CyLaw-Report VI

CyLaw-Report VI : „Zugangs- und Eingabekontrolle“

Entscheidung des OVG Hamburg vom 07.07.2005 – 1 Bf 172/03

Das FÖR[1] an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) ist verantwortlich für das SicAri-Teilprojekt[*] "Cyberlaw“[2]. Mit den CyLaw-Reports soll das rechtswissenschaftliche Diskursangebot L.O.S. (Legal Open Source), das bisher nur Rechtsquellen (SicAri-Cyberlaw) enthält, um Rechtsprechung ergänzt werden. Die CyLaw-Reports-Idee ist es, auch Nicht-Juristen an grundlegender und/oder aktueller Cyberlaw-Rechtsprechung und juristischer Methodik fokusssiert teilhaben zu lassen. Fragestellungen, die spezielles juristisches Wissen voraussetzen werden mit dem Kürzel „FEX“ (Für Experten) gekennzeichnet. Hintergrundwissen wird unter der Überschrift „FÖR-Glossar“ ergänzt. Aus Gründen der Präsentationsstrategie wird zwischen „clear cases“, die eine relativ einfache rechtliche Prüfung erfordern, und „hard cases“, die eine vertiefte Diskussion erfordern, unterschieden. In keinem Falle ist mit den CyLaw-Reports die Übernahme von Haftung verbunden.

Die rechtskräftige Entscheidung des OVG Hamburg wurde in die CyLaw-Reports aufgenommen, weil sie grundlegende Bedeutung für die Erhebung von Daten aus automatisierter Verarbeitung durch nicht-öffentliche Stellen haben kann.

[*] Die Arbeiten am CyLaw-Report werden im Rahmen des Projektes SicAri vom Bundesministerium für Bildung und Forschung gefördert.

CyLaw-Report VI

Gliederung:

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**

A. Zugangskontrolle bei automatisierter Verarbeitung – „Clear Case“

I. Sachverhalt

A betreibt in Hessen eine Detektei mit acht Ermittlern und zwei Schreibkräften. R ist Mitarbeiter des Regierungspräsidiums Darmstadt. Im Rahmen eines stichprobenartigen Kontrollbesuchs bei A stellt R folgendes fest: In der Detektei gibt es vier Rechner, die von allen Mitarbeitern gemeinsam genutzt werden. Auf den Rechnern werden die Berichte über Ermittlungsergebnisse gespeichert, die unter anderem Versicherungsnummern und Stammnummern enthalten. Die Rechner sind dabei nicht gegen fremde Zugriffe geschützt.

R ordnet daher gegenüber A an, einen Passwortschutz einzurichten, um eine unbefugte Nutzung von Daten durch Dritte zu verhindern. A ist der Meinung, derartige Sicherheitsvorkehrungen seien nicht erforderlich und die Anordnung rechtswidrig.

II. Rechtsgrundlage

Rechtsgrundlage für die Anordnung des R könnte § 38 Abs. 5 S. 1 BDSG sein.

§ 38 BDSG [Aufsichtsbehörde]
(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5.(…)
(…)
(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abbe-

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**

rufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.
(…)

1. Eröffnung des Geltungsbereichs

Der Geltungsbereich von § 38 BDSG müsste eröffnet sein (§27 Abs. 1 S. 1 Nr. 1 BDSG).

§ 27 BDSG [Anwendungsbereich]
(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch
1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.
Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.
(…)

Voraussetzung ist, dass es sich um eine Verarbeitung unter Einsatz von Datenverarbeitungsanlagen handelt. (§ 27 Abs. 1 S.1 Nr. 1 BDSG). Bei der Verarbeitung unter Einsatz von Datenverarbeitungsanlagen handelt es sich um eine sogenannte „automatisierte Verarbeitung“:

a. Automatisierte Verarbeitung personenbezogener Daten

Wann personenbezogene Daten automatisiert verarbeitet werden, definiert § 3 Abs. 1 und 2 BDSG.

