Privatisierung technisch gestützter Ermittlungsmaßnahmen?

Frank Braun/Jan Dirk Roggenkamp

I. Ausgangslage

Ob und in welchem Umfang private Dienstleister in einer so sensiblen Materie wie dem strafrechtlichen Ermittlungsverfahren in die öffentliche Aufgabenerfüllung eingebunden werden können, ist bislang juristisch kaum erläutert worden. In der rechtspolitischen Diskussion sind die Stimmen ganz überwiegend ablehnend. So heißt es etwa: „Die grundrechtsrelevante Wahrnehmung und Erfüllung der Staatsaufgabe Sicherheit als Gefahrenabwehr- und Strafverfolgungsaufgabe [ist] nicht privatisierbar …, auch nicht in Teilen“[1] oder „Im Bereich der Strafjustiz muss … [ein Outsourcing] schon aus rechtlichen wie politischen Gründen an unumstößliche Grenzen stoßen“[2].

Davon lässt sich die Praxis nicht in jedem Fall abhalten. Nach einem Bericht von „SPIEGEL-ONLINE“ lagern deutsche Strafverfolgungsbehörden die Auswertung beschlagnahmter Speichermedien immer häufiger an private IT-Dienstleister aus. Anfragen hätten ergeben, dass zunehmend auch sensible Daten nicht mehr von Behörden, sondern von gewerblichen Anbietern ausgewertet würden[3]. Gerechtfertigt wurde in diesem Fall die Einbindung Privater in die staatliche Ermittlungstätigkeit mit deren „besonderen Sachkunde“[4]. Private IT-Dienstleister verfügen in der Tat über ein technisches Know-how, das als Fachwissen so im öffentlichen Dienst häufig nicht abrufbar ist. Und: Im Vergleich zur eigenverantwortlichen Aufgabenerledigung des Staates gelten private IT-Dienstleistungsunternehmen als zuverlässig, effizient und gleichzeitig kostengünstig[5]. Insoweit erscheint eine Einbindung privater Dienstleister auch in andere Ermittlungsmaßnahmen nicht abwegig, bei denen komplexe technische Hilfsmittel wie IMSI-Catcher[6] oder Software zur Durchführung einer Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingesetzt werden.

Auf Seiten der öffentlichen Hand stellen sich in diesem Zusammenhang folgende Fragen: Kann die Vornahme technisch anspruchsvoller Ermittlungsmaßnahmen zumindest teilweise Privaten übertragen werden? Können und dürfen komplexe technische Mittel – insbesondere Softwarelösungen (z.B. zur Durchführung von Online-Durchsuchungen) – „am Markt beschafft“ werden? Treffen den Staat in diesem Zusammenhang gegebenenfalls erweiterte Schutz- und Überwachungspflichten? Welche einfachgesetzlichen Regelungen sind bei „datenschutzrelevanten“ Tätigkeiten Privater im staatlichen Auftrag zu beachten?

II. Verfassungsrechtliche Grenzen

Das Grundgesetz kennt kein *ausdrückliches* Privatisierungsverbot[7]. Verfassungsrechtliche Grenzen bilden das *staatliche Gewaltmonopol* und der *Funktionsvorbehalt zugunsten des Berufsbeamtentums* aus Art. 33 Abs. 4 GG[8]. Eine Tätigkeit Privater im *Kernbereich* hoheitlicher Tätigkeit überschreitet diese Grenzen[9]. Was allerdings zu diesem privatisierungsfeindlichen „Kernbereich“ gehört, ist nicht pauschal bestimmbar. Nach hier geteilter Auffassung ist eine enge Auslegung des Begriffs vorzugswürdig[10]. Allein der Umstand, dass eine Aufgabe dem Bereich der Eingriffsverwaltung, der Gewährleistung der inneren Sicherheit, der Strafverfolgung oder des Strafvollzuges zuzurechnen ist, reicht alleine nicht aus, eine Einbindung Privater auszuschließen[11].

Sie darf indes nicht darauf hinauslaufen, dass eine genuin staatliche Aufgabe – die Durchführung der konkreten Ermittlungsmaßnahme – *vollständig* aufgegeben und der privaten Wahrnehmung überlassen wird (sog. Aufgabenprivatisierung[12] bzw. materielle Privatisierung[13]). Strafprozessuale Ermittlungsmaßnahmen sind stets Ausfluss des staatlichen Gewaltmonopols und damit einer materiellen Privatisierung von Verfassungs wegen nicht zugänglich, sondern dem Staat vorbehalten.[14]

Eine *funktionale Privatisierung* hingegen, also eine Ausführung bestimmter Aufgaben durch Private, bei der Verantwortung und Zuständigkeit auf Seiten des Staates verbleibt (Verwaltungshilfe)[15], ist nicht a priori durch das Grundgesetz ausgeschlossen. Allerdings unterfällt sie im unmittelbaren Kontext grundrechtssensibler Handlungen dem Kernbereichsvorbehalt. Eine funktional vollumfänglich privatisierte Online-Durchsuchung, eine (Quellen-)TKÜ oder ein „Lauschangriff“ sind dementsprechend unzulässig, da sie massive Grundrechtseingriffe darstellen. Das jeweilige eingriffsrelevante Handeln ist dem Staat vorbehalten und kann von diesem grundsätzlich nicht auf Private delegiert werden. Im vor- und nachbereitenden Umfeld der Maßnahme (z.B. bestimmte Datenverarbeitungsvorgänge) ist eine Einbindung Privater jedoch verfassungsrechtlich zulässig. Den verfassungsrechtlichen Schranken wird dabei – stark vergröbert – genüge getan, wenn die Einbindung Privater in die hoheitliche Aufgabenerfüllung auf *unselbständige* (untergeordnete) *Hilfstätigkeiten* beschränkt bleibt und die *Letztentscheidungskompetenz*[16] bzw. das eingriffsrelevante Handeln selbst dem Hoheitsträger vorbehalten wird[17].

