查詢電信用戶主資料案（二）

德國聯邦憲法法院 2020 年 5 月 27 日第一庭裁定
- 1 BvR 1873/13 -
- 1 BvR 2618/13 -
BVerfGE 155, 119-238

傅玲靜　譯

要目

關鍵詞

人工查詢資料程序（Manuelles Auskunftsverfahren）
用戶主資料（Bestandsdaten）
登入資料（Zugangsdaten）
通訊紀錄（Verkehrsdaten）
資料之傳輸（Übermittlung）
資料之調取（Abruf）
資料之利用（Verwendung）
雙門扉圖像（Bild einer Doppeltür）
分配動態IP位址（Zuordnung dynamischer IP-Adressen）
資訊自決權（Recht auf informationelle Selbstbestimmung）
電信通訊秘密自由（Telekommunikationsgeheimnis）
指明原則（Zitiergebot）
目的拘束原則（Gebot der Zweckbindung）
干預門檻（Eingriffsschwelle）
干預嚴重性（Eingriffsgewicht）

裁判要旨

1. 立法者於建構查詢資料之程序時，基於其對傳輸資料及調取資料之各自權限，皆應建立本身符合比例原則之法律依據。
   關於傳輸及調取由電信服務業者提供之用戶主資料（Bestandsdaten）之規定，應充分限制利用資料之目的，故資料之利用應受到特定目的、構成要件中之干預門檻及應具備充分重要性之法益保護的限制。
2. 傳輸資料規定之立法者即負有義務，以明確規範限制可能之資料利用目的。僅於傳輸資料規定涉及全部屬於聯邦立法權限範圍之事務，且該規定包括了與其交互作用之利用資料目的規定，而其規範明確並封閉，始得一併以調取資料規定限制利用之目的。
3. 調取資料之權限不僅本身應符合比例原則，且——基於法律明確性之理由——亦應限定於傳輸規定中所限制之利用目的。此時調取資

料規定之立法者享有自由，使調取資料更應受到其他要求之限制。

4. 一般傳輸及調取用戶主資料之權限，儘管具備適當之干預嚴重性，然而為了防禦危險及為了情報機關之行為，原則上在個案中仍應存在具體危險，且為了追查刑事犯罪行為，則應存在初始懷疑（Anfangsverdacht）。

此外，分配動態網際網路通訊協定位址（Internet Protocol Address；下稱IP位址），基於其干預嚴重性已提高，則應有助於保障或維護具特別重要性之法益。再者，關於作成決定之依據，尚應有可理解及可審查之紀錄。

在危險防禦及情報機關行為的領域中，只要在涉及法益保護、防範至少為具重要性之刑事犯罪行為（一般性查詢用戶主資料）或具特別重要性之刑事犯罪行為（分配動態IP位址）之範圍內，存在具體化之危險，即足以作為干預之門檻。

案由

I. 第一案（1 BvR 1873/13）

N女士及B博士委託訴訟代理人，對於下列法律規定提起憲法訴願：電信法（Telekommunikationsgesetz）第113條，聯邦警察法（Bundespolizeigesetz）第22a條，聯邦憲法保護法（Bundesverfassungsschutzgesetz）第8d條，及2013年6月20日修正公布之聯邦軍事反情報局法（MAD-Gesetz）第4b條，2013年6月20日修正公布，並於2015年12月3日再次修正公布之海關緝私局法（Zollfahnungsdienstgesetz）第7條第5項至第9項，及第15條第2項至第6項，2013年6月20日修正公布，並於2016年12月23日再次修正之聯邦情報局法（BND-Gesetz）現行第4條，2017年6月1日修正公布之聯邦刑事局法（Bundeskriminalamtgesetz）第10條及第40條。

II. 第二案（1 BvR 2618/13）

S先生及其餘5827名聲請人委託訴訟代理人，對於下列法律規定提起憲法訴願：電信法第113條，聯邦刑事局法第7條第3項至第7項、第20b條第3項至第7項與第22條第2項至第4項，聯邦警察法第22a條，海關緝私局法第7條第5項至第9項與第15條第2項至第6項，聯邦憲

法保護法第8d條，聯邦情報局法第2b條，及2013年6月20日修正公布之聯邦軍事反情報局法第4b條。

裁判主文

聯邦憲法法院第一庭於2020年5月27日裁定：

1. a）電信法第113條，

   b）聯邦警察法第22a條第1項第1句於未涉及第21條第2項第2款之部分及同條第2項，

   c）海關緝私局法第7條第5項第1句與第6項，第15條第2項第1句與第3項，

   d）聯邦憲法保護法第8d條第1項第1句及第2項第1句，

   e）聯邦情報局法第2b條第1句及第4b條第1句，於涉及聯邦憲法保護法第8d條第1項第1句及第2項第1句之部分，以上規定皆係於2013年6月20修正公布，

   f）2016年12月23日修正公布之聯邦情報局法第4條第1句，於涉及聯邦憲法保護法第8d條第1項第1句及第2項第1句之部分，及

   g）2017年6月1日修正公布之聯邦刑事局法第10條第1項第1句與第2項與第40條第1項第1句，於未涉及第39條第2項第2款之部分，及同條第2項，依裁定理由意旨，與基本法第2條第1項結合第1條第1項及第10條第1項之規定不符。

2. 上開經宣告與基本法不符之規定，於修法前依裁定理由意旨繼續適用，最長至2021年12月31日止。
3. 憲法訴願其餘部分駁回。
4. 德意志聯邦共和國應償還聲請人因憲法訴願程序支付之必要費用。

理　由

A. 事實

本件係針對電信法第113條及其他聯邦各專業法律中關於人工查詢用戶主資料規定所提起之憲法訴願。系爭電信法第113條允許電信服務業者得於所謂人工查詢資料程序中傳輸用戶主資料，其他系爭聯邦各專業法律，則規範不同之聯邦國家安全主管機關得調取該資料。

所有修正後之系爭規定係為落實聯邦憲法法院2012年1月24日裁定之意旨（BVerfGE 130, 151 = NJW 2012, 1419 - Bestandsdatenauskunft I，查詢用戶主資料案I裁定），該裁定宣告2004年6月22日之電信法第113條（下稱修正前電信法第113條）部分規定為違憲，並指摘各專業法律中調取資料規定之違失。

查詢用戶主資料之基礎為電信法第111條，該條規定課予以營利方式提供電信服務之業者一定義務，應蒐集並儲存由其所分配或備置之固網連線用戶的電話號碼，固網連線識別碼，行動終端設備電話號碼與相關個人資料，以及契約起始日及——如已知——契約終止日。此外，凡蒐集之所有電子郵件信箱之識別碼及客戶資料，亦應予儲存。行政機關為獲得此等用戶主資料，請求查詢資料的方式，分為電信法第112條之自動查詢資料程序及第113條之人工查詢資料程序。第112條規定凡提供公共電信服務之業者應確保聯邦電力、瓦斯、電信通訊、郵務及鐵路運輸網路署（簡稱聯邦民生網路署）得隨時調取依電信法第111條儲存之資料，第113條則規定人工查詢資料程序，該程序直接基於同條第3項列舉之行政機關提出之請求而開始，負有回覆查詢之義務者為所有以營利方式提供電信通訊服務或參與提供電信服務之業者。於自動查詢資料程序中，僅得查詢依電信法第111條應予儲存之用戶主資料，然於人工查詢程序中，亦得查詢由電信服務業者依電信法第95條基於營業目的儲存、但非依法負有儲存義務之資料。電信服務業者於其依契約關係範圍內蒐集及利用之用戶主資料即屬之，一般例如契約相對人之姓名地址、約定之電信服務類型、交由使用者使用之設備及固網連線識別碼，同時亦包括與帳號相關之資料，如帳單寄送地址、銀行帳戶、直接付款授權及特別費率要件。

2013年6月20日修正公布，同年7月1日生效之電信法第113條規定如下：

電信法第113條（人工查詢資料程序）

（第1項）[1]以營利方式提供電信服務或參與提供電信服務之業者，為履行其對於第3項所列行政機關之查詢回覆義務，得依第2項規定利用其依第95條及第111條蒐集之資料。[2]對於用以保護造訪終端設備，或設置於終端設備或與其空間上分離之儲

存裝置中之資料，亦適用之。[3]依據於特定時點分配之IP位址而可確定之資料，亦得為列入查詢之資料；為此亦得自動化利用通訊紀錄。[4]提供第3句所稱列入查詢之資料，應審酌企業內部整體資料來源。

（第2項）[1]第3項所稱之行政機關應就個案以書面提出資料查詢之請求，且僅為追查刑事犯罪行為或違反秩序行為，為防禦公共安全或秩序之危險，或指明允許其取得第1項所列相關資料之法律規定時，始得提出資料查詢之請求；第1項之資料不得傳輸至其他公家或非公家之機關。[2]如有立即危險而以其他方式提出請求者，亦得提供查詢之資料。[3]於此情形，應立即以書面嗣後確認該提出之請求。[4]對於請求資料查詢之合法性，由第3項所稱之行政機關負其責任。

（第3項）第1項所稱之行政機關，包括：

1. 主管追查刑事犯罪行為或違反秩序行為之行政機關；
2. 主管防禦公共安全或秩序之危險之行政機關；
3. 聯邦與邦之憲法保護機關、聯邦軍事反情報局及聯邦情報局。

（第4項）[1]以營利方式提供電信服務或參與提供電信服務之業者，應立即並完整傳輸經請求查詢之資料。[2]關於提供資料之請求及為資料之提供，義務人對於資料之當事人及第三人應予保密。

（第5項）[1]以營利方式提供電信服務或參與提供電信服務之業者，對於提供資料所採取之必要預防措施，應於其責任範圍內自行負擔費用。[2]如其客戶逾十萬人者，對於接收查詢資料之請求及相關資料之提供，應依第110條第3項所稱之技術指引（TR TKÜV）提供安全之電子介面，防止未經授權者知悉相關資料，以保障資料之安全傳輸。[3]此時應確保所有查詢資料之請求由專責之專業人員檢查是否符合第2項規定之形式要件，且須檢查之結果為符合者，始得為後續之處理。

於電信法第113條人工查詢資料程序中得查詢之資料，除依同法第111條規定應予儲存之用戶主資料外，亦包括電信服務業者依同法

第95條規定基於營利目的，不負有儲存義務卻予以儲存之資料。至於其他系爭聯邦法律規定，使聯邦國家安全主管機關為履行其各自任務，得向電信服務業者請求查詢其依電信法第95條及第111條規定蒐集之資料。電信法中規定人工查詢用戶主資料之契機，為聯邦憲法法院2012年1月24日之裁定（BVerfGE 130, 151 - Bestandsdatenauskunft I，查詢用戶主資料案I裁定）。依該裁定之見解，須區分向有權查詢資料之行政機關為資料之傳輸，及由請求查詢資料之行政機關為資料之調取。資料交換係透過請求查詢及傳輸資料彼此互相配合的干預而進行，且皆應各自有其法律依據。以圖像而言，立法者不僅應開放傳輸資料之門，亦應開放調取資料之門。只有二者之法律依據如同雙門扉（Doppeltür）般彼此交互作用，始得進行與個人有關資料之交換（BVerfGE 130, 151 <184>）。因此，對於聯邦法律規定之事務，亦需要相當的調取資料規定，該規定超越了單純的蒐集資料權限，並建立電信服務業者獨立之查詢回覆義務（參見BVerfGE 130, 151 <202>）。

基於雙門扉圖像，電信法第113條扮演了雙門扉中第一扇必要門扉。修正前本條僅明文為開放條款規定，使電信服務業者僅有在依各專業法律調取資料規定提出之請求存在時，始有權並負有義務為資料之傳輸。對應地，現行電信法第113條第2項第1句即規定，調取資料之行政機關調取資料時，需要相當之法律依據（參見BTDrucks 17/12034, S. 12）。聯邦憲法法院於先前裁定要求獲取登入資料，亦應僅於其利用之要件存在時始得為之，並未規定於電信法第113條，而是規定於各專業法律中不同之調取資料規定。而電信法第113條第1項第3句則僅對於查詢依據動態IP位址而確定之用戶主資料，建立了法律依據。

至於聯邦各專業法律中首次出現之調取資料規定，應係建立了資料交換所必要之第二扇門扉。相關規定授權不同有權查詢資料之聯邦行政機關，得調取依電信法第95條及第111條蒐集之資料，並創設電信服務業者獨立之查詢回覆義務（參見BTDrucks 17/12034, S. 13）。至於調取登入資料及可辨識之IP位址分配，則有通知義務之規定，而對於調取登入資料，尚有法官保留之規定（參見BTDrucks

17/12879, S. 4 ff., 11）。

本件聲請人為固網及行動終端設備之連線用戶，使用不同電信服務業者提供之網際網路登入服務，其主張上開系爭規定侵害其基本法第10條第1項及第2條第1項結合第1條第1項保障之基本權。

本件憲法訴願於合法之部分，大部分為有理由。

B. 憲法訴願程序合法性之審查

[63] 本件憲法訴願大部分為合法。

I. 憲法訴願之標的

[64] 聲請人於其提起之法規憲法訴願中，訴請審查人工查詢資料程序傳輸及調取用戶主資料之規定，其主張係直接針對授權電信服務業者一般性傳輸用戶主資料（電信法第113條第1項第1句），傳輸登入資料（電信法第113條第1項第1句及第2句），及傳輸依據動態IP位址而確定之用戶主資料（電信法第113條第1項第1句及第3句）等個別權限規定。此外，聲請人亦訴請審查授權不同國家安全主管機關對應之調取上開資料的個別權限規定。聲請人之主張間接擴及於系爭規定中之其他規定，乃立法者為確保合比例性而附加之權限規定，且如無此附加規定即無法判斷系爭規定之合憲性。

[65] 因此本件憲法訴願之標的，即為2013年6月20日修正公布之電信法第113條，聯邦刑事局法第7條第3項至第7項、第20b條第3項至第7項、第22條第2項至第4項，聯邦警察法第22a條，海關緝私局法第7條第5項至第9項、第15條第2項至第6項，聯邦憲法保護法第8d條，聯邦情報局法第2b條，聯邦軍事反情報局法第4b條，2017年6月1日修正公布之聯邦刑事局法第10條及第40條，2016年12月23日修正公布之聯邦情報局法第4條，及2015年12月3日修正公布之海關緝私局法第7條第7項、第15條第4項。

II. 憲法訴願部分不合法

[66] 憲法訴願部分為不合法，第一案聲請人以嗣後提出之書面聲請，擴張審查標的及於2016年12月23日修正公布之聯邦情報局法第4條，2015年12月3日修正公布之海關緝私局法第7條第7項及第15條第4項的部分，其憲法訴願已逾期。雖然其已在法定期間內訴請審查上開個別規定之修正前規定，但憲法訴願無法自動地及於取代相關

修正條文之新規定；即使修正規定之內容與修正前規定相同——如聯邦情報局法第4條——，憲法訴願仍為不合法（參見BVerfGE 87, 181 <194>）。

[67]雖然提起憲法訴願之法定期間，不會因條文僅為文字修正而非內容修正而重新起算——如本案情形——（參見BVerfGE 12, 139 <141>；BVerfGK 18, 328 <335>；亦參見Peters, in: Barczak, BVerfGG, 2018, § 93 Rn. 141），聲請人並非不得聲請轉換其憲法訴願之標的為修正後之新規定（參見BVerfGE 87, 181 <194>）。如聲請人已針對修正前之法律規定提起憲法訴願而聲請轉換標的，其轉換之聲請須遵守一年法定期間。然聯邦情報局法第4條已於2016年12月31日生效，海關緝私局法第7條第7項及第15條第4項已於2016年1月1日生效，聲請人於2019年4月1日始聲請擴張審查標的及於上開修正後規定，已逾聯邦憲法法院法第93條第3項規定之一年法定期間（關於聯邦憲法法院法第78條第2句規定擴張審查標的，另參見下述[267]）。

