Datenschutz in der Justiz

PC-Vernetzung, Administration durch Fremdfirmen, gerichtlicher Datenschutz – Antworten des hessischen Datenschutzbeauftragten

von Friedrich von Zezschwitz

I. Grundnorm: HDSG

Maßgebend für die datenschutzrechtlichen Pflichten ist das hessische Datenschutzgesetz, im Rahmen verfassungskonformer Eingrenzungen ergänzend das Grundrecht auf informationelle Selbstbestimmung. Das HDSG legt die folgenden Grundsätze für die Richterschaft fest:

– Die materiell-rechtliche Geltung des HDSG für alle richterlichen Handlungen, einschließlich der Entscheidungsfindung und der vorausgehenden Schritte (§ Abs. 1 Satz 1 HDSG).

– Die Einrichtung eines – weisungsfreien – gerichtlichen Datenschutzbeauftragten zur gerichtsinternen Sicherstellung des Datenschutzes (§ 5 Abs. 1 HDSG). Ihm stehen allerdings keine Befugnisse zu, die die richterliche Unabhängigkeit einschränken können (Art. 97 Abs. 1 GG). Im Grundsatz ist das HDSG zu vollziehen, verfassungsrechtliche Einwendungen unterliegen dem Verwerfungsmonopol des Bundesverfassungsgerichts.

– Die Beschränkung der Kontrollbefugnisse des HDSB auf Tätigkeiten, die außerhalb richterlicher Unabhängigkeit liegen (§ 24 Abs. 1 Satz 3 HDSG).

Abweichungen vom allgemeinen Datenschutzrecht

Divergenzen gegenüber den allgemeinen datenschutzrechtlichen Pflichten ergeben sich für Richter vor allem aus:

– der institutionellen Garantie richterlicher Unabhängigkeit,
– den verfahrensrechtlichen Regelungen der Prozessordnungen, insbesondere den dort begründeten Übermittlungs- und Benachrichtigungspflichten,
– bundesrechtlichen Sondervorschriften der Strafprozessordnung und des Strafvollzugsgesetzes, des HGB (Handelsregister), der Insolvenzordnung (Veröffentlichung), des BGB (Vereins- und Güterrechtsregister).

II. Einzelne Problembereiche:

1. Arbeit am PC – Dienstausübung ohne Grundrechtsschutz

Richterliche Tätigkeiten am PC oder im gerichtseigenen Netz (Serverbetrieb) erfolgen in Dienstausübung und unterstehen daher keinen grundrechtlichen Beschränkungen. Richterliche Unabhängigkeit stellt keine Individualrechtsgewährleistung dar, so dass keine persönlichen informationellen Abwehrrechte daraus herzuleiten sind. Die dienstlich bedingten Zugriffsrechte der einzelnen Richter sind vom Präsidium bzw. Vorsitzenden Richter des Spruchkörpers genau und vorab festzulegen. Die Einrichtung der Zugriffsrechte erfolgt durch die Administratoren nach den Vorgaben des Präsidiums. Eigenständige Zugriffsrechte der Geschäftsstellen, des Präsidenten/Direktors oder des Pressesprechers dürfen nicht vorgesehen werden, soweit richterliche Tätigkeiten von sonstigen ununterschieden gespeichert sind.

Quelle unbekannt

2. Technische Sicherheitsmaßnahmen

Der richterliche Arbeitsplatz ist durch technische Sicherheitsmaßnahmen gegen unberechtigte Zugriffe zu sichern (§ 10 HDSG). Einzelarbeitsplätze, die am gerichtlichen Netz hängen, müssen nicht nur gegen externe, sondern auch gegen unberechtigte interne Zugriffe geschützt werden, da erfahrungsgemäß ca. 80% der unberechtigten Zugriffe von innen kommen. Dies kann mit Firewalls am Arbeitsplatz, Intrusion Detection Systemen oder vergleichbaren Maßnahmen erreicht werden. Passwortschutz allein reicht nicht aus.

Der Rechtsgrund für die Sicherheitsmaßnahmen liegt im Amtsgeheimnis (§§ 203, 353b StGB) und im Datengeheimnis (§ 9 HDSG). Geschützt ist das Vertrauen in das amtliche Stillschweigen.

