的利用在幾近所有生活領域的情況下，使得刑事訴追如同危險防範般變得困難，而且現代通信科技漸增在被用於不同犯罪行為的犯行上且促進犯罪行為的效率化。但合議庭多數於狹義比例原則審查時，依本席的看法並未就這發展給予應有的重力尺度。

b)此外合議庭多數將立法者的考量與形成空間侷限於對犯罪行為辨識和危險防範領域為對人民保護相應的適當和可期待的規定上，且以實際結果看幾近完整。藉此合議庭多數亦遵守憲法法官自我節制（judicial self-restraint）的要求，相對於對民主正當立法者不充分考量的構作式裁判。合議庭多數依照立法行為指引給予立法者一項到細節均依照（立法）行為指引的法律規定，其就解答而言對立法者並無留予值得一提的空間，該行為指引就已給定，持續上的關係在電信領域中依其考量是正確的。

本判決規定六個月的儲存期（亦即透過歐洲共同體指令被要求的最低標準）作為上限且充其量憲法上合理的，對於立法者規定技術上去規定使用目的規定同時需包含探訪要件，這要件限於刑法中的行為目錄技術且排除為藉助電信工具著手的難辨識的犯

罪行為的辨識的往來資料利用的可能性以及以確定之方式擴張報告義務與法律保障最低限度要件。其後留給立法者而言就政治者責任的構作上沒有更值得一提的遊動空間。立法者實質上限於，在邊緣範圍針對刑事程序法上的聲請對目錄作細微的適應與變更。立法者若不想違反共同體的新規定，就必須將判決轉換為新立法。藉此，本判決於實際結果上*取代(ersetzt)*立法在細節上制定出只在憲法上可允許的規定。

3.合議庭多數要求立法者於使用目的規定範圍內同時應該創設關於探訪要件和程序確保的要求上的明確性。藉此合議庭多數對立法者採行規則技術上的可能性，藉由一補充性法律基礎的體系，如同其在其他領域迄今未受爭論般去工作。故合議庭多數例如在所謂的帳戶存簿判決中於憲法上並未去指摘，聲請就履行其他方面規定的任務而言是必要的，然而聲請誘因與要件被規定在其他法律中(參照: BVerfGE 118, 168 <191>)。合議庭多數與此相反在所謂的自動識別結構(automatische Kennzeichenerfassung)判決中，但其於系爭法律並未列出使用目的的陳述且因此當時所有合理的使用目的均被包含在內，視使用目的說明因此為不充足的(參照: BVerfGE120,378<409>)。在此的情況是另一回事（電信法第113b條）。本條於當這些法律要件與標準，其領域專門上於一個各別牽涉法律領域的自身規範中被規定，資料透過聲請而導致對干預實質上的強化時，因此直接致力於規範明確性與透明性。二個規定均自明的服從於（也許亦在其共同作用中）憲法上的要求與憲法上的審查。即使當聯邦立法者本身較之於邦立法者負有儲存往來資料的責任，邦法上多少補充的規定同樣要合於憲法。因此法律保護赤字在此不應出現。

與此相應，在此沒理由於刑事訴訟法第100g條中，為憲法訴願人所部分聲明不服的刑法逮捕規範之外，亦針對為危險防範與情報任務目的的往來資料的利用的近似要件加以討論。

4.合議庭完全對立法者排除針對並非在刑事訴訟法第100g條第2項中所列舉的，然而於個案中仍有重大意義的，如同這樣的行為，其借助於電信而著手的（刑事訴訟法第100g條第1項第1句第1和2號）的犯罪行為的辨識而對往來資料的提取性。在此合議庭多數同樣未充份的關注被考慮到的犯罪行為 (立法者視其為難以辨識)與該犯罪行為對於犯罪行為的有效辨識的意義的力度。在刑事訴訟法第100g條第1項第1句第1號的案型中，立法者針對合議庭於2003年3月12日判決((BVerfGE 107, 299 <322>)就電信連線資料的交付所衡量的判準。合議庭於那時發展出，那樣的干預只得