[68]第二案聲請人對於2013年6月20日修正公布之聯邦刑事局法第7條第3項至第7項、第20b條第3項至第7項及第22條第2項至第4項提起之憲法訴願，欠缺權利保護利益，因上開規定已於2018年5月25日失效（參見BVerfGE 100, 271 <281 f.>；108, 370 <383>）。此時權利保護利益亦無法例外地繼續存在，否則即不具備審查憲法上原則重要性問題的意義（參見BVerfGE 81, 138 <140>；100, 271 <281 f.>；固定實務見解）。至於聯邦刑事局法第10條及第40條修正前規定出現的問題，於第一案聲請人聲請審查修正後新規定仍同樣存在，此部分亦將予以審查。

III. 憲法訴願其餘部分合法

[69]憲法訴願其餘部分為合法。

[70]1. 聲請人具備提起憲法訴願之訴權。

[71]a）聲請人使用手機通訊卡、固定連線及登入網際網路之服務，並主張透過依本案系爭規定，傳輸及調取依電信法第95條及第111條儲存之資料，將侵害其依基本法第2條第1項結合第1條第1項保障之資料自決權及第10條第1項維護電信通訊秘密之基本權。無論如何，應認為有可能產生基本權之侵害。

[72]b）系爭規定直接並現時涉及聲請人之自身權利，其憲法訴願滿足直接對於法律提起憲法訴願之特別要求。

[73]aa）聲請人之權利直接因系爭規定而受影響。儘管本案關於傳輸及調取用戶主資料之系爭規定，僅基於後續執行行為以請求及提供查詢資料之形式，始發生影響力，然而如聲請人無法知悉相關措施，或雖規定應為嗣後之通知，但基於廣泛的例外規定，長遠看來可能無須為通知，致使聲請人無法採取法律救濟者，則針對需要執行之法律規定，亦可認為係直接影響基本權之情形（BVerfGE 150, 309 <324 Rn. 35>；固定實務見解）。本案即為此情形。

[74] 聲請人本身並未明確知悉向電信服務業者所提出之查詢資料請求及所提供之查詢資料（亦參見BVerfGE 133, 277 <312 Rn. 84>；150, 309 <324 f. Rn. 36>）。關於請求登入資料之規定及調取依據動態IP位址而確定之資料的調取規定，於所規範的通知義務範圍內，即出現此情形，因為相關規定包括廣泛的例外情形，且可能很晚始應予適用（參見BVerfGE 120, 378 <394>；141, 220 <261 Rn. 82>）。而調取一般性用戶主資料，則自始無須踐行通知義務。

[75]bb）聲請人之自身權利亦現時因系爭規定而受影響。因其始終未明確知悉採取之執行行為，如其已釋明相關措施可能影響其權利，即為已足。對此重要的是，依電信法第113條及其他調取資料規定而得進行之資料查詢，可能涵蓋廣大的輻射範圍，且可能意外地擴及第三人。聲請人須自行指稱自己有刑事犯罪行為之陳述，因涉及自身利益而無必要，亦無必要說明其對於危害安全或與情報事務有關之行動負有責任（BVerfGE 130, 151 <176 f.>）。

[76]2. 本件憲法訴願符合補充性之要求。

[77]a）於提起法規憲法訴願之前，基於補充性原則，主張基本權受侵害原則上亦須窮盡所有救濟途徑。提起確認訴訟或不作為訴訟，即屬於可能之救濟途徑，使專業法院得審查一般法律中對於裁判具有重要性之事實問題或法律問題（參見BVerfGE 150, 309 <326 ff. Rn. 41 ff.>；固定實務見解）。但如僅涉及直接基於憲法而得出法規解釋之界限時，則有不同。如對於法規判斷本身即特別引發憲法上應由聯邦憲法法院回答之問題，而無法期待由專業法院先行審查以

提出改善之裁判基礎者，即毋庸由專業法院先行審查（參見BVerfGE 123, 148 <172 f.>；143, 246 <322 Rn. 211>；固定實務見解）。就此而言，尚未訴請專業法院審查，而直接針對法律提起憲法訴願，仍為合法（BVerfGE 150, 309 <326 f. Rn. 44>）。課予訴請專業法院審查之義務，亦不具可期待性（參見BVerfGE 150, 309 <327 f. Rn. 45>）。

[78]b）是以，聲請人於提起憲法訴願前，對於系爭規定無須尋求專業法院之權利保護。僅針對法律提起之憲法訴願，本質上本身即特別引發憲法上應由聯邦憲法法院回答之問題，無法期待專業法院先行審查而提出實質改善之裁判基礎。憲法上之判斷與專業法院對於系爭傳輸及調取用戶主資料之個別構成要件要素的解釋無關，而主要係與充分之法律限制及法律明確性有關。

[79-81]3. 本件針對2013年6月20日修正公布之電信法第113條及各專業法律調取資料規定提起之憲法訴願，未逾法定期間。第一案聲請人對於其提起之憲法訴願，聲請變更標的為2017年6月1日修正公布，2018年5月25日生效之聯邦刑事局法第10條及第40條，未逾一年法定期間。

[82]4. 本件對於2013年6月20日修正公布之系爭規定提起之憲法訴願，並未因2016年1月1日海關緝私局法第7條第7項與第15條第4項之些微修正，及2016月12月31日聯邦情報局第2b條修正為第4條，而喪失權利保護利益。法律規定之內容並未修正，因此本件憲法訴願於此範圍內並未喪失其標的。（亦參見BVerfGE 108, 370 <383>）。

IV. 歐洲聯盟法觀點下憲法訴願之合法性

[83] 系爭規定部分與歐洲聯盟（下稱歐盟）指令（Richtlinie）及規章（Verordnung）中個人資料保護之規定有關，然因皆未涉及強制之歐盟法規定之轉換，故聯邦憲法法院對於系爭規定之審查仍具有審判權，本件憲法訴願為合法。

[84]1. 聯邦憲法法院原則上對於歐盟專業法律無審查權限，只要歐盟基本權普遍提供了有效之基本權保障，且與基本法無條件提供之個別基本權保障本質上同樣應予遵守者，特別是普遍保障之基本權本質，則聯邦憲法法院審查基本權保障時，即非依基本法基本權保障之標準；就此部分，重要的是與基本法個別基本權有關之普

遍考量（參見 BVerfGE 73, 339 <387>；102, 147 <162 f.>；125, 260 <306>；BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 47 a.E.——被遺忘權裁定II）。依聯邦憲法法院至今之實務見解，此等原則亦適用於審查轉換歐盟強制規定為德國法之內國法（參見 BVerfGE 118, 79 <95 ff.>；BVerfG, Beschluss des Zweiten Senats vom 11. März 2020, - 2 BvL 5/17 -, Rn. 65）。針對歐盟專業法律強制規定提起之憲法訴願，原則上為不合法（參見 BVerfGE 118, 79 <95>；121, 1 <15>；125, 260 <306>；反之，關於聯邦憲法法院依歐盟基本權之標準審查歐盟強制法律規定之*適用*及審查轉換歐盟強制法律規定之內國法規定之*適用*，參見 BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 52；聯邦憲法法院依歐盟基本權標準為*法規審查*之可能性目前尚無定論，BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 276/17 -, Rn. 51 a.E.；Beschluss des Zweiten Senats vom 13. Februar 2020 - 2 BvR 739/17 -, Rn. 116 - Einheitliches Patentgericht）。

[85-86]2. 系爭規定並未涉及轉換歐盟法之強制規定，故得依基本法之標準為審查。

[87] 故如非涉及完全由歐盟法決定之權利——如本案情形——，而是涉及在未完全統一之範圍內的內國法規定，聯邦憲法法院則依基本法基本權之標準審查系爭規定。原則上，無論系爭規定依歐洲法院見解是否同時得視為基本權憲章第 51 條第 1 項第 1 句所稱歐盟法之執行規定（就此參見 RL 2002/58/EG EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 78 ff.；Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 29 ff.），及是否因此得主張適用歐盟基本權（就此參見 BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 39——被遺忘權裁定I，詳見下述[261]），皆為如此。

[88]3. 至於是否可直接由歐盟次要法得出其他法律要求，特別是 2002/58/EG 指令第 15 條第 1 項關於對電信服務業者課予之義務範圍，則在所不問。歐盟專業法律之解釋及適用，並非聯邦憲法法院

之權限，而是各專業法院結合歐洲法院之責任（參見BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 85之詳細說明——聯邦情報局——境外偵查）。

C. 憲法訴願實體有無理由之審查

[89]本件憲法訴願大部分為有理由，且系爭規定大部分不符合比例原則之要求。

I. 基本權之干預

[90]傳輸及調取用戶主資料之規定為對於受基本法第2條第1項結合第1條第1項保障之資訊自決權之干預，而於其授權傳輸及調取依據動態IP位址而確定之用戶主資料的範圍內，則為對於受基本法第10條第1項保障較特別之電信通訊秘密自由之干預。

[91]1. 電信法第113條第1項第1句、第2句及與其相對應之各專業法律之調取資料規定（聯邦刑事局法第10條第1項第1句及第2句、第40條第1項第1句及第2句；聯邦警察法第22a條第1項第1句及第2句；海關緝私局法第7條第5項第1句及第2句、第15條第2項第1句及第2句；聯邦憲法保護法第8d條第1項第1句及第2句；聯邦情報局法第2b條第1句及聯邦軍事反情報局法第4b條第1句，於涉及聯邦憲法保護法第8d條第1項第1句及第2句之部分），干預人民之資訊自決權。

[92]a）資訊自決權應考量基於與資訊相關之措施所為之現代化資料處理對於人格所生的危險及侵害（參見BVerfGE 65, 1 <42>；120, 378 <397>）。人格之自由發展，以保障個人對於其個人資料不得為無限制之蒐集、儲存、利用及移轉為前提，此由基本法第2條第1項結合第1條第1項之基本權保障之。就此而言，該基本權保障個人原則上有權決定其個人資料之揭露及利用（參見BVerfGE 113, 29 <46>之詳細說明）。當與個人有關之資料，經由國家行政機關以當事人無法掌握或控制之方式為利用及連結，致人格之發展受到危害時，應特別予以保障（參見BVerfGE 118, 168 <184>）。而電信通訊提供模式之資訊，亦屬於與個人有關之資料（參見BVerfGE 130, 151 <184>；另參見EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 51）。

[93]授權國家行政機關得處理與個人有關資料之法規，通常產生不同但彼此互相關聯之干預，此時應區分資料之蒐集、儲存及利用（參見BVerfGE 100, 313 <366 f.>；120, 378 <400 f.>；125, 260 <310>；vgl. auch EGMR（GK）, S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 67；EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238, Rn. 34 ff.）。關於為履行國家任務而交換資料之規定，則尚須區分由提供查詢資料之行政機關所為之資料傳輸，及由請求查詢資料之行政機關所為之資料調取。經由查詢及傳輸所為之干預措施彼此互相配合，進行資料交換，而各干預措施應各自有其法律依據。以圖像而言，立法者不僅應開啟傳輸資料之門，亦應開啟查詢資料之門。只有二者之法律依據如同雙門扉般彼此交互作用，始得進行與個人有關資料之交換（BVerfGE 130, 151 <184>）。

[94]b）系爭規定為對於個人資訊自決權之干預。

[95]首先，電信法第113條第1項第1句及第2句，課予電信服務業者基於有權調取資料之行政機關的請求，就其依電信法第95條及第111條儲存之資料，負有提供查詢回覆之義務，建立了獨立之基本權干預態樣（參見BVerfGE 130, 151 <185>）。相關規定本身並未授權進行資料交換，——基於雙門扉之圖像——尚需要另一個調取資料之法律依據（參見BVerfGE 125, 260 <312>；130, 151 <185>；150, 244 <278 Rn. 80>；150, 309 <335 Rn. 68>）。儘管對於有權調取資料之行政機關而言，電信法第113條以其具有取得資料之權限為要件，但電信法第113條第1項第1句及第2句作為傳輸資料之法律依據，本身即具備干預之性質（參見BVerfGE 130, 151 <185>）。關於利用目的之規定及賦予傳輸資料之權限而作為利用資料規定之部分，即具有干預之特徵。至於電信法第113條係涉及由民間電信服務業者為資料之傳輸，則在所不問（參見BVerfGE 125, 260 <312>）。

[96]與此須區別之獨立干預類型，為與電信法第113條第1項第1句及第2句相對應之聯邦機關調取資料之規定，其以電信法第113條規定之構成要件為前提，而由有權調取資料之行政機關為資料之調取（參見BVerfGE 130, 151 <185>）。

[97]2. 電信法第113條第1項第3句及與其相對應之各專業法律調取資料規定（聯邦刑事局法第10條第2項、第40條第2項；聯邦警察法第22a條第2項；海關緝私局法第7條第6項、第15條第3項；聯邦憲法保護法第8d條第2項第1句；聯邦情報局法第2b條第1句及聯邦軍事反情報局法第4b條第1句，於涉及聯邦憲法保護法第8d條第2項第1句之部分），允許得分配動態IP位址，為對於基本法第10條第1項基本權之干預。

[98]a）基本法第10條第1項保障之電信通訊秘密自由，保障借助電信通訊向個別接收者無形地傳輸資料，不為公權力所知悉。本項規定不僅保障通訊之內容，受保障者亦包括通訊過程詳細細節之私密性，尤其是包括是否、何時及多久與何人或何電信通訊設備已進行或嘗試進行的電信通訊（參見BVerfGE 125, 260 <309>之詳細說明；固定實務見解）。然而基本法第10條第1項本即保障具體電信通訊過程之私密性，而非僅止於保障將電信通訊識別碼或靜態IP位址分配予固網連線用戶本身。除非正在進行電信通訊，相關識別碼僅提供抽象的資料，即何人使用何種電信通訊方式，並可透過該方式與其取得聯繫，而與特定電信通訊過程無直接關聯。就此部分而言，個別通訊過程之私密性並未受影響（參見BVerfGE 130, 151 <180 f.>）。

[99]反之，以可辨識方式分配動態IP位址，則非如此，而係屬於基本法第10條第1項之保障範圍（參見BVerfGE 130, 151 <181>；亦參見EGMR, Benedik v. Slovenia, Urteil vom 24. April 2018, Nr. 62357/14, §§ 130 ff.，依其見解，此類措施影響歐洲人權公約第8條第1項保障之私人生活應受尊重之權利）。然而此非謂分配動態IP位址即必然與特定電信通訊過程有關，而可藉此過程間接同樣地得出查詢之資料。因為就此部分而言，查訊資料本身僅涉及抽象地分配予固網連線用戶之資料。反之，基本法第10條第1項之基本權受影響者，係電信服務業者為識別動態IP位址，而於中間階段必須審視其客戶之相關連線資料，且為此目的須獲悉具體之電信通訊過程。由電信服務業者儲存之電信通訊連線資料，屬於電信通訊秘密自由之保障範圍，且不論係由電信服務業者基於契約之基礎（參見電信法第96條）而儲存者（參見BVerfGE 130, 151 <181 ff.>），或基於法定之義務（參見電信法第113a

