「告知IP位址義務案」裁定

Verpflichtung zur Übermittlung von IP-Adressen

德國聯邦憲法法院第二庭第三分庭2018年12月20日裁定

- 2 BvR 2377/16 -

陳俊榕 譯

要目

關鍵詞

網際網路協定位址（Internetprotokolladressen）
電信監察（Telekommunikationsüberwachung）
秩序措施（Ordnungsmitteln）
網路位址轉換程序（NAT-Verfahren）
電子資料處理系統（EDV-System）
職業從事自由（Berufsausübungsfreiheit）
雙扇門模式（Doppeltürenmodell）
電訊秘密（Fernmeldegeheimnis）
往來資料（Verkehrsdaten)
扼殺性效果（erdrosselnde Wirkung）

案 由

聯邦憲法法院
案號：– 2 BvR 2377/16 –

聲請人L先生
－委託位於柏林Görlitzer路74號（郵遞區號：10997）的Johannes Eisenberg事務所律師Stefan König博士教授及

Stefanie Schork博士為全權代理人－

針對：a)斯圖加特邦法院於2016年9月1日之- 19 Qs 48/16 -號裁定，

b)斯圖加特區法院於2016年8月9日之- 27 Gs 6403/16 -號裁定

所提起之憲法訴願，聯邦憲法法院第二庭第三分庭之Hermanns法官、Müller法官以及Langenfeld女法官，依1993年8月11日公布之聯邦憲法法院法（BverfGG）第93b條與第93a條（聯邦法律公報第1冊，第1473頁）之規定，於2018年12月20日一致決議：

裁判主文

憲法訴願不受理。

理　由

I.本案之事實、法律爭點及歷審判決

本憲法訴願涉及的問題是，若電子郵件服務的供應商基於既有的資料保護服務而未記錄擁有帳號之客戶的網際網路協定位址（Internetprotokoll-adressen）（以下簡稱：網路位址（IP-Adressen））時，該供應商在合法規範的電信監察（Telekommunikationsüberwachung）框架下，是否也有義務將網路位址交給偵查機關。

1.從2009年起，訴願人開始經營註冊的「XX...」電子郵件服務商。其服務標榜對於客戶資料的特別有效保護，並且將資料安全及資料節約（Datensparsamkeit）原則視為義務。訴願人只有在基於技術上的理由是必要的，或者－基於其觀點－於法律規定時，才會調取和儲存資料。

2.斯圖加特檢察署針對從帳號僅知其暱稱的電子郵件帳號使用者r…，以懷疑其涉及數量不少的麻醉藥品不法交易以及違反戰爭武器控制法為由，對其展開偵查程序。

3.基於檢察署依刑事訴訟法第100a條、第100b條於2017年8月17日為了更有效及更加符合實際的刑事訴訟程序所為之修訂（聯邦法律公報第1冊，第3202頁）生效前的舊法所提出之聲請，斯圖加特區法院於2016年7月25日以裁定命令須確保、反映和提交所有在「XX...」伺服器中儲存的相關電子郵件帳號，「以及所有關於該帳號未來所產生的全部資料（包括內容、往來資料和網路位址，尤其是未來在登錄過程中的網路位址）」。該處分首先至2016年9月24日有效，區法院後來於2016年9月19日以裁定延長至2016年11月24日。

4.巴登–符騰堡邦刑事局於2016年7月28日向訴願人通知了其所命令的監察處分（Überwachungsmaßnah-

me）以及需監察的帳號。訴願人也在同一天安排了電信監察，並就此告知了邦刑事局。然而，訴願人指出，由於使用者的往來資料並未被「登錄」，因此也無法提供包含網路位址在內的這些資料。

檢察署於2016年7月29日以書面向訴願人表示，訴願人在監察處分期間內，有將相關帳號的往來資料和尤其是網路位址加以「記錄」的法律義務。從當天起代理訴願人的律師則以書狀對此予以反駁。訴願人無法從「XX...」調取有關的網路位址，而且這些網路位址也不存在。為監察目的所需之資料調取而採取的技術上防護措施以及同時不妨礙正常商業運作的義務是不存在的。

關於這一點，檢察署於2016年8月1日以書面警告訴願人，要對其聲請宣告秩序措施（Ordnungsmitteln）。訴願人的論述最多只適用於過去。然而訴願人誤解了現在的電信監察。電信監察的協力義務是出自舊刑事訴訟法第100b條第3項第1句，並且透過電信法（Telekommunikationsgesetz, TKG）第110條、電信監察處分之技術及組織實施命令（TKÜV），以及實施法定電信監察處分之技術準則（TR TKÜV）來加以具體化。依電信監察處分之技術及組織實施命令第5條第1項及第2項之規定，義務人必須為有權單位（berechtigten Stelle）提供有關其設備所處理的，包括電信最近情況之資料在內的完整電信副本。此外，依實施法定電信監察處分之技術準則的規定，義務人也必須將作為所屬事件一部分的網路位址，連同受監察之電子郵件的完整副本一併提交。毫無疑問的是，在對電子郵件或是其他對帳號存取之開啟或中止時點的相關網路位址，是涵蓋在電信監察處分之技術及組織實施命令第7條第1項第4款的規範之中。

