## Humanistische Union

# Verfassungsrechtssprechung unter dem Vorzeichen der Sicherheitspolitik

Fachtagung zur Entscheidung über Online-Durchsuchungen zeigt Licht und Schatten in der virtuellen Freiheitssphäre. Aus: Mitteilungen Nr. 201, S. 6-10

Verfassungsrechtssprechung unter dem Vorzeichen der Sicherheitspolitik

Die Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung vom 27. Februar 2008 bietet reichlich Material für rechtspolitische Diskussionen. Die Begründung eines neuen Grundrechts nährt die Hoffnung, dass bisherige Lücken des Rechtsschutzes geschlossen werden. Im vorliegenden Fall verspricht das neue Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme einen besseren Schutz für „ruhende" Daten, erstmals aber auch einen Schutz der zugrundeliegenden Verarbeitungssysteme, den es so bisher im Datenschutzrecht nicht gab.

Angesichts der kurz nach der Entscheidung einsetzenden Gesetzgebung in Bayern und im Bund stellt sich die Frage, ob der Richterspruch wirklich den Datenschutz beflügelt oder ob es sich dabei nicht um einen „roten Teppich" handelt, auf dem die Innenminister jetzt ihre Vorhaben zur Online-Durchsuchung ausbreiten können – und das auch noch mit höchstrichterlicher Zustimmung.

Humanistische Union und Friedrich-Naumann-Stiftung hatten für den 28. April gemeinsam zu einer Fachtagung eingeladen, um über die „Konsequenzen des Karlsruher Richterspruchs" zu diskutieren. Eine ausführliche Dokumentation der Fachtagung findet sich im Internet, die Beiträge der Tagung sind in einem Sammelband im Berliner Wissenschafts-Verlag erschienen (s. Anzeige auf S. 10). Dieser Beitrag beschränkt sich deshalb darauf, die rechtspolitischen Diskussionen der Tagung im Kontext der aktuellen Sicherheitspolitik darzustellen.

#### Falsch verstanden: Das neue Computer-Grundrecht nur eine Vorlage für das BKA-Gesetz?

Bei aller Kritik an der Entscheidung vom 27. Februar 2008 – dazu später mehr – steht außer Frage, dass damit mehr als nur ein vernichtendes Urteil über das nordrhein-westfälische Verfassungsschutzgesetz gesprochen wurde. Die Etablierung eines neuen Grundrechts passiert nicht aller Tage und so hätte man erwarten können, dass die Sicherheitspolitiker genauer nachlesen, welche Probleme und Aufgaben ihnen die Entscheidung möglicherweise aufgibt. Bisher haben jedoch weder Herr Schäuble noch Frau Zypries erkennen lassen, dass sie – außer dem geplanten Ausbau des Bundeskriminalamts – über die nötigen Konsequenzen nachdenken. Die politische Diskussion nach der Entscheidung ist einmal mehr darauf verengt, welche neuen Sicherheitsbefugnisse unter den Vorzeichen des neuen Grundrechts gerade noch vertretbar seien.

Auf der Fachtagung der Humanistischen Union kamen einige Probleme zur Sprache, bei denen dringender

Handlungsbedarf besteht:

• Der aus dem neuen Grundrecht abgeleitete Schutzanspruch erstreckt sich nicht nur auf heimlich durchsuchte Systeme. Nach Einschätzung von Prof. Dr. Hans-Heiner Kühne gilt bereits jetzt kraft der Entscheidung des Bundesverfassungsgerichts, dass auch bei der Beschlagnahme und offenen Durchsuchung von Computersystemen ein Schutz der Intimsphäre zu beachten sei. Obwohl sich dieser Schutzanspruch unmittelbar aus der Entscheidung ergebe, sei er in der Praxis kaum durchsetzbar, erklärte er in seinem Vortrag zu den strafprozessualen Konsequenzen der Entscheidung. Wenn man bedenke, dass man als Rechtsanwalt einem Staatsanwalt erklären müsse, dass ein beschlagnahmter Rechner jetzt nicht mehr ohne weiteres komplett durchsucht werden dürfe, könne er sich gut vorstellen, „dass das schwierig ist". Kühne schlug deshalb vor, für die Beschlagnahme und Auswertung von Computern (§97 StPO) einen vergleichbaren Schutz des Kernbereichs privater Lebensgestaltung einzuführen wie beim Großen Lauschangriff (§100c Abs. 4 StPO).

