Reinhard Fraenkel, Volker Hammer

Vom Staats- zum Verfassungstrojaner

Während die Euro-Krise die Medien dominiert, sind die „Vorfälle" zur Quellen-TKÜ medial schon leise in der Versenkung verschwunden. Das ist verhängnisvoll, denn es ist zu befürchten, dass die Strafverfolgungsbehörden Grundrechte nicht beachten.

Einleitung

Seitdem die FAS am 9.10.2011 über die Enttarnung eines sogenannten „Bundestrojaners" berichtet hat, hat eine teils polemische, teils abwieglerisch geführte Debatte um den staatlich organisierten Einsatz von Schadsoftware eingesetzt. Die Bandbreite der Diskussion wird, wenn man einmal von der Politik absieht, durch die Äußerung des ehemaligen Präsidenten des BVerfG Papier auf der einen Seite markiert. Papier sieht keine Rechtsgrundlage für die sogenannte Quellen-TKÜ. Damit, so Papier, sei der Einsatz von Trojanern bei der Strafverfolgung nicht erlaubt. Er plädiert für eine (noch zu schaffende) Regelung, die sich an den vom Verfassungsgericht aufgestellten Leitlinien seiner Entscheidung vom 27.2.2008 zur Zulässigkeit der Online-Durchsuchung zu orientieren habe.[1] Das BVerfG hatte in seiner Entscheidung das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kreiert. In derselben Ausgabe der FAS plädiert Michael Jürgs vehement für den weitgehend ungehinderten Einsatz der „Trojaner" als letztlich einziges Mittel der Strafverfolgungsbehörden, dem organisierten Verbrechen Paroli bieten zu können. Damit ist die Bandbreite der Diskussion im Wesentlichen abgesteckt.

Die Diskussion um die Zulässigkeit des Einsatzes der „Staatstrojaner" muss mit großer Ernsthaftigkeit geführt werden, da deren Einsatz die Basis unseres Gemeinwesens tangiert. Es ist nämlich zweifelhaft, ob die Informationsbeschaffung der Strafverfolgungsbehörden unter Einsatz dieser Mittel von den entsprechenden Gesetzen gedeckt, also legal ist. Die Dignität des Rechtsstaats aber ist seine Legalität. Der Verlust dieses Prinzips, also das Überschreiten des das Handeln von Behörden limitierenden Rechtsrahmens durch sie selbst, wiegt schwerer als jede Euro-Krise. Bei der Euro-Krise geht es letztlich nur um Geld. Der mögliche Verlust des Geldes ist schmerzhaft. Demgegenüber wäre der Verlust des Legalitätsprinzips oder dessen stillschweigende Auflösung der fundamentale Verlust der Freiheit. Insofern also ist die Klärung der Frage, ob der Einsatz eines „Staatstrojaners" durch Ermittlungsbehörden verfassungsrechtlich und durch einzelrechtliche Bestimmungen gedeckt ist, keine bloße intellektuelle Fingerübung, sondern demokratische Pflicht.

Die nachfolgende, allerdings nur kursorische Prüfung klärt zunächst, wie ein „Staatstrojaner" zu qualifizieren ist. Gibt es für seinen Einsatz Rechtsgrundlagen? Falls nein, hätten die Ermittlungsbehörden rechtwidrig gehandelt. Falls ja, stellt sich die weiterführende Frage, ob die gesetzliche Grundlage verfassungsgemäß ist. Abschließend muss das Verhältnis von Ermittlungsbehörden zur Judikative angesprochen werden: Soll der Richtervorbehalt der notwendige Schutz des Einzelnen vor ungerechtfertigten Ermittlungsmaßnahmen der Strafverfolgungsbehörden sein, müssen die Richter genaue Kenntnisse über die geplanten Ermittlungsmethoden haben. Nur dann können Sie auch abschätzen, ob die Maßnahmen sich im verfassungsmäßigen Rahmen bewegen.

Zulässigkeit des Einsatzes

Der Staatstrojaner ist ein Programm, mit dessen Hilfe entweder die Inhalte auf der Festplatte eines Fremdrechners ohne Kenntnis des Besitzers des Rechners ausgespäht werden oder mit dessen Hilfe die sogenannte Quellen-TKÜ ausgeführt wird. Der Staatstrojaner ist also ein Programm, mit dessen Hilfe personenbezogene Daten erhoben werden.[2] Fraglich ist, ob der Einsatz dieser Software durch ein Gesetz gedeckt ist. Der Frage soll auf Basis der BKA-Gesetzes einerseits und des Bayrischen Polizeiaufgabengesetzes (PAG) andererseits nachgegangen werden.