訴願人於2016年8月2日以書狀描述其系統結構時，否定了「XX...」擁有網路位址的看法。基於安全的理由，「XX...」將內網中關於所謂的網路位址轉換程序（NAT-Verfahren），亦即將數據包（Datenpaket）內的位址資訊與其他位址資訊自動替換，與網路嚴格地加以區隔。因此，客戶的網路位址已經在系統的外部邊界遭丟棄，而且訴願人也無法存取。同樣地，訴願人在2016年8月2日向區法院交存了一份保護狀（Schutzschrift），其以本質上相同的理由來反對依刑事訴訟法第70條第1項之規定所聲請宣告之秩序措施。

5.斯圖加特區法院於2016年8月9日以遭指摘的裁定，對訴願人科處了500歐元的秩序罰鍰，用以取代七天的秩序拘留。基於2016年7月25日的裁定，訴願人有義務在未來就往來資

料，以及特別是網路位址加以調取。其對於連結資料之反向調取的法律依據是錯的。訴願人基於法律規定而有義務建構其技術設施，以擔保資料的調取。尤其是鑑於偵查程序的重大意義，秩序罰鍰的金額與替代的秩序拘留實施，顯得非常適當。

6.訴願人於2016年8月15日以書狀提出對2016年8月9日裁定的抗告。其主要主張區法院並未充分地就其論點加以辯論。在檢察署遞交一份事先並未送交訴願人的聲請狀後，訴願人在2016年8月26日以書狀補充了其訴願內容。對法律評價的關鍵是在刑事訴訟法第100g條，因為該條規定不僅對於已經存在的，同時也對於未來所產生的往來資料，是相對於刑事訴訟法第100a條的特別法（lex specialis）。然而，此處的網路位址並不在往來資料的概念下，因為網路位址無法從「XX...」調取、處理或利用。基於電信法第110條而來的基礎設施義務規範，同樣也不能作為資料調取的法律依據。最終，秩序罰鍰的裁定也因此而違法，因為該裁定想要強迫訴願人去做他無法做到的事情。訴願人並沒有所需的資料，而且也無法快速地取得，而是只能藉由其電子資料處理系統（EDV-System）昂貴的更新結構始能取得。但是，此類基礎設施義務不能藉由刑事訴訟法的強制措施（Zwangsmittel）來實現。

7.斯圖加特邦法院於2016年9月1日以無理由裁定駁回抗告。法院贊同了檢察署的意見。僅僅使用網路位址轉換程序，並不能免除訴願人交付包含網路位址在內的完整電信副本義務。這個義務來自舊刑事訴訟法第100b條第3項第2句、電信法第110條，以及電信監察處分之技術及組織實施命令第3條和第5條並第7條之「連同其所發布的準則」。依電信監察處分之技術及組織實施命令第5條之規定，受監察的電信係由電信最近情況的內容及資料所組成。在此範圍內，訴願人有義務將電信的完整副本提供給有權單位。根據2016年7月25日之裁定，訴願人有義務在必要時建立技術上的先決條件，以便履行其協力義務，而且盡可能完整地將網路位址提交，以便進行評價。

8.針對2016年9月1日的裁定，訴願人於2016年10月11日以書狀提出「根據刑事訴訟法第33a條之意見陳述」。該裁定並未深入分析訴願人所提出的主要法律與事實上的論據，並因此而侵害了法定聽審權。此外，邦法院也誤認了訴願人建立調取客戶網路位址技術上先決條件之花費和預期後果。依所公布的抗告裁定，根據成本估算，一個為期12個月的項目，且在保守估算下的成本量為至少80,000歐元。

9.邦法院解釋了作為聽審異議之

書狀，並於2016年10月28日以裁定駁回。抗告庭的決定是以訴願人的詳細論據為基礎。以此排除了刑事訴訟法第33a條的適用，因為決定內容上的錯誤，並不涵蓋在聽審異議的架構中。

10.邦刑事局於2016年11月18日通知訴願人可以關閉監察合作。秩序罰鍰則是在2017年1月2日繳納。

II. 憲法訴願人提起憲法訴願之主張

訴願人的憲法訴願是針對區法院於2016年8月9日所科處之秩序罰鍰裁定，以及邦法院於2016年9月1日之抗告裁定。訴願人指控其職業從事自由（Berufsausübungsfreiheit）（基本法第12條第1項第2句）和源於基本法第2條第1項（連結基本法第20條第3項）、第2條第2項第2句以及第14條之基本權受到侵害。

對這些基本權的保護領域所為之干預並無正當性，因為欠缺了一般法律上的基礎。秩序罰鍰的宣告和秩序拘留的警告是逼迫訴願人基於事實上的理由，無法完成之事（詳下述1.）也無法律上之義務（詳下述2.）。此外，秩序罰鍰的科處，並不符合比例（詳下述3.）。