• Der Berliner Beauftragte für den Datenschutz und die Informationsfreiheit, Dr. Alexander Dix, erinnerte daran, dass der Staat mit dem neuen Computer-Grundrecht in der Verantwortung ist, „seinen Bürgerinnen und Bürgern Instrumente zum informationellen Selbstschutz gegen heimliche Ausspähung an die Hand zu geben und ihren ungehinderten Einsatz zu gewährleisten." Das schließe einen Bildungsauftrag ein, etwa um jungen Menschen eine hinreichende Sensibilität für Probleme des Datenschutzes bei der Internetnutzung und eine höhere Medienkompetenz zu verschaffen.

• Alexander Dix als auch der Informatiker Prof. Dr. Andreas Pfitzmann erinnerten daran, dass vorbeugender Datenschutz nicht erst in der Techniknutzung beginnt, sondern bereits bei deren Entwicklung ansetzen müsse. Pfitzmann erinnerte daran, dass die Gefahren des Ausspioniertwerdens nicht nur von inländnischen Geheimdiensten ausgehen. Gegen derartige Angriffe müsse der Staat seine Bürger wirksam schützen. Vorrangige Aufgabe des Gesetzgebers sei es deshalb, Rahmenbedingungen für eine datenschutzfreundliche Technikgestaltung zu setzen. Dix erinnerte in diesem Zusammenhang an die bereits 1999 von Datenschützern erhobene Forderung nach einer Neuordnung der Telekommunikationspolitik: Telekommunikationsanbieter sollten gesetzlich dazu verpflichtet werden, ihre Dienstleistungen datenschutzgerecht anzubieten. Dazu gehöre unter anderem eine kostenlose Verschlüsselung (etwa von Telefonverbindungen oder Internetzugängen), natürlich ohne „Generalschlüssel" für die Sicherheitsbehörden. Gleiches ist nach Pfitzmann für die Entwicklung von IT-Systemen und deren Software zu fordern: Internetzugänge ohne eingeschalteten Anonymisierungsdienst, E-Mail-Programme ohne integrierte Verschlüsselung oder Betriebssysteme ohne Verschlüsselung aller Dateiinhalte sind der vorprogrammierte Datengau. Wenn aus dem Urteil zur Online-Durchsuchung deshalb ein gesetzgeberische Handlungsbedarf abgeleitet werde, dann bestünde der eher beim Telekommunikationsgesetz (TKG) und dem Telemediendienstgesetz (TMDG), in denen der Anspruch auf die Gewährleistung der Vertraulichkeit und Integrität bisher nicht eingelöst werde.
Schließlich bleibt daran zu erinnern, dass das Verfassungsgericht (leider) nicht darüber geurteilt hat, ob Online-Durchsuchungen überhaupt sinnvoll und notwendig sind. Dr. Burkhard Hirsch wies in seinem einleitenden Referat darauf hin, dass der Gesetzgeber bisher jeden Beweis schuldig geblieben sei, welchen Sicherheitsgewinn die zahlreichen neu geschaffenen Überwachungsgesetze der vergangenen Jahren erbracht haben. Das gelte auch für die Online-Durchsuchung. Die ständigen Versprechen, mit mehr Überwachungsbefugnissen ließe sich mehr Sicherheit schaffen, bezeichnete er als „politische Zechprellerei". Eine ausgewogene Sicherheitsgesetzgebung müsste nicht nur prüfen, ob die von ihr vorgeschlagenen Maßnahmen geeignet sind, die beschriebenen Gefahren einzudämmen. Sie müsste auch prüfen, welche Erfahrungen (und nicht intendierten Folgen) die praktische Anwendung neuer Überwachungsbefugnisse hervorbringt. Beiden Aufgaben sei der Gesetzgeber bisher nicht nachgekommen.