§ 3 BDSG [Weitere Begriffsbestimmungen]
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.
(…)

- **„Personenbezogene Daten“**

Personenbezogene Daten sind Informationen, die sich auf eine bestimmte natürliche Person beziehen oder die geeignet sind, einen Bezug zu ihr herzustellen.[3] Dies können Angaben über menschliche Eigenschaften und Charakteristika sein („persönliche Verhältnisse“), aber auch Daten, die Aussagen über eine Sache enthalten („sachliche Verhältnisse“).[4]

Danach enthalten die Ermittlungsberichte personenbezogene Daten: Es entspricht dem Berufsbild eines Detektivs, derartige Informationen über Personen zu ermitteln und die gewonnenen Erkenntnisse an die Auftraggeber weiterzugeben. Versicherungsnummern und Stammnummern stellen ebenfalls Informationen dar, die sich auf eine bestimmte natürliche Person beziehen.

- **„Automatisierte Verarbeitung“**

Auf den Computern werden die Ermittlungsberichte geschrieben und gespeichert. Die Speicherung ist Teil der Verarbeitung (§ 3 Abs. 4 S. 1 BDSG) und, da sie unter Einsatz von Datenverarbeitungsanlagen erfolgt, Teil einer automatisierten Verarbeitung.

§ 3 BDSG [Weitere Begriffsbestimmungen]
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. (…)

b. Nicht-öffentliche Stelle

A müsste als nicht-öffentliche Stelle zu qualifizieren sein (§ 2 Abs. 4 BDSG).

§ 2 BDSG [Öffentliche und nicht-öffentliche Stellen]
(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gel-

ten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.
(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.
(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn
1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.
Andernfalls gelten sie als öffentliche Stellen der Länder.
(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

Die Detektei des A ist ein privatwirtschaftliches Unternehmen. Ein Bezug zu öffentlichen Stellen oder die Erfüllung hoheitlicher Aufgaben ist nicht ersichtlich. Daher ist die Detektei eine nicht-öffentliche Stelle.

Der Geltungsbereich ist eröffnet (§ 27 Abs. 1 S. 1 Nr. 1 BDSG).

2. Zuständigkeit der Aufsichtsbehörde

R müsste zuständige Aufsichtsbehörde sein. Dies ist nach dem Sachverhalt der Fall. Die Aufsichtsbehörden werden von der jeweiligen Landesregierung bzw. den von diesen ermächtigten Stellen bestimmt (§ 38 Abs. 6 BDSG). In Hessen wurde diese Aufgabe dem Regierungspräsidium Darmstadt übertragen.[5]

3. Technische oder organisatorische Mängel (§ 9 BDSG)

Anordnungen der Aufsichtsbehörde sind nur zur Beseitigung technischer oder organisatorischer Mängel möglich (§ 38 Abs. 5 S. 1 BDSG).

§ 38 BDSG [Aufsichtsbehörde]
(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. (…)

Die technischen und organisatorischen Mängel beziehen sich dabei nur auf die Anforderungen nach § 9 BDSG, der seinerseits durch die Anlage zum BDSG konkretisiert wird.

§ 9 BDSG [Technische und organisatorische Maßnahmen]
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage zu § 9 Satz 1 BDSG
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

Prof. Dr. Viola Schmid, LL.M. (Harvard) - **schmid@jus.tu-darmstadt.de**

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es ist noch nicht einmal ein einfacher Passwortschutz vorgesehen. A hat also keine Maßnahmen getroffen, um zu verhindern, dass unbefugte Dritte auf die in der Detektei verwendeten Computer zugreifen können (Zugangskontrolle). Jeder, der Zugriff auf die Hardware erlangt, hat auch vollen Zugriff auf alle gespeicherten personenbezogenen Daten. Auch ein Schutz gegen Angriffe von Hackern besteht nicht. Maßnahmen der Zugangskontrolle fallen in den Katalog der erforderlichen Maßnahmen (§ 9 S. 1 BDSG i.V.m. Nr. 2 der Anlage zu § 9 BDSG). Ihr Fehlen begründet nach einhelliger Kommentarmeinung[6] („dogmatische Auslegung“) einen technischen und organisatorischen Mangel.

