AJP/PJA 4/2008

Das Grundrecht auf Computerschutz

Axel Tschentscher,
Prof. Dr. iur., LL.M., Bern

Inhaltsübersicht

Ordinarius für Staatsrecht, Rechtsphilosophie und Verfassungsgeschichte an der Universität Bern. Mein Dank gilt Frau Dominika Blonski für Unterstützung bei den Recherchen zu diesem Beitrag.

Selbst in Verfassungsstaaten mit ausgebautem Grundrechtssystem erzwingt die Entwicklung der Technik einen fortwährenden Verfassungswandel. In seltenen Fällen kommt es dadurch zur Anerkennung neuartiger Grundrechte. Das deutsche Bundesverfassungsgericht hat in seiner jüngsten Rechtsprechung ein solches neues Grundrecht in das System des deutschen Grundgesetzes eingefügt. Das Grundrecht soll die Vertraulichkeit und Integrität von informationstechnischen Systemen garantieren, ist also ein spezifisches Schutzrecht für die Nutzung privater Computer (Computerschutzrecht). Reagiert wird damit auf gesetzgeberische Vorstösse zur staatlichen Ausspähung von Computern durch Infizierung mit versteckten Hintertüren (Trojanern). Das sind Methoden, deren sich der Staat bisher nicht bedient hat, die jetzt aber diskutiert und experimentell ausprobiert werden. Ungeachtet der rechtspolitischen Implikationen stellt sich grundrechtsdogmatisch die Frage, welche Schutzlücke hier durch Einsatz welchen Instrumentariums und mit welcher Wirkung gefüllt wird. Speziell für die Schweiz fragt sich, ob die Lage unter der Bundesverfassung vergleichbar ist und die Anerkennung des Computerschutzrechts auch hierzulande naheliegt. Das wäre die erste Neuentdeckung eines Grundrechts seit der Totalrevision der Bundesverfassung.

A. Die Anerkennung des neuen Computerschutzrechts

Der jüngste Entscheid des Bundesverfassungsgerichts[1] ist gleich zweifach aussergewöhnlich. Erstens haben die Beschwerdeführer erfolgreich die Nichtigerklärung einer Schlüsselnorm des reformierten Verfassungsschutzgesetzes in Nordrhein-Westfalen erreicht – mithin mehr, als in den Fällen verfassungskonformer Interpretation üblich ist. Und zweitens haben sie das Gericht dazu bewegen können, ein ganz neues Grundrecht zu entdecken. Das war zuletzt 1983 beim «Informationellen Selbstbestimmungsrecht» aus Anlass des Volkszählungsurteils[2] der Fall und kann folglich als äusserst seltenes Ereignis gelten. Das Gericht liefert damit in

[1] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370, 595/07 – Informationstechnische Systeme; zur Publikation in der amtlichen Sammlung vorgesehen; bisher publiziert unter <www.bverfg.de>. Vgl. aus der schweizerischen Presseberichterstattung dazu beispielsweise NZZ vom 28. Februar 2008, 1: Deutsche Hürden für Online-Durchsuchungen.

[2] BVerfGE 65, 1 – Volkszählung.

überraschender Eindeutigkeit einen neuen verfassungsrechtlichen Rahmen für die seit drei Jahren geführte Debatte über die politische Opportunität und verfassungsrechtliche Zulässigkeit internettechnischer Aufklärungsmassnahmen.[3]

I. Gefährdungslage

Nachdem der Bundesgerichtshof bereits entschieden hatte, dass den Strafverfolgungsbehörden für die Durchführung von Online-Durchsuchungen eine gesetzliche Grundlage in der Strafprozessordnung fehlt,[4] sind Gesetzesnovellen sowohl im Bund als auch in den Ländern diskutiert worden. Das Land Nordrhein-Westfalen preschte anlässlich der Revision seines Verfassungsschutzgesetzes vor und erliess die erste und bisher einzige ausdrückliche Ermächtigung zu Online-Durchsuchungen und -Überwachungen. Die vom Bundesverfassungsgericht für nichtig erklärte Bestimmung findet sich unter den Befugnisnormen dieses Gesetzes. Dort war neu vorgesehen:

> «(2) Die Verfassungsschutzbehörde darf ... zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Massnahmen anwenden: ...
>
> 11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel. ...»[5]

Diese Neuregelung umfasst mit der verdeckten Teilnahme und dem heimlichen Zugriff zwei gesonderte Eingriffstatbestände, die vom Bundesverfassungsgericht beide als verfassungswidrig erachtet wurden.[6] Unter einem heimlichen Zugriff auf informationstechnische Systeme muss man sich das unerkannte Eindringen mit nachfolgender Kontrolle über einen Personalcomputer, einen Laptop oder ein Smartphone vorstellen. Dazu können die Behörden wie Hacker unterschiedliche Mittel einsetzen: sie können unerkannte oder noch nicht beseitigte Sicherheitslücken ausnutzen, absichtlich von Programmierern eingebaute Hintertüren (Backdoors) verwenden oder sogar selbst solche Hintertüren durch eigene Spähprogramme installieren (Trojaner). Im Extremfall genügt eine E-Mail oder eine präparierte Webseite, zum Beispiel in der Online-Steuerverwaltung, um den Computer zugänglich zu machen; konventioneller ist die Installation von Überwachungssoftware anlässlich der heimlichen Installation von akustischen oder optischen Abhörsystemen in Wohnungen (Grosser Lauschangriff).

Wenn der private Computer erst einmal infiltriert ist, dann kann damit jede Nutzung des Geräts von aussen über das Internet beobachtet werden, ohne dass der Benutzer davon das geringste erfährt. Es ist sogar möglich, das Mikrofon im Computer heimlich einzuschalten und damit Gespräche abzuhören, die gar nicht als Telefonate über das Internet geführt werden – eine ferninstallierte Wanze sozusagen. Als durchaus beabsichtigte Konsequenz führt das zu einer umfassenden Überwachungs- und Ausforschungsmöglichkeit: Die Behörden können Tastenanschläge, Internetaktivitäten oder Bildschirminhalte mitprotokollieren, Passwörter ausspähen und Festplatteninhalte herunterladen. Zu den mittelbaren und nicht beabsichtigten Konsequenzen kann nach Auffassung der vom Bundesverfassungsgericht angehörten Experten allerdings auch gehören, dass Dritte den Mechanismus erfolgreich analysieren und sich dann die behördliche Hintertür für kriminelles Handeln zueigen machen. Ausserdem kann es je nach Ausgestaltung der Hintertür zu einer Unverträglichkeit mit einzelnen anderen Programmen kommen, was wiederum Funktionsstörungen und Datenverluste beim Benutzer befürchten lässt.

Eine besondere grundrechtliche Gefährdungslage ergibt sich für einzelne Berufsgruppen und Parteipolitiker, die durch ihre Tätigkeit zwangsläufig in den weiteren Bereich von Online-Überwachungen des Verfassungsschutzes geraten, selbst wenn sie persönlich nicht das direkte Ziel der Massnahmen sind. So verhielt es sich auch bei den Beschwerdeführenden. Die klagende Journalistin besuchte im Rahmen ihrer Recherchetätigkeit regelmässig die Online-Präsenzen von verfassungsfeindlichen Personen und Organisationen und nahm an Online-Diskussionen (Chats) teil, in denen auch Rechtsextremisten aktiv waren. Der beschwerdeführende Politiker, ein Mitglied der Partei Die Linke, war durch die gesetzliche Neuregelung persönlich betroffen, weil die gesamte Partei vom Landesverfassungsschutz überwacht

---

[3] Früh beispielsweise Manfred Hofmann, Die Online-Durchsuchung – staatliches «Hacken» oder zulässige Ermittlungsmassnahme?, NStZ 2005, 121 ff.; jüngere Beiträge von Johannes Rux, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden. Rechtsfragen der «Online-Durchsuchung», JZ 2007, 285 ff.; Maximilian Warntjen, Die verfassungrechtlichen Anforderungen an eine gesetzliche Regelung der Online-Durchsuchung, JURA 2007, 581 ff.; Markus Hansen/Andreas Pfitzmann, Online-Durchsuchung, DRiZ 2007, 225 ff.; Alexander Rossnagel, Verfassungspolitische und verfassungsrechtlich Fragen der Online-Durchsuchung, DRiZ 2007, 229 f.; zur Kritik insbesondere Ralph Neumann, Die elektronischen Schlapphüte kommen. Was soll, was kann und wozu nützt eine Online-Durchsuchung?, DRiZ 2007, 226; Christoph Braunbeck, Bundesrat gegen Online-Durchsuchungen privater Computer, DRiZ 2007, 231.

