Überwachung, Datenschutz und Bürgerrecht

Informationsdossier zur aktuellen Lage

1. Was ist ein Überwachungsstaat?

Der Begriff Überwachungsstaat beschreibt ein Szenario, in dem ein Staat seine Bürger mit allen zur Verfügung stehenden und staatlich legalisierten Mitteln überwacht. So sollen Gesetzesverstöße besser und schneller erkannt und verfolgt werden können. Befürworter führen die Verhinderung von Straftaten, organisierter Kriminalität und Terrorismus als Notwendigkeit für die Etablierung einer umfassenden Überwachung der Bürger an. Kritiker halten einen Überwachungsstaat hingegen für nur schwer oder gar nicht mit einer freiheitlichen Demokratie vereinbar.

Im Überwachungsstaat werden die Erkenntnisse aus der Überwachung hauptsächlich zur Verhinderung und Ahndung von Gesetzesverstößen, sowie zur Gewinnung von geheimdienstlichen Informationen über die einzelnen Individuen und Bevölkerungsgruppen genutzt. Die Gefahr des Missbrauchs für politische Zwecke ist dabei stehts zugegen. Die Prävention von Straftaten und anderen unliebsamen Verhaltensweisen der Bürger findet im Überwachungsstaat bereits indirekt durch den ständigen Beobachtungsdruck statt. Die kann sogar soweit führen, dass so genannte „präventive Festnahmen“ gegen verdächtige Bürger unternommen werden können.

Der Überwachungsstaat zeichnet sich durch die Einschränkung des Datenschutzes, der Privatsphäre und der informationellen Selbstbestimmung aus. So gesehen ist die informationelle Selbstbestimmung ein direkter Gegenspieler des Überwachungsstaats. Als Beispiele für typische Maßnahmen des Überwachungsstaates seien Rasterfahndungen, Kameraüberwachung öffentlicher Plätze, die routinemäßige Erstellung von Bewegungsprofilen, Gendatenbanken (Genetischer Fingerabdruck), biometrische Datenbanken sowie umfassende Kommunikationsüberwachung.

2. Überwachung vs. Recht

Zwischen der Überwachung des Bürgers und dessen Rechten herrscht ein unüberwindbares Spannungsverhältnis. Auf der einen Seite steht die Kontrolle über gesellschaftliche Individuen und somit die Einschränkung der Freiheitsrechte, auf der anderen Seite die Unverletzlichkeit jener Freiheitsrechte und somit auch der Verlust der Kontrolle. Das Gleichgewicht zwischen freiheitlichem demokratischen Rechtssystem und autoritärem Überwachungsstaat wird somit zu einem gefährlichen Drahtseilakt, denn beides lässt sich nicht miteinander verbinden. Deshalb sollte sich jeder selbst die Frage stellen: Freiheit oder Kontrolle?

Um diese Frage zu beantworten, muss man zuerst die Gründe verstehen, die dahinter stecken. Denn was bewegt eine Gesellschaft, oder besser gesagt dessen Regierung, dazu die Freiheiten des Bürgers einzuschränken? Nun, einerseits ist es das ständig wachsende Bedürfnis nach Sicherheit in einer Welt, die als zunehmend unsicher empfunden wird. Komplexe Medienpsychologische Effekte führen dabei zu einer erhöhten Gefahrenempfindung wider rationale Fakten.[1] Politisch lässt sich daraus Profit schlagen, da sich Sicherheit wesentlich einfacher verkaufen lässt als Freiheit. Andererseits aber auch das ständig wachsende Bedürfnis die Kontrolle über den Bürger, oder besser gesagt den Wähler, zu erringen in einer Gesellschaft, die zunehmend pluralistischer wird. Um es also kurz zu fassen, es ist irrationale Angst, die eine Gesellschaft und deren Regierung dazu treibt, die eigenen Freiheiten aufzugeben.

Stellt man diese Aussagen vor den Hintergrund der „unsichtbaren Bedrohung“ des internationalen Terrorismus, bekräftigt sich die Vermutung, dass der Überwachungsstaat das Resultat einer Politik ist, die von Angst, Machtgier und wirtschaftlichen Interessen bestimmt wird. Denn ob eine ständige Überwachung tatsächlich im Interesse des unbescholtenen Bürgers liegt, ist mehr als fraglich.

Es besteht also die berechtigte Befürchtung, dass man im Rahmen der Terrorismusbekämpfung in einen totalen Überwachungsstaat abrutschen könnte und, dass in der Sicherheitsdebatte grundrechtliche Grenzen überschritten werden. Der legitime Wunsch nach Sicherheit verdrängt im radikalen Überwachungsstaat die Grundrechte wie das

[1] Durch Berichterstattung vieler Einzelfälle erhalten Zuschauer den subjektiven Eindruck, dass jene Vorfälle sich häufen würden. Dabei hat sich lediglich die mediale Erfassung Intensiviert, nicht die Anzahl tatsächlichen Vorfälle erhöht.