就立法者普遍對此賦予特別力度的，且於具體案型中有重大意義的犯罪行為，例如基於全面性威脅所造成的損害與程度，而被加以正當化。本席不認為，合議庭對之不加指摘的干預門檻就針對所謂的儲備－往來資料(Vorrats-Verkehrsdaten)的存取基本上可能被並評定另外的力度。受命法官，就討論中案例形成有義務在個案中作比例原則審查，其亦應於個別的案例中就提取往來資料的力度參與衡量且應透過其命令之見解加以限制。

關於借助電信而遂行的行為，就這些行為，合議庭同樣藉依據電信法第113a條被儲存的往來資料提取同樣想要全部獲知，並不會被給定足夠的力度，使立法者在此由極大的辨識困難出發。同樣這件事會在除了對應辨識的要件事實的特別力度，而對先被保留的往來資料的調取之外，總是在當(如同在此)立法者對調取要件藉著一項嚴格的補充性條款(Subsidiaritäts-klausel)加以建構時，被認為是適當的，據此該措施僅在當對案例事實的探究或是偵查嫌疑人的所在地，以其他方式可能會無望時且資料的調取(亦是在個案中) 與事務的意義以適當的比例呈現(刑事訴訟法第100g條第1項第2句)。

為確保一項有實效的刑事訴追且不容許出現極大的保護漏洞，是立法者的事務，對立法者而言，不應容許同樣在這方面特別嚴重的犯罪行為，於考慮到受損的法益總有的特別力度而去允許往來資料的調取，因為立法者於其考量認為，只有如此方得產生事實上持續法外空間及完全排除對辨識持續的空轉。就此該指出是例如跟蹤糾纏罪(Nachstellung) (德國刑法第238條第1項第2號，「線上追蹤(Cyber-Stalking)」)的刑事犯罪構成要件，常常就證明上處於一個「各說各話局面(Aussage gegen Aussage-Konstellation)」，但至少起初就不明人士(unbekannte Täters) 的辨明常常是唯一的偵查手段。在此，一項採集機制(Fangschaltung)的可能性繼之亦僅是有限的，因為該採集機制無法掌握例如電子郵件往來具最終亦依賴服務供應商的市場實力(Goodwill)。類似情形亦適用於對脅迫(Bedrohung)的構成要件，尤其是還有網際網路中的詐欺(Betrug) 的領域內中，於警察的犯罪統計中，有憑據的可觀的案件數量被加以討論。其他的犯罪行為(Delikte)最後也在考慮之內(德國刑法第202a至202c條，窺探資料罪，(幫助)窺探與攔截資料罪(Ausspähen und Abfangen von Daten); 亦見:德國刑法第269條，偽造具有證據價值的文件罪(Fälschung beweiserheblicher Unterlagen)，德國刑法第303a條，變更資料罪(Datenveränderung)，德國刑法第

303b 條，破壞電腦罪(Computersabotage); 德國有價證券交易法第38條第1項聯結德國有價證券交易法第14條第1項第1號，所謂的內線交易(Insidergeschäft)，德國有價證券交易法第38條第2項聯結德國有價證券交易法第39條第1項第1號，德國有價證券交易法第20a條第1項第1句第1至3號，非法操縱行為(unerlaubte Marktmanipulationen); 德國刑法第86條，散播違憲組織的宣傳內容罪(Verbreiten von Propagandamitteln verfassungswidriger Organisationen)。