4. Erforderlichkeit

Der Aufwand zur Umsetzung der angeordneten Maßnahmen müsste in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen (Erforderlichkeit, § 9 S. 2 BDSG). Der Schutz personenbezogener Daten, die bei einer Detektei besonders sensibel sein können (vergleiche auch § 3 Abs. 9 BDSG), ist ein wichtiger Schutzzweck.[7]

Ein einfacher Passwortschutz ist mit wenig Aufwand zu bewerkstelligen und dürfte angemessen und folglich erforderlich sein.

5. Ergebnis

Die Anordnung des R ist rechtmäßig.

B. Eingabekontrolle – „Hard Case“

I. Sachverhalt

Der Sachverhalt wird in Anlehnung an die Entscheidung des Hamburgischen Oberverwaltungsgerichts (OVG) vom 07.07.2005 geschildert.[8]

A betreibt in Hessen eine Detektei mit acht Ermittlern und zwei Schreibkräften. Diese nutzen gemeinsam insgesamt vier Computer, auf denen Ermittlungsberichte geschrieben und auch gespeichert werden. R ist Mitarbeiter des Regierungspräsidiums Darmstadt.

Immer wieder gehen bei R Beschwerden über die Detektei des A ein. Den Mitarbeitern des A wird von verschiedenen Behörden, unter anderem Landesversicherungsanstalten und Arbeitsagenturen, vorgeworfen, sich am Telefon als Mitarbeiter des Sozialamts ausgegeben zu haben, um so Versicherungsnummern und Stammnummern Dritter zu erfahren. Die von R informierte Staatsanwaltschaft muss ihre Ermittlungen in der Sache einstellen, da nicht mehr feststellbar ist, welcher Mitarbeiter des A die Anrufe getätigt hat.

R will wenigstens für die Zukunft den Datenschutz der Betroffenen gewährleisten. Er ordnet daher gegenüber A an,

„die notwendigen Maßnahmen zu treffen, die die lückenlose Dokumentation der Herkunft und Beschaffungsart von personenbezogenen Daten im Rahmen von Ermittlungen in oder aus Dateien durch einen konkret benannten Mitarbeiter gewährleisten und die Dokumentation für einen Zeitraum von einem Jahr nach Beendigung des Ermittlungsauftrages aufzubewahren. Aus der Dokumentation müsse ersichtlich sein, welche Mitarbeiter welche personenbezogenen Daten wann und von wem erhoben hätten und welchen Geschäftsvorgängen der Detektei diese Datenerhebungen zuzuordnen seien.“[9]

A meint,

- R sei zu einer solchen Anordnung gar nicht befugt,
- ein organisatorischer oder technischer Mangel läge nicht vor und
- jedenfalls seien die Maßnahmen nicht erforderlich.

II. Rechtsgrundlage

Rechtsgrundlage für die Anordnung des R könnte § 38 Abs. 5 S. 1 BDSG sein. R ist die für Maßnahmen nach § 38 BDSG zuständige Aufsichtsbehörde (siehe oben unter A II 2).

§ 38 BDSG [Aufsichtsbehörde]
(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. (…)

1. Eröffnung des Geltungsbereichs

Der Geltungsbereich von § 38 BDSG ist nur dann eröffnet, wenn die Voraussetzungen des § 27 Abs. 1 S. 1 Nr. 1 BDSG vorliegen.

§ 27 BDSG [Anwendungsbereich]
(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch
1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.
Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.
(…)

In Betracht kommt eine Eröffnung des Geltungsbereichs mit der Alternative: „dafür erhoben werden“, weil nicht auszuschließen ist, dass die telefonisch erhobenen Daten für eine Verarbeitung unter Einsatz von Datenverarbeitungsanlagen erhoben werden. A verarbeitet personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen (siehe oben unter A II 1 a). A ist des Weiteren als nicht-öffentliche Stelle zu qualifizieren (siehe oben unter A II 1 b).

