## Humanistische Union

# Wer sein Privatleben schützen will, ist verdächtig - Zum § 129a-StGB-Verfahren gegen Andrej Holm und andere

Grundrechte-Report 2008, Seite 42

Das Grundrecht auf informationelle Selbstbestimmung umfasst die Befugnis des Einzelnen, selbst zu entscheiden, wann und wem er zu welchem Zweck personenbezogene Daten offenbart. Ausfluss dieses Rechts sind beispielsweise die vielfältigen datenschutzrechtlichen Regelungen, die vorschreiben, unter welchen Voraussetzungen personenbezogene Daten erhoben und verarbeitet werden können. Individueller Datenschutz kann aber auch bedeuten, sich und seine Daten dadurch zu schützen, dass man vermeidet, überhaupt Datenspuren und Informationen zu hinterlassen. In Zeiten von Internet-Diensten, die jederzeit den Standort eines x-beliebigen Mobilfunkgerätes anzeigen können, von Hacker-Angriffen auf Computer-Netzwerke, von Firmen, die mit der Weitergabe von Kundendaten Geld verdienen, und den vielfältigen Formen des Daten-Phishings sind Daten vermeidende und Daten schützende Verhaltensweisen dringend notwendig. Viele Menschen nutzen daher Verschlüsselungssoftware für ihren Email-Verkehr. Der Einsatz von Anonymisierungsdiensten ermöglicht es darüber hinaus, sich unerkannt durch das Internet zu bewegen. Das Erstellen von Kundenprofilen kann dadurch vermieden werden, dass an der Kasse mit Bargeld statt mit Karte bezahlt wird.

Problematisch wird es hingegen dann, wenn der (unberechtigte) Zugriff auf die persönlichen Daten nicht durch Private, sondern durch staatliche Organisationen erfolgt - zumal der Staat hierbei vermehrt anlassunabhängig vorgeht: Mit der Gesundheitskarte, auf der Daten über die persönliche Krankheitsgeschichte gespeichert werden sollen; mit der Vorratsspeicherung von Telekommunikationsdaten, die es jederzeit ermöglicht, umfassende Persönlichkeitsprofile über die Betroffenen erstellen zu lassen; oder mit der biometrischen Kennung in Reisepässen. Vor diesem Hintergrund scheint es verständlich, wenn Menschen selber darüber bestimmen wollen, ob und wenn ja, wem man wann welche persönlichen Informationen gegenüber bekannt gibt.

## Datenschutz wird zur Konspiration

In den in Berlin geführten Verfahren gegen Andrej Holm u. a. wegen Mitgliedschaft in einer terroristischen Vereinigung (§ 129a StGB) namens „militante gruppe“ wurde den Beschuldigten der (bewusste oder unbewusste) Schutz ihrer persönlichen Daten zum Verhängnis. In den seitens der Bundesanwaltschaft angestrengten Verfahren wurde den Beschuldigten u. a. vorgeworfen, dass sie zu bestimmten Treffen oder Spaziergängen ihre Handys nicht mitgenommen hätten oder, wenn doch, dann nur im ausgeschalteten Zustand. Dies entspräche, so der Vorwurf, „den typischen Gepflogenheiten der linksextremen Szene zum Zwecke der Konspiration“. Verdächtig sei es auch, wenn am Telefon nicht über Politik gesprochen oder eine Verabredung nicht mit Ort und Zeit genau umschrieben werden würde, wenn anonyme Email-Accounts zur Kommunikation eingesetzt werden oder wenn man sporadisch Emails von einem Bekannten mit Links zu Internet-Seiten erhält, die sich mit neuen technischen Möglichkeiten staatlicher Überwachung und Verschlüsselungssoftware befassen.