1.基於所使用的網路位址轉換系統（NAT-System）之緣故，訴願人無法使用其被迫應交出的資料。在「XX...」的整體存取範圍，與用戶有關的網路位址既沒有在內部，也沒有在外部邊界。在網路與受防護的「XX...」－系統之間的邊界區域存在許多加密的，以及針對公司的公共網路位址的存取請求。應對哪個郵箱加以具體存取的資訊是位在加密的存取聯繫通道（Zugriffsverbindung）內部，而且無法對邊界或通道範圍內的所有組成部分加以開放。在執行所需動作後，數據包將再次加密，並透過這個聯繫通道再次返回傳送。在「XX...」－系統的外部邊界，最初的聯繫通道藉由公開的網路位址來加以確定，並且透過網路將加密的數據包傳送給客戶。這個所描述的傳送及轉換機制，既不能設計，也不可能過濾或分析利用其連續的內容。為此，「XX...」就必須完全地重新設計與網路的外部邊界。

2.將網路位址轉交給刑事追訴機關的義務並不存在。

刑事訴訟法第100g條作為允許刑事追訴機關在特定條件下調取往來資料的唯一相關規範，以致於根本就不必再去顧及刑事訴訟法第100a條，而且也不允許再這麼做。前面所提及的資料與刑事訴訟法第100g條所規範的往來資料無關，因為訴願人並未調取這些資料，而且因為根據電信法第96條之規定，這些資料對訴願人本身之目的而言並不需要，故而也不允許調取。據此，既不能從舊刑事訴訟法第

100g條，也不能從舊刑事訴訟法第100b條推論出訴願人具有將可疑的網路位址轉交之義務。

就算立法者有意透過2007年1月新修正的刑事訴訟法第100g條第1項將相關義務予以規範，也是如此。因為，面對相衝突的規範用語，無論如何都會欠缺一個明確的一般法律的干預基礎。此外，立法者本來就只想根據刑事訴訟法第100a條的模式下，能夠對往來資料即時監察，而不是想透過電信供應商來達到「更多」的資料調取。如果立法者並不想透過刑事訴訟法第100g條第1項來規範電信供應商為刑事追訴之目的而來的調取和儲存資料的義務，那麼這個義務的立法基礎最終也就只能出自2015年所建立的資料保存之修正形式。另外，資料調取義務－如同聯邦憲法法院所稱的「雙扇門模式（Doppeltüren-modell）」－是特殊的，而且不是在刑事訴訟法，是在電信法規範。

3.為其所追求之目的－網路位址的轉交－實現，秩序罰緩的科處並不適當。訴願人無法分配網路位址。電子資料處理系統必要之改建可能需耗時12個月左右。具體的監察措施屆時已經結束。裁定也是不恰當的，因為改建會持續很長時間、造成不合比例的高成本，而且也可能會降低安全標準。

III.聯邦最高法院的聯邦總檢察長、聯邦資料保護及資訊自由監察官、聯邦資訊安全局和聯邦網路局對本案之意見

1.聯邦最高法院的聯邦總檢察長（der Generalbundesanwalt beim Bundesgerichtshof）、聯邦資料保護及資訊自由監察官（die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit）、聯邦資訊安全局（das Bundesamt für Sicherheit in der Informationstechnik）和聯邦網路局（die Bundesnetzagentur）對於憲法訴願表明立場。

a)聯邦最高法院的聯邦總檢察長認為憲法訴願無理由。

在持續性地電信監察中，網路位址的轉交義務之法律基礎並不在刑事訴訟法第100g條第1項，而是在刑事訴訟法第100a條第1項。訴願人所辯解的相反意見在法律上是站不住腳的。有別於刑事訴訟法第100g條，刑事訴訟法第100a條之處分並不侷限於特定的資料群（往來資料、內容資料），而是包含整體的「電信」。電信法第110條要求服務供應商提供實施法定電信監察處分的技術上設備之義務，而電信監察處分之技術及組織實施命令（TKÜV）則是將該要求加以具體化。在如同訴願人所提供的電子郵件服務中，電信監察處分之技術及組織實施命令第7條第1項第1句第4款所規範的「其他定址說明（andere

Adressierungsangabe）」指的就是網路位址，而該網路位址則是分配給能連接上網路，且客戶打算藉其能夠連接上信箱的終端設備。與此相對的，則是實施法定電信監察處分之技術準則（TR TKÜV）明確規定了網路位址的提供。

訴願人的這個網路位址也是在電信監察處分之技術及組織實施命令第7條第1項第1句第4款的規範之中。如果訴願人不為本身的目的而儲存，也並不衝突，因為他是依賴且利用這個網路位址而來服務。如果不對此予以加工處理，訴願人不可能將在特定電子郵件位址下進行的通訊分配給正確的終端設備，從而分配給客戶。