[4] BGHSt 51, 211 – Online-Durchsuchung. Vgl. aus der schweizerischen Presseberichterstattung dazu beispielsweise NZZ vom 6. Februar 2007, 2: Fahndungs-Fesseln für die deutsche Polizei. Einschränkendes Urteil des Bundesgerichtshofes in Karlsruhe.

[5] § 5 Absatz 2 Nummer 11 Satz 1 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG) in der Fassung des Gesetzes vom 20. Dezemer 2006, publiziert in: Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen, Jahrgang 2006, 620 ff.

[6] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 165.

wird. Schliesslich gehörten auch Rechtsanwälte, unter ihnen der ehemalige Bundesinnenminister Gerhard Rudolf Baum, zu den Beschwerdeführern. Sie machten eine besondere Betroffenheit geltend, weil es im Rahmen ihrer anwaltlichen Tätigkeit zu Kontakten mit Personen der Führungsebene der vom Verfassungsschutz überwachten PKK kommt. An diesen Beispielen zeigt sich bereits die erhebliche Streubreite der Überwachungsmassnahme. Wenn in einer Anwaltskanzlei nur ein einziges Mandat die Überwachung auslöst, ist gleichzeitig der Kontakt zu allen anderen Mandanten im Zugriff der Sicherheitsbehörden. Ausserdem öffnet eine Hintertür, die im Computer eines einzelnen Anwalts installiert wird, gleichzeitig den Zugang zu den vernetzten Kollegen der Kanzlei.

II. Öffentliches Interesse

Das erklärte Ziel des Bundeslandes Nordrhein-Westfalen ist die effektivere Terrorismusbekämpfung.[7] Hier versagen inzwischen die klassischen Kontrollmittel der Nachrichtendienste und Polizeibehörden, weil das Internet einfach zu bedienende und kostenlose Verschüsselungsmöglichkeiten für E-Mails (PGP) und Internettelefonate (Skype) bietet. Sogar das alltägliche Browsen im Web lässt sich ohne technische Finessen über verschlüsselte Zugangsvermittlungen (Proxies) abwickeln. Die Verschlüsselungstechnik kann mangels standardisierter Eigenschaften und behördlich erreichbarer Anbieter auch nicht kontrolliert beseitigt werden, wie das bei der Überwachung von Mobiltelefonen möglich ist. Selbst ein kooperationsbereiter Telekommunikationsanbieter kann den Sicherheitsbehörden gegen die private Verschüsselung nicht helfen. Das Abhören von Leitungen oder Datenanschlüssen ist dann unergiebig. Nur unmittelbar an den Computern der Kommunikationsteilnehmer ist der Datenstrom entschlüsselt verfügbar (Endgeräteüberwachung).[8] Installiert man in den Wohnräumen akustische und optische Überwachungsgeräte («Wanzen», Grosser Lauschangriff) und beschlagnahmt später die Festplatten, so ist diese «Offline-Überwachung» ein viel aufwendigeres Verfahren und zudem weniger wirksam als eine direkte Dauerüberwachung aller Kommunikationsvorgänge. Und die immer verbreitetere Internetkommunikation mit mobilen Geräten (Laptops, Smartphones) lässt sich durch stationär installierte Überwachungsgeräte überhaupt nicht abhören. Verständlich also, dass der heimliche Zugriff auf die Quellen der Telekommunikation (Quellen-Telekommunikationsüberwachung, Online-Durchsuchung) zu den neuen Begehrlichkeiten der Nachrichtendienste und Polizeibehörden gehört.

III. Nichtigerklärung

Das Bundesverfassungsgericht hat dem Überwachungsbegehren einen breit wirksamen Riegel geschoben, der kaum noch Raum für eine Realisierung der Computerinfiltration lässt. Das Computerschutzrecht darf nach dem zweiten Leitsatz des Entscheids nur eingeschränkt werden, wenn «tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen». Zu diesen überragend wichtigen Rechtsgütern gehören nach der Rechtsprechung des Gerichts Leib, Leben oder Freiheit von Personen sowie der Bestand des Staates und die Grundlagen der menschlichen Existenz – immerhin tatbestandliche Umschreibungen, die bei drohenden Terrorhandlungen gegen Menschen oder Umwelt einschlägig sind. Ausgeschlossen wird damit von vornherein der Einsatz von Online-Überwachungen oder -Durchsuchungen im Bereich der Vermögensdelikte.

Für die Konkretheit der Bedrohung müssen nach Auffassung des Gerichts mindestens «bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr» hinweisen. Ausserdem steht die Anordnung der Infiltration nach dem dritten Leitsatz des Gerichts unter dem Richtervorbehalt und das ermächtigende Gesetz muss Begleitmassnahmen vorsehen, mit denen der absolut geschützte Kernbereich privater Lebensgestaltung von beiläufiger Überwachung ausgenommen wird. Insoweit bietet der vor vier Jahren ergangene Entscheid des Bundesverfassungsgerichts über den Grossen Lauschangriff eine Parallele.[9] Entweder die Massnahme scheitert im Falle einer «negativen Kernbereichsprognose» bereits am richterlichen Bewilligungserfordernis, oder sie wird durch ständige inhaltliche Kontrolle begleitet und nötigenfalls mit der Löschung der versehentlich aufgezeichneten Daten beendet. Dadurch sollen tagebuchartige Notizen und die Gespräche mit Familienangehörigen und anderen Vertrauenspersonen (Seelsorger, Strafverteidiger, Arzt) von der Überwachung ausgenommen bleiben. Insgesamt belässt das Gericht den Behörden nur noch einen sehr schmalen Zielkorridor, in welchem bei ganz aussergewöhnlich intensiver Gefahr und mit sehr hohem Aufwand eine Online-Überwachung und -Durchsuchung realisiert werden darf.

B. Das neue Computerschutzrecht im System der Freiheitsrechte

Das Bundesverfassungsgericht kommt zu einem neuen Grundrecht, weil es eine Lücke im Schutzsystem der übrigen Freiheitsrechte ausmacht. Den erweiterten technischen

---

7 Vgl. BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 137, 143.

8 BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 11.

9 BVerfGE 109, 279 – Grosser Lauschangriff, insbesondere Leitsatz 5.

Eingriffsmöglichkeiten des Staates soll dadurch ein entsprechend erweitertes Grundrechtssystem gegenübergestellt werden. Dieser Schutzbereichsbestimmung sei im Folgenden nachgegangen, um anschliessend nach einer Parallelkonstellation im schweizerischen Verfassungsrecht zu fragen.