Das **BKA-Gesetz** bietet eine eindeutige Rechtsgrundlage. § 20k regelt den verdeckten Eingriff in informationstechnische Systeme, also das, was gemeinhin unter Online-Durchsuchung verstanden wird. Ebenso ist die sogenannte Quellen-TKÜ gesetzlich in § 20l BKA-Gesetz geregelt. Da das BKA-Gesetz im Jahre 2009 umfassend novelliert wurde, hat der Bundesgesetzgeber auch versucht, die Vorgaben des BVerfG aus der Entscheidung zur Online-Durchsuchung umzusetzen. So dürfen insbesondere Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, nicht erhoben werden. Gegebenenfalls sind diese Daten unverzüglich zu löschen. (§ 20k Abs. 7) Eine identische Schutzvorschrift enthält auch § 20l Abs. 6 hinsichtlich der Quellen-TKÜ. Damit ist zunächst festzuhalten, dass der Bundesgesetzgeber zumindest formal zentrale Auflagen des BVerfG im BKA Gesetz umgesetzt hat.[3]

Auch das **bayerische PAG** enthält Vorschriften zur Online-Durchsuchung und zur Quellen-TKÜ in Art. 34d einerseits und Art. 34a andererseits. Während allerdings Art. 34d ansatzweise Regelungen zum besonderen Schutz der Daten enthält,

1 Papier in FAS am 23.10.2011.

2 Die vom CCC analysierten Programme enthalten außerdem auch Funktionen zum Erstellen und Übertragen von Screenshots. Auch das Nachladen und Ausführen von Funktionen und damit die Manipulation von Beweisen sei möglich. Die Möglichkeit des Gegenbeweises ist dem Betroffenen abgeschnitten. Auf diesen Umstand, der aus dem Schreckenskabinett von Diktatoren und deren Geheimdiensten stammen könnte und dessen Rechtwidrigkeit keiner weiteren Erörterung bedarf, wird hier nicht weiter eingegangen.

3 Dass selbst diese Regelung nicht frei von verfassungsrechtlichen Bedenken ist, hat der BfDI in seinem 22. Tätigkeitsbericht nachdrücklich deutlich gemacht (S. 47 ff.). Dieser Auffassung ist offensichtlich auch Prof. Papier, denn sonst wäre sein eingangs zitiertes Statement in der FAS nicht erklärlich. Im Übrigen ist gegen das Gesetz noch eine Verfassungsbeschwerde anhängig.

die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind, fehlen entsprechende Schutzregelungen in Art. 34a hinsichtlich der Quellen-TKÜ. Daher vertritt der Bayerische Landesbeauftragte für den Datenschutz die Auffassung, Art. 34a PAG enthalte keine speziellen Befugnisse zur Quellen-TKÜ (vgl. 24 Tätigkeitsbericht 2010, 3.7).

Somit ist als erstes Ergebnis festzuhalten: Sowohl das BKA-Gesetz als auch das Bayerische PAG enthalten Rechtsgrundlagen sowohl für die Online-Durchsuchung als auch für die Quellen-TKÜ. Streit besteht zwar darüber, ob diese rechtlichen Vorschriften den Vorgaben des BVerfG entsprechen bzw. überhaupt als Rechtsgrundlage für die Quellen-TKÜ anzusehen sind, aber dieser Streit ist im politischen Raum auszutragen oder gegebenenfalls vor Gericht zu klären.

Allerdings muss den Polizeibehörden klar sein, dass der Einsatz dieser elektronischen Mittel immer problematisch ist. Gerade daher kommt den allgemeinen datenschutzrechtlichen Vorschriften eine besondere Bedeutung zu, weil sie geeignet sein können, im Vorfeld zu klären, ob der Einsatz der entsprechenden Programme auch unter den besonderen Bedingungen der bereichsspezifischen datenschutzrechtlichen Ausnahmeregelungen zulässig ist. Denn nach den Maßgaben des BDSG setzt der Einsatz entsprechender Programme die sogenannte Vorabkontrolle der behördlichen Datenschutzbeauftragten gemäß § 4d Abs. 5 BDSG zwingend voraus.