立法者固可就這些(刑法)構成要件個別在由合議庭要求的嚴重刑事犯罪行為目錄中加以採納。然而對此立法者指出對責任原則(Schuldprinzip)負有義務的適當的，想要被合理化的刑罰嚇阻的界限。不是於經營上被採行的或是於個案中不引起特別高損害的犯罪行為(Delikte)，幾乎不被允許如合議庭所呈現的收進這樣的目錄中。同樣對於因單純經營技術上仍存有的「非儲備的資料(Nicht-Vorratsdaten)」的迴溯幾乎不能對辨識赤字(Aufklärungsdefizite)去加以減輕。在此介於不同的服務供應商間有經驗上大的差距。其中一部分服務供應商不會保留資料，一部分服務供應商於數小時或數天後便已將資料刪除。導致向申請法官命令的偵查手段(Ermittlungsmaßnahmen)，且其後已為這般申請作準備，以及就聲請為裁決等，較之往來資料因營運技術上的理由而在服務供應商處備妥提供，常常需要較長的時間。

5.合議庭為危險防範目的設定的調取門檻處於類似的情況。由合議庭認為具充分力度法益，以便將往來資料視為可調取與可利用的，此法益必須就對有明顯被要求於公共利益中被維持價值的事物的非同時普通危險的防範也考量在內。對此本席無法理解的是，即在這個意義上將仍受基本權保護的(參照: 基本法第14條第1項)有意義的事物價值排除在外。對此保護利益的涵括考量，當針對往來資料提取(例如於聯邦刑警局法第20m條)有規定一項補充性條款時，至少不是不適當的 (以其他方式可能會無望時或根本上極困難時) 。

6.只在合議庭多數最終假定對於對往來資料提取的案型而言，告知義務(Benachrichtigungspflicht)的擴張以及對於刑事訴訟法原則上不再有所謂的*公開(offene)的*(資料)調取，而主張一個所謂的「*前於* (*vor*) 聲請或傳送(Abfrage beziehungsweise Übermittlung)」達成的告知義務，於當保護非與研究目的對立時，則要求信賴立法者的構想且如此延伸到立法者的形成空間。立法者的構想在於，就所有的「*秘密的(verdeckte)*偵查手段(Ermittlungsmaßnah-men)」去規範，就此立

法者亦明白考慮到往來資料提取(Verkehrsdatenerhebung)(Gesetzentwurf BTDrucks 16/5846, S. 2)。同樣刑事訴訟法第100g條規定，得「於嫌疑人不知情下(ohne Wissen des Betroffenen)」，調取往來資料。上述亦有它的好理由。因為偵查通常是由在被注意的變動所標示出來且加速去執行。不在「*近期(zeitnah)*」強制性的在程序確保與法律保障的目的上被積欠的花費，應「*首先(zunächst)*」被維持在一定範圍內。此外立法者亦就往來資料提取制定了關於告知義務的有差異的規定 (參照: 刑事訴訟法第101條第1項、第4項第1句第5號、第5項)，此條文並未規定事前告知。此外，立法者藉形構，首先於嫌疑人不知情下調取往來資料，採取可認知的類型化，其多數源自偵查目的，嫌疑人所在地不明或有必要加快事物辨識等與事前－告知相對立。對嫌疑人是有期待可能且因憲法之故而隨立法者之便，這很明顯的不是不恰當。

III.合議庭頒布的暫行命令應予適用

由合議庭多數就系爭規定宣布的無效宣告，雖是由多數承擔的不兼容宣告的法定結果。然而在此基於合議庭多數的憲法考量或許有更詳盡追溯聯邦憲法法院的持續的判決，對立法者去設定立新規定的期限且就現有條文規定依照由合議庭頒布的暫行命令的標準去宣告暫時繼續適用。因為合議庭給予立法者可能性，往來資料儲存義務就六個月期限加以規定且根據於判決中列舉的要件去就實質上合於暫行命令的調取規定加以創造。本判決的標準首先由暫行命令中的標準去區分, 就資料安全設定較高的要求且進一步要求報告義務。就此區分詳細的立於對無效宣告的衡量(合於聯邦憲法法院常見的實務)中，首先是不予考慮且不認為是強制的，暫時只由服務供應商因營運技術的理由仍規存資料的調取開始。因此暫時至立新法前就危險防範將是重大的赤字且就(犯罪行為) 的辨識亦需處理和忍受重大刑事犯罪行為。依照由合議庭發布的暫行命令的理由以及於此被採取的衡量已指引出。附帶的，服務供應商必須就系爭規定之轉換去採取其預防措施且必須建立舊狀態，以便於共同體法要求的新的，已修正的且花費甚鉅的法律的案型中，去重新創造要件。