受指摘的秩序罰鍰裁定是在電信監察的合法基本規定中，在形式及實質上合法的基礎下所宣告。適度科處之秩序罰鍰，也沒有不合比例。如果訴願人有建置基礎設施，而該設施當時之所以不可能轉交所要求的資料是由於訴願人自己對其彷彿視而不見時，並不會免除訴願人依舊刑事訴訟法第100b條第3項第3句連結刑事訴訟法第95條第2項之帶有秩序措施及強制措施的轉交義務。

b)聯邦資料保護及資訊自由監察官考慮到「監察總體核算（Überwachungs-Gesamtrechnung）」而表示疑慮，因為就電信供應商有義務改變其資料處理程序而言，已超出依電信法所必要的程度。

c)聯邦資訊安全局評論了訴願人所使用的網路位址轉換系統之技術事實。

d)聯邦網路局認為，訴願人分配其客戶的網路位址在事實上和法律上都是可能的，而且，就其而言，訴願人對其基礎設施有相關的結構改造義務。

2.訴願人已對這些觀點予以反駁，且重複和深化其迄今為止的說法。

3.原因程序（Ausgangsverfahren）的卷宗已呈送於法庭。

IV.駁回憲法訴願人併同本案所提出之聲請

對於併同憲法訴願所提出的暫時處分之聲請，法庭已於2016年12月12日以裁定駁回。

V.憲法訴願不受理之理由

本件憲法訴願不受理。本件不具有聯邦憲法法院法第93a條第2項所規定的受理理由，因為本件憲法訴願已經部分不受允許，而其他部分則無論如何都是無理由的。

1.針對區法院於2016年8月9日所做的原因判決（Ausgangsentscheidung）範圍內的憲法訴願是不受允許的。作為抗告法院（Beschwerdegericht）的邦法院必須自己進行全面的實質審查（參見：刑事訴訟法第308條第2項、第309條第2項），而且

也已經這麼做了。其所做的判決取代了區法院的判決；這在程序上已經覆審了（參見：聯邦憲法法院第二庭第三分庭於2015年4月17日裁定- 2 BvR 1986/14 -，juris, Rn. 10以及於2017年11月8日裁定- 2 BvR 2129/16 -，juris, Rn. 11，二者皆有更多的說明）。

2.就針對抗告決定的憲法訴願而言，無論如何都是無理由的。雖然秩序罰緩的科處，是干預了訴願人在基本法第12條第1項第2句所受保護的職業從事自由（詳下述a）。然而，邦法院對於依舊刑事訴訟法第70條第1項第2句、第95條第2項、第100b條第3項第2句連結電信法第110條第1項第1句第1款以及電信監察處分之技術及組織實施命令的相關規定之干預係合法的看法，依憲法是無可指摘的（詳下述b）。

a)秩序罰緩的科處，是干預了職業從事自由。依刑事訴訟法第70條第1項第2句、第95條第2項連結舊刑事訴訟法第100b條第3項所允許的電信法和電信監察處分之技術及組織實施命令，在確立電信服務供應商的提供設備義務範圍內之規定，是具有一種客觀職業規範的傾向（參見：BVerfGE 95, 267 [302]; 97, 228 [253 f.]; 113, 29 [48]; 129, 208 [266 f.]對此之要求；歷來判決見解），因為這些規定對於企業經營的設備，在技術和組織上做了預先規定（參見：聯邦最高法院於2015年8月20日裁定- StB 7/15 -, juris, Rn. 7; Bär, in: KMR, StPO, § 100b Rn. 14a [Juni 2016]; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2492a; 同此參見：Hermes, in: Dreier, GG, 3. Aufl. 2013, Art. 10 Rn. 28）。但不存在一個職業選擇規範（Berufswahlregelung）；尤其是使訴願人在事實上無法有意義地從事其職業（參見：BVerfGE 125, 260 [359] 關於匿名化服務）。

b)邦法院認為，依相關的法定規範對基本法第12條第1項第2句保護範圍內的干預行為是合法的，這個看法並無憲法上的疑慮。

aa)依基本法第12條第1項第2句之規定，對於職業自由（Berufsfreiheit）的干預，只有在能夠預見干預行為之範圍及界限的一般法律規定之基礎上，才是受允許的。對此，立法者在可做成的法定規範範圍內，必須自己做出所有本質上的決定（參見：BVerfGE 73, 280 [295]; 80, 1 [20]）。對於基本權保護領域的干預越是強烈，立法者的意向就必須越明確表示（參見：BVerfGE 87, 287 [317]; 98, 49 [60]）。但這並不表示干預的前提條件必須很輕易地從條文的字句中得出；只要能透過一般解釋原則的協助來加以推斷，尤其是從規範的目的、意義脈絡和歷史，就足夠了（參見：BVerfGE 19, 17 [30]; 58, 257 [277]; 62,

203 [210]; 80, 1 [20 f.]; 82, 209 [224]; 聯邦憲法法院第一庭第一分庭於2014年4月22日裁定- 1 BvR 2160/11 -, juris, Rn. 20）。

倘若對案件所做出的判決並非恣意或侵害特定的憲法權利，那麼一般是由管轄法院來對其做一般法律上的解釋及應用，而且聯邦憲法法院原則上也不再對此做事後審查（參見：BVerfGE 18, 85 [92 f.]; 34, 369 [379]）。專業法院的一個可能錯誤必須正好出現在對基本權的忽視。這種情形通常發生在：當一個基於對基本權意義在原則上是錯誤的見解，尤其是對其保護範圍的錯誤是明顯的時候，或者是當對於基本法予以理性評價而產生無法理解的法律適用錯誤（參見：BVerfGE 18, 85 [92 f.]; 62, 189 [192 f.]; 89, 1 [14]; 95, 96 [127 f.]）。

bb)對此，基本權的違反並不明顯。專業法院以憲法上可接受的方式，解釋了關於電信服務供應商的協力與提供設備義務的規範（舊刑事訴訟法第100b條第3項第2句連結電信法第110條第1項第1句第1款，電信監察處分之技術及組織實施命令第3條、第5條第1項和第2項、第6條第1項以及第7條第1項）；其可以在不違憲的情況下，認為訴願人違反這些義務（詳下述(1)）。另外，專業法院在這些情形中，根據舊刑事訴訟法第100b條第3項第3句連結刑事訴訟法第95條第2項第1句所授予的可能性，亦即刑事訴訟法第70條第1項第2句所提及的秩序措施之科處，係使用了憲法所不予非難的方式（詳下述(2)）。

