BÜRGERRECHTE

Information, Kontrolle und Privatheit

Winfried Hassemer

Derzeit ereignen sich im Bereich staatlicher Informationseingriffe tiefgreifende und dramatische Entwicklungen: Einerseits wächst das Kontrollbedürfnis, andererseits entwickelt sich die Informations-Technologie rasant und schafft neue Möglichkeiten und Kapazitäten.*

Polizeiliche Verbrechensprävention und Strafverfahren sind derzeit sinnfällige Beispiele, um die Nachdrücklichkeit der staatlichen Kontrollbedürfnisse zu illustrieren. Aus dem strafrechtlichen Ermittlungsverfahren geht es insbesondere um die folgenden Eingriffsinstrumente, die in jüngster Zeit eingerichtet beziehungsweise erweitert worden sind oder mit deren Einführung zu rechnen ist: der sogenannte Lausch- und der Spähangriff, die Rasterfahndung, die Telefonüberwachung, die langfristige polizeiliche Observation oder der Einsatz verdeckter Ermittler.

Diese Beispiele haben eine überraschend große Zahl von Gemeinsamkeiten. Sie stammen nicht nur alle aus der jüngsten Zeit und beziehen sich sämtlich auf das strafrechtliche Ermittlungsverfahren. Viel aussagekräftiger für eine Beurteilung der Situation, in der wir uns derzeit befinden, sind drei weitere Übereinstimmungen:

Diese Ermittlungsmethoden bedienen sich sämtlich informationsbeschaffender Mittel (und typischerweise informationstechnischer Einrichtungen), was man von den klassischen Ermittlungsmaßnahmen wie ärztlicher Untersuchung, Untersuchungshaft, Durchsuchung oder Beschlagnahme keineswegs sagen kann. Sie geschehen geheim und sind auf Geheimhaltung ihres Einsatzes zwingend angewiesen; wenn der Geheimnischarakter aufgehoben wird, funktionieren sie nicht mehr; die herkömmlichen Ermittlungsmethoden ereignen sich hingegen typischerweise im Angesicht des Betroffenen (was diesen beispielsweise in Stand setzt, sich darauf einzustellen, daß er beobachtet wird – ein Umstand, der vom Strafverfahrensrecht auch gebilligt, ja begrüßt wird). Sie richten sich nicht nur auf den Beschuldigten, sondern typischerweise auch, ohne daß man es technisch vermeiden kann, notwendigerweise auf unbeteiligte Dritte: den Telefonpartner, das mitbeobachtete Umfeld des Verdächtigen, andere Personen, die in der Rasterfahndung zufällig dieselben Merkmale aufweisen wie die gesuchte Person.

Ich diskutiere hier nicht, ob diese Reformen gute oder schlechte Kriminalpolitik sind, das ist nicht mein Thema an dieser Stelle. Ich will mit diesen Beispielen nur darauf aufmerksam machen, was passiert. Die Kontrollbedürfnisse führen zu einem qualitativ anderen Ermittlungsverfahren. Insbesondere was den Geheimcharakter der neuen Ermittlungsmethoden und damit im Strafprozeß die Unmöglichkeit angeht, sich auf der Stelle darauf einzurichten und sich dagegen zu wehren, weil man nichts davon bemerkt, und vor allem was die Einbeziehung Dritter in den informationellen Eingriff angeht und damit die Entwertung des Tatverdachts als Eingriffsschwelle im strafrechtlichen Ermittlungsverfahren: dies sind schwerwiegende und folgenreiche Veränderungen des Strafverfahrens.

Risikogesellschaft

In diesen Verfahrensänderungen liegt freilich nicht das eigentliche Problem. Für die Kontrollbedürfnisse des Staates und deren Befriedigung über Informationstechnologien bedeutend wichtiger ist eine Veränderung im Verhältnis von Bürger und Staat. Es ist nämlich keineswegs so, daß in der Sicht der Bürger dieses Informationseingriffe des Staates seien, gegen die man sich zur Bewahrung bürgerlicher Freiheiten wehren muß. Diese Informationseingriffe werden von den Bürgern vielmehr durchaus verstanden und gebilligt als Kampf des Staates gegen eine gemeinsame Bedrohung: organisierte Kriminalität, Korruption, Terrorismus, Kinderschändung et cetera.