**Verfassungsrichter sind keine Gesetzgeber**

Genau jene Sicherheitspolitiker, die sich über die Einmischung des Verfassungsgerichts in die Sicherheitsgesetzgebung beklagten, gaben die Leitsätze der Entscheidung zur Online-Durchsuchung hernach als Grundlage ihrer Gesetzentwürfe aus: Herr Schäuble und Herr Herrmann betonten unisono, dass ihre Gesetzentwürfe für die Legalisierung von Online-Durchsuchungen beim BKA, dem bayerischen Verfassungsschutz und der bayerischen Polizei die Maßstäbe des Verfassungsgericht 1:1 umsetzen werden. So etwas nennt man selbsterfüllende Prophezeiung. Burckhard Hirsch griff diesen sicherheitspolitischen Kurzschluss scharf an: Es sei die ureigenste Aufgabe des Gesetzgebers, den Geist der Verfassung auszugestalten und nicht nur eine Politik der Angst zu betreiben, die ständig die Grenzen der Verfassung auslotet.

Schaut man sich die versprochene „1:1 Umsetzung" an der Frage des Kernbereichsschutzes im BKA-Gesetz ( § 20k Abs. 7 BKAG-E) genauer an, findet sich die sattsam bekannte Strategie wieder, einerseits verfassungsrichterliche Grenzmarkierungen zu übernehmen, und zugleich eine gezielte Überschreitung dieser Grenzen zu versuchen. In Anlehnung an die Entscheidung des BVerfG heißt es dort in Satz 2: „Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden." Damit hat der Gesetzgeber fast wortwörtlich abgeschrieben, was ihm die Verfassungsrichter aufgetragen haben (vgl. Urteil vom 27.2.2008, Rdnr. 277). Das Verfassungsgericht hatte es bei diesem Hinweis, eine mögliche Verletzung der Intimsphäre müsse vorab geprüft und ausgeschlossen werden, belassen. Indem der Gesetzentwurf die formelhafte Ausführung des Gerichts übernimmt, überträgt er dem BKA die Entscheidung, wie die Vorkehrungen vor einer unzulässigen Überwachung des Kernbereichs aussehen. Damit hat der Gesetzgeber seine Aufgabe nicht erfüllt. Dr. Maximilian Warntjen wies in seinem Referat zum Kernbereichsschutz darauf hin, dass es sehr wohl konkrete Möglichkeiten gebe, um den möglichen Bezug zur Intimsphäre abzuschätzen: Ob ein Computer von einer Person allein oder gemeinschaftlich genutzt wird, ob er in einem privaten Umfeld oder in Geschäftsräumen aufgestellt ist – all dies gibt Hinweise darauf, welche Art von Informationen dort zu finden sind. Nichts davon findet sich jedoch im BKA-Gesetz. Letztlich werden also wieder Gerichte entscheiden müssen, wo die Grenzen des „soweit möglich" liegen. Der Gesetzgeber entzieht sich damit nicht nur seiner Aufgabe, unter der Hand wird so aus einer verfassungskonformen Regelung ein impliziter Verstoß gegen übermäßige Eingriffe in die Privatsphäre.

Damit aber nicht genug: Neben dem impliziten findet sich im BKA-Gesetzentwurf zugleich der offensive Verstoß gegen Überwachungsgrenzen. Nach § 20k Abs. 7 Satz 1 ist auf Online-Durchsuchungen nur dann zu verzichten, wenn Anhaltspunkte dafür gegeben sind, dass dadurch „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden". Ein paar unbedenkliche Dateien, die beim besten Willen nicht der Intimsphäre des Betroffenen zuzurechnen sind, lassen sich schließlich auf jedem Rechner finden. Der Schutz des Kernbereichs würde mit diesem Gesetzesvorschlag faktisch abgeschafft.