Briefgeheimnis, das Fernmeldegeheimnis und den Datenschutz. Die Sensibilität für die Gefahren solcher Einschränkungen der Bürgerrechte scheint auf der politischen Bühne nicht vorhanden zu sein. Vielleicht lässt sich das auch damit erklären, dass die so genannten Volksvertreter sich generell gerne selbst von den Maßnahmen ausnehmen und somit wenig Anreiz haben sich die Tragweite ihrer Beschlüsse vollends klar zu machen.

Aus diesem Grund ist es umso wichtiger den Bürger auf diesen Missstand aufmerksam zu machen, um der einseitigen politischen Diskussion ein Ende zu bereiten, denn auch in Luxemburg ist der Überwachungsstaat ein konkretes Problem, welches allerdings größtenteils ignoriert wird.

3. Aktuelle Beispiele

Dass der Überwachungsstaat keine dystopische Vorstellung der Zukunft ist, sondern bereits jetzt ein konkretes Problem darstellt, sollen folgende Beispiele verdeutlichen, die allerdings nur einen sehr kleinen Teil des tatsächlichen Ausmaßes darstellen können. Des Weiteren, soll verdeutlicht werden, dass sich der Überwachungsstaat nicht nur auf das Abhören der Telefone oder der Kameraüberwachung öffentlicher Plätze beschränkt, sondern, dass es unzählige Möglichkeiten zur Überwachung des Bürgers gibt, welche teilweise viel subtiler sind. Denn die moderne Technik erlaubt es, detaillierte Verhaltensmuster eines jeden Bürgers zu erstellen. So ist es möglich nicht nur den Aufenthaltsort zu ermitteln, sondern auch welches Konsumverhalten man an den Tag legt, also was und wie viel und wo man kauft, welche Vorlieben und Abneigungen man hat, wie viel man verdient, wo man ausgeht, welche Meinungen man vertritt, welche Freunde man hat usw…, die Liste kann man unbegrenzt fortführen, denn praktisch alles lässt sich heutzutage überwachen und dank leistungsstarker Computer, fast alles gleichzeitig.

- **Videoüberwachung**

Videoüberwachung ist die Beobachtung von Orten durch optisch-elektronische Einrichtungen, so genannten Videoüberwachungsanlagen. Nicht selten werden Computer zur automatischen Analyse der Daten herangezogen, so dass dieser Bereich heute eng mit der Informatik verknüpft ist. Die Weiterverarbeitungsmöglichkeiten sind sehr vielfältig, etwa zur

automatischen Nummernschilderkennung im Straßenverkehr oder der automatischen Personenerkennung in öffentlichen Orten.

Die Befürworter der Videoüberwachung wollen hier neue technische Möglichkeiten zur Aufklärung von Straftaten, aber hauptsächlich zur Prävention nutzen: Wer weiß, dass er ständig beobachtet wird, verhält sich anders als jemand, der sich unbeobachtet fühlt. Unter Beobachtungsdruck leidet derjenige, der überwacht wird. Er wird in seiner Freiheit und Unbeschwertheit beeinträchtigt. Man spricht bereits von Überwachungsdruck, wen der Betroffene glaubt, überwacht zu werden oder dies zumindest nicht ausschließen kann, und dadurch sich in seiner Freiheit und Unbeschwertheit beeinträchtigt fühlt. Um er kurz zu sagen, man kann nicht mehr in der Nase bohren, wenn man gerade Lust dazu hat.

Bestes Beispiel für die Videoüberwachung öffentlicher (und teilweise auch privater) Orte ist Großbritannien, dem Land mit der größten Überwachungskameradichte der Welt. So sind alleine in der Hauptstadt London über 500.000 Kameras installiert, die jeden Bewohner am Tag durchschnittlich 300 mal filmen[2]. Dabei werden allerdings nicht nur Personen überwacht, sondern auch z.B. die Autokennzeichen von Verkehrssünder erfasst. Doch damit nicht genug, so steht bereits die nächste Generation von Überwachungskameras in Planung, die den Bürger regelrecht „ausziehen“, also die Möglichkeit haben durch die Kleidung von Passanten zu schauen[3]. Oder wie wäre es, wenn man einfach per Fernsehen den Nachbar bespitzeln könnte? Ein neues englisches Überwachungs-Tv[4] erlaubt es dem gelangweilten Bürger als Auge des Gesetzes zu agieren, schließlich lauert die Gefahr ja überall.

Jedoch stellt die Kameraüberwachung nicht nur in Großbritannien ein Problem dar, auch in Luxemburg wird über eine Aufstockung der Kameras nachgedacht. Mehr Kameras, eine bessere Überwachung gewisser Gefahrenzonen- dies kündigte Justizminister Luc Frieden

[2] Wall Street Journal
[3] Spiegel.de
[4] Tagesschau.de

bereits an. Dabei geraten besonders die "Kinnekswiss", der centre Aldringer sowie das Bahnhofsviertel wieder ins Visier der Ermittler und so wird ein schon lange eingeschlagene Weg weiterbeschritten.