Diese Argumentation kommt nicht von ungefähr. Die Betroffenen wurden monate-, zum Teil sogar jahrelang komplett überwacht. Die Handys und Festnetzanschlüsse der Betroffenen wurden abgehört, der gesamte Email-Verkehr aufgezeichnet, so genannte „stille SMS“ stündlich auf die Handys geschickt haben, um den Standort des Betroffenen feststellen zu können und um zu überprüfen, ob das Handy ausgeschaltet war oder nicht. Ordnerweise wurden Auskünfte von den Kreditinstituten, von der Deutschen Bahn AG und Autovermietern eingeholt. Der Freundeskreis wurde durchleuchtet, die Wohnungseingänge mit Kameras überwacht etc. Gefunden haben Bundesanwaltschaft und Bundskriminalamt nichts, was ihre Vermutungen rechtfertigen würde. Der Schluss, die Verfahren einzustellen und den zugrunde liegenden Irrtum anzuerkennen, war aber ausgeschlossen. Stattdessen wurde das Fehlen von Ermittlungsergebnissen mit dem angeblich hochkonspirativen Verhalten der Beschuldigten begründet. Ein vom BKA beobachtetes Treffen zweier Beschuldigter erhielt seine Konspirativität u. a. dadurch, dass die Observierten sich während des Treffens öfter umgeschaut hätten. Die Reaktion auf eine scheinbar auffällig durchgeführte Observation wird somit zum Verdachtsmoment.

## Mach dein Handy nicht aus

Die Betroffenen in so einem Verfahren haben kaum eine Chance, sich verdachtsneutral verhalten zu können. Wenn private oder berufliche Kontakte, politisches Engagement und wissenschaftliche Veröffentlichungen ausreichen, um des Terrorismus beschuldigt zu werden, hat man kaum Chance, sich einer solchen Falschbeschuldigung zu entziehen. Neutrale und vollkommen interpretationsoffene Verhaltensweisen dienen nur als Bestätigung des Vorwurfs. Entlastende Schlüsse werden bewusst nicht gezogen. Will man sich den in politischen Verfahren üblichen Überwachungen und Ausforschungen des persönlichen Lebensbereiches entziehen - sei es, weil man grundsätzlich die eigene Privatsphäre als etwas Schützenswertes ansieht, weil man als bürgerrechtlich und politisch interessierter Mensch von der Möglichkeit weiß, aus welchen nichtigen Gründen man in das Visier der Staatsschutzbehörden geraten kann oder einfach nur deswegen, weil man die Observationsmaßnahmen bemerkt hat - macht man sich der Konspiration verdächtig und „erhärtet“ somit den eigentlich unbegründeten Verdacht.

## Wer Grundrechte wahrnimmt, muss sich rechtfertigen

Die Wahrnehmung von Grundrechten - der Schutz der eigenen Privatsphäre - gerät so unter Rechtfertigungsdruck. Nicht der staatlicherseits geführte Überwachungs- und Ermittlungsaufwand bedarf mehr der Begründung. Vielmehr gerät der Betroffene für seinen aktiven Grundrechtsschutz unter Erklärungszwang. Die Ausübung von Grundrechten ist damit nicht mehr voraussetzungslose Selbstverständlichkeit, sondern Anlass für staatliches Misstrauen. Die Funktion der Grundrechte wird damit in ihr Gegenteil verkehrt.

Wohlgemerkt, bei den „verdächtigen“ Verhaltensweisen handelt es sich nicht um verbotene Handlungen, sondern um ganz legale Möglichkeiten, sich und seine Daten zu schützen. Dass der Staat dies in einem anderen Kontext genauso sieht - und entsprechende Vorkehrungen sogar empfiehlt - ist eine weitere Absurdität in diesen Verfahren. So wurde vom Bundeswirtschaftsministerium die Entwicklung des sehr häufig verwendeten Anonymisierungsdienstes An.On. finanziert. Auf seiner Homepage ( www.bsi.de/produkte/mds/index.htm) informiert das Bundesamt für Sicherheit und Informationstechnik über den von ihm in Zusammenarbeit mit Siemens entwickelten Mobilfunkdetektor MDS, mit dessen Hilfe festgestellt werden kann, ob Mobilfunkgeräte Signale aussenden oder nicht und damit auch, ob sie

beispielsweise als räumliche Überwachungseinrichtungen eingesetzt werden.

Diese Möglichkeit der Verwendung hatte wohl auch ein Staatsanwalt von der BAW vor Augen, als er in einer Zeugenvernehmung im besagten Verfahren darauf bestand, dass der Zeuge und sein anwaltlicher Beistand ihre Mobilfunkgeräte ausschalten. Ob dies seitens der auch anwesenden BKA-Beamten als Indiz dafür angesehen wurde, dass im Rahmen der Vernehmung terroristische Straftaten geplant werden sollten, ist nicht überliefert (siehe zur Kritik an § 129a StGB auch den Beitrag von Wolfgang Kaleck in diesem Band, S. 170).

---