條及第113b條）而應予以儲存者（參見BVerfGE 125, 260 <312>）。即使並未揭露連線資料本身，仍應依基本法第10條第1項，評估利用相關資料時國家所課予之義務（參見BVerfGE 130, 151 <182 f.>）。

[100]此時，除基本法第10條外，並不適用由基本法第2條第1項結合第1條第1項導出之資訊自決權，因為針對電信通訊而言，基本法第10條包含了特別保障，而應優先於一般規定適用，且透過干預電信通訊秘密獲取資料之特殊要求，即可得出該特別保障。就此部分而言，聯邦憲法法院由基本法第2條第1項結合第1條第1項發展出之標準，應可廣泛地轉而適用於基本法第10條之特別保障（參見BVerfGE 100, 313 <358 f.>；125, 260 <310>）。

[101]b）因電信法第113條第1項第3句允許分配固網連線用戶之動態IP位址，依據上述標準，本句規定即為對於受基本法第10條第1項保障之基本權的干預。查詢資料之標的雖然僅為受查詢之動態IP位址之固網連線客戶及相關用戶主資料，然電信服務業者如就此部分提供查詢之資料，則首先須取得由其儲存之通訊資料，必要時且可能涉及連線資料之其他企業內部資料來源（參見電信法第113條第1項第4句），並須運用相關資料。一旦依電信法第113條第1項第3句，得利用依資料庫儲存相關規定而儲存之通訊紀錄，即應依基本法第10條第1項為衡量，因本句規定允許對於以基本法第10條第1項構成干預之方式取得的資料，得為後續之利用（參見BVerfGE 125, 260 <312 f.>）。

[102]c）系爭各專業法律資料查詢規定，只要係授權個別有權查詢之行政機關得查詢依據動態IP位址而確定之用戶主資料，即構成對於基本法第10條第1項之獨立干預。

II. 形式合憲性

[103]系爭規定形式上合憲，特別是聯邦對於電信法第113條及對於個別專業法律之資料調取規定，享有立法權限。

[104]1. 聯邦得依基本法第73條第1項第7款關於電信通訊之立法權，基於實質關聯性而制定電信法第113條中所包括之規定。

[105]a）實質關聯性之權限，使聯邦自然而然在只有與建置電信通訊基礎設施及經由電信通訊設備而傳輸資料等有關部分，

得制定資料保護之法律規定（參見BVerfGE 125, 260 <314>；130, 151 <192>）。除資料保護規定外，亦得對應規定該保護之界限，並確定為履行公共任務而於何種情形下及基於何種目的得利用資料（BVerfGE 130, 151 <192 f.>）。因此，聯邦得授權電信服務業者，並——配合專業法律中確立之資料查詢義務——使其負有義務，為達特定、且由聯邦詳細規定之目的，於有效之資料查詢請求存在時，應將相關資料傳輸予特定行政機關（BVerfGE 130, 151 <200 f.>之詳細說明）。特別是聯邦得制定必要之規定，將資料傳輸至追查刑事犯罪行為與防禦危險之行政機關及情報機關，以滿足基本權之要求（參見BVerfGE 125, 260 <315>）。反之，涉及調取該資料之部分，即不屬此立法權限範圍。授權調取資料本身，需要獨立之立法權限規定或應由邦為之（參見BVerfGE 125, 260 <315>；130, 151 <193>）。

[106]b）電信法第113條已遵守上述界限。本條規定限於授權電信服務業者傳輸資料，並規定國家獲取資料之目的及條件；就此部分而言，其在結構上符合業經解釋為合憲之修正前規定（參見BVerfGE 130, 151 <200 ff.>）。國家獲取資料及課予民間電信服務業者義務——在聯邦對於此類規定享有專業法律立法權限之範圍內——，應由調取資料規定自行規範之。電信法第113條第4項課予電信服務業者及時並完整傳輸資料之義務，及關於提供查詢資料之保密義務，亦屬於聯邦之權限。此類規定與其他已建立之資料傳輸義務相連結，明確規定提供為履行公共任務之資料的條件。

[107]2. 聯邦基於其享有之立法權限，亦得制定系爭之調取資料規定。

[108]a）制定調取資料規定本身，取決於一般之立法權限。此不得援引基本法第73條第1項第7款規定，因為同時強制私人揭露其客戶資料之義務，不再屬於與電信通訊相關之資料保護的界限規定，而係為與調取資料不可分之要件（參見BVerfGE 130, 151 <201>）。因此必須基於為利用資料所遵循之任務而由立法者規範之個別權限規定，建構調取資料之規定（參見BVerfGE 113, 348 <368>；125, 260 <314, 346>）。除調取資料之授權外，一般之立法權限尚包括建置利用資料應遵循之其他憲法要求，例如尤其是通知當事人及保障有效權

利保護之規定（參見BVerfGE 125, 260 <346 f.>）。

[109] 至於危險防禦領域（亦涉及防範刑事犯罪行為部分），立法權限主要歸屬於各邦（參見BVerfGE 113, 348 <368 f.>；125, 260 <346>）。然而聯邦在此等領域中，仍享有部分之專屬立法權限或競合立法權限。

[110]b）關於本案系爭之調取資料規定，聯邦享有立法權限。

[111-119] 聯邦刑事局法第10條第1項及第40條，聯邦警察法第22a條，海關緝私局法第7條及第15條，聯邦憲法保護法第8d條，聯邦情報局法第2b條第1句及聯邦軍事反情報局法第4b條第1句，於涉及聯邦憲法保護法第8d條第1項第1句及第2句之部分，屬於聯邦之專屬立法權限或競合立法權限。於競合立法權限部分，則因追查刑事犯罪行為而與基本法第74條第1項第1款第4目刑事訴訟程序之競合立法權限有關。基本法第74條第1項第1款第4目所稱「訴訟程序」之權限規定，應為廣義理解，涵蓋刑事訴訟法中偵查及判斷刑事犯罪行為之法律；對於刑事犯罪行為之調查及追查應屬之，並包括調查及追查後對刑事犯罪行為進行搜索（參見BVerfGE 150, 244 <273 Rn. 67>），因此於系爭規定涉及經授權之行政機關對於刑事犯罪行為採取壓制性行動之範圍內，亦屬之。此外，基本法第74條第1項第1款第4目亦及於預防性刑事訴追（參見BVerfGE 103, 21 <30>；113, 348 <370 f.>；150, 244 <274 Rn. 68>）。

[120]3. 關於分配動態IP位址之系爭規定，符合基本法第19條第1項第2句對於干預秘密通訊自由應適用之指明原則（Zitiergebot）。2013年6月20日以包裹立法方式制定通過之修正法（BGBl I S. 1602）第9條，明確指出修正法第1條至第8條為對於基本法第10條之干預，此已符合指明原則之警示及思慮功能（Warn- und Besinnungsfunktion）（參見BVerfGE 64, 72 <79 f.>；120, 274 <343>）。受限制之基本權僅規定於修正法之單一條文，而非於授權限制基本權之個別條文中分別地明定，在憲法上為可接受的，儘管最符合指明原則之作法為於各授權規定中具體指明（參見Huber, in: von Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 19 Rn. 96；亦見Singer, DÖV 2007, S. 496 <501>；Krebs, in: von Münch/Kunig, GG, Bd. 1, 6.

Aufl. 2012, Art. 19 Rn. 14；不同見解Axer, in: Merten/Papier, HGRe, Bd. III, 2009, § 67 Rn. 31），一如聯邦憲法保護法第8d條第6項，聯邦情報局法第2b條第3句及聯邦軍事反情報局法第4b條第3句之明確作法（參見BTDrucks 17/12034, S. 15）。

[121]經由2017年6月1日修正增訂之聯邦刑事局法第10條及第40條，無須重新遵守指明原則。雖然警示及思慮功能並非僅涉及第一次限制基本權之規定，而是在每次干預要件之重要修正致產生新的基本權限制時，皆具有重要性，但是未變更而繼續適用之基本權限制規定，或——如本案情形——僅為些許變動而仍重覆基本權限制規定者，則不適用指明原則（參見BVerfGE 129, 208 <237>之詳細說明）。

III. 電信法第113條之實質合憲性

[122]電信法第113條中系爭傳輸資料之權限規定，實體上不符合基本法第2條第1項結合第1條第1項及第10條第1項之憲法上要求。

[123]1. 對於資訊自決權及電信通訊秘密自由之干預，如同所有基本權之限制，需要以追求合法之公共利益為目的且符合比例原則之法律授權（參見BVerfGE 65, 1 <44>；100, 313 <359 f.>；固定實務見解）。因此，為達到合法之目的，基本權之限制應適當、必要，且符合狹義比例原則（參見BVerfGE 141, 220 <265 Rn. 93>；固定實務見解）。基本權之限制應有法律依據，以充分限制基於特定目的而為資料之利用。此外，應以法律明確性原則衡量所有系爭權限規定，法律明確性原則係有助於人民預見干預之發生，對於行政之權限為有效之限制，並得由法院為有效之監督（BVerfGE 141, 220 <265 Rn. 94>；亦參見EuGH, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 91；EGMR（GK）, S. and Marper v. The United Kingdom, Urteil vom 4. Dezember 2008, Nr. 30562/04 u.a., § 99）。

[124]2. 系爭之資料傳輸規定有助於合法目的之達成，而為此目的亦屬適當且必要。

[125]a）相關規定使國家安全機關特別是可獲悉將電信通訊固網連線與分配動態IP位址予個別固網連線用戶之情形，並可查詢終端設備與儲存裝置之登入資料，藉此以支持國家任務之履行，而有助於追查刑事犯罪行為、防禦危險及情報機關履行任務之有效性，故原則上得

正當化干預資訊自決權及電信通訊秘密自由之合法目的（參見BVerfGE 125, 260 <316 f.>；130, 151 <187, 205>；亦參見EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 57）。

[126]b）為達上述目的，電信法第113條保障之傳輸資料權限，係屬適當。傳輸資料之權限規定創造了原本不存在的偵查可能性，鑑於電信通訊日益增加之重要性，電信通訊在許多情形下亦使犯罪行為之準備及實施有成功的可能。即使人工查詢資料程序無法確保得可靠地傳輸用戶主資料，因（潛在之）犯罪行為人及其他目標對象會利用例如公共熱點、網咖，或以假身分登入連線，或使用特別的程式掩飾分配予其之IP位址，然無論如何皆可促進目的之達成。為達此目的，不同之權限亦屬必要。且已無其他明顯之方式，可使行政機關以較不具影響性的方法，同樣有效地獲取資料。

[127]3. 資料傳輸規定僅於對個別權限之利用目的，依其干預嚴重性，自行在規範上為充分明確之限制時，始與狹義比例原則之要求相符（a）。系爭規定中關於一般性傳輸用戶主資料（b），傳輸登入資料（c），及傳輸依據動態IP位址而確定之用戶主資料（d），即使關於資料安全性之規定並無疑慮（e），皆不符狹義比例原則之要求。

[128]a）如傳輸資料規定欲達成之目的與預期達成目的所造成之干預嚴重性並非不成比例者，該規定即符合狹義比例原則（參見BVerfGE 141, 220 <267 Rn. 98>；148, 40 <57 f. Rn. 49>）。干預嚴重性主要取決於資料之類型、範圍、可想像之用途及其濫用之危險（aa）。利用資料之目的，已由傳輸資料規定之立法者自行認定為合比例，並於規範上明確限制之（bb）。此外，憲法上要求傳輸資料時資料之安全性應獲保障（cc）。

[129]aa）干預嚴重性主要取決於資料之類型、範圍、可想像之用途及其濫用之危險（參見BVerfGE 65, 1 <45 f.>）。具有重要性者為基本權之主體、人數與受影響之程度，及於何種條件下發生基本權受影響之情事，特別是是否因基本權主體而產生了該影響。重要的標準為當事人之人數及受影響之強度（參見BVerfGE 100, 313 <376>），而主要取決於資料之資訊解讀能力及利用可能性。國家干預措施之私密性，亦導致干預嚴重性之提高（參見BVerfGE 115, 320 <353>；141,

220 <265 Rn. 94>；亦參見EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970, Rn. 100）。

[130]bb）立法者如課予建立用戶主資料之義務或於主要目的外開放用戶主資料，一如本案中為履行國家任務而利用私人企業之用戶主資料，則立法者同時負有義務，基於憲法上正當性，強制地確定必要之利用目的與干預門檻，及為保障目的之拘束力而規範可能必要之法律效果（目的拘束原則，參見BVerfGE 118, 168 <187>；120, 378 <408>；125, 260 <344 f., 355>；亦參見EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238, Rn. 57 ff.；Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93）。此種確定或變更目的之基本權正當性的規範負擔，已包含於傳輸資料規定中，相關規定係課予建立用戶主資料之義務或為履行國家任務而得開放用戶主資料。此規定——即使僅為第一扇門扉——本身即應充分限制利用之目的（參見BVerfGE 125, 260 <344 f., 355>），因此資料之利用應受限於特定目的及構成要件規範之干預門檻，並應具備充分重要性之法益保護，以便整體地遵守憲法之要求。而調取資料規定——作為第二扇門扉——之立法者享有自由，得使資料之調取受限於（甚至）更高的要求。反之，不得無視該目的規定而建立資料庫，使其利用依不同國家當局之需求及政治裁量而嗣後為決定（參見BVerfGE 65, 1 <46>；100, 313 <360>；125, 260 <345>；130, 151 <187>；亦參見EuGH, Urteil vom 6. Oktober 2015, Schrems, C-362/14, EU:C:2015:650, Rn. 93 f.）。

[131]（1）首先，上述要求適用於立法者開放由其自行規定應予儲存之用戶主資料。不得抽象地認定儲存資料之要求為正當，而是只有在其有助於具充分重要性、並已具體指明之目的範圍內，始為正當（參見BVerfGE 65, 1 <46>；118, 168 <187 f.>；125, 260 <327, 345 f.>）。如未確定利用之目的，則缺乏必要之目的拘束，並產生將資料利用於非屬其原蒐集目的之風險（參見BVerfGE 120, 378 <408>）。如果建立一個依其目的設定為完全開放的資料庫，儲存資料及儲存目的間之必要關聯可能被阻斷（參見BVerfGE 125, 260 <345, 355 f.>）。而且對人民而言，範圍亦不具有可預測性。因此，利用規定對於儲存

義務之合憲性而言，為必要之要件。此並不排除——於權限劃分之範圍內——對於利用規定為特別之規範。故利用規定之合比例設計，不僅影響其建構了獨立的干預規定本身是否合憲，亦影響儲存資料本身之合憲性（參見BVerfGE 125, 260 <327 f.>）。

[132]（2）上述要求亦適用於為履行國家任務而開放私人之用戶主資料。立法者即使允許獲取資料，原則上仍不得阻止電信服務業者為履行其契約約定而儲存資料。在一個動態的業別，如電信通訊服務業，除基於國家命令而儲存之資料外，其他資料對於國家任務之履行亦可能具有重要性，而因此開放資料（參見BVerfGE 130, 151 <206 f.>）。然如為了異於原蒐集資料之目的而開放用戶主資料，則對於可獲取此資料之權限規定應設定要求，目的拘束原則即特別具有重要性。因此，如立法者規定與原儲存目的不同之資料利用，則應儘可能地精準確定——新的——利用目的（參見BVerfGE 100, 313 <360>；120, 351 <366 f.>）。

