資安漏洞案

德國聯邦憲法法院 2021 年 6 月 8 日第一庭裁定
- 1 BvR 2771/18 -
BVerfGE 158, 170-202

李寧修 譯

要目

關鍵詞

資訊科技系統（informationstechnischer Systeme）
機密性及完整性（Vertraulichkeit und Integrität）
安全漏洞（Sicherheitslücken）
電子通訊來源之監察（Quellen-Telekommunikationsüberwachung）
零日缺漏（Zero-Day-Schwachstellen）

裁判要旨

1. 德國基本法第 10 條第 1 項除作為防禦權外，尚委託國家保護人民不受來自私人之第三方，對受秘密通訊保障之通訊造成之侵害（經 BVerfGE 106, 28 <37> 確認）。
2. a）維護資訊科技系統機密性及完整性之基本權，課予國家應致力於保護該系統免於遭受第三方攻擊之義務。

b）國家之基本權保護義務亦要求訂定法規，以與基本權相符之方式解決目標之衝突，一方面保護資訊科技系統免於遭受第三方透過尚未知悉之安全漏洞進行攻擊，另一方面，保持該類漏洞之開放，讓基於危害防止之電子通訊來源監察成為可能。

3. 主張違反法定保護義務須負特定之舉證責任。此種憲法訴願必須完整掌握法律規定間之關聯。於此包括闡明與系爭規範整體有所關聯法規之基本特徵，並指明為何其於憲法上之保護不夠充分。
4. 若直接針對法律聲請憲法訴願，依據補充性原則，向行政法院提起確認或不作為之訴訟，得被認為屬事前應採行之法律救濟。若規範之判斷僅引起具體之憲法問題，並經由專門法院事前之審查，預期應裁判之基礎並不會改善，則其即非必要（stRspr）。此亦適用於指摘違反法定保護義務之情形。

案　由

聲請人……

反對轉化歐盟第2016/680號指令於巴登—符騰堡邦之警察及修正於2020年10月6日所訂定其他警察法規之法律（法律公報第735頁）中，巴登—符騰堡邦警察法（PolG BW）第54條第2項。

聯邦憲法法院第一庭在Harbarth院長、Paulus法官、Baer法官、Britz法官、Ott法官、Christ法官、Radtke法官及Härtel法官之參與下，於2021年6月8日作成決定：

裁判主文

憲法訴願予以駁回。

理　由

A. 事實

[1] 本憲法訴願涉及警察機關處理系統製造商亦尚未知悉，而存在於程式或其他資訊科技系統中安全漏洞之方式（所謂之零日缺漏）。聲請人就此表示反對，認機關針對其已知悉之安全漏洞並不會進行通報，因其希望避免製造商因而關閉這些漏洞，以致得利用該漏

洞執行警察之監控措施。憲法訴願之背景係邦法授權警察機關採行電子通訊來源之監察，而藉由此類零日缺漏之幫助，其因此得以實施。

I.

[2]1. 邦立法機關於2017年12月8日生效之巴登—符騰堡邦警察法中新增第23b條（法律公報2017，第624頁），而其中之第2項即包括對系爭電子通訊來源監察之授權。於聲請憲法訴願後所通過之轉化歐盟第2016/680號指令於巴登—符騰堡邦之警察及修正於2020年10月6日所訂定其他警察法規之法律（法律公報第735頁），其於2021年1月17日施行，與此處相關之電子通訊來源監察權限部分，亦原封不動地規定於新的巴登—符騰堡邦警察法第54條第2項中。聲請人於2021年3月10日之書面聲明中，將其憲法訴願之標的轉換為新的巴登—符騰堡邦警察法第54條第2項。

[3]巴登—符騰堡邦警察法第54條於相關之各項中，規定如下：

巴登—符騰堡邦警察法第54條

電子通訊監察

（1）警察執行職務得於當事人不知情之情況下監控及記錄其電子通訊，

1. 其依據第6條或第7條應負責，避免對人民之生命、身體或自由、對聯邦或邦之存續或安全或對重要基礎設施或其他提供社區具直接意義之重要設施，造成急迫且重大之危害，
2. 於特定事實足資證明，其將於可預見之時間內，以至少於性質上屬具體之方式，針對第1款所提及之法益實施犯罪，且藉以達成，
   a）使民眾受到嚴重恐嚇，
   b）透過武力或武力威脅非法脅迫機關或國際組織，或
   c）消滅或嚴重影響國家或國際組織之政治、憲法、經濟或社會基本架構，

   且透過其行為或影響之形式，可能對國家或國際組織造成重大損害，
3. 其個別之行為顯現具體之可能性，其將於可預見之時間內，以至少於性質上屬具體之方式針對第1款所提及之法益實施犯罪，

且藉以達成，

a）使民眾受到嚴重恐嚇，

b）透過武力或武力威脅非法脅迫機關或國際組織，或

c）消滅或嚴重影響國家或國際組織之政治、憲法、經濟或社會基本架構，

且透過其行為或影響之形式，可能對國家或國際組織造成重大損害，

4. 於特定事實足資證明，其接收或傳遞旨在發送給或源自第1款所定人員之訊息，或

5. 於特定事實足資證明，第1款所定之人將使用其電子通訊連接或終端設備。

資料之蒐集，僅限於警察任務之履行，除此之外將可能無法達成或面對重大困難時，方得採行。若第三方將不可避免地受到影響，亦得進行資料蒐集。

（2）於當事人不知情的情況下，得透過以科技方法，侵入當事人使用之資訊科技系統，監控及記錄其電子通訊，若

1. 透過科技措施確保，僅監控及記錄正在進行之電子通訊，且

2. 為了監控及記錄電子通訊，特別是為了取得未加密形式之電子通訊，侵入乃屬必要。

（3）採取第2項所定措施時，必須確保

1. 對於資訊科技系統進行變更，僅限於因資料蒐集而不可免除時，且

2. 若科技上可行，於措施完成後，使所採行之變更自動回復。

應採行防護未經授權使用之方法。複製之資料應防護其免於遭受竄改、未經授權之刪除及未經授權之存取。

[……]

[4]2. 聲請人反對該電子通訊來源監察之權限，因其將導致為了進行監控，機關知悉但製造商未知悉之資訊科技系統中之安全漏洞，可能保持開放之結果，而此將可能導致來自第三方之攻擊。