3. Vorabkontrolle

Da die Arbeit am PC oder Server „automatisierte" Datenverarbeitung (Definition: § 3 Abs. 2 BDSG, enger § 2 Abs. 6 HDSG) darstellt, sind Vorabkontrollen durchzuführen und Verfahrensverzeichnisse zu erstellen (§§ 6, 7 Abs. 6 HSDG). In die Verfahrensverzeichnisse kann jedermann einsehen. Die bisherige Regelung in § 6 Abs. 2 Satz 2 Ziff. 2 HDSG wird durch § 491 Abs. 2 StPO überlagert.

4. Zuständigkeits- sind Zugriffsgrenzen

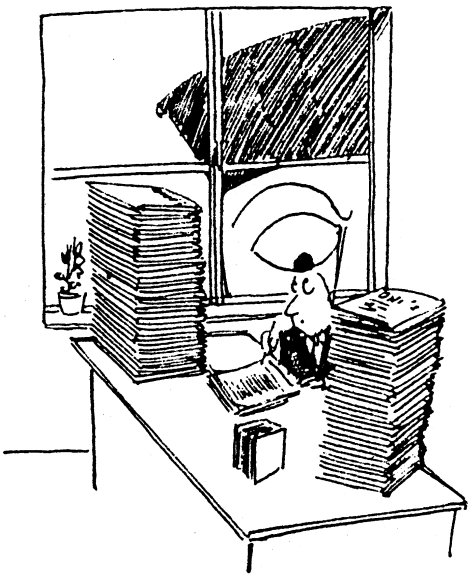
Zuständigkeitsübergreifende Zugriffe (bspw. des leitenden Richters oder des Dienstherrn) auf den Arbeitsplatz sind unzulässig. Nicht ausgeschlossen sind Zugriffe im Vertretungsfall, da der Vertreter den Richter uneingeschränkt ersetzt (zum Zugriff auf Entwürfe vgl. unten Ziff. 10). Ist der Vorsitzende des Spruchkörpers Vertreter, so steht auch ihm das Zugriffsrecht zu.

5. Dienstordnungs- und strafverfolgende Zugriffe
Zugriffsbefugnisse im Zuge von Ermittlungen gegen den Richter bestehen nur in Disziplinarverfahren oder zur Strafverfolgung (bspw. Vorwurf der Rechtsbeugung, Bestechlichkeit). Insofern gilt das Gleiche wie bei Papierakten. Problematisch ist, ob § 22a HDO auch gegenüber diesbezüglichen Speicherungen im richterlichen PC gilt. Soweit ein förmliches Verfahren eröffnet oder Vorermittlungen für die Verfügung eines Verweises angeordnet sind, sieht das HRiG keine Abweichung vom allgemeinen Dienstordnungsrecht vor. Sofern nicht besondere Gründe vorliegen, die dafür sprechen, dass der Zugriff auf Daten die richterliche Unabhängigkeit in Frage stellen kann und soll, ist § 22a auch bei richterlichen PC-Arbeitsplätzen anzuwenden.

6. Administration
Die alltäglichen Fehler am PC (Abstürze, Programmmängel, Zugriffsverweigerung, Passwortirrtümer) zwingen zur Vorhaltung einer professionellen Administration der PC oder der Server. Die Administration sollte weder durch staatliche Fernwartungsanbieter noch durch außenstehende Firmen erfolgen, da deren Verhalten im Netz nur schwer kontrollierbar ist (vgl. HDSB-Mustervertrag Fernwartung, unter www.datenschutz.hessen.de/Musterverträge). Es ist dringend zu empfehlen, dass gerichtsinterne Administratoren durch Dienstanweisung auf unerlässliche Datenzugriffe beschränkt und – ergänzend zu § 9 HDSG – zu besonderer Geheimhaltung verpflichtet werden.