Ich glaube, wir sehen den informationshungrigen, den strafenden Staat, zumindest zur Zeit, nicht mehr als den Leviathan an, nicht mehr als den, den man an die Kette der Gesetze legen muß, sondern vor allem als einen möglichen Verbündeten im Kampf gegen Risiken. »Tausche Freiheit gegen Sicherheit« ist heutzutage eine treffende Bezeichnung der Einstellung der Bürger zu Informationseingriffen des Staates. Hier vollziehen sich wichtige gesellschafts- und staatspolitische Veränderungen, welche keineswegs auf Normen beschränkt sind, sondern die Köpfe und Herzen der Menschen ergreifen.

Dies hat mit unserem Umgang mit Risiken zu tun. Hier ist der Begriff der »Risikogesellschaft« von Ulrich Beck aussagekräftig. Ich beziehe mich auf dieses Konzept: Wir erfahren täglich, daß wir mit Risiken konfrontiert sind, deren Umfang und deren Einzelheiten wir nicht ermessen können und die wir nicht beherrschen können; treten sie ein, verheeren sie alles. Wir sehen uns in einer Situation, in der wir mit dem Rücken zur Wand stehen. In einer solchen Situation ist es schwierig, der Bevölkerung den Sinn der Grund- und Freiheitsrechte zu vermitteln. Will man vor allem Sicherheit und Risikobeherrschung, dann ist das Konzept »Tausche Freiheit gegen Sicherheit« rational. Genau dazu paßt die neue Informations- und Kommunikationstechnologie, die eine solche Beherrschung verspricht.

* Bei diesem Beitrag handelt es sich um einen Ausschnitt aus einem Vortrag aus der »2. Christian-Broda-Vorlesung«, einer jährlich vom VBSA (Verein für Bewährungshilfe und soziale Arbeit) sowie vom Institut für Rechts- und Kriminalsoziologie organisierten Veranstaltung. Sie wurde heuer am 18.3. in Wien abgehalten. Der vollständige Vortrag und die Diskussionsbeiträge werden demnächst in einer Broschüre abgedruckt werden, die bei den Veranstaltern bezogen werden kann.

Technologien

I. Akten

Die staatliche Verwaltung hatte ihr Wissen herkömmlich vor allem in Akten aufbewahrt. Akten sind gekennzeichnet durch zwei Eigenschaften: Chaos und Vergessen. Manches, das in Akten gespeichert ist, bleibt auch dort, weil man es nämlich später nicht mehr findet, wenn man es braucht. Der Grund dafür ist nicht Schlampigkeit oder Borniertheit der Aktenführung, sondern die Natur der Sache:

Es stellt sich beispielsweise immer wieder heraus, daß man gewisse Informationen, die man unter einem bestimmten Aspekt gesammelt und geordnet hat, nun plötzlich unter einem anderen Aspekt sehen muß. Wenn die Akten nach Aspekt A geordnet wurden, läßt sich eine Ordnung nach Aspekt B nicht oder jedenfalls nicht mühelos organisieren. Bisweilen ist auch nicht ganz klar, was der früher wohldefinierte »Aspekt A« in einem neuen Einzelfall konkret bedeuten mag: wie man jetzt suchen muß. Und überdies gibt es natürliche Grenzen hinsichtlich der Menge der in Akten einstellbaren Informationen: räumliche, zeitliche, menschliche. Chaos und Vergessen, im menschlichen Alltag bisweilen durchaus hilfreich, haben jedenfalls für eine Verwaltung eindeutig negative Konnotationen.