[5]a）利用資訊科技系統中之安全漏洞係依據巴登—符騰堡邦警察法第54條進行電子通訊來源監察之數種可能方法之一。若要使此

類監控可行，必須使用監控軟體滲透目標系統。其以何種方式進行，於法律中並未規範。透過「物理」途徑進行滲透，應屬得以想像者。該軟體將於現場由調查人員安裝於目標系統中，例如秘密潛入住所、透過臥底調查人員潛入住所或於住所外於海關或交通檢查時。或亦可選擇透過遠端存取滲透目標系統。其得透過電子郵件附件之形式向目標人員傳送滲透軟體，後續經由該人開啟，或透過利用目標系統硬體或軟體中之安全漏洞來達成。相較於德國基本法第13條對於物理性進入住所之限制且以用戶有不當行為作為前提，後者之作法特別具備實務上之優勢。憲法訴願僅針對此種利用安全漏洞之類型。

[6]b）聯邦資訊科技安全局法（BSIG）第2條第6項，針對安全漏洞有法律上之定義：

聯邦資訊科技安全局法第 2 條

定義

[……]

（6）本法所稱安全漏洞，係指程式或其他資訊科技系統之屬性，利用這些屬性，第三方得違背有權者之意願，存取其資訊科技系統或影響資訊科技系統之功能。

[7] 安全漏洞得依據製造商是否已知悉（所謂之N日，因為製造商已經知悉一定之天數）或仍然尚未知悉（所謂之零日，因為製造商知悉之日數仍屬零），加以區別。從資訊科技安全（IT安全）之觀點而言，兩者有根本的差異，因為製造商就其知悉之安全漏洞得予以關閉，而就其尚未知悉之漏洞則僅得於執行其他更新之過程中偶然地將其關閉。以警察機關之角度而言其亦存在差異。只有當製造商儘管知道但尚未提供更新或此類更新通常不再發生時，N日缺漏方得用於滲透目標系統。此外，如果製造商已提供更新但受影響之用戶尚未安裝，則N日缺漏仍可能被利用。另一方面，零日缺漏則很容易被用來滲透目標系統，因為製造商欠缺對相應缺漏之掌握而無從開發及提供關閉漏洞之更新。

II.

[8] 聲請人透過提請憲法訴願對巴登—符騰堡邦警察法第54條第2項之規定表示反對。其核心之主張認為，該權限危及資訊科技系統

之機密性及完整性，因機關並沒有興趣向製造商通報其所知悉之漏洞，因其得以利用這些安全漏洞滲透資訊技術系統，以用於巴登—符騰堡邦警察法第54條第2項所允許採行之電子通訊來源監察。

[9] 聲請人於2018年12月7日聲請憲法訴願，並於2021年3月10日補充書面聲明，指控受基本權保障之資訊科技系統之機密性和完整性遭到侵害。其並未明確抨擊巴登—符騰堡邦警察法第54條第2項，因國家透過此授權而侵害其基本權。而是指摘巴登—符騰堡邦透過導入電子通訊來源監察之權限，違反了基本權客觀法律層面之保護義務。此種保護義務係獨立於電子通訊來源監察之權限而存在。然而，導入該權限導致與其相關風險之增加，且使得制定保護資訊科技系統之具體法律要求有其必要。透過巴登—符騰堡邦警察法第54條第2項，立法機關鼓勵警察機關不通報安全漏洞——而其亦為犯罪份子或外國情報機構所感興趣者。對於安全性研究亦存在不向製造商通報所知悉缺漏之誘因，以便得將其出售給機關。因此，巴登—符騰堡邦警察法第54條第2項導致了危害，而立法機關依據憲法有義務避免之。

[10] 該邦未能制定缺漏管理之強制性配套法規，特別是必須禁止使用存在於製造商尚未知悉存在於相關系統之安全漏洞。即便不認為利用零日缺漏與國家之保護義務完全不相容，仍應訂定行政程序——並考量基本權之關聯性，透過制定法予以規範——經其授權之機關應就其已知悉之安全漏洞，依據其重要性進行檢查及分類，以立於此基礎上決定如何處理漏洞。此外，國家必須採取預防措施，防止其對於安全漏洞之認知遭第三方竊取。迄今為止，巴登—符騰堡邦之機關尚未提出得適用於電子通訊來源監察之評估缺漏之程序，也沒有任何得據以決定向製造商通報相關缺漏之程序及標準。

[11] 系爭規範直接影響聲請人，因為其未得採取任何進一步之行動。因為沒有必要針對他們採取任何進一步的行動。其受影響之處，正是來自國家對其資訊科技系統提高危險之結果，因為警察因巴登—符騰堡邦警察法第54條第2項而未向相關程式之製造商報告其所發現之安全漏洞。不能要求其提出特定、被國家保密之缺漏以證立其憲法訴願之合理性，因為其無從得知機關已知悉之具體缺漏。無論巴登—符騰堡邦之警察目前是否確實取得或蒐集零日缺漏，危害之情況皆存

在。具決定性者，係其利用此缺漏——例如透過其他單位所提供之研究軟體，這些缺漏即屬其中之一部分。僅是藉此，即會促使不向製造商報告缺漏。

III.

[12]1. 聯邦政府認為，即使考慮與資訊科技系統缺漏相關之危害，德國維護資訊科技安全及資料保護之現行監管體系仍屬充足。電子通訊來源之監察係以保護極其重要之其他法益為目的，其與確保最大可能之資訊科技安全之目的間所產生之緊張關係，應於立法機關之形成範圍內，以最大程度保護所有受影響之法益，予以解決。一方面，資訊科技系統中之缺漏會產生危害，此亦為原則上應致力於儘可能降低開放性缺漏數量之原因。另一方面，若滲透無法透過其他方式達成，則在不利用缺漏之情況下，電子通訊來源監察之法定權限往往無法執行，甚至是遭到架空。然而，作為危害防止之一種手段，電子通訊來源監察之必要性與日俱增，因端對端之加密益發普遍地被使用，以避免犯罪及通訊工具遭刑事追訴機關及安全機關存取。

[13]2. 內政、數位化暨移民部代表巴登—符騰堡邦政府表示意見。其認為憲法訴願無理由。於此並未具有制定進一步保護性法規之憲法上義務，因為巴登—符騰堡邦警察並未專門取得或蒐集與屬預防性警察之電子通訊來源監察相關之零日安全漏洞。無論如何，現有之法規體系及其他保護措施係屬適當且充分，足以消解電子通訊來源監察之負面結果，並有效防止利用此類缺漏對資訊技術系統進行犯罪性之攻擊。