Vorabkontrolle

Und spätestens hier beginnen die Merkwürdigkeiten. Zwar wird der Einsatz der „Staatstrojaner" von den betreffenden Strafverfolgungsbehörden nicht in Abrede gestellt. Aber Teile der Politik und natürlich die betreffenden Polizeibehörden überbieten sich mit Versicherungen, die eingesetzten Mittel hätten den rechtlichen Vorgaben der Gesetze bzw. auch des BVerfG entsprochen. Keiner der Apologeten aber behauptet, der jeweilige behördliche Datenschutzbeauftragte sei in die Beschaffung der Software eingeschaltet gewesen. Kein Behördenleiter und auch kein Minister hat sich bisher dazu geäußert, ob das bei der Beschaffung von Software übliche Verfahren eingehalten wurde. Der Besteller erstellt ein Anforderungsprofil der Software, das zumindest bei derartig sensibler Software vom behördlichen DSB freigegeben werden muss, soll die Vorabkontrolle nicht ins Leere laufen.

Im BKA-Gesetz spielt der behördliche DSB eine ganz besondere Rolle. In § 20k BKA Gesetz heißt es u. a.: *„Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 des Bundesdatenschutzgesetzes).*" Die Regelung an sich wirft viele Fragen auf, denen aber hier nicht weiter nachgegangen wird. Relevant ist, dass das BKA-Gesetz eine ex-post-Kontrolle vorsieht. Datenschutzrechtlich geboten aber ist schon die ex-ante-Kontrolle der Software und ihrer Verwendungszwecke. § 4d BDSG gilt auch für das BKA.

Wenn das BKA sich also zur Vorabkontrolle nicht äußern kann, dann ist zumindest ein datenschutzrechtliches Vollzugsdefizit zu beklagen. Allein dies gibt Anlass zur Sorge. Je stärker Ermittlungsmaßnahmen in Grundrechte der Bürger eingreifen, desto genauer müssen die Schutzvorschriften zugunsten der Bürger beachtet werden. Ganz bewusst sieht das BDSG die Vorabkontrolle vor. Sie kann und darf nicht durch eine kuriose ex-post-Kontrolle ersetzt werden.

Das BDSG gilt natürlich nicht für die bayerische Polizei. Hier ist einschlägig das Bayerische Datenschutzgesetz. Die Vorabkontrolle ist nur knapp in Art. 26 BayDSG geregelt. Eine nähere Auseinandersetzung mit dieser Norm erübrigt sich allerdings in diesem Zusammenhang, denn gemäß Art. 49 PAG findet Art. 26 BayDSG keine Anwendung. Insofern, diese ironische Bemerkung sei gestattet, gibt es bei der Anwendung des Staatstrojaners in Bayern wenigstens kein datenschutzrechtliches Vollzugsdefizit zu beklagen.

Regelungsdefizite

Auch wenn die Polizeibehörden beim Einsatz der „Staatstrojaner" sich zumindest auf gewisse Rechtsgrundlagen berufen können, offenbart deren Einsatz legislatorische Mängel. Eine zu mehr Rechtsklarheit führende Regelung in der StPO ist dringend geboten. Eine einheitliche Regelung, die den Bedenken und Leitlinien des Bundesverfassungsgerichts Rechnung trägt, kann einer weiteren Zersplitterung der Verfassungswirklichkeit in den Polizeigesetzen von Bund und Ländern Einhalt gebieten. Nur so kann eine bundeseinheitliche Praxis in der Anwendung der „Staatstrojaner" erreicht werden. Diese Forderung gilt sowohl hinsichtlich der Online-Durchsuchung als auch im Hinblick auf die Quellen-TKÜ. Beide Maßnahmen sind vom Einsatz der technischen Hilfsmittel her vergleichbar. Entsprechend vergleichbar ist die Eingriffstiefe in die Grundrechte der betroffenen Bürger. Der Weg, der in letzter Zeit von einzelnen Gerichten beschritten wurde, zumindest die Befugnis zur Quellen-TKÜ unter Verweis auf § 100a StPO (Telefonüberwachung) in der Strafprozessordnung zu verorten, ist ein verhängnisvoller[4] Irrweg.

Dringend geboten sind auch einheitliche Leitlinien für die Beschaffung und/oder Erstellung der entsprechenden Software. Eine Einheitssoftware kann es nicht geben.[5] Mit anderen Worten: Die Beschaffung der Software ist kein einmaliger Akt. Die Software muss immer wieder angepasst werden an die fallspezifischen Bedürfnisse und gleichzeitig muss immer wieder geprüft werden, inwieweit die modifizierte Software noch den Anforderungen des BVerfG entspricht. Insofern muss auch die Vorabkontrolle gestärkt werden, wenn am datenschutzrechtlichen Konzept der Binnenkontrolle festgehalten werden soll. Für Bayern gilt dann noch einmal besonders, dass eine dem BDSG vergleichbare Regelung der Vorabkontrolle für das PAG überhaupt erst geschaffen werden muss.

