Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2019

geleitet durch Prof. Dr. Paul Molitor

Überwachungsstaat mittels neuer Technologien

Jan Bittner & Daniel Schreiber

Inhaltsverzeichnis

Gender-Hinweis: Die weibliche Form ist der männlichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde die männliche Form gewählt.

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch die oben genannten Autoren erstellten Bericht. Der Dozent hat lediglich Schreib- und Kommatafehler entfernt sowie Formatierung angepasst.

1 Einleitung

1.1 Zur Methodik der Arbeit

Bei der Ausarbeitung des Themas haben wir drei Leitfragen entwickelt:

1. Welche Überwachungsmethoden gibt es in Deutschland zur Zeit?
2. Welche technischen Möglichkeiten zur Überwachung gibt es?
3. Was macht dieses Wissen mit uns?

Diese drei Fragen, die im Umfang bereits mehrere Doktorarbeiten füllen könnten, sind der rote Faden dieser Arbeit. Wir versuchen sie hier überblicksartig zu beantworten und müssen weitere Fragen, die naheliegend wären, in den Horizont verschieben. Wir grenzen diese Arbeit ab von einer historischen Sichtweise (z.B. DDR) und einer internationalen Sichtweise (z.B. China, Amerika) und hoffen, dass diese Aspekte von den Teilnehmern und Teilnehmerinnen in die Diskussion eingebracht werden können.
Im ersten Punkt verschaffen wir uns einen Überblick über die derzeitigen Überwachungsmethoden in Deutschland. Es soll ein Gefühl dafür vermittelt werden, was alles in Deutschland an Überwachung möglich ist, um in einer Diskussion die Vor- und Nachteile zu diskutieren, sowie deren Verhältnismäßigkeit auszuloten.
Im zweiten Punkt erläutern wir einen Kernbereich der Informatik - die Verschlüsselungstechnik. Sie ist zurzeit ein Problem für polizeiliche Behörden und deshalb Anlass für aktuelle mediale und politische Debatten. Auch hier soll ein Gefühl dafür vermittelt werden, was es bedeutet, Daten in einer Zeit zu schützen, in der sie potentiell abgegriffen werden können.
Der dritte Punkt ist bewusst subjektiv formuliert und zielt auf ganz unterschiedliche Fragestellungen ab. Wie handeln wir, wenn wir wissen, wir werden überwacht? Wie können und wollen wir uns schützen? Haben wir Probleme mit Überwachung? Haben wir ein Recht auf Anonymität? Als Anregung möchten wir ein kleines Gedankenexperiment wagen.
Doch bevor wir über diese Fragen philosophieren, schaffen wir zunächst eine Wissensbasis. Und wir beginnen mit der Frage: *Was ist ein Überwachungsstaat?*

1.2 Was ist ein Überwachungsstaat?

1.2.1 Mindmap *Überwachungsstaat*

Als wir mit der Ausarbeitung des Themas begannen, erstellten wir zuerst eine Mindmap, um uns über die Thematik des Überwachungsstaates einen Überblick zu verschaffen. Im Seminar wollten wir allen Teilnehmern die Möglichkeit geben, ihre Gedanken einzubringen. Dabei stellten wir fest, dass das Seminar die Schlagwörter um die Thematik *Daten* vernachlässigte. Um diesen Bereich hatten wir beispielhaft Dienste wie *Facebook* und *Whatsapp* gruppiert. Mit jeder Nutzung dieser Dienste stellen wir Daten zur Verfügung, die potentiell überwacht werden können.
Im Seminar wurde dann angemerkt, dass in unserer Mindmap die Thematik fehlt, *was für Auswirkungen die Überwachung auf Menschen hat.* Dabei fiel der Begriff *Einheitsmensch*, der auf das Problem des Konformismus abzielt. Wenn wir überwacht werden, wer traut sich dann noch, gegen die allgemeine Norm zu verstoßen? In diesem Zusammenhang wurde auch darauf hingewiesen, dass *Überwachung* mit *Kontrolle* einhergeht. Wir werden im folgenden Unterkapitel gleich feststellen, dass dieser Aspekt in der von uns gewählten Definition *Überwachungsstaat* fehlt.

1.2.2 Definition

In diesem ersten Abschnitt der Arbeit versuchen wir zu klären, was unter dem Stichwort *Überwachungsstaat* verstanden werden kann. Insbesondere muss der Frage nachgegangen werden, ab wann ein Staat als Überwachungsstaat gilt.