7. Gerichtliche Datenschutzbeauftragte
Der – weisungsunabhängige und zur Geheimhaltung verpflichtete – gerichtliche Datenschutzbeauftragte muss ungeachtet der Schranken aus Art. 97 GG überall dort auf Erfüllung der datenschutzrechtlichen Pflichten durch die Richterschaft dringen, wo eine verfassungskonforme Reduktion den Auslegungsspielraum überschreiten würde. Das gilt insbesondere für die Prüfung, ob die institutionellen datenschutzrechtlichen Sicherungen auf den Richter-PC und Arbeitsplätzen eingehalten sind.

8. Elektronische Kommunikation innerhalb der Gerichte
Der Umfang elektronischer Kommunikation innerhalb der Gerichte hängt vom Willen der Teilnehmenden ab und stellt deswegen keine Gefahr für die richterliche Unabhängigkeit dar. Die Grenze liegt daher im Datenschutz: Soweit personenbezogene Daten Parteien/Beteiligter weitergegeben werden, handelt es sich um eine Übermittlung, die aufgrund



Zeichnung: Philipp Heinisch

des prozessualen Verfahrensrechts legitimiert ist und damit im Rahmen der Zweckbestimmung liegt. Diese darf nur ausnahmsweise durchbrochen werden (§§ 13 II, 12 II HDSG). Regelmäßig darf innerhalb des Spruchkörpers und des Instanzenzuges übermittelt werden. Eine „Beiziehung“ zu anderen Verfahren muss über die jeweiligen Verfahrensordnungen oder § 12 II HDSG legitimiert werden.

Neben der technischen Absicherung des richterlichen Arbeitsplatzes muss auch die Kommunikation und der Datenaustausch unter Richtern und deren Hilfskräften sicher (verschlüsselt) ablaufen. Neue Betriebssysteme wie zum Beispiel Windows 2000 bieten die dazu nötigen Funktionen.

9. Elektronische Kommunikation mit Außenstehenden
Elektronische Kommunikation mit Parteien/Beteiligten/Angeklagten setzt deren ausdrückliche Zustimmung voraus. Sie wird durch die Angabe einer E-mail-Adresse nicht erteilt. Zugangsfragen werden derzeit beraten. Alle Datenschützer fordern, auch hier die 3-Tagesfrist gelten zu lassen. Die Kommunikation bedarf aus datenschutzrechtlichen Gründen der Verschlüsselung. Außerdem ist bei verfahrensbestimmenden Verfügungen und Entscheidungen mit einer qualifizierten elektronischen Signatur (ggf. mit Anbieterakkreditierung) zu arbeiten. Einfacher ist allerdings die nachfolgende Versendung in Papierform.

10. Speicherungen vor Verkündung
Speicherungen vor Verkündung der Entscheidung berühren neben datenschutzrechtlichen Fragen auch die richterliche Unabhängigkeit. Eine Einsichtnahme durch Dritte erlaubt diesen möglicherweise, den Entscheidungsprozess nachzuvollziehen und ggf. anders zu beeinflussen, als das ohne die so erlangte Kenntnis stattfände.
Der Zugriff des Vertreters auf vorbereitende Überlegungen setzt die Einwilligung des eigentlich Zuständigen voraus, denn der Vertreter entscheidet aus eigener Beurteilung; im Übrigen kann er zugreifen.

11. Speicherungen nach Rechtskraft
Speicherungen nach Rechtskraft der Entscheidung berühren nur noch Datenschutz. Da gerichtliche Entscheidungen das Zivil- oder Verwaltungsrechtsverhältnis bestimmen, zuweilen sogar gestalten, sind sie zu dokumentieren. Das Gleiche gilt für Strafakten, deren lebensgestaltende Wirkung über den Tag der Entscheidung hinausreicht; auch sie sind zu dokumentieren. Aufbewahrungsort kann die traditionelle Papierakte oder ein grundsätzlich gleichwertiges elektronisches Aktenverwaltungssystem sein. Zugang zu dieser Dokumentation ist den Verfahrensbeteiligten zu gewähren und staatlichen Instanzen, denen eine Zugriffsbefugnis gesetzlich eingeräumt worden ist.