Die Durchführbarkeit heimlicher Online-Durchsuchungen steht und fällt mit der Frage, ob und wie den Ermittlern der unerkannte Zugriff auf den gewünschten Computern gelingt. Bereits im Vorfeld der Gerichtsentscheidung hatten die Koalitionsparteien lange darüber gestritten, ob den Ermittlern ein heimlicher Wohnungszutritt gestattet werden solle, um die „Remote Forensic Software" (so die technizistische Beschreibung des Bundestrojaners) unerkannt auf dem Zielrechner zu installieren. Das hätte nach Einschätzung vieler Experten eine weitere Aufweichung des Wohnraumschutzes, sprich: eine Änderung von Artikel 13 Grundgesetz nötig gemacht. Nachdem die SPD dies abgelehnt hatte, blieben nunmehr zwei Varianten für den heimlichen Einbruch in den Computer übrig: Entweder wird der Bundestrojaner mit Hilfe Dritter (z.B. verdeckter Ermittler) installiert oder die Ermittler versuchen, über bestehende Schwachstellen während einer Online-Verbindung in den Rechner einzudringen. Beide Varianten sind in besonderem Maße problematisch.

Andreas Pfitzmann ging in seinem Referat vor allem auf die Schwierigkeiten der zweiten Zugriffsmethode, den von außen erfolgenden Angriff ein. Dieser kann durch infizierte Webseiten, verseuchte E-Mail-Anhänge oder einen zugespielten Datenträger erfolgen, ebenso wäre ein Einbruch während einer bestehenden Internetverbindung denkbar. Alle Zugriffsszenarien von außen weisen erhebliche Gefahren auf, dass die Ermittler den falschen Computer durchsuchen. Pfitzmann verwies hier auf die mündliche Verhandlung vor

dem Bundesverfassungsgericht, in der ein Mitarbeiter des BKA zugeben musste, dass man erst dann, wenn man die durchsuchten Daten auswerte, wissen könne, ob man den richtigen Computer durchsucht habe. Im Unterschied zu Lauschangriffen bestehe bei einer von außen gestarteten heimlichen Online-Durchsuchung ein stärkeres Verwechslungsrisiko. Dazu reiche beispielsweise eine sich kurzfristig ändernde IP-Adresse nach der Unterbrechung des Internetzugangs; oder die infizierte Webseite werde zufällig von anderen Personen besucht, der infizierte E-Mail-Anhang versehentlich an Dritte weitergeleitet, die zugespielte CD mit der Schadsoftware von jemand anderem in den Computer eingelegt...

Dass die SPD eine weitere Änderung des Artikels 13 verhindert hat, ist sicherlich begrüßenswert – eine rechtsstaatlich akzeptable Online-Durchsuchung hat sie mit der jetzt vereinbarten Zugriffslösung jedoch nicht erreicht. Vielmehr hätte sie angesichts solcher Unsicherheiten auf das zweifelhafte Instrument der Online-Durchsuchung ganz verzichten sollen.

#### Lücken in der Entscheidung

Während man dem Gesetzgeber vorwerfen kann, die Karlsruher Entscheidung zur Online-Durchsuchung einseitig, nur mit Blick auf die gewünschten Überwachungsbefugnisse zur Kenntnis zu nehmen, müssen sich auch die Verfassungsrichter die Frage gefallen lassen, inwiefern sie in ihrer Entscheidung auf die politische Diskussion um Online-Durchsuchung und die dabei bestehenden Erwartungen antworten.

Wurden Vertreter der Sicherheitsbehörden vor der Gerichtsentscheidung auf die schwierige Umsetzung einer Online-Durchsuchung angesprochen, dann betonten sie immer wieder, dass diese natürlich in Kombination mit anderen Überwachungsmaßnahmen (Telefonüberwachung ...) eingesetzt werde. Deshalb hätte das Verfassungsgericht – so Hans-Heiner Kühne – davon ausgehen müssen, dass das BKA gewillt sei, den Bundestrojaner notfalls auch mit Hilfe Dritter in den Zielrechner einzuschleusen, wenn ihm selbst der heimliche Zutritt in die Wohnung der Verdächtigen verwehrt bleibe. Im Stillen gehe man beim BKA offenbar davon aus, dass man über eine sog. Annexkompetenz verfüge, was Kühne jedoch ablehnte. Die dahinter stehende Auffassung, dass wer ein Recht habe, auch alle gegebenen Mittel dafür einsetzen könne, verstoße in eklatanter Weise gegen das Rechtsstaatsgebot. Nach Kühnes Einschätzung wäre es deshalb wünschenswert gewesen, wenn sich das Gericht auch zu der umstrittenen Annexkompetenz geäußert hätte.

