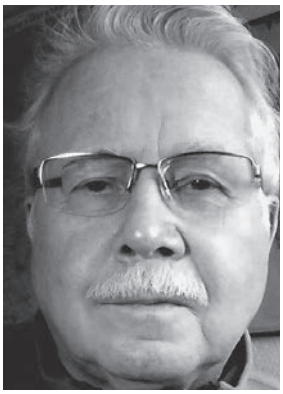
»Vernunft« und »Besonnenheit« am vernetzten Richterarbeitsplatz

Die Administration von EDV-Netzen der Justiz durch externe Institutionen stellt eine Beeinträchtigung der richterlichen Unabhängigkeit dar – Abhilfe kann nur durch Entnetzung erfolgen*

von Karlheinz Held



Karlheinz Held ist Richter am OLG Frankfurt am Main i. R.

I. Unabhängig weil alternativlos?

Die Vorstellung der Richter, dass sich jemand aus dem Finanzministerium für die Daten der Richter interessiert, ist paranoid. (Staatssekretär Harald Lemke am 19.06. 2005[1])

Das Dienstgericht des Bundes (BGH) hat mit seiner Entscheidung vom 06.10.2011 die Revision gegen das Urteil des Hessischen Dienstgerichtshofs für Richter bei dem Oberlandesgericht Frankfurt am Main vom 20.04.2010 – DGH 4/8–[2] zurückgewiesen[3]. Die dagegen gerichtete Verfassungsbeschwerde hat das Bundesverfassungsgericht mit begründetem Beschluss vom 17.01.2013 – 2 BvR 2576/11 – nicht zur Entscheidung angenommen.

Die Entscheidung des BGH enthält bemerkenswerte Feststellungen, die über den juristischen Anlass des Falles hinaus von Interesse sind (zu der Entscheidung des BVerfG hat schon Schwamb[4] zutreffend Stellung bezogen, weswegen hier nur ergänzende Ausführungen gemacht werden).

Die Ausführungen des BGH, wonach die richterliche Unabhängigkeit (nur) dann verletzt sei, wenn mit der Beobachtung der richterlichen Tätigkeit im EDV-Netz der Hessischen Justiz Maßnahmen verbunden würden, die dazu bestimmt oder geeignet wären, die richterliche Rechtsfindung durch psychischen Druck oder auf andere Weise unmittelbar oder mittelbar zu beeinflussen (seit BGH, Urteil vom 14.04.1997 – RiZ(R) 1/96, DRiZ 1998, 467, 469), münden für den konkreten Fall in folgende Feststellung:

»Die Administration des EDV-Netzes der Hessischen Justiz für den Rechtsprechungsbereich des Oberlandesgerichts Frankfurt am Main durch die HZD gibt Richtern vernünftigerweise keine Veranlassung, damit zu rechnen, das EDV-Netz werde von dienstvorgesetzten Stellen oder Dritten, die nicht allein der Aufsicht und Leitung der Gerichte, d. h. der Richter bzw. der Gerichtspräsidien, unterstehen, zu einer inhaltlichen Kontrolle richterlicher Dokumente im Kernbereich der Rechtsprechung genutzt, und deshalb von der Erstellung und Speicherung solcher Daten im EDV-Netz abzusehen.«

Und weiter (Rn. 30):

»Ebenso wenig ist ersichtlich, dass die richterliche Arbeitsweise durch die Befürchtung einer solchen Kontrolle beeinflusst wird. Da somit nicht davon ausgegangen werden kann, dass die bloße Eignung des EDV-Netzes zu einer inhaltlichen Kontrolle richterlicher Doku-

* Eine Anmerkung zu BGH – Dienstgericht des Bundes – Urteil vom 06.10.2011 – RiZ(R) 7/10 (BGH RiZ(R) 7/10) und BVerfG, Beschluss vom 17.01.2013 – 2 BvR 2576/11.

mente Richter veranlasst, das EDV-Netz nicht in dem von ihnen für sachgerecht gehaltenen Umfang zu nutzen, liegt eine Beeinträchtigung der richterlichen Unabhängigkeit nicht vor.«

Nach Meinung des BGH fehlt den anfänglich zwölf Vorsitzenden Richtern des OLG Frankfurt, die die sogenannte »Netzklage« zunächst im Widerspruchsverfahren und sodann über die Instanzen betrieben haben (bis wegen Erreichen des Ruhestands der übrigen Kläger nur noch eine Vorsitzende Richterin das Verfahren vor dem BGH und dem BVerfG weiter zum Ende betreiben konnte), jeder vernünftige Anlass, der Administration des EDV-Netzes, in das ihre Arbeitsplätze integriert sind, zu misstrauen und deswegen von der Erstellung und Speicherung richterlicher Daten im Netz abzusehen. Es handelt sich um den »kollegialen« Rat, die Vernunft zu gebrauchen, die nach allgemeiner Definition (auch) auf einer Tätigkeit des Verstandes beruht[5]. Der frühere Staatssekretär im hessischen Innenministerium Harald Lemke drückt dies nur etwas unhöflicher aus.

Der BGH hat aber übersehen, dass den Richter an zentral vernetzten Arbeitsplätzen die Möglichkeit fehlt, »von der Erstellung und Speicherung richterlicher Daten im Netz« überhaupt abzusehen. Es ist ein ehernes Gesetz einer jeden zentralen Vernetzung, dass sich der Einzelne ihr nicht entziehen kann. Unabhängig von dem gewählten Medium zur Erstellung richterlicher Daten landet schließlich jede richterliche Hervorbringung im Netz, wenn nicht schon am Richterarbeitsplatz selbst oder bei der Übermittlung an die Sitzgruppe, dann jedenfalls aber durch die Mitarbeiter/innen in den Geschäftsstellen und den Kanzleien. Um bis zur Einführung des elektronischen Rechtsverkehrs dem Netz zu entgehen, müssten Voten, Beschlussentwürfe etc. mit der Hand, einer mechanischen Schreibmaschine oder mit dem eigenen Computer hergestellt, ausgedruckt und per Bote in Umlauf gegeben werden. Dies bedeutete die Begründung und Aufrechterhaltung einer Parallel- oder Gegenstruktur[6] zur Gerichtsverwaltung, die alle betroffenen Richter auf sich nehmen müssten. Es kann vernünftigerweise nicht angenommen werden, dass Richter ein solches Arbeitsverhalten, durch das auch der Zugang zu vielen nur elektronisch vorgehaltenen Arbeitsmitteln versperrt wäre, überhaupt erwägen und durchhalten könnten. Der »Logik« des BGH folgend kann also schon deshalb nicht festgestellt werden, dass die richterliche Arbeitsweise durch die Befürchtung einer netzgesteuerten Kontrolle beeinflusst wird, weil eine Alternative zu dieser Arbeitsweise realistisch schon gar nicht mehr besteht. Das Argument des BGH an die Realität angepasst, führt seine Beweiskraft ad absurdum. Mit der Einführung des elektronischen Rechtsverkehrs entfällt schließlich auch noch endgültig die Möglichkeit, bei der Herstellung der richterlichen Daten auf den Dienstcomputer zu verzichten. Derzeit kann der Richter nur die Kontrolle des Arbeitsvorgangs selbst, nicht aber die Kontrolle seines Produkts verhindern. Schon deswegen ist nicht »ersichtlich«, dass die Richter ihre Arbeitsweise wegen der Befürchtung einer Kontrolle nicht ändern würden. Es besteht kein vernünftiger Grund für den BGH, aus dem Ausbleiben eines unmöglichen Alternativverhaltens Schlüsse zu ziehen und darauf die Entscheidung zu gründen, eine Beeinträchtigung der richterlichen Unabhängigkeit liege nicht vor.

Die Gefahr für die richterliche Unabhängigkeit besteht also nicht darin, dass sich die Richter wegen der im EDV-Netz möglichen technisch totalen Kontrolle des Gebrauchs der ihnen gestellten elektronischen Arbeitsmittel enthalten würden, sondern exakt darin, dass sie dies nicht könnten, selbst wenn es dafür vernünftige Gründe gäbe. Und diese Gründe gibt es bei dem derzeitigen Zustand der landesweiten zentralen Netzadministration, nicht nur im Bereich der HZD (Hessische Zentrale für Datenverarbeitung), in Hülle und Fülle. Die Begründung des BGH ist unlogisch und daher unvernünftig.

Alles bleibt, wie es im »Papierzeitalter« war

Der BGH hält die Vernetzung der richterlichen Arbeitsplätze für keine so einschneidende Maßnahme, dass daraus eine Veränderung des richterlichen Verhaltens zu erwarten wäre. Sie eröffne zwar die technische Möglichkeit, dass das EDV-Netz zur inhaltlichen Kontrolle richterlicher Dokumente, etwa zur systematischen Suche, Einsichtnahme, Kopie, Bearbeitung und Weiterleitung richterlicher Dokumente, genutzt werde[7]. Diese Möglichkeit bestehe aber unabhängig davon, ob das EDV-Netz durch eine nicht zum Geschäftsbereich des Ministers der Justiz gehörende Behörde wie die HZD oder durch den Minister der Justiz bzw. die Gerichtspräsidenten als unmittelbare Dienstvorgesetzte betrieben und verwaltet werde. Eine solche theoretische Zugriffsmöglichkeit der dienstaufsichtführenden Stellen auf richterliche Dokumente im Kernbereich der Rechtsprechung sei in der deutschen Justiz weithin gegeben.

Die »theoretische Zugriffsmöglichkeit« im Papierzeitalter[8], die eher doch eine praktisch aber nur vereinzelt anwendbare, zeitlich und räumlich eingegrenzte und vor allem von dem einzelnen Richter bemerkbare Zugriffsmöglichkeit ist, wird durch die Vernetzung, der tiefgreifendsten Innovation seit der Erfindung des Buchdrucks[9], aber durch eine permanente (zeitlich unbegrenzte), umfassende, technisch totalitäre Kontrolle sowohl der Arbeitsergebnisse als auch des Verhaltens schlechthin ersetzt, von der im Missbrauchsfalle die Richter regelmäßig nichts bemerken können. Dass die Richter, auch die des BGH, sich vielleicht dennoch nicht »kontrolliert« wähnen, beruht im Wesentlichen auf einem Mangel an Vorstellungskraft im Zeitalter der Vernetzung. Wo die Vorstellung (Anschauung) fehlt, können keine Begriffe gebildet werden[10]. Der BGH hat ganz offensichtlich nicht erkannt, um welche Dimensionen der technischen Überwachung es hier geht. Aber auch das BVerfG a. a. O. hat keinen zutreffenden Blick auf den Sachverhalt, wenn es ausführt:

»Eine derartige verbotene Einflussnahme kann auch dann vorliegen, wenn ein besonnener Richter durch ein Gefühl des unkontrollierbaren Beobachtetwerdens (vgl. im Zusammenhang mit der sog. Vorratsdatenspeicherung BVerfGE 125, 260 <332>) von der Verwendung der ihm zur Erfüllung seiner richterlichen Aufgaben zur Verfügung gestellten Arbeitsmittel abgehalten würde.«

Dass die Richter des BVerfG selbst einer unkontrollierbaren Beobachtung unterliegen, von der sie bei der Beschlussfassung im Ja-

nuar 2013 noch nichts bemerkt zu haben scheinen, ist ihnen zwischenzeitlich vielleicht bewusst geworden (siehe unter II. unten). Ob ihnen aber auch die Erkenntnis zugewachsen ist, dass sich die Richter des Arbeitsmittels überhaupt nicht enthalten können, wenn sie und ihre Peripherie zentral vernetzt sind, kann derzeit nur vermutet werden.