[14]透過基本權之保護義務並未導出警察向軟體製造商報告缺漏之義務。確保資訊科技之安全並防止未經授權存取資訊科技系統，主要是軟體製造商及供應商之責任，為此其亦有可觀之支出。憲法上並未要求，透過訂定向製造商報告之法定義務，將系統安全之部分責任轉移給警察。另外尚應考慮，電子通訊來源監察之權限有助於在重要法益受到特別緊急或重大威脅之情況下，完成警察之危害防止任務。由於電子通訊採用端對端加密之情形與日俱增，若缺乏電子通訊來源監察之權限，則一般預防性電子通訊來源監察之權限也逐漸被架空。確保資訊科技安全及履行警察之法定任務間可能存在之目的衝突，並

不會因此產生立法之行動需求。由於單純使用尚未知悉之安全漏洞並不會危及資訊科技安全，因此沒有理由立法禁止或制定限制使用此類安全漏洞或課以向製造商報告義務之法規。

[15]制定進一步之法律規定，亦不具有憲法上之必要性，因有為數眾多之法規皆保護資訊科技系統免受第三方未經授權之存取。巴登—符騰堡邦警察法第54條之規定——特別是巴登—符騰堡邦警察法第54條第3項第2句——確保電子通訊來源監察之實施不會提供第三方取得相關系統或警方已知悉安全漏洞之機會。除此之外，防止第三方利用尚未知悉之安全漏洞並操縱資訊科技系統之犯罪行為，係屬警察之任務，因此若其已知悉相應之安全漏洞，依據巴登—符騰堡邦警察法第3條，依其合義務性之裁量採行必要之措施。警察於巴登—符騰堡邦警察法第1、3及5條之範圍內進行危害分析時，應考慮安全漏洞之散布及影響，以及採取對應措施及技術解決方案來關閉漏洞之可能性，該漏洞被第三方發現之可能性，以及最後是利用該漏洞進行犯罪可能造成之損害。進一步之法律規定並不會產生附加價值。此外，國家亦透過刑法保護這些系統免受私人攻擊。在資料保護法制部分，應特別關注轉化歐盟第2016/680號指令（JI指令）第29條之巴登—符騰堡邦警察法第78條中維護資料處理安全之規定。

[16]邦政府進而提及了聯邦資訊科技安全局之任務。致力改善網路安全之巴登—符騰堡邦法律草案——於此期間已通過（見下Rn.63）——，該草案亦有助於改善網路安全。隨後，邦機關「巴登—符騰堡邦網路安全辦公室」將會成立。其主要任務之一即是於所有巴登—符騰堡邦之網路安全事務中推動一個集中協調及通報點，以促進公法單位間之合作。

[17]3.聯邦資料保護暨資訊自由監察官認為，系爭法律條款不符合保護資訊科技系統免受第三方侵害的憲法上要求。資訊科技系統中之安全漏洞——特別是製造商尚未知悉之安全漏洞——對通訊之機密性及人民之隱私構成巨大之潛在威脅，因為存在著被第三方試探張望之危險。若法律欲允許安全機關利用安全漏洞，其亦應就細節予以規範。就此涵蓋例如，允許安全機關「儲存」關於安全漏洞資訊之範圍，或將資訊傳遞予相關製造商或聯邦資訊科技安全局之義務。這些

要求並未被滿足。

[18]4. 巴伐利亞邦資料保護監察官與聲請人具有相同之憲法上思考。保護措施之憲法上必要性亦來自於，公部門自身於法制上引導非公部門在資訊科技系統之安全水準。若國家單位證明資訊科技系統具有充分之安全水準，然而警察卻利用尚未知悉之安全漏洞進行滲透，則其可能會出現矛盾。此種緊張關係應該透過足夠明確且具體之法規予以化解。其必須針對滲透目標系統之前提要件以及獲取及保留關於至今一般尚未知悉之安全漏洞資訊之限制，充分並明確地說明。

[19]5. 萊茵蘭—伐爾茲邦之資料保護監察官亦主張，巴登—符騰堡邦警察法之規定對於資訊科技系統之一般性保護並未包含充分具體之法律上要求。基本權之保障因具開放性之零日安全漏洞所帶來之危害，並未受到充分有效之維護。針對要求關閉安裝軟體所使用之安全漏洞，或一般性地要求對與集體資訊科技安全相關措施之影響進行評估，均欠缺規範。

B. 合法性

[20] 憲法訴願不合法，因為違反現行保護義務之可能性尚未得到充分闡明，且因其不符合廣義之補充性要求。

I.

[21] 聲請人原則上得作為基本權之主體，因此具備聲請人之資格。此亦適用於聲請人5至7，其作為依民法登記之社團（參照 BVerfGE 3, 383 <390>；10, 221 <225>；24, 278 <282>；97, 228 <253>；105, 279 <292f.>）、登記之合作社（參照BVerfGE 118, 168 <168, 203>）及公司（參照BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 2. September 2002 - 1 BvR 1103/02 -, Rn. 6），因此屬德國基本法第19條第3項所稱國內法人，而得作為基本權主體。法人原則上得主張適用於聲請人之資訊科技系統保密性及完整性之基本權保障，惟限於非以德國基本法第1條第1項為其依據之範圍。（參照 Drallé, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 68 ff.；Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 153；Gersdorf, in: BeckOK InfoMedienR, 30. Ed. 1. August 2019, GG, Art. 2

Rn. 33）。其保護需求於此與自然人相似。然而，不同之處在於，法人之行為範圍與自然人不同，其通常受到特定目的之限制。確認基本權保障時，必須考慮自然人及法人於保護需求之差異（參照 entsprechend zum Recht auf informationelle Selbstbestimmung BVerfGE 118, 168 <203 f.>；128, 1 <43>；vgl. zu Art. 10 Abs. 1 GG BVerfGE 100, 313 <356>；106, 28 <43>；107, 299 <310>）。

II.

[22] 憲法訴願具備可受理之訴願標的。聲請人直接針對巴登—符騰堡邦警察法第54條第2項聲請憲法訴願。此侵害其基本權，因其允許利用這些系統中製造商尚未知悉之缺漏，利用科技方法對資訊科技系統進行干預，且無須事先向製造商通報。其亦主張，立法機關未配合巴登—符騰堡邦警察法第54條第2項，引入法律上之缺漏管理程序作為個別情況下安全漏洞之評估，從而侵犯其基本權。聲請人將此二者皆立論於維護資訊科技系統機密性及完整性之基本權保護面向上。其認為立法機關未能訂定相應之配套法規而違反其保護義務。因此，其訴願係針對依其觀點所認為對基本權不充分之法律上規定。此應屬合法（參照 zuletzt BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 95 - Klimaschutz）。

III.