II. Automatisierung

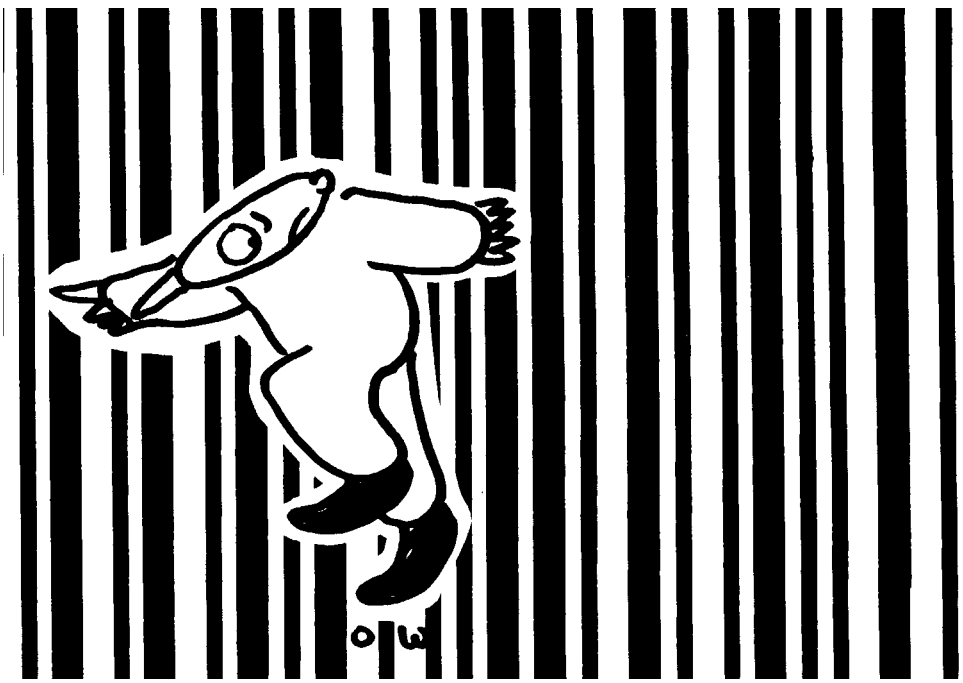
Die moderne, die automatisierte Datenverarbeitung konnte und kann demgegenüber dreierlei: Sie kann fast unendlich viele Daten verarbeiten; sie hat einen Hunger, der sich praktisch niemals stillen läßt. Sie kann darüber hinaus alle Daten, derer sie habhaft wird, sortieren und so ordnen, daß man sie sicher wiederfindet. Das ist schon ein kleines Wunder, daß sich Daten, die man bereits in ein bestimmtes System gebracht hat, auch unter veränderten Gesichtspunkten vollständig wiederfinden lassen. Das dritte Merkmal bedingt eine neue Qualität der Datenverarbeitung. Es läßt zu, daß man Dateien miteinander abgleicht, etwa auf der einen Seite die Sozialdateien einer Stadt (die darüber informieren, wer Sozialhilfe bekommt) und auf der anderen Seite die Dateien der Kfz-Halter (die darüber informiert, wer immerhin so viele Mittel hat, um sich ein Auto leisten zu können). Ich brauche Ihnen nicht zu sagen, sondern mit diesem Beispiel nur anzudeuten, daß da gewaltige Erkenntnisgewinne winken.

III. Netze und Verwandtes

Modernste Technologien von Kommunikation und Information können aber noch viel mehr als das. Sie sind bald für fast alle Menschen bezahlbar und für Laien gut zugänglich. Frühere Möglichkeiten, die Folgen einer Datenverarbeitung gering zu halten, weil man sehr viel finanzielle Mittel aufwenden und gut ausgebildet sein mußte, spielen heute keine Rolle mehr. Man kann Informationen auf kleinstem Raum speichern. An der Chip-Karte kann man die revolutionäre Entwicklung in der Datenverarbeitung sehen. Es gibt neue intelligente Technologien, die für viele Konstellationen unseres Alltags große Bedeutung haben können und haben werden:

So können etwa biometrische Verfahren individuelle Merkmale der Hand oder des Auges für Kontrollinteressen nutzen, sogar ohne daß die Betroffenen es bemerken. Wir hatten in der Bundesrepublik eine Auseinandersetzung, welche die Datenschützer vorerst gewonnen haben, welche sie am Ende aber vermutlich verloren geben müssen. Es ging um die Erhebung einer Maut auf den Autobahnen und um die Verfahren zur Feststellung der Erhebungsvoraussetzungen im Einzelfall. Diese Verfahren hätten zu einer permanenten elektronischen Kontrolle des gesamten Autobahnverkehrs führen können – technisch ein durchaus lösbares Problem.