[133]（3）如法律授權得對於資料自決權或電信通訊秘密自由為干預，則法律明確性原則亦具有特殊功能，以確保充分精準地劃定相關資料利用目的之範圍（參見BVerfGE 118, 168 <187>；125, 260 <345>）。藉此方式，強化已蒐集資訊之憲法上目的拘束原則（參見BVerfGE 130, 151 <202>之詳細說明）。因此，立法者應針對特定領域，精準並規範明確地確定個別干預之原因、目的及範圍（參見 BVerfGE 65, 1 <44 ff.>；100, 313 <359 f.>；125, 260 <328>；130, 151 <202>；固定實務見解）。具體而言，規範要求主要依干預之嚴重性而有差異，且就此部分與比例原則之個別實質要求密切相關（BVerfGE 141, 220 <265 Rn. 94>援引BVerfGE 110, 33 <55>）。

[134]（4）聯邦作為傳輸資料規定之立法者，應確定為追查刑事犯罪行為、為防禦危險、或為情報機關履行任務之目的而利用資料之相當要件（參見BVerfGE 125, 260 <346>）。立法者不得將要件之具體化交由嗣後之立法者——特別是邦——為之（參見BVerfGE 125, 260 <355 f.>）。聯邦立法者必須於傳輸資料規定中即充分履行其規範之責任，並合比例地建構規定本身。基於法律明確性之考量，此不僅適用於其實際開放用戶主資料而將調取資料規定保留由邦為之，

亦包括由其自身行使調取資料規定之立法權限。此並不排除立法者於屬其權限範圍之事項，將資料之傳輸與調取合併於單一規定中（參見BVerfGE 130, 151 <184, 203>）。但是僅於開放資料涉及完全屬於聯邦權限範圍之事項，且相關傳輸資料及調取資料之規定——依法律明確性要求之標準——依其交互作用，就資料利用為封閉之目的規定時，始得於調取資料規定中限制利用資料之目的（就此參見BVerfGE 125, 260 <351 f.>）。

[135]cc）最後，憲法上要求應保障資料之安全性。就本案系爭之傳輸資料規定而言，關於資料傳輸安全性之規定即屬之。

[136]b）電信法第113條第1項第1句中關於一般性查詢用戶主資料之權限規定，並未滿足上述要求。因缺乏具限制功能之干預門檻，其規範範圍違反比例原則。

[137]aa）對於依電信法第95條及第111條蒐集之資料，同法第113條第1項作為利用之規定，授權電信服務業者得為資料之傳輸。本項規定目前在規範上顯然僅視為單純的開放條款（參見BVerfGE 130, 151 <202>），僅於電信法第113條第3項所列之行政機關基於各專業法律調取資料規定提出有特別理由之請求時，電信服務業者始負有傳輸資料之義務。就此部分而言，前提是應有允許調取具體依電信法第95條及第111條所蒐集之資料的法律規定（參見電信法第113條第2項第1句）。立法者已清楚指明，調取資料應有相對應之相當法律依據（參見BTDrucks 17/12034, S. 12），其不得僅規定簡要的資料調取權限，更應明確且封閉地就電信法第113條第3項所涉及之行政機關為規定（亦參見BVerfGE 130, 151 <202>）。

[138]bb）電信法第113條第1項第1句開放一般性查詢用戶主資料，對於資訊自決權構成一定程度、但並非非常嚴重之干預。

[139]（1）畢竟為查詢資料而取得依電信法第111條幾乎廣泛儲存保有之資料，並因此實際上得調查及獲知所有電信通訊識別碼及每一位固網連線用戶，此規定即已包含非輕微之干預。查詢資料之標的亦可為得識別個人之內容，如生日或地址（參見BVerfGE 130, 151 <188>），及依同法第95條蒐集之資料，依契約內容亦得包括如銀行帳戶、職業、或固網連線用戶之家屬或配偶之姓名（參見BVerfGE 130,

151 <206 f.>）。此外，提供所查詢資料之隱密性，亦提高了干預嚴重性。

[140]（2）儘管如此，電信法第113條第1項第1句構成之干預並非非常嚴重（亦參見EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 61）。查詢資料限於內容上受嚴格限制之資料，並未涵蓋高度個人性之資訊，亦無法得以建立人格或社會生活之特徵（參見BVerfGE 130, 151 <189 f.>；亦參見EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, § 92（未確定））。即使因蒐進資料之特定關聯性而可得出敏感資訊，但查詢該資訊內容本身仍受有限制，且尚取決於進一步調查，而調查之合法性應依其他規定判斷之（BVerfGE 130, 151 <197>）。查詢資料，並未提供電信通訊之情境及內容；行政機關只要詢問固網連線用戶，即可獲悉通訊之情境或內容。此外，無論如何皆未有應儲存依電信法第95條蒐集之資料的義務，且可能的查詢範圍，取決於個別電信服務業是否已建立超越電信法第111條範圍之用戶主資料及其超越的程度，干預嚴重性即因此而減輕。然而，實際上通常無法避免揭露上述取得重要電信通訊服務之資料。

[141]（a）目前亦不會經由個人化的分配靜態IP位址而提高干預嚴重性，因為依電信法第111條第1項第1款「固網連線識別碼」概念之解釋，——與動態IP位址不同——，靜態IP位址係可能應予儲存之資料（反對見解：Graulich, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 111 Rn. 11；Hey/Pauly/Kartheuser, ZD 2012, S. 455 <456>；Dalby, CR 2013, S. 361 <362 Fn. 14>），或為同法第95條得自願儲存之資料。相較於識別電話號碼，分配IP位址予固網連線用戶，雖然在範圍及內容上可獲得更為廣泛的資訊，因為IP位址之固網連線用戶資料，同時包括了以電子方式而固定、並在更長期間內可反覆檢視之聯繫內容資訊（參見BVerfGE 125, 260 <342>；130, 151 <198 f.>），且必要時，亦得反向地查詢已知姓名之固網連線用戶的靜態IP位址，但是依聯邦政府之說明，依現行科技技術及實務，私人使用者作為個別客戶，原則上並不會受靜態IP位址之分配。網際網路協定版6.0相較於前版有更多之位址空間，因此原則上可分配固

定IP網址予所有使用者，然即使在持續引入網際網路通訊協定第6版的期間，至今仍為分配動態IP位址。目前本即可經由歐洲境外平臺檢視靜態IP位址之分配，該分配主要仍限於機構及大型用戶（就此參見BVerfGE 130, 151 <198>）。

[142]（b）另一方面，於電信法第113條第3項所稱之行政機關為履行任務以書面就個案提出請求時，始得提供查詢之資料，干預嚴重性即因此受有限制（參見電信法第113條第2項第1句）。故傳輸資料規定明確授權僅得就個案提供與任務有關之查詢資料。即使以營利方式提供電信服務之業者，如其客戶逾十萬人，依電信法第113條第5項第2句規定，對於接收查詢之請求及對於相關查詢資料之提供，應準備安全之電子介面，此時仍保有個案之關聯性，故聲請人此部分之主張並不可採。電信法第113條第5項僅規範接收查詢資料之請求及提供查詢資料時必要之技術環境，至於提供查詢資料之實質與形式要件，則未因準備安全之電子介面義務而有變更。即使利用該介面，對於電信服務業者提出之查詢資料請求，仍應與個案相關。此於電信法第113條第5項第3句有明確規定，即使經由電子介面接收查詢資料之請求，仍須注意所有請求皆由專責之專業人員檢視是否符合同條第2項規定之形式要件，且僅於檢查之結果為符合後，始得為後續之處理。藉此以確保不至於發生自動查詢資訊的情形，而是每一個請求皆會由資料提供者進行檢視；是以，並不允許自動檢視之情形（參見BTDrucks 17/12034, S. 12），此外，本規定亦未包括得為大量查詢或簡化大量查詢之程序。建置安全之電子介面之主要目的，毋寧更在於提升資料之安全性（參見BTDrucks 17/12034, S. 12）。

[143]（c）人工查詢資料程序對於進行查詢之行政機關而言，亦帶來一定之程序負擔，此可能導致行政機關僅於有充分需求，或所需查詢之資料具一定重要性時，始為資料之查詢（關於修正前規定，參見BVerfGE 130, 151 <206>）。即使利用電子介面，——如前所述——，亦未減少該程序負擔。

[144]cc）儘管賦予傳輸資料之權限所造成之干預嚴重性為適度，然其範圍未受任何干預門檻之限制，仍違反比例原則。

[145]（1）即使電信法第113條第1項第1句規定之傳輸資料之權

限規定並未構成非常嚴重的干預，並考量其在防禦危險、追查刑事犯罪行為及情報事務之領域中對於履行國家任務之重要性，但仍需要具限制功能之特別干預門檻。即使資料之資訊解讀能力及利用可能性受到嚴格之限制，查詢資料仍不得毫無標準地一律許可（參見BVerfGE 130, 151 <205>）。查詢資料僅有個案關聯性及與目的相關，即得提供資料——如本案情形——，並不足夠。反之，仍應有具限制功能之干預門檻，以確保僅有具備事實依據之干預原因存在時，始得查詢資料。在行政機關主管之整體任務範圍內建立一個開放的資料庫，供各種不同利用用途，而無外在干預原因作為限制，則不得為之（就此參見BVerfGE 125, 260 <355 f.>）。

[146]（a）因此，就防禦危險而言，原則上在個案中必須存在警察法概括條款所稱之具體危險。此界限亦包括存在危險之可能性。同樣地，此並非自始即限制一般警察法及秩序法中所稱負警察義務之人查詢資料，只是仍非毫無界限，致使考量適度之干預嚴重性而可能為不合比例。特別是查詢資料不得成為行政權之一般手段，而是應以個案中所涉及之任務具有保護安全法制之特性為要件（參見BVerfGE 130, 151 <206>）。就追查刑事犯罪行為而言，有初始懷疑即為已足（參見BVerfGE 130, 151 <206>）。原則上必須有以事實上依據為基礎的具體危險，此不僅適用於情報機關，亦同樣適用於防禦公共安全及秩序危險之主管機關（參見BVerfGE 125, 260 <343 f.>）。如有此類相當之干預門檻，則鑑於一般性查詢用戶主資料之適度干預嚴重性，及其對於任務有效履行之特別重要性，即無須有特別提高之法益保護，以確保資料傳輸之合比例性。

[147]（b）自憲法角度言之，立法者並非對於履行任務之所有類型皆受有限制，應配合傳統安全保護法模式，為防禦具體且直接即將到來之危險或目前之危險，創設干預之構成要件。反之，立法者於特別情形下，得降低對於因果過程可預見性之要求，進一步設定界限（參見BVerfGE 141, 220 <272 Rn. 112>），然而必須始終確保在事實認定及結論上，存在具體明確之事實上依據（BVerfGE 113, 348 <386>）。受危害之法益愈重要及其因個別行為受影響之情形愈深遠，則對於推論即將發生損害之可能性程度的要求即愈低，且必要

時，對於推論法益受危害之事實的充分要求即愈低（參見BVerfGE 100, 313 <392>；亦參見BVerfGE 110, 33 <55, 60>）。反之，受危害之法益的重要性較低時，則對於預測確定性之要求及考量危害程度及其強度之要求則愈高（參見BVerfGE 113, 348 <386>）。

[148]是以，於干預之依據中，通常至少應有充分具體之危險存在。如已有特定事實顯現個案中存在急迫之危險，而尚無法以具有充分可能性預測導致損害發生之因果過程時，仍可認定有具體危險之存在。為此，一方面必須依事實之性質，至少可以推論出具體且時間上可預見之事件發生，另一方面，於有特定人參與之情形下，限於至少為已知其身分，而得以對其採行監控措施，且主要限於對該特定人為之（參見BVerfGE 141, 220 <272 Rn. 112>援引BVerfGE 120, 274 <328 f.> und 125, 260 <330 f.>）。基於比例原則，此等干預嚴重性之降低，係與對於具體受保護法益之要求提高密不可分（參見BVerfGE 141, 220 <272 Rn. 112>）。

[149]為保護具重要性之法益，例如為防範恐怖份子之刑事犯罪行為，即使依其性質尚無法認定有具體且時間上可預見之事件發生，然而至少依個人之個別行為，可確定其於可預見之未來有從事此種刑事犯罪行為之具體可能性時，即得進一步降低對於事件發生過程可預見性之要求，而得為干預（參見BVerfGE 141, 220 <272 f. Rn. 112, 291 Rn. 164>）。然而始終應予審酌者，為具體措施之干預嚴重性。一方面，對於嚴重干預私人領域之措施，就干預門檻之降低，設立明確的限制，另一方面對於較不嚴重之干預，則有更廣泛之形成可能性（參見BVerfGE 141, 220 <269 Rn. 104>）。

[150]因此，較不嚴重之干預，——如同其對於一般性查詢用戶主資料而言——，若係有助於保護至少具有相當重要性之法益，則於存在具體危險之情形下，即為正當（就此參見BVerfGE 150, 244 <284 Rn. 99>；150, 309 <336 Rn. 73>），例如防範至少為具重要性之刑事犯罪行為（Straftat von erheblicher Bedeutung）（就此參見BVerfGE 141, 220 <270 Rn. 107>之詳細說明）[1]，即屬之。反之，如干預嚴重

[1] 譯註：德國刑事訴訟法以列舉方式規定重大犯罪行為（schwere Straftat）及特

性遠不及具體危險，或涉及嚴重干預私人領域之權限行使，始應有高位階、極為重要或特別重要之法益（參見BVerfGE 115, 320 <346>；120, 274 <328>；141, 220 <270 Rn. 108>）。

[151]（c）此等憲法上之要求，原則上適用於所有以預防為目的之干預授權規定，且亦適用於情報機關之利用資訊行為（參見BVerfGE 125, 260 <331>），是以其行為亦應有充分具體之危險作為干預之基礎（參見上述[148]以下），以滿足憲法上之要求。且就此部分，仍應有事實依據（參見BVerfGE 120, 274 <330>）。至於針對未嚴重干預私人領域，且整體而言較不具有嚴重性之干預行為——如本案情形——，為於個案中對特定、應受情報機關監控之行動或團體為調查，而有必要為資料之查詢，即為已足（就此參見BVerfGE 130, 151 <206>），因為至少以依其性質為具體且可預見之事件發生為要件。鑑於情報機關之任務範圍，自始即具備有助於保護特別重要法益之特性（參見BVerfGE 141, 220 <339 Rn. 320>；亦參見BVerfGE 133, 277 <326 Rn. 118>），對於法益保護即無須有進一步之要求。

[152]（d）另一方面，於追查刑事犯罪行為領域中，在事實面向上低於初始懷疑之干預門檻，就認定對於基本權具有重要性之干預而言，並不足夠。雖然對於設定以預防為目標之措施而言，得以降低因果過程可預測性之要求，以擴展特定領域之範圍（參見上述[147]），但要件始終是以與事實相關為基礎，即使是危險防禦法制中承認「具體危險」及「急迫危險」為干預門檻，在時間面向上已提前至前置階段，仍是以有事實上依據可認定將發生具體危險為要件（參見BVerfGE 141, 220 <272 Rn. 112>）。對於追查刑事犯罪行為之措施而言，亦同。即使於前置階段，亦僅於有事實依據時，始得考慮採取措施（參見BVerfGE 113, 348 <386>；117, 244 <263>）。反之，僅有模

別重大犯罪行為（besonders schwere Straftat），然而具重要性之刑事犯罪行為（Straftat von erheblicher Bedeutung）則非刑事訴訟法規定之犯罪行為類型，而是學說及實務發展之概念。依聯邦憲法法院之見解，具重要性之刑事犯罪行為係指至少屬於中等程度之犯罪行為，且明顯干擾法律和平，並足以嚴重侵害人民對於法律安定之感情；參見BVerfGE 103, 21 <34>；107, 299 <322>；109, 279 <344>。

