來源端電信監察與線上搜索
——德國刑事追訴機關之新手段[1]——

■德國特里爾大學法學院 Prof. Dr. Mark A. Zöller
譯者：臺北大學法律系助理教授 王士帆

■■■ 目 次 ■■■

壹、前言

透過 2017 年 8 月 24 日生效的《刑事程序更有效率與更契合實務之調整法案》（Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens）[2]，德國刑事追訴機關在我們的《刑事訴訟法》取得兩種新偵查措施：來源端電信監察（Quellen-Telekommunikationsüberwachung）和線上搜索（Online-Durchsuchung）。這類措施的憲法容許性，在德國迄今有著

[1] 本文為 Prof. Dr. Mark A. Zöller 於 108 年 3 月 4 日在法務部司法官學院演講之手稿，並非正式發表之文章。

[2] BGBl. I S. 3202.

強烈爭議，連立法程序也有些奇怪。這兩項措施完全沒有出現在原始的立法草案。一直到德國聯邦國會的法律暨消費者保護委員會，幾乎可以說是「走後門」，才偷渡到立法程序。此次立法革新雖然有複雜的技術基礎和重大的法治國疑慮，卻沒有進行在這類情形常見的專家公聽會，反而在德國聯邦國會改選前一刻才進入立法程序。

我們《刑事訴訟法》因這次修法引發的變動，也就是我今天想向各位介紹的，是在處理秘密且「以科技方法」入侵「受干預人使用之資訊系統」。這種干預，如果是以入侵取得已加密的資料傳輸為目的，一般會借用傳統的電信監察（TKÜ）偵查手段的概念，稱作「來源端電信監察」，德文簡稱叫「Quellen-TKÜ」，因為通訊資料是在各自的「來源端」取得，也就是在通訊雙方電腦本身上所取得。而對於國家機關希望也存取儲存在電腦的其他資料，而不單只是通訊資料的情況，德國文獻以及現在的法律條文（德國刑事訴訟法第 100b 條）使用的術語，也稱為「線上搜索」（Online-Durchsuchung）。「以科技方法之干預」，技術上意味著違反使用者的意思而在目標系統上安裝特殊的監察軟體。

貳、來源端電信監察

一、要件

來源端電信監察的權限，是在回應日漸普及的加密通訊；如果沒有獲知金鑰，加密通訊將逃避國家單位的監察，因而為罪犯打開不受監察的通訊空間。實際執行上，偵查機關會在被監察通訊（例如透過網路電話、簡訊或即時通訊服務）的電腦安裝一個軟體，這個軟體會在通訊加密之前進行備份並傳送到刑事追訴機關。因此，來源端電信監察是一種特殊形式的電信監察，其取得通訊過程的時間點是通訊加密之前或解密之後，或能使通訊過程解密。也就是說，來源端電信監察特別之處在於，主要是克服解密（Überwindung der Entschlüsselung）。原則上，藉由來源端電信監察，不得獲取以「傳統」電信監察手段也未能取得的資訊。

所以，在 2017 年新修正的德國《刑事訴訟法》第 100a 條，來源端電信監察形式上只是作為「一般」電信監察的補充規範。從而，來源端電信監察和一般電信監察之合法性，原則上立於相同條件。其必要條件是，對於違犯重大犯罪，存在以一定事實所建立的初始嫌疑；而所謂重大犯罪的立法定義，規

定在德國《刑事訴訟法》第 100a 條第 2 項範圍廣泛的犯罪目錄。再者，促成發動監察之犯罪，必須在個案上具備嚴重性。除此之外，必須是以其他方法調查犯罪事實或探查被告所在地有顯著困難或預期無結果。

但是，新修正的德國《刑事訴訟法》第 100a 條在來源端電信監察之內，區分兩種不同的干預型態：

1、侵入受干預人所使用之資訊科技系統，進行中電信之監察與記錄（德國刑事訴訟法第 100a 條第 1 項第 2 句）。

2、監察與記錄儲存於受干預人資訊科技系統之通訊內容與狀態（德國刑事訴訟法第 100a 條第 1 項第 3 句）。

兩者干預授權的共通點，是「以科技方法」實施之。這是指藉由可使刑事追訴機關存取資訊科技系統的國家監察軟體（所謂「國家木馬」），入侵各個資訊科技系統。兩者共同之處還有得在受干預人不知情下實施監察。此外，他們必須是「必要的」手段，亦即，只在一般電信監察沒有預期效果時，始能採用。

德國《刑事訴訟法》第 100a 條第 1 項第 2 句的適用範圍因此至為清楚。這項規定包含對聲音和影像通訊傳輸的存取，是在由各通訊方使用通訊工具加密之前或在接收方已經解密之後進行存取。據此，條文目的是一種對分析電信內容的授權，而這是指經加密傳輸並因此在「一般」電信監察範圍未能發揮作用的電信內容。相較於此，德國《刑事訴訟法》第 100a 條第 1 項第 3 句則有完全不同的規定。對於受干預人資訊科技系統上儲存的通訊內容和狀態，進行監察和記錄的干預權限，也應該可以監察和記錄由即時通訊服務所寄出、通常會被加密，並且已儲存在受干預人資訊科技系統的訊息。所以，詳細觀察可以發現，這裡並不是一種電信監察和記錄，而是一種資料的秘密扣押，當然，其只可針對偵查機關以「一般」電信監察在核准時間內原本能取得的通訊資料。最後，在德國《刑事訴訟法》第 100a 條第 1 項第 3 句的措施方面，這是時間和內容受到限制的線上搜索形式（zeitlich und inhaltlich beschränkte Form der Online-Durchsuchung），並不是一種電信監察措施。

在新規定的德國《刑事訴訟法》第 100a 條第 3 項，由於電信監察內容的分析可能性被擴張到加密內容，可能受干預之人的範圍也被再一次地擴大。亦即，現在除了被告和有一定事實認定為被告接收或轉達給予被告或源於被告之訊息之人外，新法也包括可認為被告有使用其通訊線路或資訊科技系統之人。光是這裡，新法就出現解釋問題

了。舉例而言，「資訊科技系統」的特徵，僅指個人桌上型電腦、筆記型電腦、平板、智慧型手機等的個人機器，還是說條文也包含被告放置資料的雲端服務伺服器，就有疑問了。

二、限制

根據德國《刑事訴訟法》第 100a 條第 5 項第 1 句第 1 款，當所使用之軟體可確保只取得進行中之電信通訊，而不會取得除此以外的資料時，核准來源端電信監察才是合法的。即便依德國《刑事訴訟法》第 100a 條第 1 項第 3 句監察與記錄儲存於電腦系統的通訊內容和狀態（例如 Whatsapp 或 Line 等即時通訊之訊息），也只有在刑事追訴機關所使用的軟體可擔保依第 100e 條第 1 項核准對於進行中傳輸過程亦得以「一般」電信監察取得之通訊內容與紀錄，自核准時點之後的通訊內容與狀態，始為合法。所以，關鍵是儲存在受干預人資訊科技系統上的訊息，是何時透過公共電信網路寄送的。對此，條文是以監察措施的核准命令時點為準，因此尤其不是以監察軟體何時植入資訊科技系統的時間為準。如果監察軟體已事先植入，它也只能傳輸核准命令時點之後所寄出的訊息。那麼，應該會與「一般」電信監察成為「功能等價」。一個無法擔保如此取證限制的軟體，自始即不得使用。

除此之外，來源端電信監察措施的比例性，應由以下方式確保：在來源端電信監察關連下的必要之系統干預，應盡可能輕微和自動回復原狀，並盡可能阻止第三人在使用國家軟體下進行干預（德國刑事訴訟法第 100a 條第 5 項第 1 句第 2 款和第 3 款）。再者，應擔保從受感染之設備所複製資料的完整性和可靠性，以及防止他人無權知悉（德國刑事訴訟法第 100a 條第 5 項第 2 句和第 3 句）。最後，在德國《刑事訴訟法》第 100a 條第 6 項有規定對於使用軟體的特別書面記錄義務。

參、線上搜索

一、「大監聽」的類似手段

在德國新修正的《刑事訴訟法》第 100b 條是所謂線上搜索規定，乃是真正的刑事訴訟創新。迄今為止，這樣的干預措施在德國並不可用於追訴犯罪之目的。這在 2017 年 8 月生效的規定，一方面以《聯邦刑事警察局法》第 20k 條舊法及德國聯邦憲法法院對該條文宣告部分違憲的裁判為立法條文範本[3]，另一方面則依循目前已有的住

[3] BVerfGE 141, 220.

宅監聽規定，住宅監聽在我們德國多半稱為「大監聽」。可以粗略地說，德國《刑事訴訟法》第 100b 條線上搜索的要件，大多和第 100c 條的住宅監聽要件相符。兩者「特別嚴重犯罪」要件使用共同的犯罪目錄，以立法定義哪些犯罪是實施兩者措施所必要的發動犯罪，已清楚表現這一點（德國刑事訴訟法第 100b 條第 2 項）。不過，新創設的線上搜索在一根本之處，仍與 1998 年增訂的住宅監聽有所不同：不同在於，對於核准線上搜索而言，不需有事實根據認為其將取得對於調查犯罪事實或探查共同被告所在地有重要性的資訊。

二、長期監察之危險

德國《刑事訴訟法》第 100b 條第 1 項允許「以科技方法」「干預」受干預人使用之資訊科技系統，並由該系統取得「資料」。此處所謂「以科技方法干預」，應和來源端電信監察脈絡下的科技方法作相同理解，亦即，是指由國家監察軟體秘密滲透到資訊科技系統。不過，這裡的資料概念會比德國《刑事訴訟法》第 100a 條所包含的（進行中）電信資料來得更廣。德國《刑事訴訟法》第 100b 條第 1 項允許取得所有資料，而沒有任何時間或內容限制。如果更仔細觀察，「線上搜索」這樣的措施名稱是會誤導人的。「線上搜索」不同於傳統的搜索，前者並不是點狀進行的措施。確切而言，在令狀核准時間之內，可以繼續取得其他（包括已經存在和新建立的）資料。因此，這不是一種一次性的搜索，而是全面、秘密的線上系統監察。當然，基於比例性，資料取得必須限於與程序相關的資料。依德國《刑事訴訟法》第 100e 條第 3 項第 3 款和第 4 款，管轄法院核准的令狀上，應盡可能仔細敘述所應取得之資料，以避免過度取得資料。但為了使德國實務能識別出與程序相關的資料，必然也會結合警方偵查人員借助監察軟體實況同步檢視資料的權限。