2. Anordnungsbefugnis

R ist nur zu Anordnungen „zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz,

- soweit diese die automatisierte Verarbeitung personenbezogener Daten oder
- die Verarbeitung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln,“

befugt (§ 38 Abs. 5 S. 1 BDSG).

a. „automatisierte Verarbeitung“ (§ 38 Abs. 5 S. 1 BDSG)

Die Besonderheit am Begriff der automatisierten Verarbeitung ist, dass sie die Phasen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 3 Abs. 2 S. 1 BDSG) definitionsgemäß umfasst.[10]

§ 3 BDSG [Weitere Begriffsbestimmungen]
(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. (…)

Voraussetzung ist jeweils der Einsatz von Datenverarbeitungsanlagen.

OVG Hamburg:
„Die Anordnungsbefugnis hängt also nunmehr davon ab, ob die Aufsichtsbehörde von ihr mit dem Ziel Gebrauch macht, den Datenschutz nach solchen Vorschriften zu gewährleisten, die die automatisierte Verarbeitung personenbezogener Daten regeln.“[11]

Problematisch ist hier, dass die Erhebung der Daten nicht unter Einsatz von Datenverarbeitungsanlagen erfolgt (telefonische Auskünfte) und es sich deswegen nicht um eine Erhebung im Sinne einer automatisierten Verarbeitung handelt.

OVG Hamburg:
„Vielmehr will die Beklagte sicherstellen, dass die Klägerin bei ihren Recherchen Daten nur rechtmäßig erhebt. Sie verlangt, dass die Klägerin die Herkunft und Beschaffungsart von personenbezogenen Daten im Rahmen von Ermittlungen in oder aus Dateien lückenlos dokumentiert. Insbesondere mit der Verpflichtung zu dokumentieren, welcher Mitarbeiter welche personenbezogenen Daten wann und von wem erhoben hat, will sie eine nachträgliche Aufklärung der Erhebung der Daten sicherstellen und eine Grundlage für eine zuverlässige Überprüfung durch die Aufsichtsbehörde legen. Dass es ihr dabei nicht um die Art und Weise der Verarbeitung der von der Klägerin ermittelten Daten geht, bestätigt der Anlass für ihr Einschreiten. Anlass war die Beschwerde der Landesversicherungsanstalt Rheinland-Pfalz über Ausspähver-

suche, die von einem Telephonapparat der Klägerin ausgingen. Diese Ausspähversuche sind der Phase der Datenerhebung zuzuordnen.“[12]

Ziel der Anordnung ist also nicht die Kontrolle einer Erhebung als Bestandteil einer automatisierten Verarbeitung, sondern die Kontrolle einer nicht automatisierten Erhebung. Nach Ansicht des OVG Hamburg handelt es sich nämlich beim Versuch, Stammnummern und Versicherungsnummern per Telefon zu erfragen, nicht um eine Erhebung mittels einer Datenverarbeitungsanlage:

OVG Hamburg:
„Allerdings will die Beklagte sicherstellen, dass die Klägerin nicht in rechtswidriger Weise personenbezogene Daten erhebt, die in den automatisierten Datenverarbeitungsanlagen der Landesversicherungsanstalten und anderer Sozialleistungsträger gespeichert sind und dem Sozialdatenschutz unterfallen. Jedoch erhebt die Klägerin die Daten über ihre Zielpersonen insoweit nicht unter Einsatz von Datenverarbeitungsanlagen. Die Klägerin erhebt unmittelbar keine Daten aus den Datenverarbeitungsanlagen der Landesversicherungsanstalten etc.. Es ist nichts für die Annahme ersichtlich, die Klägerin könnte sich etwa wie ein "Hacker" verhalten und sich einen technischen Zugang über das Internet oder andere Wege zu den genannten Datenverarbeitungsanlagen verschaffen. In Rede steht nur der Verdacht, Mitarbeiter der Klägerin könnten Bedienstete der Landesversicherungsanstalten oder der Bundesagentur für Arbeit etc. fernmündlich unter Vortäuschung falscher Identitäten etc. dazu veranlassen, ihnen in den dortigen Dateien gespeicherte, geschützte personenbezogene Daten zu übermitteln.“[13]