(1)專業法院可以在不違憲的情況下，認為訴願人有義務從監察帳戶的命令開始時，向刑事追訴機關提供該帳戶所產生的外部網路位址，因為刑事訴訟法第100a條所規定的電信監察，不僅包含電信內容，也包含詳細的電信情況、包含可疑的網路位址（詳下述(a)）。在這方面，不同於邦法院之見解，訴願人依電信法第110條第1項第1句第1款連結電信監察處分之技術及組織實施命令第3條、第5條第1項和第2項、第6條第1項以及第7條第1項第1句第4款之規定，有義務將其營運建構為可提供這些－其所擁有的－網路位址，作為合法電信監察的一部分，依憲法並沒有什麼好反對的（詳下述(b)）。從刑事訴訟法第100g條也不會得出不同結論（詳下述(c)）。

(a)－合憲的（參見：BVerfGE 129, 208）－刑事訴訟法第100a條對電信監察和紀錄予以授權。依學界和實務的通說，電信的概念在援引電信法第3條第22款之立法定義下，是合憲的。因此，「電信」係指藉由科技設備或系統而以符號、語言、圖畫或聲音形式呈現的每一種方式來發送、

傳遞及接收訊息的技術過程，且該方式作為一種訊息，能夠發送、改編、轉傳、接收、調節或控制可識別的電磁或光學訊號（參見：聯邦憲法法院第二庭第三分庭於2016年7月6日裁定 - 2 BvR 1454/13 -, juris, Rn. 25 ff.有更多說明，以及反對意見）。在這種「廣泛的」電信概念之背景下，對於電子郵件通訊的存取，就無論如何都會涉及到，從寄件人的設備透過其郵件伺服器而向電子郵件供應商的郵件伺服器傳送訊息，以及之後收件人的收取訊息，而此也毫無爭議地屬於刑事訴訟法第100a條的適用範圍（參見：Schmitt, in: Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 100a Rn. 6b; Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 16 ff.; Bär, in: KMR, StPO § 100a Rn. 28 [Juni 2016]; Graf, in: BeckOK, StPO, § 100a Rn. 54 [1. Januar 2018]; Wolter/Greco, in: SK-StPO, 5. Aufl. 2016, § 100a Rn. 36; Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 73; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; Singelnstein, NStZ 2012, S. 593 [596]; 對於存取儲存在供應商的郵件伺服器內之電子郵件，參見：BVerfGE 124, 43）。

於此應注意的是，對於刑事訴訟法第100a條「電信」的詳細解釋，特別也須遵守基本法第10條關於受監察之關係人的基本權保護，因為電訊秘密（Fernmeldegeheimnis）是對於暫時性資料的秘密監察之憲法標準（參見：聯邦憲法法院第二庭第三分庭於2016年7月6日裁定- 2 BvR 1454/13 -, juris, Rn. 32有更多說明；亦參見：BVerfGE 100, 313 [358 f.]; 113, 348 [364 ff.]; 129, 208 [240 ff.]; Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 4; Bär, in: KMR, StPO § 100a Rn. 10 [Juni 2016]; kritisch Wolter/Greco, in: SK-StPO, 5. Aufl. 2016, § 100a Rn. 38 ff.）。但基本法第10條第1項對於電訊秘密的保護，並非僅限於通訊內容，而是也包括電信的詳細情況在內（參見：BVerfGE 129, 208 [240 f.]）。對此，特別包含：在哪些人或哪些終端設備之間，是否、何時以及多常發生或嘗試進行電信通訊（參見：BVerfGE 67, 157 [172]; 85, 386 [396]; 107, 299 [312 f.]; 129, 208 [241]）。於此，基本法第10條第1項包含所有藉由電信通訊技術所進行的資訊傳輸，不論是由誰來操作傳輸和轉傳設備（參見：BVerfGE 107, 299 [322]; 129, 208 [241]）。

不過，即使將此保護內容納入對於刑事訴訟法第100a條的解釋之中，亦即，只要在電信法第3條第30款所規範的往來資料（Verkehrsdaten）（早期稱為連接資料（Verbindungs-daten））是在受電信監察之範圍內產