有可能受到線上搜索干預之人的範圍，在德國《刑事訴訟法》第 100b 條第 3 項有明文規定。依此，線上搜索原則上只能針對被告為之（德國刑事訴訟法第 100b 條第 3 項第 1 句）。但是，基於特定事實可認為被告使用他人的資訊科技系統，而且如果只入侵被告資訊科技系統，將無法調查犯罪事實或探查共同被告之所在地時，得例外入侵他人的資訊科技系統。德國立法者在這一條規定，並無意以所涉及的資訊科技系統之財產關係為絕對標準。誰把資訊科技系統當作自己的財產在使用，就是「屬於」那個人的，他在民法上未必是資訊科技系統的所有權人。這個設計引發法律疑問。在此脈絡下的問題，舉例來說，在多人使用的資訊科技系統（例

如網咖和服務站公共電腦，或雲端服務者的伺服器），經過被告簡單、也許只是一次性的共同使用，可否就使監察整部系統和多數未參與犯罪之人合法化。

肆、配套修法

一、保護私人生活核心領域及拒絕證言權人

德國《基本法》（GG）我們的憲法第 1 條第 1 項規定，人性尊嚴不可侵犯。尊重及保護人性尊嚴是所有國家權力的義務。尤其當國家方面探查所謂「私人生活形成之核心領域」時，會侵害人性尊嚴擔保。依德國聯邦憲法法院見解，表達高度屬人性的感受、感覺及思考、觀點和體驗等內在歷程，而無須畏懼國家監控，乃是屬於私人生活形成之核心領域。當陳述形式包含已計畫之犯罪或已違犯之犯罪時，才有所不同。在此背景下，新修正的德國《刑事訴訟法》第 100d 條將原本散落在第 100a 條到第 100c 條的各個核心領域條文合併起來。德國《刑事訴訟法》第 100d 條第 1 項和第 2 項規定，在僅涉及核心領域關係時之絕對證據取得禁止（這是過去已經存在的規定），而對於取得核心領域之所有相關資訊，則應予證據使用禁止。此外，德國《刑事訴訟法》第 100d 條第 3 項包含一種至少形式上是針對線上搜索的廣泛保護規定。根據該規定，技術上，亦即透過監察軟體相關的程式限制，應盡可能確保不會取得涉及核心領域之資料。這個規定從兩個理由來看是失敗的：一方面，判定是否屬於核心領域相關資料，邏輯上乃以事先分析系統上的檔案為前提條件。另一方面，要將檔案判別屬於私人生活核心領域，需要一種複雜和規範層面的衡量過程，沒有人為操控的電腦程式，至少依照當今的科技水準，完全無法應付這樣的思考過程。

在德國《刑事訴訟法》第 100d 條第 5 項，規定了過去在舊法第 100c 條第 6 項保護特定群體的拒絕證言權人，特別是有職業秘密之人。這個規定從現在起延伸到線上搜索。相反的，對於來源端電信監察就跟一般電信監察一樣，比較沒有廣泛的保護（參見德國刑事訴訟法第 160a 條）。

二、程序規定

關於新法來源端電信監察的命令核准權限，根據德國《刑事訴訟法》第 100e 條第 1 項，適用目前「一般」電信監察所適用的規定（偵查法官保留、檢察官緊急權限、監察期限與相關的 3 個月延長規定）。反之，對於線上搜索，根據根據德國《刑事訴訟法》第 100e 條第 2 項，則適用對於核准住宅監聽的規定（邦地方法院保留、審

判長之緊急權限、監察期限與相關的 1 個月延長規定）。德國《刑事訴訟法》第 100e 條第 3 項是令狀形式與內容的規定，這些規定應該會使程序整體而言更加透明。不同於過去，現在對於德國《刑事訴訟法》第 100a 條到第 100c 條的所有措施，令狀必須敘述應取得資訊的類型和重要性。除此之外，在來源端電信監察和線上搜索，必須確切標示所干預的資訊科技系統。關於措施之停止和執行過程之告知，規定在對於所有措施一體適用的德國《刑事訴訟法》第 100e 條第 5 項；於此，住宅監聽方面更嚴格的規定也適用在線上搜索。最後，來源端電信監察和線上搜索，有被納入德國《刑事訴訟法》第 101 條關於秘密措施之一般性程序規定內。而且，現在德國新法《刑事訴訟法》第 101b 條有整併納入來源端電信監察和線上搜索的統計義務和報告義務之規定。

伍、「使用科技技術」之評論

一、概念性問題

在上述德國新法的背景下，至少適合對新法允許使用的監察技術提出簡短的批評觀點。從科技的角度，光是「來源端電信監察」概念和「線上搜索」概念就是誤解。一般人，至少身為外行人而言，會將它們與普遍已接受和建立的偵查措施做一定密切關係的連結。但現實則是另一回事。在傳統的電信監察，只是在電信線路被動竊聽。與此相對的，以結合來源端電信監察的間諜軟體滲透到電腦，是一種變更目標系統的主動過程。線上搜索也是相似的情況。透過概念上和一般搜索的密切關係，雖然絕對也可以聯想到強烈干預的措施，但是搜索就其性質來看，是一種公開、逐一和一次性的措施，被告於搜索時可在場，並能監看警察和檢察官執行職務。再者，來源端電信監察未必比線上搜索之干預強度輕微。這在很多案例實際上就是如此。當然不可忘記的是，來源端電信監察和線上搜索這兩種情形都是目標系統被滲透，而且手段是潛在的完全擷取目標系統之資源。由刑事追訴機關使用的間諜軟體，如同在目標系統內扮演「程式操控的臥底偵查人員」。可是，真人的臥底偵查人員縱使以虛偽身分執行職務，周遭環境仍然是隨時可察覺他的。相反的，間諜軟體不僅目的是秘密的，甚至連它的存在本身都是秘密的。

二、關於來源端電信監察之評論

來源端電信監察的新條文，應該專門用來擷取加密的檔案。當為了傳輸檔案而使用之金鑰是偵查機關所不知悉，而且是「端對端」才被解密時，來源端電信監察始終是必要的。簡言之，

檔案傳輸的發出系統和目標系統約定共同的秘密金鑰。這把金鑰通常只存在於雙方的系統，而且也只適用於檔案傳輸期間。被寄出的檔案在進入網路之前，金鑰已使其在發出系統內被加密。在加密檔案抵達目標系統時，加密檔案得使用同一金鑰再回到可理解的符號序列。若不知悉金鑰，亦即檔案在複雜的網路傳輸路途，檔案的真正內容對第三人而言，完全是無法理解的。這個對於刑事追訴機關構成的科技門檻，將可透過德國新法《刑事訴訟法》第 100a 條予以克服，藉此重建一方面是警察和檢察官、另一方面是使用新加密通訊形式的（潛在）被告之間的機會平等。

三、關於線上搜索之評論

相較之下，德國《刑事訴訟法》第 100b 條的線上搜索，從科技和法治國觀點來看，應該是明顯更有問題的。光是條文文字已有高度不確定性。允許「入侵」資訊科技系統和從其「取得資料」，是包括任何對於系統所使用資料載體，進行 1 比 1 複製位元之製作與傳輸這樣由程式控制的資料處理，乃至於到完全可從外部控制系統（包括其通訊行為在內）。德國《刑事訴訟法》第 100e 條第 3 項新法雖然要求線上搜索的核准令狀上，應以書面限制措施之範圍及方法和應取得之資訊，但撇除這個不談，線上搜索的干預強度並無法單純與住宅監聽的干預強度兩相比擬。即便干預被監控系統的目的，應該只是為了能取得資料，但從科技觀點來看，線上搜索的規定正是在秘密影響目標系統方面超出這樣的目的。

陸、憲法限制

在演講結束前，請容許我表達一些簡短的評論，是關於刑事訴訟新偵查手段的憲法歸類。毫無疑問的是，來源端電信監察和線上搜索至少大大侵犯受監察人的一般人格權（德國基本法第 2 條第 1 項連結第 1 條第 1 項）。惟另一方面，目前在德國一般社會氣氛，特別有利於引進新的監控權限。在場各位一定知道，我們德國和其他西方國家是蓋達或伊斯蘭國（IS）等伊斯蘭恐怖組織的焦點。尤其是 2016 年 12 月 19 日在我們首都柏林市中心的聖誕市集恐怖攻擊，它發生在緊鄰威廉皇帝教堂的柏林 Breitscheid 廣場，造成 11 人死亡，55 人重傷，這不是只有使德國人民感到震驚。人民之個人自由和群體之安全需求，這兩者之間的敏感平衡也因這場恐怖攻擊顯著往後者加重傾斜。因此，來源端電信監察和線上搜索的刑事訴訟新干預授權規定，也應該始終在普遍恐怖威脅的背景下被看待。

一、適合性與必要性

根據德國聯邦憲法法院見解，對國際恐怖主義之危險預防，在刑事追訴之脈絡下也是一種正當目的。在 2016 年關於德國《聯邦刑事警察局法》的指標裁判中[4]，德國聯邦憲法法院就干預特別嚴重之措施，雖然表示必須以對於優越重要法益——例如個人生命、身體和自由或涉及危害人類生存基礎的公共法益——存在危險為準。若套用到追訴犯罪的刑事法，這類的危險會以犯罪目錄取代，在這些犯罪具一定嫌疑程度時，立法授權發動各個的刑事訴訟偵查措施。從而，在電信監察措施，必須有事實得以認定成立德國《刑事訴訟法》第 100a 條第 2 項所稱「嚴重犯罪」之初始嫌疑，而在線上搜索，則是德國《刑事訴訟法》第 100b 條第 2 項所敘述的「特別嚴重犯罪」。然而，在這些範圍廣泛的犯罪目錄，其列舉的所有犯罪，實際上是否分類妥當，應該被批判性探討。諸如德國《刑法》第 146 條、第 154 條偽造貨幣罪和偽造有價證券罪（德國刑事訴訟法第 100b 條第 2 項第 1c 款），或第 224 條第 1 項第 2 款結夥竊盜罪（德國刑事訴訟法第 100b 條第 2 項第 1h 款），從其不法內容來看，說他們事實上等同於恐怖危險，這幾乎經不起嚴格論證。就此而言，這些犯罪目錄至少在某些部分太過擴張了。

二、比例性

如果看一下德國聯邦憲法法院目前的裁判，那麼對於為了刑事追訴而引進來源端電信監察一事，應該沒有原則上的憲法疑慮。監察電信通訊過程，畢竟是長久以來即被承認和合法的偵查措施，只是因為當前科技變化和進步，尤其是透過使用金鑰技術，才使得目前的偵查方法再也不能發揮成效。甚至於，德國法律文獻的少數意見因此主張，在 2017 年來源端電信監察新法之前，藉由德國舊《刑事訴訟法》第 100a 條的附屬權限，即可認為來源端電信監察是合法的手段[5]。德國聯邦憲法法院認為沒有違憲問題，只要在來源端電信監察具有與傳統電信監察技術上之功能等價。如果可確保來源端電信監察只限於監察進行中之電信，則是合法的。但是，傳統電信監察和來源端電信監察的類似性，只有在進行中通訊如何實際上被監察。依此觀之，在依德國《刑事訴訟法》第 100a 條第 5 項第 1b 款取得的資料，亦即在令狀核准之後、但在實際技術干預之前所儲存的資訊，德國聯邦憲法法院的干預正當化就起不了作用