Zwar geeignet, aber nicht bestimmt!

»Das Steuergeheimnis ist in einem Rechtsstaat ein hohes Gut. Gleichzeitig müssen wir in den letzten Jahren feststellen, dass vieles, was früher gehütet wurde, sich auf einmal in der Öffentlichkeit befindet. Das liegt vielleicht an der Technologie, die das erleichtert.« (Dr. Wolfgang Schäuble, Bundesminister der Finanzen. Interview mit der FAZ vom 07.02. 2014)

Die systemimmanente Einsichts- und Zugriffsmöglichkeit der obersten Administratoren des EDV-Netzes, so führt der BGH aus, sei nicht zur inhaltlichen Kontrolle richterlicher Dokumente bestimmt. Sie diene vielmehr dem sachgerechten Betrieb und der ordnungsgemäßen Verwaltung des EDV-Netzes und sei zu diesem Zweck unerlässlich.

Der BGH berücksichtigt nicht, dass auch technisch notwendige Maßnahmen ihre Auswirkungen auf die Betroffenen haben. Wäre es aber nicht schon denkbar, dass eine »systemimmanente Einsichts- und Zugriffsmöglichkeit«, die in ihrer konkreten Ausgestaltung auch noch technisch notwendig wäre, die richterliche Unabhängigkeit beeinträchtigen könnte? Müsste dann diese Beeinträchtigung hingenommen werden? Genügte es dann, dass das EDV-Netz zur totalen Kontrolle der richterlichen Arbeit und des Verhaltens der Richter am Arbeitsplatz zwar geeignet, aber dazu »nicht bestimmt« sei? Wie kann bemerkt werden, wenn die Bestimmung nicht beachtet wird? Wenn dies (aus technischen Gründen) nicht bemerkt werden kann, was dann?

Dann würde nur eine »Vernunft« weiter helfen, die ihre regulative Leitidee in einem unkritischen, unreflektierten Glauben an die Obrigkeit gefunden hätte. Ist dies diejenige Vernunft, die der BGH den Netzklägern anempfiehlt?

Wegen der Eigenschaften eines zentralen Computernetzes, das einen technisch totalitären Anspruch hat[11], kann aber letztlich dahinstehen, ob die technische Eignung zur Kontrolle oder die Bestimmung dieser Technik zur Kontrolle oder beide Gesichtspunkte maßgeblich sind: Denn anders als in den bisher von dem BGH entschiedenen Fällen (etwa BGH, Urteil vom 24.11.1994 – RiZ(R) 4/94, NJW 1995, 731, 732 = Telefonanlage) handelt es sich nicht um eine mögliche Beeinträchtigung der richterlichen Unabhängigkeit durch die technische Peripherie zur Unterstützung der Rechtsprechungstätigkeit, die von den Richtern durchaus erkannt, umgangen oder mit Hilfe des Rechtswegs zu den Dienstgerichten abgewendet werden könnte. Im Falle der Eignung einer technischen Einrichtung zur vollständigen, totalen Überwachung ist diese auch zur Kontrolle der Richter bestimmt, wenn die nach dem Gesetz erforderlichen technischen und organisatorischen Maßnahmen (§ 10 Abs. 1 Hessisches Datenschutzgesetz, HDSG) unterbleiben oder unwirksam sind. Denn der Effekt wird dann billigend in Kauf genommen. Es kommt dann nicht mehr auf diese Unterscheidung an.

Nicht bemerkbare Kontrolle beeinträchtigt die richterliche Unabhängigkeit

Die negative Auswirkung besteht in jedem Fall in dem Verhalten der Richter, die sich ständig überwacht fühlen müssen (BVerfG a. a. O. = dem Verhalten »besonnener« Richter!). Es ist nicht der »drohende Verlust« des Arbeitsmittels, der die richterliche Unabhängigkeit gefährdet, sondern es ist die Konsequenz aus einer »gesteigerten Öffentlichkeit« der richterlichen Arbeit, die technisch durch das Phänomen der Konnektivität bedingt ist. Menschen verhalten sich anders, wenn sie mit einer »erweiterten« Kenntnisnahme ihrer Tätigkeit rechnen müssen, als dies im Kontext ihrer Arbeit eigentlich vorgesehen ist. Es kommt zu den bekannten Erscheinungen der Selbstzensur bis zum vorauseilenden Gehorsam. Schon die Überlegung, ob man nicht besser eine Formulierung oder die Mitteilung eines Gedankens vermeiden solle, tritt nicht erst bei der Herstellung des Endprodukts auf, das letztlich auch für die Öffentlichkeit bestimmt ist, sondern schon im Vorfeld der Meinungsbildung (etwa bei einer Beratung), wenn Schriftliches niederzulegen ist. Nur noch die Gedanken sind dann frei (Chilling Effects = Die Schere im Kopf). Der Anschluss an das EDV-Netz ist doch dann im Sinne der Definition des BGH »dazu bestimmt oder geeignet, die richterliche Rechtsfindung durch psychischen Druck oder auf andere Weise unmittelbar oder mittelbar zu beeinflussen«. Das BVerfG a. a. O. hat sogar auf unkontrollierbares Beobachtetwerden als eine verbotene Einflussnahme auf einen »besonnenen Richter« und auf den Zusammenhang mit der sog. Vorratsdatenspeicherung BVerfGE 125, 260 <332> hingewiesen, die Relevanz dieser Erkenntnis für die eigene Entscheidung aber damals nicht erkannt. Das hat sich möglicherweise inzwischen geändert, weil es sich bei den Richtern des BVerfG um »besonnenen Richter« handeln dürfte (siehe Endnote 46).

Das Gefühl, das Beratungsgeheimnis nicht mehr schützen zu können, müsste den Richtern, auch denen des BGH und erst recht denen des BVerfG meiner Meinung nach emotional mindestens so nahe gehen, wie der Verlust des Steuergeheimnisses dem Bundesminister der Finanzen Dr. Wolfgang Schäuble.

Die Welt verändert sich, aber eine bewährte Rechtsprechung muss sich nicht anpassen!

Durch die Vernetzung werden nicht nur die Menschen vernetzt, sondern auch verschiedene Rechtsgebiete werden durch die Technik zusammengeführt, die früher »getrennt« vorstellbar waren. Auch das verkennt der BGH, wenn er ausführt, die Vereinbarkeit der Maßnahme mit dem verfassungsrechtlichen Gebot organisatorischer Selbständigkeit der Gerichte (Art. 20 Abs. 2 Satz 2, Art. 92, 97 GG) und mit anderen Gesetzen und Rechtsvorschriften sei nicht Gegenstand des vorliegenden Verfahrens. Insbesondere die Überprüfung der Vereinbarkeit der Maßnahme mit da-

tenschutzrechtlichen Bestimmungen sei den Verwaltungsgerichten vorbehalten, wie sich aus BGH, Urteil vom 24. November 1994 – RiZ(R) 4/94, NJW 1995, 731, 732 mwN ergäbe. Der BGH hatte sich dort aber ausschließlich mit der Frage zu befassen, ob die Beobachtung und Kontrolle weniger äußerer Daten, die von einer Telefonanlage mit Gesprächsdatenerfassung erfasst und aufgezeichnet werden, mit der richterlichen Unabhängigkeit vereinbar ist oder nicht. Hier geht es aber um ein System, das zur totalen Kontrolle sowohl der erzeugten Daten als auch des Arbeitsverhaltens geeignet ist. Der Sachverhalt ist völlig verschieden.

Es war vorliegend unstreitig, dass am 06.08.2009 auf den Dienstcomputern aller hessischen Richter, die damals zentral vernetzt waren, ein sogen. VNC-Server installiert worden war. Damit war es möglich, die Dienstcomputer aus der Ferne »zu übernehmen«, ohne dass dies die Richter hätten bemerken müssen oder es hätten verhindern können. Es bestand damit die Möglichkeit, etwa den Bildschirminhalt eines Dienstcomputers auf einem entfernten Rechner wiederzugeben, dem Richter also bei seiner Arbeit »über die Schulter zu schauen« (Fall 1). Stellte man sich dagegen vor, ein Mitglied der Justizverwaltung beträte das Dienstzimmer eines Richters auf Probe (ohne vorher anzuklopfen!), um ihm bei der Arbeit zuzusehen (über die Schulter zu schauen, Fall 2), wäre die Empörung groß. Der VNC-Server hat die Richter »kalt gelassen«. Der Grund, warum mit einem Vorfall in der Art des Falles Nr. 2 nicht zu rechnen ist, liegt aber darin, dass ein solches Vorgehen von dem betroffenen Richter bemerkt würde. Alle Fälle, in denen der BGH in seiner Rechtsprechung mit »Übergriffen« zu tun hatte, sind vorher bemerkt worden. Es hat sich dort noch niemand beschwert, der den gerügten Verstoß nicht bemerkt hätte. Künftig werden solche Fälle nicht mehr auftreten, schlicht weil sie nicht bemerkt werden (können).

Aus dem Vergleich des Vorfalls mit dem VNC-Server (Fall 1) und dem gedachten Vorgang eines unangemeldeten Besuchs im Zimmer des Proberichters (Fall 2) kann man ohne weiteres ersehen, dass alle denkbaren verbotenen Übergriffe auf die Arbeitsergebnisse oder den Arbeitsvorgang der Richter im Netz nur noch unter Verletzung datenschutzrechtlicher Bestimmungen wie des HDSG möglich sind (etwa § 10 HDSG), weil die Arbeit im Netz erbracht und technisch vollständig und zentral durch die Netzadministration kontrolliert wird . Während der Fall 2 keinen datenschutzrechtlichen Aspekt haben muss und von der Zuständigkeit des BGH nach seiner Rechtsprechung erfasst würde, müsste der Fall 1 den Verwaltungsgerichten vorbehalten bleiben, wobei offen bleiben muss, wie Richter dort den Zustand ungeplanter Öffentlichkeit ihrer Tätigkeit überhaupt rügen könnten. Künftig würde es gar keine gleichgelagerten Fälle mehr geben und dem BGH ginge die Arbeit in weiten Teilen aus. Dass seine Rechtsprechung den durch die Technik veränderten Bedingungen angepasst werden muss, ist dem BGH (noch) nicht aufgefallen.