生的，刑事訴訟法第100a條的電信監察也就會涉及這些資料（參見：Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 14, 57; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; 亦參見：BVerfGE 107, 299 [314 ff.]），那麼在憲法上也就沒有什麼好反對的。在這個意義下的往來資料也恰恰包含所產生的網路位址。因此，這些就會被列為對從服務供應商所允許調取的往來資料做最終確定的電信法第96條第1項第1句規定中的作為參與連接或設備之編號（Nummern）（參見：電信法第3條第13款）（參見：聯邦議會公報15/2316，第89頁－關於當時的電信法第94條－；Braun, in: Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 96 Rn. 7; Lutz, in: Arndt/Fetzer/Scherer/ Graulich, TKG, 2. Aufl. 2015, § 96 Rn. 6 f.; Klesczewski, in: Säcker, TKG, 3. Aufl. 2013, § 96 Rn. 5; 關於往來資料的動態網路位址分類，參見：BVerfGE 130, 151 [181 ff.]; 聯邦最高法院於2011年1月13日判決- III ZR 146/10 -, juris, Rn. 22 ff.）。因此，電子郵件服務供應商的客戶打算透過能以動態或靜態的網路位址連接網路的終端設備來存取他們的電子郵件帳號，原則上就屬於刑事訴訟法第100a條的適用範圍（同此，參見：聯邦最高法院於2015年8月20日裁定- StB 7/15 -, juris）。

(b)依照刑事訴訟法第100a條所發布之命令框架下的電子郵件往來監察也包含所涉及到的網路位址，但這種情況並不表示訴願人作為電信設備的營運商（Betreiber），為了也提供這些網路位址給刑事追訴機關之目的，就有義務去做預防措施。就這點而言，舊刑事訴訟法第100b條第3項第2句所指的就是電信法和電信監察處分之技術及組織實施命令之規定。

依電信法第110條第1項第1句第1款之規定，公共電信服務的營運商從營運時起，有義務自費維持實施電信監察的技術設施，並採取相關的組織上預防措施，以確保其能立即實施。實施監察處分的基本技術要求和組織重點，於此係由電信法第110條第2項之授權基礎所發布的電信監察處分之技術及組織實施命令來加以規範。據此，訴願人也具有維持義務；電信監察處分之技術及組織實施命令第3條第2項對於某些類型的電信設備之例外規定情形，於此既無主張，也不明顯。

需提供的資料範圍規定在電信監察處分之技術及組織實施命令第5條第1項和第2項連結第7條第1項之中。依電信監察處分之技術及組織實施命令第5條第1項之規定，需監察的電信－符合刑事訴訟法第100a條廣泛的電信概念－是由關於電信詳細的內容和資料所組成。根據該條第2項之規

定，義務人應提供關於其電信設備所處理的完整電信副本。作為監察副本的一部分，義務人最終還是必須依電信監察處分之技術及組織實施命令第7條第1項第1句第2、3及4款之規定，提供其所擁有的關於撥號或其他定址訊息之資料。依照電信法的用語，在電信時所產生的網路位址很容易被納入「其他定址訊息」的概念下，因其恰恰就是拿來定址之用，也就是用於達到或尋找網路上的特定目標（Ziel）。因此，－如前所述－網路位址屬於電信法第3條第13款的立法定義，而根據該定義，電信法中的編號（Nummern）就是在電信網路中，為定址目的而產生的字符串（Zeichenfolgen）（參見：北萊茵－威斯特法倫邦高等行政法院於2011年5月26日裁定- 13 B 476/11 -, juris, Rn. 13 ff.; Lünenbürger/ Stamm, in: Scheurle/Mayen, TKG, 3. Aufl. 2018, § 3 Rn. 35; Büning, in: Beck‘scher TKG-Kommentar, 4. Aufl. 2013, § 3 Nr. 49; Fetzer, in: Arndt/Fetzer/ Scherer/Graulich, TKG, 2. Aufl. 2015, § 3 Rn. 79; Säcker, in: Säcker, TKG, 3. Aufl. 2013, § 3 Rn. 38; 亦參見：聯邦議會公報16/2581，第22頁）。

本案中，問題可能在於訴願人是否有電信監察處分之技術及組織實施命令第7條第1項第1句所規範的網路位址。訴願人在其憲法訴願中指出，在他的系統結構中並沒有其客戶的公開網路位址。在「XX. . .」的整體存取區域中，與用戶有關的網路位址既沒有在內部，也沒有在外部邊界（亦即，在網路位址轉換器（NAT-Lastverteiler））。然而，就其整體來說，並非如此。從訴願人所描述的系統結構可知，訴願人必須至少在通訊期間儲存其客戶的公開網路位址，否則他根本無法將檢索到的數據包傳送給他的客戶。這點與聯邦資訊安全局的意見是一致的，而根據該意見，網路位址轉換器內的軟體必須在整個連接期間，將內部的連接資料分配給外部的連接資料，否則就不可能成功通訊。因此，訴願人在回覆聯邦資訊安全局的意見時，承認網路位址有儲存在程式內部的資料結構（Datenstruktur）之中。不重要的是，訴願人是否藉由根據其所陳述的「暫時」儲存來調取聯邦資料保護法（BDSG）第3條第3項的公開網路位址（對此，參見：Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 102 ff.）。在存取受監察的電子郵件帳號時，無論如何都會產生資料，對此至少暫時地知道訴願人的電信設備，而且也利用於與要求通訊的客戶建立成功的通訊。訴願人手中擁有資料（Daten），且該資料作為由電信設備所產生的受監察電信之完整副本的一部分，因此，提供資料無論如何在憲法上都是合理