1. Erstellung von Software mit Bezug zur hoheitlichen Aufgabenerfüllung durch Private

Problematisch ist die Entwicklung und Programmierung von Software, die aufgrund ihres Verwendungszweckes eine besondere Nähe zur Erfüllung hoheitlicher Kernaufgaben aufweist. Aktuelles Beispiel hierfür ist die stark kritisierte Software zur Durchführung einer Quellen-TKÜ (sog. „Staatstrojaner“[18]). Es erscheint nicht ganz abwegig, die Entwicklung und Programmierung der Software als dem Staat vorbehaltene, nicht privatisierungsfähige hoheitliche Tätigkeit i.S.d. Art. 33 Abs. 4 GG zu qualifizieren.

a) Grundsatz: Keine „hoheitliche Tätigkeit“ i.S.d. Art. 33 Abs. 4 GG

Grundsätzlich hat die Entwicklung und Herstellung von Software einen nachhaltigen Einfluss auf die Wahrnehmung der betreffenden staatlichen Aufgaben und insoweit auch unmittelbaren Bezug zur hoheitlichen Aufgabenerfüllung. So bestimmt die Software regelmäßig die Handlungsmöglichkeiten der Hoheitsträger und damit auch die Wahrnehmung der hoheitlichen Aufgabe selbst. Im Falle des Staatstrojaners war einer der Hauptkritikpunkte, dass die Softwarelösung des privaten Herstellers weitreichendere Funktionalitäten aufwies, als nach der

„Online-Durchsuchungs-Entscheidung" des *BVerfG* zulässig.[19] In einem Fall nutzte die Ermittlungsbehörde die Funktionalitäten zur Anfertigung unzulässiger Screenshots.[20]

Allerdings reicht dieser „Nähebezug" regelmäßig nicht aus, um die Entwicklung und Herstellung derartiger Software selbst als hoheitliche Tätigkeit zu qualifizieren. Das wäre nur dann der Fall, wenn es sich bei der Entwicklung und Herstellung der Software um eine Gestaltungsentscheidung handelte, die aufgrund eines damit verknüpften Verantwortungszusammenhangs zur eigentlichen Aufgabenwahrnehmung den spezifischen Bindungen hoheitlicher Tätigkeiten unterliegenmüsste. Nur dann wäre die Herstellung und Entwicklung als „hoheitliche Kernaufgabe" durch staatliche Handlungsträger zu bewerkstelligen. Grundsätzlich ist aber die Entwicklung von Software keine solche hoheitliche Tätigkeit, sondern bloße „nachgeordnete" Hilfstätigkeit. Denn bei der Entwicklung und Herstellung von Software setzt der private Auftragnehmer regelmäßig keine selbstbestimmten, eigenverantwortlichen Maßstäbe, die auf die Aufgabenerfüllung durchschlagen. Vielmehr handelt es sich um eine von der öffentlichen Hand determinierte „Auftragsarbeit" bzw. (im Falle bereits geleisteter Entwicklungsarbeit) um eine bewusste Auswahlentscheidung des Hoheitsträgers für eine konkrete Software mit bestimmten Funktionalitäten. Die grundlegenden Entscheidungen über die Entwicklung, Herstellung oder Auswahl der Software werden von dem Träger der eigentlichen Aufgabe getroffen, Herstellung und Entwicklung geschehen nach Maßgabe der beschaffenden Behörde[21].

Aus dem „Nähebezug" zwischen der Herstellung und Entwicklung von Software und der daran anknüpfenden eigentlichen hoheitlichen Aufgabenwahrnehmung lässt sich demnach grundsätzlich keine Privatisierungsschranke aus Art. 33 Abs. 4 GG ableiten. Ebenso wenig wie die Bundeswehr militärisches Gerät zu Verteidigungszwecken selbst entwickeln und herstellen muss, sind die Strafverfolgungsbehörden verpflichtet, die für ihre Ermittlungstätigkeit benötigten Radarmessgeräte, IMSI-Catcher, GPS-Sender oder Kfz-Kennzeichenlesegeräte in Eigenregie anzufertigen und zu programmieren. Sie können sich auf dem „privaten Markt" eindecken.

b) Ausnahme: Programmierung als staatliche Schutzpflicht

Etwas anders gilt aber dann, wenn die eingesetzte Technik die hoheitliche Aufgabenerfüllung rechtlich wie faktisch determiniert. Dies ist, wie zu zeigen ist, bei einer Onlinedurchsuchung als auch einer Quellen-TKÜ der Fall.

aa) Grundrechtliche Verpflichtung zum „Datenschutz durch Technik"

In neueren Entscheidungen hat das *BVerfG* mehrfach und unmissverständlich darauf hingewiesen, dass in spezifischen Sachzusammenhängen eine *grundrechtliche Verpflichtung* zum Datenschutz durch Technik besteht[22]. Der Staat muss spezifischen Gefährdungen, die aus dem Technikeinsatz hervorgehen, seinerseits mit Technikeinsatz begegnen. Es wird insoweit das Paradigma vom „Grundrechtsschutz durch technische Verfahren" aufgegriffen.[23] Durch Systemdatenschutz und durch gezielte Steuerung der eingesetzten technischen Systeme kann (im Optimalfall) erreicht werden, dass bestimmte Daten zwar verarbeitet, aber nicht gespeichert werden, sodass staatliche Grundrechtseingriffe minimiert werden.

Bemerkenswerte Ausführungen hierzu finden sich in der Entscheidung zur Online-Durchsuchung[24]. Das *BVerfG* verpflichtete Polizei und Ermittlungsbehörden für den Fall eines heimlichen Zugriffs auf informationstechnische Systeme dazu, Maßnahmen für einen automatisierten Persönlichkeitsschutz zu treffen. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach Feststellung des *BVerfG* zwar nicht so zuverlässig, „dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte."[25] Das bedeutet allerdings nicht, dass entsprechende Schutzvorkehrungen nicht erforderlich wären. Denn so stellt das Gericht fest: „Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten *soweit wie informationstechnisch* und ermittlungstechnisch *möglich* unterbleibt. Insbesondere sind *verfügbare informationstechnische Sicherungen einzusetzen*." Die staatlichen Ermittler haben also im Falle einer Online-Durchsuchung nicht nur dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte zweckentfremdet werden kann, sondern in gleichem Maße auch, dass durch die eingesetzte Software Eingriffe in das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme sowie in den Kernbereich privater Lebensgestaltung minimiert werden.[26]