Man kann dem Richter von Ferne über die Schulter schauen

Der Schutz der richterlichen Unabhängigkeit in den Netzen ist letztlich nur noch durch technische und organisatorische Maßnahmen im Sinne von § 10 HDSG zu bewirken, wobei sich aus dem Vergleich von § 1 Abs. 1 Ziff. 2 HDSG mit § 10 Abs. 1 HDSG ergibt, dass dabei Kostengesichtspunkte keine Rolle spielen dürfen. Nach § 10 Abs. 1 Satz 2 HDSG steht nämlich ausdrücklich nur der Schutz personenbezogener Daten des § 1 Abs. 1 Ziff. 1 HDSG unter dem Vorbehalt der Angemessenheit, nicht jedoch die Bewahrung des auf dem Grundsatz der Gewaltenteilung beruhenden Staatsgefüges vor einer Gefährdung (§ 1 Abs. 1 Ziff. 2 HDSG). Ähnliches gilt auch für den Bereich der Gerichtsorganisation[12]. Die Richter haben jedoch keine verwaltungsgerichtlichen oder sonstigen Rechtsbehelfe, um ein System anzugreifen, das als solches das Beratungsgeheimnis gefährdet oder mit an Sicherheit grenzender Wahrscheinlichkeit verletzt, wenn sie keine konkrete Kenntnis über »den einzelnen Fall« mehr erlangen können, weil sie vollständig auf eine für sie nicht durchschaubare Netzadministration angewiesen sind!

Kein vernünftiger Grund?

»Das Speichern von Kommunikationsdaten darf nicht die Berufsgeheimnisse der Anwälte, Ärzte, der Journalisten und der Geistlichen aushebeln. Aber der US-Geheimdienst hält sich an die Gesetze der EU-Staaten so wenig wie an die Urteile des Europäischen Gerichtshofs. Er sitzt potenziell in jedem elektronischen Anwaltspostfach, er hat jedenfalls die technischen Möglichkeiten, dort die gesamte Kommunikation abzugreifen. (…) Anders als Ärzte, Seelsorger und Journalisten werden die Anwälte per Gesetz gezwungen, künftig bestimmte elektronische Kommunikationsmethoden zu verwenden – ohne dass der Staat die Sicherheit dieser Methoden gewährleisten kann. Das ›Gesetz zur Förderung des elektronischen Rechtsverkehrs‹ wird daher, wie es aussieht, unfreiwillig zu einem Gesetz zur Förderung der Spionage und zur Beendigung des Anwaltsgeheimnisses.«
(Heribert Prantl, Süddeutsche Zeitung vom 07.05.2014, S. 4.)

Heribert Prantl hat die Richter nicht erwähnt, für die das gleiche gilt, denn sie sitzen »am anderen Ende« des vorgesehenen und zum Teil schon eingerichteten elektronischen Rechtsverkehrs und sollen die Akten elektronisch bearbeiten, was sie in Teilen schon jetzt tun. Dort geht es um das Anwaltsgeheimnis, hier um das Beratungsgeheimnis und infolge dessen massiver Gefährdung um die Unabhängigkeit der Richter. Der dem BGH vorliegende Fall gibt genügend Anlass, daran zu zweifeln, ob die Netzkläger, sämtlich »besonnene Richter«, nicht doch vernünftige Gründe vorgebracht haben, die im Sinne ihrer Anträge umzusetzen gewesen wären.

Soweit der BGH »Dritte, die nicht allein der Aufsicht und Leitung der Gerichte, d. h. der Richter bzw. den Gerichtspräsidenten unterstehen«, gegen jedes vernünftige Misstrauen verteidigt, hat er (auch) einen konkreten Sachverhalt bewertet, der sich aus dem Abschlussbericht der Arbeitsgruppe »EDV-Netzbetrieb für die Dritte Gewalt« [13] ergibt und im gesamten Verfahren unstreitig war. In der Anlage 6 – Sitzungsprotokoll der 5. Sitzung der Kommission (welches dem BGH wie der auch der gesamte Kommissionsbericht im übrigen vorlag) heißt es:

Foto: Frank Schreiber

»Sodann führt Frau Dembowski (Mitarbeiterin des Hessischen Datenschutzbeauftragten, der Verf.) aus, dass anlässlich einer Prüfung durch den Hessischen Datenschutzbeauftragten bei der HZD leider festgestellt werden musste, dass das Masterpasswort der obersten Administratoren unzulässig und ohne Mitteilung an die Justiz sowohl an Mitarbeiter der HZD in Wiesbaden als auch externe Dienstleister weitergegeben wurde.
Herr Dr. Köbler (Mitarbeiter des Justizministeriums, der Verf.) bezeichnet dieses Vorgehen der HZD als klaren Vertragsbruch.
In der Sache habe Herr Staatssekretär Dr. Schäfer den die Dienstaufsicht führenden Herrn Staatssekretär Dr. Arnold schriftlich um Aufklärung gebeten; eine Antwort stehe derzeit noch aus.
Herr Ebner (Leiter der Stabsstelle e-government im Hessischen Ministerium des Innern, der Verf.) machte aus seiner Sicht deutlich, dass es sich bei den Weitergaben der Passwörter um fachlich notwendige Schritte gehandelt habe, da lediglich so der Fachverstand zur korrekten Administration in die Lage versetzt wurde, Problemstellungen zu beheben.
Die aus den Räten entsandten Mitglieder der Arbeitsgruppe hingegen sind der Auffassung, dass gerade dieses Vorgehen die Bedenken der widerspruchsführenden Richter am Oberlandesgericht zu bestätigen vermag.«

Mit den »Dritten« sind also nicht nur die Mitarbeiter der HZD, sondern auch nicht näher bezeichnete »externe Dienstleister« und deren Bedienstete gemeint, gegen die nach Meinung des BGH ein Misstrauen der Richterschaft unberechtigt ist. Zwar haben laut Protokoll die Mitarbeiterin des Datenschutzbeauftragten und der Vertreter des Justizministeriums ihr Bedauern über die Weitergabe des obersten Master-Passwortes an jene Dritte geäußert bzw. dieses Verhalten als »klaren Vertragsbruch« bezeichnet, die Richter allerdings haben dennoch nach Meinung des BGH keinen vernünftigen Grund, deshalb von der »Erstellung und Speicherung« ihrer richterlichen Daten wegen der Administration des EDV-Netzes der Hessischen Justiz für den Rechtsprechungsbereich des Oberlandesgerichts Frankfurt am Main im EDV-Netz abzusehen (wenn sie es nur könnten!).

Der frühere hessische Datenschutzbeauftragte Professor Dr. Friedrich von Zezschwitz hatte im 30. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vom 31. Dezember 2001 unter »Datenschutz in der Justiz Ziff. 28.2, 6«[14] die Auffassung vertreten, die Administration des Justiznetzes sollte weder durch staatliche Fernwartungsanbieter noch durch außenstehende Firmen erfolgen, da deren Verhalten im Netz nur schwer kontrollierbar sei[15]. Dass von einer Kontrolle aber gänzlich abgesehen wird, indem einer unbekannten Anzahl externer Dienstleister und damit einer unbekannten Anzahl von deren Mitarbeitern durch Überlassung des obersten Master-Passwortes der unbeschränkte und unkontrollierbare Zugriff auch auf alle richterlichen Daten, auch die, die dem Beratungsgeheimnis unterliegen, eingeräumt wird, hätte er sich sicher nicht träumen lassen. Der BGH hat die Relevanz dieses Vorgangs nicht übersehen können, denn er hat in seinem Urteil auf Seite 4, Rn 3, übrigens abweichend von dem insoweit unverständlichen Vortrag des Landes, zutreffend ausgeführt:

»Die Dokumente der Rechtsprechung werden auf dezentralen Servern bei den Gerichten und Staatsanwaltschaften gehalten. Administratoren der HZD haben Zugriff auf alle Systemdateien des Gesamtnetzes und – in den meisten Betriebssystemen – auf alle Dokumentendateien. Sie verfügen über die technische Möglichkeit, sämtliche im EDV-Netz der Hessischen Justiz gespeicherten Dokumente einzusehen, protokollierte Vorgänge

der Datenbearbeitung zur Kenntnis zu nehmen und die Daten zu verarbeiten.«

Aus dieser Feststellung folgt notwendig (vernünftigerweise) die Einsicht, dass mit der Überlassung des Master-Passwortes an »externe« nicht in die Organisation des Staates eingebundene Dienstleisternein Zugriff auf alle richterlichen Daten im Netz eingeräumt wird. Es handelt sich um einen Vorgang, der strafrechtlich zum Teil so zu bewerten ist, wie die Überlassung dem Anwaltsgeheimnis anvertrauter Daten an externe Dienstleister, wobei es sich hier noch zusätzlich um richterliche Dienstgeheimnisse (§ 353b StGB) handelt.

Um die Möglichkeiten des »cloud computing« ohne Verstoß gegen § 203 StGB nutzen zu können, sieht der Deutsche Anwaltstag einen rechtspolitischen Handlungsbedarf[16] und schlägt vor, § 203 StGB dahingehend zu ändern, dass externe Dienstleister wie in die Kanzlei integrierte Gehilfen zu behandeln wären und der Anwalt keine Gefahr läuft, einen Straftatbestand zu begehen, wenn er »externen Dienstleistern« den Zugriff auf Mandantendaten ermöglicht[17]. Das Gutachten der großen Strafrechtskommission des deutschen Richterbunds geht allerdings davon aus, dass eine Bewertung des selbstständigen IT-Dienstleisters als berufsmäßiger Gehilfe des Anwalts nach derzeitiger Rechtslage nicht möglich ist.[18] Der BGH hat übersehen, dass der vorstehend beschriebene Vorgang (Überlassung des Master-Passwortes an externe Dienstleister) strafrechtliche Relevanz hat. Die Wertung des Gesetzgebers, solche Zugriffe mit den Mittel des Strafrechts zu unterbinden, gibt aber nach seiner Meinung den Richtern vernünftigerweise keine Veranlassung, damit zu rechnen, das EDV-Netz werde von Dritten, die nicht allein der Aufsicht und Leitung der Gerichte, d. h. der Richter bzw. der Gerichtspräsidien, unterstehen, zu einer inhaltlichen Kontrolle richterlicher Dokumente im Kernbereich der Rechtsprechung genutzt. Wahrscheinlich hält sich der BGH im Rahmen seiner bisherigen Rechtsprechung nicht für zuständig, strafrechtlich relevante Vorgänge in seine Rechtsprechung einzubeziehen, wie auch die Fragen der Gerichtsorganisation und des Datenschutzes nicht in seine Kompetenz fallen sollen, selbst dann, wenn sie die richterliche Unabhängigkeit massiv bedrohen und es keine anderweitigen Rechtsbehelfe für die Richter gibt, als die Anrufung des Richterdienstgerichts.

Die Weitergabe (besser: der Verrat) des Master-Passwortes führt sonst regelmäßig zur fristlosen Kündigung der Verantwortlichen wegen Vertrauensverlustes[19]. Weil der Abschlussbericht der Kommission »EDV-Netzbetrieb für die dritte Gewalt« keine Aufklärung des Vorgangs enthält, wie er in der Anlage 6 – Sitzungsprotokoll der 5. Sitzung der Kommission – eigentlich angekündigt worden ist, stellte sich die Frage nach einer vernünftigen Erklärung doch auch für den BGH[20]. Weder wurden Mitarbeiter der HZD dienst- oder arbeitsrechtlich belangt noch strafrechtlich verfolgt. Der derzeitige hessische Datenschutzbeauftragte (Nachfolger von Herrn Prof. Dr. Friedrich von Zezschwitz) hatte zunächst durch seine Mitarbeiterin den Vorgang bedauern lassen (»leider festgestellt werden musste, ...«). In keinem Tätigkeitsbericht (seit 2005) des (neuen) hessischen Datenschutzbeauftragten, Herrn Prof. Dr. Michael Ronellenfitsch, findet sich aber auch nur ein Wort über den von seiner eigenen Behörde aufgedeckten Vorgang und auch keine Angaben über die der Landesregierung von ihm vorgeschlagene Abhilfe. Statt dessen kümmert er sich verdienstvoll etwa um Videokameras im Fuldaer Stadtschloss[21].