I. Allgemeines Persönlichkeitsrecht

Das schon früh aus einer Gesamtschau der Handlungsfreiheit und des Menschenwürdesatzes abgeleitete allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) bildet im System der grundgesetzlichen Freiheitsrechte einen Auffangschutzbereich, soweit der Schutz nicht durch spezifischere Garantien wie die Vertraulichkeit der Kommunikation oder den Schutz der Wohnung gewährleistet ist (Art. 10, 13 GG). Die lückenschliessende Gewährleistung soll nach ständiger Rechtsprechung diejenigen Elemente der Persönlichkeit schützen, die zwar nicht Gegenstand der besonderen Freiheitsgarantien sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit entsprechen.[10] Das allgemeine Persönlichkeitsrecht galt nach dieser Konzeption ursprünglich als ein «unbenanntes» Freiheitsrecht, das neben die «benannten» Freiheiten des Grundgesetzes tritt.[11] Inzwischen ist es sogar als selbständiges, wenn auch nach wie vor ungeschriebenes Grundrecht anerkannt.[12] Anders als das in Deutschland anerkannte Auffanggrundrecht der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) beschränkt sich das allgemeine Persönlichkeitsrecht nicht auf *aktive* Entfaltungsweisen der Persönlichkeit, ist insoweit also weiter. In anderer Hinsicht ist es enger, weil es nur einen Bereich der *engeren* Persönlichkeitssphäre schützt. Das allgemeine Persönlichkeitsrecht ist damit das Auffanggrundrecht für Fallgruppen mit intensiver Ingerenz. Das gilt für Schutzbegehren des grundlegenden Ehrenschutzes ebenso wie für die Eingriffe in das Recht auf informationelle Selbstbestimmung. Im Ergebnis hat das Gericht das neue Computerschutzrecht in Parallele zum allgemeinen Persönlichkeitsrecht entwickelt.[13]

II. Telekommunikationsgeheimnis

Das Grundrecht auf Schutz der Vertraulichkeit von Telekommunikation (Art. 10 Abs. 1 GG) soll auf die spezifischen Gefahren der räumlich distanzierten Kommunikation reagieren und beschränkt sich demgemäss auf die unkörperliche Übermittlung von Informationen an individuelle Empfänger. Wenn sich nach Abschluss der Kommunikation noch Daten im Herrschaftsbereich des Empfängers befinden, unterstehen diese dem räumlichen, nicht kommunikativen Grundrechtsschutz. Werden die Computer der Bürger als Ganze überwacht oder durchsucht, so unterliegt auch das übrige Arbeiten mit dem Gerät insgesamt der Beobachtung durch die Sicherheitsorgane. Folglich ist nur ein kleiner Teil der im Zugriff befindlichen Informationen durch das Telekommunikationsgeheimnis geschützt. Die Rede von einer «Quellen-Telekommunikationsüberwachung» ist insofern irreführend. Es wird durch die Infiltration – sei es bewusst, sei es unbewusst – sehr viel mehr überwacht als der eigentliche Vorgang der Telekommunikation. Entsprechend konstatiert das Bundesverfassungsgericht hier eine Schutzlücke.[14]

III. Unverletzlichkeit der Wohnung

Für die räumlich zuzuordnenden Informationen bietet sich ergänzend das Grundrecht auf Unverletzlichkeit der Wohnung an (Art. 13 GG). Es schützt diejenige räumliche Sphäre, die der Mensch als elementaren Lebensbereich für seine Persönlichkeitsentfaltung benötigt. Dringt der Staat mit akustischen oder optischen Abhöreinrichtungen in diesen Raum ein oder misst er Abstrahlung von Computern, die in einer Wohnung benutzt werden, so ist das Grundrecht betroffen. Damit wäre für die Standardfälle der Online-Überwachung und -Durchsuchung ein anschlussfähiger Schutzbereich gefunden. Trotzdem konstatiert das Bundesverfassungsgericht auch hier eine Schutzlücke. Denn die spezifische Gefährdung, die durch neue internetbasierte Überwachungstechniken für die Bürger entsteht, ist nicht deckungsgleich mit dem räumlichen Schutz der Wohnung. Sie ermöglicht dem Staat, unabhängig vom konkreten Standort der Computer, in diese einzudringen, also auch bei mobilen Geräten, die sich nur zeitweilig oder gar nicht in einer Wohnung befinden – das Gericht erwähnt als Beispiele die Laptops, Personal Digital Assistants (PDAs) und Mobiltelefone.[15]

IV. Schutz der Privatsphäre

Damit bleiben für die Verortung des Grundrechtsschutzes noch die spezifischen Ausdrucksformen des allgemeinen Persönlichkeitsrechts, die vom Bundesverfassungsgericht in seiner früheren Rechtsprechung bereits anerkannt worden sind. Anders als in der moderneren Bundesverfassung der Schweiz (Art. 13 BV) kennt das Grundgesetz keine geschriebene Garantie der Privatsphäre, so dass das Grundrecht als unbenanntes Freiheitsrecht unter dem allgemeinen Per-

---

[10] BVerfGE 54, 148 (153) – Eppler; 99, 185 (193) – Scientology; 101, 361 (380) – Caroline von Monaco II; 114, 339 (346) – Manfred Stolpe.

[11] BVerfGE 54, 148 (153) – Eppler.

[12] Horst Dreier, in: ders. (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl., 2004, Art. 2 I, Rz. 33, 68 ff. Zur Differenzierung siehe hinten C.III.

[13] Dazu im Detail hinten VI.

[14] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 187.

[15] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 194.

sönlichkeitsrecht anerkannt werden musste. Es bietet dem Grundrechtsträger einen räumlich und thematisch umrissenen Bereich, den er frei von unerwünschter Einsichtnahme halten kann, insbesondere frei von Einwirkungen der öffentlichen Gewalt.[16] Das unbefangene Verhalten wäre beeinträchtigt, wenn nicht die innerlichen Auseinandersetzungen, die man Tagebüchern oder Ehepartnern anvertraut, die Details der eigenen Sexualität oder der eigenen Krankheit vor den Augen Dritter verborgen blieben. Der Schutz des Grundrechts gilt nach neuester Rechtsprechung nicht nur für den häuslichen Bereich, sondern die Privatsphäre «folgt» dem Grundrechtsträger und bietet dadurch auch Handhabe gegenüber einer unbegrenzten Nachstellung durch Paparazzi.[17] Selbst Prominente, die sich freiwillig zu Personen des öffentlichen Lebens gemacht haben, müssen grundsätzlich die Möglichkeit behalten, sich in der abgeschiedenen Natur oder in abgeschiedenen Ortschaften frei zu bewegen, ohne dass Photojournalisten ihnen überall mit Teleobjektiven nachstellen. Insofern liegt zwischen dem früher anerkannten Privatsphären- und Wohnungsschutz ein ähnliches Verhältnis vor wie zwischen dem neuen Computer- und Wohnungsschutz: viele Fälle betreffen gleichzeitig den häuslichen Raum; und doch sind die Grundrechtsgefährdungen nicht deckungsgleich. Ein weiteres Argument belegt indes noch stichhaltiger die begrenzte Wirkungskraft des Privatsphärenschutzes gegenüber Online-Überwachung und -Durchsuchung: Viele Daten, die bei der Nutzung von Computern anfallen, betreffen thematisch nicht die Privatsphäre. Zwar mag der private Computer zunehmend auch als elektronisches Tagebuch verwendet werden, doch darin besteht nicht seine typischerweise zentrale Funktion.

V. Informationelles Selbstbestimmungsrecht

Damit bleibt schliesslich noch das Recht auf informationelle Selbstbestimmung, wie es das Bundesverfassungsgericht im Volkszählungsurteil anerkannt hat. Es geht über den Schutz der Privatsphäre hinaus, weil es nicht nur die persönlichkeitsnahen, sondern alle persönlichen Daten in die Verfügungshoheit des Grundrechtsträgers legt und so den besonderen Gefährdungen durch moderne Datenverarbeitung Rechnung trägt.[18] Weil die Bürgerinnen und Bürger durch dieses Recht selbst kontrollieren können, welche persönlichen Daten preisgegeben und verwendet werden, scheint damit für die Online-Überwachung und -Durchsuchung ein geeigneter Anknüpfungspunkt gefunden. Die Daten auf dem persönlichen Computer sind ja schon durch ihre Nutzung einem bestimmten Besitzer zugeordnet und somit als dessen persönliche Daten anzusehen, gleich ob sie besonders sensible oder alltägliche Inhalte zum Gegenstand haben. Der heimliche Zugriff auf persönliche Computer stellt sich dann stets als ein rechtfertigungsbedürftiger Eingriff in die grundrechtlich geschützte Befugnis dar, selbst zu entscheiden, wann und innerhalb welcher Grenzen man persönliche Sachverhalte offenbaren will.