Zusammenfassend ist festzuhalten, dass die erste Alternative – „automatisierte Verarbeitung“ (§ 38 Abs. 5 S. 1 BDSG) – nicht erfüllt ist. § 38 Abs. 5 S. 1 BDSG kann aber auch dann Anordnungsgrundlage sein, wenn eine Verarbeitung „in oder aus nicht automatisierten Dateien“ erfolgt.

b. „Verarbeitung … in … automatisierten Dateien“ (§ 38 Abs. 5 S. 1 BDSG)

- **„Verarbeitung“ nach § 38 Abs. 5 S. 1 BDSG i.V.m. § 3 Abs. 3 und 4 BDSG**

Anders als die Definition der „automatisierten Verarbeitung“ umfasst die (nicht automatisierte) Verarbeitung **nicht die Erhebung** (§ 3 Abs. 3 und 4 BDSG).

§ 3 BDSG [Weitere Begriffsbestimmungen]
(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. (…)

Im vorliegenden Sachverhalt handelt es sich um eine telefonische Erhebung von Daten, die in automatisierten Dateien verarbeitet sind. Weil der „Verarbeitungsbegriff" nach § 38 Abs. 5 S. 1 BDSG i.V.m. § 3 Abs. 3 und 4 BDSG nicht die Erhebung umfasst, fehlt es zunächst an einer Anordnungsgrundlage.

- **„Verarbeitung" nach § 38 Abs. 5 S. 1 BDSG i.V.m. § 27 Abs. 2 BDSG**

Zu prüfen ist, ob § 38 Abs. 5 S. 1 BDSG in systematischer Auslegung mit § 27 Abs. 2 BDSG eine Anordnungsgrundlage zu entnehmen ist. § 27 Abs. 2 BDSG bestimmt, dass bei der offensichtlichen Entnahme personenbezogener Daten aus einer automatisierten Verarbeitung der Geltungsbereich des BDSG eröffnet ist. Die telefonische Datenerhebung müsste eine Entnahme von Daten aus einer automatisierten Verarbeitung darstellen.

§ 27 BDSG [Anwendungsbereich]
(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

Nach Ansicht des OVG Hamburg stammen Daten der Landesversicherungsanstalten zwar offensichtlich aus einer automatisierten Verarbeitung.[14] § 27 Abs. 2 BDSG bezieht sich nach dem OVG Hamburg aber nur auf die Phasen der Datenverarbeitung und –nutzung und nicht auf die Datenerhebung:

OVG Hamburg:
„Dieser Hinweis rechtfertigt es aber nicht, die Anordnungsbefugnis der Aufsichtsbehörde im Bereich der Datenerhebung auszudehnen. Sinn und Zweck des § 27 Abs. 2 BDSG ist es lediglich, den Anwendungsbereich des Abschnittes über die Datenverarbeitung nicht-öffentlicher Stellen zu erweitern und zu verhindern, dass personenbezogene Daten, die außerhalb von nicht automatisierten Dateien, wie z.B. in bestimmten Akten, verarbeitet und genutzt werden, auch dann aus dem Schutzbereich der Regelungen über die Datenverarbeitung nicht-öffentlicher Stellen herausfallen, wenn sie zuvor offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind. Um den Anwendungsbereich dieser Regelungen, insbesondere der Regelung des § 28 BDSG über die Zulässigkeit der Datenerhebung durch nicht-öffentliche Stellen geht es hier aber nicht. Maßgeblich ist vielmehr: Die Differenzierungen, die § 38 Abs. 5 Satz 1 BDSG zwischen der Datenerhebung unter dem Ein-