Schluckebier

Eichberger法官對於第一庭於2010年3月2日之判決所提之不同意見書

- 1 BvR 256/08 -
- 1 BvR 263/08 -
- 1 BvR 586/08 –

本席就合議庭多數的裁判於部分結果上和實質的說理殊難贊同。本席

原則上在此參與Schluckbier法官的批評，本席在結果上與說理上壓倒性的連繫於Schlackbier 法官的意見。因此本席就以下限於就支持本席立場的考量以簡短的摘要。

1.依本席之見，對電信往來資料的儲存的法定命令要求，在對於法律規定的資料處理考量到，其人與事上完整的範圍，其無誘因且相當長的持續，亦是對基本法第10條第1項有力度的干預，然而儲存義務本身在此限於就往來資料而不是電信過程內容之掌握，而且因為儲存義務去中心化的由私人服務提供商達成，故此隨儲存而來的干預亦並非如合議庭多數一般的認定係重大的干預。

合議庭多數對於造成人民通信行為上的寒蟬效應的憂慮，本席認為是無理由的，至少在經驗上不成立，本席考量到資料儲存的立法構想，其繫於由去中心化由私人服務供應商儲存往來資料以令國家機關自由取得且為資料提取規定了內容上與程序上嚴格的門檻(特別是補充性的法官保留)或是亦依本席就這樣的法定規定尚待補充之見，係不具理由且無論如何在經驗上無法證明。

對於基本法第10條第1項的保護利益的實質的負擔效應，此效應由對市民的資料儲存規定出發，因此依本席之見首先植基於因大量資料儲存而起的潛在的危害，其係透過服務供應商一方，透過無權限的第三方抑或是透過為刑事訴追或警察機關的過度的利用等所生的濫用。上揭情況在此是必須擔憂的。因此本席無限制的贊同合議庭多數就此高要求的，由立法者對資料提供商所加規定的資料確保立場。就其他對於為資料儲存、資料提取，以及資料的進一步使用（刪除與記錄義務，透明化的法律保障規定）的程序上之確保，這些合議庭多數對之主張要求的大部分，本席原則上與之意見一致；然而合議庭多數於判決中，以此種關聯為立法者所制定的預先規定，依本席看法大部分太過細瑣且並不充分考量憲法於這個關聯中亦給予立法者的形成空間。

2.本席與合議庭多數不同的，且與 Schluckebier 法官一致的意見如下，依電信法第113a條與第113b條為基礎的，為儲存規範與資料取得之層級式法律上責任的立法構想，原則上是合憲的。在此構想範圍內，電信法第113b條並未構成獨立且超出在電信法第113a條中資料儲存規定範圍外的對基本法第10條第1項的干預。毋寧本條包含對於往來資料儲存而言，正符合憲法要求的目的規定。直到在電信法第113b條第1句規定由法律上另行對往來資料的提取授權而導致一項新的，超出迄今為止成功資料儲存的意義上的對基本法第10條第1項的干預。以此方式聯邦立法者彷彿對於就

各自具體領域有權限的聯邦，或憑其憲法與民主正當性而來的授與邦權限的立法者，課予負擔去決定，是否以及以何種範圍內，立法者為刑事訴追，危險防範或是情報單位的利益而應該去掌握電信往來資料。在此個別的立法者很自明的需在自己責任對於合比例取得往來資料的憲法界限去加以保護。