Für den Fall einer *Quellen-TKÜ* macht das Gericht in derselben Entscheidung dann sogar die Zulässigkeit der Maßnahme selbst von geeigneten technischen Sicherungsmechanismen abhängig. Eine Quellen-TKÜ ist nur zulässig, wenn sich die Überwachung „ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang" beschränkt. Das muss „*durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt*" werden[27]. Folglich ist eine Quellen-TKÜ unzulässig, solange keine rechtskonforme Software existiert[28]. Die bis Ende 2011 verwandte Software entsprach nicht den Vorgaben des BVerfG[29]. Bislang wurde eine solche auch noch nicht geschaffen[30].

bb) Schutzpflicht aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Mit dem Vorgesagten wird die Interdependenz des „neuen" Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[31] auf die Entwicklung staatlicher Ermittlungssoftware auf den Begriff gebracht. Anders als bei „herkömmlichen" Ermittlungsmaßnahmen ist bei Onlinedurchsuchung und Quellen-TKÜ die Entwicklung der hierzu erforderlichen technischen Mittel nicht mehr nur bloße „nachgeordnete Hilfstätigkeit" im Rahmen der Erfüllung der hoheitlichen Ermittlungsmaßnahme .Sie ist *selbst wesentlicher Bestandteil der hoheitlichen Aufgabenerfüllung*. Schließlich verpflichtet das „neue" Grundrecht die öffentliche Hand ausdrücklich dazu, dafür Sorge zu tragen, dass die eingesetzte Software bestimmte Funktionalitäten aufweist bzw. gerade nicht aufweist.

(**1**) Die Entwicklung und Programmierung von Überwachungssoftware könnte somit als Teil der „hoheitlichen Aufgabenerfüllung" und damit grundsätzlich als nach Art. 33 Abs. 4 GG dem Staat vorbehalten angesehen werden. Das Vorhandensein bestimmter Funktionalitäten der eingesetzten Software entscheidet etwa, ob bei ihrem Einsatz eine Quellen-TKÜ oder eine nach der StPO unzulässige „überschießende" Onlinedurchsuchung vorliegt[32].

Der absolut privatisierungsresistente „Kernbereich“ hoheitlicher Aufgabenerfüllung ist dadurch jedoch noch nicht berührt. Das wäre erst der Fall, wenn private Dienstleister auch in die Durchführung der Maßnahme eingebunden würden. So könnte eine Übertragung der hoheitlichen Aufgabe „Softwareentwicklung“ jedenfalls durch Schaffung einer formellgesetzlichen Rechtsgrundlage (also durch eine Beleihung[33]) gerechtfertigt werden. An dem Bestehen eines anerkannten verfassungsrechtlichen Rechtfertigungsgrundes kann dabei nicht gezweifelt werden. Denn ein begründeter Ausnahmefall, der eine Beleihung rechtfertigen kann, liegt jedenfalls vor, wenn zur Erfüllung der konkreten Aufgabe Private wesentlich besser geeignet sind als staatliche Stellen, etwa weil seitens des Privaten eine besondere Sach- und Fachkenntnis oder technische Ausstattung[34] vorliegt. Das ist für den Bereich der Softwareentwicklung eindeutig zu bejahen.

Folge dieser Argumentation wäre, dass eine gesetzliche Regelung erforderlich wäre, um private Dienstleister mit der Entwicklung entsprechender Software zu beauftragen. Die Beleihung würde zwischen dem beliehenen privaten Softwarehaus und der beleihenden öffentlichen Stelle ein öffentlich-rechtliches Auftrags- und Treuhandverhältnis begründen. Die zugrunde liegenden Rechte und Pflichten ergäben sich aus zu schaffenden öffentlich-rechtlichen Vorschriften, insb. dem speziellen Beleihungsgesetz und aus den konkreten Beleihungsumsetzungsakten.

(2) Man könnte aber auch – was naheliegender erscheint –feinsinniger argumentieren und zu dem Schluss kommen, dass vorliegend nicht die Entwicklung der Software Teil der öffentlichen Aufgabenwahrnehmung ist, sondern nur die Gewährleistung, dass die Software bestimmte abstrakt umschriebene Funktionalitäten aufweist bzw. nicht aufweist. Dann bestünde nur eine konkrete, direkt aus dem Grundgesetz abgeleitete Aufsichtspflicht des Staates gegenüber dem privaten Softwareentwickler. Letzterer wäre Verwaltungshelfer, da er bei der Gewährleistung des Einsatzes verfassungskonformer Software und damit bei der öffentlichen Aufgabenwahrnehmung „weisungsgebundene Hilfstätigkeiten“ leistet. Ein Konflikt mit dem Funktionsvorbehalt des Art. 33 Abs. 4 GG bestünde dann nicht. Jedoch darf sich der Staat in diesem Fall nicht seiner *Leitungs- (bzw. Legitimations-)verantwortung* entziehen. Es ist zu berücksichtigen, dass sich die Leistung des funktionalen Verwaltungshelfers unmittelbar auf die Verwirklichung der Staatsaufgabe auswirkt. Staatlichem Lenkungs- und Kontrollverlust ist deshalb effektiv vorzubeugen. Diese Verpflichtung findet ihre Grundlage im *Rechtsstaatsprinzip und hier auch im Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Nach *Burgi*[35] soll in dem Moment, in dem der Staat private Vorbereitungsgeschäfte zulässt, an sie anknüpft oder sie sich zu eigen macht, eine *Strukturschaffungspflicht* entstehen, um aus der praktischen Aufgabenverteilung auch eine „gemeinwohlverträgliche Verantwortungsteilung“ werden zu lassen. Spaltet der Staat Teile seiner Verantwortung an Private ab, wandelt sich seine Pflicht zur Einhaltung der verfahrensmäßig-organisatorischen Verfassungsanforderungen in eine Strukturschaffungspflicht gegenüber dem eingeschalteten Privaten im Sinne einer normativen Leistungsverantwortung[36]. Bezüglich des Inhalts derartiger Strukturen wird vor allem die Sicherung der umsichtigen *Auswahl des privaten Verwaltungshelfers* hinsichtlich dessen Neutralität, Objektivität und Leistungsfähigkeit gefordert, die Statuierung effizienter und flexibler *Kontrollmöglichkeiten*, eine angemessene Präventivsteuerung über *Weisungsrechte* usw.[37]Wie die „Staatstrojaner-Affäre“ eindrucksvoll gezeigt hat, sind die staatlichen Ermittlungsbehörden diesen Verpflichtungen bei Beschaffung der Überwachungssoftware nicht nachgekommen. Sowohl die Ausführungen des Chaos-Computer-Clubs[38], der die eingesetzte Technik analysiert und damit den Stein des Anstoßes ins Rollen gebracht hat, als auch ein Bericht des Bundesdatenschutzbeauftragten[39] und des bayerischen Datenschutzbeauftragten[40] lassen den Schluss zu, dass der Staat seine Schutzpflichten eindeutig missachtet hat. Das, so suggerieren es die Einlassungen der zuständigen Behörden zumindest, mag an bislang fehlenden technischen Kompetenzen gelegen haben.[41]