Lässt man Online-Durchsuchungen überhaupt zu, so stellt sich immer die Frage, wie die Privatsphäre der Betroffenen, insbesondere ihr Kernbereich privater Lebensgestaltung geschützt werden kann. Das betrifft nicht nur die oben genannte Abwägung vor Beginn der Durchsuchung, sondern auch jenen Zeitpunkt, wenn die Daten heimlich an die Sicherheitsbehörden übertragen und dort ausgewertet werden. Maximilian Warntjen wies darauf hin, dass ein solcher nachträglicher Schutz nur bedingt wirksam sei. Er erinnerte an die Mahnung Hans Liskens: „Was einmal erlauscht ist, ist kaum aus den Köpfen (der Ermittler) herauszubekommen." Deshalb verwundere es umso mehr, dass das Gericht für diese Phase des Grundrechtsschutzes keine genaueren Vorgaben aufstellte. Im Vorfeld der Entscheidung war darüber diskutiert worden, ob eine erste Sichtung der erhobenen Daten durch einen Ermittlungsrichter vorzusehen sei, der unzulässig erhobene Daten sperren und damit die unvermeidbare Kenntnisnahme intimer Details durch die Ermittler ausschließen könne („Richterband"). Dieses Modell wurden von den Verfassungsrichtern jedoch nicht aufgegriffen.

#### Kritische Stimmen zum neuen Computer-Grundrecht

Insbesondere die Ausführungen der Richter zur Frage des Kernbereichschutzes riefen auf der Fachtagung

kritische Stimmen hervor und zeigten, dass auch Bürgerrechtler die in Karlsruhe aufgestellten Maßstäbe für den Schutz der Freiheitssphäre kritisch hinterfragen sollten. Maximilian Warntjen wies in seinem Vortrag darauf hin, dass die Verfassungsrichter sehr wohl erkannt hätten, dass ein vorbeugender (=absoluter) Schutz des Kernbereichs kaum zu leisten, eine Verletzung der Intimsphäre bei Online-Durchsuchungen „praktisch unvermeidbar" sei. Die automatisierte Durchsuchung von Zielrechnern (etwa nach Dateinamen, Stichwörtern etc.) bietet eben keine Gewähr dafür, dass die gefundenen Dateien keine intime Angaben enthalten. Das wird sich regelmäßig erst während der Auswertung der erhobenen Daten feststellen lassen. Warntjen erinnerte deshalb an das Sondervotum der Richterinnen Hohmann-Dennhardt und Jaeger aus der Entscheidung zum Großen Lauschangriff: Wenn bestimmte Überwachungsinstrumente selbst Minimalstandards des Freiheitsschutzes unterlaufen, sollte eine freiheitliche Gesellschaft auf sie verzichten. Bei der Online-Durchsuchung wäre einmal mehr die Gelegenheit gewesen, jene rote Linie zu markieren, die staatliche Überwachung um keinen Preis überschreiten darf. Diese Gelegenheit blieb leider ungenutzt.

Bekanntlich hat sich das Verfassungsgericht anders entschieden: Die Richter erklärten Online-Durchsuchungen dann für zulässig, wenn eine polizeiliche Prognose auf die Entstehung einer konkreten Gefahr für überragend wichtige Rechtsgüter hinweise. Mit dieser Beschreibung des Gefahrenstadiums gingen die Verfassungsrichter einen fragwürdigen Kompromiss ein: Offenbar scheuten sie davor zurück, die Eingriffsschwelle für Online-Durchsuchungen auf eine polizeirechtlich gesehen konkrete Gefahr festzulegen. Solche konkreten Gefahrenlagen setzen u.a. voraus, dass auch der Zeitpunkt des Gefahreneintritts bekannt ist – für die Vorbereitung einer Online-Durchsuchung wäre es dann in der Regel zu spät. Anstatt die Online-Durchsuchung also an ihrer technisch bedingten Vorlaufzeit scheitern zu lassen, eröffnete das Verfassungsgericht die Möglichkeit, Online-Durchsuchung im Bereich der polizeilichen Gefahrenvorsorge einzusetzen. Die seit Jahrzehnten zu beobachtende Vorverlagerung polizeilicher Überwachungsmaßnahmen wird also fortgesetzt.