Selbstverständliche Pflichten der Behörden

Verantwortlicher Umgang mit den Grundrechten der Bürger heißt in diesem sensiblen Feld auch genaue Kenntnis der eingesetzten Software. Die Einlassun-

4 Vgl. beispielhaft LG Landshut, Beschluss vom 20.01. 2011, 4Qs 346/10; siehe dazu auch die lesenswerte Urteilsanmerkung von Florian Albrecht, http://www.jurpc.de/aufsatz/20110059.htm.

5 Darauf hat der BfDI nachdrücklich hingewiesen. Im 22. Tätigkeitsbericht 2007/08 hat er in diesem Zusammenhang ausgeführt: *„Gegen die Eignung der Online-Durchsuchung spricht, dass sie in jedem Einzelfall die Entwicklung maßgeschneiderter Software erforderlich macht und damit technisch sehr aufwendig ist."* (aaO S. 47).

gen der Behörden, man habe den Funktionsumfang der Software nicht gekannt, da sich die Firma Digitask geweigert habe, den Source Code offen zu legen, sind völlig inakzeptabel. Ohne Kenntnis des Funktionsumfangs und einer entsprechenden Prüfung des Source Codes darf die Software nicht eingesetzt werden. Die angeblichen Betriebsgeheimnisse der Firma DigiTask haben gegenüber den Grundrechten der Bürger keinen Vorrang. Hat es überhaupt ein eindeutiges Anforderungsprofil an die Software gegeben? Nicht einmal das scheint gesichert. Die Strafverfolgungsbehörden haben zumindest billigend in Kauf genommen, dass die eingesetzte Software tiefer als geboten und erlaubt in die Grundrechte der Betroffenen eingreifen konnte. Insofern haben sie grob fahrlässig gehandelt.

Und dann die Speicherung der Daten auf einem Server in den USA. Wie will man das denn rechtfertigen? Dies alles sind Indizien dafür, dass es in den Behörden keine datenschutzrechtliche Binnenstruktur gibt, die auf die Einhaltung der entsprechenden Vorschriften und damit der Grundrechte achtet. Natürlich haben es die Strafverfolgungsbehörden oft mit Schwerkriminellen zu tun. Natürlich gibt es einen hohen Ermittlungsdruck sowohl innerhalb der Binnenstruktur einer Ermittlungsbehörde als auch seitens der Öffentlichkeit und der Politik. Aber darüber darf nicht vergessen werden, dass auch die Verdächtigen und auch die Täter Träger von Grundrechten sind.

§ 4f Abs. 2 BDSG beschreibt das Anforderungsprofil eines behördlichen DSB. Danach hat sich das Maß der Fachkunde, die ein behördlicher DSB aufzuweisen hat, insbesondere an dem Umfang und dem Schutzbedarf zu orientieren, dem die von der verantwortliche Stelle zu erhebenden Daten unterliegen. Daraus folgt aber, dass die behördlichen DSB des BKA und anderen Polizeidienststellen zu den qualifiziertesten Kräften ihrer Profession zählen müssten. Die von ihnen vorzunehmende Vorabkontrolle ist vorgelagerter Grundrechtsschutz. Dass von ihnen in der aktuellen Diskussion gar nicht gesprochen wird, könnte verschiedene Gründe haben – alle aber enden in unguten Vermutungen.

Man kann sich nicht des Eindrucks erwehren, als würden die Ermittlungsbehörden bei ihrer – zugegebenermaßen oft frustierenden – Arbeit die ihnen von Verfassungs wegen gesteckten Grenzen verletzen. Insofern haben gerade auch sie Anspruch darauf, dass ihre Handlungsoptionen klar geregelt sind und mögliche Grauzonen handlungsleitend ausgeleuchtet werden. Insofern steht der Gesetzgeber in einer doppelten Verpflichtung sowohl gegenüber den Bürgern als auch gegenüber den Strafverfolgungsbehörden. Solange er aber dieser Verpflichtung in verfassungskonformer Weise nicht nachkommt, ist besondere Wachsamkeit das Gebot der Stunde. Und erste Bürgerpflicht.

Richtervorbehalt?!