Insoweit bleibt die Frage zu stellen, welche staatlichen Stellen (Kern)kompetenzen aufweisen, die gegenständlich nutzbar gemacht werden könnten. Die Antwort fällt leicht: das *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, dessen diesbezügliche Fähigkeiten und personelle Ausstattung unbestritten sind. Für eine Einbindung des BSI bei der Gewährleistung der verfassungskonformen Gestaltung technischer Überwachungsmittel streitet auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[42]. Kern der grundrechtlichen IT-Schutzpflichten ist die Entwicklung und der Ausbau der rechtlichen Grundlagen zum Aufbau einer IT-Sicherheitsstrategie. So begründet die aus dem „neuen“ Grundrecht resultierende Schutzpflicht eine Pflicht des Staates, die Kompetenzen und Befugnisgrundlagen im Bereich der IT-Sicherheit im Geiste der verfassungsrechtlichen Garantien weiterzuentwickeln.[43] Die nationalen Strukturen sind dabei so auszugestalten, dass die staatlichen Handlungsträger in die Lage versetzt werden[44], den Herausforderungen der IT-Sicherheitsgewährleistung effektiv zu begegnen. Mit der Stärkung des BSI wurden hierfür in den vergangenen Jahren erste Schritte gegangen. Ihm wurde bereits eine Vielzahl von Aufgaben im Zusammenhang mit der Gewährleistung der IT-Sicherheit und damit zugleich auch im Hinblick auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zugewiesen. Dazu zählen Informations- und Beratungspflichten, die Unterstützung von Polizei-, Sicherheits- und Verfassungsschutzbehörden sowie Grundlagen- und Forschungsarbeit etwa zur Analyse von Sicherheitsrisiken und Bekämpfungsstrategien oder die Entwicklung von Kriterien zur Bewertung und Zertifizierung der IT-Sicherheit. Insoweit ist es originäre Aufgabe des BSI, die Herausforderungen im Zusammenhang mit der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in technischer Hinsicht zu erforschen, Schutzvorkehrungen zu ermitteln, über einen geeigneten Selbstschutz aufzuklären und zu informieren usw.[45]. Dabei ist es notwendig, den Aufgabenzuschnitt und die Handlungsbefugnisse den sich stetig wandelnden Herausforderungen der Informationstechnologie anzupassen und das BSI insoweit „wettbewerbsfähig“ zu halten[46]. Das muss nicht zwingend durch die Aufnahme operativer Befugnisse in das Handlungsinstrumentarium des BSI geschehen; wohl aber durch eine Einbindung als Kontrollinstanz bei der Entwicklung und Auftragsvergabe staatlicher Überwachungssoftware an private Dienstleister.

Kurzum: Soweit überhaupt eine verfassungskonforme Technikgestaltung im Rahmen einer Onlinedurchsuchung oder einer Quellen-TKÜ möglich ist[47], kann derzeit nur das BSI sicherstellen, dass die in privater Regie erstellte Software den rechtlichen Anforderungen entspricht.

2. Zwischenausblick: „Make“ statt „Buy“

Natürlich bleibt es dem Staat unbenommen, den benötigten Bedarf durch eigene Kraftanstrengung zu decken. Im Nachgang zur Staatstrojaner-Affäre wurde beschlossen ein „Kompetenzzentrum Informationstechnische Überwachung (CC ITÜ)“ einzurichten. Hierzu wurde im BKA ein Aufbaustab eingesetzt und im Haushalt für das BKA dreißig zusätzliche Planstellen vorgesehen. Eine Beteiligung des BSI wird „geprüft“.[48]

III. Einfachgesetzliche Vorgaben

Die Hilfstätigkeit Privater unterliegt im Weiteren dem Regime einfachgesetzlicher Vorgaben. Im Rahmen der Privatisierung technikgestützter Ermittlungstätigkeit sind insbesondere datenschutzrechtliche[49] Implikationen zu beachten. Datenschutzrelevante Unterstützungstätigkeiten durch Private sind in vielen Konstellationen denkbar. So wird z.B. bei einer Maßnahme nach § 100i StPO eine Vielzahl personenbezogener Daten erhoben, übermittelt und gespeichert.[50] Eine Hilfestellung durch Private als weisungsgebundenes „Bedienpersonal“ für die komplexen technischen Geräte ist dabei alles andere als abwegig.[51]