[23] 於此與JI指令中歐盟之資料保護法制之相關規定，與憲法訴願之合法性並未衝突。無論是系爭條款本身，或是遭聲請人批評有缺漏之規範組成，均非完全由歐盟法律決定（參照 BVerfGE 121, 1 <15>；125, 260 <306 f.>；130, 151 <177 f.>；133, 277 <313 f. Rn. 88>；152, 152 <168 Rn. 39>；152, 216 <233 Rn. 42 f.>；154, 152 <214 f. Rn. 84>；155, 119 <165 Rn. 87>）。

IV.

[24] 德國聯邦憲法法院法第93條第3項所定聲請憲法訴願之1年期限有被遵守。其適用於2018年12月7日聲請之憲法訴願，最初係針對2017年12月8日生效之舊巴登—符騰堡邦警察法第23b條第2項。聲請人於2021年3月10日亦及時將憲法訴願轉為針對2021年1月17日生效之新巴登—符騰堡邦警察法第54條第2項（參照 dazu BVerfGE

155, 119 <158 Rn. 67>）。

V.

[25] 然而，聲請人並未相應闡明其符合德國聯邦憲法法院法第23條第1項第2句及第92條之要求，而有權提出憲法訴願之聲請。依據德國基本法第93條第1項第4a款及德國聯邦憲法法院法第90條第1項規定，合法之憲法訴願之前提要件為，聲請人主張其基本權或相當於基本權之權利受到公權力之侵害，且其至少顯得有可能（參照BVerfGE 79, 1 <13 ff.>；83, 216 <226>；83, 341 <351 f.>；129, 49 <67>）。其對於憲法訴願仍有不足。更進一步而言，尚須存在基本權之保護義務（1），且聲請人已充分闡明其自身基本權現時且直接受到影響（2）。然而，本憲法訴願並未充分證明保護義務可能遭到違反（3）。

[26]1. 為了保護基本權，國家對於資訊科技系統之安全負有責任。在此須判斷之情形中，機關已知悉製造商尚未知悉之安全漏洞，則國家負有保護基本權之具體義務。其有義務保護資訊科技系統之使用者免於受到第三方對此系統之攻擊。

[27]a）於此受到影響者為，秘密通訊及維護資訊科技系統機密性及完整性之基本權。

[28] 若第三方取得正在進行中之電子通訊內容及情況，則涉及受德國基本法第10條第1項保護之通訊秘密（參照BVerfGE 120, 274 <307>；141, 220 <309 Rn. 228>）。

[29] 除此之外，資訊科技系統之滲透涉及德國基本法第2條第1項結合第1條第1項所導出維護資訊科技系統機密性及完整性之基本權（參照BVerfGE 120, 274 <307 ff.>）。系爭規定授權主管機關僅就進行中之電子通訊過程採行電子通訊來源監察（參照巴登—符騰堡邦警察法第54條第2項第1款），因此國家基於巴登—符騰堡邦警察法第54條第2項所為侵害於此範圍內應依據德國基本法第10條第1項為衡量。然而，若第三方透過尚未知悉之安全漏洞侵入系統，不僅是進行中之電子通訊，甚至全部資訊科技系統及其資料集均可被其存取。其得進行刺探、操縱並透過操縱進行勒索，特別是以銷毀資料為威脅。

[30]b）涉及各基本權之保護面向，從而導出國家負有具體之基本權保護義務。

[31]aa）依據德國聯邦憲法法院持續之判決，基本權之保障內涵不僅限於其防禦功能，同時亦包括憲法之客觀價值決定，而可據其得出國家保護義務之正當性（參照BVerfGE 39, 1 <42>；stRspr）。

[32]德國基本法第10條第1項除作為防禦權外，尚委託國家保護人民不受來自私人之第三方，對受秘密通訊保障之通訊造成之侵害（參照BVerfGE 106, 28 <37>；zur Schutzdimension des Grundrechts auf informationelle Selbstbestimmung BVerfG, Beschluss der 3. Kammer des Ersten Senats vom 17. Juli 2013 - 1 BvR 3167/08 -, Rn. 19 f.；zur Ausstrahlungswirkung in das Privatrecht BVerfGE 152, 152 <189 ff. Rn. 85 ff.> - Recht auf Vergessen I）。

[33]受基本權保障之資訊科技系統之保密性及完整性具有之保護面向。特別在於，基本權上顯著之保護需求係來自於對資訊科技系統使用之依賴，以藉此實現自由及一般人格發展，以及與此使用具備關聯之人格威脅（參照bereits BVerfGE 120, 274 <306>）。法庭已於2008年更詳細地解釋了受基本權保護之發展自由於此期間極為仰賴資訊科技之使用（a.a.O., S. 303 ff.）。此後，發展自由與資訊科技間之連結變得更加緊密。由早期類比過程邁向數位過程之轉換，及非最終之不斷擴張之資訊科技系統之行動化使用，皆持續增加對資訊科技之依賴。每個人愈來愈無法在不使用資訊科技系統之情況下實現其基本自由，也愈來愈無法透過放棄使用資訊科技系統來避免因此所產生之危險。於此背景下，基本權不僅要求國家本身尊重對此類系統應具備完整性及保密之合法期待（參照BVerfGE 120, 274 <306>）。國家更負有義務，促進資訊科技系統之完整性及機密性，使其免於遭受第三方之攻擊（siehe auch Petri, DuD 2008, S. 443 <446 f.>；Roßnagel/Schnabel, NJW 2008, S. 3534 <3535>；Hoffmann-Riem, AöR 134 <2009>, S. 513 <533 ff.>；Gudermann, Online-Durchsuchung im Lichte des Verfassungsrechts, 2010, S. 228 f.；Kutscha, DuD 2012, S. 391 <393 f.>；Schulz, DuD 2012, S. 395 <396>；Kutscha/ Thomé, Grundrechtsschutz im Internet, 2013, S. 60 f.；Schliesky/Hoffmann/

Luch/ Schulz/Bor-chers, Schutzpflichten und Drittwirkung im Internet, 2014, S. 107 ff., S. 115 f.；Heinemann, Grundrechtlicher Schutz informationstechnischer Systeme, 2015, S. 209 ff.；Derin/Golla, NJW 2019, S. 1111 <1114 f.>；Poscher/Lassahn, in: Hornung/ Schallbruch <Hrsg.>, IT-Sicherheitsrecht, 2021, § 7 Rn. 40 ff.）。