Denken Sie auch an die sogenannte Kryptographie; ich werde heute noch zweimal darauf zurückkommen (G.I.3., G.II.4.). Sie befindet sich derzeit in einer rasanten Entwicklung. Kryptographie ist die Technik, Informationen zu verschlüsseln und sie nur bestimmten Berechtigten zu öffnen. Sie ist Voraussetzung gesicherter und vertrauensvoller Kommunikation in ansonsten offenen Netzen – also Voraussetzung beispielsweise einer auch ökonomischen Nutzung des Internet. Diese intelligente Verbindung von Feuer und Wasser wird nicht nur für die miteinander kommunizierenden Menschen, sondern auch für die wirtschaftliche Entwicklung der modernen Staaten von großer Bedeutung sein. Ein kryptographischer Anwendungsfall ist die sogenannte Steganographie, also die Kunst, Informationen – beispielsweise in übertragenen Bildern – so zu verstecken, daß der Betrachter nicht einmal auf die Idee kommen kann, daß hier etwas an ihm vorbei kommuniziert wird. Es bedarf keiner großen Phantasie, um solchen Verfahren lukrative Anwendungen vorherzusagen.



»In der modernen Kommunikationstechnologie ist auf die Abwesenheit des Staates kein Verlaß; das wäre schon angesichts der virulenten staatlichen Kontrollbedürfnisse eine naive Erwartung«

IV. Privatheit?

Das alles sind freilich bloße – wenn auch beeindruckende – Einzelheiten. Wichtiger ist, was hinter diesen Einzelheiten steht. Dieses Allgemeine ist nichts Geringeres als eine Umwälzung unseres kommunikativen Verhaltens.

Denken Sie dabei an die riesigen, fast sternenweiten Kommunikationsräume, die bereits existieren, insbesondere an das Internet. Diese Kommunikationsräume haben weitreichende Konsequenzen. Die Informationen lösen sich von ihrem Träger ab und werden damit zu einer

Weise von Kommunikation, wie sie die Menschheit bis jetzt noch nicht gekannt hat. Wer Informationen ausgesendet hat, ist – wenn nicht besondere Verfahrensarten angewendet werden – nicht als Sender identifizierbar. So gibt das Internet beispielsweise die Möglichkeit zu ganz wunderbaren und neuartigen Rollenspielen.

Der Staat ist bei diesen neuen Informationstechnologien nicht mehr anwesend. Ein Teil ihres Reizes liegt deshalb wohl auch gerade in ihrer Verheißung der Grenzenlosigkeit und Freiheit des Privaten. Das heißt freilich nicht, daß die

»Wir sehen den informationshungrigen, den strafenden Staat, zumindest zur Zeit, nicht mehr als den Leviathan an, nicht mehr als den, den man an die Kette der Gesetze legen muß«

modernen Kommunikationsräume Freiheitsräume sind – fast im Gegenteil:

In der modernen Kommunikationstechnologie ist auf die Abwesenheit des Staates kein Verlaß; das wäre schon angesichts der virulenten staatlichen Kontrollbedürfnisse eine naive Erwartung. In der Sache ist wichtig, daß bei der Nutzung der modernen Technologien von Information und Kommunikation eine große Menge personenbezogener Daten anfällt und auch ohne große Mühen vorgehalten und abgerufen werden kann: über Kreditwürdigkeit, über Gesundheit, Reiseverhalten, Kaufstile, sexuelle Orientierung, Mediennutzung. Diese Daten sind ökonomisch hoch interessant, sie werden verkauft, sie werden zusammengeführt, sie können vernetzt und abgeglichen werden. Man darf sicher sein, daß diese Datenverarbeitung weltweit aus einem ökonomischen Interesse heraus bereits eingerichtet ist.