一項為不確定目的對於儲備資料蒐集的違憲規定，在此不成立。聯邦立法者在電信法第113b條中，同時藉根據電信法第113a條服務供應商就資料儲存所負義務而列舉以下目的，依之被儲存的資料得被加以利用。不過由聯邦立法者藉資料儲存規定對於透過資料儲存立法加諸於市民負擔所生的潛在危害所承接的負擔，依本席見解(就這點本席在出發點上同意合議庭多數的立場)除了對使用目的加以作基本的規定外，亦要求無論如何對最低干預的門檻的確定，如同此確定於電信法第113b條第1句第1號聯結同時被發布的刑事訴訟法第100g條第1項，為了刑事訴追和在電信法第113b條第1句第2項中為了危險防範等而規定的「重大危害(erhebliche Gefahren)」的概念，但無法與在電信法第113b條第1句第3號為履行情報單位任務所規定的相比。上述的作法需要相應的補充。對於使用目的一項仔細且完全的規定，如合議庭多數對聯邦立法者同時藉資料儲存規定所主張的，本席因憲法之故不認為係必須的。

3.本席最後且特別是對合議庭多數的衡量結果，只要其可能在於刑事訴訟法第100g條中規定的對於依據電信法第113a條所儲存的資料的為刑事訴追目的的使用內容或視為違憲的範圍內則不予贊同。首先，這看法的原因在於，合議庭多數依我的看法在出發點上，就對方透過資料儲存規定引致對基本法第10條第1項的干預係評價為一項過大的比重且就有效的刑事訴追和有效的危險防範合理的涉及整體暨個別公民，相對的對之評價為微不足道。此外，合議庭多數對於賦予立法者對於集體保護利益的評價與規範形成的空間的關注太少。就此請參閱本席由Schluckbier法官的不同意見書中指出的說明。

合議庭多數的比例原則審查總是犯了，在它們的衡量一直是由對於一項完全的，最終對相關公民的運動側寫或社會側寫中的資料提取的最大可能干預出發。對此本席實際上主張的干預是，此干預於其門檻上不亞於對於針對牽涉到市民的電信內容的一項有力度的掌握。然而，這個視角並未考慮到，對個別事件的大量資料提取，短時間且電信關係僅得以或多或少的人（如一個人一天中或是特定的幾個鐘頭內的電信聯繫）為對象。明顯的，一項僅極少的，不與截取通訊內

容相較的干預力度合於這樣的資料提取，而不注意在其係向完整安置的資料集被探詢的。合議庭多數為求視每項資料提取為一對基本法第10條第1項之特別嚴重的干預，在不顧及其個別具體的範圍，且因此一般而言可能是因憲法之故彷彿有義務對立法者設立極高的干預門檻，儘管對此有爭論，依我的看法，合議庭多數意見彷彿總是達成在價值衝突上妥協，就同類的資料毫不加以質疑便任由機關得探詢，儘管這些資料並非依電信法第113a條，而是由資料提供給人因經營的原因而加以儲存的。

依此出發，本席儘管因出發點上不同的力度評價，得接受由合議庭多數就為危險防範與情報任務的目的（CV2b和c）而對往來資料的允許使用所作的標準形式要件仍表贊同，但不及於就他們對於刑事訴追（CV2a和CV1 3 a aa）的要求。就這點而言本席認為由立法者在刑訴100g條中創設的為刑事訴追的目的而對資料提取與資料使用為合憲的。此為在每一個案中需就資料探詢的許可的裁判的受命法官的任務，去就當事人基於基本法第10條第1項應受保護之利益，在考慮到各自干預的力度作合適的考量，是項考量如同對於藉助電信而為的犯罪行為於刑訴第100g條第1項第2句被立法者特別明文所要求的由合議庭多數的本身立場看來，在本席的看法可能單純是對系爭規定的違憲性去加以確定且相應的就此事發布的暫行命令至少是就到合憲的新規定被創設前，這段期間內的資料提取與資料儲存加以規定。藉由對規定的無過渡期的無效宣告且課予對基於暫行命令所取得的往來資料的刪除義務，合議庭多數見解造成了為刑事訴追的缺點，尤其是無法排除所有危險的風險，雖然資料探詢是合於暫行命令中被形式化的要求，原則上亦被視為合憲且相應的法律規定如預期。對一個這樣的解決方法本席不予贊同。

法官：Eichberger