Netzsicherheit

Das Internet - Mehr Neuland als man denkt

Die groß angelegten Überwachungsaktionen bzw. Datendiebstähle durch US-amerikanische und britische Geheimdienste haben Europa vor Augen geführt, dass die Möglichkeiten der digitalen Kommunikation bis zu einem gewissen Maße auch als Gefahr zu betrachten sind. Die Bedenken einiger Bürgerinnen und Bürger, dass Sicherheitsbehörden die Möglichkeiten des Internets nutzten könnten, um die Bevölkerung systematisch zu überwachen, wurde von der Politik lange Zeit nicht ernst genommen. Man muss sich eingestehen, dass das Szenario, in dem Sicherheitsbehörden bei ihrer Überwachung nicht verhältnismäßig zur Gefahrenabwehr handeln, sondern ihre technischen Möglichkeiten ohne jegliche Rücksicht ausschöpfen, häufiger verkommt. Auch wenn die Onlineüberwachung in einigen Fällen zur Verhinderung von Terroranschlägen geführt haben mag, haben die Geheimdienste ihre Kompetenzen im Rahmen der Terrorabwehr weit überschritten. So handelt es sich bspw. bei der Bespitzelung von Abgeordneten, dem Kanzleramt oder der Europäischen Kommission ganz eindeutig um wirtschaftlich/politisch motivierte Spionage. Kurz um: Das Internet kann durchaus als ‚rechtspolitisches Neuland' bezeichnet werden. Es sind in Bezug auf die gesetzlichen Regeln der digitalen Kommunikation noch einige grundlegende Fragen offen.

Bürgerrechte und Onlineüberwachung

Das Internet als digitaler öffentlicher Raum ist ein Feld, in dem, genau wie in der realen Welt, Kriminalität stattfindet. Es steht außer Frage, dass staatliche Sicherheitsbehörden Instrumente nutzen müssen, um diese zu bekämpfen. Gleichzeitig muss es jedoch gesetzlich definierte Grenzen geben, um die Rechte der Bürgerinnen und Bürger zu schützen.

Grundsätzlich müssen Sicherheitsbehörden die Kompetenzen zugestanden werden, die notwendig sind, um die Bürgerinnen und Bürger vor Gefahren zu schützen. Dem Schutz vor Terrorismus wird dabei zu Recht Priorität eingeräumt. Dabei entsteht ein Zielkonflikt: Grundrechte, die hier in der Diskussion stehen, sind vor allem Persönlichkeitsrechte, insbesondere das Recht auf informationelle Selbstbestimmung, sowie das Post- und Fernmeldegeheimnis. Problematisch ist dabei, dass individuelle Freiheiten und Privatsphäre unter Umständen gegen Leben und Gesundheit von Menschen aufgewogen werden müssen. Grundsätzlich nach dürfte die körperliche Unversehrtheit eines Menschen schwerer wiegen, als der Schutz von Daten.

Eine totale Überwachung lässt sich jedoch trotzdem nicht durch die Notwendigkeit der Gefahrenabwehr rechtfertigen. Sicherheit muss Freiheit ermöglichen. Die Freiheit darf nicht zu Gunsten der Sicherheit geopfert werden.

Internetnutzer müssen davor geschützt werden, dass der Staat ohne Einverständnis der Betroffenen über personenbezogene Daten verfügen kann. Jedoch gibt es hier kaum Abwehrmöglichkeiten. Da Geheimdienste verdeckt arbeiten müssen ist eine Kontrolle durch die Bevölkerung oder einzelne Nutzer praktisch ausgeschlossen.
Um übertragene Daten zu schützen besteht nur die Möglichkeit der vollständigen Verschlüsselung. Die Programme dafür existieren, überwiegend wird jedoch US-amerikanische Software eingesetzt, die solche Schutzmechanismen nicht oder nur unzureichend zur Verfügung stellt bzw. sogar Hintertüren für US-amerikanische Nachrichtendienste zur Verfügung stellt. Aus diesem Grund muss die Verbreitung und der Einsatz europäischer und quelloffener Software gefördert werden. Diese muss sich an die hohen Standards beim Datenschutz halten. Insbesondere vor dem Hintergrund, dass durch den Trend zur Cloud, immer mehr private Daten im Netz gespeichert werden.