Man darf aber auch sicher sein, daß, wenn man diese Datenverarbeitung einrichtet, der Staat von einem Zugriff auf die so verarbeiteten Daten nicht abgehalten werden kann, wenn er den Zugriff (etwa über das Mittel der Beschlagnahme) nach seiner Ansicht braucht. Auch wenn der Staat in der modernen Kommunikationsverarbeitung mit bloßem Auge nicht sichtbar ist, folgt daraus nicht, daß für die Privatheit keine Gefahr mehr bestünde. Sowohl der Staat als auch die datenverarbeitenden privaten Stellen bleiben bedrohlich, ja sie sind für die Privatheit vermutlich noch bedrohlicher, weil ihr Wirken nicht sichtbar ist, weil es nicht als bedrohlich auffällt.

Konsequenzen

Daraus folgt zuerst einmal, daß die alten Konzepte des Schutzes von Privatheit oder des Schutzes von personenbezogenen Daten nicht mehr greifen. Ich möchte ein paar dieser Konzepte näher beleuchten und Ihnen sagen, warum sie nicht mehr funktionieren.

1. Private Datenverarbeitung

Wenn es nicht mehr nur der Staat ist, der die Privatheit der Bürgerinnen und Bürger in bezug auf ihre informationelle Selbstbestimmung bedroht, wenn vielmehr die Datenverarbeitung in den Händen mächtiger Privater dezentral und vernetzt ein zumindest gleich intensives Bedrohungspotential aufgebaut hat, dann kommen wir – jedenfalls in der Bundesrepublik – mit unserem Verfassungsverständnis in Schwierigkeiten.

Unser Verständnis von Datenschutz folgt, wie ich das vorgetragen habe, dem Verständnis der klassischen Grundrechte als Abwehrrechte gegen den Staat, Abwehrrechte gegen private Datenverarbeitung und gegen private Datenzusammenführung sind hingegen nicht so einfach zu konzipieren. Damit ist das Problem einer Drittwirkung von Grundrechten angesprochen, womit, grob gesagt, gemeint ist: Die Privaten sollen sich untereinander – jedenfalls normalerweise – nicht auf Grundrechte berufen. Sie sollen sich auf ihre Privatautonomie berufen, sie sollen diese realisieren und dabei ihre Rechte gegenüber den anderen Privaten verfolgen und sichern.

Bei Grundrechten hingegen denken wir herkömmlich an Unterordnungsverhältnisse, an eine Institution, welche über dem einzelnen ist, welche bedrohlich ist und Verletzungskapazitäten hat, die dem Privaten gegenüber dem Privaten eigentlich nicht zur Verfügung stehen. Dieses Verständnis von Grundrechten trifft jedenfalls im Bereich der Informationstechnologien die Realität nicht mehr. Hier sind Bedrohungs- und Verletzungskapazitäten in großem Umfang in private Hände geraten.

2. Rechtfertigende Zustimmung

Auch das klassische Legitimationskonzept für informationelle Eingriffe funktioniert nicht mehr.

Die Vorstellung, wonach derjenige, der einem Eingriff aus freien Stücken zustimmt, sich über den Eingriff dann nicht beschweren darf (»Volenti non fit injuria«), war und ist eine sinnfällige Rechtfertigungsfigur, welche der autonomen Person das Recht auf folgenreiche Teilnahme in Staat und Öffentlichkeit einräumt und sie damit ernst nimmt. Im Bereich der neuen Informationstechnologien hat diese Figur ihre rechtfertigende Kraft verloren. Ich möchte Ihnen das am Beispiel der Gesundheitskarten zeigen.