4 BVerfGE 141, 220.

5 Vgl. *Meyer-Goßner/Schmitt*, StPO, § 100d Rn. 2.

了。這裡所涉及的，事實上是一種（限制的）線上搜索。

在此，德國聯邦最高法院正確認為，基於處理資訊科技系統而來的基本權干預強度，可和德國《基本法》第13條住宅不可侵犯性之干預相比擬。從而，核准令狀的保留條件是，若無系爭措施，調查犯罪事實將有顯著困難或預期無結果。這裡和德國聯邦憲法法院其實是附帶表達的一句話有關：「公開取得被鎖定人的資料檔案，原則上優先於秘密滲透，這也是屬於個案上對比例原則之尊重」[6]。此結果必然是，德國《刑事訴訟法》第100b條第1項第3款對於線上搜索的核准要件，在個案中必須予以特別嚴格審查，並應敘明為何公開的搜索無法發揮預期效果。除此之外，在國家監察措施的脈絡下，干預之強度始終由措施之期間來決定。德國聯邦憲法法院還可以接受3個月的上限。這個時間界線在新法下只是表象維持著。依據德國《刑事訴訟法》第100e條第2項第4句，線上搜索核准期間雖然原則上只有一個月，但法律並沒有規定最高期限。法律只有規定在執行6個月後，由邦高等法院決定後續之延長（德國刑事訴訟法第100e條第2項第6句）。這個依德國《刑事訴訟法》新法最後可能是無期限限制的持續監控資訊科技系統，在比例原則觀點底下不再具備正當性，所以應認為是違憲的。

柒、結論

對於深入評價新法規定而言，在現在這個時點似乎言之過早。目前尚無處理新法干預權限的實證分析。不過，在明顯感受國際恐怖主義威脅的時代，即便我們無法否認來源端電信監察和線上搜索的原則上正當性，仍要注意新法條文一些「立法者倉促開槍」的地方。這裡在細節上絕對還有修補必要。來源端電信監察只是作為對於通訊使用進步金鑰技術的回應，雖然其不存在根本的憲法障礙，但新法藉由在被滲透系統上的普遍取得（未來的）通訊資料，已經超出來源端電信監察之目的。況且，資訊科技專家指出在很多通訊使用上，取得各自通訊軟體所使用的金鑰並接著在「線路」取得資料，不但技術上可行，而且足以獲知通訊內容。

以線上搜索秘密滲透資訊科技系統及持續從中取得資料的干預權限，在其目前（寬鬆的）條文版本上，成為一種極度強烈和幾乎難以正當化的基本權侵犯，理由還包括其技術之不確定性、

6　BVerfGE 141, 220 (305 f.).

實際無時間期限之執行，以及欠缺措施之事後實際可審查性。

最後，在每種使用國家間諜軟體的情形，都會留下一個問題，即為了讓間諜軟體成功運作，必須利用資訊系統中的安全漏洞。國家因而儼然成為「漏洞利用市場」的參與者。這件事應該被阻止，因為至少在德國，國家應盡力改善人民的一般資訊科技安全。就此而言，有一系列對於來源端電信監察和線上搜索之刑事訴訟新規定的憲法訴訟，正繫屬在位於 Karlsruhe 城市的德國聯邦憲法法院，就不意外了。可預料的是，憲法法院法官於此至少在細節上將要求德國立法者進行改善。所以，直到德國聯邦憲法法院這個裁判出來前，在考慮將德國《刑事訴訟法》的新規定作為規範榜樣時，應該非常謹慎。

非常感謝各位的專注聆聽！

附錄：德國《刑事訴訟法》摘錄

第 100a 條——電信通訊監察

（1）有下列情形時，即使受干預人不知情，仍得監察及記錄電信通訊：

1. 一定事實懷疑成立第 2 項所稱嚴重犯罪之正犯、共犯、未遂犯或預備犯；
2. 犯罪個案情節重大，並且
3. 以其他方法調查犯罪事實或探查被告所在地有顯著困難或預期無結果。

當為了尤其得以依解密方式進行監察與記錄而有必要時，亦得以科技設備侵入受干預人所使用之資訊科技系統，進行電信通訊之監察與記錄。儲存於受干預人資訊科技系統之通訊內容與狀態亦得監察與記錄，當其在公共電信線路以加密方式所進行之傳輸過程原本即可監察與記錄者。

（2）第 1 項第 1 款之嚴重犯罪，為下列之罪：

1.《刑法》：

a) 第 80a 條至第 82 條、第 84 條至第 86 條、第 87 條至第 89a 條、第 89c 條第 1 項至第 4 項、第 94 條至第 100a 條違反和平罪、內亂罪、危害民主法治國罪與叛國罪、外患罪。
b) 第 108e 條民意代表貪瀆罪。
c) 第 109d 條至第 109h 條妨害國防罪。
d) 第 129 條至第 130 條妨害公共秩序罪。
e) 第 146 條及第 151 條偽造貨幣及有價證券罪，及其各結合第 152 條，與第 152a 條第 3 項及第 152b 條第 1 項至第 4 項之罪。
f) 第 177 條第 6 項第 2 句第 2 款第 176a 條、第 176b 條妨害性自主罪，以及第 177 條之罪。

g) 第 184b 條第 1 項與第 2 項、第 184c 條第 2 項散布、購買及持有兒童及青少年色情文書罪。
h) 第211條與第212條謀殺及殺人罪。
i) 第 232 條、 第 232a 條 第 1 項至第 5 項、第 232b 條、第 233 條第 2 項、第 233a 條、第 234 條、第 234a 條、第 239a 條與第 239b 條妨害人身自由罪。
j) 第 244 條第 1 項第 2 款結夥竊盜與第 244a 條加重結夥竊盜罪。
k) 第 249 條至第 255 條強盜與恐嚇取財罪。
l) 第 260 條及第 260a 條常業贓物、集團贓物與常業集團贓物罪。
m) 第 261 條第 1 項、第 2 項與第 4 項洗錢及隱匿不法財產所得罪；第 261 條第 9 項第 2 句之不罰，因第 261 條第 9 項第 3 句被排除而成立可罰性者，僅以不法行為之標的物源於第 1 款至第 11 款所稱之嚴重犯罪為限。
n) 第 263 條第 3 項第 2 句要件與第 263 條第 5 項之詐欺與電腦詐欺罪，以及各結合第 263a 條第 2 項之罪。
o) 第 264 條第 2 項第 2 句要件與第 264 條第 3 項結合第 263 條第 5 項之補助款詐欺罪。
p) 第 265e 條第 2 句之運動比賽詐欺罪與操控職業運動比賽罪。
q) 第 267 條第 3 項第 2 句要件與第 267 條第 4 項之偽造文書罪，以及各結合第 268 條第 5 項或第 269 條第 3 項，以及第 275 條第 2 項及第 276 條第 2 項之罪。
r) 第 283a 條第 2 句破產罪。
s) 第 298 條、第 300 條第 2 句以及第 299 條不正競爭罪。
t) 第 306 條至第 306c 條、第 307 條第 1 項至第 3 項、第 308 條第 1 項至第 3 項、第 309 條第 1 項至第 4 項、第 310 條第 1 項、第 313 條、第 314 條、第 315 條第 3 項、第 315b 條第 3 項以及第 316a 條、第 316c 條公共危險罪。
u) 第 332 條與第 334 條受賄及行賄罪。

2.《租稅通則》：
a) 第 370 條第 3 項第 2 句第 5 款要件之逃漏稅罪。
b) 第 373 條常業性、暴力性及集團性走私罪。
c) 第 374 條第 2 項稅贓物罪。

3.《對抗禁藥法》：第 4 條第 4 項第 2 款字母 b 之犯罪。

4.《難民法》：
a) 第 84 條第 3 項誘使濫用難民申請罪。
b) 第 84a 條常業性及集團性誘使濫

用難民申請罪。

5.《居留法》：

a) 第 96 條第 2 項外國人偷渡罪。

b) 第 97 條偷渡致死罪以及常業性與集團性偷渡罪。

6.《對外貿易法》：第 17 條與第 18 條之故意犯罪。

7.《麻醉藥品法》：

a) 與第 29 條第 3 項第 2 句第 1 款有關且符合該款要件之犯罪。

b) 第 29a 條、第 30 條第 1 項第 1 款、第 2 款與第 4 款，以及第 30a 條及第 30b 條之犯罪。

8.《麻醉藥品原料監管法》：符合第 19 條第 3 項第 2 句要件之第 19 條第 1 項之犯罪。

9.《戰爭武器管制法》：

a) 第 19 條第 1 項至第 3 項、第 20 條第 1 項及第 2 項與第 20a 條第 1 項至第 3 項之犯罪，以及各結合第 21 條之犯罪。

b) 第 22a 條第 1 項至第 3 項之犯罪。

9a.《新興精神活性物質法》：第 4 條第 3 項第 1 款字母 a 之犯罪。

10.《國際刑法》：

a) 第 6 條滅絕種族罪。

b) 第 7 條危害人類罪。

c) 第 8 條至第 12 條戰爭罪。

d) 第 13 條侵略罪。

11.《武器法》：

a) 第 51 條第 1 項至第 3 項之犯罪。

b) 第 52 條第 1 項第 1 款及第 2 款字母 c 及 d，以及第 5 項與第 6 項之犯罪。

（3）電信監察命令只得針對被告為之，如有一定事實認為接收或轉達給予被告或源於被告之訊息之人或被告使用其通訊線路或資訊設備之人，亦得對其命令電信監察。

（4）根據電信監察之監察與記錄命令，任何提供或參與電信通訊業務之人應協助法院、檢察官及其執行警察職務之偵查人員（法院組織法第 152 條）實施本條文之措施，並應立即提供必要之回復。是否與在如何範圍之內採取防護措施，由《電信通訊法》（Telekommunikationsgesetz）及《電信通訊監察規則》（Telekommunikations-Überwachungsverordnung）定之。第 95 條第 2 項之規定準用之。

（5）實施第 1 項第 2 句與第 3 句措施時，技術上應確保：

1. 只可監察與記錄

a) 進行中之電信通訊（第 1 項第 2 句），或

b) 依第 100e 條第 1 項核准對於在公共電信線路以加密方式進行傳輸時亦得監察與記錄之通訊內容

與紀錄，自核准時點開始之通訊內容與狀態（第 1 項第 3 句）。

2. 在資訊科技系統只可進行為取得資料所必須之變更。
3. 措施結束時，技術上應盡可能使所進行之變更自動回復。

所採用之方法應依科技狀態防止他人無權使用。所複製之資料應依科技狀態保護免於變更、無權刪除或無權知悉。

（6）每次使用科技方法時，應書面記錄：

1. 科技方法之名稱以及使用的時點；
2. 資訊技術系統的識別資料以及所採取非暫時性的變更；
3. 說明得調查取得之資料；
4. 執行措施之機關單位。

第 100b 條——線上搜索

（1）有下列情形時，即使受干預人不知情，仍得以科技方法入侵受干預人使用之資訊科技系統，並得由該系統取得資料（線上搜索），

1. 一定事實懷疑成立第 2 項所稱嚴重犯罪之正犯、共犯或未遂犯；
2. 犯罪個案情節重大，並且
3. 以其他方法調查犯罪事實或探查被告所在地有顯著困難或預期無結果。