[34]bb）若國家知悉製造商及使用者均尚未知悉之安全漏洞，一般保護之委託就會增強為具體之基本權上義務，以保護資訊科技系統之使用者免於遭受第三方透過尚未知悉之安全漏洞滲透到使用中之系統（1）。國家這項具體之基本權保護義務，並不排除利用尚未知悉之保護漏洞進行電子通訊來源監察之可能性。然而，其須透過法規解決目前程序中所存在之目標衝突，一方面防止第三方之滲透，另一方面藉由尚未知悉之保護漏洞進行電子通訊來源監察之可能，以達到危害防止之目的（2）。

[35]（1）若國家之機關已經知悉安全漏洞，國家之一般保護委託即會強化為具體之基本權保護義務（參照entsprechend zu Art. 2 Abs. 2 Satz 1 GG BVerfGE 142, 313 <338 Rn. 71>）。這項具體之保護義務係基於安全漏洞潛在之高危險及損害（a），相關人欠缺自我保護之可能（b）及機關已知悉安全漏洞（c）。

[36]（a）若安全漏洞維持開放，資訊自決即會面臨特別之危害。資訊科技系統開啟廣泛之使用可能性，所有皆與資料之產生、處理及儲存相關。任何取得資料之人，皆得獲取與使用者人格相關之廣泛認識（näher bereits BVerfGE 120, 274 <305 f.>）。若複雜之資訊科技系統在技術上遭滲透，透過滲透已克服刺探整個系統並獲取如此廣泛資訊之決定性障礙（參照BVerfGE 120, 274 <308 f.>）。

[37]由於資訊科技系統之廣泛使用及對此使用之普遍依賴，安全漏洞還可能造成遠超出個人相關資訊外洩之潛在損害——例如在企業營運及商業。若第三方透過安全漏洞攻擊資訊科技系統並對其進行操縱，則可能會破壞各種不同形式之流程，從而造成相關人之損害。第三方滲透之風險也與特定之勒索危險相關。

[38]此危害相當大，因為可能存在許多未被發現之缺漏。聯邦資訊科技安全局建議，始終假設所使用之軟體包含漏洞

（„Assume-Breach-Paradigma“，參照Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2017, S. 18；Die Lage der IT-Sicherheit in Deutschland 2019, S. 8；Die Lage der IT-Sicherheit in Deutschland, 2020, S. 22 ff., 34, 44 f., 79, 81）。

[39]（b）面對利用製造商尚未知悉且因此無法透過更新系統來關閉之零日缺漏，個人通常無法有效地保護自己免於遭受危害。有一部分甚至完全無法察覺到此種攻擊，但無論如何，其僅得於有限之程度上進行防禦（參照BVerfGE 120, 274 <305 f.>）。

[40]（c）同時，正是主管機關對於此處待判斷之情形意識到存在安全漏洞，而因此能糾正之。聲請人並未提出如機關應積極尋找安全漏洞之主張。反之，其呼籲以保護基本權之方式處理機關已知悉但製造商尚未知悉之漏洞。即僅有機關已知悉安全漏洞之情形方具疑義；不論其係自行發現或是從第三方獲知。正是出於此一認知及製造商同時尚未知悉及相關人欠缺自我保護可能性，國家之特別保護義務由此而生（參照auch BVerfGE 142, 313 <338 f. Rn. 73> zu Art. 2 Abs. 2 Satz 1 GG）。

[41]（2）於此所稱之保護義務包括立法機關有義務規範警察機關如何處理製造商尚未知悉之安全漏洞。

[42]若未授權電子通訊來源監察，機關可能因此沒有興趣利用安全漏洞滲透資訊科技系統，則其會定期向製造商通報其所發現之漏洞，以履行基本權之保護義務，而製造商因此得以關閉漏洞。然而，若機關被授權基於危害防止之目的進行電子通訊來源監察，則會產生目標之衝突，一方面，係為確保資訊科技系統最大安全性之公共利益，另一方面，則是為保護其他重要法益而保持電子通訊來源監察之可能性。以結果而言可能存在著機關不作為之危險，其既不鼓勵關閉漏洞或甚至積極確保漏洞維持尚未知悉之狀態（參照bereits BVerfGE 120, 274 <326> zur Online-Durchsuchung）。同時，單單國家監察權限之存在，即可能會成為第三方不向製造商報告其所知悉安全漏洞之誘因，反而以提供此資訊向國家機關索取報酬。其提升了不向製造商報告安全漏洞之危害。

[43]由於這些對資訊科技系統安全之危害，透過使用尚未知悉之

安全漏洞進行電子通訊來源監察因此須具備更高之正當性要求，但其並非憲法自始所不許（參照 bereits zur Online-Durchsuchung BVerfGE 120, 274 <325 f., 328>；141, 220 <304 f. Rn. 211 f.>）。維護資訊科技系統機密性及完整性之基本權並未因此產生完全禁止透過使用尚未知悉之安全漏洞進行電子通訊來源監察之請求權。其亦無法作為請求課以機關針對任何尚未知悉之安全漏洞立即且無條件向製造商通報義務之依據。

[44] 然而，基本權之保護義務要求訂定法規，針對機關於決定是否維持尚未知悉之安全漏洞時，一方面提供必要之保護以防止第三方滲透，另一方面保持電子通訊來源監察之可能性，解決其間之目標衝突。當機關知悉零日保護漏洞時，應於個案中權衡對立之利益。必須確保者為，機關每次決定讓尚未知悉之安全漏洞保持開放時，一方面確認該安全漏洞資訊進一步散布所造成之危害，另一方面利用漏洞之可能機關滲透之數量及質量，並將兩者依比例衡量，若保持安全漏洞開放之利益並未大於關閉安全漏洞，則向製造商通報安全漏洞。

[45]2. 聲請人已指明，此保護義務之違反，將使其自身直接且現時受到影響。

[46] 其闡明，其自身受到影響，係因其所使用之資訊技術系統，可能存在尚未知悉之漏洞，且因此可能會遭第三方循此路徑予以滲透。眾多人民可能面臨此種危險。然而，沒有進一步個別化之必要。於憲法訴願之程序中，一般並未要求聲請人自身受影響之程度相較於一般人受影響程度，須具有超越一般人之特別影響（參照 BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 110 - Klimaschutz）。