Das sind Chips mit außerordentlich hoher Verarbeitungskapazität. Auf diesen Chips stehen personenbezogene Daten intimsten Charakters wie Krankheiten oder Medikamentenbehandlung. Nun stellt sich die Frage, ob die Bürgerin und der Bürger das Recht hat zu sagen, daß er oder sie eine solche Karte nicht haben will. Wenn die tatsächliche Entwicklung so ist, wie ich sie erwarte, daß nämlich 99 Prozent der Leute solche wunderbaren Chips haben wollen, dann hat das verbleibende eine Prozent zwar theoretisch das Recht, die Karte zurückzuweisen, aber praktisch keine Chance, mit diesem Recht auch im Alltag vernünftig zurechtzukommen. Dieses eine Prozent von Menschen kommt in eine Situation, in der es nicht mehr gleichberechtigt agieren kann, es sei denn formal; es ist marginalisiert, spielt keine Rolle, kann bei künftigen Entwicklungen technologisch und ökonomisch vernachlässigt werden.

In dieser Situation wäre es lebensfremd und rechtlich unbegründet, die 99 Prozent, welche sich gegen eine Gesundheitskarte nicht zur Wehr setzen, mit der Rechtsfigur zu konfrontieren, sie hätten der Datenverarbeitung auf ihrer Karte in Inhalt und Verfahren zugestimmt, weil sie die Karte für sich akzeptiert haben. Offenkundig gibt es Massenprozesse, denen Menschen sich nur deshalb einreihen, weil außerhalb des großen Stroms schmerzliche Vereinzelung droht, nicht aber deshalb, weil sie dem zustimmen, was im Strom sich ereignet. Konkret: Wer die Zustimmung der Menschen als Rechtfertigungstopos gegenüber Eingriffen retten will, kann sich nicht schlicht und abstrakt auf die Tatsache stützen, daß der Mensch sich gegen den Eingriff nicht gewehrt hat, sondern muß konkret nach Handlungsalternativen fragen und nach technologischen Möglichkeiten suchen, welche die Ebene einer vernünftigen Konkretisierung erreichen und dem Problem gerecht werden. Ich komme darauf zurück.

3. Eingriffsrechte in Netzen

Auch die Eingriffsrechte des Staates gegenüber privater Kommunikation kommen mit den neuen Technologien von Kommunikation und Information schnell an ein konzeptionelles Ende. Ihre Durchsetzung muß neu durchdacht werden. Dieses Problem wird derzeit unter dem Begriff »Kryptokontroverse« diskutiert.

Mit diesem Begriff ist folgende Situation bezeichnet: In offenen Netzen läßt sich folgenreich und ernsthaft nicht kommunizieren, wenn man nicht die Chance hat, bestimmte Informationen zu verschlüsseln. Das gilt nicht nur für Beispiele wie den Bankenbereich; es gilt für alle Informationen, die nicht nur Geschwätz sind. All diese Bereiche können im Internet nicht funktionieren, wenn nicht die Möglichkeit der Kryptographie besteht, also die Möglichkeit, die Informationen ausschließlich demjenigen zugänglich zu machen, an den sie sich richten.

Solange und soweit das Internet Schwatzbude ist, spielt Kryptographie keine Rolle. Soweit die Netze aber ein Instrument gezielter Information und Kommunikation sind, entsteht ein dringen-

der Bedarf an kryptographischen Verfahren, die es mittlerweile in großer Anzahl und guter Qualität gibt. Daraus entsteht die Kryptokontroverse.

Die Kryptokontroverse wird um nichts Geringeres geführt als um das Überleben der staatlichen Eingriffsrechte in Kommunikation. In ihr steht nicht der normative Bestand dieser Rechte zur Diskussion, sondern die faktische Möglichkeit, die Rechte zu realisieren.

Wenn es den Bürgern, die in den Netzen kommunizieren, ermöglicht wird, ihre Nachrichten zu verschlüsseln, dann können Sie den Lauschangriff, die Telefonüberwachung und alle Informationseingriffe des modernen Staates vergessen. Denn der Staat kommt an die so verschlüsselten Informationen nicht heran, sie sind auch ihm gegenüber kryptograph. Die Kryptokontroverse besteht deshalb, von der anderen Seite her betrachtet, in der Frage: Hat der Staat das Recht, seine Rechte auf den Informationseingriff, die ihm ja gesetzlich verbürgt sind, dadurch durchzusetzen, daß er kryptographische Verfahren jedenfalls teilweise und insoweit verbietet, als er selbst von ihnen betroffen ist?