Seit längerem bastelt die luxemburgische Regierung an einem Konzept des Bürgerschutzes. Kameras werden installiert, Polizisten zeigen mehr Präsenz und der Kern der Hauptstadt soll vor potenziellen Straftätern geschützt werden um so ein größtmögliches Sicherheitsgefühl zu vermitteln, wenn auch wahrscheinlich nur ein subjektives. So sind seit November 2007 mehr als 40 Überwachungskameras auf dem Gebiet der Stadt Luxemburg operational. 50 weitere werden bis Anfang 2008 folgen[5]... Es darf bezweifelt werden, dass diese Maßnahme große Wirkung zeigen wird, zeigt doch ein Bericht des britischen Innenministeriums auf, wie wenig effektiv diese Form der Überwachung ist. 80% der Bilder die in dem Land mit der höchsten Kameradichte weltweit aufgezeichnet werden sind laut jenem Bericht unbrauchbar. Dies weckt Zweifel am Sinn der Überwachungsmaßnahmen. Diese Zweifel werden von einer Pilotstudie der Berliner Verkehrsbetriebe gestärkt: Seit Beginn der Überwachung gab es keinen Rückgang der Verbrechensrate, sie stieg sogar leicht an. Die Vermutung, dass außerdem die Kosten der Videoüberwachung in keinem Verhältnis zum Nutzen stehen wird bekräftigt durch die Legalisierung der Videoüberwachung von Taxis in Wien. Sind Taxis doch ein Schwerpunktgebiet für Raubdelikte, so haben die Taxiunternehmen nach abwägen der Kosten und des Nutzen quasi einheitlich auf die Überwachung verzichtet.[6] Die Politik allerdings zahlt die Überwachungsmaßnahmen bekanntermaßen aus den Taschen der Bürger, hier scheint das Kosten/Nutzen Verhältnis (un?)verständlicherweise kaum eine Rolle zu spielen.

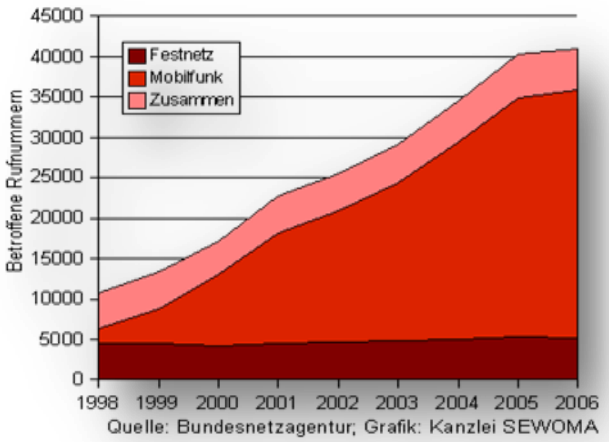
Auch Polizeichef Pierre Reuland äußerte sich noch 2002 in einem Interview kritisch gegenüber einer allgemeinen Kameraüberwachung: „Ich persönlich glaube nicht, dass die allgemeine Kameraüberwachung im öffentlichen Raum das Allheilmittel der Kriminalitätsbekämpfung ist."[7] Dabei mag es zwar stimmen, dass ein Mangel an Sicherheit die Freiheit einschränkt, es wird aber außer Acht gelassen, dass zu viel Sicherheit die Freiheit gleichermaßen beschneiden kann.

[5] tageblatt.lu
[6] heise.de
[7] Interview

- **Telekommunikationsüberwachung**

Telekommunikationsüberwachung ist die im Strafverfahrensrecht und Polizeirecht übliche Bezeichnung für die Überwachung von Telekommunikationsvorgängen und -inhalten. Dazu zählen das Abhören von Telefongesprächen und das Mitlesen von E-Mails, Kurzmitteilungen (SMS) und Telefaxen.

Im Zuge der Entwicklung der modernen Kommunikationsmedien hat auch die Überwachung von Telefongesprächen ein erheblicher Zuwachs zu verzeichnen[8]. So wurden z.B. in Deutschland zwischen 2006 - 2007 mehr als 40.915 Telefonate mitgehört[9]. Im Vergleich zu den 9.802 abgehörten Telefonaten im Jahre 1998, hat sich die Telefonüberwachung in Deutschland somit verfünffacht[10]. Während der geplanten Vorratsdatenspeicherung soll die Telekommunikationsüberwachung für das Jahr 2008 noch verschärft werden.