Es ist aber nicht nur die Grauzone zu beklagen, in der die Ermittlungsbehörden agieren. Problematisch ist auch das ganz offensichtliche Versagen des Richtervorbehalts. Seiner Funktion nach ist der Richtervorbehalt gewissermaßen eine weitere „Firewall".

Die Strafverfolgungsbehörden dürfen bestimmte Maßnahmen gegen Verdächtige nur auf Basis einer entsprechenden richterlichen Verfügung durchführen. So sollen Verdächtige vor unnötigen besonders schweren Eingriffen in ihre Grundrechte geschützt werden. Die Exekutive muss ihre Maßnahmen begründen. Sie muss auch begründen, warum kein milderes Mittel zur Verfügung steht.

Die Judikative hat die Zulässigkeit von Ermittlungsmaßnahmen im von der Staatsanwaltschaft angestoßenen Antragsverfahren zu prüfen und dann über ihren Einsatz zu entscheiden. Wenn schon nicht die Polizeigesetze die verfassungsrechtlichen Anforderungen an Online-Durchsuchung bzw. Quellen-TKÜ abbilden, so hat doch aber zumindest die Judikative zu prüfen, ob die von ihr selber aufgestellten Regeln zum Schutz der Grundrechte durch die geplanten Maßnahmen eingehalten werden. Insofern markiert der Richtervorbehalt eine verfassungsrechtliche Schutzmauer. Soll sie ihre Funktion im Rechtsstaat erfüllen und nicht zum bloßen Fetisch verkommen, dann muss dieses Institut gestärkt werden.

In den aktuellen Fällen aus Bayern hat sich der Richtervorbehalt als zahnloser Tiger erwiesen, wie es in der FAS vom 9.10.2011 heißt (vgl. aaO, S. 42). Auch in DIE ZEIT wird das Versagen des Richtervorbehalts beklagt. Kai Biermann nennt in seinem Artikel auch die Ursachen: Personalmangel und oft eine zu große Nähe der Richter zu den Strafverfolgungsbehörden. Aus Zeitmangel unterbleibt die rechtlich gebotene Prüfung, und wenn dann auch noch die Staatsanwaltschaft mit einem ausformulierten, bereits in Form eines Beschlusses begründeten Antrags auf die Richter zugeht, ist die Versuchung groß, diesen Antrag ohne weitere Prüfung zu unterschreiben.[6]

Der Rechtsstaat ist teuer. Seine Institutionen dürfen aber durch Personalmangel nicht ausgehöhlt werden. Vielmehr ist zu fordern, dass auch die Richterschaft so weiterqualifiziert wird, dass sie an Hand von im Antragsverfahren vorzulegenden Dokumenten, beispielsweise den Pflichtenheften der für den konkreten Einsatz vorgesehenen Software, selbst beurteilen kann, ob die einzusetzende Software den verfassungsrechtlichen Vorgaben entspricht.

Fazit

Die aufgedeckten Fälle und die Reaktionen der Verantwortlichen zeigen, dass bei vielen Verantwortlichen der Schutz der Grundrechte nicht mehr oberste Priorität genießt und hinter dem Aufklärungsinteresse zurück steht. Dies ist im Rechtsstaat inakzeptabel. Sicherheit ist kein Selbstzweck. Es muss auch das Interesse der Behördenleiter sein, für einen effektiven Datenschutz innerhalb der Behörden zu sorgen und durch eine effektive Vorabkontrolle in den Behörden selbst für einen vorgelagerten Grundrechtsschutz zu sorgen. Eine zusätzliche neue „Zertifizierungsstelle", wie auch schon vorgeschlagen, ist überflüssig. Wir – die Bürger – brauchen in den Behörden Personal, das sich seiner Verantwortung bewusst ist und sie auch wahrnimmt. Dafür werden die Beamten eingestellt und bezahlt. Und sollten sie selbst über die Zulässigkeit von Maßnahmen im Zweifel sein: Der BfDI und die Landesbeauftragten stehen als gesetzliche Ansprechpartner zur Verfügung.

Die Durchsetzung der datenschutzrechtlichen Standards gerade bei so sensiblen Ermittlungsmethoden wie der Online-Durchsuchung oder der Quellen-TKÜ muss das Ziel sein. Dabei tut Eile Not. Sonst metastasiert der „Bundestrojaner", höhlt die Grundrechte aus und wird zum Verfassungstrojaner.

6 Vgl. „Rettet den Richtervorbehalt" von Kai Biermann in DIE ZEIT online vom 12.10.2011.