1. Datenschutzrechtlich relevante Vorgaben

a) Grundfrage: Auftragsdatenverarbeitung oder Funktionsübertragung

Nach allgemeinem Datenschutzrecht können Dritte – je nach Art und Umfang ihrer konkreten Tätigkeit – im Wege eines Auftragsverhältnisses oder einer sogenannten Funktionsübertragung in die Datenverarbeitung eingebunden werden. Im öffentlichen Bereich ist Letztere, sofern nicht ausdrücklich gesetzlich gestattet, unzulässig.[52] Eine Beteiligung Privater kommt ausschließlich im Wege einer sogenannten Auftragsdatenverarbeitung in Betracht. Eine solche liegt immer dann vor, wenn personenbezogene Daten im Auftrag durch eine andere Stelle erhoben, verarbeitet oder genutzt werden sollen. Der Auftragnehmer ist bezüglich der Aufgabenerbringung streng an die Weisungen des Auftraggebers gebunden und unterliegt dessen Kontrolle. Er wird ohne eigenen Wertungs- und Entscheidungsspielraum tätig.[53] Der (öffentliche) Auftraggeber bleibt „Herr der Daten“, der private Dienstleister fungiert lediglich als „technischer Gehilfe“. Datenschutzrechtlich gilt er nicht als „Dritter“, sondern als ausgelagerte Einheit des Auftraggebers[54]. Er ist – was die rechtlichen Anforderungen betrifft – privilegiert. So stellt z.B. der Datentransfer zwischen den beteiligten Stellen keine rechtfertigungsbedürftige datenschutzrechtliche Übermittlung dar. Dem Auftragnehmer obliegt nur die tatsächliche technische Ausführung der Datenerhebung und Datenverarbeitung im Sinne eines Abarbeitens genau vorgegebener Erhebungsmuster[55]. Der Dienstleister ist im Wesentlichen nur verpflichtet, die technischen und organisatorischen Maßnahmen zur Datensicherheit zu treffen, damit die Daten verfügbar, integer und vertraulich sind und diese Eigenschaften prüfbar bleiben. Im Übrigen bleibt die Verantwortung zur Einhaltung der datenschutzrechtlichen Vorschriften beim öffentlichen Auftraggeber. Dieser haftet im Außenverhältnis allein[56].

Demgegenüber erledigt bei einer *Funktionsübertragung* der Auftragnehmer den übertragenen Datenverarbeitungsprozess selbständig und in eigener Verantwortung. Eine solche liegt vor, wenn nicht nur die praktisch-technische Datenverarbeitung, sondern die gesamte Aufgabe, der die Datenverarbeitung dient, an Dritte übertragen wird[57]. Maßgebliches Kennzeichen der privilegierten Auftragsdatenverarbeitung in Abgrenzung zur Funktionsübertragung ist die *fehlende Entscheidungsbefugnis* des Auftragnehmers und seine *Weisungsabhängigkeit* gegenüber dem Auftraggeber.

Die *Sensibilität der zu verarbeitenden Daten* spielt für die Zulässigkeit einer Auftragsdatenverarbeitung grundsätzlich keine entscheidende Rolle, da die öffentliche Stelle als Auftraggeber „Herrin der Daten“ bleibt und für den Datenschutz und die Datensicherheit umfassende Verantwortlichkeit zeichnet. *Dennoch*: Wenn Private Umgang mit sensiblen hoheitlichen Daten haben, besteht die erhöhte Gefahr einer missbräuchlichen Verwendung oder auch nur eine versehentliche Eröffnung des Zugangs an Dritte, sowie die *Gefahr eines Datenverlustes und einer Verfälschung der Datensätze*. Insoweit beinhaltet jede Weitergabe sensibler Daten an private Dienstleister regelmäßig einen zusätzlichen Grundrechtseingriff bzw. eine veritable Grundrechtsgefährdung. Insoweit bedarf es effektiver Kontroll- und Überwachungsmaßnahmen des öffentlichen Auftraggebers, damit diesen Gefahren wirksam begegnet werden kann (vgl. auch § 9 BDSG sowie die Anlage zu § 9 BDSG).

Nur in Einzelfällen sind derart sensible Datensätze betroffen, dass eine Auftragsdatenverarbeitung per se ausscheiden muss, etwa bei Daten, die die höchstpersönliche Lebenssphäre des Betroffenen berühren können (z.B. Daten aus einer TKÜ, einer Onlinedurchsuchung, einer Quellen-TKÜ oder eines „Lauschangriffs“) oder wenn die betreffenden Daten einer Geheimhaltung unterliegen (z.B. Steuerdaten – Steuergeheimnis).

Darüber hinaus gelten keine grundsätzlichen Restriktionen für Daten aus dem Justiz- oder Polizeibereich, die gemeinhin als „besonders“ sensibel anzusehen sind. Generell ist zu bemerken, dass das Auslagern der Datenverarbeitung öffentlicher Stellen an Private nicht ungewöhnlich ist[58] – auch wenn sensible Datensätze betroffen sind. Man denke nur an die Bearbeitung von Beihilfedaten[59], Sozialdaten[60] oder Patientendaten[61].

b) Auftragsdatenverarbeitung im Ordnungswidrigkeiten- und Strafprozessrecht

Nach § 49c Abs. 2 OWiG dürfen *nur* Gerichte, Staatsanwaltschaften, Verwaltungsbehörden und die Polizei personenbezogene Daten (nach Maßgabe der §§ 483, 484 Abs. 1 und § 485 StPO) in Dateien speichern, verändern oder nutzen, soweit dies zu Zwecken des Bußgeldverfahrens erforderlich ist. Ähnliches ist für das Strafverfahren in § 483 Abs. 1 StPO geregelt. Die Aufzählung der berechtigten Stellen in § 49c Abs. 2 OWiG bzw. § 483 StPO ist – nach dem eindeutigen Wortlaut der Vorschriften – abschließend. D. h. private Stellen dürfen im Rahmen eines Bußgeldverfahrens bzw. eines Strafverfahrens keine personenbezogenen Daten speichern, verändern oder nutzen. Dies gilt aber *nicht*, wenn deren Einbindung im Wege einer *Auftragsdatenverarbeitung* erfolgt. Denn in dieser Konstellation bleibt die beauftragende Behörde in jedem Moment „Herrin der Daten“, der private Auftragnehmer fungiert lediglich als „technischer Gehilfe“. Als solcher gilt er datenschutzrechtlich nicht als „Dritter“, sondern ist wie eine ausgelagerte Stelle der beauftragenden Behörde zu behandeln[62]. D.h., dass in der Konstellation einer Auftragsdatenverarbeitung der öffentliche Auftraggeber als „Verwaltungsbehörde“ i.S.d. § 49c OWiG bzw. § 483 StPO anzusehen ist. Die Tatsache, dass tatsächlich auch Daten bei einem privaten Auftragnehmer gespeichert bzw. sonst verarbeitet werden, ist dagegen rechtlich irrelevant. Eine Auftragsdatenverarbeitung Privater ist demnach durch StPO und

OWiG nicht grundsätzlich ausgeschlossen und richtet sich nach den allgemeinen Regelungen des BDSG[63].