（2）第 1 項第 1 款之嚴重犯罪，為下列之罪：

1.《刑法》：

a) 第 81 條、第 82 條、第 89a 條、第 89c 條第 1 項至第 4 項、第 94 條、第 95 條第 3 項與第 96 條第 1 項，以及各結合第 97b 條，與第 97a 條、第 98 條第 1 項第 2 句、第 99 條第 2 項、第 100 條及第 100a 條第 4 項違反和平罪、內亂罪、危害民主法治國罪與叛國罪、外患罪。

b) 第 129 條第 1 項連結第 5 項第 3 句成立組織犯罪，以及第 129a 條第 1 項、第 2 項、第 4 項、第 5 項第 1 句第 1 選項之成立恐怖組織罪。

c) 第 146 條及第 151 條偽造貨幣及有價證券罪，及其各結合第 152 條，與第 152a 條第 3 項及第 152b 條第 1 項至第 4 項之罪。

d) 第 176a 條第 2 項第 2 句或第 3 項妨害性自主罪，以及第 177 條第 6 項第句第 2 款之罪。

e) 第 184b 條第 2 項散布、購買及持有兒童及青少年色情文書罪。

f) 第 211 條與第 212 條謀殺及殺人罪。

g) 第 234 條、第 234a 條第 1 項及第 2 項、第 239a 條與第 239b 條妨害人身自由罪，與第 232 條第 3 項販賣人口罪、第 232a 條第 3 項及第 4 項後半句、第 232b 條

第 3 項或第 4 項結合第 232a 第 4 項或第 5 項後半句之強迫性交易罪和強迫工作罪，和第 233a 條第 3 項或第 4 項後半句之剝奪自由剝削罪。

h) 第 244 條第 1 項第 2 款結夥竊盜與第 244a 條加重結夥竊盜罪。

i) 第 250 條第 1 項或第 2 項、第 251 條加重強盜致死罪。

j) 第 255 條強盜式恐嚇取財罪，與符合第 253 條第 4 項第 2 句要件之第 253 條嚴重恐嚇取財罪。

k) 第 260 條及第 260a 條常業贓物、集團贓物與常業集團贓物罪。

l) 符合第 261 條第 4 要件之第 261 條嚴重洗錢及隱匿不法財產所得罪；第 261 條第 9 項第 2 句之不罰，因第 261 條第 9 項第 3 句被排除而成立可罰性者，僅以不法行為之標的物源於第 1 款至第 7 款所稱之嚴重犯罪為限。

m)符合第 335 條第 2 項第 1 款至第 3 款要件之第 335 條第 1 項嚴重賄賂罪。

2.《難民法》：

a) 第 84 條第 3 項誘使濫用難民申請罪。

b) 第 84a 條常業性及集團性誘使濫用難民申請罪。

3.《居留法》：

a) 第 96 條第 2 項外國人偷渡罪。

b) 第 97 條偷渡致死罪以及常業性與集團性偷渡罪。

4.《麻醉藥品法》：

a) 符合第 29 條第 3 項第 2 句第 1 款要件之第 29 條第 1 項第 1 句第 1 款、第 5 款、第 6 款、第 10 款、第 11 款或第 13 款之嚴重犯罪。

b) 第 29a 條、第 30 條第 1 項第 1 款、第 2 款與第 4 款，以及第 30a 條之犯罪。

5.《戰爭武器管制法》：

a) 第 19 條第 2 項或第 20 條第 1 項之犯罪，以及各結合第 21 條之犯罪。

b) 第 22a 條第 1 項連結第 2 項之犯罪。

6.《國際刑法》：

a) 第 6 條滅絕種族罪。

b) 第 7 條危害人類罪。

c) 第 8 條至第 12 條戰爭罪。

d) 第 13 條侵略罪。

7.《武器法》：

a) 第 51 條第 1 項連結第 2 項之嚴重犯罪。

b) 第 52 條第 1 項第 1 款連結第 5 項之嚴重犯罪。

（3）線上搜索只得對被告為之。但基於一定事實認有以下情形，亦得入侵

他人之資訊科技系統：

1. 第 100e 條第 3 項令狀上記載之被告，其所使用之他人資訊科技系統；
2. 如只入侵被告資訊科技系統，將無法調查犯罪事實或探查共同被告之所在地。

執行線上搜索使其他人不可避免被干預時，亦得為之。

（4）第 100a 條第 5 項與第 6 項，除第 5 項第 1 句第 1 款外，於線上搜索準用之。

第 100c 條——住宅監聽

（1）有下列情形時，即使受干預人不知情，仍得以科技方法監聽和記錄住宅內非公開之談話，

1. 一定事實懷疑成立第 100b 條第 2 項所稱特別嚴重犯罪之正犯、共犯或未遂犯；
2. 犯罪個案情節重大；
3. 有事實根據認為監察可取得對調查犯罪事實或探查共同被告所在地具有重要性之被告談話，而且
4. 以其他方法調查犯罪事實或探查共同被告所在地有顯著困難或預期無結果。

（2）住宅監聽僅得對被告為之，而且僅限於被告住宅內執行。但基於一定事實認有以下情形，亦得在他人住宅為之：

1. 第 100e 條第 3 項令狀上記載之被告處於他人住宅者；
2. 如只在被告住宅監聽，將無法調查犯罪事實或探查共同被告之所在地。

執行住宅監聽將使其他人不可避免被干預時，亦得為之。

第 100d 條——私人生活型態核心領域；拒絕證言權人

（1）第 100a 條至第 100c 條措施，有事實根據認為其只取得出自私人生活核心領域之資訊時，不得為之。

（2）由第 100a 條至第 100c 條措施取得出自私人生活核心領域之資訊，不得使用。應立即刪除此資訊之紀錄。應以書面記錄該資訊之取得與刪除。

（3）執行第 100b 條措施時，技術上應盡可能確保不會取得涉及私人生活核心領域之資料。由第 100b 條措施取得之資訊，若涉及私人生活核心領域，應立即刪除，或檢察官陳報核准法院，由法院裁判取得資訊之證據能力及是否刪除。法院關於證據使用能力之裁判，對後續程序有拘束力。

（4）有事實根據認為監察不會取得屬於私人生活核心領域之陳述時，始得

核准第 100c 條之措施。在監察過程中有依據得知取得屬於私人生活核心領域之陳述時，應立即停止監聽與記錄。已停止之措施，得在第 1 項要件下繼續進行。檢察官對措施之停止或繼續進行有疑問時，應立即聲請法院裁判；準用第 100e 條第 5 項。所取得之資訊有可能依第 2 項成立使用禁止時，檢察官應立即聲請法院裁判。第 3 項第 3 句之規定準用之。

（5）在第 53 條之情形，不得為第 100b 條與第 100c 條之措施；若在措施執行期間或執行後發覺有第 53 條之情形時，準用第 2 項規定。在第 52 條與第 53a 條之情形，由第 100b 條與第 100c 條措施所取得之資訊，僅在考慮信賴關係之重要性與調查案情或探查被告所在地之追訴利益未失均衡時，始得使用。第 160a 條第 4 項之規定準用之。

第 100e 條——第 100a 條至第 100c 條措施之程序

（1）第 100a 條之措施，只得依檢察官聲請，由法院核准。遲延即生危險時，得由檢察官核准之。檢察官之核准，未於 3 個工作日內經法院補正認可者，失其效力。核准之執行期間，不得逾 3 個月。當核准之要件在考量所取得之偵查結果後認為繼續存在時，得延長執行之，但每次延長不得逾 3 個月。

（2）第 100b 條及第 100c 條之措施，只得依檢察官聲請，由其所屬轄區之《法院組織法》第 74a 條第 4 項規定之邦地方法院合議庭核准之。遲延即生危險時，得由該合議庭之審判長核准。審判長之核准，未於 3 個工作日內經合議庭補正認可者，失其效力。核准之執行期間，不得逾 1 個月。當核准之要件在考量所取得之偵查結果後認為繼續存在時，得延長執行之，但每次延長不得逾 1 個月。延長執行期間整體已達 6 個月時，其後續之延長應由邦高等法院決定。

（3）核准命令以書面為之。核准命令之主文應記載：

1. 盡可能敘述措施受干預人之姓名與地址，
2. 核准執行措施之犯罪事實，
3. 措施之方法、範圍、持續期間與截止時間，
4. 措施應取得之資訊類型及其對刑事程序之意義，
5. 在執行第 100a 條之措施，應記載電話號碼或應監察之通訊線路或終端

設備之其他識別碼，若無法從一定事實得知此識別碼同時屬於其他終端設備者；在第 100a 條第 1 項第 2 句及第 3 句之情形，盡可能明確標示入侵之資訊科技系統名稱，

6. 在第 100b 條之措施，盡可能明確標示應從中取得資料之資訊科技系統名稱，
7. 在第 100c 條之措施，被監察之住宅或被監察之房間。

（4）在第 100a 條至第 100c 條措施之核准命令或延長命令，其理由應敘述核准要件與重要之考量因素。尤其應敘述與個案相關之以下事項：

1. 構成犯罪嫌疑之特定事實；
2. 措施必要性及比例原則之重要考量
3. 在第 100c 條之措施，應記載第 100c 條第 4 項第 1 句規定之事實依據。

（5）核准之要件消滅時，應立即停止所核准之措施。措施停止後，應將執行結果報告核准之法院。於第 100b 條與第 100c 條之措施，並應向核准之法院報告執行過程。核准之要件消滅，檢察官未停止執行措施者，法院必須命令停止執行。停止執行第 100b 條與第 100c 條措施之命令，亦得由審判長為之。

（6）由第 100b 條與第 100c 條取得且可使用之個人資料，得依下列規定作為其他目的使用：

1. 為了調查第 100b 條或第 100c 條措施所針對之犯罪，或調查此類犯罪之被告所在地時，得不經受監察人同意而使用於其他刑事程序。
2. 個人資料，亦包括依第 100d 條第 5 項第 1 句後半句所取得之個人資料，只為預防個案之生命危險，或預防對個人身體、人身自由或國家安全或存續之急迫危險，或預防對供應國民需求具有重要價值之物、具文化重大價值之物或《刑法》第 305 條所稱物品之急迫危險，始得為預防危險之目的而使用。為預防個案中對其他重要財產價值之急迫危險，亦得使用個人資料。資料對於預防危險如不再有必要性，或對於先於法院或法院本身審查預防危險所作成處分不再有必要性，預防危險之主管機關應立即刪除資料之紀錄。刪除應在卷宗予以記錄。僅因可能有先於法院或法院本身之審查而暫緩刪除之個人資料，其只得使用於此目的；該個人資料應封鎖，不得用於其他目的。
3. 由相關之警察法措施取得可使用之個人資料，為了調查第 100b 條或第 100c 條措施所針對之犯罪，或調查此類犯罪之被告所在地時，得不經受監察人同意而於刑事程序使用。

Quellen-Telekommunikationsüberwachung und Online-Durchsuchung als neue Instrumente der deutschen Strafverfolgungsbehörden[1]

Prof. Dr. Mark A. Zöller

I. Vorbemerkungen

Durch das am 24. August 2017 in Kraft getretene Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens[2], haben die deutschen Strafverfolgungsbehörden in unserer Strafprozessordnung zwei neue Ermittlungsmaßnahmen erhalten: die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung. Die verfassungsrechtliche Zulässigkeit solcher Maßnahmen ist in Deutschland bis heute stark umstritten. Insofern war auch das Gesetzgebungsverfahren einigermaßen kurios. Beide Maßnahmen waren im ursprünglichen Gesetzentwurf gar nicht enthalten. Sie wurden erst im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages, also sozusagen „durch die Hintertür", in das Gesetzgebungsverfahren eingeschleust. Trotz komplexer technischer Grundlagen und massiver rechtsstaatlicher Bedenken wurden die gesetzlichen Neuerungen ohne eine in solchen Fällen übliche Sachverständigenanhörung noch kurz vor der anstehenden Neuwahl des Deutschen Bundestages durch das Gesetzgebungsverfahren gebracht.