Dem Bundesverfassungsgericht genügt diese bisherige Schutzmöglichkeit indes noch nicht. Das informationelle Selbstbestimmungsrecht weist nämlich nach Auffassung des Gerichts ein andersartiges Schutzprofil auf, als im Falle von Online-Überwachungen und -Durchsuchungen erforderlich ist. Es will verhindern, dass für sich genommen nicht besonders sensible Einzelinformationen durch die vielfältigen Datenverarbeitungsmöglichkeiten des Staates (oder auch Privater) zu weitergehenden Informationen über die Person kombiniert werden und dann dessen Geheimhaltungsinteressen und schliesslich sein unbefangenes Verhalten beeinträchtigen. Wenn sich der Staat hingegen Zugriff auf persönliche Computer verschaffe, stehe ihm direkt ein potentiell äusserst grosser und aussagekräftiger Datenbestand zur Verfügung, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmassnahmen angewiesen zu sein. Der Grundrechtsträger könne die Gefahr auch nicht mindern, weil er zu seiner Persönlichkeitsentfaltung heutzutage auf die Nutzung informationstechnischer Systeme angewiesen sei. Ein Zugriff auf persönliche Computer gehe darum in seinem Gewicht für die Persönlichkeit des Betroffenen weit über die einzelnen Datenerhebungen und -verwendungen hinaus, vor denen das Recht auf informationelle Selbstbestimmung schützt.[19]

VI. Das Computerschutzrecht

Da im bisherigen Schutzsystem der Grundrechte kein hinreichender Schutz vor Persönlichkeitsgefährdungen gewährleistet ist, die daraus entstehen, dass die Grundrechtsträger zu ihrer Persönlichkeitsentfaltung neuerdings auf die intensive Nutzung von Computern angewiesen sind, aktiviert das Bundesverfassungsgericht das allgemeine Persönlichkeitsrecht in seiner lückenfüllenden Funktion. Über die bisher anerkannten Gehalte hinaus wird ein selbständiges Freiheitsrecht auf «Integrität und Vertraulichkeit informationstechnischer Systeme» spezifiziert (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Es ähnelt dem Recht auf informationelle Selbstbestimmung, schützt aber auch insoweit, als der Staat persönliche Computer insgesamt kontrolliert, statt nur auf einzelne Kommunikationsvorgänge oder einzelne gespeicherte Daten zuzugreifen.

Diese Abgrenzung zum informationellen Selbstbestimmungsrecht zieht gleichzeitig eine Grenze des sachlichen

---

[16] Grundlegend BVerfGE 6, 32 (41) – Elfes; 27, 344 (350) – Ehescheidungsakten.

[17] BVerfGE 101, 361 (383 f.) – Caroline von Monaco II.

[18] Vgl. BVerfGE 65, 1 (43) – Volkszählung; 84, 192 (194) – Offenbarung der Entmündigung; 96, 171 (181) – Stasi-Fragen.

[19] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 200.

Schutzbereichs. Vom Computerschutzrecht sind solche Systeme, die lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthalten, nicht erfasst – etwa haustechnische Steuerungsgeräte oder einfache Telefone mit ihren Speicherinhalten.[20] Der prototypisch geschützte Gegenstand ist der heimische Personalcomputer und die ihm funktional verwandten Geräte, also Mobilcomputer (Laptop, PDA) und Mobiltelefone mit grossem Funktionsumfang (Smartphone). Abgrenzungsfragen wird man dadurch bewältigen können, dass nach der typischen Gefährdungsrichtung von Online-Überwachung und -Durchsuchung nur solche Geräte die nötige Persönlichkeitsnähe aufweisen, mit denen der Nutzer im Internet aktiv wird (Surfen, E-Mail oder IP-Telefonate). Nur hier stimmt das Argument des Gerichts, dass der Benutzer ohne Ausweichmöglichkeit auf das informationstechnische System angewiesen sei. Und nur hier besteht die neuartige Gefahr einer für den Staat besonders einfachen, weil *online* durchgeführten Überwachung oder Durchsuchung. Soweit sich die Internetnutzung dabei auf eine einzelne, bereits von klassischen Grundrechten geschützte Funktion beschränkt, fehlt es zudem an der grundrechtlichen Schutzlücke, weshalb hier allein das klassische Grundrecht einschlägig ist – so etwa bei dedizierten Internettelefonen (IP-Phone) das Telekommunikationsgeheimnis.

Der Schutz der so umrissenen informationstechnischen Systeme ist gegen die zwei Eingriffsmodalitäten der Vertraulichkeits- und der Integritätsverletzung gerichtet. Die grundrechtlich anzuerkennende Vertraulichkeitserwartung besteht darin, dass niemand während der Arbeit mit dem eigenen Computer virtuell über die Schulter schauen kann oder nachträglich auf die dadurch erzeugten Daten Zugriff nimmt, solange der Benutzer sie nicht explizit freigegeben hat. Etwas weniger griffig ist der Tatbestand der Integritätserwartung. Nach Auffassung des Gerichts liegt bereits dann ein Eingriff in die Integrität des informationstechnischen Systems vor, wenn der Staat eine Hintertür installiert, selbst wenn sich noch keine Beeinträchtigungen bei der Benutzung des Computers ergeben. Die Integritätsbeeinträchtigung liegt in diesen Fällen darin, dass die «Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden *können*».[21] Ein infiltriertes System ist ein in seiner Integrität beeinträchtigtes System, selbst wenn es aus Sicht des Benutzers weiterhin unverändert funktioniert.

Interessanterweise unterscheidet das Bundesverfassungsgericht weder in der Begründung noch in den Kriterien zwischen solchen Hintertüren, die als eine Infizierung *online* zum Benutzer gelangen, und anderen, die anlässlich eines physischen Eindringens der Sicherheitsbehörden in die Wohnung auf konventionelle Art installiert werden. Die Gleichsetzung ist nicht ganz selbstverständlich, denn die Installation in Hackermanier, das heisst ohne Eindringen in die Wohnung, ist für staatliche Behörden so viel einfacher als die klassische Vorgehensweise, dass sich die reale Gefährdung für Grundrechtsträger durch diese Option erheblich intensiviert. Auslöser der rechtspolitischen Diskussion war darum auch die *online* ausgelöste Überwachung und Durchsuchung. Wird aber eine Hintertür *offline* installiert und danach *online* genutzt, stellt sich für den Grundrechtsträger die Lage im praktischen Ergebnis gleichartig dar. In beiden Fällen ist seine Systemintegrität und die Vertraulichkeit vollständig und andauernd beeinträchtigt. Die für nichtig erklärte Regelung in Nordrhein-Westfalen enthielt keine Bestimmung über die Art der Installation, sondern regelte nur den heimlichen Zugriff über das Internet – gleichgültig, wie es dazu kommt. Es ist darum konsequent, wenn das Bundesverfassungsgericht zur Art der Installation keine weiteren Unterscheidungen trifft.

C. Der Grundrechtsschutz in der Schweiz

Bisher führt man die Diskussion zu Online-Überwachung und -Durchsuchung in der Schweiz noch nicht vergleichbar heftig wie in Deutschland, doch finden sich in den Reformvorschlägen zum Gesetz über die innere Sicherheit bereits erste Anhaltspunkte, dass die neuen Instrumente auch hierzulande Platz greifen und dann eine entsprechende Gefährdungslage für die Grundrechtsträger auslösen werden. Der Gesetzgebungsprozess wurde bereits durch kritische Stimmen begleitet.[22] In Österreich ist die Entwicklung weiter fortgeschritten – dort gibt es die praktische Anwendung von Online-Eingriffen schon heute.[23] Angesichts der annähernd synchron verlaufenden Entwicklung zwischen den deutsch-

---

[20] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 202 f.

[21] BVerfG 1 BvR 370, 595/07 – Informationstechnische Systeme (FN 1), Rz. 204; Hervorhebung hinzugefügt, A.T.

[22] Beispielsweise durch den Datenschutzbeauftragten Hans-Peter Thür, Interview «Gefährlicher als die Fichenaffäre», St. Galler Tagblatt vom 21. Februar 2006, 7: «Wird dieses Gesetz eingeführt, drohen sehr massive Eingriffe in die Privatsphäre und die Persönlichkeitsrechte jedes Einzelnen, ohne dass man dem Betroffenen einen konkreten Verdacht auf das Begehen einer strafbaren Handlung zur Last legen könnte.» Ausserdem Philipp Mäder, Der falsche Weg für mehr Schutz vor Terror, Tages-Anzeiger vom 8. Juli 2006, 9, der für eine Verortung der Eingriffsbefugnisse im Strafgesetzbuch plädiert.