Ebenso zwiespältig fiel das Urteil von Alexander Dix darüber aus, wie sich das Verfassungsgericht zur unbeobachteten Nutzung des Internets verhalten haben. Zwar habe das Gericht das Internet als solches zum informationstechnischen System erhoben und damit in den Schutzbereich der Vertraulichkeit und Integrität einbezogen. Zugleich verneinten die Richter in der Entscheidung zur Online-Durchsuchung, dass es sich allein bei der Erhebung öffentlich zugänglicher Informationen aus dem Internet um einen Grundrechtseingriff handle. (Diese Linie wurde inzwischen mit einem weiteren Urteil zur Zulässigkeit der Erhebung steuerrelevanter Daten aus öffentlichen Verzeichnissen fortgesetzt - Entscheidung 1 BvR 2388/03 vom 10.3.2008). Ein grundrechtlicher Schutzanspruch ergebe sich erst dann, wenn die Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt" (Rdnr. 307). Damit folgt das Verfassungsgericht einmal mehr der Tendenz, wonach die Erhebung persönlicher Daten durch staatliche Stellen unproblematisch sei.

Schließlich unterzog Prof. Dr. Oliver Lepsius in seinem Vortrag über „Herleitung, Funktion und Überzeugungskraft" die verfassungsdogmatische Einordnung des neuen Computer-Grundrechts einer kritischen Prüfung. Um Raum für das neue Computer-Grundrecht und dessen Systemdatenschutz zu schaffen, habe Karlsruhe den Schutzbereich des Rechts auf informationelle Selbstbestimmung auf persönlich erzeugte Daten begrenzt, um im Gegenzug die beim Betrieb von IT-Systemen automatisch anfallenden Daten dem Schutzbereich des neuen Grundrechts zuzuordnen. Dabei hätte es eine naheliegende Alternative gegeben: Statt eines neuen Grundrechts hätte man auch die bereits etablierten Begriffe der Erhebung und Verarbeitung von individualisierbaren Daten ausweiten können.

Dass diese Alternative nicht erwogen wurde, lag offenbar auch darin begründet, dass die Richter mit dem neuen Grundrecht ein Gewährleistungsanspruch verankern wollten. Positiv lässt sich darin die Einsicht erkennen, dass die Nutzung von Computern für eine freie Entfaltung der Persönlichkeit heute unverzichtbar ist. Die zunehmende Bedeutung von Informationstechnologien im Alltag macht es nach Ansicht der Verfassungsrichter notwendig, auch die dafür nötige Infrastruktur zu schützen. Der objektivrechtliche Gewährleistungsgehalt des neuen Grundrechts könne insofern – so Lepsius – als Antwort der Richter auf die flächendeckende, präventive Überwachungspolitik verstanden werden. Allerdings berge die Begründung

eines Gewährleistungsrechts die Gefahr, dass der Schutzanspruch des Einzelnen unter einem „Gesellschaftsvorbehalt" gestellt werde. Gewährleistungsansprüche bemessen sich üblicherweise an funktionalen oder organisatorischen Bedingungen, die gesellschaftliche Freiheitsvorstellungen garantieren sollen. Wenn jedoch das individuelle Verhalten des Einzelnen nicht mit diesen objektiven Freiheitsbestimmungen übereinstimme, könnten die individuellen Freiheitsbelange zu kurz kommen und betroffene Bürger ihren Schutzanspruch nicht mehr wirksam einfordern, warnte Lepsius.

Ob die Entscheidung zur Online-Durchsuchung deshalb einen Gewinn für den Schutz der Privatsphäre bringen wird, lässt sich heute noch nicht abschätzen. Betrachtet man die Reaktionen der Politik auf das Urteil, sind Zweifel angebracht, ob der Gesetzgeber das neue Computer-Grundrecht angemessen ausfüllen wird. Umso mehr bedarf es jener Engagierten, die sich den Problemen einer datenschutzgerechten Technikentwicklung und der Medienbildung annehmen.

*Sven Lüders*
*ist Geschäftsführer der Humanistischen Union*

Eine Dokumentation aller Vorträge findet sich auf dieser Seite.

---