Neben diesen technischen Aspekten müssen auch politische Maßnahmen getroffen werden. Die Möglichkeit der parlamentarischen Kontrolle muss intensiviert werden. Es erscheint zu diesem Zweck sinnvoll, dass sowohl die deutschen als auch die europäischen Sicherheitsdienste dazu verpflichtet werden, quartalsweise einen „Überwachungsbericht“ vorzulegen, der Art, Umfang und Ergebnis der erfolgten Überwachung darstellt. Dieser ist dem parlamentarischen Kontrollgremium vorzulegen, welches darüber entscheidet, ob dieses Vorgehen gerechtfertigt ist oder entschärft bzw. intensiviert werden muss. Ggf. könnte dies unter Beteiligung einer Justizbehörde und den Datenschutzbeauftragten erfolgen.

Cyberkrieg – Eine Grauzone des internationalen Rechts

Die klassischen Formen der Aufklärung und Spionage werden in den Verteidigungsstrategien von Staaten und im internationalen Völkerrecht hinreichend bedacht. Die Aufklärung fremden Territoriums durch Spionageflugzeuge wird im internationalen Völkerrecht als Kriegerischer bzw. Aggressiver Akt gewertet. Die meisten Staaten behalten sich vor solche Flugzeuge in ihrem Luftraum anzugreifen, was die USA während des Kalten Krieges in mehreren Fällen akzeptiert haben. Auch auf die klassische Spionage durch Agenten wird in den meisten Staaten ähnlich reagiert. Selbst in den USA wurden nach dem Zweiten Weltkrieg noch Menschen hingerichtet, die wegen Spionage zum Tode verurteilt worden sind. Sogenannte Datendiebstähle oder Cyberangriffe sind in den internationalen Beziehungen hingegen vergleichsweise neu und stellen eine Grauzone des internationalen Rechts dar.
Insofern muss Deutschland sich darum bemühen, die o.g. Kontrollmöglichkeiten von nationaler Ebene auf die internationale Ebene zu tragen.

Die Zusammenarbeit innerhalb der EU muss auf diesem Feld vertieft werden. Die EU-Staaten müssen bei der Abwehr von Datendiebstählen enger zusammenarbeiten und sich auf einheitliche Standards nach dem deutschen Vorbild beim Datenschutz verständigen.
Die EU muss Mitgliedstaaten (z.B.: Großbritannien), welche Bürger, Unternehmen oder Institutionen anderer EU-Staaten überwachen, wirkungsvoll sanktionieren.

Digitalwirtschaftsstandort Deutschland

Die digitale Wirtschaft ist eine der Wachstumsbranchen der Zukunft. Es muss der Anspruch Deutschlands sein ein wesentlicher Standort für die Digitalwirtschaft zu sein. Hierfür muss die Politik Rahmenbedingungen schaffen.
Es muss EU-einheitliche Standards nach dem deutschen Vorbild im Datenschutz geben, die für alle Unternehmen, die innerhalb der EU Dienstleistungen anbieten wollen, gelten. Der Datenschutz muss auch von Unternehmen aus Nicht-EU-Staaten eingehalten werden, die innerhalb der EU tätig sein möchten. Zuwiderhandlungen müssen von der Europäischen Kommission mit der gleichen Härte verfolgt werden, wie Verstöße gegen das Wettbewerbs- bzw. Kartellrecht.
Die unterschiedlichen Auffassungen zwischen US-amerikanischen und britischen Datenschutzstandards einerseits und die in den anderen Ländern vertretenen Auffassungen andererseits dürfen nicht zu einer Aufweichung des europäischen Datenschutzes führen. Die Übermittlung personenbezogener Daten in die USA ist derzeit kritisch zu betrachten. Eine mögliche Freihandelszone zwischen der EU und den USA ist nur möglich bzw. erstrebenswert, wenn die USA ihre Standards anpassen.
Neben den Verbrauchern digitaler Dienstleistungen müssen auch die Unternehmen selbst gewisse Standortfaktoren vorfinden. Der Schutz vor Industriespionage ist dabei von entscheidender Bedeutung und wurde offensichtlich bisher vernachlässigt. Deutschland kann als Hochtechnologie- und Innovationsstandort nur bestehen, wenn Staat und Wirtschaft sich wirksam gegen Industriespionage verteidigen können. Im Zuge des Ausbaues von E-Government sind entsprechende Maßnahmen zu ergreifen, damit sensible Daten von Bürgern und Unternehmen nicht ausgespäht werden können. Schließlich gehört zu einem umfassenden Datenschutz ein Grundverständnis von Bürgern und Unternehmen dafür wie Netzwerke und Datenbanken funktionieren. Der verantwortungsvolle Umgang mit den eigenen Daten und das Wissen um mögliche Formen des Missbrauches sind für einen wirksamen Datenschutz unabdingbar.