糊之線索或猜測，則並不足夠（參見BVerfGE 115, 166 <197 f.>；124, 43 <66 f.>）。

[153] 因此，於追查刑事犯罪行為領域，如在事實面向上已偏移至低於初始懷疑之干預門檻，並不足夠。成立初始懷疑，僅須以對於刑事犯罪行為有充足之事實上依據為要件（參見BGH, Beschluss vom 12. Januar 2005 - 5 StR 191/04 -, Rn. 7）。此類事實上依據，對於部分干預措施而言，依其資訊解讀能力，仍低於部分調查措施所要求之「特定事實」，此即何以初始懷疑已為刑事訴訟法規定在事實要件上之最低懷疑程度（參見BVerfGE 109, 279 <350>；129, 208 <268>）。如果再繼續降低要件，就只需要模糊的依據了。

[154]（2）電信法第113條第1項第1句並未滿足上述憲法上要求。傳輸資料規定非常廣泛地開放了人工查詢資料程序，允許一般性地以防禦危險、追查刑事犯罪或違反秩序行為、情報機關履行任務為目的，而查詢資料（電信法第113條第2項第1句），且未包括任何進一步具限制範圍功能之干預門檻（參見BVerfGE 130, 151 <205>）。換言之，本句規定允許為履行任務，即可提供查詢之資料。

[155]（a）儘管單就相關資料而言，資訊內容有限，其利用可能性狹隘，並對於有權查詢之行政機關有效履行任務具有相當重要性，但利用資料之目的卻未充分受有限制。雖然法律規定之利用目的涉及維護安全之核心任務，然考量電子通訊方式逐漸具有重要性，及人民於所有生活領域中現行之通訊行為，行政機關即亦特別依賴得以個別分配電信通訊識別碼。即使考量本案系爭規定僅為適當之干預嚴重性，然只要調取資料與國家履行任務有任何關聯，而可認為有個案關聯性，無須以具備事實依據之干預原因為要件，即得提供查詢之資料，則系爭規定之範圍過於寬泛，亦即開放了情境多元，且在各方面皆不受限制之利用行為。

[156]（b）必要之干預門檻，亦無法藉由解釋電信法第113條之方式——如修正前規定——而得出。

[157] 雖然修正前電信法113條規定之文句大致相同，同樣未包括具限制功能之干預門檻，但仍得由聯邦憲法法院以解釋方式查明得出干預門檻。聯邦憲法法院主要是基於構成要件中之前提要件具有限制

性作用為依據，依該要件，僅於個案中始得提出查詢資料之請求，且須為履行任務所必要者。據此，聯邦憲法法院就與危險防禦有關之規定為解釋，認為查詢資料應以「具體危險」為要件，且於情報機關之任務範圍內，至少在個案中，對於特定、應受情報機關監控之行動或團體，有必要查詢資料之情形。即使查詢資料與追查刑事犯罪及違反秩序行為有關，但基於個案必要性之要求，得出至少仍應存在初始懷疑（參見BVerfGE 130, 151 <205 f.>）。

[158] 本案系爭傳輸資料之規定則無法重新依此意義為明確解釋，無論其文義及明確可知之立法者意思，皆與之不符。與修正前條文不同的是，電信法第113條第2項第1句進一步規定同條第1項第1句允許之傳輸要件，本即未以提供查詢資料應以有權查詢機關為履行任務而有「必要」為要件，而此必要性恰為聯邦憲法法院於其關於修正前規定之裁判中，在個案關聯性之外，認為具有重要性者。聯邦憲法法院正是由個案必要性之要求，得出修正前電信法第113條中——雖然很低的——干預門檻。於此背景下，立法者目前反而僅規定利用目的本身，卻未規定具限制功能之干預門檻，且同時取消為履行任務而提供查詢資料之必要性特徵，則聯邦憲法法院於再次解釋之範圍內，即不得忽視此點。此外，此亦可能不符立法者之意思。於最初由聯邦政府提出之草案中，完全未規定提供查詢資料應限於與任務相關之限制（參見BTDrucks 17/12034, S. 5），——依對於聯邦眾議會反對意見之一般說明（參見BRDrucks 664/12 [Beschluss], S. 1 f.；BTDrucks 17/12034, S. 17）——聯邦政府認為由新的、且由聯邦憲法法院所設定之雙軌法律體系可知，電信法第113條不得再規定提供查詢資料限於與任務相關之限制，其並非涉及電信服務業者之傳輸資料權限，而是行政機關蒐集資料之權限，提供調取資料之要件——正如草案基於對聯邦憲法法院裁判（參見BVerfGE 125, 260 <344 f., 355>；130, 151 <184 f.；202 f., 207 ff.>）之誤解所為之說明——僅規定於個別專業法律中（參見BTDrucks 17/12034, S. 20）。雖然立法者最後未完全遵循聯邦政府之意見，但至少增訂限於個案始得查詢資料之限制，並規定提供查詢資料之利用目的，藉此說明其欲對於個別特別領域創設之權限規定設立了實質界限（參見BTDrucks 17/12879, S.

10），但立法者顯然並未欲設定其他進一步之限制，此亦得由同時創設之專業法律調取資料規定可知，於多數情形下，並未包括任何具限制功能之干預門檻，且特別是未以具體危險之存在為要件（就此參見下述 [206] 以下）。

[159]c）電信法第 113 條第 1 項第 2 句授權得傳輸登入資料，牴觸基本法第 2 條第 1 項結合第 1 條第 1 項之規定。

[160]aa）電信法第 113 條第 1 項第 2 句允許提供查詢之資料，係保護造訪終端設備或外加之儲存裝置之登入資料。本項規定不論其利用之要件為何，授權得提供查詢之登入資料，且規定在內容上——儘管文字變更——與 2004 年 6 月 22 日公布之電信法第 113 條第 1 項第 2 句相符，而該規定業經聯邦憲法法院以 2012 年 1 月 24 日裁定宣告牴觸基本法第 2 條第 1 項結合第 1 條第 1 項之規定（參見 BVerfGE 130, 151 <152>）。聯邦憲法法院之說理為該規定違反比例原則，因行政機關可在無明確理由，不論關於利用資料之要求，必要時因而得於更寬鬆之條件下，即得請求查詢登入資料。然蒐集登入資料應視所追求之目的，且僅於其利用之要件亦存在時，始得為之（參見 BVerfGE 130, 151 <209>）。

[161] 法規雖經宣告違憲，但並未阻止立法者再次制定內容上文句相同的規定（參見 BVerfGE 77, 84 <103 f.>），只是此時立法者不得忽視聯邦憲法法院已確認原法律規定違憲之理由。而再次為相同規定本身應有特別之理由，特別是基於憲法判斷為重要之事實上或法律上關係之重大變更，或依所根據之觀點而可得出之重大變更。如缺乏此等理由，聯邦憲法法院即無須再次說明已裁判之憲法問題（參見 BVerfGE 96, 260 <263>）。

[162]bb）本案中並未見此等理由存在。修正後電信法第 113 條第 1 項第 2 句未包括基於比例原則所必要之限制，係因立法者認為為符合聯邦憲法法院之標準，已於聯邦各專業法律新創設之調取資料規定中有限制之規定（參見 BTDrucks 17/12034, S. 13, 20）。然而此係立於對聯邦政府就開放用戶主資料之基本權規範責任之錯誤理解而生的見解，即使是為履行國家任務而開放資料，仍應考量嗣後利用資料應有規範明確之限制的要求（參見 BVerfGE 125, 260 <344 f., 355>；上

述[130]）。就此而言，聯邦憲法法院對於修正前規定——不論應由聯邦或邦規範之調取資料規定——，因其無充分之利用限制而宣告為違憲（參見BVerfGE 130, 151 <207 ff.>）。第一扇門扉之缺失，——不得如本案情形——，由「強化」第二扇門扉而予以補強（參見Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Abschnitt G Rn. 177）。

[163]d）於電信法第113條第1項第3句中新創設之權限，亦得依據動態IP位址傳輸特定之用戶主資料，不符合比例原則之要求，因此牴觸基本法第10條第1項規定。

[164]aa）電信法第113條第1項第3句以符合必要之規範明確性方式，規定依據動態IP位址而確定之用戶主資料，亦為得查詢之資料。本句亦同樣明確規定為準備查詢上述資料，亦得運用通訊紀錄。因此立法者同時對於依電信法第96條為營業目的而蒐集之通訊紀錄，單獨規範了利用規定（參見BTDrucks 17/12034, S. 12），為了準備依同法第113條第1項第3句規定資料之查詢，及從而為了履行國家任務，立法者基於目的關聯性而開放通訊紀錄（參見上述[132]）。雖然在2013年電信法第113條第1項第3句修正時，電信服務業者僅係基於同法第96條蒐集通訊紀錄，然而該權限規定無進一步限制，且一般表明得運用通訊紀錄，至少依其規範之文句，事實上亦應包括自2017年7月1日起，依電信法第113a條及第113b條，由提供者可公開造訪之電信服務業者負有義務而儲存之通訊紀錄（然關於現行儲存義務之運作，參見上述[12]）。因為利用依電信法第113條第1項第3句規定查詢之資料，已於同法第113c條第1項第3款明文規定，由上述二規定之交互作用觀之，關於電信法第113條第1項第3句法律明確性之要求，並無疑義。

[165]bb）相較於一般性查詢用戶主資料，電信法第113條第1項第3句之干預嚴重性則已提高。本句為對於基本法第10條第1項之干預，且針對受查詢之用戶主資料及為確定其內容而由電信服務業者運用之通訊紀錄，就其資料解讀能力及利用可能性而言，本句規定具有更重大之人格關聯性。

[166]（1）行政機關對於辨識動態IP位址之資料查詢請求權的成

立，基於受查詢之用戶主資料的資料解讀能力及利用可能性，具有相當重要性。立法者藉此對於網際網路之通訊條件產生影響，並限制其匿名之範圍。基於動態IP位址之分配，並與依電信法第113條第3項所為無須理由而系統性儲存之網路登入資料相結合，在很大程度上即得調查使用網路者之身分（參見BVerfGE 125, 260 <341 f.>）。此法律規定之理念，基本上不會因目前停止實施相關資料之儲存義務（就此參見上述[12]）而受影響。

[167]雖然分配動態IP位址，在某種程度上與辨識電話號碼有類似性，然而查詢電信號碼之所有者並不必然地須提供具體通訊行為之資訊，反之，查詢動態IP位址固網連線用戶之資料，則必然同時包括該IP位址在特定時點曾被使用及經由何固網連線而被使用之資訊。因網路端的內容為電子式固定的，且可在較長時間內反覆檢閱，IP位址之個別化同時提供了通訊內容之資訊。相較於辨識電話號碼，由範圍而言，及特別是得藉由查詢而知之通訊內容而言，IP位址之個別化具有更重大之人格關聯性，二者無法相提併論（參見BVerfGE 130, 151 <204>援引BVerfGE 125, 260 <341 ff.>）。

[168]（2）電信服務業者為確定受查詢之資料，亦得運用通訊紀錄，相較於單純之用戶主資料，自始即具有更高之人格關聯性，此亦進一步提高了干預嚴重性。雖然通訊紀錄只涉及連線資料，應該未包括通訊之內容，但是在廣泛蒐集及運用之情形下，原則上可由通訊紀錄建立具有資料解讀能力之人格及社會生活的特徵（參見BVerfGE 125, 260 <319>）。

[169]然而，由於請求查詢資料之行政機關於分配動態IP位址時，對於通訊紀錄一無所知，干預嚴重性即因此有所減輕。行政機關並非自行調閱通訊紀錄，而僅是獲得由電信服務業者經由通訊紀錄及必要時之其他資料（例如來源埠口號碼，參見上述[42]）而查出之與特定固網連線用戶有關的個人資料。受查詢之用戶主資料的資訊解讀能力依然有限，利用通訊紀錄僅可獲知何人為固網連線用戶，而在特定時點經由安全主管機關已知之IP位址登入網際網路之資訊（參見BVerfGE 125, 260 <341>），其有助於增進理解之價值仍為個別的。僅依據相關之查詢資料，仍無法進行一段較長期間之系統性調查，或

建立人格及社會生活之特徵（參見BVerfGE 125, 260 <341>）。

[170]（a）此首先適用於依電信法第96條蒐集之通訊紀錄。此處涉及電信服務業者根據其營業需求，於有限範圍內依電信法第96條得儲存之通訊紀錄，且個人以契約內容得部分不予儲存（參見BVerfGE 125, 260 <352>）。通訊紀錄，亦包括IP位址本身，並未完整地、亦未系統地予以儲存，而依電信服務業者、契約內容及使用服務之不同，儲存資料之實務作法亦截然不同。依專業法院之司法見解，用於檢測、限制、排除故障或錯誤所為之儲存（電信法第96條第1項第2句；第100條第1項），無須有具體理由，但至少應於網際網路連線終止後7日內為之（參見BGH, Urteil vom 13. Januar 2011 - III ZR 146/10 -, Rn. 22；Urteil vom 3. Juli 2014 - III ZR 391/13 -, Rn. 23；亦參見Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten, Stand 19. Dezember 2012, S. 4 f.），然電務業者於不同範圍內為儲存，於部分情形甚至完全未儲存。再者，網際網路連線中斷之頻率，及與儲存期間開始有關之連線終止，得依契約內容而部分協議變更，並可因使用者而受影響。

[171]（b）然而關於動態IP位址之分配，不僅得運用依電信法第96條蒐集之通訊紀錄，原則上亦得利用由可公開造訪之電信服務業者無須理由且系統性儲存10週（電信法第113b條第1項第1款）之通訊紀錄（參見BVerfGE 125, 260 <328, 352>；關於目前儲存義務之運作，參見上述[12]）。由此，原則上即伴隨著干預嚴重性之顯著提高。除了相關資料本身並非查詢之標的外，當然仍須審酌自始僅有固定的少部分資料用於分配IP位址，而其儲存得以明顯較寬鬆之要件為之。為辨識動態IP位址，僅儲存對於查詢資料有必要之網際網路登入資料，相較於幾乎完整儲存所有電信通訊資料而言，應明顯具有較低之嚴重性（參見BVerfGE 125, 260 <341>）。故本來對於利用預防性儲存之通訊紀錄所適用之重要、特別嚴格的要求，並不同樣地適用於此類資料（參見BVerfGE 125, 260 <340>）。

[172]（c）依電信法第113條第1項第4句，除依據動態IP位址提供查詢之資料外，尚應考量企業內部整體之資料來源，就此部分而言，並不會產生任何進一步提高干預嚴重性之效力。本句規定顯示

電信服務業者無法自由選擇或縮減為辨識IP位址所必要之資料（參見Graulich, in: Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl. 2015, § 113 Rn. 29；Löwnau/Ipsen, in: Scheurle/Mayen, TKG, 3. Aufl. 2018, § 113 Rn. 11），此時僅涉及一個技術上之開放說明，並非得開放利用非法儲存之分配動態IP位址的資料，——聲請人相關主張不可採——。

