**Aufgabe:**

1. **Markiere wichtige Begriffe/Abschnitte im Text.**
2. **Erörtere ob du einen Widerspruch zwischen Freiheit und Sicherheit in unserer Demokratie siehst.**

**Freiheit oder Sicherheit?**

Meike Laaff ([fluter.de](http://www.fluter.de/freiheit-oder-sicherheit) )

Über staatliche Überwachungsmaßnahmen wird derzeit viel diskutiert. Aber worüber wird sich dabei eigentlich genau gestritten? Um das herauszufinden, hat Fluter Experten gefragt – sowohl solche, die Überwachung als Garanten von Sicherheit befürworten, als auch solche, die die Maßnahmen als Einschränkung ihrer persönlichen Freiheit ablehnen. Vier Fragen – und vier völlig unterschiedliche Antworten.

**1. Überwachungsmaßnahmen werden von den einen als Eingriff in die Freiheit der Bürger/innen verstanden, von anderen als Garant für mehr Sicherheit. Warum sind sie notwendig – oder warum bedrohen sie die Freiheit der Bürger/innen?**

SICHERHEIT  
Markus Beyer, Sprecher des Bundesinnenministeriums: "Das Grundgesetz fordert die Gewährleistung der Sicherheit durch den Staat. Ohne Sicherheit keine Freiheit – das wusste schon Humboldt. Sicherheit ist die Grundlage, auf der Freiheit sich erst vollends entfalten kann. Freiheit und Sicherheit sind untrennbare zwei Seiten einer Medaille. Deshalb sind alle die Sicherheit gewährleistenden Maßnahmen gleichzeitig auch als Maßnahmen zu begreifen, die Freiheitsentfaltung gewährleisten und fördern. Ein Gewinn an Sicherheit stärkt im demokratischen Rechtsstaat die Freiheit. Die Bekämpfung des Terrorismus ist dabei ein entscheidender Beitrag zur Wahrung des inneren Friedens und der Sicherheit unseres Landes. Die Bevölkerung hat einen Anspruch darauf, dass unsere Sicherheitsbehörden auch zukünftig jederzeit in der Lage sind, solchen Entwicklungen im Frühstadium Einhalt zu gebieten. Dazu gehören ausreichend Personal, der neueste Stand der Technik sowie die erforderlichen Befugnisse."

FREIHEIT  
Beate Rösseler, Philosophin: "Der Respekt für die Privatheit einer Person ist der Respekt für sie als einem autonomen Subjekt, das ist die entscheidende Einsicht. Wir müssen generell, um uns selbstbestimmt verhalten zu können, daran glauben und davon ausgehen können, dass wir nicht beobachtet werden, belauscht, getäuscht über die Weitergabe und die Erfassung von Daten, über die Anwesenheit von Personen und darüber, was anwesende Personen von uns wissen und "wer" sie deshalb "für uns" sind. Aus dem gleichen Grunde nützt es nichts, wenn Personen wissen, dass sie beobachtet werden oder dass Informationen über sie gespeichert werden, wenn sie nicht beobachtet oder auf diese Weise erfasst werden wollen – denn es ist genau die Tatsache, dass sie sich auf die Beobachtung und Kontrolle einstellen müssen, die sie daran hindert, selbstbestimmt, authentisch zu agieren."

**2. Wozu dient die Vorratsdatenspeicherung, für die Telekommunikationsanbieter sechs Monate lang Telefon- und Internet-Verbindungsdaten speichern müssen?**

SICHERHEIT  
Jörg Ziercke, Präsident des Bundeskriminalamts: "spielen bei der Aufklärung von schweren Straftaten eine bedeutende Rolle. So ist dieIP-Adresse eines Internetnutzers oftmals die einzige Spur zu den Tätern. Deshalb ist es wichtig, dass die Internetprovider – nicht die Sicherheitsbehörden – jetzt gesetzlich berechtigt sind und ab 01. Januar 09 verpflichtet werden, Verbindungsdaten ihrer Kunden für sechs Monate zu speichern. Ohne diese Daten wäre das Internet ein verfolgungsfreier Raum und die Polizei stünde im Kampf gegen zahlreiche Formen der Kriminalität – wie etwa der Kinderpornografie – völlig im Dunkeln."

FREIHEIT  
Ralf Bendrath, Netzbürgerrechtler vom AK Vorratsdatenspeicherung: "Vorratsdatenspeicherung heißt, dass die gesamte Bevölkerung ohne Anfangsverdacht überwacht wird. Wen ich wann und von wo aus anrufe, wann ich ins Internet gehe oder wem ich wann eine Mail schreibe, geht aber  
niemanden etwas an, schon gar nicht den Staat. Es gibt deutliche Hinweise darauf, dass die Menschen ihre Kommunikation reduzieren, weil sie sich nicht mehr unbeobachtet fühlen. Das kann nicht das Ziel eine Informations- und Kommunikationsgesellschaft sein. Sicherheit heißt immer auch Sicherheit vor dem Staat und vor Überwachung. Wie die Telekom-Datenskandale gezeigt haben, werden gespeicherte Datenhalden immer wieder missbraucht."