Die dadurch verursachten Änderungen unserer Strafprozessordnung, die ich Ihnen heute vorstellen möchte, behandeln verdeckte und „mit technischen Mitteln"

---

1 本文為 Prof. Dr. Mark A. Zöller 於 108 年 3 月 4 日在法務部司法官學院演講之手稿，並非正式發表之文章。

2 BGBl. I S. 3202.

durchgeführte Eingriffe „in von dem Betroffenen genutzte informationstechnische Systeme“. Wenn bei einem solchen Eingriff das Ziel verfolgt wird, Zugriff auf verschlüsselten Datenverkehr zu erhalten, spricht man in Anlehnung an das klassische Ermittlungsinstrument der Telekommunikationsüberwachung (TKÜ) von Quellen-Telekommunikationsüberwachung, kurz: „Quellen-TKÜ“, da die Kommunikationsdaten jeweils an der „Quelle“, also auf dem Rechner selbst erhoben werden. Für den Fall, dass von den Sicherheitsbehörden ein Zugriff auch auf andere, auf einem Rechner gespeicherte Daten und nicht nur auf Kommunikationsdaten gewünscht wird, wird in der Literatur und nun auch im Gesetzestext (§ 100b StPO) der Terminus „Online-Durchsuchung“ gebraucht. Technisch bedeutet ein „Eingriff mit technischen Mitteln“ die Installation einer speziellen Überwachungssoftware auf dem Zielsystem gegen den Willen des Benutzers.

II. Die Quellen-Telekommunikationsüberwachung

1. Voraussetzungen

Die Befugnis zur Quellen-TKÜ reagiert auf die zunehmende Verbreitung verschlüsselter Kommunikation, die sich ohne Kenntnis des Schlüssels der Überwachung durch staatliche Stellen entzieht und somit Kriminellen überwachungsfreie Kommunikationsräume eröffnet. Faktisch wird auf dem Computer, mit der die zu überwachende Kommunikation (z.B. per Internettelefonie, SMS oder Messenger-Diensten) getätigt wird, eine Software installiert, welche die Kommunikation vor der Verschlüsselung mitschneidet und an die Strafverfolgungsbehörde übermittelt. Die Quellen-TKÜ ist somit eine besondere Form der Telekommunikationsüberwachung, die den Kommunikationsvorgang zu einem Zeitpunkt erfasst, *bevor* dieser verschlüsselt wird oder *nachdem* dieser entschlüsselt wurde bzw. die die Entschlüsselung ermöglicht. Besonders ist an ihr also vor allem die *Überwindung der Entschlüsselung*. Grundsätzlich können mit ihrer Hilfe keine Informationen erlangt werden, die nicht auch durch eine „konventionelle“ Telekommunikationsüberwachung erlangt würden.

In dem im Jahr 2017 neu gefassten § 100a StPO ist die Quellen-TKÜ deshalb formal nur als *Ergänzung* der „normalen“ Telekommunikationsüberwachung normiert worden. Beide Maßnahmen sind daher grundsätzlich unter den gleichen Voraussetzungen zulässig. Erforderlich ist ein durch bestimmte Tatsachen begründeter Anfangsverdacht für die Begehung schwerer Straftaten, die in § 100a Abs. 2 StPO durch einen umfangreichen Straftatenkatalog gesetzlich definiert werden. Außerdem muss die Tat, die Anlass zur Überwachung gibt, auch im Einzelfall schwer wiegen. Zudem muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein.

Der neue § 100a StPO unterscheidet aber innerhalb der Quellen-TKÜ zwischen zwei verschiedenen Eingriffsmodalitäten:

1. dem Überwachen und Aufzeichnen der laufenden Telekommunikation durch Eingriff in das informationstechnische System des Betroffenen (§ 100a Abs. 1 S. 2 StPO) und
2. der Überwachung und Aufzeichnung der auf dem Computersystem gespeicherten Kommunikationsinhalte und -umstände (§ 100a Abs. 1 S. 3 StPO).

Beiden Eingriffsermächtigungen ist die Tatsache gemeinsam, dass sie „mit technischen Mitteln“ erfolgen. Damit ist eine Infiltration des jeweiligen IT-Systems mit Hilfe einer staatlichen Überwachungssoftware (sog. „Staatstrojaner“) gemeint, die den Strafverfolgungsbehörden Zugriff auf das IT-System verschafft. Ebenso gemeinsam ist beiden Maßnahmen, dass diese ohne Wissen des Betroffenen durchgeführt werden dürfen. Zudem müssen sie „notwendig“ sein, d.h. auf sie kann nur in Fällen zurückgegriffen werden, in denen die „normale“ TKÜ keinen Erfolg verspricht.

Der Anwendungsbereich der Regelung in § 100a Abs. 1 Satz 2 StPO leuchtet somit unmittelbar ein. Durch diese Regelung wird das Ausleiten von Sprach- und Videokommunikation erfasst, *bevor* diese durch das jeweils verwendete Kommunikationstool verschlüsselt wird bzw. *nachdem* diese beim Empfänger entschlüsselt wurde. Zweck der Regelung ist demnach die Ermöglichung der Auswertung von Telekommunikationsinhalten, die verschlüsselt übertragen und damit im Rahmen

einer „normalen“ TKÜ nicht nutzbar gemacht werden können.

Etwas gänzlich Anderes regelt demgegenüber § 100a Abs. 1 Satz 3 StPO. Durch diese Befugnis zur Überwachung und Aufzeichnung von auf dem IT-System des Betroffenen gespeicherten Inhalten und Umständen der Kommunikation soll auch die Überwachung und Aufzeichnung von über Messenger-Dienste versendeten, regelmäßig verschlüsselten Nachrichten ermöglicht werden, die bereits auf dem IT-System des Betroffenen gespeichert sind. Bei genauer Betrachtung handelt es sich daher hierbei nicht um eine Überwachung und Aufzeichnung von Telekommunikation, sondern um eine *heimliche Beschlagnahme von Daten*. Diese darf sich allerdings nur auf solche Kommunikationsdaten erstrecken, welche die Ermittlungsbehörden auch durch eine „normale“ TKÜ im Anordnungszeitraum hätten erlangen können. Letztlich handelt es sich also bei Maßnahmen nach § 100a Abs. 1 Satz 3 StPO um eine *zeitlich und inhaltlich beschränkte Form der Online-Durchsuchung* und nicht um eine Telekommunikationsüber wachungsmaßnahme.

Infolge der inhaltlichen Ausweitung der Möglichkeiten zur Telekommunikationsüberwachung auf verschlüsselte Inhalte ist im neuen § 100a Abs. 3 StPO auch der *Kreis der Personen*, der hiervon *betroffen* sein kann, noch einmal erweitert worden. So sind nun neben dem Beschuldigten und Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben, neuerdings auch solche Personen genannt, bei denen anzunehmen ist, dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt. Schon hier stellen sich in Bezug auf das neue Gesetz erste Auslegungsfragen. So ist etwa zweifelhaft, ob mit dem Merkmal des „informationstechnischen Systems“ nur persönliche Geräte wie PCs, Laptops, Tablets oder Smartphones gemeint sind oder ob die Norm beispielsweise auch die Server von Cloud-Diensten erfasst, in denen der Beschuldigte seine Daten abgelegt hat.

2. Beschränkungen

§ 100a Abs. 5 S. 1 Nr. 1 StPO lässt die Anordnung einer Quellen-TKÜ nur zu, wenn die eingesetzte Software technisch sicherstellt, dass nicht auf Daten zugegriffen werden kann, die über laufende Kommunikationsvorgänge hinausgehen. Auch die Überwachung und Aufzeichnung der auf dem Computersystem gespeicherten Kommunikationsinhalte und -umstände nach § 100a Abs. 1 Satz 3 StPO ist nur zulässig, wenn die von den Strafverfolgungsbehörden eingesetzte Software sicherstellt, dass nur solche gespeicherten Kommunikationsdaten (z.B. Nachrichten von Messengerdiensten wie Whatsapp oder Line) erhoben werden, die nach Erlass der Anordnung nach § 100e Abs. 1 StPO auch während eines laufenden Übertragungsvorgangs mittels „normaler" TKÜ hätten überwacht und aufgezeichnet werden können. Entscheidend ist somit, *wann* die Nachrichten, die auf dem IT-System des Betroffenen gespeichert sind, über das öffentliche Telekommunikationsnetz verschickt wurden. Diesbezüglich stellt die Vorschrift auf den *Anordnungszeitpunkt* der Überwachungsmaßnahme ab. Es kommt somit insbesondere nicht darauf an, wann die Überwachungssoftware auf dem IT-System installiert wurde. Diese darf, auch wenn sie schon vorher installiert wurde, nur diejenigen Nachrichten ausleiten, die *nach dem Zeitpunkt der Anordnung* versendet wurden. So soll eine „funktionale Äquivalenz" zur „normalen" TKÜ hergestellt werden. Eine Software, die diese Begrenzung nicht sicherstellt, darf von vornherein nicht eingesetzt werden.