[173]（d）最後，電信法第113條第1項第3句亦未開啟任何特定之濫用危險。特別是本句規定並未允許於其明文規定之目的外，就通訊紀錄為其他之利用。立法者以本句規定已充分顯示，僅允許利用通訊紀錄，就行政機關已知之個別IP位址為資料之查詢（亦參見BTDrucks 17/12034, S. 10, 12）。本句規定——即使結合電信法第113條第1項第4句——，亦不包括授權行政機關開放查詢尚未知電信通訊連線資料之固網連線用戶（就此參見BVerfGE 125, 260 <357>）。因此，傳輸一固網連線用戶於特定時點所受分配之IP位址，而該用戶之其他資料（例如姓名及地址）為查詢之行政機關已知者，即不得為之（參見Graulich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 10 BKAG Rn. 20）。電信法第113條第1項第3句及第4句之文句明確顯示通訊紀錄及所有其他企業內部之資料來源，完全僅得利用於分配IP位址。亦無法由修正法第9條（BGBl I 2013 S. 1602）包含之一般性規定，即秘密通訊自由因本案系爭修正後規定而受有限制，而可得出進一步之授權，聲請人相關主張並不可採。遵守指明原則之明文規定，並不足以成立干預秘密通訊自由之權限。

[174]cc）即使考量電信法第113條第1項第3句干預嚴重性已提高，本句規定仍未符合由比例原則所導出受查詢資料之利用目的應受有充分限制之要求。

[175]（1）如為分配IP位址，非僅獲取依電信法第96條蒐集之通訊紀錄，亦可及於預防性儲存之通訊紀錄，雖然對於直接利用所有預防性儲存之通訊紀錄，在憲法上並不存在應適用之特別嚴格要件（參見BVerfGE 125, 260 <340>），但仍應透過受充分限制之利用目的，將提高之干預嚴重性列入考量。進一步限制電信法第113條第1項第3句範圍之干預門檻，及限於保障或維護具特別重要性之法益，原則上即為必要。

[176]（a）分配動態IP位址——如同調取一般用戶主資料——，需要具限制功能之干預門檻，以確保不得毫無標準地調取資料。因此，原則上應有相當之干預門檻，而以在個案相關事實基礎上之初始懷疑或具體危險為要件，後者適用於情報機關及所有主管防禦公共安全與秩序之危險的行政機關（參見BVerfGE 125, 260 <343 f.>）。

[177]（b）再者，電信法第113條第1項第3句開放調取用戶主資料，應經由與基本權干預相關之充分重要法益予以合理化，此屬於禁止過度原則之要求。雖然此時原則上無須有具限制功能之法益或刑事犯罪行為類型，然而主要基於經處理之資料的種類、範圍及利用可能性，提高了分配IP位址之干預嚴重性，因此即使為了防禦任何危險及為了追查或防範任何違反秩序行為，仍不允許普遍且無限制地分配IP位址。且考量將網際網路通訊連線分配予個別行為者，以保護法益或維護法秩序可能產生之利益日益增加，並考量網際網路對於日常生活不同領域之重要性日增，利用網際網路於犯罪行為及不同種類之權利侵害行為之危險亦因此增加，則取消網際網路之匿名性，至少需要有法益受損害，法益受損害乃法規範賦予特別之重要性。然而，並不完全排除為追查或防範違反秩序行為而查詢資料，但就此部分而言，仍必須涉及——即使於個案中——特別重大而應由立法者另外明確指明之違反秩序行為（參見BVerfGE 125, 260 <344>）。於危險防禦之領域，同樣地亦非任何受保護法益之危險即等相當於具備干預門檻（參見BVerfGE 150, 244 <286 Rn. 106>），否則，由於涵蓋危險防禦法制保護範圍之整體法規範的不可侵犯性，任何違反法規之行為皆可能成為分配IP位址之原因。

[178] 因此，個別化分配動態IP位址，為支持其正當性，在任何情形下皆應具備有助於保障或維護特別重要法益之理由，以與其干預嚴重性相當（參見BVerfGE 125, 260 <344>）。至於僅基於與特定情形相關而個別的分配網際網路通訊，並不需要進一步之特別重要性法益保護。無論如何，藉由追查刑事犯罪行為而受保障之法益，即屬於具特別重要性之法益。為追查或防範其他相當重要之違法行為，立法者亦得容許查詢用戶主資料，而分配IP位址對於打擊該違法行為具有重要性，其中得包括特別重大之違反秩序行為（就此參見BVerfGE

125, 260 <344>；150, 244 <284 Rn. 99>）。

[179]（c）然而，干預門檻及法益保護之法律規定處於一種交互關係，以致授與分配IP位址之權限，亦非全然需要存在傳統意義之具體危險。即使降低干預門檻，授與干預權限亦可滿足比例原則之要求。此時原則上存在具體危險（上述[148]以下），即為已足。依據應受保護法益之重要性，如依其類型，可認定將發生具體且時間上可預見之事件，或另一種情形為當事人之個別行為構成其於可預見未來，將從事特定刑事犯罪行為之具體可能性，即為已足（參見BVerfGE 141, 220 <272 f. Rn. 112, 291 Rn. 164 f., 305 Rn. 213>）。此不僅適用於一般之危險防禦，亦適用於情報機關之任務領域。

[180]如此種具體危險已構成得行使干預權限之事由，而干預嚴重性係依受查詢用戶主資料之種類、範圍與利用可能性及為此而運用之通訊紀錄而確定，考量因分配IP位址所提高之干預嚴重性，對於資料之查詢即應限於保護至少為特別重要之法益（就此參見BVerfGE 141, 220 <270 Rn. 108>之詳細說明）。立法者於傳輸資料之規定中，應自行具體指明具特別重要性之法益，或至少應以規範明確確定所必須之重要性。

[181]於危險防禦與防範刑事犯罪行為有關之範圍內，應涉及至少為重大犯罪行為（schwere Straftat）[2]（亦參見BVerfGE 125, 260 <328 f.>）。立法者應最終確定以開放用戶主資料所涵蓋刑事之構成要件，此時，其得運用既有之類型或建立獨立之類型，以涵蓋對於分配IP位址具有特別重要性之行為。然而將刑事犯罪行為認定為重大犯罪行為，應於刑事法規範中——例如由其刑罰範圍——尋求客觀之體現（參見BVerfGE 109, 279 <343 ff.；insbesondere 347 f.>）。反之，概括條款或僅概括提及未進一步受有限制之刑事犯罪行為，並不足夠（亦參見BVerfGE 125, 260 <329>）。

[182]另一方面，於情報機關之事務領域中，則無須有此種法益限制之明確規定，因為其行為自始即有助於保護於此意義上之特別重

[2] 譯註：德國刑事訴訟法係以列舉方式規定重大犯罪行為（schwere Straftat）及特別重大犯罪行為（besonders schwere Straftat）之態樣，若非屬法律列舉規定之情形，即非屬重大犯罪行為或特別重大犯罪行為。

要法益（參見BVerfGE 141, 220 <339 Rn. 320>；亦參見BVerfGE 133, 277 <326 Rn. 118>）。此時，以充分具體之危險作為干預門檻之要件，即確保於個案中亦存在具充分重要性之法益。

[183]（2）電信法第113條第1項第3句不符合上述要件，分配動態IP位址並未與任何具限制功能之干預門檻有關，故違反比例原則。

[184]（a）電信法第113條第2項第1句進一步規定傳輸資料之要件，亦規定分配動態IP位址之利用目的，但並未以初始懷疑或以基於事實依據之具體危險為要件。

[185]再者，就一般性之危險防禦而言，——亦基於此種相當之干預門檻——，權限行使缺乏限於具充分重要性之法益保護的必要限制。只為了防禦公共安全及秩序之危險（參見第113條第2項第1句）而開放分配IP位址，而未依相關受保護法益之重要性進行權衡，整體上涉及法秩序之不可侵犯性（參見BVerfGE 150, 244 <286 Rn. 106>），缺乏限於為防禦具特別重要性法益之危險的限制。

[186]上述與追查刑事犯罪行為有關之說明，針對電信法第113條第2項第1句允許為追查任何違反秩序行為而提供查詢資料之部分，亦有其適用，其並未限於特別重要之違反秩序行為。即使違反秩序罰法（OWiG）第46條第3項第1句，亦未符合必要之明確規範的要求。如相關措施可能涉及電信通訊秘密，且為追查違反秩序行為，在事實層面上得以相關措施排除分配IP位址之危險，本句規定仍以罰鍰程序一般——甚至廣泛地——禁止追查違反秩序行為。當資料之傳輸及調取涉及專屬於聯邦享有立法權之事務時（上述[110]以下），一如本案情形，即使不同規定中——整體而言為合憲——得完全就資料利用為封閉的規範（參見BVerfGE 125, 260 <351 f.>），然前提為相關規定以其交互作用，可充分精準且規範明確地限制利用資料之目的，以確保資料交換整體上符合基本權之要求。但是，違反秩序罰法第46條第3項第1句及本案系爭之傳輸資料規定——甚至彼此未相互提及——，對於資料之利用而言，為彼此無法調和之衝突規定。

[187]（b）電信法第113條第2項第1句對於分配IP位址之權限，亦未以降低之干預門檻限制之。特別是對於一般性危險防禦及對於情報機關之行為，並未以具體危險為要件。同法第113條第2項第1句

於涉及依電信法第113條第1項第3句查詢資料之部分，並未要求至少應有依其類型而具體且可預見之事件發生，或要求個人之個別行為應構成於可預見之未來將從事刑事犯罪行為之具體可能性。再者，關於一般性之危險防禦，對於此類干預門檻之降低，缺乏限於保護至少特別重要法益之必要限制，——如涉及防範刑事犯罪行為——，則缺乏限於至少防範重大犯罪行為之限制。

[188]e）反之，本案系爭之傳輸資料規定，就憲法上要求之資料安全部分，並無任何疑義。儲存資料義務及開放私人用戶主資料，為規範上不可分之要件，其與利用資料應符合有明確規範之限制的要求相同，皆為憲法上關於資料安全性之保障（關於儲存資料義務，參見BVerfGE 125, 260 <344>）。除關於儲存資料之安全性的相關規定外，關於資料傳輸之安全性的相關規定亦屬之（參見BVerfGE 125, 260 <345>）。因此，必要之預防措施，一方面涉及依非本案系爭之電信法第95條、第96條、第111條、第113a條及第113b條——本身——之資料儲存規定；就此部分，資料安全性則規定於如電信法第109條以下及第113d條。另一方面，經調取之資料的傳輸安全性，應予保障，就此部分，電信法第113條第5項第2句規定如電信服務業者之客戶逾十萬人者，其應設置安全之電子介面，本句規定由實施監控電信通訊及提供查詢資料之法定措施技術指引（TR TKÜV）B部分予以具體化。此義務不適用於小型電信服務業者，但並非意味減損了憲法上傳輸資料安全性之最低要求。就此而言，電信法第109條第1項之一般性規定無論如何皆為重要規範，要求所有電信服務業者應依現行技術標準採行資料保護之預防措施。

IV. 各專業法律中調取資料規定之實質合憲性

[189]與電信法第113條相對應之調取資料規定，於實體上，大多數不符合基本法第2條第1項結合第1條第1項及第10條第1項之憲法要求。

[190]1. 因傳輸及調取與個人有關之資料皆構成獨立之基本權干預，個別之調取資料規定，亦應視個別受影響之基本權及其干預嚴重性，符合比例原則及法律明確性原則之要求。相關憲法上之要求特別源於狹義比例原則，其要件為調取資料規定應個別以其各自充分明確

之法律依據為基礎，且該法律規定應充分限制資料之利用須限於特定目的。

[191]2. 系爭之調取資料規定，——如同就電信法第113條之說明（上述[124]以下）——，有助於達成合法之目的，且為達目的係適當且必要。

[192]特別是關於查詢登入資料，無須如聲請人主張應有補充條款之必要，亦即只有在預計蒐集之資料無法以其他方式，特別是無法經由直接使用電信服務業者查詢之資料內容而獲取時，始得查詢登入資料。對於使用登入資料以保護儲存於終端設備及經由其可造訪之外部儲存媒介中之資訊內容，為達所追求之目的，直接使用電信服務業者之資料，並非同樣適當之手段。通常電信服務業者並未持有終端設備，因此即便其知悉使用者身分模組（SIM）卡之個人識別碼（PIN）或個人解除鎖定碼（PUK），且終端設備並未另外以個人登入安全密碼而受保護時，電信服務業者本身仍無法取得儲存於終端設備或間接可查閱之資料，如照片、通訊內容、或其他電信服務業者之電子郵件信箱。

[193]反之，以使用查詢登入資料方式而欲取得外部儲存裝置中之資訊內容，只要屬於電信法之適用範圍者，例如造訪語音信箱，或必要時造訪電子郵件信箱（但關於網頁之電子郵件服務，參見EuGH, Urteil vom 13. Juni 2019, Gmail, C-193/18, EU:C:2019:498），亦得透過直接向電信服務業者提出交付要求（搜索、保全或沒收），或對於正在進行之通訊為監控（電信通訊監察、線上搜索）之方式為之（參見BVerfGE 124, 43 <55>）。此類措施基於比例原則，通常亦限於特定期間（如刑事訴訟法第100a條、第100e條第1項第4句及第5句、第100b條、第100e條第2項第4句及第5句），或限於特定時間之內容或其他可限定之內容（關於用戶主資料之沒收，參見BVerfGE 113, 29 <55 f.>；124, 43 <68>）。就此而言，相較於以傳輸登入密碼而造訪儲存設備之方式，獲得之資料更為有限（亦參見BTDrucks 19/17741, S. 38）。當然於個案中運用調取登入資料之權限，仍應遵守必要性原則之要求，並未因此受影響，以確保不致獨立於利用登入資料之要求外，於必要時得在更寬鬆之條件下單獨查詢登入資料（就此參見

BVerfGE 130, 151 <208 f.>）。即使利用登入資料，亦得限於僅得在特定期間內為之，或僅得就可以其他方式限定之內容為之。就此部分而言，成立有限制之蒐集禁止。

[194]3. 調取資料之規定，僅於個別調取資料之權限受有充分之限制，並遵守透明性、權利保護及監督等必要之廣泛要求下，始符合狹義比例原則（a）。一般性調取用戶主資料之系爭權限規定（b），與調取登入資料之權限規定相較（c），大部分未符合上述要求。同樣關於調取依據動態IP位址而確定之用戶主資料之權限，大部分亦未充分受有限制（d）。此外，整體而言，亦不符合憲法上要求之程序法保障（e）。

[195]a）如系爭規定追求之目的與干預之嚴重性並未失衡，即與狹義比例原則之精神相符。系爭規定規範上必須充分明確，並為資料之調取建立相當之授權基礎（aa）。考量其干預嚴重性及個別遵循之目的，系爭規定應包涵充分之利用規定，並就此部分本身為合比例之規範（bb）。再者，調取資料之權限——基於法律明確性——亦應限於在傳輸資料規定中所限定之利用目的（cc）。此外，基於比例原則，所有調取資料規定皆應遵守關於透明性、個別權利保護、監督及資料利用與銷燬規定之一定程度的廣泛要求（dd）。

[196]aa）鑑於法律明確性原則對於資訊自決權及電信通訊秘密自由之干預具有特殊功能，以直接對於第三方私人提出查詢請求之形式時，調取資料即需要明確之法律依據，以單獨建立電信服務業者之查詢資料義務。必要的是在單純蒐集資料之權限外，更應有足夠充分之調取資料規定，並明確規範電信服務業者應負有向何行政機關具體為資料傳輸之義務（參見BVerfGE 130, 151 <202 f.>）。