In den USA ist das Mitlauschen seit dem für verfassungswidrig erklärten „patriot act“ bereits Gang und Gäbe. Trotz der verfassungswidrigen Inhalte, wurde dieses „Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Werkzeuge, um Terrorismus aufzuhalten und zu blockieren“ 2006 mit geringfügigen Änderungen durch Präsident Bush abgesegnet[11]. Im Endeffekt scheint die Gesetzeslage aber eh uninteressant, wird sie doch konsequent ignoriert, so sie nicht den Wünschen der Geheimdiensten entspricht. Trotz anders lautender Gesetze empfinden es die US amerikanischen

[8] taz.de
[9] bitkom.org
[10] Kanzlei Sewoma
[11] Library of Congress

Kommunikationsunternehmen schon seit längerem als normal ihre Kunden, in Zusammenarbeit mit der NSA, konsequent auszuhorchen.[12]

Die Telekommunikationsüberwachung ist somit ein ernst zu nehmendes Problem, welches die Rechte des Bürgers weiterhin einzuschränken droht. Aber nicht nur Telefonate können abgehört werden, sondern auch, im Zuge der geplanten Vorratsdatenspeicherung, E-mails, Sms und der komplette Internetverkehr dessen Kerndaten gar für sechs Monate verdachtsunabhängig gespeichert werden sollen..

- **Vorratsdatenspeicherung**

Die Richtlinie über die Vorratsdatenspeicherung[13] ist eine Richtlinie der Europäischen Union, durch die die unterschiedlichen nationalen Vorschriften der EU-Mitgliedsstaaten zur Speicherung von Telekommunikationsdaten auf Vorrat vereinheitlicht werden sollen. So soll sichergestellt werden, dass die Daten für einen bestimmten Zeitraum zum Zweck der Ermittlung und Verfolgung von schweren Straftaten aufbewahrt werden.

Die Richtlinie ist politisch und rechtlich umstritten. Während ihre Befürworter die Vorratsdatenspeicherung als unverzichtbares Instrument zur Terrorismusbekämpfung und Strafverfolgung bezeichnen, verweisen ihre Kritiker auf die damit verbundenen Eingriffe in die Privatsphäre der Bürger, die sie als weiteren Schritt hin zum Überwachungsstaat ansehen. Des weiteren besteht der dringende Verdacht, dass eines der Hauptziele rein wirtschaftlicher Natur ist: Die radikale Durchsetzung der Urheberrechte im Internet.

Die Richtlinie verpflichtet die Mitgliedsstaaten der Europäischen Union, nationale Gesetze zu erlassen, nach denen bestimmte Daten, die bei der Bereitstellung und Nutzung öffentlicher elektronischer Kommunikationsdienste anfallen, von den Dienstanbietern auf Vorrat gespeichert werden müssen. Gespeichert werden sollen insbesondere Verkehrs- und Standortdaten. Diese sogenannten Verkehrsdaten erlauben Rückschluss auf individuelle Nutzung des Internets, Gesprächspartner am Telefon, und – wie bei E-Mails und SMS-Kurzmitteilungen, wo technische Daten und Inhalte nicht trennbar sind – auch Aufschluss auf die Inhalte von Kommunikation. Durch die Verkehrsdaten ist es etwa möglich, anonyme Äußerungen im Internet oder anonyme Teilnehmer an Tauschbörsen einem Telefonanschluss

[12] heise.de
[13] Gesetzestext zur EU-Vorratsdatenspeicherung

zuzuordnen. Daher sind Polizei- und Strafverfolgungsbehörden, Nachrichtendienste und auch private Dritte, insbesondere die Musikindustrie, daran interessiert, diese Daten für ihre Zwecke auszuwerten. Sollten diese Daten anfangs nur bei schweren Straftaten abrufbar sein, so ist inzwischen sogar die Rede davon, zum Beispiel der Musikindustrie direkten Zugang auf die Daten zu gewähren.

Dabei ist es noch höchst umstritten ob die Vorratsdatenspeicherung tatsächlich zu einer merklichen Verbesserung der Aufklärungsquote von Straftaten beitragen kann. So soll tatsächlich nur eine 0,006% höhere Quote erreicht werden[14]. Ob dies einen weiteren Schritt zum gläsernen Bürger rechtfertigt wäre somit mehr als fraglich. Hält man sich die amtlichen Statistiken über die Aufklärungsquoten[15] verschiedener Delikte vor Augen, so findet sich auch dort erschreckendes. Für im Internet begangene Straftaten liegt die Aufklärungsquote bereits jetzt mit beeindruckenden 85% höher als zum Beispiel bei Vergewaltigungen (83%). Die durchschnittliche Aufklärungsrate für in der realen Welt begangene Straftaten liegt bei lediglich 55%. Bei Straftaten rund ums Urheberrecht im Internet schwankt die Quote um 90%, Raubdelikte im realen Leben kommen auf knapp 50%, Diebstahl auf 15%. Dennoch wird die Überwachung des Netzes kostenintensiv hochgefahren, die Personalstärke der Polizei jedoch reduziert.

- **Online-Durchsuchung**

Als Online-Durchsuchung wird der heimliche staatliche Zugriff auf informationstechnische Systeme über Kommunikationsnetze bezeichnet. Der Begriff umfasst dabei sowohl den einmaligen Zugriff wie auch eine sich über einen längeren Zeitraum erstreckende Überwachung.