[47] 聲請人目前亦直接受到影響。系爭規定直接造成了（犯罪上）利用未通報安全漏洞之風險，因無須藉由授權進行電子通訊來源之監察。聲請人表示反對，巴登—符騰堡邦警察法第 54 條第 2 項直接提高了危害，若機關沒有此監察之權限，則應會向製造商通報並由其關閉漏洞，而現在則不會進行通報，且因此可能繼續遭第三方利用。此與邦政府主張，目前尚未取得或蒐集與預防性警察之電子通訊來源監察有關之缺漏，並不衝突。因其並不表示，已經偶然或透過其他

（公法）單位取得，而依據巴登—符騰堡邦警察法第54條第2項尚未向製造商通報之相關缺漏資訊不存在。

[48]3. 然而，聲請人並未充分闡明，基本權之保護義務可能遭到違反。

[49]a）一方面是透過基本權所衍生出對國家侵害之主觀防禦權，另一方面是由於基本權之客觀意義而產生之保護義務，兩者之間存在著本質上之差異，因為防禦權從目標和內容而言禁止特定之國家行為，而保護義務原則上則未特定。保護概念之確立及規範之轉化係屬立法機關之權責，即使立法機關基本上有義務採取措施保護法益，其原則上仍保有評估、評價及形成之空間。其亦留有空間，以關注相互競合之公益及私益（參照BVerfGE 96, 56 <64>；121, 317 <356, 360>；133, 59 <76 Rn. 45>；142, 313 <337 Rn. 70>；stRspr）。

[50]僅有在完全未採取保護措施，相關法規及所採取措施明顯不適當或完全難以達成所需之保護目標，或顯著低於保護目標之情況下，德國聯邦憲法法院方得認其違反保護義務（so zu Art. 2 Abs. 2 Satz 1 GG zuletzt BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 152 m.w.N. - Klimaschutz；stRspr）。因此，關於需要採取何種措施以提供保護之決定，僅得於憲法上進行有限度之審查。僅有在特殊情況下，立法機關之形成自由方得被限縮到只能透過具體措施來履行保護義務之程度（參照BVerfGE 56, 54 <73 ff.>；77, 170 <214 f.>；79, 174 <202>；142, 313 <337 f. Rn. 70 f.>）。

[51]確立立法機關違反保護義務之要求與聲請人之特別闡明負擔有關。聲請人之基本權受到侵害之可能性，一般係由陳述中得知，僅有當其不限於籠統之主張並逐一詳細指摘法律狀況中之不足之處時，方得成立。進而有必要整體掌握法律上規定之關聯性，於此——依據個案情情況——至少包括，闡明系爭規定屬不充分而受批評之規範整體，並說明為何主張立法上理念之失敗。

[52]透過本庭就氣候保護法所作成之裁判，並不會產生不同結果。其中雖指出，聲請人無須查明所有相關措施以作為憲法訴願權能之理由。然而，於此並不適用，因立法機關本身已經制定了一項總結

性之規定，而得將聲請人之指摘限於此（參照BVerfG, Beschluss des Ersten Senats vom 24. März 2021 - 1 BvR 2656/18 u.a. -, Rn. 134）。其與此之情況不同。

[53]b）憲法訴願不符合前述闡明之要求。有不同之法律規定用以保護資訊科技系統，其——儘管不能於此進行最終憲法上評估——於當前背景下仍可能具重要性。聲請人於憲法訴願中針對現行法規既未闡述其基本原則，亦未說明該規定失敗之具體理由。儘管其於2021年3月10日之意見陳述中對此進行補充，但這並非意味著，違反保護義務之可能性已經得到充分闡明。

[54]aa）首先，授權基礎本身包含立法機關基於「保護資料安全且關注來自第三方之侵擾」之目標，所規定之各種保護措施（LTDrucks 16/2741, S. 31）。無論如何，聲請人應提及巴登—符騰堡邦警察法第54條第3項第2句，依據該規定，應採行防護未經授權使用之方法。其並未顯然排除，該規定具有解釋之空間，以適當解決規範適用層面所遭遇，存在於成功存取之公益及資訊科技系統最大可能之安全性間之目標衝突。

[55]值得思考者為，巴登—符騰堡邦警察法第54條第3項第2句中所稱「方法」係指滲透軟體，而非指其引入使用之安全漏洞，因為該漏洞無關乎警察之行為而存在於目標系統中。然而，巴登—符騰堡邦警察法第54條第3項第2句亦可能以法律專業為另一種解釋，認經利用之缺漏亦為「使用之方法」之要件所涵蓋。此可能造成，其——例如透過向製造商通報——必須保護免於遭受未經授權之使用。就此聲請人雖於2021年3月10日之補充書面聲明中有非常簡短地闡述。然而，當時憲法訴願之期限已過，因此該陳述並未遵守憲法訴願及提交理由之期限（參照BVerfGE 145, 20 <52 Rn. 79>）。其亦非屬就先前已經充分說理且因此受理之憲法訴願所為之單純補充（參照dazu BVerfGE 127, 87 <110>）。

[56]bb）一方面機關對電子通訊之存取權限及另一方面資訊科技系統最大可能安全性所欲維護之公益間之目標衝突，亦可能指向資料保護影響評估之範圍。此規定於巴登—符騰堡邦警察法第80條中，其係增訂於2020年10月6日之轉換JI指令第27條之修正法律中。巴

登—符騰堡邦警察法第80條規定如下：

巴登—符騰堡邦警察法第 80 條

資料保護影響評估

（1）若特定形式之處理，特別是在使用新科技時，考量處理之性質、範圍、情況及目的，可能會對當事人之法益帶來高度風險時，則警察必須就此預計處理過程對當事人之影響進行事先評估。

（2）針對具有類似高潛在危害之多個類似處理過程之調查，可以進行共同影響評估。

（3）影響評估必須考慮因處理受影響之當事人之權利及正當利益，並應包括至少以下之內容：

1. 針對所計畫之處理過程及處理目的之系統化說明，
2. 評估處理過程與其目的相關聯之必要性及合比例性，
3. 對當事人法益危害之評估，以及
4. 應有助於解決現存危害之措施，包括確保個人資料保護並證明遵守法律要求之安全預防措施及程序之保證。