Überlassung des Masterpassworts der HZD an externe Dienstleister

Nachdem der Richterschaft (und im Verfahren über die Netzklage auch dem BGH) von dem beklagten Land keine Aufklärung über die Hintergründe des Sachverhalts gegeben worden ist[22], bedarf es einer »vernünftigen« Erklärung für die Hintergründe des »klaren Vertragsbruchs« (Dr. Köbler). Sie kommt von der Stabsstelle e-government im Hessischen Ministerium des Innern (HMdI)[23] in dem vorstehend wiedergegebenen Sitzungsprotokoll der 5. Sitzung der Kommission: Es handle sich bei den Weitergaben der Passwörter um fachlich notwendige Schritte, da lediglich so der Fachverstand zur korrekten Administration in die Lage versetzt wurde, Problemstellungen zu beheben (Herr Ebner).

Das Unterbleiben jeglicher Reaktion auf den von dem Vertreter des HMdJ als klaren Vertragsbruch bezeichneten Vorgang ist vernünftigerweise nur damit zu erklären, dass das von dem Datenschutzbeauftragten und dem HMdJ zunächst kritisierte Verhalten von höchster Stelle als korrekte Administration »durch Hinzuziehung von Sachverstand« (der bei der HZD wohl fehlte?) angeordnet oder doch gebilligt worden ist. Auch »besonnene« Richter haben deswegen allen Grund, vernünftigerweise mit allem zu rechnen. Sie müssen wegen der Weigerung des beklagten Landes, den Sachverhalt aufzuklären, damit rechnen, dass die zunächst als Vertragsbruch bedauerte Vorgehensweise als »normale Netzadministration« bis zum heutigen Tag beibehalten wird. Unter solchen Umständen sollte die Vernunft gebieten, jeglichen Gebrauch des Netzes zu unterlassen, wenn dazu die Möglichkeit bestünde. Denn wenn eine Kontrolle wegen der Art und Weise der Netzadministration nicht (mehr?) ausgeübt werden kann, besteht auch für besonnene Richter (BVerfG a. a. O.) vernünftiger Anlass, mit Übergriffen von innen und von außen zu rechnen.

Nachdem der Staat zwischenzeitlich auch einräumen muss, den unerlaubten Zugriff auf die Netze nicht verhindern zu können (und wie nachstehend unter II. noch ausgeführt werden wird, auch nicht von innen auf die gespeicherten Daten), erscheint es vielmehr unvernünftig, ohne die erforderliche Anpassung der Systeme etwa auch noch den elektronischen Rechtsverkehr einzuführen. Es handelt sich ersichtlich nicht nur um Bereiche des Strafrechts, Datenschutzrechts oder des Rechts der Justizorganisation, für die der BGH eine Zuständigkeit ablehnt (Seite 11, Rn 25). Denn wenn die Richterschaft (vernünftigerweise) auf den Schutz – etwa des Beratungsgeheimnisses – durch »sonstige Rechtsvorschriften« nicht mehr setzen kann, dann ist der Zustand erreicht, den der BGH selbst als dazu bestimmt oder geeignet beschreibt, die richterliche Rechtsfindung durch psychischen Druck oder auf andere Weise unmittelbar oder mittelbar

zu beeinflussen (seit BGH, Urteil vom 14.04.1997 – RiZ(R) 1/96, DRiZ 1998, 467, 469, BVerfG a. a. O.).

Mit anderen Worten: wenn keine technischen Maßnahmen (§ 10 Abs. 1 HDSG) mehr greifen und Übergriffe von innen oder von außen nicht zuverlässig erkannt und verhindert werden können, schützen die entsprechenden Rechtsvorschriften die richterliche Unabhängigkeit nicht mehr. Der BGH ist dann aber auch zur Beurteilung dieses Sachverhalts originär zuständig, weil er sonst die selbst definierte Aufgabenstellung nicht mehr wahrnehmen würde. So liegt der Fall, wenn eine unbekannte Zahl von unbekannten Mitarbeitern von unbekannten »externen Dienstleistern« ohne kontrolliert werden zu können, im »Justiznetz« mit »obersten« Administratorenrechten agieren kann. Die Vernunft des BGH folgt jedoch eigenen Prinzipien. Es kann dies nur ein unreflektiertes Vertrauen in die »Obrigkeit« sein, was vorliegend dazu geführt hat, dass ein offensichtlicher Sachverhalt nicht zur Kenntnis genommen wird.

Ein klarer Vertragsbruch bei der HZD hatte keine Konsequenzen

Nach Meinung des BGH (Urteil Rn. 30) dient die Zugriffsmöglichkeit der »obersten Administratoren« dem sachgerechten Betrieb und der ordnungsgemäßen Verwaltung des EDV-Netzes und ist zu diesem Zweck unerlässlich. Dass hier externe Dienstleister und weitere Mitarbeiter der HZD in Wiesbaden die Rolle der »obersten Administratoren« unstreitig eingenommen haben, weil sie mit dem Master-Passwort Administratorenrechte (Rechte im technischen, nicht rechtlichem Sinne!) ausüben können, soll die Richter nicht beunruhigen, obwohl dieser Sachverhalt außerhalb der Grenzen einer ordnungsgemäßen Administration, eher auf dem Gebiet des Strafrechts, angesiedelt ist (HMdJ: »klarer Vertragsbruch«, Mitarbeiterin des Datenschutzbeauftragten: »leider festgestellt werden musste«). Der BGH hält sich auch unter solchen Umständen für die Einhaltung des Datenschutzes und der Regeln der Gerichtsorganisation[24] aber für »nicht zuständig« und beschäftigte sich nicht mit der Frage, warum die Richter des OLG Frankfurt (und anderer Gerichte auch) dennoch ihr Arbeitsverhalten nicht ändern. Vom Datenschutzbeauftragten ist dazu nichts zu hören.

II. Was hat sich geändert? Hat sich überhaupt etwas geändert?

Wir fahren in einer Kutsche ohne Dach und hoffen, dass es nicht regnet.
(Michael Hange, Präsident des Bundesamtes für die Sicherheit in der Informationstechnik.[25])

Der BGH setzt ein von ihm vermutetes (aber auch durch keine Beweise empirisch belegtes) Verhalten der Richterschaft im Papierzeitalter, in dem doch auch »theoretisch?« Zugriffsmöglichkeiten auf richterliche Dokumente bestünden, unzulässig mit einem vermuteten in der Sache doch unmöglichen Verhalten unter den völlig geänderten Bedingungen des vernetzten Arbeitsplatzes gleich. Es ist durchaus möglich, aber wenig vernünftig, dass die Richterschaft weitgehend auch noch heute keinen Anlass sieht, ihr Verhalten aufgrund der Erkenntnisse »anzupassen«, die seit Jahren in den Medien verbreitet werden.[26] Man muss dabei aber berücksichtigen, dass die hessische Richterschaft jahrelang von der Landesregierung mit der Behauptung falsch informiert worden ist, auf die richterlichen Daten könne die Netzadministration nicht zugreifen (Siehe Netzbeschreibung im Abschlussbericht EDV-Netzbetrieb für die dritte Gewalt, S. 79):

»4.3 Details zur Persönlichen Ablage
Die Persönliche Ablage ist exklusiv für den Anwender bestimmt. Sie ist für jeden anderen Anwender – insbesondere für die HZD-Systemadministratoren, die ADV-Fachbetreuer und die örtlichen Systembetreuer – unzugänglich. Im persönlichen Verzeichnis kann jeder Anwender Daten ablegen, die nur von ihm gelesen und bearbeitet werden können. Anderen Anwendern wird der Zugriff auf diese Ablage verweigert.«

Ähnliches wurde über die Instanzen der Netzklage hin weiter behauptet und ist nunmehr durch den BGH in verdienstvoller Deutlichkeit als unzutreffend bezeichnet worden (Urteil auf Seite 4 Rn. 3).

Zur Zeit meines aktiven Dienstes habe ich als Vorsitzender des Richterrats des OLG Frankfurt mit Kollegen gesprochen, die an diese Darstellung (damals noch) glaubten. Mit zunehmender Erkenntnis, dass es am Richterarbeitsplatz keine »Geheimnisse« mehr gibt, wird sich diese Einschätzung, wenn sie sich nicht schon in neuerer Zeit verändert haben sollte, hoffentlich anpassen. Ein Richter kann in Verfahren, in denen es ihm aus irgend einem einschlägigen Grund erforderlich erscheint, wegen der Gefahr der unzulässigen Beobachtung die Nutzung des EDV-Netzes zwar nicht ohne Mitwirkung der Justizverwaltung, so wie diese selbst es aber immer kann, unterlassen[27], er wird sich aber anpassen. Dieses Verhalten wird leider um sich greifen, wenn bekannt wird, dass in den großen Netzen, an denen auch die Richterschaft angeschlossen ist, mit der derzeit vorhandenen Software und Hardware keine rechtlich einwandfreie und die Belange der Rechtsprechung wahrende EDV-Versorgung überhaupt möglich ist. Wenn die Richterschaft die Erkenntnis des Präsidenten des Bundesamtes für die Sicherheit in der Informationstechnik teilte (siehe Endnote 25) und ein dem zutreffend gewählten Bild entsprechendes Empfinden entwickelte, würde sie es auch nicht für unwahrscheinlich halten, dass Dienstvorgesetzte sich ein »Bild machen« werden, wenn deren Zugriffe nicht nachvollziehbar sind. Denn im Papierzeitalter konnte solches »auffliegen«, im EDV-Zeitalter kann dies leicht unentdeckt bleiben.

Eine die Belange der Rechtsprechung wahrende EDV-Versorgung ist in großen Netzen nicht möglich

Hessische Richter etwa, die mit Vergabesachen befasst sind, würden vielleicht ihre Voten lieber nicht im Netz abgespeichert haben, wenn ihnen bekannt gewesen wäre, dass die in den Vergabeverfahren durch die HZD rechtswidrig bevorzugten »externe Dienstleister«, mit Master-Passwort im Netz beschäftigt sind[28]. Die Richter des Hessischen Finanzgerichts würden es bei entsprechender Sensibilität vielleicht unangemessen finden, dass der »Gegner« der steuerpflichtigen Bürger die Daten der Prozesse verwaltet und ihre Arbeit vollständig kontrollieren kann (was sie

mit der »Mentalität des Papierzeitalters« ablehnen würden, wenn Finanzbeamte in den Geschäftsstellen persönlich anwesend wären und die Geschäfte dort abwickelten). Der frühere Staatsekretär Lemke müsste sich überlegen, ob mangelndes Interesse an den Daten der Richter des Hessischen Finanzgerichts den Beamten des Finanzministeriums zur Zierde gereichte.