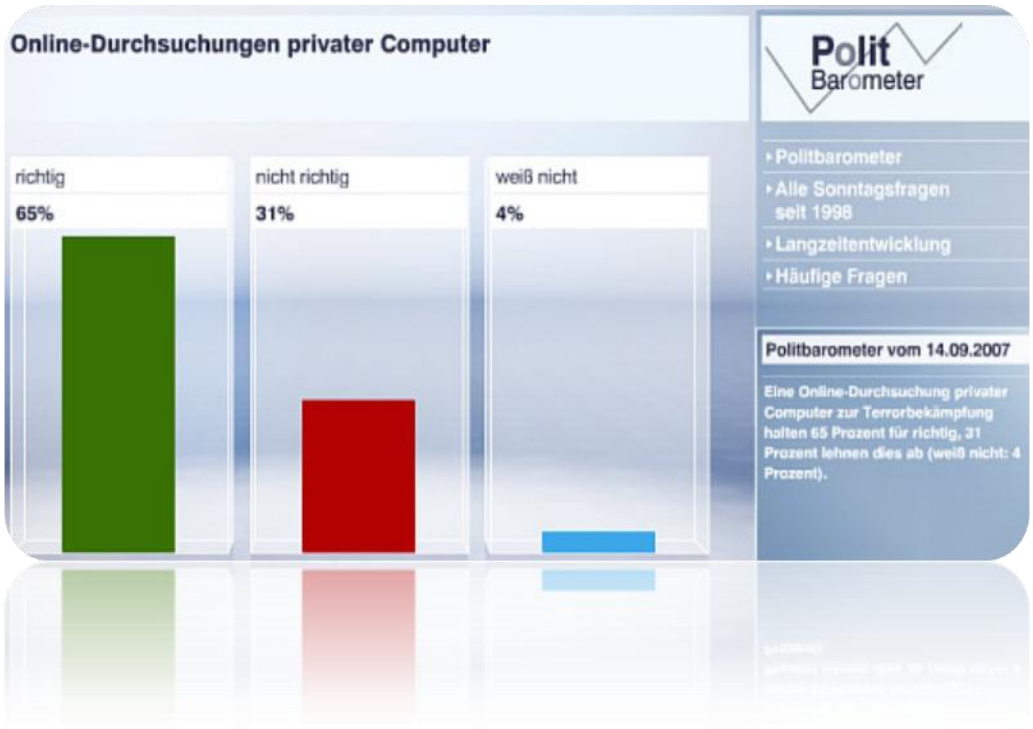
Ist die Online-Durchsuchung bisher in Deutschland noch keine gesetzlich geregelte Methode staatlicher Informationsgewinnung (was weder Minister daran hindert gut zu heißen, dass es ohne gesetzliche Grundlage praktiziert wird, noch die Geheimdienste daran hindert es zu tun) so ist diese bereits in Österreich teilweise Realität. Dort wurde am 17. Oktober 2007 eine Einigung erzielt welche erlaubt, die „Online-Fahndung“, wie sämtliche Ermittlungsmethoden an Privatcomputern, bei Verbrechen, die mit über zehn Jahren Strafe

[14] heise.de
[15] Zahlen für die BRD

bedroht sind, einzusetzen. Allerdings sollen nun bis Ende Februar die Rahmenbedingungen ausgeweitet werden, sodass ein Gesetz bereits vor dem Sommer 2008 beschlossen werden könnte.

Glaubt man allerdings dem Politbarometer des ZDF, der besagt, dass 65% der deutschen Bevölkerung die Online-Durchsuchung für richtig halten und überträgt dieses Resultat auf die europäische Bevölkerung, so ist es allerdings nur eine Frage der Zeit, bis die Online-Durchsuchung nicht nur in Deutschland, sondern auch europaweit harte, politische Realität wird.

"Wenn das BKA-Gesetz in der vorliegenden Fassung verabschiedet wird, entsteht de facto eine Geheimpolizei, wie sie in Deutschland zuletzt in der DDR existierte", sorgen sich die Sicherheitsexperten des sogenannten Chaos Computer Clubs[16], die den umstrittenen Gesetzesentwurf zur Online-Durchsuchung in Deutschland veröffentlicht haben. Angesichts der sich häufenden Berichte über privaten und behördlichen Missbrauch von Überwachungsbefugnissen warnen sie zugleich davor, "dem Gesetz auch nur teilweise zuzustimmen". Das Trennungsgebot von Polizei und Geheimdiensten dürfe nicht weiter ausgehöhlt werden.



[16] heise.de

- **Biometrischer Pass**

Auch der neue biometrische Pass, der in Luxemburg seit Ende 2006 ausgestellt wird biete neue Möglichkeiten der Überwachung. Dieser sogenannte „ePass“ enthält das Bild des Passinhabers in elektronischer Form. Ab dem Jahr 2007 wird zusätzlich der elektronische Fingerabdruck aufgenommen. Diese Information wird auf einem Funk-Mikrochip (RFID) gespeichert. Dabei ist es fraglich inwieweit der biometrische Pass die informationelle Selbstbestimmung verletzt, denn die im ePass gespeicherten Daten können an internationalen Grenzen ausgelesen und in Datenbanken gespeichert werden. Niemand weiß, wer Zugriff darauf hat und was mit den sensiblen biometrischen Daten weiter passiert.