[57] 聲請人就此並未有所著墨。其於此並不會因為巴登—符騰堡邦警察法第80條中關於資料保護影響評估之規定，係於聲請憲法訴願後且於憲法訴願期限過後方制定，而屬於可以被忽略者。若憲法訴願期限屆滿後事實及法律情況發生變更，聲請人必須補充提交資料（參照BVerfGE 106, 210 <214 f.>）。其特別適用於，當其主張違反保護義務，且於憲法訴願期限屆滿後，有可能得履行此保護義務之新法律生效之情形。此外，於憲法訴願時，立法機關已經有義務根據JI指令第27條之規定採行資料保護影響評估，因此聲請人必須於其轉化至邦法前，先針對此歐盟法律之規定進行研究。

[58] 於零日安全漏洞保持開放之情況下，是否應採行此種影響評估，似非無疑。毫無疑問者為，於導入監控軟體前，必須依據巴登—符騰堡邦警察法第54條第2項採行資料保護影響評估。較不明確者為，其是否亦適用於機關就已知悉之安全漏洞而未向製造商通報並從而保持其開放之決定。然而，就此JI指令第27條得以說明，其透過巴登—符騰堡邦警察法第80條予以轉化，並規定如下：

JI 指令第 27 條
資料保護影響評估

（1）若處理之形式，特別是在使用新科技時，考量處理之性質、範圍、情況及目的，而可能會對自然人之權利或自由帶來高度風險時，則成員國應規定管控者必須就預計採行之處理過程對個人資料保護之影響進行事先評估。

（2）依據第 1 項所採行之影響評估應考慮資料處理之當事人及其他相關人之權利及法益，並應至少包括欲採行處理過程之一般性說明及關於當事人權利及自由所存在風險之評估，以及預計採行之補救措施、保障、安全預防及程序，藉此確保個人資料之保護並作為遵守本指令之證明。

[59]JI指令第27條可能提供了巴登—符騰堡邦警察法第80條一種解釋，除針對受到具體處理過程（於此係指電子通訊來源監察措施）之直接或間接影響者之法益風險外，亦應將（未涉及之）他人之風險納入考量。JI指令第27條第1項一般性地提及自然人權利及自由之風險，而JI指令第27條第2項則區分了受資料處理影響之當事人及其他相關人，由此可知，雙方之權利及法益皆應納入影響評估。

[60]然而，仍有疑義者為，維持安全漏洞之開放是否屬巴登—符騰堡邦警察法第80條第1項所指「處理過程」（關於「處理」之構成要件參照巴登—符騰堡邦警察法第12條第2款）。其至少並未排除，將處理過程理解為一體之生活事實，其並非始於真正進行電子通訊來源監察期間提取資料時，而是於此之前即已存在之準備步驟中即已展開。維持機關已知悉安全漏洞之開放，得被視為電子通訊來源監察之準備步驟，因此有巴登—符騰堡邦警察法第80條之適用。此處遭第三方利用安全漏洞滲透資訊科技系統而產生之重大危害，是否亦屬巴登—符騰堡邦警察法第80條第1項所稱處理過程之「後果」（即保持安全漏洞之開放），仍需要進一步釐清。

[61]聲請人並未處理這些疑義。德國聯邦憲法法院之任務並不在於獨立地指引專業法制，針對被視為保護規範之法規應在何種程度上，被解釋為符合基本權之保護委託或實屬欠缺。

[62]德國聯邦憲法法院依據歐盟運作條約第267條所提交之意見

書可以釐清有關歐盟法中影響評估法規（JI指令第27條）之解釋問題，但此於本憲法訴願程序中並未被考慮。其雖有適用，但因憲法訴願不受理，故該問題因此對判決不具重要性。此外，即使JI指令第27條不要求對零日安全漏洞進行影響評估，亦不會與巴登—符騰堡邦警察法第80條之廣泛解釋產生衝突（參照JI指令第1條第3項）。即使憲法訴願被受理，JI指令第27條之解釋對德國聯邦憲法法院之裁判亦不具重要性。

[63]cc）聲請人亦未充分闡明巴登—符騰堡邦之網路安全法制中所包含保護條款之程度。2021年2月17日生效之強化網路安全及修訂其他法規法（GBl 2021, S. 182,於下簡稱：網路安全法<CSG>）生效。該法規定設立巴登—符騰堡邦網路安全機構（參照網路安全法第1條第1項、第3條）。其被賦予作為巴登—符騰堡邦公務單位間，就網路安全事務共同合作之集中協調及通報單位（參照網路安全法第4條第1項），特別是針對防止網路安全危害所必要之所有資訊，包括安全漏洞，進行蒐集及評估（參照網路安全法第4條第2項第1款）。透過網路安全法，從2022年1月起，邦機關亦負有向網路安全機構報告安全漏洞之義務（參照網路安全法第4條第3項），並授予網路安全機構防止網路安全危害之權限（參照網路安全法第5條）。網路安全機構亦得向公眾或相關群眾發布關於安全漏洞之警告、建議及資訊——通常是在事先聽取製造商之意見後（參照網路安全法第8條第1項）。

[64] 網路安全法雖係於聲請憲法訴願後且於憲法訴願期限經過後方生效，就此而言，憲法訴願中之論述仍非屬於可以被忽略者（oben Rn. 57）。聲請人於2021年3月10日之補充書面聲明中就網路安全法所提出之意見，雖因該法於2021年2月17日始生效，因此聲請人無法於憲法訴願期限內提交其意見，故應予以考慮。但就此而言，其論述仍未達到正當性之要求。為了說明違反保護義務之可能性，有必要對整體保護措施進行分析；從中選擇性地擇取單一，可能不充分之法規並不足夠。然而，最重要的是，聲請人並未解釋相關規定是否得解釋為，具備憲法上充分保護基本權免於遭受第三方對資訊科技系統攻擊之問題。

[65]dd）最後，聲請人並未提及法律之外就通報標準之規定。在關於建立資訊科技計畫委員會之契約及關於聯邦及各邦行政導入資訊科技之共同合作基礎——實施德國基本法第91c條之契約（IT-Staatsvertrag in der Fassung der Bekanntmachung vom 13. Dezember 2019, BGBl I S. 2852）生效後，資訊科技計畫委員會於2017年10月5日通過了「針對資訊科技安全事故於行政電腦緊急因應團隊——聯盟（VCV）中交換資訊之具約束力通報程序——（通報標準）」（Nr. 2017/35）。藉此已決議將聯邦及各邦之資訊交換作為資訊科技國家契約第3條第1項（現為第2條第1項）所稱具有拘束力之資訊科技安全標準（參照資訊科技國家契約第2條第2項第2句），資訊科技安全之事故，無法排除其影響僅限於各邦及聯邦或預估亦關係到其他國家之資訊科技安全事件，必須通報（§ 2 Abs. 1 des Beschlusses）。該通報向聯邦資訊科技安全局為之。資訊科技產品中之新型安全漏洞亦屬於通報義務之範圍（參照§ 2 Abs. 2 in Verbindung mit Anlage 1 des Beschlusses）。依據該決議第3條，聯邦及邦均負有報告義務。在這方面，似乎可以想像，聯邦資訊科技安全局在決定進一步處理此類資訊，行使裁量權時——特別是在依據聯邦資訊科技安全法第7條第1項第1句第1款第a目之規定，向公眾或相關群眾發布關於資訊科技系統中安全漏洞之警告及製造商之資訊——可以而且應該考慮到基本權保護義務之履行。