satz von Datenverarbeitungsanlagen einerseits trifft und der - nicht die Datenerhebung umfassenden - Datenverarbeitung in oder aus nicht-automatisierten Dateien andererseits können nicht deshalb beiseite geschoben werden, weil die Daten zuvor von der übermittelnden Stelle und nicht der die Daten erhebenden Stelle offensichtlich einer automatisierten Datenverarbeitung entnommen sind. Entsprechend dem Wortlaut des § 38 Abs. 5 Satz 1 BDSG bleibt es dabei, dass die Aufsichtsbehörde hinsichtlich der Phase der Datenerhebung nur die Ausführung datenschutzrechtlicher Vorschriften sicherstellt, soweit diese die automatisierte Verarbeitung personenbezogener Daten regeln. Dass danach außerhalb des Bereiches automatisierter Datenverarbeitung die Phase der Datenerhebung von der Anordnungsbefugnis ausgenommen bleibt, macht Sinn. Denn das Gesetz begegnet mit der Ausdehnung der Anordnungsbefugnis auf die Phase der Datenerhebung unter dem Einsatz von Datenverarbeitungsanlagen gerade den mit derartigen Anlagen verbundenen spezifischen Gefahren für den Datenschutz."[15]

Das OVG Hamburg legt also sowohl § 27 Abs. 2 BDSG als auch § 38 Abs. 5 S. 1 BDSG restriktiv aus, mit der Folge, dass R keine Anordnungsbefugnis hat. Das OVG Hamburg beendet damit die Prüfung nicht: Selbst wenn die Anordnungsbefugnis auch für die Erhebung aus automatisierten Dateien zu bejahen wäre, fehlt es nach Auffassung des Gerichts an den weiteren Voraussetzungen des § 38 Abs. 5 S. 1 BDSG, nämlich den „ …. Anforderungen nach § 9 …". Diese weiterführende Hilfsprüfung des OVG Hamburg erklärt sich vielleicht daraus, dass die Kommentarliteratur eine extensive Interpretation von § 27 Abs. 2 BDSG fordert:

Simitis, in: Simitis, Kommentar zum BDSG:
„… so wenig geht es an, in dieser Vorschrift lediglich ein Umgehungskorrektiv zu sehen und sie daher möglichst restriktiv auszulegen. Eine verfassungsrechtlich korrekte, an der informationellen Selbstbestimmung ausgerichtete Interpretation erfordert vielmehr, § 27 Abs. 2 konsequent zu nutzen, um das Schutzdefizit im nichtöffentlichen Bereich möglichst zu verringern."[16]

3. Technische oder organisatorische Mängel (§ 9 BDSG)

Voraussetzung wäre, dass die Verhaltensweisen der Mitarbeiter von A, denen R mit seiner Anordnung entgegenwirken möchte, einen technischen oder organisatorischen Mangel darstellen (§ 9 BDSG).

§ 9 BDSG [Technische und organisatorische Maßnahmen]
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschrif-

ten dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9 BDSG wird insoweit durch die Anlage zum BDSG konkretisiert (s. o. unter A II 3).

In der vorangegangenen Instanz argumentierte das Verwaltungsgericht Hamburg:[17]

VG Hamburg:
„Auch liege ein Verstoß gegen die in Nr. 5 der Anlage zu § 9 BDSG geregelte Eingabekontrolle vor, durch die nachträglich festgestellt werden könne, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben würden."[18]

Das OVG Hamburg vertritt demgegenüber die Auffassung, dass die in der Anlage zu § 9 BDSG formulierten Anforderungen ebenfalls an eine automatisierte Datenverarbeitung anknüpfen. Dafür könnte der Wortlaut von Satz 1 und Satz 2 der Anlage zu § 9 BDSG sprechen:

Anlage zu § 9 Satz 1 BDSG
Werden personenbezogene Daten **automatisiert verarbeitet oder genutzt**, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind **insbesondere** Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. (…)

Wie das Wort „insbesondere" in Satz 2 zeigt, handelt es sich bei dem Maßnahmenkatalog um eine Konkretisierung der Anforderungen, die allgemein in Satz 1 formuliert sind. Satz 1 bezieht sich ausdrücklich nur auf die automatisierte Verarbeitung:

OVG Hamburg:
„Nach der genannten Anlage ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird, wenn personenbezogene Daten automatisiert verarbeitet oder genutzt werden. Damit knüpfen auch die Anforderungen dieser Anlage gerade an den Vorgang der automatisierten Datenverarbeitung und damit der Erhebung unter dem Einsatz von Datenverarbeitungsanlagen an. Dass gerade das mit dem Einsatz von Datenverarbeitungssystemen verbundene erhöhte Risikopotential im Blickpunkt der Regelung steht, zeigt sich auch an den in Satz 2 der genannten Anlage aufgeführten Beispielen für technische und organisatorische Maßnahmen des Datenschutzes. Dort sind nur geeignete Maßnahmen der Zutrittskontrolle zu Datenverarbeitungsanlagen, der Zugangskontrolle, der Zugriffskontrolle, der Weitergabekontrolle, der Eingabekontrolle, der Auftragskontrolle und der Verfügbarkeitskontrolle sowie der Option getrennter Verarbeitung zu unterschiedlichen Zwecken erhobener Daten aufgeführt."[19]

Damit können nach Auffassung des OVG Hamburg technische oder organisatorische Mängel im Sinne des § 38 Abs. 5 S. 1 BDSG nur im Rahmen einer automatisierten Datenverarbeitung vorliegen.

OVG Hamburg:
„Auf die Eindämmung derartiger spezifisch mit der automatisierten Datenverarbeitung verbundener Risiken zielt die Anordnung der Beklagten nicht. Denn die Beklagte will nicht regeln, in welcher Weise die Klägerin im Wege automatisierter Datenverarbeitung personenbezogene Daten erhebt. Ihr geht es darum, zu verhindern, dass die Mitarbeiter der Klägerin fernmündlich geschützte personenbezogene Sozialdaten über die Mitarbeiter der Sozialleistungsträger ausspionieren.“[20]

Die telefonische Datenerhebung erfolgt nicht automatisiert, so dass insoweit den Anforderungen nach § 9 BDSG und damit den Anforderungen nach § 38 Abs. 5 S. 1 BDSG nicht genügt wird. Auch hiermit beendet das OVG Hamburg die Prüfung nicht. Selbst bei einer Erstreckung der technischen und organisatorischen Mängel auf die Erhebung fehle es an der datenschutzrechtlichen Erforderlichkeit.

4. Erforderlichkeit

Die Anordnung des R müsste sich ferner auf technische und organisatorische Maßnahmen beziehen, die zur Gewährleistung der datenschutzrechtlichen Anforderungen erforderlich sind (§ 9 S. 1 BDSG). Dies ist nur der Fall, wenn der notwendige Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 9 S. 2 BDSG).
Daran fehlt es nach Ansicht des OVG Hamburg. Zwar ist der Schutz von Sozialdaten nach dem OVG Hamburg ein gewichtiger Schutzzweck. Allerdings werde die Berufsausübung das A unverhältnismäßig beeinträchtigt:

OVG Hamburg:
„Die Beklagte erschwert den Geschäftsbetrieb der Klägerin in unzumutbarer Weise, wenn jede Ermittlung beispielsweise einer Adresse unter Angabe der Datei, der die Adresse entnommen ist, des Zeitpunktes und des Namens des recherchierenden Mitarbeiters dokumentiert werden muss. Derartige Dokumentationen kosten Zeit und damit Geld in einer Größenordnung, die bei einer Preisstruktur der Klägerin von ca. 30 Euro je Auftrag ins Gewicht fällt. Insbesondere liegt auf der Hand, dass es die Recherchearbeit einer Detektei wesentlich beeinträchtigt, wenn - wie die Beklagte auf S. 11 des Widerspruchbescheides betont - die Mitarbeiter der Klägerin auch dokumen-

tieren müssen, von wem und wann sie welche personenbezogenen Daten erhoben haben."[21]

Außerdem wird A nach Auffassung des OVG Hamburg im Wettbewerb benachteiligt:

OVG Hamburg:
„Die Wettbewerbsfähigkeit einer Detektei leidet erheblich, die anders als ihre Konkurrenten ihre Tätigkeit derartig umfassend dokumentieren und insbesondere die Identität ihrer Informanten und die von diesen gegebenen Informationen ständig im einzelnen offen legen muss. Die Auffassung des Verwaltungsgerichts, es sei nicht nachvollziehbar, dass die geforderte Dokumentationspflicht Kosten verursacht, die die Klägerin in ihrer Existenz gefährden könnten, greift zu kurz. Der Aufwand für den Datenschutz ist nicht erst dann unangemessen, wenn er zu einer Existenzgefährdung führt."[22]

5. Ergebnis

Die Anordnung des R gegenüber A war rechtswidrig, da R zu der getroffenen Anordnung bei der Datenerhebung nicht befugt war und ein organisatorischer oder technischer Mangel nicht vorlag. Darüber hinaus waren die angeordneten Maßnahmen nicht erforderlich und daher unverhältnismäßig.

C. Schlussfolgerungen aus dem Urteil des OVG Hamburg

- Die Datenschutzaufsicht nach § 38 BDSG bezieht sich auf alle vom BDSG geregelten Phasen der automatisierten Datenverarbeitung: die Erhebung, die Verarbeitung und die Nutzung.
- Anordnungen im Bereich der Datenerhebung darf die Aufsichtsbehörde aber nur treffen, soweit es um die Erhebung von Daten unter Einsatz von Datenverarbeitungsanlagen geht (automatisierte Verarbeitung).
- Der Aufwand technischer oder organisatorischer Maßnahmen kann bereits dann im Verhältnis zum Schutzzweck unangemessen sein, wenn die Wettbewerbsfähigkeit erheblich leidet. Eine Existenzgefährdung muss nicht vorliegen.

---

[1] Informationen zu FÖR (Fachgebiet Öffentliches Recht) finden Sie unter http://www.bwl.tu-darmstadt.de/jus4/?FG=jus.
[2] Cyberlaw (in einer öffentlich-rechtlichen Betrachtung) ist ein Oberbegriff für Medien-, Telekommunikations-, Computer-, Internet-, Informations-, Datensicherheits- und Datenschutzrechte, die sich mit den Themen des Cyberspace und der Cyberworld befassen.
[3] Gola/Schomerus, BDSG, Kommentar, 8. Aufl. 2005, § 3, Rn. 3.
[4] Gola/Schomerus, BDSG, Kommentar, 8. Aufl. 2005, § 3, Rn. 4 ff.
[5] FEX: Die Regelungen in den einzelnen Bundesländern unterscheiden sich insoweit. Während in Hessen das Regierungspräsidium Darmstadt zuständig ist, haben manche Bundesländer den jeweiligen Landesdatenschutzbeauftragten als Aufsichtsbehörde bestimmt (etwa Hamburg, Niedersachsen, Nordrhein-Westfalen).
[6] Gola/Schomerus, BDSG, Kommentar, 8. Aufl. 2005, § 9, Rn. 12 ff., 24; Walz, in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 38, Rn. 39.
[7] In der Terminologie der Vorlesung des Fachgebiets Öffentliches Recht an der Technischen Universität Darmstadt „Rechtfertigungsrechtsgut".
[8] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310.
[9] Zitiert nach dem Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03 (über juris).
[10] FEX: Dies war nach dem BDSG a.F. noch anders: Die Anordnungsbefugnis nach § 38 Abs. 5 S. 1 BDSG a.F. umfasste nicht die Phase der Datenerhebung – so zumindest das OVG Hamburg, Urteil vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (311).
[11] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (312).
[12] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (311).
[13] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (312).
[14] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (312).
[15] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (312 f.).
[16] Simitis, in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 27, Rn. 29.
[17] Urteil des VG Hamburg vom 21.11.2002, Az.: 22 VG 2830/99.
[18] Zitiert nach dem Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03 (über juris).
[19] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (313).
[20] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (313).
[21] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (313).
[22] Urteil des OVG Hamburg vom 07.07.2005, Az.: 1 Bf 172/03, NJW 2006, 310 (313).