[197]bb）與為了開放用戶主資料而發展出的標準相同，於調取資料規定部分，亦應充分限制利用資料之目的。此時，針對資料之調取，應依領域特性精準、明確地確定個別干預之原因、目的及範圍（參見BVerfGE 130, 151 <202>）。干預門檻對於調取資料亦為必要，以確保只有在具備事實依據之干預原因存在時，始得查詢資料。於行政機關整體履行任務之範圍內，進行多元且利用不受限制之資料調取，則不得為之（參見BVerfGE 125, 260 <355 f.>）。於保障相對應

重要之法益的範圍內，考量干預之嚴重性，亦得降低干預門檻（上述[147]以下）。

[198]cc）調取資料之權限本身不僅應合比例，且——基於法律明確性——亦應限於在傳輸資料規定中所限定之利用目的。即使憲法上對此並無要求，仍應適用之。

[199]（1）在應由各邦制定調取資料規定之事務中，因針對開放用戶主資料及與其相關之進一步利用資料之必要限制，邦並無立法權限，各邦即不得基於自己之決定進一步開放用戶主資料。

[200]（2）無論如何，只有邦法及聯邦法之調取資料規定，包括了傳輸資料規定限定之利用目的之範圍，始與法律明確性原則相符。惟有如此，傳輸資料規定及調取資料規定始得以其交互作用，對於資料交換之利用目的確定充分精確之界限。

[201]依據雙門扉之圖像，——個別主管之——立法者不僅應開放傳輸資料之大門，亦應開放調取該資料之大門（參見BVerfGE 130, 151 <184>）。就此而言，傳輸資料規定之立法者必須基於較嚴格之規範義務，對於確定為何種目的及以何種界限而開放第一扇門扉，作出明確且終局之決定（參見BVerfGE 125, 260 <355>）。即便是第二扇門扉之立法者，亦無法進一步開放第一扇門扉，而就此部分仍應受限於在傳輸資料規定中已規範之利用規定（亦參見Brodowski, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, S. 137）。雖然調取資料規定之立法者得自行決定有權限之行政機關調取資料時，應受限於更狹隘之目的、更嚴格的干預門檻、或為保障或維護更重要之法益（參見Bäcker, Kriminalpräventionsrecht, 2015, S.505），但基於法律明確性原則，即使立法者——如本案情形——同時為調取資料規定之立法者，如未損及在傳輸資料規定中限定之利用目的，並授權行政機關得為其他更廣泛之目的而調取資料時，仍得規定較低之干預門檻或較不重要之法益保護。雖然——於憲法容許之範圍內——，調取資料規定配合以此方式降低干預門檻之利用規定，得授權行政機關為資料之調取，但電信服務業者並未被授權或課予義務為資料之查詢（參見電信法第113條第2項第1句）。是以，此類調取資料規定包括了一個自始與傳輸資

料規定不相符之規範缺失。應交換之資料的利用目的正應透過傳輸資料規定及調取資料規定之交互作用，在規範上明確限制之，故不得給予外界一種印象，行政機關得不顧在傳輸資料規定中規範之利用規定而獲取資料，否則即可能開啟濫用且無法預測之獲取資料可能性。

[202] 傳輸資料規定與受到較少限制之調取資料規定間的衝突，亦無法透過資料交換應基於較嚴格要件之傳輸規定始得為之的方式獲得解決。電信服務業者在實體上，無法也不得檢視行政機關是否遵守該較嚴格之要件，反之此僅為有權查詢資料之行政機關的責任（參見電信法第113條第2項第4句），且僅得由行政機關為可靠之判斷。但各專業法律之調取資料規定可能授權行政機關得更廣泛地調取資料，而未保障應依傳輸資料規定之標準為機關內部之監督。就此部分而該，也可能開啟了法治國中不再受約束且無法預見之獲取資料可能性（就此參見Dieterle, ZD 2016, S. 517 <521>）。

[203]dd）此外，基於比例原則，亦得出對於透明性、個別權利保護及監督之一定程度的廣泛要求，其取決於個別之事務權限，並應於調取資料規定中確定之（參見BVerfGE 125, 260 <344 ff.>；150, 244 <285 Rn. 101>；固定實務見解），且應依規定中之干預嚴重性，詳細規定之。憲法上亦要求對於資料之利用及資料之銷燬應有可行之規定（參見BVerfGE 65, 1 <46>；150, 244 <285 Rn. 101>）。

[204]b）各專業法律中授權一般性調取用戶主資料之規定，大部分不符合上述憲法之要求，但是相關規定則符合程序法上廣泛之要求（參見下述e，[244] 以下）。

[205]aa）對於電信法第113條規定為傳輸而開放之資料而言，個別調取資料規定建立了充分特定且規範明確之特別授權依據。除了對於有權查詢之行政機關為授權外，相關規定亦規範了第三方私人之義務，從而為電信服務業者提供調取資料之義務單獨建立了特別之法律依據。所有規定皆指明個別有權查詢之行政機關，並明文規定應與「依電信法第95條及第111條蒐集之資料」及應與同法第113條有關。

[206]bb）然而就干預嚴重性而言，主要係依相關資料之種類、範圍及利用可能性決定之，系爭規定內容大部分與比例原則有違。幾乎所有規定並未以對於調取資料具限制功能之干預門檻為要件，亦未

以明確援引其他規定之方式，以包括干預之門檻。

[207]（1）聯邦刑事局法第10條第1項第1句，海關緝私局法第7條第5項第1句與第15條第2項第1句，聯邦憲法保護法第8d條第1項第1句，及聯邦情報局法第2b條第1句與聯邦軍事反情報局法第4b條第1項第1句於涉及聯邦憲法保護法第8d條第1項第1句之部分等規定，授權一般性調取用戶主資料，惟未受充分限制，故不符比例原則。

[208-218]聯邦刑事局作為中央機關，其任務主要限於履行協調任務（參見BVerfGE 110, 33 <51>），並未獲授權履行警察防禦危險及追查刑事犯罪之任務，而僅是進行協調與資訊之連繫。聯邦刑事局於其中央機關任務範圍內，支援警察機關防範及追查跨國、國際或具重要性之刑事犯罪行為（聯邦刑事局法第2條第1項）。為履行此任務，聯邦刑事局應蒐集及評估為此而必要之資訊，提出策略性及行動性之刑事警察分析報告，並維護及協調建立刑事科技調查之設備等。如對於上述任務之履行有必要者，聯邦刑事局法第10條第1項第1句授權其得查詢用戶主資料，然本句規定並未包括進一步限制其範圍之干預門檻，亦缺乏應限於個案。聯邦刑事局法第10條第1項第2句及第3句授權聯邦刑事局於保護各憲法機關與自身指揮（聯邦刑事局法第6條）及證人保護（聯邦刑事局法第7條）之事務範圍內，如其請求之資料係為履行任務所必要者，得調取資料，亦皆未以有具體之干預原因為要件。

海關緝私局法第15條第2項第1句授權海關緝私局為履行其同法第4條第2項至第4項所列之任務，得調取用戶主資料。本句規定僅與海關刑事局法針對對外貿易、跨境貨物流通及打擊國際組織洗錢為監控時，為履行任務之必要性有關，然而並未以干預原因為要件。上述對於聯邦刑事局法第10條第1項第1句第1款及海關緝私局法第15條第2項第1句之考量，大部分可適用於海關緝私局法第7條第5項第1句，只要是屬於預防性警察事務領域中之任務，皆未以具限制功能之干預門檻為要件。

聯邦憲法保護法第8d條第1項第1句，及聯邦情報局法第2b條第1句與聯邦軍事反情報局法第4b條第1句於涉及聯邦憲法保護法第8d

條第1項第1句及第2句之部分，同樣不符合狹義比例原則之要求。上開規定既未包括具限制功能之干預門檻，亦未包括應限於個案之限制，而只是著重於個別情報機關任務履行之必要性。

[219-228]（2）聯邦刑事局法第40條第1項第1句授權聯邦刑事局得一般性調取用戶主資料，於其依同法第39條第1項及第2項偵查事實或調查人民居住地之規定而有必要之範圍內，僅部分符合比例原則之要求。

聯邦刑事局法第40條第1項第1句，於涉及同法第39條第1項之範圍內，不符合狹義比例原則，皆未以具限制功能之干涉界限為要件，或應僅限於個案相關性，反而是如一般有助於打擊國際恐怖主義之危險而查訊資料時，即允許調取資料。雖然立法者建立干預之構成要件時，自始並未限於有助於防禦具體危險，但於採取防範刑事犯罪行為之措施時，至少應有以特定事實存在為依據之預測，而非僅依據一般經驗法則所為與具體危險有關之預測（上述[147]）。至少依性質可認定具體且時間上可預見之事件將發生，原則上即屬之。特別是與恐怖主義有關之刑事犯罪行為，取而代之者，立法者亦得視人民之個別行為，是否具備於可預見之未來將從事此等刑事犯罪行為之具體可能性。聯邦刑事局法第39條第2項第1款並未以至少依性質可認定具體且時間上可預見之事件為要件，或另外以依人民之個別行為可確定其於可預見之未來有從事此種刑事犯罪行為之具體可能性為要件，亦即其對於因果過程之可預見性，並未包括具限制功能之要求。

反之，聯邦刑事局法第40條第1項第1句，於其涉及同法第39條第2項第2款之部分，並無憲法上疑義。聯邦刑事局法第39條第2項第2款允許對於通訊行為人為資料之調取，立法者對於目標對象整體社交範圍，並非毫無標準地開放監控可能性，而是要求應詳細說明接近犯罪行為的程度。此外，隨著干預門檻之降低，應提升應受保護法益重要性之要求，亦無疑義地獲得滿足。鑑於一般調取用戶主資料有限之干預嚴重性，亦即應限於防範至少為重大犯罪行為（上述[150]），防範詳細具體之恐怖主義犯罪行為，無論如何皆為已足。

[229-233]（3）聯邦警察法第22a條第1項第1句，於其涉及同法第21條第1項之範圍內，不符合比例原則，未包括具限制其範圍功能

之干預門檻，或應僅針對個別情形調取資料之限制。同法第22a條第1項第1句，於其涉及第21條第2項第1款之部分，亦未受充分限制。同法第21條第2項第1款涉及未來可能之犯罪行為的資料，就此而言，雖然有事實可認定人民欲從事聯邦警察法第12條第1項所稱具重要性之刑事犯罪行為，即得調取用戶主資料，但該款規定並未包括充分建構之預測要求。

反之，聯邦警察法第22a條第1項第1句，於其涉及同法第21條第2項第2款之部分，本身符合憲法之要求。立法者對於目標對象整體社交範圍，並非毫無標準地開放監控可能性，而是超越一般經驗法則，以事實為依據之具體期待為標準。故於本句規定之適用範圍內，單純之通訊或當事人與目標對象之個人親近程度，尚未符合規定之要件，此亦滿足因果過程可預見性之要求。同時隨著降低干預門檻而提高應受保護法益之重要性的要求，亦獲得滿足，調取資料之權限限於防範聯邦警察法第12條第1項所稱具有重要性之犯罪行為。

[234-236]c）調取登入資料之系爭權限規定，本身受有充分之限制，合乎比例原則，其亦符合程序法上之廣泛要求（參見下述e，[244]以下）。僅於利用資料之法定要件存在時，始得請求調取資料，此為所有調取資料規定應具備之相同要件。因此調取資料規定確保不得獨立於登入資料之利用要求外，及因而如有必要得在更寬鬆之條件下，單獨查詢登入資料。

[237-243]d）關於調取依據動態IP位址而確定之用戶主資料之規定，整體而言，大部分未受有充分之限制，因此違反比例原則。只有聯邦刑事局法第40條第2項，於其涉及同法第39條第2項第2款之部分，符合憲法之要求；但該項規定並不符合程序法上之廣泛要求（參見下述e，[244]以下）。

雖然基於比例原則，原則上並未要求調取依據動態IP位址而確定之用戶主資料，應以較查詢一般用戶主資料而更嚴格之干預門檻為要件（參見[176]、[179]），但仍需要與個別干預門檻具交互作用之充分重要的法益保護。關於IP位址之分配，如規定之干預門檻在危險防禦部分係以具體危險為要件，而在追查刑事犯罪行為部分係以初始懷疑為要件，則仍有必要將干預之權限限於保護特別重要之法益

（上述[177]以下）。另一方面，如干預門檻已降低，而立法者就資料之查詢欲以防禦具體危險為已足者，鑑於分配動態IP位址具特別之干預嚴重性，無論如何應限於保護特別重要之法益（上述[180]）。系爭規定——除了普遍缺乏具限制功能之干預門檻外——，大部分不符合憲法之要求。另一方面，部分調取資料規定有規範法益之保護，其本身與降低之干預門檻結合後而有充分之保障。

聯邦刑事局法第10條第2項結合第1項第1句第1款，則需要為不同觀察。雖然該規定有助於保護具重要性之法益，然而本案涉及防範刑事犯罪行為之前置領域，仍應以保護特別重要之法益為必要，而應以防範至少為重大犯罪行為為要件，但上開規定並未包括此類限制。至於其他調取資料之規定，則自始即未包涵於個案中限於有應受保護法益之充分限制。

反之，雖然聯邦警察法第22a條第2項結合同法第21條第2項第2款，及聯邦刑事局法第40條第2項結合同法第39條第2項第2款等規定，包括充分受有限制之干預門檻，但只有聯邦警察法第40條第2項符合考量干預嚴重性而對於分配動態IP位址所設定之法益保護之要求，即——如本案情形——於防範刑事犯罪行為領域而降低干預門檻時，分配動態IP位址應有助於防範至少為重大之犯罪行為（上述[181]）。

[244]e）系爭規定基本上符合由比例原則導出而應遵守之透明性、個別權利保護及監督之廣泛要求，且亦包括了關於利用資料及銷燬資料之適當規定。然而，對於行政機關調取依據動態IP位址而確定之用戶主資料，並未課予作成紀錄之義務，於憲法上應予指摘。

[245]aa）相對於具較高干預嚴重性之隱密性措施，一般性調取用戶主資料之行為，基於其較低之干預嚴重性，相對而言毋庸負通知義務（Benachrichtigungspflichten）（參見BVerfGE 130, 151 <210>；亦參見EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, § 107（未確定）；EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 60 f.）。基於比例原則之觀點，使當事人得以知悉後續對其採取措施之範圍內將提供查詢之資料，並得由專業法院審查其合法性，即為已足（參見BVerfGE 150, 244 <302 Rn.