Schon die Fragestellung ist neu und für ein juristisches Denken beunruhigend. Es geht um eine seltene Kombination empirischer und normativer Faktoren: Daß der Staat die Eingriffsrechte hat, steht aufgrund der gesetzlichen Erlaubnisse außer Streit. Streitbefangen ist nur die Frage, ob eine faktische Entwicklung die normative Situation ihrerseits definieren und die gegebenen Rechte aushebeln kann beziehungsweise – anders formuliert – welche Kosten in Kauf zu nehmen sind, damit der Staat seine normativen Befugnisse zum Eingriff auch unter veränderten faktischen Durchsetzungsbedingungen wahrnehmen kann.

In meinen Augen ist diese Frage derzeit offen. Ich glaube, daß technisch noch nicht das letzte Wort gesprochen ist. Auch hier fände ich eine Entweder-oder-Lösung (wie schon bei der Gesundheitskarte) nicht akzeptabel: entweder Kryptographie zugunsten staatlicher Eingriffsrechte ganz zu verbieten oder sie trotz staatlicher Eingriffsrechte unbegrenzt zuzulassen.

4. Strafbarkeit in Netzen

Das letzte Konzeptproblem, das ich hier vorstellen möchte, ist die Strafbarkeit von Informationen in Netzen und deren Verfolgung. Vor allem an Pornographie und Nazi-Parolen im Internet ist dieses Problem bei uns diskutiert worden.

Auch beim materiellstrafrechtlichen Aspekt verhält es sich im Ausgangspunkt nicht anders als beim verfahrensrechtlichen der staatlichen Eingriffsbefugnisse: Es geht nicht um die Rechtsprobleme im strengen Sinn, sondern vielmehr um die Implementation des Rechts. Die materielle Strafbarkeit steht nicht in Frage. Die fraglichen Verhaltensweisen sind im Internet genauso verboten wie außerhalb.

Das neue Problem an dieser Stelle lautet: Wen mache ich haftbar? Den Menschen, welcher die strafbaren Informationen in das Netz gebracht hat, kann ich durchaus nicht aus normativen, zumeist aber aus faktischen Gründen nicht haftbar machen: den finde ich fast nie. Darf ich folglich den Provider haftbar machen, also denjenigen, der die Brücke darstellt zwischen dem, der kommuniziert, und dem Netz?

Die Haftung der Provider ist kriminalistisch ein naheliegender, strafrechtlich aber ein zumindest dornenvoller Ausweg. In Frage käme im Notfall nur eine Unterlassenshaftung, weil der Provider nicht eingeschritten ist. Diese aber setzt so etwas wie eine gesteigerte Schutzpflicht für die gefährdeten Rechtsgüter voraus, eine Garantenpflicht, und die ist nicht so einfach zu begründen. Bezieht sie sich auf schlechthin alles, entsteht sie erst dann, wenn der Verantwortliche schon einmal aufgefallen und deshalb verwarnt worden ist? Was muß der Provider alles tun, damit er die vielen Ströme an Informationen, die durch ihn ins Internet gehen und vielleicht gefährlich sind, tauglich überwachen kann? Im Zweifelsfall kann er dies nicht. Was ist mit dem Verletzungsvorsatz angesichts der Informationsflut? Welche rechtfertigende Rolle spielt das Grundrecht der Meinungs- und Informationsfreiheit?

Man schätzt, daß es nur ungefähr zwei Prozent der Informationen im Internet gibt, die in dieser Weise gefährlich sind. Man muß aufpassen, daß man die Gewichte nicht falsch setzt und daß man das Augenmaß behält.

Prof. Dr. Winfried Hassemer
ist Richter am Bundesverfassungsgericht