Darüber hinaus soll die *Verhältnismäßigkeit* der Maßnahme dadurch gewährleistet werden, dass die notwendigen Systemeingriffe im Zusammenhang mit der Quellen-TKÜ möglichst gering gehalten, automatisiert rückgängig gemacht werden und Eingriffe von Dritten unter Nutzung der staatlichen Software möglichst verhindert werden (§ 100a Abs. 5 Satz 1 Nr. 2 und 3 StPO). Außerdem ist die Integrität und Authentizität der vom infizierten Gerät kopierten Daten sicherzustellen und die Kenntnisnahme durch Unbefugte zu verhindern (§ 100a Abs. 5 Satz 2 und 3 StPO). Und schließlich sind in § 100a Abs. 6 StPO besondere Dokumentationspflichten für den Einsatz der Software geregelt.

III. Die Online-Durchsuchung

1. Parallele zum „großen Lauschangriff“

Bei der Regelung der sog. Online-Durchsuchung im neuen § 100b StPO handelt es sich um ein echtes strafprozessuales Novum. Bislang war diese Ermittlungsmaßnahme in Deutschland zu repressiven Zwecken unzulässig. Die im August 2017 in Kraft getretene Regelung orientiert sich einerseits am Regelungsvorbild des früheren § 20k des Bundeskriminalamtsgesetzes (BKAG) inklusive der diesen teilweise für verfassungswidrig erklärenden Entscheidung des BVerfG[3], andererseits an der bestehenden Regelung zur akustischen Wohnraumüberwachung, die bei uns in Deutschland meist als „großer Lauschangriff“ bezeichnet wird. Ganz grob kann man sagen, dass die Voraussetzungen für eine Online-Durchsuchung nach § 100b StPO überwiegend denen für eine akustische Wohnraumüberwachung nach § 100c StPO entsprechen. Dies verdeutlicht bereits ein *gemeinsamer Katalog* von „besonders schweren Straftaten“ (§ 100b Abs. 2 StPO), der die für beide Maßnahmen erforderlichen *Anlasstaten* legal definiert. In einem wesentlichen Punkt weicht die neu geschaffene Online-Durchsuchung jedoch von der bereits im Jahr 1998 eingeführten Wohnraumüberwachung ab: Anders als dort muss für die Anordnung einer Online-Durchsuchung nicht aufgrund tatsächlicher Anhaltspunkte anzunehmen sein, dass die Maßnahme Erkenntnisse bringen wird, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind.

2. Gefahr der Dauerüberwachung

§ 100b Abs. 1 StPO erlaubt den „Eingriff“ in ein vom Betroffenen genutztes informationstechnisches System und die Erhebung von „Daten“ hieraus „mit technischen Mitteln“. Ein solcher „Eingriff mit technischen Mitteln“ ist dabei genauso wie im Zusammenhang mit der Quellen-TKÜ zu verstehen. Gemeint ist die verdeckte Infiltration von IT-Systemen durch staatliche Überwachungssoftware. Der Datenbegriff geht hier jedoch (weit) über die von § 100a StPO erfassten (laufenden) Telekommunikationsdaten

[3] BVerfGE 141, 220.

hinaus. § 100b Abs. 1 StPO erlaubt die Erhebung *aller* Daten *ohne jede zeitliche oder inhaltliche Beschränkung*. Bei näherer Betrachtung ist dann auch die Bezeichnung der Maßnahme als „Online-Durchsuchung“ ist irreführend. Im Gegensatz zu einer klassischen Durchsuchung handelt es sich bei der „Online-Durchsuchung“ nicht um eine punktuelle Maßnahme. Vielmehr dürfen innerhalb des Anordnungszeitraumes laufend weiter (sowohl bereits vorhandene, als auch neu hinzukommende) Daten erhoben werden. Es handelt sich daher nicht um eine einmalige „Durchsuchung“, sondern um eine umfassende, verdeckte *Online-Systemüberwachung*. Allerdings muss sich die Datenerhebung aus Gründen der Verhältnismäßigkeit auf verfahrensrelevante Daten beschränken. Die zu erhebenden Daten sind gem. § 100e Abs. 3 Nr. 3 und 4 StPO bereits in der Anordnung der Maßnahme durch das zuständige Gericht möglichst präzise zu bezeichnen, um eine überschießende Datenerhebung zu vermeiden. Um verfahrensrelevante Daten aber in der Praxis überhaupt identifizieren zu können, ist damit aber zwangsläufig immer auch die Befugnis zu einer Live-Durchsicht der Daten durch einen ermittelnden Beamten der Polizei mittels der Überwachungssoftware verbunden.

Der *Personenkreis*, der von einer Online-Durchsuchung *betroffen* sein kann, wird durch § 100b Abs. 3 StPO bestimmt. Danach darf sich die Maßnahme grundsätzlich nur gegen den *Beschuldigten* richten (§ 100b Abs. 3 Satz 1 StPO). Eine Infiltration der informationstechnischen Systeme *anderer Personen* darf ausnahmsweise aber dann erfolgen, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte das IT-System der anderen Person benutzt und dass allein der Eingriff in das IT-System des Beschuldigten keine Aufklärung des Sachverhalts oder Ermittlung des Aufenthaltes eines Mitbeschuldigten erwarten lässt. Der Gesetzgeber wollte bei dieser Regelung nicht zwingend auf die Eigentumsverhältnisse an den betreffenden IT-Systemen abstellen. Das IT-System „gehört“ also demjenigen, der es als eigenes nutzt, mag er auch im zivilrechtlichen Sinne nicht dessen Eigentümer sein. Diese Konstruktion wirft rechtliche Zweifelsfragen auf. Fraglich ist in diesem Zusammenhang beispielsweise, ob bei informationstechnischen Systemen, die von vielen Personen genutzt werden (z.B. Computer in öffentlichen Internet-Cafés und Service-Points oder Server von Cloud-

Dienstleistern) schon eine einfache, möglicherweise nur einmalige Mitbenutzung durch den Beschuldigten eine Überwachung des gesamten Systems und damit einer Vielzahl unbeteiligter Personen rechtfertigen kann.

IV. Begleitende Änderungen

1. Schutz des Kernbereichs privater Lebensgestaltung sowie von Zeugnisverweigerungsberechtigten

Nach Art. 1 Abs. 1 des deutschen Grundgesetzes (GG), unserer Verfassung, ist die Würde des Menschen unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Eine solche Verletzung der Menschenwürdegarantie liegt insbesondere vor, wenn von staatlicher Seite der sog. „Kernbereich privater Lebensgestaltung“ ausgeforscht wird. Dazu gehört nach Ansicht des deutschen Bundesverfassungsgerichts jedenfalls, die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne Angst vor staatlicher Überwachung zum Ausdruck zu bringen. Etwas anderes gilt lediglich dann, wenn es sich um Äußerungsformen handelt, die Angaben über geplante oder begangene Straftaten enthalten. Vor diesem Hintergrund fasst der neu formulierte § 100d StPO nun die bisher über verschiedene Eingriffsmaßnahmen verstreuten Kernbereichsregelungen für die §§ 100a bis 100c StPO zusammen. Die Absätze 1 und 2 regeln das auch schon bislang bestehende absolute Beweiserhebungsverbot bei alleinigem Kernbereichsbezug und das Beweisverwertungsverbot für alle erhobenen kernbereichsrelevanten Informationen. § 100d Abs. 3 StPO enthält zudem eine zumindest formal weitergehende Schutzregelung für die OnlineDurchsuchung. Soweit möglich muss danach technisch, also durch eine entsprechende Programmbeschränkung der Überwachungssoftware, sichergestellt werden, dass Kernbereichsdaten nicht erhoben werden. Diese Regelung ist aus zweierlei Gründen misslungen: Zum einen setzt die Feststellung, ob es sich um kernbereichsrelevante Daten handelt, eine vorherige Analyse der Daten auf dem System denknotwendig voraus. Zum anderen erfordert die Einordnung von Daten als

zum Kernbereich privater Lebensführung gehörend einen komplexen und normativen Abwägungsvorgang, den ein Computerprogramm ohne menschliche Steuerung zumindest nach dem derzeitigen Stand der Technik gar nicht leisten kann.

In § 100d Abs. 5 StPO findet sich eine bislang in § 100 c Abs. 6 StPO a.F. enthaltene Normierung des *Schutzes von bestimmten Gruppen zeugnisverweigerungsberechtigter Personen*, insbesondere der Berufsgeheimnisträger. Diese Regelung wird nunmehr auf die Online-Durchsuchung erstreckt. Für die QuellenTKÜ gilt demgegenüber – genau wie für die „normale“ TKÜ – lediglich ein weniger weit reichender Schutz (nach § 160a StPO).

2. Verfahrensvorschriften

Hinsichtlich der *Anordnungskompetenz* gilt für die neu eingeführte Quellen-TKÜ nach § 100e Abs. 1 StPO das schon bislang für die „normale“ TKÜ Gültige (Ermittlungsrichtervorbehalt, Eilkompetenz der Staatsanwaltschaft, Befristung und entsprechende Verlängerung von drei Monaten). Für die Online-Durchsuchung kommen dagegen nach § 100e Abs. 2 StPO die Regelungen für die Wohnraumüberwachung zur Anwendung (Landgerichtskammervorbehalt, Eilkompetenz des Vorsitzenden, Befristung und entsprechende Verlängerung von einem Monat). §100e Abs. 3 StPO enthält Regelungen zu *Form und Inhalt der Anordnung*, die das Verfahren insgesamt transparenter machen sollen. Anders als früher müssen nun für alle Maßnahmen nach §§ 100a bis 100c StPO Art und Bedeutung der zu erhebenden Informationen angeführt werden. Bei der Quellen-TKÜ und der Online-Durchsuchung muss außerdem das betroffene informationstechnische System genau bezeichnet werden. Regelungen über die *Beendigung* der Maßnahme und die *Unterrichtung* über den Verlauf finden sich zusammengefasst für alle Maßnahmen in § 100e Abs. 5 StPO, wobei auch hier die strengeren Vorschriften der Wohnraumüberwachung für die Online-Durchsuchung gelten. Schließlich wurden die Quellen-TKÜ und die OnlineDurchsuchung in die allgemeinen Verfahrensregelungen für verdeckte Maßnahmen in § 101 StPO einbezogen. Und in einem neuen § 101b StPO finden sich nunmehr zusammengefasst und unter Einbeziehung

der Quellen-TKÜ und der Online-Durchsuchung *Statistik- und Berichtspflichten*.