[23] Der so genannte Terrorparagraph des Strafgesetzbuches (§ 278b), der zu Online-Ermittlungsmethoden der Polizei ermächtigt, wurde zur Abhörung des Internet- und E-Mail-Verkehrs eingesetzt und hat zu gerichtsverwertbaren Beweisen geführt; siehe die Berichterstattung in der NZZ vom 14. März 2008, 5: Unbedingte Strafen im Wiener Terrorprozess. Islamistisches Ehepaar als Überzeugungstäter verurteilt; zur Vorgeschichte ausserdem NZZ vom 26. September 2007, 2: Engagierte Grundrechtsdebatte in Österreich. Heikle DDR-Analogie des Präsidenten des Verfassungsgerichts.

sprachigen Rechtsordnungen ist es naheliegend, für die grundrechtlichen Schutzbereiche der Bundesverfassung zu fragen, ob analog zum Befund des Bundesverfassungsgerichts auch in der Schweiz mit den fortgeschrittenen staatlichen Eingriffsmöglichkeiten eine Schutzlücke entstehen wird, die durch Anerkennung eines neuen Grundrechts zu füllen wäre.

I. Gefährdungslage

Mit den Anschlägen auf das World Trade Center am 11. September 2001 hat sich das schon zuvor anerkannte und im Bundesgesetz über die Massnahmen zur Wahrung der inneren Sicherheit (BWIS)[24] konkretisierte Bedürfnis nach durchgreifenden Handlungsvollmachten für Sicherheitsorgane nochmals intensiviert. Die Revision BWIS-II sieht im neuen Abschnitt über die besonderen Mittel der Informationsbeschaffung unter anderem eine Erweiterung mit folgendem Wortlaut vor:

> *«Art. 18m Geheimes Durchsuchen eines Datenverarbeitungssystems*
>
> Lassen konkrete und aktuelle Tatsachen oder Vorkommnisse vermuten, dass ein mutmasslicher Gefährder oder eine mutmassliche Gefährderin ein ihm oder ihr zur Verfügung stehendes und gegen Zugriff besonders gesichertes Datenverarbeitungssystem benutzt, kann dieses vom Bundesamt durchsucht werden. Die Durchsuchung kann ohne Wissen des mutmasslichen Gefährders oder der mutmasslichen Gefährderin erfolgen.»[25]

Die Botschaft zum Revisionsvorschlag weist – ähnlich wie die Begründung des Landes Nordrhein-Westfalen zu der vom Bundesverfassungsgericht für nichtig erklärten Bestimmung – darauf hin, dass die Überwachung durch Sicherheitsbehörden wegen des verbreiteten Einsatzes von Verschlüsselungstechniken erschwert wird.[26] Selbst dort, wo ein Eindringen in passwortgeschützte Bereiche möglich wäre, sei dies, so die Botschaft, bisher durch strafrechtliches Verbot ausgeschlossen (Art. 143bis StGB Unbefugtes Eindringen in ein Datenverarbeitungssystem). Mit der neuen Eingriffsbefugnis werde dieser Verbotstatbestand überwunden, so dass zukünftig auch nichtöffentliche Websites und Chaträume sowie andere passwortgeschützte Bereiche der Überwachung zugänglich würden. Eine «Durchsuchung» im Sinne der Norm ermächtigt dabei nicht zu solchen Infiltrationstechniken, die Funktionsstörungen oder Datenverluste zur Folge haben.

Die Formulierung des vorgeschlagenen Artikels lässt offen, ob mit dieser Norm auch zur Online-Überwachung und -Durchsuchung ermächtigt werden soll. Immerhin könnte die Befugnis auch mit klassischer Technik sinnvoll durchgeführt werden – etwa durch die Einsichtnahme in verschlüsselte Computerdaten anlässlich einer Wohnungsdurchsuchung. Für eine Ermächtigung zur Online-Kontrolle spricht einerseits, dass die Massnahmen «ohne Wissen» des Grundrechtsträgers, also heimlich, durchgeführt werden dürfen. Das ist gerade ein Charakteristikum der über das Internet ausgeführten Überwachung und Durchsuchung. Ausserdem wird die von der Botschaft nur oberflächlich wiedergegebene rechtspolitische Reformdiskussion in der Presse schon länger direkt mit der Infiltration durch Trojaner in Verbindung gebracht.[27] Laut diesen Presseberichten experimentiert der Dienst für besondere Angelegenheiten (DBA) des Justiz- und Polizeidepartements sogar schon zu Testzwecken mit dieser Technik. Realistischerweise wird man darum den neuen Artikel so lesen müssen, dass er – wenn auch mit geringer Normenklarheit – auch zu Online-Überwachung und -Durchsuchung ermächtigen soll.

II. Schweizerischer Grundrechtsschutz gegen Online-Eingriffe

1. Persönliche Freiheit (Art. 10 Abs. 2 BV)

In der schweizerischen Grundrechtsordnung bildet das Recht auf persönliche Freiheit die Grundgarantie des verfassungsrechtlichen Persönlichkeitsschutzes. Deren wichtigste Komponente, die körperliche Integrität, hatte das Bundesgericht als ungeschriebenen Teilgehalt der persönlichen Freiheit anerkannt, bevor er mit der Totalrevision als besonderer Schutzgegenstand ausdrücklich festgehalten wurde.[28] Neben den weiteren spezifisch geschützten Teilgehalten der geistigen Unversehrtheit und der Bewegungsfreiheit bleibt für die persönliche Freiheit ein Grundtatbestand, der sich deutlich von demjenigen des deutschen Persönlichkeitsschutzes unterscheidet. Er umfasst nämlich nur die elementaren Erscheinungen der Persönlichkeitsentfaltung und schützt somit keine allgemeine Handlungsfreiheit.[29] Für den Schutz gegen Online-Überwachung und -Durchsuchung stellt dieser Unterschied indes keine Hürde dar, denn die heutzutage besonders persönlichkeitsnahe Nutzung privater Computer

---

[24] SR 120, Gesetz vom 21. März 1997, massgeblich geändert durch eine Reform gegen Gewalt bei Sportveranstaltungen vom 24. März 2006, aktueller Stand: 1. Januar 2008.

[25] Entwurf zur Änderung des BWIS vom 15. Juni 2007, BBl 2007 5139, 5148 f.

[26] Botschaft zur Änderung des BWIS vom 15. Juni 2007, BBl 2007 5037, 5109 f.

[27] Siehe Jean François Tanda, Trojaner schnüffeln für den Schweizer Staatsschutz. Bei Ermittlungen können Computer ausspioniert werden, SonntagsZeitung vom 14. Oktober 2007, 7. Vgl. ausserdem die frühe Berichterstattung in NZZ Online vom 19. August 2005, Das neue Arsenal der Staatsschützer. Der Gesetzesentwurf zur Stärkung der inneren Sicherheit, sowie die politischen Zielvorstellungen am 5. April 2007, Leitplanken für den «Lauschangriff». Auftrag an das EJPD zur Ausarbeitung einer Botschaft; beides dokumentiert unter <www.nzz.ch>.

[28] BGE 89 I 93 E. 3 S. 97 f. – Blutuntersuchung.

[29] BGE 122 I 360 E. 5a S. 362 f. – VPM-Fichen; 123 I 112 E. 4a S. 118 – Organtransplantation Genf.

lässt sich zu den elementaren Erscheinungen der Persönlichkeitsentfaltung zählen. Die grundrechtliche Beurteilung kann im Ausgangspunkt an die Entscheide des Bundesgerichts über erkennungsdienstliche Massnahmen anknüpfen. Unter Rückgriff auf frühere Entscheide zu Einzelaspekten hatte das Gericht dort den umfassenden Grundrechtsschutz der Bürgerinnen und Bürger als «Anspruch auf eine persönliche Geheimsphäre» qualifiziert und dem Grundrecht auf persönliche Freiheit zugeordnet.[30] Inzwischen sind für den Schutz der Privatsphäre im Allgemeinen (Art. 13 Abs. 1 BV) und den Schutz der persönlichkeitsbezogenen Daten im Besonderen (Art. 13 Abs. 2 BV) allerdings schon wieder spezifischere Grundrechtstatbestände gebildet, die, soweit im Schutzbereich einschlägig, dem Recht auf persönliche Freiheit vorgehen. Der Blick auf die Entwicklung des Persönlichkeitsrechts zeigt allerdings, dass die persönliche Freiheit von jeher als ein Generator von Grundrechtsschutz gegen neuartige Bedrohungen der Persönlichkeit verstanden wurde. Insofern erfüllt das Grundrecht – ähnlich dem allgemeinen Persönlichkeitsrecht und der allgemeinen Handlungsfreiheit in der deutschen Grundrechtssystematik – eine *Auffang- und Reservefunktion*.