Es vergeht kaum eine Woche, in der nicht geheime Nachrichten aus justiziellen und anderen Verfahren in die Öffentlichkeit dringen. Die Ermittlungen der Staatsanwaltschaft Göttingen gegen die Ermittler im Fall des früheren Bundespräsidenten Christian Wulff wegen Verletzung von Dienstgeheimnissen[29] aus dem Ermittlungsverfahren gegen Herrn Wulff haben nach bisheriger Erkenntnis nicht zu einer Aufklärung geführt. Ebensowenig die Ermittlungen im Fall des Bundestagsabgeordneten Edathy, in dem 15 leitende Mitarbeiter der zuständigen Staatsanwaltschaft in Verdacht geraten sind, denen ein dienstinterner Bericht elektronisch zugegangen war, der dann unerlaubt in die Öffentlichkeit gelangte[30]. Auf die Steuerakte von Uli Hoeneß hatten tausende Finanzbeamte Zugriff. Mit »hoher Wahrscheinlichkeit« habe ein Informant, der »unmittelbaren Zugriff« auf die über Hoeneß gespeicherten Daten gehabt habe, einen Steuerbescheid für Hoeneß dem Magazin »Stern« zugespielt, ein »bestimmter Tatverdächtiger« habe aber nicht ermittelt werden können. Aufgrund eines »Programmfehlers« seien seit März 2013 nicht einmal mehr jene Zugriffe vollständig erfasst worden, bei denen das normalerweise der Fall war. Die wenigen noch verfügbaren Daten seien »ohne jede Aussagekraft« und ließen keinerlei Rückschlüsse auf einen unbefugten Abruf des Hoeneß-Steuerbescheids von Ende 2011 und dessen Weitergabe an die Presse zu. Die Strafverfolger sahen schließlich keine weiteren erfolgversprechenden Ermittlungsansätze und gaben daher auf[31]. Die Reihe der einschlägigen Ereignisse ließe sich beliebig fortsetzen[32].

Der Bundesminister der Finanzen Dr. Schäuble hat eine Erklärung dafür, warum in letzter Zeit Dienstgeheimnisse häufig verraten werden. In einem Interview mit der FAZ vom 07.02.2014 äußert er sich wie folgt:

»FAZ: Im Fall Hoeneß hat die Staatsanwaltschaft eine Hausdurchsuchung beim Finanzamt gemacht.
Schäuble: Nochmals: Das Steuergeheimnis ist in einem Rechtsstaat ein hohes Gut. Gleichzeitig müssen wir in den letzten Jahren feststellen, dass vieles, was früher gehütet wurde, sich auf einmal in der Öffentlichkeit befindet. Das liegt vielleicht an der Technologie, die das erleichtert.«

Verstöße gegen Geheimhaltungspflichten werden kaum aufgeklärt

Genau: Was früher gehütet wurde, befindet sich »auf einmal« in der Öffentlichkeit. Daran ist die Technologie »schuld«, denn diese erleichtert den Verrat von Dienstgeheimnissen. Und diese Einsicht haben nicht nur Bundesminister wie Herr Dr. Schäuble, sondern hoffentlich im Gegensatz zu der Feststellung des BGH zum vermuteten Verhalten der Richter auch zunehmend sie selbst.

Der »bayerische« Fall lässt vermuten, dass es sich hier um den Verlust der Datenkontrolle über die Gruppenrichtlinien im »active directory«[33] der Netzadministration handelt, weil die Zugriffe nicht vollständig protokolliert wurden und man demnach keine Anhaltspunkte für unberechtigte Zugriffe finden konnte. Nicht dafür legitimierte Nutzer haben in solchen Fällen Zugriff auf Daten, die ihnen eigentlich versperrt sein müssten oder aber Daten sind nicht mehr für Berechtigte verfügbar. Zuständigkeitsgrenzen sind dann keine Zugriffsgrenzen mehr. Ursache ist auch die Datenflut in den Netzen, die leider nicht über entsprechende Vorgaben gesteuert wird. Schließlich gehen die Übersicht und damit die Kontrolle verloren. Die »Reparatur« ist äußerst aufwendig, wenn überhaupt möglich.

Ein Beispiel aus der Wirtschaft gibt die Erläuterung von David Lin, Enterprise Sales Manager bei Varonis Systems[34], die naturgemäß eher auf die Funktionsfähigkeit der Unternehmen als auf die Geheimhaltung in Behörden oder Gerichten abstellt, aber recht deutlich den beklagenswerten Zustand des Verlustes der Datenkontrolle beschreibt. Auch in den Wirtschaftsbetrieben wird der Ablauf gestört, wenn nicht mehr geregelt werden kann, wer auf Daten berechtigt zugreift, oder wenn nicht geklärt werden kann, wer auf welche Daten zugegriffen hat.

Eine nämliche Situation, die eine »Rechtebereinigung« erforderlich macht, besteht derzeit im Bereich der HZD, und damit ein Zustand, in dem die Kontrolle über die Daten jedenfalls zum Teil verloren gegangen ist. Ein inkonsistentes Dateisystem führt dazu, dass ein direkter Zugriff auf diejenigen Verzeichnisse, in denen die Rechte nicht gelöscht wurden, nach wie vor möglich ist, wenn man den Verzeichnispfad kennt, der in vielen Fällen leicht zu erraten ist (z. B. \\[servername]\abteilungsablage\gremien\präsidium\). Ein Schutz von Daten vor unberechtigtem Zugriff ist dann kaum noch möglich, die Funktionsfähigkeit von Anwendungen ist gefährdet. Die Richter haben keine Möglichkeit, diese Mängel im allgemeinen Interesse der Rechtsprechung ohne Nachweis einer Verletzung eigener Rechte etwa vor den Verwaltungsgerichten geltend zu machen.

Zugleich hat sich herausgestellt, dass eine Gruppe von Administratoren der HZD – darunter die Mitarbeiter des User Service Center – über Vollzugriffsrechte auf die Abteilungsablagen einzelner Gerichte und Staatsanwaltschaften verfügen.[35] Diese bei der Einrichtung der Abteilungsablagen notwendigen Berechtigungen wurden anschließend bei vielen Dienststellen nicht oder nur unvollständig wieder beseitigt. Administratoren (die Systemadministration ohnehin) der HZD könnten aufgrund dieser Berechtigungen Einsicht in Dokumente auf der Abteilungsablage nehmen und haben damit entgegen den allgemeinen Grundsätzen des Datenschutzes und der IT-Sicherheit aktuell mehr Berechtigungen, als sie zur Erfüllung ihrer Aufgaben benötigen. Über die Abteilungsablagen verschoben zur aktiven Dienstzeit des Autors dieses Beitrags die meisten Richter ihre Beschlussentwürfe etc., um sie den Mitarbeitern der Geschäftsstellen zur Weiterverarbeitung zu übermitteln. Das wird jetzt nicht anders sein, weil weiterhin ein DMS (Dokumentenmanagement-System) fehlt. Diese Arbeitsweise hat es im Übrigen bewirkt, dass von einem Dokument am Ende eine Vielzahl von Versionen in

den verschiedensten Verzeichnissen der Richter und der Geschäftsstellen existierte und nur noch schwer oder gar nicht festgestellt werden konnte, welches der Papierakte entsprach. In der Folge kam es zu peinlichen Verwechselungen, wenn die Parteien Abschriften erhielten, die ganz oder zum Teil einer im Arbeitsprozess verworfenen Version entsprachen und damit Aufschluss über den richterlichen Entscheidungsprozess gegeben haben (Beratungsgeheimnis). Auch dies wird sich zwischenzeitlich nicht gebessert haben. Unter solchen Umständen arbeiten zu müssen führt bei vernünftiger Lageeinschätzung zu »chilling effects«[36] bei den Richtern, jedenfalls bei denen, die von den Wirkungen einer zentralen Vernetzung eine »Anschauung« und damit einen Begriff haben, um ihre Vernunft anwenden zu können. Es sind dies gerade die »besonnenen Richter«, die das Gefühl des »Beobachtetwerdens« entwickeln müssten, und deren Beeinflussung durch dieses Gefühl das BVerfG a. a. O. als Verstoß gegen die richterliche Unabhängigkeit erwähnt, ohne aber dieser Erkenntnis für die eigene Entscheidung Bedeutung beizumessen.

In den vorstehend aufgeführten Fällen liegen die Schwachstellen im Bereich der Netzadministration im Grunde darin begründet, dass man mit möglichst geringem Personaleinsatz ein riesiges, das ganze Land übergreifende System mit unterschiedlichen Domänen (Domains[37]) betreibt, in dem Vertrauensstellungen transitiv eingerichtet werden, um riesige Mengen von Clients verwalten zu können (der Freund meines Freundes ist mein Freund etc...). Aus dem Abschlussbericht »EDV-Netzbetrieb für die dritte Gewalt«, S. 20/21 (siehe Endnote 13) ergibt sich, dass bei der HZD damals lediglich fünf bis sechs Personen die notwendige Befähigung besaßen, ein Netz umfassend zu administrieren. Aber nicht nur die Schwachstellen einer solchen hypertrophen Administration, die auf die Belange der Rechtsprechung keine vernünftige Rücksicht nehmen kann, führt zur Gefährdung des Beratungsgeheimnisses (und zu ständigen Verstößen gegen alle denkbaren einschlägigen Gesetze). Auch die eingesetzte Software und Hardware bietet weder nach innen noch nach außen eine hinreichende Sicherheit vor Übergriffen.

Der Sicherheitsexperte Dr. Sandro Gaycken von der Freien Universität Berlin, Berater der Bundesregierung, hält es derzeit für nicht möglich, sich gegen »starke Angriffe« durch organisierte Kriminelle oder Nachrichtendienste zu schützen. Bei der ersten Anhörung des Bundestagsausschusses für die Digitale Agenda führte er laut einem Beitrag im Blog für Netzpolitik und digitale Agenda im Bundestag auf Fragen der Abgeordneten aus[38]:

> Ein Schutz gegen starke Angriffe ist durch die normale Rechnersicherheit nicht möglich

»Das ›normale‹ Modell der Rechnersicherheit ist diesen Angreifern gegenüber konzeptionell überfordert und überholt«, schrieb er in seiner Stellungnahme zu einem Fragenkatalog des Ausschusses. Gaycken geht davon aus, dass »viele Basistechnologien viele tausend kritische Sicherheitslücken« enthalten. Aktuelle Informationstechnik müsse gegenüber starken Akteuren daher »als zutiefst unsicher bewertet werden«. Gaycken schlägt vor, die aktuelle IT nach den Kriterien des Orange Book des US-Verteidigungsministeriums von 1983 neu zu entwickeln. Nicht verifizierbare Teile wie Hardware müssten unter Hochsicherheitsbedingungen hergestellt werden. Er räumte aber ein, dass eine komplette Erneuerung der Basistechnologie aufwendig und teuer sei.«

In einem Artikel der ZEIT vom 17.01.2013[39] geht Dr. Gaycken darauf ein, wie etwa Nordkorea auf die Bedrohung reagiert und schlägt vor, ein eigenes Betriebssystem zu entwickeln, weil derzeit nur handgeschriebene Zettel sicher seien. DIE ZEIT kommentiert:

»Also doch von Nordkorea lernen und lieber eigene Computer konstruieren, eigene Programme für Regierungen und sensible Einrichtungen schreiben: »Auch bei den Computern der Bundesregierung gibt es inzwischen im Durchschnitt sieben ernste Hackerangriffe pro Tag«, sagt Sandro Gaycken, ein Computerwissenschaftler an der FU Berlin und Exhacker beim Chaos Computer Club, der das Auswärtige Amt berät. Vergleichsweise sicher seien eigentlich bloß handgeschriebene Zettel und Datenverarbeitungssysteme, die ganz auf Hochsicherheit getrimmt sind. Die Letzteren, sagt Gaycken, müsse man aber erst noch erfinden. Er will der Bundesregierung jetzt vorschlagen, genau das zu tun. Auch Deutschland brauche ein eigenes, neues Betriebssystem und neue Programme für sensible Einsätze. »Wir fangen an den Computer noch mal völlig neu zu entwickeln«, kündigt der ehemalige Hacker bereits an. ...