[66]基本權之保護義務於多少程度上得透過法律外所規範之通報義務而履行，以及此標準化之法律依據是否足夠，仍需要進一步檢證。由於所採用之通報標準可能屬整體法規中防止第三方未經允許使用缺漏之其中一部分，因此聲請人亦應於就此提出說明。

VI.

[67]此外，憲法訴願不合法，因其並未符合廣義補充性之要求。

[68]1.a）補充性之要求並不僅限於採取正式且開放之法律方法以實現該程序之直接目標，而是要求使用一切得以補救其主張受侵害基本權之方法。其係為確保德國聯邦憲法法院無須基於不確定之事實及法律基礎上作成影響深遠之裁判，而其主要是由負責普通法解釋及適用之專門法院先處理事實及法律之情況。

[69] 因此，補充性原則原則上要求，於聲請憲法訴願前採取所有足資運用之程序上選擇，以糾正所指摘違反憲法之行為或防止基本權之侵害。當對於是否允許在具體案件中以合法方式採取相應之法律救濟，存有疑問時，亦有其適用。

[70] 若憲法訴願係直接針對法律提出，則提起確認或不作為訴訟應屬得事先採行之法律救濟措施。但其本身並未排除，即使法規已經最終確定，而專門法院之審查所能得出之最有利之結果，乃依據德國基本法第100條第1項將系爭法律提交至德國聯邦憲法法院。於此之關鍵同樣在於，為避免德國聯邦憲法法院在不確定之事實及法律基礎上作成裁判，是否有由專門法院予以釐清之必要。通常會出現此種情況，即系爭規定中若有需要並能夠被解釋之法律術語，則其解釋及適用會相當程度地取決於聲請人針對系爭規定在事實上及法律上爭執之程度（參照BVerfGE 143, 246 <321 f. Rn. 210>；145, 20 <54 f. Rn. 85 f.>；150, 309 <326 f. Rn. 42 ff.>）。

[71] 然而，若規範之判斷僅提出特定之憲法上問題，而應由德國聯邦憲法法院答覆，而無法期待事前專門法院之審查得以改善裁判之基礎時，則無須先經專門法院作成判決（參照BVerfGE 150, 309 <326 f. Rn. 44> m.w.N.）。此外，為了維護補充性原則，因而於聲請憲法訴願前，違反處以刑罰或罰金之法律規範，並置身於相應處罰之風險中，以使違憲之規範於刑罰或罰金之裁罰程序中被適用，應無此必要（參照BVerfGE 145, 20 <54 Rn. 85> m.w.N.）。若系爭規定迫使聲請人作成後續無法糾正之重要安排，而向專門法院提起訴訟顯然毫無意義及希望，或其不可期待時，則仍得例外無須事前向專門法院提起訴訟（參照BVerfGE 150, 309 <327 f. Rn. 45> m.w.N.）。然而，即便沒有判決支持該個案情況於法律救濟之合法性，向專門法院提起訴訟亦不應自始即被視為毫無希望（參照BVerfGE 145, 20 <54 Rn. 85>）。

[72]b）這些原則亦適用於主張違反法律上保護義務之情形。通常，只有專門法院首先全面處理所據事實及普通法之情況，並慮及憲法上之要求，方得準確地確定特定問題上法律上規定之漏洞。即使在立法不作為之情況下，其亦避免了德國聯邦憲法法院必須在事實上及普通法上尚未釐清之基礎上作成裁判。

[73]2. 其尚未滿足憲法訴願之要求。在此待裁判之個案中，出現了有關普通法解釋的廣泛問題。機關在決定不向製造商通報其已知悉之零日缺漏之前，是否必須依據現行法制進行符合基本權保護義務之考量，取決於眾多警察、資料保護、網路安全以及資科技安全法制中不同規定之解釋（oben Rn. 53 ff.）。這些規定多屬新近之專門法制，其意義至今尚未透過法院判決或其他法律適用行為或專業文獻進行更詳細之闡述。為避免德國聯邦憲法法院必須於不確定之基礎上作成裁判，首先必須讓主要負責解釋及適用普通法之專門法院有機會審查事實及法律情況。因此，聲請人應先試著要求專門法院之權利保護，例如透過向行政法院提起確認或預防性不作為之訴訟。對於資訊科技系統使用者之基本權是否需要（進一步）預防措施，以於作成維持尚未知悉之安全漏洞之開放，供特定電子通訊來源監察之決定時，充分考慮到保護此類系統免於遭受第三方之滲透的問題，依據新近之行政法院判決，其並未排除專門法院就此問題亦得實現權利保護（參照 zur Zulässigkeit einer negativen Feststellungsklage BVerwGE 157, 8 <10 f. Rn. 13>；157, 126 <128 f. Rn. 15>；zur vorbeugenden Unterlassungsklage BVerwG, Urteil vom 22. Oktober 2014 - 6 C 7/13 -, Rn. 15 ff.；Urteil vom 13. Dezember 2017 - 6 A 6/16 -, Rn. 14；BVerwGE 161, 76 <77 f. Rn. 12 ff.>）。

[74] 沒有明顯之理由說明，聲請人於專門法院採取法律行動不具期待可能性。特別是其於聲請本憲法訴願前，相關憲法法院裁判即曾多次提及向行政法院提起確認之訴或不作為之訴之要求（參照 BVerfGE 143, 246 <321 f. Rn. 210>；145, 20 <54 f. Rn. 86>；原訴願期限屆滿後，但於巴登—符騰堡邦警察法第 80 條施行前與巴登—符騰堡邦網路安全法通過前，亦可參閱 BVerfGE 150, 309 <326 f. Rn. 42 ff.> - KFZ-Kennzeichenkontrolle BW-HE）。

法官：

Harbarth　　Paulus　　Baer

Britz　　Ott　　Christ

Radtke　　Härtel