154>）。

[246] 關於資料之查詢，如顯示出干預嚴重性已提高，例如分配IP位址及——潛在地——查詢登入資料，各專業法律調取資料規定原則上定有應嗣後通知之規範。雖然只有於查詢用戶主資料之目的並未受阻礙時，應為通知，且如與第三人或當事人值得保護之重要利益相牴觸者，亦得不為通知，但相關規定仍符合憲法之要求（參見BVerfGE 125, 260 <344>；129, 208 <250 f.>）。課予行政機關作成紀錄之義務的理由，以確保在一定時間經過後，重新審查其要件是否存在。此外，毋庸通知之事由並無須由法院認定（參見BVerfGE 125, 260 <344>）。但於調取登入資料之情形，得由利用資料之授權依據中得出較高之要求。

[247]bb）關於監督，除專業監督外，資料保護法規之監督係由聯邦資料保護專門委員（Bundesdatenschutzbeauftragter）及機關之資料保護專門委員（Datenschutzbeauftragte）為之。因調取登入資料係以個別行政機關之指揮而提出請求為要件，就此而言，在內部監督上，即有一個更進一步、至少已系統化的層級。

[248]cc）然而關於調取依據動態IP位址而確定之用戶主資料，並無記錄決定依據之義務，即與比例原則之要求不符。

[249] 鑑於一般性查詢用戶主資料僅具有輕微之干預嚴重性，且考量通常係隱密地採行措施，嗣後亦不會通知當事人已提供查詢之資料，即無必要記錄作成決定之依據。如因只於行政機關內部決定查詢用戶主資料，即亦無作成紀錄之必要（就此BVerfGE 150, 244 <303 Rn. 157>）。儘管僅得由行政機關確保查詢資料之請求應滿足實體要件，但因其須以書面向電信服務業者提出查詢資料之請求，並指明法律依據，於此部分無論如何皆為向外界為之（參見電信法第113條第2項第1句）。

[250] 另一方面，分配動態IP位址，鑑於其干預嚴重性已提高，僅於採行此等措施之決定依據以可理解及可審查之方式作成紀錄之情形下，始得認為符合比例原則。與查詢資料請求相對應之法律依據及事實依據，應有紀錄以供查明（BVerfGE 125, 260 <344>）。一方面，如作成決定之行政機關本身就其決定之依據必須提出說明時，作成紀

錄即合理化及正當化其決定。另一方面，只有作成紀錄，始可使資料保護專門委員得以進行監督。最後，紀錄亦可減輕行政法院監督之負擔（參見BVerfGE 150, 244 <303 Rn. 157>）。反之，調取登入資料則無須一般地課予作成紀錄義務之規定，只要其基於個案之干預嚴重性而為必要者，通常即可由利用資料之個別授權依據得出相對應之要求。

[251]dd）然而，並無以法律規定對於議會及公眾負報告義務之必要。基於比例原則之理由，向議會為報告之義務以達到直接民主正當性之監督及審查，只有在對於深入干預私人領域行使調查及監控之權限，而有可能產生特別廣泛影響之基本權侵害時，始有其必要（參見BVerfGE 141, 220 <268 f. Rn. 103, 285 Rn. 142 f.>詳細說明）。對於——如本案情形——並非特別密集干預之措施，則此類監督及評價之方式並無必要。

[252]ee）由獨立之機關進行事前審查，例如由法院作成命令之方式，基於比例原則之理由，於憲法上並無必要。因此，調取資料之規定，於一般法律中僅針對調取登入資料規定法官保留，而於情報事務領域則規定由G10委員會[3]為事前審查，且對於調取登入資料所規定之法官保留另有許多例外規定，並無憲法上疑義。

[253]（1）如一法律規定授權行政機關得對於當事人秘密採行措施，且涉及應特別受保護之私密領域，或顯現特別高度之干預嚴重性時，則應透過程序上之預防措施，以考量基本權受干預之嚴重性，且特別應規定由獨立之機關為事前之監督，例如由法官作成命令之方式（參見BVerfGE 120, 274 <331>；141, 220 <275 Rn. 117>；亦參見EGMR, Szabó und Vissy v. Hungary, Urteil vom 12. Januar 2016, Nr. 37138/14, § 77）。除隱密性外，主要應考量者，為採行之措施可預期將涵蓋高度私密之資訊（參見BVerfGE 141, 220 <275 Rn. 117>；亦參見EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a.,

[3] 譯註：德國基本法第10條為保障郵件及電信通訊秘密自由，於情報事務領域中對於人民之郵件及電信通訊所為之監控，則另制定有專法（簡稱為G10法）。該法規定，於情報事務領域中所為之監控，應由依法組成之獨立G10委員會為事前監督。

C-203/15 u.a., EU:C:2016:970, Rn. 99, 120, 125）。是以，預防性監督係基本權有效保障之重要要素，且如基於措施之隱密性，致當事人本身事前無法察覺其利益將受影響者，應保障採行隱密措施之決定須充分考量當事人之利益（參見BVerfGE 120, 274 <331 f.>）。

[254]（2）查詢依據動態IP位址而確定之用戶主資料，而基於契約或基於預防性儲存之通訊紀錄而請求運用該資料者，相較於一般性調取用戶主資料而言，儘管干預嚴重性已提高，但仍無須法官保留（參見BVerfGE 125, 260 <344>）。至於得就資料庫中所有儲存之通訊紀錄為資料調取之規定，原則上應以法官保留為必要（參見BVerfGE 125, 260 <337 f.>；參見EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15u.a., EU:C:2016:970, Rn. 120, 125），而以往僅就通訊紀錄為個別且間接之利用而調查固網連線用戶之資料，現今可查詢固網連線用戶之資料，並不以應有預防性獨立審查之額外保障為必要。

[255]（3）關於授權調取與利用要件相關之登入資料之規定，原則上亦有同樣情形。儘管查詢登入資料本身已超越規定之資料利用，因其妨礙當事人之資訊自主保護，使其對於通訊關係私密性之信賴落空，而具備獨立之干預效力，然而干預嚴重性主要僅能由登入資料之利用而予以確定，因此獲取相關資料，在程序法面向，則亦取決於其利用之要件。

[256]比例原則並未要求應對於蒐集登入資料本身，規定獨立之要件，且亦未要求就此部分應無例外地適用法官保留。於法治國中，僅要求提供保障登入之資料——實體上及程序法上——亦應限於具備依個別查詢情事所具體追求之利用目的之要件（參見BVerfGE 130, 151 <208 f.>）。此應依個別之法律依據判斷之，並依干預之種類與嚴重性，及程序與實體之面向，而有所不同。因每一筆登入資料之查詢同時亦須具備其利用之要件，如基於利用之干預強度而在憲法上為必要者，應無限制地保障事前之法官審查（參見Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, Bd. 1, 2009, S. 99 <114 f.>）。

[257]儘管在一般專業法律之層面上，不論利用之要件而對於查

詢所有登入資料，可以說過度地皆有獨立之法官保留的規定，其例外情形並不致使上開相關規定違反比例原則。如規定之法官保留僅係用以取代由個別利用規定所得出之法官保留要求，則此處討論之例外情形，其範圍本身在憲法上即有疑義。如當事人知悉或可得知悉欲進行登入資料之查詢，此時例外地無法官保留規定之適用，此並未排除對此僅得嗣後地提供法律保護，則與嗣後受通知之情形相較，當事人並未受到更好之保障。相對而言，法官保留正可確保預防性之監督，並在必要時，可避免一開始即產生基本權之干預。如法院已經裁判得利用資料，而查詢資料即無須法官保留者，則無法確保進行查詢之行政機關就資料之利用享有權限，且就此存在必要之要件（參見Hauck, StV 2014, S. 360 <364>）。然而正因為相關規定並未以個別利用規定所生之法官保留要求，取代在獲取登入資料時之法官保留要求，而是以其存在為前提，故其於憲法上無須受指摘。

[258] 關於由進行查詢之行政機關為資料之安全、其他利用及銷燬之規定，符合憲法上之要求。

[259]（1）針對由聯邦刑事局、海關刑事局及聯邦警察所為之查詢用戶主資料，聯邦個人資料保護法（BDSG）第47條規定資料處理之一般原則，其中包括目的拘束原則（聯邦個人資料保護法第47條第2款）。此外，聯邦個人資料保護法第64條確立了資料安全之要求，同法第74條則包括資料傳輸之前提要件。再者，依同法第75條第2項規定，如與個人有關之資料，其處理為不合法、為履行法律之義務而應銷燬、或知悉該資料對於任務之履行已無必要者，即應立即銷燬之。

[260]（2）各專業法律本身包涵了補充性規定。聯邦刑事局法第12條規定目的拘束原則，依同法第25條以下規定對於國內傳輸及國際傳輸設定了限制。此外，聯邦刑事局法第69條以下規定包括對於資料保護、資料安全及當事人權利保障之要求。個別之保護規定嚴格地取決於不同之干預授權規定，而因此有不同之內容。聯邦警察法及海關緝私局法亦包括相對應之規定（聯邦警察法第二章第二節第二項，海關緝私局法第33條以下），上開相關規定補充了由聯邦個人資料保護法提供之保護水準的範圍。具體與情報事務有關之法律亦包括

各自之補充性規定，如聯邦憲法保護法第27條第2款、聯邦情報局法第32a條第2款及聯邦反軍事情報局法第13條第2款中皆援引聯邦個人資料保護法第64條。

D. 歐洲聯盟基本權憲章之觀點

[261]姑且不論聯邦憲法法院對於此類案件享有審判權之範圍，由歐盟基本權亦不會得出不同之標準。即使基於2002/58/EG指令第15條或DSG規章第6條（參見上述[85]-[87]），應將本案系爭規定部分視為基本權憲章第51條第1項第1句所稱執行歐盟法之規定，仍無具體及足夠之根據可認為針對應受審查之本案，目前所採基本法基本權保障之解釋，無法提供與歐洲法院裁判關於歐盟基本權憲章相同之保護水準（參見BVerfG, Beschluss des Ersten Senats vom 6. November 2019 - 1 BvR 16/13 -, Rn. 67 ff.），特別是無法由歐洲法院關於資料庫儲存指令之裁判（EuGH, Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u.a., C-293/12 u.a., EU:C:2014:238）及關於成員國資料庫儲存權限之裁判（EuGH, Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u.a., C-203/15 u.a., EU:C:2016:970）得出此種見解。於上開裁判中，涉及於內國全面蒐集電信通訊連線資料，而可幾乎完整地建立個別通訊參與者之人格特徵。於分配動態IP位址時，僅間接且個別地使用通訊紀錄，基本上與其不同。且由歐洲法院於「Ministerio Fiscal」案之裁判見解（EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788）亦無法得出任何根據，可認為基本權憲章之保障水準超出基本法之基本權保障。反而是上開裁判明確說明公家機關獲取由電信服務業者儲存之用戶主資料，不得視為較嚴重之基本權干預，而僅得用於打擊重大之刑事犯罪行為（參見EuGH, Urteil vom 2. Oktober 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 63；vgl. auch EGMR, Breyer v. Germany, Urteil vom 30. Januar 2020, Nr. 50001/12, §§ 95, 101（未確定））。在歐洲，取向於多元基本權保障之範圍內，本案中基本法之基本權保障無法提供歐盟基本權憲章之保護水準，此點並不明顯（亦參見BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 326）。

E. 法律效果

[262] 應宣告系爭規定大部分違反基本法第 2 條第 1 項結合第 1 條第 1 項及基本法第 10 條第 1 項。

I. 宣告系爭規定因侵害基本權而大部分違憲

[263]1. 確認法律規定違憲，原則上應產生其為無效之效果（聯邦憲法法院法第 95 條第 3 項第 1 句；參見 BVerfGE 101, 397 <409>）。然而如依聯邦憲法法院法第 31 條第 2 項第 2 句及第 3 句所得出之情形，聯邦憲法法院亦得自我限制而僅宣告違憲之規定與基本法不符（參見 BVerfGE 109, 190 <235>）。此時，聯邦憲法法院得同時將違反基本法之違憲宣告與於一定期限內繼續適用該違憲規定之命令相結合。如立即宣告應受指摘之規定無效，可能使保護公共福祉之重要法益喪失其基礎，並對於相關基本權為利益衡量，而認為於過渡期間內應接受此基本權干預者，則得為之（參見 BVerfGE 150, 244 <306 Rn. 168> 之詳細說明；固定實務見解）。聯邦憲法法院得對於過渡期間作成暫時命令，在立法者建立合憲之情狀前，使行政機關之權限應限縮至依該利益衡量要求之程度（參見 BVerfGE 141, 220 <351 Rn. 355> 之詳細說明）。

[264]2. 依此標準，如法律規定違憲者，並不宣告其為無效。本案應受指摘之傳輸及調取用戶主資料之規定違憲，主要係因無充分之干預門檻，及缺乏對於法益保護之要求。違憲之理由並未涉及相關規定所賦予之權限核心，而是其法治國之內涵設計。立法者就此部分得立即著手修正法律規定，進而以合憲之方式實現相關規定追求之目標。鑑於立法者得考量查詢用戶主資料對於履行國家任務之重要性，於此情形下，相較於宣告相關規定為無效而言，暫時繼續適用相關規定應更為可接受。

[265-267]3. 因此，應宣告系爭規定——於主文中明顯可知之範圍內——違反基本法。

[268]4. 違反基本法之宣告應與暫時繼續適用至 2021 年 12 月 31 日止之命令相結合，該命令涵蓋所有宣告違憲之權限及電信法第 113 條第 2 項至第 5 項規定之程序法要求。然考量受影響之基本權，該命令仍應有具限制功能之標準。此標準指向於現行規定，至於立法者制

定修正之規定時，當然享有不同之立法可能，特別是確定查詢用戶主資料之利用目的應受到憲法要求之限制。限制權限範圍之干預門檻，及於分配IP位址之範圍內無論如何亦應有充分重要之法益保護，恆為必要之要求。如——考量利用之資料的種類、範圍及利用可能性——已相對應提高法益保護之要求者，亦得降低干預之門檻（參見BVerfGE 141, 220 <272 f. Rn. 112>）。於修正之規定公布前，適用下列標準：

[269]a）如查詢資料係涉及防禦警察法一般性條款中所稱之具體危險而有必要者，或涉及情報機關為調查個案中特定而應受情報機關監控之行動或團體而有必要者，電信法第113條第1項第1句及本案系爭之一般性調取資料規定，得繼續適用。涉及追查刑事犯罪行為或違反秩序行為者，於至少有初始懷疑存在時，電信法第113條第1項第1句得繼續適用。

[270]b）此外，如查詢資料係為防範聯邦刑事局法第39條第2項或聯邦警察法第21條第2項之刑事犯罪行為而有必要者，電信法第113條第1項第1句，聯邦刑事局法第40條第1項第1句或聯邦警察法第22a條第1項第1句，於其各自交互作用範圍內，得繼續適用。此時，僅應於有特定事實可認定人民在可預見之期間內，至少依其性質以具體方式，欲從事聯邦刑事局法第5條第1項第2句所稱之犯罪行為，或聯邦警察法第12條第1項所稱具重要性之刑事犯罪行為者，或由其個別行為可認定其於可預見之期間內有將從事此等刑事犯罪行為之具體可能性者（參見BVerfGE 141, 220 <272 f. Rn. 112>），聯邦刑事局法第39條第2項第1款及聯邦警察法第22a條第2項第1款始得依此標準繼續適用。

[271]c）如於個案中，亦存在可利用依電信法第113條第1項第2句取得之資料之要件者，該句規定亦得繼續適用（參見BVerfGE 130, 151 <210>）。

[272]d）如於上述a）之標準外，為防禦對於具特別重要性法益之危險，或為追查刑事犯罪行為或至少為特別重大之違反秩序行為而查詢資料者，電信法第113條第1項第3句及本案系爭關於依據動態IP位址而確定之用戶主資料之查詢資料規定，得繼續適用。

[273]e）此外，電信法第113條第1項第3句，聯邦刑事局法第40條第2項或聯邦警察法第22a條第2項，於其各自交互作用範圍內，及於其涉及聯邦刑事局法第39條第2項與聯邦警察法第21條第2項之範圍內，考量上述a）及b）之標準，得繼續適用。至於聯邦警察法第22a條第2項，則須查詢資料係為防範聯邦警察法第12條第1項之重大犯罪行為而有必要者，得繼續適用。

II. 費用償還之裁定

[274] 基於聯邦憲法法院法第34a條第2項及第3項作成費用償還之裁定。

[275] 本裁判關於電信法第113條第1項第1句結合第2項第1句是否符合比例原則要求之部分，一票反對。

法官：

Harbarth　　Masing　　Paulus

Baer　　Britz　　Ott

Christ　　Radtke