Ist die Administration des EDV-Netzwerks durch eine privatrechtliche Firma zulässig? Wie ist der Schutz richterlicher Tätigkeitsergebnisse zu erreichen? – Eine Beschwerde an den Hessischen Datenschutzbeauftragten.

Aufgrund der Informationen, die ich aus der vom Hessischen Ministerium der Justiz (HMdJ) herausgegebenen Broschüre „Modernisierung der hessischen Justiz. Informationen zum EDV-Netzwerk“ (Stand Juni 2001) und den teilweise widersprüchlichen öffentlichen Verlautbarungen des HMdJ zu diesem Thema gewinnen konnte, möchte ich Sie auf folgende Bedenken aufmerksam machen, die in erster Linie die Einbeziehung des richterlichen Arbeitsplatzes in das allgemeine Netz betreffen:

1. Nach den Informationen des hessischen Justizministeriums soll die Fernwartung durch die HZD erfolgen. Es existiert ein Kabinettsbeschluss, nach welchem die HZD alsbald in eine Gesellschaft privaten Rechts umgewandelt werden soll. Dies ist meines Erachtens nicht mit der von Ihnen vertretenen Auffassung in Ihrer Stellungnahme „Datenschutz in der Justiz“ vom 20.11.2001 zu vereinbaren, in der Sie ausführen:
„Die Administration sollte weder durch staatliche Fernwartung noch durch außenstehende Firmen erfolgen, da deren Verhalten in Netz nur schwer kontrollierbar ist.“
Verstößt die vom HMdJ geplante Fernwartung unter diesen Umständen nicht gegen § 4 HDSG?

2. In Ihrer Stellungnahme vom 20.11.2001 führen Sie weiter aus:
„Der richterliche Arbeitsplatz ist durch technische Sicherheitsmaßnahmen gegen unberechtigte Zugriffe zu sichern.“
Nach den bekannt gewordenen Plänen des HMdJ können demgegenüber unbekannte Administratoren auf die persönliche Ablage der Richter zugreifen, ohne dass dies durch die Richter festgestellt werden kann.
Diesen von der Verwaltung inzwischen nicht mehr bestrittenen Sachverhalt halte ich nicht für hinnehmbar.

3. Nach den Informationen des HMdJ besteht weiterhin die Absicht, sämtliche Dokumente, die in einer Abteilung erstellt werden, unabhängig von der Zuständigkeit abzuspeichern. Meines Erachtens sind solche Gerichtsablagen auch in den bereits bestehenden Netzen so eingerichtet worden. Meines Erachtens dürfen solche eigenständige Zugriffsrechte der Geschäftsstelle und der Justizverwaltung nicht vorgesehen werden, soweit richterliche Tätigkeitsergebnisse gespeichert werden (u.a. Voten, Vermerke über Beratungsergebnisse, Entscheidungsentwürfe usw.). Anderenfalls besteht die Möglichkeit, dass die Dienstaufsicht in den Bereich richterlicher Entscheidungsfindung eindringt und sich durch technische Einrichtungen die Möglichkeit verschafft, die richterliche Arbeit in ihrem Kernbereich zu beobachten und zu kontrollieren. Dies ist in jedem Fall unzulässig und gesetzwidrig (Art. 97 Abs. 1 GG, § 26 Abs. 1 DRiG; ebenso: Piorreck, Aufgaben der Richtervertretungen im Modernisierungsprozess, in: Betrifft JUSTIZ, 2001, S. 218 <221>).

4. Neben der technischen Absicherung des richterlichen Arbeitsplatzes muss, wie Sie in Ihrer Stellungnahme vom 20.11.2001 ausführen, auch die Kommunikation und der Datenaustausch unter Richtern und deren Hilfskräften verschlüsselt ablaufen. Von dem Einsatz von Verschlüsselungsprogrammen ist in den Informationen des hessischen Justizministeriums jedoch keine Rede.

5. Auch Ihre Auffassung, dass die Einrichtung der Zugriffsrechte durch die Administratoren nach den Vorgaben des Gerichtspräsidiums erfolgen soll, erscheint mir sinnvoll und konsequent. Eine danach notwendige Einbeziehung des jeweils zuständigen Präsidiums ist nach den Plänen jedoch nicht vorgesehen und meines Wissens bisher auch noch nicht erfolgt.
...