2. Schutz von Kommunikationsgeheimnissen (Art. 13 Abs. 1 BV)

Mit der neuen Bundesverfassung ist die Achtung der Vertraulichkeit des Fernmeldeverkehrs nunmehr umfassend geregelt, statt den Grundrechtsschutz an einzelne Formen (Postsendungen, Telegramme, Telefonate) anzuknüpfen. Demgemäss sind auch beliebige neue Formen der Fernkommunikation mitgeschützt, was das Bundesgericht für E-Mails bereits ausdrücklich bestätigt hat.[31] Entsprechend unterliegen auch Internettelefonate, gleich ob verschlüsselt oder unverschlüsselt, dem grundrechtlichen Vertraulichkeitsprinzip – und zwar (selbstverständlich) auf beiden Seiten der Kommunikationsleitung.[32] Das Vertraulichkeitsgebot gilt sowohl für den Inhalt als auch für die so genannten Randdaten über formelle Umstände der Kommunikation (Zeitpunkt, Dauer, Anschluss- oder Teilnehmeridentifizierung).[33]

Wenn durch Online-Überwachung die mittels persönlicher Computer geführte individuelle Fernkommunikation für die Sicherheitsbehörden mithörbar oder protokollierbar wird, liegt folglich ein Eingriff in den Grundrechtsschutz des Kommunikationsgeheimnisses vor. Ausserdem ist, wenn nach Abschluss des Kommunikationsvorgangs im Wege der Online-Durchsuchung auf die lokal gespeicherten Repräsentationen des Kontakts, etwa auf E-Mail-Texte oder auch nur auf Kontaktlisten für Internettelefonate, zugegriffen wird, ebenfalls ein Eingriff in das Grundrecht gegeben. Der Schutz ist zudem ortsunabhängig, wirkt also auch für Kommunikation, die von mobilen Internetgeräten aus geführt wird. Gleichwohl ist er auf einen typischerweise sehr kleinen Ausschnitt der gesamten Computernutzung beschränkt. So ist die nichtindividuelle Internetkommunikation, etwa die Speicherung und der Abruf aus geschützten Foren, ebensowenig erfasst wie die lokale Nutzung zur Vorbereitung von Kommunikation, etwa wenn ein Flugblatt oder ein Brief auf dem Computer geschrieben wird, um dann später ausgedruckt und konventionell verbreitet zu werden. Ganz ausserhalb des Schutzbereichs bleiben die solipsistischen Kommunikationsformen, beispielsweise die Erstellung von Notizen, Arbeitslisten oder Tagebucheinträgen. Insgesamt kann der Schutz des Kommunikationsgeheimnisses darum nur einen kleinen Teil der Ingerenzen abdecken, die durch Online-Überwachung und -Durchsuchung entstehen.

3. Schutz der Wohnung (Art. 13 Abs. 1 BV)

Während das Kommunikationsgeheimnis funktionalen Schutz bewirkt, ist der Wohnungsschutz räumlich radiziert. Die Norm schützt in erster Linie das Hausrecht der Grundrechtsträger, das diese einer staatlichen Durchsuchung entgegensetzen können. Die unter engen Voraussetzungen anerkannten Hausdurchsuchungen erfolgen regelmässig in Gegenwart des Bewohners. Demgegenüber sind Online-Durchsuchungen typischerweise heimlich und beschränken sich nicht auf den räumlichen Bereich einer Wohnung oder Geschäftsstätte, sondern folgen dem Grundrechtsträger an alle Orte, an denen er mit seinen persönlichen Computern und Kommunikationsgeräten einen Internetzugang aktiviert. Die Online-Durchsuchung ist in Umfang und Wirkungsweise andersartig als die Wohnraumdurchsuchung. Schon aus diesem Grund ist der Schutzanteil, der durch den Wohnungsschutz vermittelt wird, für die Problematik der Online-Eingriffe insgesamt nicht relevant.

4. Schutz des Privatlebens (Art. 13 Abs. 1 BV)

Die Achtung des Privatlebens bildet unter den Schutzbestimmungen der Privatsphäre den am allgemeinsten gehaltenen Schutzbereich. Alle Lebenssachverhalte, die der Einzelne als Privatsache ansieht und von der Öffentlichkeit abschirmen möchte, fallen darunter. Sogar bei einem Auftreten in der Öffentlichkeit muss der Grundrechtsträger nicht davon ausgehen, unter fortwährender Beobachtung zu stehen, sondern hat ein berechtigtes Interesse daran, mit seiner Lebensweise

---

30 BGE 122 I 360 E. 5a S. 361 ff. (362) – VPM-Fichen m.w.N.
31 BGE 126 I 50 E. 6a S. 65 – Swiss Online.
32 BGE 122 I 182 E. 4b S. 189 – Mitbenützerüberwachung.
33 BGE 126 I 50 E. 6b S. 66 – Swiss Online. Anders insoweit die deutsche Schutzbereichssystematik, nach der die Randdaten (in Deutschland: «Verbindungsdaten») dem Informationellen Selbstbestimmungsrecht, nicht dem Kommunikationsgeheimnis zugeordnet sind: BVerfGE 115, 166 (181 ff.) – Verbindungsdaten.

grundsätzlich unerkannt und undokumentiert zu bleiben.[34] Bei der Online-Überwachung ist diese Ortsunabhängigkeit besonders augenfällig. Es kann für die Schutzbedürftigkeit nicht darauf ankommen, ob der Computerbenutzer eine Notiz in den heimischen Personalcomputer tippt oder ob er dasselbe unterwegs mit dem Mobiltelefon erledigt; in beiden Fällen wäre staatliche Überwachung eine gleich intensive Beeinträchtigung des Anspruchs auf Anerkennung des Privatlebens. Und doch bleiben Zweifel, ob der Schutz des Privatlebens in ausreichender Breite dem Phänomen der Online-Überwachung Rechnung tragen kann. Anknüpfungspunkt ist ja jeweils die besondere Persönlichkeitsnähe: die Zuordnung des Lebenssachverhalts zu einer Intim- oder jedenfalls Geheimsphäre. Unter den Tätigkeiten, die mit persönlichen Computern ausgeführt werden, sind die ihrem Inhalt nach vertraulichen aber nur ein Ausschnitt. Viele andere Aktivitäten würde der Benutzer genauso in einem öffentlichen Internetcafé mit Einsichtnahmemöglichkeit anderer Besucher ausführen. Derlei Nutzungsweisen gehören für sich genommen nicht zum Geheimbereich. Und doch hat der Benutzer ein berechtigtes Interesse daran, dass diese Einzelnutzungen nicht permanent staatlich mitverfolgt und zu einem persönlichen Nutzungsprofil kombiniert werden. Schon allein der Modus der Online-Überwachung begründet eine neue grundrechtliche Gefährdungslage, die durch den konventionellen Schutz des privaten Geheimbereichs nicht vollständig erfasst wird.