Es bedarf nicht immer »starker Angreifer«[40], wie sie sich etwa in der organisierten Kriminalität sicher vermuten lassen und wie sie bei den Geheimdiensten sicher vorhanden sind. Begabte Pennäler oder Informatiker können in die Systeme eindringen, z.B. wenn – wie es hin und wieder leider vorkommt – die Fa. Microsoft ein update-patch wegen Sicherheitslücken mit genauer Beschreibung des Sicherheitsproblems ankündigt, dieses patch aber erst viel später ausliefert. In der Zwischenzeit sind die Tore weit geöffnet. Zunächst wird aber die Sicherheitslücke erst einmal dem amerikanischen Geheimdienst gemeldet[41], selbstverständlich nur zu dem Zweck, die Systeme der amerikanischen Regierung zuerst zu härten.

In einem Beitrag von Richard M. Stallman vom Februar 2010 ist auch eine verlinkte Beschreibung der »universellen Hintertür« von Microsoft Windows für den NSA enthalten[42].

Würden die Richter des BGH den Serverraum des BGH aufsuchen, würden sie – wenn sie überhaupt Zutritt erhalten – mit großer Sicherheit Netzwerkkomponenten der (US-amerikanischen) Fa. Cisco vorfinden (Hubs, Router, Switches). Die Vernunft gebietet zu unterstellen, dass diese Komponenten von der NSA bei der Ausfuhr für deren Zwecke »angepasst« worden sind. Der stellvertretende Vizepräsident der Fa. Cisco hat sich darüber beklagt, dass die Produkte der Firma bei der Ausfuhr von der NSA manipuliert werden. Man sieht auf den von Reportern aufgenommenen Bildern Mitarbeiter der NSA, wie sie die Pakete öffnen und die Netzwerkkomponenten entnehmen[43].

Der angesehene Technikexperte Steve Blank beschreibt auf seiner Internetseite[44], warum er davon ausgeht, dass die Prozessoren der Fa. Intel und AMD durch Sicher-

heitsupdates der Fa. Microsoft manipuliert worden seien und warum Präsident Putin inzwischen wieder Schreibmaschinen an Stelle von Computern einsetzt.

Im NSA-Untersuchungsausschuss des Bundestages wird erwogen, wieder auf mechanische Schreibmaschinen zurückzugreifen, um geheime Dokumente zu verfassen, wie der Vorsitzende des Untersuchungsausschusses, Patrick Sensburg (CDU), am Montag, 14.07.2014 im ARD-»Morgenmagazin«[45] mitteilte.

Jedenfalls in »die Kutsche« des BVerfG dürfte es inzwischen schon »hinein geregnet« haben: Laut einem Bericht der Legal Tribune Online vom 13.02.2014[46] befürchtete der Präsident des BVerfG, Herr Voßkuhle, auf Grund von Angaben von Herrn Snowden, dass ein solcher Übergriff erfolgt sei, und hatte zunächst erwogen, die Angelegenheit überprüfen zu lassen:

»Ich habe mich aber dagegen entschieden«, sagte er am Mittwochabend in Karlsruhe. Im übrigen sei die Affäre »sehr unappetitlich«. Das BVerfG sei gegen Abhörmaßnahmen gut abgesichert«.

Ist es unvernünftig, auch für die anderen Gerichte Sicherheit zu fordern, weil die Empfindung, die ganze Angelegenheit sei unappetitlich, ebenso berechtigt wäre wie der Wunsch, das richterliche Beratungsgeheimnis auch im EDV-Zeitalter zu wahren? Genügt es, gegen »Abhörmaßnahmen« gesichert zu sein, wenn es um das »Hereinhacken« in das IT-Netz des BVerfG geht?

Ist es vernünftig, in den Gerichten, Behörden, Betrieben der Wirtschaft Privatgeheimnisse, Geschäftsgeheimnisse, Dienstgeheimnisse und letztlich Staatsgeheimnisse mit Systemen zu verwalten, die man nicht kennt, weil man sie nicht kennen kann? Bei sämtlichen Windows-Programmen einschließlich der Betriebssysteme ist der Programm-Quellcode unbekannt, weil er geheimgehalten wird. Durch die Übersetzung (Interpreter, Compiler) des Programmquellcodes in die »Maschinensprache« des Prozessors entsteht eine Folge von Bytes, die sowohl Befehle als auch Daten repräsentieren. Eine »Rückübersetzung« in eine höhere Programmiersprache so, dass über die vorhandenen Algorithmen eine vernünftige und abschließende Aussage gemacht werden kann, ist unmöglich. Wenn also etwa der Präsident des BGH die Richter im Gebrauch der EDV kontrollieren darf (Urteil des BGH, Rn. 27), um Missbräuche zu verhindern oder abzustellen, vertraut er der Fa. Microsoft mehr als den Richtern. Diese kann er kontrollieren, jene aber nicht. Ist das vernünftig?

III. Das Programm der »Netzkläger« ...

Die Beeinträchtigung der richterlichen Unabhängigkeit durch die bloße Eignung einer technischen Einrichtung zur unzulässigen Beobachtung und inhaltlicher Kontrolle richterlicher Tätigkeit muss durch organisatorische, technische und rechtliche Sicherheitsmaßnahmen soweit gemindert werden, dass die Beeinträchtigung rechtsstaatlich noch vertretbar ist. ...
(Revisionsschrift der Netzkläger vom 20.05.2010)

Die Kontrolle des Netzes muss von den Präsidien verantwortet werden

Die »Netzkläger« sehen ihre richterliche Unabhängigkeit dadurch als beeinträchtigt an, dass der Betrieb und die Administration des EDV-Netzes der Hessischen Justiz für den Rechtsprechungsbereich des Oberlandesgerichts Frankfurt am Main bei der Hessischen Zentrale für Datenverarbeitung (HZD), einer Oberbehörde der Landesfinanzverwaltung, und nicht bei den Gerichten, d.h. allein dem Gerichtspräsidium verantwortlichen Personen, angesiedelt ist, und der Justizminister das duldet.

Nach dem Urteil des BGH, Rn. 30, eröffne das EDV-Netz zwar die technische Möglichkeit, dass es zur inhaltlichen Kontrolle richterlicher Dokumente, etwa zur systematischen Suche, Einsichtnahme, Kopie, Bearbeitung und Weiterleitung richterlicher Dokumente, genutzt wird[47]. Diese Möglichkeit bestehe aber unabhängig davon, ob das EDV-Netz durch eine nicht zum Geschäftsbereich des Ministers der Justiz gehörende Behörde wie die HZD oder durch den Minister der Justiz bzw. die Gerichtspräsidenten als unmittelbare Dienstvorgesetzte betrieben und verwaltet werde.

Hätte sich der BGH überlegt, warum, wie von den Netzklägern vorgetragen und unstreitig, der Landesrechnungshof Hessen und der Hessische Landtag jeweils über ein eigenadministriertes, separates EDV-Netz verfügen, dann hätte er den Unterschied verstanden. Zwar können auch dort die Administratoren auf die Daten der Mitglieder des Landtags und derjenigen des Landesrechnungshofs zugreifen und die Arbeitsvorgänge unterliegen da wie dort einer technisch totalen Kontrolle, der Sicherheitsgewinn ist aber enorm. Das Land, das die Notwendigkeit getrennter Netze für den Landtag und den Rechnungshof nicht ohne Grund anerkennt, scheut nur den Aufwand für die Rechtsprechung, obwohl sich aus § 1 Abs. 1 Ziff. 2 i. V. m. § 10 Abs. 1 HDSG ergibt, dass Kostengesichtspunkte keine Rolle spielen dürfen. All dies hat der BGH übersehen, wenn er einen Unterschied bei der »Kontrolleignung« nicht feststellen kann, weil er den Sicherheitsgewinn durch eine transparente Netzadministration im Sinne der Netzkläger nicht verstanden hat. Sie hatten ihr »Programm« in der Revisionsschrift vom 20.05.2010 auf S. 6 nochmals wie folgt zusammengefasst:

»Der Dienstgerichtshof hat es ferner unterlassen, der Frage nachzugehen, ob eine Beeinträchtigung der richterlichen Unabhängigkeit durch die bloße Eignung einer technischen Einrichtung zur unzulässigen Beobachtung und inhaltlicher Kontrolle richterlicher Tätigkeit durch organisatorische, technische und rechtliche Sicherungsmaßnahmen soweit gemindert werden kann, dass die Beeinträchtigung rechtsstaatlich noch vertretbar und von den Antragstellern hinzunehmen ist. Dies ist nach Auffassung der Antragsteller der Fall, setzt aber zwingend voraus, dass der Netzbetrieb einschließlich der Administration, soweit es um die Rechtsprechung geht, den Gerichten überlassen wird. Daher reichen die vom Dienstgerichtshof vorgeschlagenen Sicherungsmaßnahmen in Form von bloßen Verwaltungsvorschriften (BU S. 30) bei weitem nicht dafür aus, die Beeinträchtigung der richterlichen Unabhängigkeit der Antragsteller auf ein rechtsstaatlich noch vertretbares Maß zu mindern.«

Die Bestimmung des Dienstgerichtshofs für Richter bei dem Oberlandesgericht Frankfurt am Main in seinem Berufungsurteil vom 20.04.2010 (DGH 04/08), wonach die Überlassung der Verwaltung des EDV-Netzes der Hessischen Justiz für den Rechtsprechungsbereich an die Hessische Zentrale für Datenverarbeitung (HZD) unzulässig ist, solange nicht die Art der Behandlung von Dokumenten des richterlichen Entscheidungsprozesses durch die HZD für den Rechtspflegebereich durch Verwaltungsvorschriften seitens des Ministeriums der Justiz konkret festgelegt und deren Einhaltung durch den Minister der Justiz im gleichberechtigten Zusammenwirken mit gewählten Vertretern der Richter überprüft werden kann, ist in einem landesweiten zentralen Computernetz überhaupt nicht »im gleichberechtigtem Zusammenwirken« mit gewählten Vertretern der Richter umsetzbar.