的。

就算訴願人－目前－無法存取外部網路位址，也並不衝突。因為資料本身並非不存在，而是僅僅因為訴願人出於資料保護的理由而決定將其隱藏在內部系統之中，且不予以記錄。然而，不做相關的記錄並不必然與使用網路位址轉換器有關，而是僅僅歸責於訴願人有意所選擇的商業暨系統模式。這點不僅已在聯邦資訊安全局的意見中得到確認，其甚至還建議應做相關的紀錄，而且訴願人的報告也證實，即使會耗費不少的技術及經費，其也可以重新設計其系統。

在這個脈絡下，聯邦憲法法院不必決定哪一種具體的系統模式在資料保護方面看起來比較好。而是只需要去決定專業法院對於法律規定的解釋，是否有侵害到訴願人的基本權。根據前述說明，邦法院的法律見解看不出有違反恣意禁止（Willkürverbot）或特殊憲法（spezifisches Verfassungsrecht）之處。雖然看起來訴願人所關切的，是提供一個最佳資料保護且因此會對許多使用者具有吸引力的商業模式，而且在基本法第12條第1項的觀點下，是完全值得保護的。然而，這並不能免除其在電信法和電信監察處分之技術及組織實施命令中，所考慮到一個運作良好的刑事司法之憲法要求下的合理解釋規定（參見：BVerfGE 133, 168 [199 Rn. 57]；歷來判決見解）。

最後，這個結論也不會與根據2017年7月11日新公布的電信監察處分之技術及組織實施命令第7條第1項第1句第9款之新增規定，現在已明確擴及義務人之電信設備所知悉的參與者之公開網路位址一事相衝突。因為，這個新規定無論如何都不能將迄今可疑的網路位址排除在應提供的資料範圍之外，來作為憲法上的必然結論。更確切地說，新增的電信監察處分之技術及組織實施命令第7條第1項第1句第9款之規定，顯然更具有澄清的功能。因為，根據聯邦政府的草案理由，歐洲電信標準協會（Europäischen Instituts für Telekommunikationsnormen）之標準（所謂的ETSI-Standards）與以之為基礎的實施法定電信監察處分之技術準則之規定，應「在法律上確保」基於網路電信服務之監察。這些已經規定在監察處分的範圍內，除了其他資料以外，也應告知各個網際網路協定位址（Internetprotokoll-Adresse）（對此，參見：die Anlagen F.1 und F.2.1 zur TR TKÜV）。在實務上，有關的電信公司已經履行了這些要求（參見：聯邦參議院公報243/17，第26頁）。

(c)與訴願人見解相反的是，刑事訴訟法第100g條第1項在涉及對未來電信（即時）監察範圍內，並未取代

刑事訴訟法第100a條規定。雖然立法者將電信監察的新法版本和其他隱密偵查處分的版本，以及根據刑事訴訟法第100a條而來的2007年12月21日2006/24/EG實施準則（聯邦法律公報第1冊，第3198頁），擴大作為調取往來資料的一般性及廣泛的授權（參見：聯邦議會公報16/5846，第50頁）。但是，其目的是在克服以前對於往來資料和電信內容資料的即時調取（Echtzeiterhebung）係僅在當時版本的刑事訴訟法第100a條、第100b條之條件下受允許的相同處理方式。這是因為根據刑事訴訟法第100a條規定，由於干預強度不同，一個對於往來資料即時調取的可能限制是不必要的（參見：上開聯邦議會公報16/5846）。立法者想透過新的刑事訴訟法第100g條第1項來限制刑事訴訟法第100a條適用範圍的說法是受到質疑的。相反地，立法者想建立一個與刑事訴訟法第100a條明確嚴格的干預條件相較之下，對於往來資料存取可能性較容易。就未來的電信及對其即時調取而言，相對於較廣泛適用的刑事訴訟法第100a條，刑事訴訟法第100g條第1項因而適用於往來資料的存取（參見：Bruns, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 100a Rn. 24; Hauck, in: Löwe-Rosenberg, StPO, 26. Aufl. 2014, § 100a Rn. 59; Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2482a; 亦參見：Eckhardt, CR 2007, S. 336 [341]）。從訴願人所援引的2015年12月10日採用往來資料儲存義務及最長儲存期限的立法理由（聯邦法律公報第1冊，第2218頁）來看，也不會得出不同結論。其所提出的來源，僅包含規範適用範圍的一般性說明，看不出立法者想要透過新的規定來限縮刑事訴訟法第100a條的適用範圍（參見：聯邦議會公報18/5088，第27、31頁）。

(2)在本案中，對秩序罰鍰的科處，依憲法也同樣沒有什麼好反對的。

(a)對於秩序罰鍰的宣告具備法定要件。

當服務供應商拒絕履行其義務時，依照舊刑事訴訟法第100b條第3項第3句連結刑事訴訟法第95條第2項之規定，可以處以刑事訴訟法第70條所規定的秩序及強制措施，尤其是秩序罰鍰及－作為替代手段的－秩序拘留。根據區法院於2016年7月25日的裁定，訴願人有義務讓刑事追訴機關能夠實現所命令的電信監察，以及立即提供其必要訊息。在這種情況下，他所應做的適當預防措施，還包括－如前所述－訴願人就未來所產生而對於命令中所涉及的標記加以存取的網路位址之傳輸。這些作為該命令所涉及的電信完整副本的一部分而由訴願人來提供，沒有任何在憲法上須被指