c) Exkurs: Elektronische Akte in Strafsachen

Anders fällt diese Bewertung im Rahmen der geplanten Einführung elektronischer Akten in Strafverfahren aus. Anfang Juni 2012 hat das BMJ einen Diskussionsentwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen[64] veröffentlicht. Enthalten sind explizite Vorgaben zur Auftragsdatenverarbeitung. Der Kreis der möglichen Auftragnehmer wird in § 496 Abs. 3 StPO-E auf „andere öffentliche Stellen oder juristische Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform" beschränkt. Eine Datenverarbeitung durch Private ist im Falle der elektronischen Aktenführung in Strafsachen also ausgeschlossen. In der Begründung wird die Führung elektronischer Strafakten als „eine der hoheitlichen Kernaufgabe der Staatsanwaltschaft und Gerichte besonders nahestehende Datenverarbeitungstätigkeit"[65] bezeichnet.[66] Mit Blick auf die hohe Sensibilität der regelmäßig in Strafakten enthaltenen Daten (z.B. TKÜ-Protokolle – siehe bereits oben) ist diese Einschätzung zustimmungswürdig.[67]

III. Fazit

Auch im strafrechtlichen Ermittlungsverfahren als genuin hoheitlicher Aufgabe ist eine Einbindung Privater als Verwaltungshelfer möglich. Gerade bei technisch komplexen Datenerhebungs- und -verarbeitungsmaßnahmen kann die Sachkompetenz privater IT-Dienstleister gewinnbringend genutzt werden. Erforderlich ist dabei aber zumindest, dass die Aufgaben zwischen Staat und privatem Dienstleister klar verteilt sind, der private Verwaltungshelfer nur unterstützende vor- oder nachbereitende Maßnahmen trifft, keinen Umgang mit kernbereichsrelevanten[68] oder sonstigen „hochsensiblen" Daten erhält und vor allem der öffentliche Auftraggeber seine Kontroll- und Gewährleistungsfunktionen transparent wahrnimmt und Gefährdungen des Datenschutzes durch nachhaltige organisatorische und technische Maßnahmen vorbeugt. Letzteres wird die öffentlichen Auftraggeber regelmäßig vor nicht unerhebliche Probleme stellen. Wenn mangelnder technischer Sachverstand in den beschriebenen Fällen das vorrangige Privatisierungsmotiv ist, bedarf es gerade auch eines solchen Sachverstandes, um die verfassungsrechtlichen Kontroll- und Steuerungspflichten gegenüber den in die Aufgabenerfüllung eingebundenen privaten Dienstleister wahrnehmen zu können. Dieses Paradoxon kann nur aufgelöst werden, wenn kompetente und hochspezialisierte staatliche Stellen mittels kontrollierbarer Techniksteuerung nachprüfbare Schranken setzen; etwa durch Zertifizierung, Setzung von Standards, Normung, spezielle Zulassungsverfahren oder andere Instrumente, welche die sach- und fachgerechte Beauftragung leistungsfähiger und vertrauenswürdiger privater Partner und deren Produkterstellung steuern. Wahrlich neu sind diese Erkenntnisse im Ermittlungsverfahren freilich nicht. Geschwindigkeitsüberwachungsgeräte, Rotlichtüberwachungsanlagen oder Abstandsmessanlagen dürfen von der Polizei nur mit Bauartzulassung der Physikalisch-Technischen Bundesanstalt (PTB) und gemäß Eichordnung betrieben werden. Im Prinzip Ähnliches muss auch (freilich unter Gewährleistung der erforderlichen Geheimhaltung) gelten, wenn es nicht um des Deutschen liebste Kinder – Auto und Führerschein – sondern um seine persönlichsten Daten geht. Auch das macht die „Staatstrojaner-Affäre" zur Affäre: Nämlich die Tatsache, dass sich staatliche Stellen, denen der Gesetzgeber nicht zutraut, in freier Entscheidung eine Rotlichtüberwachungsanlage zu beschaffen, für befähigt hielten, die Erstellung einer Software zur Überwachung der Internettelefonie in Auftrag zu geben. Insoweit wurde nun mit der Einrichtung eines Kompetenzzentrums Informationstechnische Überwachung (CC ITÜ) ein erster Schritt in die richtige Richtung getan.

Fußnoten:

1 *Weiner*, DVBl. 2005, 755.
2 *Beukelmann*, NJW-Spezial 2008, 280
3 „Privatermittler sichten Beweise bei Kinderporno-Anklagen", http://www.spiegel.de/netzwelt/web/outsourcing-privatermittler-sichten-beweise-bei-kinderporno-anklagen-a-533078.html. Siehe hierzu die kleine Anfrage der Abgeordneten *Piltz*, *Addicks*, *Ahrendt*, weiterer Abgeordneter und der Fraktion der FDP an die Bundesregierung, BT-Drs. 16/8335 sowie *Beukelmann*, NJW-Spezial 2008, 280.
4 Vgl. BT-Drs. 16/8335 S. 1 f. „Soweit es zur Erforschung des Sachverhalts erforderlich ist, sind Staatsanwaltschaft (nach § 161a StPO) und Polizei (nach § 163 StPO) befugt, Sachverständige mit Untersuchungen zu beauftragen. Die Tätigkeit des Sachverständigen ist dadurch bestimmt, den Ermittlungsbehörden Tatsachenstoff zu unterbreiten, der nur aufgrund besonderer Sachkunde gewonnen werden kann …".
5 *Braun*, in: Lohmann/Stober, Kooperationsvereinbarungen mit der öffentlichen Hand, 2012, S. 39 (48).
6 Dazu *Braun*, DPolBl. 2010, 12 ff.
7 Das *BVerwG* führt an, dass der Staat nicht gehalten ist, jede von ihm als erforderlich angesehene Maßnahme durch eigene Dienstkräfte zu erledigen. Er könne sich auch privater Personen bedienen, weil nicht festgelegt sei, in welcher Weise der Staat seinen Pflichten genüge, BVerwG NVwZ-RR 1997, 648 (650).
8 Hierzu *Gramm*, Privatisierung und notwendige Staatsaufgaben, 2001, S. 98 ff.
9 Mit dieser Charakterisierung ist aber wenig gewonnen, weil sie lediglich das Gewaltmonopol betont und auf den im Wesentlichen unklaren Begriff des „Kernbereich" (*Baer*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts I, 2006, § 11 Rn. 28) rekurriert, während andere – mögliche – Privatisierungsbeiträge ausgeklammert werden.
10 *Barisch*, Die Privatisierung im deutschen Strafvollzug, 2010, S. 110 ff.
11 *Barisch*, Die Privatisierung im deutschen Strafvollzug, 2010, S. 108 ff. m.w.N.
12 *Ballhausen*, IT-Einsatz in der Justiz, 2011, S. 120.
13 *Mayen*, DÖV 2001, 110 (111).
14 Näher dazu *Mayen*, DÖV 2001, 110 (112).
15 *Ballhausen*, IT-Einsatz in der Justiz, 2011, S. 121 f. m.w.N.
16 Hierzu BVerfG DVBl. 1995, 1291; *Schulte*, Schlichtes Verwaltungshandeln, 1995, S. 121 ff., S. 173 ff.
17 Siehe die Nachweise bei *Battis*, in: Sachs, GG, 5. Aufl. 2009, Art. 33 Abs. 4, Rn. 55.; *Pieroth*, in: Jarass/Pieroth, GG, 9. Aufl. 2007, Art. 33 Rn. 41; *Lecheler,* in: Isensee/Kirchhof, HdbStR Bd. III, 3. Aufl. 2005, § 72 Rn. 28.
18 Näher *Braun/Roggenkamp*, K&R 2011, 681 (681 f.).
19 So dezidiert der Prüfbericht des bayerischen Datenschutzbeauftragten v. 30.07.2012, vgl. http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf; ebenso *Roggenkamp*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, 2012, S. 267 ff.
20 LG Landshut, 20.01.2011 – 4 Qs 346/10, NStZ 2011, 479 m. Anm. *Albrecht*, JurPC Web-Dok. 59/2011; *Bär*, MMR 2011, 691; *Braun*, juris-PR-ITR 3/2011 Anm. 3.
21 Soweit im Rahmen des öffentlichen Auftrags Entscheidungsspielräume für eigene „Akzente" der Hersteller und Entwickler bleiben, sind diese Spielräume regelmäßig Ergebnis einer bewussten Entscheidung des Trägers der hoheitlichen Aufgabe, hier gerade keine Vorgaben machen zu wollen, was ebenso von der staatlichen Aufgabenverantwortung gedeckt ist.
22 BVerfG, Beschl. v. 17.02.2009 – 2 BvR 1372/07 – Kreditkartenabgleich; BVerfG, Beschl. v. 17.02.2009 – 2 BvR 1372/07 – Kfz-Kennzeichenerfassung; BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05 – Onlinedurchsuchung.
23 Hierzu bereits früh *Peters*, CR 1986, 790 ff.
24 BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05.
25 BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 Absatz-Nr. 278.
26 *Braun*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, 2012, S. 39 (70).
27 BVerfG, 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07 – Abs. 189 f.
28 *Braun/Roggenkamp*, K&R 2011, 681 ff.
29 *Braun*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, 2012, 39, 71; hierzu *Braun/Roggenkamp*, K&R 2011, 681 ff.; *Popp*, ZD 2012, 51 ff.; vgl. auch Der Bayerische Landesbeauftragte für den Datenschutz, Prüfbericht Quellen-TKÜ v. 30.07.2012.
30 *Braun/Roggenkamp*, K&R 2011, 681 ff.; *Roggenkamp*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, S. 267.
31 BVerfG v. 27.02.2008 – 1 BvR 370/07; hierzu *Jaeger*, AnwZert ITR 13/2008, Anm. 3; *Hornung*, CR 2008, 299.
32 Hierzu näher *Braun/Roggenkamp*, K&R 2011, 681 ff.