Dabei sind sogar biometrische Pässe nicht 100% fälschungssicher, wie leicht sich ein Fingerabdruck fälschen lässt, zeigt folgende Demonstration des CCC. Ohne ausreichende Sicherheitsmaßnahmen könnten auch RFID-Chips im Reisepass dazu führen, dass die gespeicherten Daten ohne willentliche und aktive Handlung des Besitzers (wie dem Vorzeigen des Ausweises) verdeckt ausgelesen werden könnten. Dieses unbemerkte Auslesen könnte z. B. durch den Aufenthalt in einem mit RFID-Lesetechnik bestückten Bereich erfolgen oder durch Annäherung einer Person mit einem mobilen Lesegerät auf kurze Distanz zum Betroffenen bzw. seinem Reisepass.

Bei einer Studie der renommierten London School of Economics, an der 10.000 Freiwillige teilnahmen, versagte das System bei 20 Prozent der Fingerabdrücke[17]. Auch die Nachhaltigkeit biometrischer Daten stellt ein großes Problem dar, denn Biometrische Informationen können derzeit nicht widerrufen werden. Da physische Merkmale wie das Gesicht oder Fingerkuppen nicht einfach geändert werden können, können einmal gestohlene biometrische Merkmale lange Zeit missbraucht werden. Identitätsdiebstähle häufen sich bereits Heute, zu erwarten, dass biometrischen Daten nicht missbraucht werden erscheint mehr als nur naiv.

Biometrische Daten auf einem Pass werden bisher nur auf diesem gespeichert. Die Europäische Kommission denkt jedoch darüber nach, ein zentrales „Europäisches Passregister“ einzuführen. Dadurch soll erreicht werden, dass sämtliche biometrischen Daten, die auf einem Pass gespeichert sind auch an einer zentralen Stelle gesammelt werden. Den Nutzen, den sich die Europäische Union dadurch erhofft, besteht darin, dass mit Hilfe einer

[17] ard.de

zentralen Stelle viele öffentliche Stellen auf diese Daten zugreifen können, um übergreifend Personenabfragen durchführen zu können. Es ist davon auszugehen, dass diese Daten auch an Länder weitergegeben werden, die keinerlei Datenschutzbestimmungen ratifiziert haben. Bereits heute passiert dies im Rahmen des Flugpassagierdatenaustausches mit den USA in großem Umfang, obwohl es nach Meinung unabhängiger Rechtsexperten dafür keinerlei gesetzliche Grundlage gibt, ja die Praktik sogar illegal sein dürfte.

- **Sonstige Formen der Überwachung**

Auf Panopti.com wird auf eindrucksvolle Weise dargestellt, auf welche Art und Weise man sonst noch Überwacht wird. Dabei geht es eher um private Informationserfassung als um staatliche Kontrolle, allerdings ist es schon erschreckend wie viel Information über die eigene Person gesammelt wird.

4. Was spricht für den Überwachungsstaat?

Das Hauptargument des Überwachungsstaates ist die Stärkung der Sicherheit des Bürgers, die ständige Kontrolle soll potentielle Straftäter von Gesetzeswidrigkeiten abhalten und den staatlichen Sicherheitekräften einen Vorteil in der Verbrechensbekämpfung geben. Die Befürworter führen somit oft die Verhinderung von Straftaten, organisierter Kriminalität und Terrorismus als Notwendigkeit für die Etablierung einer umfassenden Überwachung der Bürger an. In einem rezenten Interview hat auch Polizeichef Reuland in diese Kerbe gehauen. Dazu zitierte er eine französische Studie die angeblich einen 40 prozentigen Rückgang der Kriminalitätsrate in von Kameras überwachten Gebieten aufgezeigt hat. Wie der Feierkrop

aufdecken musste existiert diese "Studie" (die wir auch auf eigene Nachforschungen hin nicht finden konnten) allerdings gar nicht. Die weiter oben zitierte Studie aus Berlin die keinen Einfluss feststellen konnte mag die Politik weniger arrangieren, dafür ist sie aber real.

Von Seiten der Befürworter heißt es, eine dauerhafte Beobachtung (z.B. durch Kameraüberwachung öffentlicher Orte) könnte die Häufigkeit von Straftaten verringern dadurch, dass man dem Straftäter den Schutz der Anonymität nimmt, was zu einer Prävention der Straftat an sich führen könnte. Denn vielleicht überlegt sich der Straftäter seine Handlung zweimal, wenn er weiß, dass er erkannt werden könnte. Des Weiteren kann eine permanente Überwachung zur Aufklärung bereits begangener Verbrechen beitragen, weil das Geschehen aufgenommen wurde. Zumindest sofern die Bilder nicht unbrauchbar sind, was wie bereits beschrieben eher die Regel als eine Ausnahme ist. Der Schritt zum Überwachungsstaat könnte also rein theoretisch zu einer größeren Sicherheit des Bürgers, sowie einer geringeren Verbrechensquote und einer höheren Aufklärungsquote führen. Vieles deutet aber darauf hin, dass dies so einfach nicht ist.