5. Schutz vor Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV)

Der grundrechtliche Schutz persönlichkeitsbezogener Daten hat sich aus dem Auffangtatbestand der persönlichen Freiheit heraus zur Selbständigkeit entwickelt. So war die Veröffentlichung der Namen von Verlustscheinschuldnern im kantonalen Amtsblatt noch als Verletzung der persönlichen Freiheit qualifiziert worden, bevor dann das informationelle Selbstbestimmungsrecht als eigenständiger Ausdruck des Grundrechtsschutzes in Lehre und Rechtsprechung anerkannt wurde, was wiederum in die gesonderte Schutzregelung der neuen Verfassung mündete (Art. 13 Abs. 2 BV).[35] Heute schützt diese Bestimmung die Befugnis des Grundrechtsträgers, selbst darüber zu bestimmen, wem er wann und in welchem Umfang persönliche Daten, Meinungen, Gedanken und Empfindungen anvertrauen möchte.[36] Der Fokus liegt dabei im einzelnen Datum und seinem Kontext. Entsprechend orientiert sich die Eingriffsrechtfertigung ebenfalls an einer Begründung, für welche Zwecke welche persönlichkeitsbezogenen Informationen erhoben, gesammelt, verarbeitet, aufbewahrt und weitergegeben werden dürfen. Das dürfte zwar im Ergebnis sämtliche Daten, die auf einem persönlichen Computer anfallen, erfassen, denn diese erlangen ihren besonderen Persönlichkeitsbezug ja dadurch, dass sie überhaupt auf einem persönlichen Gerät zu finden sind. Doch ist die Schutzperspektive eine andere als die Gefährdungsperspektive. Es geht beim Datenschutz letztlich um eine Abschichtung der Inhalte nach ihrer Sensibilität. Dagegen sind Online-Überwachung und -Durchsuchung gerade deshalb ein intensiver Eingriff, weil sie unabgrenzbar die gesamte Computernutzung erfassen. Ausserdem dient der Datenschutz, wie im Begriff «informationelle Selbstbestimmung» treffend ausgedrückt, der Autonomie des Grundrechtsträgers bei der Gestaltung des Bildes, das Dritte von ihm haben sollen: er schafft sich positiv selbst. Die Computerüberwachung greift hingegen viel mehr als diese Selbstbestimmung an; sie richtet sich zunächst wahllos gegen alles, was mit einem Computer gemacht werden kann, sei es nun höchstpersönlich, politisch, erzieherisch, beruflich oder anders ausgerichtet.

6. Bedürfnis nach einer neuartigen Schutzrichtung

Ein einzelnes Grundrecht kann der neuartigen Grundrechtsgefährdung, die sich durch staatliche Online-Überwachung und -Durchsuchung ergibt, nicht umfassend begegnen. Dadurch droht das Entstehen von Schutzlücken. Selbst wenn man die Massnahmen an einem relativ intensiv gegen Eingriffe geschützten Grundrecht wie dem Kommunikationsgeheimnis orientiert,[37] bleibt das spezifisch Neue der Gefährdung unberücksichtigt. Es liegt in der überschiessenden Kontrolle, die geradezu zwangsläufig bei einer Überwachung persönlicher Computer entsteht: ihre Ausdehnung auf unverdächtige Dritte, auf andere Computer im Netzwerk, auf nichtkommunikative Daten, auf höchstpersönliche Informationen (Krankheitsdaten, Tagebuchaufzeichnungen, Liebesbriefe), auf besonders vertrauensbedürftige Kommunikationsinhalte (Seelsorge, Rechtsberatung). Das Neue der Gefährdung liegt ausserdem in der zusätzlichen Ingerenz durch allgemeine Integritätsbeeinträchtigung: in den möglichen Funktionsstörungen durch Wechselwirkung mit anderen Computerprogrammen, in der Unberechenbarkeit des heimlichen Datentransports durch das Internet, in der Ausnutzbarkeit

---

[34] Walter Kälin/Regina Kiener, Grundrechte, Bern 2007, 148; Rainer J. Schweizer, § 43 Verfassungsrechtlicher Persönlichkeitsschutz, in: Daniel Thürer u.a. (Hrsg.), Verfassungsrecht der Schweiz, Zürich 2001, 691 ff., 702.

[35] Vgl. zur Entwicklung BGE 107 Ia 52 E. 3c S. 57 – Fruchtlose Pfändung; 122 I 153 E. 6b.aa S. 162 – Klinik Schlössli Oetwil.

[36] Siehe dazu Jörg Paul Müller, Grundrechte in der Schweiz. Im Rahmen der Bundesverfassung von 1999, der UNO-Pakte und der EMRK, 3. Aufl., Bern 1999, 45 – unter Rückgriff auf die frühe Entwicklung eines «Right to Privacy» in den Vereinigten Staaten von Amerika.

[37] So geplant für die «besonderen Mitteln der Informationsbeschaffung» nach BWIS-II; vgl. Botschaft BWIS-II (FN 26), 5105 ff.

staatlicher Hintertüren durch Dritte. Der Grundrechtsschutz sollte darum bei Online-Eingriffen zu einem neuen und eigenständigen Schutzprofil fortentwickelt werden. Nur fragt sich, wie ein solches Grundrecht auf Computerschutz systematisch einzuordnen wäre.

Eine Möglichkeit zeichnet sich in der Botschaft zur Reform des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit ab. Dort wird allgemein von einem Recht auf Privatsphäre und dessen Beeinträchtigung gesprochen, so als gäbe es in Artikel 13 BV zusätzlich zu den Einzelgewährleistungen noch einen Grundtatbestand, der als Auffanggrundrecht dienen könnte.[38] Das ist pragmatisch vorteilhaft, grundrechtsdogmatisch allerdings problematisch, weil dann die Argumentationsformen und Grenzziehungen, die für die Einzelgrundrechte entwickelt wurden, in der Diffusität eines Gesamtschutzbereichs unterzugehen drohen. Immerhin wäre für Online-Eingriffe eine umfassende Kategorie gefunden, denn unter dem einen oder anderen Gesichtspunkt lassen sich alle dadurch ausgelösten Beeinträchtigungen als solche der Privatsphäre verstehen. In diese Richtung geht die Botschaft, wenn sie zugesteht, in der neuen Überwachungsmassnahme liege eine «schwerwiegende Einschränkung der Privatsphäre».[39] Offen bleibt dabei allerdings die Frage, ob man ein Grundrecht auf Computerschutz nicht nur als subsidiären Privatsphärenschutz, sondern als neuen eigenständigen Schutzgehalt systematisch begründen kann.

III. Grundrechtsdogmatische Einordnung neuer Schutzgehalte

Deutsche und schweizerische Grundrechtsdogmatik sind in der Vergangenheit unterschiedliche Wege gegangen, wenn neue Schutzgehalte in die Grundrechtssystematik einzuordnen waren. In der Schweiz gibt es eine lange Tradition der Anerkennung ungeschriebener Grundrechte. Die deutsche Lehre und Rechtsprechung kennt einerseits solche echten rechtsschöpferischen Neuheiten, spricht aber zusätzlich gern von normtextlich unbenannten Freiheitsrechten (Innominatfreiheitsrechten), wenn es um die Anerkennung einzelner Schutzgehalte in ihrer Besonderheit und Eigenständigkeit geht. Beide Ansätze ergänzen sich und können alternativ für den Grundrechtsschutz der Computerintegrität fruchtbar gemacht werden.

1. Anerkennung als ungeschriebenes Grundrecht

Unter der Bundesverfassung von 1874 hat das Bundesgericht den schweizerischen Grundrechtsschutz durch Anerkennung ungeschriebener Grundrechte vorangetrieben. In der Begründungsweise nahm es insbesondere solche Schutzgehalte als ungeschriebene Grundrechte an, die für die Ausübung der anderen, bereits ausdrücklich in der alten Bundesverfassung geschützten Freiheiten unentbehrlich sind. Dabei half jeweils der Blick auf die jüngeren kantonalen Grundrechtsordnungen. So wurde etwa die persönliche Freiheit im Sinne physischer Freiheit anlässlich der Pflichtuntersuchung im Vaterschaftsprozess als ein notwendiges Korrelat anderer Freiheiten eingestuft, weshalb das Recht auf körperliche Unversehrtheit zu den ungeschriebenen Freiheitsrechten zähle.[40] Die Geltungskraft solcher Freiheiten stünde derjenigen geschriebener Verfassungsrechte in nichts nach; sie bildeten «einen unentbehrlichen Bestandteil der rechtsstaatlichen Ordnung des Bundes.»[41] Weitere Argumente für eine Anerkennung ungeschriebener Grundrechte waren der «allgemeine Konsens» in der Rechtsgemeinschaft sowie die Überzeugung, dass ein Schutzgehalt «unentbehrlicher Bestandteil eines rechtsstaatlichen und demokratischen Gemeinwesens» sei.[42] Noch früher hat das Gericht in sehr allgemeiner Weise auf die «dem modernen Staate *sich selbst gegenüber* bestehende, unmittelbar aus der eigenen Zweckbestimmung entspringende Pflicht» abgestellt.[43]