V. Bemerkungen zur eingesetzten Technik

1. Problematische Begrifflichkeiten

Vor dem Hintergrund der geschilderten neuen Rechtslage in der Bundesrepublik Deutschland empfiehlt sich zumindest ein kurzer und kritischer Blick auf die dadurch einsetzbare Überwachungstechnik. Aus technischer Sicht sind schon die Begriffe „Quellen-Telekommunikationsüberwachung“ und „Online-Durchsuchung“ irreführend. Mit ihnen verbindet man jedenfalls als Laie eine gewisse Nähe zu allgemein akzeptierten und etablierten Ermittlungsmaßnahmen. Die Realität ist aber eine andere. Bei der klassischen Telekommunikationsüberwachung wird lediglich passiv im Telekommunikationsnetz mitgehört. Die mit der Quellen-TKÜ verbundene Infiltration eines Computers durch ein Spähprogramm ist demgegenüber ein aktiver Vorgang, der das Zielsystem verändert. Entsprechendes gilt für die Online-Durchsuchung. Durch die begriffliche Nähe zur allgemeinen Durchsuchung assoziiert man zwar durchaus auch eine eingriffsintensive Maßnahme. Allerdings ist die Durchsuchung von ihrer Natur her eine offene, punktuelle und einmalige Maßnahme, bei der ein Beschuldigter auch anwesend sein und Polizei und Staatsanwaltschaft bei ihrer Arbeit beobachten kann. Hinzu kommt, dass eine Quellen-TKÜ nicht zwangsläufig weniger eingriffsintensiv sein muss als eine Online-Durchsuchung. Dies mag in vielen Fällen in der Tat so sein. Allerdings darf man nicht vergessen, dass in beiden Fällen das Zielsystem infiltriert wird, und zwar mit einem *potentiellen Vollzugriff* auf dessen Ressourcen. Die von den Strafverfolgungsbehörden eingesetzte Spähsoftware operiert wie ein „programmgesteuerter verdeckter Ermittler“ im Zielsystem. Menschliche verdeckte Ermittler sind aber, auch wenn sie unter falscher Identität operieren, jederzeit für ihre Umgebung wahrnehmbar. Bei einer Spähsoftware ist demgegenüber nicht nur ihr Zweck verdeckt, sondern sogar ihre Existenz.

2. Bemerkungen zur Quellen-TKÜ

Speziell die neuen gesetzlichen Regelungen zur Quellen-TKÜ sollen den Zugriff auf verschlüsselte Datenströme ermöglichen. Dies ist immer dann notwendig, wenn der für die Übertragung genutzte Schlüssel den Ermittlungsbehörden unbekannt ist und wenn „Ende zu Ende (end to end)“ verschlüsselt wird. Vereinfacht gesagt vereinbaren das Ausgangs- und das Zielsystem der Datenübertragung einen gemeinsamen geheimen Schlüssel. Dieser Schlüssel existiert in der Regel nur auf diesen beiden Systemen und auch nur für die Dauer der Datenübertragung. Mit ihm werden die zu sendenden Daten auf dem Ausgangssystem verschlüsselt, bevor diese ins Netzwerk gelangen. Auf dem Zielsystem angekommen, können diese dann mit demselben Schlüssel wieder in verständliche Zeichenfolgen zurückgerechnet werden. Ohne Kenntnis des Schlüssels, d.h. auf dem kompletten Übertragungsweg der Daten im Netz, sind die eigentlichen Inhalte des Datenstroms für Außenstehende komplett unverständlich. Diese technischen Hürden für die Strafverfolgungsbehörden werden durch den neu gefassten § 100a StPO überwunden und dadurch die Chancengleichheit zwischen Polizei und Staatsanwaltschaft auf der einen und (potenziellen) Beschuldigten auf der anderen Seite, die sich neuer, verschlüsselter Kommunikationsformen bedienen, wiederhergestellt.

3. Bemerkungen zur Online-Durchsuchung

Aus technischer und rechtsstaatlicher Sicht ist die Online-Durchsuchung gemäß § 100b StPO demgegenüber als deutlich problematischer einzustufen. Schon der Wortlaut des Gesetzes ist in hohem Maße unbestimmt. Die Erlaubnis, in ein informationstechnisches System „einzugreifen“ und aus diesem „Daten zu erheben“, erfasst jede Art programmgesteuerter Datenverarbeitung von der Anfertigung und Ausleitung einer bitweisen 1:1-Kopie der vom System verwendeten Datenträger bis hin zur vollständigen Fremdsteuerung des Systems einschließlich seines Kommunikationsverhaltens. Unabhängig davon, dass durch die neuen Anforderungen an die Anordnungsentscheidung nach § 100e Abs. 3 StPO der Umfang der Maßnahme sowie die Art der durch die Maßnahme zu erhebenden Informationen schriftlich eingeschränkt werden sollten, ist die Eingriffsintensität der Maßnahme nicht bloß mit der einer akustischen

Wohnraumüberwachung vergleichbar. Auch wenn die Eingriffe in das überwachte System ausschließlich dem Zweck dienen sollen, die Datenerhebung zu ermöglichen, geht die Regelung aus technischer Sicht gerade im Hinblick auf die verdeckte Einflussnahme auf das Zielsystem deutlich darüber hinaus.

VI. Verfassungsrechtliche Schranken

Gestatten Sie mir deshalb zum Abschluss einige kurze Bemerkungen zur verfassungsrechtlichen Einordnung der neuen strafprozessualen Ermittlungsinstrumente. Insofern ist unbestritten, dass sowohl die Quellen-TKÜ als auch die Online-Durchsuchung in erheblichem Maße jedenfalls in das *Allgemeine Persönlichkeitsrecht* (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) der von der Überwachung betroffenen Personen eingreift. Andererseits ist das allgemeine gesellschaftliche Klima derzeit in Deutschland für die Einführung neuer Überwachungsbefugnisse besonders günstig. Wie Sie sicherlich wissen, steht unser Land ebenso wie andere westliche Staaten im Fokus islamistischer Terrorgruppierungen wie Al-Qaida oder Islamischer Staat (IS). Besonders der terroristische Anschlag auf den Weihnachtsmarkt am Berliner Breitscheidplatz direkt an der Gedächtniskirche und damit im Herzen unserer Hauptstadt am 19. Dezember 2016, bei dem elf Menschen starben und 55 Personen teilweise schwer verletzt wurden, hat nicht nur die Menschen in Deutschland erschüttert. Er hat auch die sensible Balance zwischen individuellen Freiheitsrechten der Bürger und kollektivem Sicherheitsbedürfnis erheblich zu Lasten des Letzteren verschoben. Damit sind auch die neuen Befugnisnormen zur strafprozessualen Quellen-TKÜ und Online-Durchsuchung immer vor dem Hintergrund der generellen terroristischen Bedrohung zu sehen.

1. Geeignetheit und Erforderlichkeit

Die Abwehr von Gefahren durch den internationalen Terrorismus ist nach Ansicht des deutschen Bundesverfassungsgerichts auch im Kontext der Strafverfolgung ein *legitimes Ziel*. In seiner wegweisenden Entscheidung zum Bundeskriminalamtsgesetz aus dem

Jahr 2016[4] hat es bei den besonders eingriffsintensiven Maßnahmen allerdings darauf abgestellt, dass eine Gefahr für überragend wichtige Rechtsgüter, wie Leben, Leib, Freiheit einer Person oder Güter der Allgemeinheit, deren Bedrohung die Grundlagen der Existenz der Menschen berührt, bestehen muss. Übertragen auf den Bereich des repressiven Strafrechts tritt an die Stelle einer solchen Gefahr ein *Katalog derjenigen Straftaten*, die bei einer entsprechenden Verdachtslage zu der jeweiligen strafprozessualen Ermittlungsmaßnahme ermächtigen. So müssen bei Telekommunikationsüberwach ungsmaßnahmen bestimmte Tatsachen einen Anfangsverdacht hinsichtlich einer im Katalog des § 100a Abs. 2 StPO genannten „schweren Straftat“ und bei der Online-Durchsuchungen sogar hinsichtlich einer in § 100b Abs. 2 StPO aufgeführten „besonders schweren Straftat“ begründen. Ob diese Einstufung bei allen der in diesen umfangreichen Straftatkatalogen aufgeführten Delikten tatsächlich zutrifft, ist allerdings kritisch zu hinterfragen. Dass etwa die Geld- und Wertzeichenfälschung nach §§ 146, 151 StGB (§ 100b Abs. 2 Nr. 1c StPO) oder der Bandendiebstahl nach § 244 Abs. 1 Nr. 2 StGB (§ 100b Abs. 2 Nr. 1h StPO) von seinem Unrechtsgehalt her tatsächlich einer terroristischen Gefahr gleichsteht, wird sich kaum ernsthaft begründen lassen. Insofern dürften diese Straftatkataloge jedenfalls in Teilen zu weit geraten sein.

2. Verhältnismäßigkeit

Blickt man auf die bisherige Rechtsprechung des Bundesverfassungsgerichts, so dürften gegenüber der Einführung der *Quellen-Telekommunikationsüberwachung* für Zwecke der Strafverfolgung keine grundsätzlichen verfassungsrechtlichen Bedenken bestehen. Schließlich geht es mit der Überwachung von Telekommunikationsvorgängen um eine seit langem anerkannte und zulässige Ermittlungsmaßnahme, die lediglich aufgrund zwischenzeitlicher technischer Veränderungen und Fortschritte, insbesondere durch den Einsatz von Verschlüsselungstechnik, mit den bisherigen Mitteln nicht mehr erfolgversprechend durchgeführt werden kann. Von einer Mindermeinung im juristischen Schrifttum wurde sie deshalb sogar schon vor der gesetzlichen Neuregelung von 2017

4 BVerfGE 141, 220.

im Wege einer Annexkompetenz auf der Grundlage von § 100a StPO a.F. für zulässig gehalten.[5] Das Bundesverfassungsgericht sieht keine verfassungsrechtlichen Probleme, solange bei der Quellen-TKÜ ein *technisches Funktionsäquivalent zur konventionellen Telekommunikationsüberwachung* eingesetzt wird. Solange also sichergestellt ist, dass die Maßnahme auf die Überwachung der laufenden Telekommunikation beschränkt ist, ist sie zulässig. Eine solche Parallelität zwischen TKÜ und Quellen-TKÜ besteht aber nur soweit, wie tatsächlich die laufende Telekommunikation überwacht wird. Bei Daten nach § 100a Abs. 5 Nr. 1 b StPO, d.h. Informationen, die *nach der Anordnung* der Maßnahme, aber *vor dem tatsächlichen technischen Zugriff* gespeichert wurden, versagt demnach die Eingriffsrechtfertigung durch das Bundesverfassungsgericht. Hier handelt es sich tatsächlich um eine (beschränkte) Online-Durchsuchung.