5. Was spricht gegen den Überwachungsstaat?

Kritiker halten einen Überwachungsstaat hingegen für nur schwer oder gar nicht mit einer freiheitlichen Demokratie vereinbar. Denn von dem Verlust der Anonymität sind nicht nur Verbrecher, sondern auch unbescholtene Bürger (und dies noch im größeren Umfang) betroffen. Die ständige Überwachung des Bürgers würde so gleichzeitig zu einer tiefgreifenden Einschränkung des Privatrechtes führen. Die teils invasiven Methoden eines Überwachungsstaates sind nämlich in einigen wesentlichen Bereichen unvereinbar mit den Rechten des Bürgers, dies betrifft vor allem den Informationsschutz. Ein Staat sollte nicht das Recht haben, die Kommunikation zwischen seinen Mitbürger willkürlich mitzuhören oder den Bürger in seinem eigenen Haus zu beobachten. Somit würde eine ständige Überwachung des Bürgers eine ernste Gefährdung der bürgerlichen Freiheit mit sich bringen.

Des Weiteren ist es nach wie vor höchst umstritten in welchem Ausmaß eine ständige Überwachung tatsächlich zu einer Verringerung der Kriminalitätsrate beiträgt. Besonders jene Straftaten, welche im Affekt ausgeführt werden, können so kaum verhindert werden. Ein besonderes Problem liegt aber darin, dass das Risiko für Bagatelldelikte bestraft zu werden unkontrollierbar wird. Im Zusammenspiel mit Personalabbau und schlampigen Ermittlungen

kann jeder unerwartet ins Visier geraten. Das Beispiel einer Chinesin die in Deutschland Monatelang in Untersuchungshaft saß, nachdem sie von der GVU[18] des Verkaufs von Raubkopien beschuldigt wurde ist exemplarisch für die Risiken eines aus dem Ruder laufenden Rechtsstaates. Aufgrund stetig verschärfter Gesetze und überlasteter Ermittlungsbehörden wurde die Klägerin (GVU) als Experte der Anklage ernannt. Was in einem modernen Rechtsstaat unmöglich erscheint geschah somit: Die Klägerin wurde zum Richter und nur dem Anwalt der Chinesin, der der GVU die gezielte Fälschung der Beweise nachweisen konnte, ist es zu verdanken, dass die Frau nach ein paar Monaten frei kam. Dies ohne sich je etwas zu Schulden kommen gelassen zu haben.

Dies ist ein Einzelfall, aber ein sehr erschreckender, da hier der Rechtsstaat offensichtlich komplett versagt hat und vor einer Industrie kapituliert hat die scheinbar immer mehr an Macht gewinnt. Mit Janelly Fourtou sitzt die Frau des Vivendi Chefs an zentraler Stelle der EU um den Urheberrechtsschutz zu radikalisieren. Die USA haben gar auf Wunsch der Musiklobby Russland die Aufnahme in die WTO verweigert für den Fall, dass das Land einen Internet Musikshop nicht schließt. Die gleiche Industrie ist drauf und dran sich in einigen europäischen Ländern direkten Zugang auf die kompletten Überwachungsdaten der Kommunikation gewähren zu lassen. So hat sich im Zuge der Vorratsdatenspeicherung in Deutschland bereits der Kampf um die Zugangsdaten begonnen; Film- und Musikindustrie verlangen Zugriff auf jene Daten, die eigentlich nur in Fällen von „schweren Delikten“ zugänglich gemacht werden dürfen.[19]

Sie sehen wohin dieser Ausflug ins Urheberrecht führt. Es zeichnet sich, auf diesem Gebiet exemplarisch dargelegt, erschreckendes ab. Eine Verschärfung der Gesetze geht einher mit weniger sorgfältigen Ermittlungen und dem Einsatz von zweifelhaften "Privatsheriffs" die eigene Interessen vertreten und somit ein unkalkulierbares Risiko darstellen. Diese Troika wird durch enorm ansteigende Mengen an Information vervollständigt. Haben sie schon einmal ein Lied aus dem Internet herunter geladen? Oder ein Video einer Privatfeier gedreht auf dem im Hintergrund Musik zu hören ist? Vielleicht mit jemandem telefoniert der Kontakt zu Terroristen hat? In einem Staat der alle Kommunikation überwacht und speichert könnten Sie schneller in Probleme geraten als Sie denken.

[18] Gesellschaft zur Verfolgung von Urheberrechtsverletzungen
[19] heise.de

Nicht nur, dass solche Unmengen an Daten kaum zu überblicken sind und somit falsche Interpretation entstehen können, nein es ist in einigen EU-Ländern schon dir Rede davon, diese Daten privaten Ermittlern zur Verfügung zu stellen. Sollte dieses unglaubliche Szenario wahr werden und der Wirtschaft gestattet werden sich direkt in die Strafverfolgung einzuschalten, die Konsequenzen wären kaum auszudenken.