Der Hessische Dienstgerichtshof berücksichtigt nicht, dass die im Rechtsprechungsbereich erforderliche Ausstattung der Richterarbeitsplätze und der Kanzleien eine gänzlich andere Administrationsstruktur ermöglicht und erfordert, die, wie vorstehend ausführlich belegt worden ist, in den großen Netzen nicht gewährleistet werden kann. Hier ergänzen sich also technische, datenschutzrechtliche, gerichtsverfassungsrechtliche und verfassungsrechtliche Anforderungen wie etwa die Überlegungen von Bertrams in NWVBl. 2007, 205 (211):

»*… kommt als verfassungsrechtlich unbedenklich allein eine Lösung in Betracht, bei der für den Bereich der Dritten Gewalt ein eigenes, organisatorisch getrenntes Rechenzentrum eingerichtet wird*«.

Die Befürchtungen des Datenschutzbeauftragten sind weit übertroffen worden

Der frühere hessische Datenschutzbeauftragte Prof. von Zezschwitz, hatte in einem Vortrag in der Evangelischen Akademie Arnoldshain im November 2001 der hessischen Richterschaft dringend angeraten, gegen die Anbindung der Richterarbeitsplätze an ein zentrales Landesnetz zu kämpfen und dazu beizutragen, dass allenfalls auf der Ebene der Landgerichte eine Vernetzung erfolgen solle. Als Grund gab Herr Prof. von Zezschwitz die Gefahren an, die von der Anbindung der Richterarbeitsplätze an ein zentrales Landesnetz für die richterliche Unabhängigkeit ausgingen. Alle Befürchtungen des früheren Datenschutzbeauftragten haben sich leider nicht nur bestätigt, sondern sind in unvorstellbarem Ausmaß negativ übertroffen worden.

Durch die neuerlichen Erkenntnisse des Umfangs krimineller Zugriffe auf gesicherte Netze großer Unternehmen oder die Möglichkeiten von Insidern, unbefugt an Daten zu gelangen (und etwa in Form von Steuer-CDs) gewinnbringend zu veräußern oder wie im Falle von Edward Snowden, den amerikanischen Geheimdienst NSA (der über bessere Möglichkeiten als die HZD verfügen dürfte) weitgehend »auszuräumen«, werden diese Befürchtungen zur einer Realität, der sich auch die Rechtsprechung des BGH nicht einfach verweigern kann. Als technische Lösung wird nunmehr exakt diejenige von berufener Stelle vorgeschlagen, die nach Meinung der Netzkläger eine Beeinträchtigung der richterlichen Unabhängigkeit auf ein rechtsstaatlich noch vertretbares Maß mindert.

Die Landesregierung, die es im Falle etwa des Landesrechnungshofs für geboten hält, aus Gründen der besseren Absicherung ein gesondertes Netz zur Verfügung zu stellen, hat aber durch den früheren Staatssekretär Lemke den Vorwurf paranoiden Verhaltens gegen die Richter erhoben (siehe Endnote 1). Der damalige Justizminister hat mit seiner Antwort auf die Kleine Anfrage des Abgeordneten. Dr. Andreas Jürgens (BÜNDNIS 90/DIE GRÜNEN) vom 21.07.2005 betreffend Datenschutz und richterliche Unabhän-

Anmerkungen

1 HR3 – defakto vom 19.06.2005, (275 MB!)
http://www.hefax.de/khh/Anlagen/BigBrother.mpg.

2 Urteil des Hessischen Dienstgerichtshofs für Richter bei dem Oberlandesgericht Frankfurt am Main vom 20.04.2010 – DGH 4/8
http://www.hefax.de/khh/Anlagen/DGH4_08.pdf.

3 Besprechung von Schwamb, NRV-Info Hessen, Heft 6/2010, S. 24 ff
http://www.hefax.de/khh/Anlagen/HES-2008-07_info.pdf

4 NJW-aktuell Heft 17/2013, S. 14
http://www.hefax.de/khh/Anlagen/NJW-aktuell_Heft17.pdf.

5 Vernunft in der Bedeutung als dem gegenüber dem Verstand höheren Erkenntnisprinzip, der Fähigkeit, aus dem Erkannten Schlüsse zu ziehen, die Frage nach den Gründen.

6 Das Hessische Ministerium der Justiz hat zeitgleich mit der Einführung des landesweiten Computernetz das mit eigenen und Drittmitteln errichtete, selbstadministrierte Netz der Richter der Familiensenate des OLG Ffm gegen deren Willen »stillgelegt«.

7 Die technische Kontrolle des Arbeitsvorgangs selbst erwähnt der BGH nicht.

8 Zudem verboten! K. F. Piorreck, Referat – »Aufgaben der Richtervertretungen Modernisierungsprozess«
http://www.hefax.de/khh/Anlagen/Piorreck_Oberaula.pdf

9 Karlheinz Held, Vernetzung – Das Ende des Industriezeitalters, Betrifft JUSTIZ, (Nr. 70), S. 300,
http://www.hefax.de/khh/Anlagen/bj200206.pdf

10 Kant: AA III, Kritik der reinen Vernunft, S. 108.

11 Es wären auch andere technische Lösungen möglich: Dezentralisierung durch autonome Teil-/Gerichtsnetze – also nicht von oben nach unten eingreifen sondern von unten nach oben abgeben, oder Lösungen und Schutzmechanismen, wie sie von Raubkopierern und »Illegalen« auf ihrer Flucht vor der Obrigkeit und Copyright-Inhabern ohne großen Aufwand eingesetzt werden. Zu teuer?

12 Dr. Michael Bertrams, Präsident des VGH NRW und des OVG NRW, »Zentralisierung der Informationstechnik in der Landesverwaltung NRW unter Einbeziehung der Dritten Gewalt?« VBl. 6/2007 Nordrhein-Westfälische Verwaltungsblätter
http://www.hefax.de/khh/Anlagen/Bertrams01.pdf

und Zentralisierung der IT-Orga-nisation unter der Aufsicht des Finanzministers,
Unabhängigkeit der Dritten Gewalt in Gefahr: Interview mit PrVerfGH und PrOVG NRW Dr. Michael Bertrams, Münster, nrv-magazin | schleswig-holstein 3 | 2011, S. 14
http://www.hefax.de/khh/Anlagen/Bertrams02.pdf

13 Gemeinsame Arbeitsgruppe aus Mitgliedern der Bezirksrichterräte der ordentlichen Gerichtsbarkeit, der Verwaltungsgerichtsbarkeit, der Arbeitsgerichtsbarkeit und der Sozialgerichtsbarkeit, des Richterrats des Hessischen Finanzgerichts, des Bezirksstaatsanwaltsrats und des Hauptpersonalrats bei dem Hessischen Ministerium der Justiz, der Stabsstelle e-government bei dem Hessischen Ministerium des Innern, dem Hessischen Datenschutzbeauftragten und dem Hessischen Ministerium der Justiz
http://www.hefax.de/khh/Anlagen/Abschlussbericht.pdf

14 Datenschutz in der Justiz
http://www.hefax.de/khh/Anlagen/DatenschutzinderJustiz.pdf

15 Diese Auffassung des Datenschutzbeauftragten wird in dem Kommissionsbericht an mehreren Stellen wiedergegeben, etwa auf S. 46.

gigkeit abgestritten, dass diese Äußerung gefallen sei[48], obwohl die entsprechende Behauptung im Hessischen Fernsehen in der Sendung defakto vom 19.06.2005 aufgestellt worden ist (Endnote 1), was man sich heute noch durch Click auf den Link ansehen und anhören kann. Wo die Argumente fehlen, wird die Wahrheit verdreht. Wer die Antworten des damaligen Justizministers mit den wahren Fakten, wie sie vorstehend beschrieben und belegt worden sind, vergleicht, erkennt den großen Unterschied zwischen den politischen Behauptungen und der mehr als bescheidenen Realität. Darüber hat der Minister das Parlament nicht zutreffend unterrichtet. Warum?

Gaycken: Man kann sicher mehr tun, und bisher ist das Vorgehen sehr unentschlossen. Das Bundesamt für Sicherheit in der Informationstechnik hat zum Beispiel damit begonnen, eigene Betriebssysteme zu entwickeln, weil man sagt: Das ganze kommerzielle Zeug kann man nicht gebrauchen, das ist sehr unsicher. Das begrüße ich.
ZEIT: Wir brauchen ein Bundes-Windows?
Gaycken: Die andere plausible Lösung ist die Trennung bestimmter Netze …

Entnetzung statt Vernetzung

Das ist das Schlagwort in der Diskussion um mehr Sicherheit für Computersysteme gegen Angriffe von innen und von außen[49]. Gerade die in letzter Zeit ans Licht kommenden Vorfälle, über die täglich in den Medien berichtet wird, zeigen, dass das Programm der Netzkläger nicht nur rechtlich, sondern auch technisch geboten ist, um die Funktionsfähigkeit der Rechtsprechung zu sichern und zu erhalten, und dass die derzeitige Vernetzung der Richterarbeitsplätze deren Unabhängigkeit in Frage stellt.

> Die plausible Lösung
> ist nur die Trennung
> bestimmter Netze

Das Programm der Netzkläger ist in rechtlicher und technischer Hinsicht heute aktueller und notwendiger denn je und hat durch die aktuelle Entwicklung in jeder Beziehung Gewicht gewonnen. Jetzt geht es zunächst darum, die Entscheidung des Hessischen Dienstgerichtshofs für Richter bei dem Oberlandesgericht Frankfurt am Main vom 20. April 2010 – DGH 4/8 – umzusetzen. Davon kann bisher keine Rede sein.

Der Abgeordnete der Grünen im Hessischen Landtag, Dr. Andreas Jürgens, hat die wichtigsten Gründe in der Landtagsdebatte vom 03.12.2011 über die Errichtung der Informationstechnik-Stelle der Hessischen Justiz und Regelung justizorganisatorischer Angelegenheiten sowie Änderung von Rechtsvorschriften zusammengefasst[50]. Er zitiert zunächst den Tenor des Urteils des Hessischen DGH und führt dann weiter aus:

»In dem vorliegenden Gesetzentwurf hat allerdings die Landesregierung – besser gesagt: der Justizminister – wieder einmal nicht beachtet, dass die Justiz keine Behörde wie jede andere ist, sondern – das gilt zumindest bezogen auf die Gerichte – die dritte Gewalt im Staat. Nach der Rechtsprechung des Bundesverfassungsgerichts gilt aber die Gewaltenteilung auch für den jeweiligen Verwaltungsunterbau. Bisher wurde dieses Trennungsgebot eingehalten, weil bisher die Gemeinsame IT-Stelle, abgekürzt GIT, eine eigenständige, von der Justiz selbst getragene Behörde war, genauer gesagt: von den jeweiligen Gerichtspräsidenten getragen. Jetzt soll die GIT eine eigenständige Landesoberbehörde unter Aufsicht des Justizministers werden, in der Verantwortungen also von der dritten zur zweiten Gewalt hinüber wandern. Frau Hofmann hat es schon gesagt: In der Anhörung wurden erhebliche Zweifel geäußert, ob diese Konstruktion tatsächlich mit der Gewaltenteilung noch vereinbar ist. Zwar ist eine IT-Kontrollkommission vorgesehen, aber auch die kann diese Zweifel eigentlich nicht beseitigen. Denn dort sind zwar Vertreter der jeweiligen Richterräte vorgesehen, doch

16 Spatscheck, AnwBl 2012, 478–482
http://www.hefax.de/khh/Anlagen/Anwaltsblatt.pdf

7 Google und Konsorten sollen zu Gehilfen des Anwalts erklärt werden!

18 Kintzi, DRiZ 2007, 245, m. w. N.

19 RA Oliver Klein, Anwalt24.de: Arbeitsgericht Düsseldorf, Urteil vom 29.06.2007, Az. 1 Ca 3212/07
http://www.anwalt24.de/beitraege-news/fachartikel/weitergabe-von-passwort-recht-fertigt-fristlose-kuendigung

20 Noch mit Schriftsatz vom 11.03.2010, S. 4, im Verfahren vor dem BGH hat das Land eine Aufklärung ausdrücklich verweigert.