**3. Eine der kontroversesten Entscheidungen im neuen BKA-Gesetz sind die Onlinedurchsuchungen: Um an Informationen über Terroristen/innen und schwere Verbrecher/innen zu kommen, sollen Privatrechner ausgespäht werden dürfen. Garantiert das mehr Sicherheit oder bedroht es die Freiheit der Bürger/innen?**

SICHERHEIT  
RolfTophoven, Essener Terrorismusforscher: "Terroristen nutzen moderne Kommunikationsmittel. Darum muss die Polizei das Instrumentarium der Onlinedurchsuchung in die Hand gegeben bekommen, damit sie auf einer Augenhöhe mit den Terroristen operiert.  
Bei Onlinedurchsuchung geht es auch um psychologische Abschreckung: Terroristen, die wissen, dass sie schon auf dem Schirm der Behörden sein könnten, würden im besten Falle ihr Planungsverhalten im Netz ändern. Allerdings hat das Bundesverfassungsgericht enge Grenzen für die Onlinedurchsuchung gesetzt: Das Ausspähen ist nur dann verfassungsgemäß, wenn es konkrete Anhaltspunkte für konkrete Gefahr für Menschenleben und den Staat gibt – und sie darf nur auf richterliche Anordnung erfolgen. Darum ist die ganze Hysterie rund um die Onlinedurchsuchung übertrieben."

FREIHEIT

Andreas Popp, Vorsitzender der Netzaktivisten-Organisation Piratenpartei Bayern: "Online-Durchsuchungen stellen einen massiven Eingriff in die Privatsphäre des Einzelnen dar. Der Computer ist ein privater Lebensraum, genauso wie die eigene Wohnung, das hat das Bundesverfassungsgericht bestätigt. Die Daten auf privaten Rechnern gehen von E-Mails mit privatem Inhalt über Privatfotos bis hin zu Bankdaten. Onlinedurchsuchungen umgehen dabei die Grundrechte. Sie finden heimlich, ohne das Wissen des Durchsuchten statt. Das ist eine massive Verletzung der Rechtsstaatlichkeit. Erst recht, weil dabei ein Polizist heimlich in die Wohnung einbrechen müsste, um die Schnüffelsoftware zu installieren.  
Gleichzeitig ist der Beitrag zur inneren Sicherheit mehr als bescheiden. Terroristen und organisierte Kriminalität sind ja nicht blöd, die wissen, wie sie sich gegen solche Maßnahmen zur Wehr setzen können. Treffen würde es schließlich den einfachen Bürger. Wenn wir uns jetzt nicht alle gemeinsam dagegen stemmen, dann werden alle irgendwann auf unseren Rechnern herumwühlen wollen."

**4. Im neuen ePass werden biometrische Passfotos und seit November 2007 Fingerabdrücke gespeichert. Warum ist das sinnvoll – und besteht die Gefahr des Missbrauchs oder Ausspähens?**

SICHERHEIT  
Markus Beyer, Sprecher des Bundesinnenministeriums: "Mitgliedstaaten der EU haben sich nach den Anschlägen des 11. September 2001 auf die Einführung der Biometrie bei Pässen, Visa und Aufenthaltstiteln verständigt. Für den Fingerabdruck als zweites biometrisches Merkmal entschieden sich die EU-Mitgliedstaaten aufgrund der hohen Praxistauglichkeit. Zwei verschiedene biometrische Merkmale erhöhen die Flexibilität bei Kontrollen.  
Seit der ersten Generation sind die elektronischen Pässe gegen unbemerktes und unberechtigtes Auslesen durch einen wirkungsvollen Mechanismus geschützt. So kann nur derjenige mit einem speziellen Lesegerät die elektronischen Daten vom Chip des Passes lesen, der die identischen aufgedruckten Daten im Passdokument sehen und einscannen kann. Seit dem ePass der zweiten Generation kommt ein zusätzlicher Zugriffschutz zum Tragen: Nur Staaten, die von Deutschland spezielle Zugriffsberechtigungen erhalten, können auf die Fingerabdrücke im Chip zugreifen."

FREIHEIT  
Andreas Popp, Vorsitzender der Netzaktivisten-Organisation Piratenpartei Bayern: "Der Nutzen des ePasses erschließt sich uns gar nicht. Viel fälschungssicherer als der herkömmliche Reisepass ist er nämlich auch nicht. Wir sehen diese Entwicklung mit großer Sorge, sie ist ein weiterer Schritt hin zur totalen Überwachung. Auf diesen Chips werden Daten zur Identität einer Person gespeichert, die dank RFID-Technologie pausenlos von überall ausgelesen werden können.  
Wenn diese Daten in falsche Hände geraten, könnte sich jemand ganz bequem für einen anderen ausgeben. Natürlich werden diese Daten dann auch noch mit anderen Staaten ausgetauscht und das mittels einer total unausgereiften Technologie, die nach Missbrauch nur so schreit. Im Prinzip ist die Erhebung dieser Daten nichts anderes als die so genannten 'Erkennungsdienstlichen Maßnahmen' der Polizei. Wir werden also von einem Volk von Bürgern zu einem Volk von Verdächtigen."

*Meike Laaff ist Journalistin in Berlin. Einer ihrer Themen-Schwerpunkte: Datenschutz und Sicherheit.*