Zu Recht nimmt das Bundesverfassungsgericht hier an, dass die Intensität des Grundrechtseingriffs auf Grund des Umgangs mit informationstechnischen Systemen mit einem Eingriff in die Unverletzlichkeit der Wohnung nach Art. 13 des deutschen Grundgesetzes (GG) vergleichbar ist. Die Anordnung steht deshalb unter dem Vorbehalt, dass die Sachverhaltserforschung ohne die Maßnahme wesentlich erschwert oder aussichtslos wäre. Hier wird ein vom Bundesverfassungsgericht eher beiläufig geäußerter Satz relevant: „Zur Beachtung des Verhältnismäßigkeitsgrundsatzes im Einzelfall gehört auch, dass ein offener Zugriff auf die Datenbestände einer Zielperson vor einer heimlichen Infiltration grundsätzlich Vorrang hat".[6] Daraus folgt zwangsläufig, dass die Anordnungsvoraussetzung für Online-Durchsuchungen nach § 100b Abs. 1 Nr. 3 StPO im Einzelfall besonders intensiv geprüft werden müssen und darzulegen ist, warum eine offene Durchsuchung keinen Erfolg verspricht. Im Übrigen wird im Zusammenhang mit staatlichen Überwachungsmaßnahmen die Intensität des Eingriffs stets auch durch die *Dauer der Maßnahme* bestimmt. Drei Monate hat das Bundesverfassungsgericht als Obergrenze gerade noch akzeptiert. Diese Zeitgrenze ist nach neuem Recht nur scheinbar gewahrt. Gemäß § 100e Abs. 2 S. 4 StPO beträgt die Anordnungsdauer

5 Vgl. *Meyer-Goßner/Schmitt*, StPO, § 100d Rn. 2.

6 BVerfGE 141, 220 (305 f.).

zwar grundsätzlich nur einen Monat. Allerdings kennt das Gesetz keine Höchstdauer. Es wird lediglich festgestellt, dass nach sechs Monaten über weitere Verlängerungen das Oberlandesgericht entscheidet (§ 100e Abs. 2 S. 6 StPO). Diese nach der neuen deutschen Strafprozessordnung letztlich unbefristet mögliche Dauerüberwachung informationstechnischer Systeme ist unter Verhältnismäßigkeitsgesichtspunkten nicht mehr zu rechtfertigen und damit als verfassungswidrig einzustufen.

VII. Fazit

Für eine eingehende Bewertung der gesetzlichen Neuregelungen erscheint es zum gegenwärtigen Zeitpunkt noch zu früh. Empirische Auswertungen zum praktischen Umgang mit den neuen Befugnissen liegen noch nicht vor. Aber auch wenn man die grundsätzliche Berechtigung von Quellen-TKÜ und Online-Durchsuchung in Zeiten einer fühlbaren Bedrohung durch den internationalen Terrorismus nicht leugnen kann, merkt man den neu geschaffenen Vorschriften doch stellenweise an, dass es sich um einen „gesetzgeberischen Schnellschuss“ gehandelt hat. In Details besteht hier durchaus noch Nachbesserungsbedarf. Zwar stehen speziell der Quellen-TKÜ als Antwort auf den fortschreitenden Einsatz von Verschlüsselungstechnik in der Kommunikation keine grundlegenden verfassungsrechtlichen Hindernisse entgegen. Allerdings schießt die neue Regelung durch die generelle Befugnis zur Erhebung der (zukünftigen) Kommunikationsdaten auf dem infizierten System über das Ziel hinaus. Dies gilt auch deshalb, weil IT-Experten darauf verweisen, dass bei vielen Kommunikationsanwendungen eine Ausleitung der vorn jeweiligen Kommunikationsprogramm verwendeten Schlüssel und eine anschließende Erhebung der Daten „aus der Leitung“ möglich und ausreichend ist.

Die Befugnis zur heimlichen Infiltration von informationstechnischen Systemen und zur dauerhaften Erhebung von Daten hieraus durch die Online-Durchsuchung stellt in ihrer derzeitigen (weiten) Fassung einen extrem intensiven und kaum rechtfertigbaren Grundrechtseingriff dar, dies nicht zuletzt wegen ihrer technischen Unbestimmtheit, der

faktisch unbegrenzten Zeitdauer und der faktischen Unüberprüfbarkeit der Maßnahme im Nachhinein.

Schließlich verbleibt bei jeder Art des Einsatzes von staatlicher Spähsoftware das Problem, dass dabei Sicherheitslücken im Zielsystem ausgenutzt werden müssen, um zu funktionieren. Der Staat wird hierdurch quasi zum Teilnehmer am sog. „ExploitMarkt". Dies konterkariert jedenfalls in Deutschland die intensiven staatlichen Bemühungen um eine Verbesserung der allgemeinen IT-Sicherheit für die Bürger. Insofern ist es kein Wunder, dass bereits eine Reihe von Verfassungsbeschwerden gegen die neuen strafprozessualen Regelungen zur Quellen-Telekommunikationsüberwachung und zur Online-Durchsuchung beim Bundesverfassungsgericht in Karlsruhe anhängig sind. Es ist zu erwarten, dass die Verfassungsrichter hier jedenfalls in Einzelheiten Nachbesserungen vom deutschen Gesetzgeber verlangen werden. Bis zu dieser Entscheidung sollten die neuen Regelungen in der deutschen Strafprozessordnung somit nur mit großer Vorsicht als Regelungsvorbild in Betracht gezogen werden.

Vielen Dank für Ihre Aufmerksamkeit!

- Gesetzestexte –

Strafprozessordnung (StPO)– Auszug

§ 100a [Telekommunikationsüberwachung]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1 aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,

b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,

c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,

d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,

f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Absatz 1 und 2, § 184c Absatz 2,

h) Mord und Totschlag nach den §§ 211 und 212,

i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 11 genannten schweren Straftaten herrührt,

n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,

o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,

p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,

q) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,

r) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,

s) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

t) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,

u) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Anti-Doping-Gesetz:

Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,

4. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:
   a) Einschleusen von Ausländern nach § 96 Abs. 2,
   b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,
6. aus dem Außenwirtschaftsgesetz:
   vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,
7. aus dem Betäubungsmittelgesetz:
   a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,
   b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,
8. aus dem Grundstoffüberwachungsgesetz:
   Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,
9. aus dem Gesetz über die Kontrolle von Kriegswaffen:
   a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,
   b) Straftaten nach § 22a Abs. 1 bis 3,

9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:
   Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,

10. aus dem Völkerstrafgesetzbuch:
   a) Völkermord nach § 6,
   b) Verbrechen gegen die Menschlichkeit nach § 7,
   c) Kriegsverbrechen nach den §§ 8 bis 12,
   d) Verbrechen der Aggression nach § 13,
11. aus dem Waffengesetz:
   a) Straftaten nach § 51 Abs. 1 bis 3,
   b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

(4) Auf Grund der Anordnung einer Überwachung und Aufzeichnung der

Telekommunikation hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) diese Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Absatz 2 gilt entsprechend.

(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:
   a) die laufende Telekommunikation (Absatz 1 Satz 2), oder
   b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

   Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b [Online-Durchsuchung]

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer

eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:
   a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,
   b) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,
   c) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,
   d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Absatz 2 Nummer 2 oder Absatz 3 und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
   e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Absatz 2,
   f) Mord und Totschlag nach den §§ 211, 212,
   g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, der §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,
   h) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,
   i) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

j) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,
k) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,
l) besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz 4 Satz 2 genannten Voraussetzungen; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 7 genannten besonders schweren Straftaten herrührt,
m) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylgesetz:
   a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,
   b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,
3. aus dem Aufenthaltsgesetz:
   a) Einschleusen von Ausländern nach § 96 Absatz 2,
   b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,
4. aus dem Betäubungsmittelgesetz:
   a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,
   b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,
5. aus dem Gesetz über die Kontrolle von Kriegswaffen:
   a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,
   b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,
6. aus dem Völkerstrafgesetzbuch:
   a) Völkermord nach § 6,
   b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,
d) Verbrechen der Aggression nach § 13,

7. aus dem Waffengesetz:
a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,
b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.

(3) 1Die Maßnahme darf sich nur gegen den Beschuldigten richten.2Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und
2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.

§ 100c [Akustische Wohnraumüberwachung]

(1) Auch ohne Wissen der Betroffenen darf das in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt,
3. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind, und
4. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.

(2) Die Maßnahme darf sich nur gegen den Beschuldigten richten und nur in Wohnungendes Beschuldigten durchgeführt werden. In Wohnungen anderer Personen ist die Maßnahme nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte sich dort aufhält und
2. die Maßnahme in Wohnungen des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

§ 100d [Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte]

(1) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100a bis 100c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig.

(2) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(3) Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(4) Maßnahmen nach § 100c dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden.

Ist eine Maßnahme unterbrochen worden, so darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Im Zweifel hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen; § 100e Absatz 5 gilt entsprechend. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, hat die Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts herbeizuführen. Absatz 3 Satz 3 gilt entsprechend.

(5) In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht. § 160a Absatz 4 gilt entsprechend.

§ 100e [Verfahren bei Maßnahmen nach den §§ 100a bis 100c]

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Maßnahmen nach den §§ 100b und 100c dürfen nur auf Antrag der Staatsanwaltschaft durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts angeordnet werden, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Bei Gefahr im Verzug kann diese Anordnung auch durch den Vorsitzenden getroffen werden. Dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen

Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

(3) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird,
3. Art, Umfang, Dauer und Endzeitpunkt der Maßnahme,
4. die Art der durch die Maßnahme zu erhebenden Informationen und ihre Bedeutung für das Verfahren,
5. bei Maßnahmen nach § 100a die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist; im Fall des § 100a Absatz 1 Satz 2 und 3 eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das eingegriffen werden soll,
6. bei Maßnahmen nach § 100b eine möglichst genaue Bezeichnung des informationstechnischen Systems, aus dem Daten erhoben werden sollen,
7. bei Maßnahmen nach § 100c die zu überwachende Wohnung oder die zu überwachenden Wohnräume.

(4) In der Begründung der Anordnung oder Verlängerung von Maßnahmen nach den §§ 100a bis 100c sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben:

1. die bestimmten Tatsachen, die den Verdacht begründen,
2. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme,
3. bei Maßnahmen nach § 100c die tatsächlichen Anhaltspunkte im Sinne des § 100d Absatz 4 Satz 1.

(5) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Bei Maßnahmen nach den §§ 100b und 100c ist das anordnende Gericht auch über den Verlauf zu unterrichten. Liegen die Voraussetzungen der Anordnung nicht

mehr vor, so hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die Staatsanwaltschaft veranlasst wurde. Die Anordnung des Abbruchs einer Maßnahme nach den §§ 100b und 100c kann auch durch den Vorsitzenden erfolgen.

(6) Die durch Maßnahmen nach den §§ 100b und 100c erlangten und verwertbaren personenbezogenen Daten dürfen für andere Zwecke nach folgenden Maßgaben verwendet werden:

1. Die Daten dürfen in anderen Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.
2 Die Verwendung der Daten, auch solcher nach § 100d Absatz 5 Satz 1 zweiter Halbsatz, zu Zwecken der Gefahrenabwehr ist nur zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person, für die Sicherheit oder den Bestand des Staates oder für Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, von kulturell herausragendem Wert oder in § 305 des Strafgesetzbuches genannt sind, zulässig. Die Daten dürfen auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte verwendet werden. Sind die Daten zur Abwehr der Gefahr oder für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen nicht mehr erforderlich, so sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.
3. Sind verwertbare personenbezogene Daten durch eine entsprechende polizeirechtliche Maßnahme erlangt worden, dürfen sie in einem Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer die Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.