Eberhard Carl

12. Nachweissystem – Anonymisierung

Für alle übrigen Nutzer ist grundsätzlich der Weg der Anonymisierung zu gehen. Die Wiederauffindung von Präjudizien wird durch Schlagworte oder Volltext-Suchfunktionen besser geleistet als durch Namen (Bsp. JURIS-Erschließung). Der Einwand zu hohen Arbeitsaufwands ist nicht begründet, da mit einfachen PC-Befehlen („Ersetzen“) Namen getilgt und durch A,B,C ersetzt werden können. Ausdrucke auf Papier sind nach Anonymisierung zu erstellen – das gilt auch für die gerichtsinterne Information und Bibliothek. Die personenbezogenen Daten sind zu löschen, sobald feststeht, dass sie nicht mehr benötigt werden (§ 19 Abs. 3 HDSG). Sofern neben dem Urteilsausdruck auf Papier elektronische Dokumente mit Personenbezug aufbewahrt werden sollen, ist die Verwendung von Disketten oder CD-ROM vorzuziehen, da diese der Akte beigefügt werden können.

13. Auswertung der Speicherungen durch die Dienststelle

Eine dienstaufsichtlich zu begründende oder organisationsrechtlich begründete Auswertung von Speicherungen in Einzel-PCs und Servern (bspw. durch das Präsidium) ist generell unzulässig, soweit die betreffenden Daten auf richterliche Tätigkeiten zurückgehen. Insoweit besteht hinsichtlich der Inhalte keine allgemeine dienstaufsichtliche Zuständigkeit. Eine „Erledigungskontrolle“ im Sinne eines Pensenschlüssels darf nicht durch Zugriffe auf den PC oder Server stattfinden; sie muss – soweit sie dienst- und personalvertretungsrechtlich zulässig ist – offen und mit Kenntnis der betroffenen Richterinnen und Richter über Art und Umfang der dabei verwendeten Daten erfolgen. Überprüft werden kann allerdings auch von der Dienstaufsicht, ob die in § 10 vorgeschriebenen informationstechnischen Sicherheitsbestimmungen eingehalten werden, ob ausreichende Verfahrensverzeichnisse erstellt worden sind, insbesondere, ob die Übermittlungsschranken aus § 13 Abs. 1 HDSG beachtet sind. Insofern sind keine Probleme richterlicher Unabhängigkeit berührt.

14. Missbrauch des Internetzugangs
Vermutete Straftaten oder vermuteter Missbrauch des Internetzugangs dürfen nur straf- oder disziplinarrechtlich verfolgt werden, nicht durch formlose Einsichtnahme. Im Straf- oder Disziplinarverfahren sind nur solche Zugriffe als „erforderlich“ i.S.v. § 11 Abs. 1 HDSG anzusehen, mit denen Dienstvergehen bewiesen werden sollen, die sich aus dem Vorgang der Entscheidungsfindung, aus anderen dienstlichen Verrichtungen oder aus allgemeinen Straftaten herleiten.

15. Internet-Nutzung und E-mails
Hier entstehen wiederkehrende Gefahren, da unberechtigte Zugriffe auf dienstliche PC oder Server von außen nicht mit Sicherheit abgewehrt werden können. Nicht einmal der Einsatz von Firewalls und Intrusion Detection Systemen bietet eine 100% ige Sicherheit. Um eine höchstmögliche Sicherheit zu erreichen, ist der Einsatz besonderer PCs zweckmäßig, die vom Gerichtsnetz physikalisch getrennt sind und auf denen sich keine zu schützenden Daten befinden. Besondere Gefahren entstehen bei der Öffnung von „Anhängen“ zu E-mails, da sie Schadprogramme enthalten können. Auch sie sollten nur auf PCs geöffnet werden, die keine Verbindung zum inneren Netz haben.