Die Gefahr des Missbrauchs der Überwachungsinstrumente, durch Wirtschaftsakteure die sich daraus Profit versprechen oder auch staatliche Organe ist enorm. Denn sind erst einmal die Rechte des Bürgers beschnitten, welchen rechtlichen Schutz kann er dann noch erwarten? Kaum jemand dürfte von sich behaupten können nie auch nur das kleinste Vergehen begangen zu haben. Alleine schon deshalb weil die Gesetzestexte längst derart umfangreich sind, dass sie nicht einmal Richter, geschweige denn der Durchschnittsbürger, alle kennen können. In einem Überwachungsstaat werden nicht alle diese Vergehen geahndet werden können, aber ein jeder wird dadurch erpressbar, dass er von jenem Damoklesschwert über seinem Kopf weiß. Wer unangenehm auffällt, dem wird man im Zweifelsfall etwas vorwerfen können. In einer funktionierenden Demokratie ist eine gezielte Anwendung dieser Möglichkeiten gegen Bürger unwahrscheinlich. Das Vorhandensein der Instrumente droht aber immer weitere Begehrlichkeiten zu wecken und sollte es einmal ein politische Radikalisierung geben, so stünden perfekte Instrumente zur Durchsetzung einer Diktatur bereits zur Verfügung.

Ähnlich wie in autoritären Regierungssystemen, könnten fortgeschrittene Überwachungsstaaten durch die „präventive Verhaftung“ potentieller Verbrecher tatsächlich unschuldige Bürger bestrafen. Man siehe zum Beispiel den rezenten Fall zweier Jugendliche die sich über Internet über einen möglichen Amoklauf unterhalten haben, den Plan jedoch nicht in die Tat umzusetzen gedachten[20]. Beide wurden festgenommen, einer der beiden beging Selbstmord. Verbrochen hatter der 17-jährige nichts. Denken sie daran bevor Sie das nächste mal scherzhaft mit Freunden einen Banküberfall "planen".

Mit Staaten wie der DDR oder Nordkorea finden sich dann auch in der Liste der Überwachungsstaaten die es bisher gegeben hat wenig Beispiele die eine positive Bewertung solcher Staaten nahelegen. Vielleicht am ehesten noch Singapur. Aber auch von Reisen dorthin wird inzwischen regelmässig abgeraten, da man nie ausschliessen kann wegen Bagatelldelikten in ernsthafte Probleme zu geraten.

[20] spiegel.de

- **Fazit**

Genau hier liegt das Hauptproblem. Überwachung ist ein komplexes und akutes Thema, das oft mit strenger werdenden Gesetzen einher geht. Ein Thema das dringend der öffentlichen Aufmerksamkeit bedarf. Dieser Überblick kann lediglich nur an der Oberfläche des Themas kratzen, dabei sollen hier weniger Detailfragen erläutert werden, sondern deutlich gemacht werden, wie sehr die Überwachungsproblematik einer gesellschaftlichen Debatte bedarf. Denn die Frage wie viel Sicherheit die Demokratie bedarf und wie viel Freiheit dem Bürger zusteht, ist eine Frage die von großer politischer Bedeutung für die Zukunft moderner Staaten ist.

Was allerdings bei der Entwicklung staatlicher Überwachung deutlich geworden ist, ist vor allem der fehlende Dialog zwischen politischer Führung und Bürger. Stattdessen wird über die Köpfe der Menschen entschieden wie viel Freiheit, wie viel Privatsphäre und wie viel Informationsschutz ein jeder haben darf, dabei sollte diese Entscheidungskompetenz eher bei denen liegen, die betroffen sind, den Überwachten. Aktuell aber scheint es so als ließe sich, getragen von irrationalem Risikoempfinden durch ständige Präsenz von Kriminalität in den Medien, der Überwachungsstaat dem wenig informierten Bürger als Sicherheitspolitik gut verkaufen. Die Risiken werden oft mit einem läppischen "Ich habe doch nichts zu verbergen" abgetan. Bei näherer Betrachtung dürfte sich das oft als Trugschluss herausstellen.

Interessant ist auch die Meinung der Oberen zum Thema. Ob Frieden, Sarkozy oder Schäuble, die Meinung der Bürger zählt wenig, die eigene viel. Elegant formuliert hat es ein Anderer: In einem Artikel von ars technica[21] von November 2007, behauptet der Direktor der amerikanischen DNI, Ronald Kerr, dass der Bürger seine Definition von Privatsphäre an die Definition der Regierung anpassen sollte (Donald Kerr, a top intelligence official with the US government, says that citizens need to change their definition of privacy to match the government's definition). Dabei muss man sich allerdings die Frage stellen, ob es nicht eigentlich umgekehrt sein sollte? Ist eine Regierung nicht gewählt um dem Volk zu dienen und seinen Willen umzusetzen? Sollte eine verantwortungsvolle Politik sich hinter Definitionen verstecken müssen um ihre Entscheidungen zu legitimieren?

Die Frage sollte sich jeder selbst beantworten…

[21] arstechnica.com