21 http://www.datenschutz.hessen.de/taetig-keitsberichte.htm

22 Der Sachverhalt wird bis heute auch auf Nachfrage nicht näher erklärt. Der »Vertragsbruch« bleibt im Dunkeln. Vermutlich handelt es sich bei den »externen Dienstleistern« um in den sogenannten Vergabeskandal der HZD verwickelte Unternehmen (HZD-Vergabeskandal http://www.hefax.de/khh/Anlagen/Vergabeskandal.pdf), vielleicht die Fa. Götzfried AG, in deren Aufsichtsrat als stellvertretender Vorsitzender der ehemalige Justizminister Dr. Wagner nach seinem Ausscheiden aus dem HMdJ 2005 umgehend eingetreten ist. Dort könnte er jetzt als Abgeordneter die Funktionen ausüben, die er als Justizminister nicht übernehmen wollte: die Kontrolle des Justiznetzes.

23 Die HZD war von 1977 bis 2003 im HMdI resortiert.

24 Siehe Endnote 12.

25 Der Präsident des Bundesamtes für die Sicherheit in der Informationstechnik bei der Anhörung durch den Bundestagsausschuss »Digitale Agenda« im Mai 2014
http://www.hefax.de/khh/Anlagen/ITAnhoerungBundestag.pdf

26 Ein Kollege formuliert folgenden Vergleich: die Richter nehmen von der nächsten Sintflut erst Notiz, wenn sie ihnen über den Aktenbock schwappt.

27 Die Justizverwaltung hat im Jahr 2000, als das Amtsgericht Wiesbaden an das EDV-Netz angeschlossen wurde, dafür Sorge getragen, dass der Ermittlungsrichter so lange nicht angeschlossen wird, als er die Akten des Ermittlungsverfahrens in der CDU-Parteispendenaffäre für den Untersuchungsausschuss des Landtages zu überprüfen hatte.

28 Die in den Vergabeskandal verwickelten Firmen waren noch als externe Dienstleister tätig, als die Landesregierung den Skandal 2011 einräumen musste, Frankfurter_Rundschau_ Pannen_als_Regelfall.pdf
http://www.hefax.de/khh/Frankfurter_Rundschau_ Pannen_als_Regelfall.pdf

29 Frankfurter Rundschau_Ermittlungen_gegen_Wulff-Ermittler
http://www.hefax.de/khh/Anlagen/FrankfurterRundschau ErmittlungengegenWulff-Ermittler.pdf

30 FAZ vom 08.05.2014, Sechsmal Edathy.

31 Süddeutsche Zeitung vom 25.08.2014
http://www.hefax.de/khh/Anlagen/Ermittlungen.pdf

32 Vgl. Schwamb »Was ist eigentlich e²A?« NRV-Info Hessen 2014, 13 (14), zur Frage von Ermittlungen des Generalbundesanwaltes mit einer elektronischen Akte in Sachen des Handys von Bundeskanzlerin Merkel. NRV Hessen-Info 2014
http://www.hefax.de/khh/Anlagen/swm201407.pdf

die IT-Kontrollkommission hat lediglich die Aufgabe, an Überprüfungen zum Schutz vor unbefugten Zugriffen durch Mitarbeiterinnen und Mitarbeiter der HZD mitzuwirken. Es geht also sozusagen um Einzelfallüberprüfungen. Die entscheidenden Fragen, etwa des Datenschutzes, der Gestaltung der Datenverarbeitung, der Zugriffsmöglichkeiten und der allgemeinen Vorkehrungen gegen Missbrauch sind gerade nicht Aufgaben der IT-Kontrollkommissionen. Deswegen kann ihre Errichtung auch die verfassungsrechtlichen Bedenken nicht beseitigen.«
(Beifall)
»Jetzt legen Sie uns nach dieser Entscheidung hier einen Gesetzentwurf vor, in dem solche Sicherungsmaßnahmen, die der Dienstgerichtshof im Einzelnen beschrieben hat, nicht einmal erwähnt, geschweige denn geregelt sind. Die bisherige GIT war auf Grundlage von Verwaltungsvorschriften errichtet worden. Deshalb sah der Dienstgerichtshof auch die Regelung von Verwaltungsvorschriften als ausreichend für die Datensicherung. Wenn Sie jetzt eine gesetzliche Grundlage schaffen, ist es nahe liegend, diese Dinge ins Gesetz hineinzuschreiben.«
»Deswegen trägt Ihr Gesetzentwurf den Makel des offensichtlichen Rechtsverstoßes, weil er den Vorgaben des Dienstgerichtshofs nicht entspricht.«

Das rechtskräftige Urteil des Hessischen Dienstgerichtshofs harrt noch seiner Umsetzung

Aus § 3 Abs. 1 i. V. m. § 2 S. 2, 3 des Gesetzes zur Errichtung der Informationstechnik-Stelle der Hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten[51] ergibt sich schon nach dem Wortlaut, dass die Daten der Richterschaft nicht in die Kompetenz der IT-Kontrollkommission fallen, sondern ausdrücklich davon ausgenommen sind, so dass schon deswegen das rechtskräftige Urteil des Hessischen Dienstgerichtshofs noch seiner Umsetzung harrt. Dies hat der Abgeordnete Dr. Jürgens nicht erwähnt, wohl übersehen. Die Richter des Bundesverfassungsgerichts aber haben bei der Vorbereitung ihrer Entscheidung vom 17.01.2013 dieses Gesetz offensichtlich nicht gründlich genug gelesen, sonst wäre aufgefallen, dass die richterlichen Daten überhaupt nicht erfasst werden. Sie hätten allein deswegen nicht ausführen können, die Umsetzung der vom Hessischen Dienstgerichtshof formulierten Bedingungen für den Betrieb des EDV-Netzes der Hessischen Justiz durch die Hessische Zentrale für Datenverarbeitung seien nach Erhebung der Verfassungsbeschwerde durch das Gesetz zur Errichtung der Informationstechnik-Stelle der hessischen Justiz (IT-Stelle) und zur Regelung justizorganisatorischer Angelegenheiten vom 16.12.2011 – JITStG HE – (GVBl I S. 778) erfolgt. »Besonnene Richter« (BVerfG a. a. O.) können eigentlich nicht davon ausgehen, dass das Urteil des Hessischen Dienstgerichtshofs umgesetzt worden ist. Es geht jetzt darum, was von Seiten der Richterschaft daraus folgen muss. Wie gehen »besonnene Richter« mit dieser Aufgabe vernünftig um? ■

33 Aktive Directory – Wikipedia
http://www.hefax.de/khh/Anlagen/ActiveDirectoryWikipedia.pdf
34 Vom Chaos zur Ordnung
http://www.hefax.de/khh/Anlagen/Kinderzimmer-1.pdf
35 Administratorenzugriff auf die Abteilungsablagen http://www.hefax.de/khh/Anlagen/Sicherheitswarnung.pdf
36 Simon Assion, Telemedikus, Recht der Informationsgesellschaft -Was-sagt-die-Rechtsprechung-zu-Chilling-Effects?
http://www.hefax.de/khh/Anlagen/Telemedicus.pdf
37 Eine Verwaltungsstruktur von Windows-Netzwerken.
38 Expertenanhörung im Bundestagsausschuss »Digitale Agenda«
http://www.hefax.de/khh/Anlagen/Bundestag_digital_de.pdf
39 Die Zeit vom 17.01.2013
http://www.hefax.de/khh/Anlagen/LoecherimNetz.pdf
40 Etwa »externe Dienstleister« mit und ohne Masterpasswort brauchen sich nicht anzustrengen, um an Daten zu gelangen, die sie interessieren.
41 Golem.de – Richard Stallman Microsoft verrät Windows-Bugs zuerst der NSA
http://www.hefax.de/khh/Anlagen/Golem.de -RichardStallman_MicrosoftverrätWindows-Bugszuerstder-NSA.pdf
42 Hintertür in Windows für den NSA?
http://www.hefax.de/khh/Anlagen/Golem.de_hatderN-SAeineHintertuer.pdf
43 NSA-Skandal-Cisco-beschwert-sich-ueber-manipulierte-Postsendungen
http://www.hefax.de/khh/Anlagen/NSA-Skandal_Cisco_beschwert_sich_ueber_manipulierte_Postsen-dungen_heise online.pdf
44 Your-computer-may-already-be-hacked-nsa-inside/
http://www.hefax.de/khh/Anlagen/NSA_Inside_Steve_Blank.pdf
45 Spiegel Online vom 14.07.2014 – Angst vor Ausspähung NSA-Ausschuss erwägt Einsatz von Schreibmaschinen (http://www.hefax.de/khh/Anlagen/Schreibmaschinen.pdf).
46 BVerfG befürchtete NSA-Spähaktion http://www.hefax.de/khh/Anlagen/BVerfG_befürchtete_NSA-Spähaktion.pdf.
47 Wobei diese Eignung nur »nach den Feststellungen des Dienstgerichtshofs« bestehen soll!
48 Kleine Anfrage der Grünen im Hessischen Landtag
http://www.hefax.de/khh/Anlagen/anfragegruene.pdf
49 Gaycken/Karger: IT-Sicherheit, Multimedia und Recht (MMR) 1/2011, S. 3 ff
http://www.he-fax.de/khh/Anlagen/Entnetzung_Gaycken_Karger_MMR_2011.pdf ;
Sandro Gaycken, Keiner redet über diesen Krieg Zeit-Online Ausgabe 18/2012,
http://www.hefax.de/khh/Anlagen/Sandro_Gaycken_Keiner_redet_ueber_diesen_Krieg_ZEIT_ONLINE.pdf
50 Beitrag des Abgeordneten Andreas Jürgens in der Landtagsdebatte vom 03.12.2011
http://www.hefax.de/khh/Anlagen/AbgDr.Juergens.pdf
51 IT-Stellen-Gesetz vom 16.12.2011, Gesetz und Verordnungsblatt für das Land Hessen Teil I Nr. 26, vom 23.12.2011
http://www.hefax.de/khh/Anlagen/IT-Stellen-G.pdf