Aus diesem Repertoir an Gründen vermag allenfalls der erste Ansatz für ein Grundrecht auf Computerschutz taugen. Denn das Vertrauen in die Integrität persönlicher Computer und Mobilgeräte nimmt eine Schlüsselstellung in der modernen Kommunikation ein. Ohne einen wirksamen Schutz müssten die Bürger, selbst wenn der tatsächliche Umfang von Online-Eingriffen gering sein sollte, ein wegen möglicher Drittbetroffenheit für den einzelnen nicht kalkulierbares Risiko staatlicher Computerüberwachung annehmen. Daraus folgt ein «chilling effect» für die Computernutzung insgesamt und mittelbar eine Beeinträchtigungen der Meinungsäusserungsfreiheit sowie aller politischen und sogar kommerziellen Aktivitäten, weil hier regelmässig das Bedürfnis nach qualifizierter Vertraulichkeit besteht. Das ungeschriebene Grundrecht auf Computerschutz liesse sich darum als notwendiges Korrelat anderer Grundrechte begründen und würde dann neben die geschriebenen Teilgehalte des Privatsphärenschutzes in Artikel 13 BV treten.

---

38 Tatsächlich wird man die persönliche Freiheit (Art. 10 Abs. 2 BV) als Auffangtatbestand auch für den Schutz der Privatsphäre ansehen müssen; vgl. KÄLIN/KIENER (FN 34), 163; im Ergebnis auch STEFAN BREITENMOSER, in: BERNHARD EHRENZELLER u.a. (Hrsg.), Die schweizerische Bundesverfassung, Kommentar, Zürich/St. Gallen 2002, Art. 13, Rz. 4 f., 9, 22, der allerdings erwägt, dass sich der Anspruch auf Achtung der Privatsphäre in Anlehnung an Art. 8 EMRK zu einem allgemeinen Auffangrecht entwickeln könnte.

39 Botschaft BWIS-II (FN 26), 5110; ebenso für die Fernmeldeüberwachung sowie für die akustische und optische Überwachung in privaten Räumen: Botschaft BWIS-II (FN 26), 5106, 5108.

40 BGE 82 I 234 E. 3 S. 237 f. – Vaterschaftsprozess.

41 BGE 89 I 93 E. 3 S. 98 – Blutuntersuchung.

42 BGE 121 I 367 E. 2b S. 371 – Existenzsicherung.

43 BGE 40 I 409 E. 2 S. 416 – Mittellose Ausländer.

2. Anerkennung als unbenanntes Freiheitsrecht

In der deutschen Grundrechtsdogmatik ist die rechtsschöpferische Anerkennung völlig neuer Grundrechte als ungeschriebene Garantien selten. Die wenigen Fälle, in denen das Bundesverfassungsgericht zu diesem Mittel griff – allgemeines Persönlichkeitsrecht, informationelles Selbstbestimmungsrecht und nun das Computerschutzrecht – stützen sich bezeichnenderweise auf eine unspezifische Kombination der grossen Allgemeinplätze des Grundgesetzes (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: Freiheit und Würde). Häufiger wurde ein anderer Weg beschritten: die Anerkennung unbenannter Freiheitsrechte (Innominatfreiheitsrechte), etwa bei der Vertragsfreiheit, der Ausreisefreiheit und dem sexuellen Selbstbestimmungsrecht. Unter der Rechtskategorie der «unbenannten» Freiheitsrechte versteht man die tatbestandlich eigenständige Herauskristallisierung von Teilgehalten der allgemeinen Handlungsfreiheit als gesonderte Schutzrichtungen, wenn auch nicht selbständige Grundrechte.[44] Nun kennt die schweizerische Grundrechtsordnung keine allgemeine Handlungsfreiheit. Gleichwohl gibt es das Bedürfnis, eigenständige Schutzgehalte unterhalb der Stufe selbständiger Grundrechte anzuerkennen, beispielsweise bei der Demonstrationsfreiheit, auf die anlässlich der Totalrevision der Bundesverfassung als selbständiges Grundrecht bewusst verzichtet wurde, die sich aber in der Herauskristallisierung einer typischen Schutzbereichs- und Einschränkungsdogmatik weitgehend eigenständig gegenüber den beteiligten Einzelgrundrechten entwickelt. In solchen Fällen ist es auch in der Schweiz sinnvoll, ein *normtextlich unbenanntes Freiheitsrecht* anzunehmen, statt jede Eigenständigkeit terminologisch zu meiden.[45] Dieser Schritt öffnet langfristig die Tür zu einer verstärkten Typisierung und Grundrechtsrationalität.

Für das Grundrecht auf Computerschutz lässt sich die Kategorie unbenannter Freiheitsrechte ebenfalls fruchtbar machen. Damit wäre tatsächlich weniger beansprucht, als das Bundesverfassungsgericht für Deutschland judiziert hat (selbständiges Freiheitsrecht), aber immerhin mehr, als mit einem isolierten Schutz gegenüber einzelnen Beeinträchtigungsformen der Online-Eingriffe erreicht werden kann. Das Grundrecht auf Computerschutz wäre auf Dauer als eigenständige Schutzrichtung des Auffanggrundrechts der persönlichen Freiheit (Art. 10 Abs. 2 BV) anerkannt.[46] Seine Besonderheit besteht dann darin, unterschiedliche Aspekte des Privatsphärenschutzes (Art. 13 BV) zusammen mit den nicht privatsphärenrelevanten elementaren Interessen an der Computernutzung zu einer neuen grundrechtlichen Schutzrichtung zu bündeln. Die für dieses Grundrecht zu entwickelnden Abwägungsgesichtspunkte würden in ihrer Eigenständigkeit auf die neue Gefährdungslage angepasst. Das muss nicht automatisch zu einem intensiveren Grundrechtsschutz im Ergebnis führen, denn auch auf der Seite des öffentlichen Interesses an der Computerüberwachung kann die technische Entwicklung abwägungsrelevante Neuheiten bieten. Im Vergleich zu einem Grundrechtsschutz, der jede Einzelbeeinträchtigung nach unterschiedlichen Normen abwickelt, würde aber jedenfalls die grundrechtliche Reflexion der neuartigen Gefährdungslage verbessert.

Le 27 février, la Cour constitutionnelle allemande a déclaré nulle la première base légale introduite en Allemagne pour la perquisition et la surveillance en ligne. Le tribunal constatait dans ce jugement de principe que le système de protection de la loi fondamentale présentait des lacunes en raison des nouvelles possibilités techniques de surveillance par l'Etat.

Le tribunal a comblé ce vide en reconnaissant un nouveau droit fondamental à «l'intégrité et la confidentialité des systèmes d'information». Bien que la protection des droits fondamentaux reconnus par la Constitution fédérale suisse ait d'autres limites et un texte normatif plus moderne que la constitution allemande en matière de protection de la sphère privée, il est nécessaire de définir dans notre pays également une nouvelle protection face à la surveillance en ligne par l'Etat. Il suffirait de développer la notion de liberté non écrite afin d'établir un droit fondamental autonome à la protection de l'ordinateur en tant qu'expression spécifique de la liberté personnelle.

(trad. LT LAWTANK, Fribourg)

---

[44] Vgl. die Systematisierung bei Dreier (FN 12), Rz. 33 ff.

[45] Axel Tschentscher, Glaubens- und Gewissensfreiheit sowie Kommunikationsgrundrechte, gemeinsam mit: Walter Kälin/Regina Kiener/Markus Müller/Pierre Tschannen, Die staatsrechtliche Rechtsprechung des Bundesgerichts in den Jahren 2006 und 2007, ZBJV 143 (2007), 683.

[46] Zum Auffangcharakter des Grundrechts auf persönliche Freiheit siehe BGE 127 I 6 E. 5a S. 12 – Basler Zwangsmedikation: «Grundgarantie zum Schutze der Persönlichkeit».