摘之處。

訴願人違反了這項義務。看不出有不必負責的依據。訴願人並未提出其行為具有能免於宣告秩序罰鍰責任（參見：Wohlers/Greco, in: SK-StPO, 5. Aufl. 2016, § 95 Rn. 31有更多說明）的禁止錯誤（Verbotsirrtum）。尤其，既未闡明也不清楚的是，訴願人在建立其系統時，對於具體的、與其計畫直接且特別有關的法律問題，有尋求並從而信賴可靠且專業的法律意見（對此，略見：聯邦最高法院於2000年2月2日裁定- 1 StR 597/99 -, juris, Rn. 27; 2017年5月16日判決- VI ZR 266/16 -, juris, Rn. 28 ff.）。因此，法院可以在所授予的衡量範圍內，處以1,000歐元以下的秩序罰鍰，並且在科處秩序罰鍰無效的情況下，可以處以秩序拘留（參閱：刑事訴訟法第70條第1項第2句連結刑法施行法第6條）。

(b)科處秩序罰鍰500歐元並未不合比例。

(aa)如果訴願人陳述秩序罰鍰的宣告對於－分配網路位址之－目的實現並不適當，因為改建其必要的電子資料處理系統可能需耗時12個月左右，而且具體的監察措施屆時已經結束了，那麼訴願人就是誤認了秩序罰鍰和秩序拘留的功能了。秩序措施既具有預防性，也具有懲罰性的功能：一方面，秩序措施有助於敦促其履行程序法上的協力義務。另一方面，也涉及到一個先前違反規定的類似刑罰之制裁（僅參見：Ignor/Bertheau, in: Löwe-Rosenberg, StPO, 26. Aufl. 2008, Anhang zu § 51 Rn. 2有更多說明）。因此，當一個預防作用已經不再能夠實現時，尤其是因為關係人在刑事訴訟法第95條的情形中，已在事後交出物品時，秩序措施仍舊持續維持著（參見：Schmitt, in: Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 95 Rn. 9; Greven, in: Karlsruher Kommentar, StPO, 7. Aufl. 2013, § 95 Rn. 4;Wohlers/Greco, in: SK-StPO, 5. Aufl. 2016, § 95 Rn. 32有更多說明；Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2328）。在舊刑事訴訟法第100b條第3項第3句連結刑事訴訟法第95條第2項的情形，也同樣適用。

(bb)鑑於訴願人拒絕履行其法定義務，所提及的秩序措施科處也是必要的。聯邦網路局為執行電信法第110條第2項連結電信監察處分之技術及組織實施命令所規定之義務，可以依照行政執行法（Verwaltungsvollstreckungsgesetz）之規定，處以500,000歐元以下的怠金（Zwangsgelder）（參見：電信法第115條第2項第1句第1款），與此並不衝突。因為怠金的科處僅用於執行法定的保留義務（Vorhaltungsverpflichtungen），

且通常涉及企業的違法設備，但依照舊刑事訴訟法第100b條第3項第3句連結刑事訴訟法第95條第2項之規定，－如前所述－一個在具體的刑事訴訟程序中的義務違反行為，無論如何都應受到處罰。因此，這些規定是有助於不同之目的而併存。尤其，服務供應商就其營運從一開始就沒有根據法律做相應的處理，此情況並不能免除其受刑事訴訟之秩序措施的宣告。

(cc)最後，秩序罰鍰的宣告符合狹義比例原則。根據過度禁止原則（Übermaßverbot），干預行為的強度不能與合法化干預的理由在程度上不成比例（參見：BVerfGE 90, 145 [173]; 109, 279 [349 ff.]; 118, 168 [195 f.]；歷來判決見解）。受干預者對於可預測性（Zumutbarkeit）的界線，必須在適當的整體評價中得到確保（參見：BVerfGE 90, 145 [173]; 120, 224 [241]）。

於此看不出對訴願人有不可期待之負擔。科處500歐元的秩序罰鍰並未被過高的裁量，而且根據訴願人自己的說明，在經濟方面也並無危害。雖然透過此舉來處罰義務違反行為，而訴願人卻只可能透過可觀的時間和高成本的重建，於現在和未來得避免對於該義務的違反。但是，這僅僅是訴願人有意選擇系統結構的結果，而這也使其無法履行身為電信供應商的協力義務。這些都是專業法院－如前所述（參見：上開V.2.b）－以憲法所不予非難的方式，所引用的法律規定。僅僅選擇資料保護優先的商業模式並不能使訴願人免除對這些義務的遵守。如果原則上由企業承擔就此所產生的費用，憲法也不會加以非難（參見：BVerfGE 125, 260 [359 ff.]）。由此產生的費用承擔所可能發生的扼殺性效果（erdrosselnde Wirkung），既未主張，也不明顯。

3.根據聯邦憲法法院法第93d條第1項第3句之規定，無須再考慮其他理由。

本裁判不得抗告。

法官：

Hermanns　Müller　Langenfeld