33 Dazu *Maurer*, Allgemeines Verwaltungsrecht, 18. Aufl. 2011, § 23 Rn. 56 ff. m.w.N.
34 Hierzu *Waechter,* NZV 1997, 332 m.w.N.
35 *Burgi,* Die Verwaltung 33 (2000), 201 f.; *ders*., Funktionale Privatisierung und Verwaltungshilfe, 1999.
36 *Burgi,* Die Verwaltung 33 (2000), 201 (202 f.).
37 *Heckmann*, in: Bräutigam, IT-Outsourcing, 2. Aufl. 2008. Kap. X m.w.N.
38 Bericht abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf.
39 So zumindest ausweislich Berichterstattungen über das unter VS-NfD stehende Dokument, vgl. http://www.golem.de/news/staatstrojaner-abgehoerte-sexgespraeche-per-skype-liessen-sich-nicht-loeschen-1202-89869.html.
40 LfD Bayern, Prüfbericht Quellen-TKÜ, vgl. http://www.datenschutz-bayern.de/0/bericht-qtkue.pdf.
41 Vgl. z.B. *Schulz*, in: F.A.Z. v. 26.10.2011, „Der Computer steht offen wie ein Scheunentor".
42 Wenn auch in anderem Kontext *Heckmann*, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 139.
43 *Heckmann*, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 139, (148).
44 *Jäger*, Die verfassungsrechtliche Pflicht zur transnationalen Zusammenarbeit im Bereich der Inneren Sicherheit, 2008, S. 332.
45 *Heckmann*, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 139 (162 f.).
46 *Heckmann*, in: Rüßmann (Hrsg.), FS Käfer, 2009, S. 139 (162 f.).
47 Für die Quellen-TKÜ lässt sich dies mit guten Gründen bestreiten, vgl. *Roggenkamp*, in: Peters/Kersten/Wolfenstetter (Hrsg.), Innovativer Datenschutz, S. 267.
48 Antwort auf schriftliche Fragen des Abgeordneten *Behrens* an BMI v. 12. Dezember 2011 (Monat Dezember 2011, Arbeits-Nr. 12 / 163 und 164).
49 Im Folgenden wird auf das BDSG Bezug genommen. In den Ländern gelten weitgehend inhaltsgleiche Landesdatenschutzgesetze.
50 Ausführlich *Harnisch/Pohlmann*, HRRS 2009, 9.
51 Im Rahmen der Durchführung von Quellen-TKÜ-Maßnahmen mit Hilfe sog. Staatstrojaner wurden zum Zwecke der Verschleierung der Datenströme dem Bericht des CCC zu Folge die Dienste eines privaten Proxyserveranbieters in Anspruch genommen.
52 Vgl. *Heckmann/Braun*, BayVBl. 2009, 581 ff. m.w.N.
53 *Gabel*, in: Taeger/Gabel, BDSG, § 11 Rn. 12.
54 Er ist gleichsam als „verlängerter Arm" für den Auftraggeber tätig, übt nur Hilfs- bzw. Unterstützungsfunktionen aus. Der Auftragsschwerpunkt ist in erster Linie auf die technische Durchführung der Datenverarbeitung gerichtet (vgl. *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 4).
55 *Stober*, in: Wolff/Bachof/Stober/Kluth, Verwaltungsrecht II, 7. Aufl. 2010, § 91 Rn. 41.
56 *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 3.
57 *Schneider*, Handbuch des EDV-Rechts, 4. Aufl. 2008, Teil B, Rn. 448; *Gabel*, in: Taeger/Gabel, BDSG, § 11 BDSG Rn. 14.
58 *Büllesbach/Rieß*, NVwZ 1995, 444 ff.
59 Dazu *Battis/Kersten*, ZBR 2000, 145 ff.; *Werres*, ZBR 2001, 429.
60 So besteht etwa nach § 80 SGB X ausdrücklich die gesetzliche Möglichkeit einer *Verarbeitung von Sozialdaten* durch nichtöffentliche Stellen, dazu *Klessler*, DuD 2004, 40 ff.
61 Vgl. etwa für Bayern Art. 27 BayKrG.
62 *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 11 Rn. 4.
63 Näher hierzu *Braun*, Auftragsdatenverarbeitung für die Polizei und kommunale Ordnungsbehörden in: Braun/Stober, Sicherheitsgewerbe und Datenschutz, 2012, 101 ff. sowie *Stober*, Verkehrssicherheitspartnerschaften, 2012, S. 72 ff.
64 Online abrufbar unter: http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/Diskussionsentwurf_Gesetz_zur_Einfuehrung_der_elektronischen_Akte_in_Strafsachen.pdf?__blob=publicationFile, i. W. „Diskussionsentwurf".
65 BMJ, Diskussionsentwurf, S. 40.
66 Ähnlich gebietet § 126 Abs. 3 GBO, dass die maschinelle Führung des Grundbuchs als automatisierte Datei nur auf den Anlagen einer „staatlichen Stelle" oder „einer juristischen Person des öffentlichen Rechts" vorgenommen werden darf, und sperrt somit von vornherein eine Aufgabenübertragung an einen privaten Dritten. Entsprechende Regelungen bestehen im Polizei- und Ordnungsrecht nicht.
67 Vgl. auch *Heckmann/Braun*, BayVBl. 2009, 581.
68 Hierzu *Braun/Fuchs*, Die Polizei 210, 185.

Diskussionsvorschlag zu einer nachhaltigen Reform der Sicherungsverwahrung

Jens Peglau

I. Übersicht

Ab 1998 sind die gesetzlichen Regelungen der Sicherungsverwahrung zunächst vielfach erweitert worden. Nach einer Entscheidung des EGMR aus dem Jahre 2009[1] setzte eine Gegenbewegung ein.[2] Dann kam die Entscheidung des BVerfG vom 04.05.2011[3], in der das Recht der Sicherungsverwahrung wegen Verstoßes gegen das Abstandsgebot für verfassungswidrig erklärt wurde und in der das Gericht im Hinblick auf den Vertrauensschutzgrundsatz Anstoß u.a. an § 66b Abs. 2 StGB a.F. und an der Abschaffung der Zehnjahreshöchstfrist für Altfälle nahm. Der Gesetzgeber hat nun – nach der vom BVerfG gesetzten Frist – noch bis zum 31.05.2013 Zeit, das Recht der Sicherungsverwahrung verfassungsgemäß neu zu regeln. Bis dahin gilt das bisherige Recht – zum Teil mit Maßgaben – weiter.

Im Gesetzgebungsverfahren befindet sich inzwischen ein „Entwurf eines Gesetzes zur bundesrechtlichen Umsetzung des Abstandsgebotes im Recht der Sicherungsverwahrung".[4] Dieser enthält – bei Beibehaltung des bisherigen Systems – eine Reihe von Ergänzungen (Anpassung an die Rechtsprechung des BVerfG – insbesondere: Erfordernis einer „psychischen Störung"; Regelungen zur Einführung einer sog. „Therapieunterbringung" – § 65 StGB-E).

Nachfolgend soll untersucht werden, wie – unabhängig vom laufenden Gesetzgebungsverfahren – eine Vereinheitlichung und Vereinfachung des Rechts der Sicherungsverwahrung unter Beachtung der Vorgaben des EGMR und des BVerfG – ohne weitere Absenkung des Schutzniveaus – möglich ist. Dabei sollen insbesondere frühere Vorschläge, die Entscheidung über die Anordnung der Sicherungsverwahrung immer erst gegen Ende der Strafhaft zu treffen[5], vertieft werden.

Es wird hier ein Vorschlag unterbreitet, der den Eintritt eines Vorbehalts *kraft Gesetzes* mit der Aburteilung der Anlasstaten vorsieht, wenn bestimmte formelle Voraussetzungen vorliegen. Über die Anordnung selbst wird dann, wie schon jetzt (§ 66a Abs. 3 StGB) zu einem späteren Zeitpunkt entschieden.

Es geht nicht darum, einen in allen Details ausformulierten Gesetzesvorschlag zu präsentieren, sondern vielmehr um die Schaffung einer Diskussionsgrundlage, die an vielen Stellen sicherlich noch der Vertiefung bedarf.

II. Warum Vereinfachung und Vereinheitlichung?

Das geltende Regelungswerk ist vielfach wegen seiner Unübersichtlichkeit und Kompliziertheit kritisiert und eine Gesamtreform befürwortet worden. [6] Aber: Rechtsvereinfachung kann kein Selbstzweck sein. Die