16. Private Mitnutzung
Die persönliche Inanspruchnahme dienstlicher Internet-Anschlüsse führt zu kaum überwindbaren Telekommunikationsproblemen, denn die Dienststelle wird damit Diensteanbieter (Provider) und darf nach TDDSG und TKG nur auf die Verbindungsdaten (zur Abrechnung und Funktionssicherung) zugreifen, die Inhalte hingegen nicht zur Kenntnis nehmen. Das aber ist für dienstliche E-mails unerlässlich (vgl. dazu das Papier: Dienstliche und private Nutzung von E-mail und www, Stand 24.10.2001, unter www.datenschutz.hessen.de). Private Mitnutzung sollte deswegen nicht gestattet werden, allenfalls der Abruf von der privaten Mailbox über dienstliche Anschlüsse.

17. Bereichsspezifische strafprozessuale Datenschutzvorschriften
Die neu gefasste StPO (§§ 474-495) enthält erstmals eigenständiges Datenschutzrecht für das Strafverfahren. Außerdem werden die Übermittlungsbefugnisse zwischen StA und Polizei und die (gelockerte) Zweckbindung bei repressiven und präventiven Zwecken geregelt. Die §§ 479, 481 StPO regeln, inwieweit die Staatsanwaltschaften andere Strafverfolgungs- und Polizeibehörden aktiv informieren dürfen. Die §§ 474-495 StPO sind als bereichsspezifische Regelung auf die Strafverfolgung beschränkt. Eine entsprechende Anwendung in anderen Bereichen der Gerichtsbarkeit scheidet aus.

18. Übermittlungen außerhalb der StPO
Die Übermittlungsbefugnisse der anderen Gerichtsbarkeiten richten sich nach den Verfahrensordnungen bzw. § 13 HDSG. Nach § 13 Abs. 1 können Übermittlungen im Rahmen der jeweiligen Zweckbestimmung erfolgen, bspw. an die Vollstreckungsinstanzen. Nach § 13 Abs. 2 i.V.m. § 12 Abs. 2 darf übermittelt werden, wenn antragsbegründende Angaben des Betroffenen überprüft werden müssen oder wenn die Abwehr erheblicher Nachteile für das Gemeinwohl oder für Leben, Gesundheit und persönliche Freiheit das gebietet, oder in Fällen, in denen sich Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben haben.

Der Autor:

Prof. Dr. von Zezschwitz, ehemals Universität Gießen, ist Hessischer Datenschutzbeauftragter.

Bürgerbefragung in den Gerichten in NRW – der Schlussbericht liegt jetzt vor

In Heft 67 (Seite 136 ff) hatten wir über die Bürgerbefragung in 6 Amts- und Landgerichten in NRW berichtet. Inzwischen liegt der Schlussbericht der Fachhochschule für Rechtspflege darüber vor. Die Beteiligung der befragten Besucher der Gerichte lag bei 37,62 %, die der Mitarbeiter sogar bei 57 %. Die Ergebnisse sind damit recht aussagekräftig. Während die Besucher insbesondere die Freundlichkeit der Mitarbeiter loben und die Sicherheitskontrollen als sehr positiv bewerten (Schulnoten 1,97 bzw. 1,92), kommen Parkplatzsituation, Zustand der Räume und Wartebereich nur etwas schlechter als "befriedigend" weg. Auffällig ist, dass die Mitarbeiter selbst ein weitaus schlechteres Urteil erwarten, als die Besucher ihnen tatsächlich ausstellen. Was nicht Gegenstand des Berichts ist und sein kann: die Untersuchung sollte nicht nur dazu führen, dass die Menschen in den Gerichten sich der externen Kritik stellen, sondern sollte weiterführende Arbeitsgruppen in den Gerichten anstoßen, sich mit den Ergebnissen auseinanderzusetzen und an einer Qualitätsverbesserung zu arbeiten. Zu hoffen ist, dass dies tatsächlich gelingt und nicht wieder einmal eine externe Untersuchung ihr Ende in einem Papierstapel findet.

Der Bericht kann bei der Fachhochschule für Rechtspflege angefordert werden (Schleidtalstraße 3, 53902 Münstereifel. Eine Kurzfassung ist auf der Homepage der Fachhochschule zu finden - www.fhr.nrw.de/buerger&justiz/buj.pdf.

Andrea Kaminski