> In einem **Überwachungsstaat** [...] überwacht der Staat seine Bürger mit einer Vielzahl verschiedener staatlich legalisierter technischer Mittel.[1]

Was hier als erstes auffällt, ist die Selbstbezüglichkeit. Der Überwachungs**staat** handelt mit **staat**lich legalisierten Techniken. Der Ausdruck *technischer Mittel* scheint zwar zu unserem Thema der Arbeit zu passen, irritiert aber zunächst, wenn man ihn nur auf technologische Mittel verkürzt. Denn auch das (analoge) Mitlesen des Briefverkehres während des zweiten Weltkrieges, würde man als Überwachung durch den Staat auffassen. Versteht man *Technik* hier aber im weitläufigeren Sinne als Verfahren, verliert die Irritation ihre Begründung. Das Zitat geht eigentlich noch weiter:

[1] [1] Wikipedia "Überwachungsstaat".

> Der Begriff ist negativ besetzt und beinhaltet sinngemäß, dass die Überwachung ein solches Ausmaß angenommen hat, dass sie ein wesentliches oder sogar zentrales Merkmal des staatlichen Handelns geworden ist.[2]

Dieser zweite Teil hebt die negative Konnotierung des Begriffes hervor und zielt auf die Frage ab, wann ein Staat ein Überwachungsstaat ist. Dieser Teil suggeriert so, dass Überwachung durch den Staat nichts Negatives ist, sofern es sich in Grenzen hält. Erst das Ausmaß lässt die Überwachung durch den Staat zu einem Staat der Überwachung werden. Das Maß spielt also eine wesentliche Rolle bei der Definition.
Denkt man im klassischen Sinne an eine Überwachungsszene aus einem Actionfilm, dann hat man zwei Menschen in einem Auto, die eine Person auf Schritt und Tritt folgen, vor Augen. Und auch wenn man das Wort *Überwachung* im Duden nachschlägt, erfährt man dort, dass es darum gehe, *genau [zu] verfolgen, was jemand (der verdächtig ist) tut.* [3] Der in Klammern gesetzte Zusatz *der verdächtig ist* wird noch für viel Diskussionsstoff sorgen, wenn im Folgenden Überwachungsmethoden besprochen werden, die vor allem auch **un**verdächtige Personen treffen. Der Terminus Überwachung suggeriert Echtzeit. Menschen beobachten andere Menschen bei etwas, das sie tun. Dabei kann die Zeitdimension auch versetzt sein, zum Beispiel wenn Briefe gelesen werden, die in vergangener Zeit abgeschickt wurden. Aber mit den neuen technologischen Möglichkeiten tritt ein anderer Aspekt im Vordergrund: Daten über Menschen (seien es Handlungen oder Kommunikationen) können gespeichert werden. Später und dann gezielter kann gespeichertes Material beobachtet und ausgewertet werden. Ein Mensch kann so auch noch im Nachgang überwacht werden, nämlich möglicherweise dann, wenn er erst in irgendeiner Hinsicht *verdächtig ist.* Auch können Daten ganz verschiedener Bereiche zusammengeführt werden, sodass Sachverhalte sichtbar werden, die im klassischen Sinne von überwachen als *verfolgen, was jemand tut*, nicht sichtbar waren.
Diese beiden Aspekte (Asymmetrie der Zeitdimension und Zusammenführung von Daten) sollte man im Hinterkopf behalten, wenn es im Folgenden um Überwachungsmethoden mit technischen Hilfsmitteln geht. Denn bei der Frage nach der Verhältnismäßigkeit von Nutzen und Nachteil dieser Methoden sollte nicht vergessen werden, dass Zeiten sich ändern und neue Daten mit ihren Kombinationsmöglichkeiten zu alten, bereits gespeicherten Daten hinzukommen.
Im Seminar wurde in der Diskussion über die *Kriterien* eines *Überwachungsstaates* die Anforderung genannt, Behörden müssten in der Lage sein, mit unerheblichem Zeit-

[2] ebd.
[3] [2] Duden "überwachen".

aufwand auf (weitestgehend) **alle** Daten eines Menschen zuzugreifen. Wir finden diese Sachdimension sollte ein wesentlicher Aspekt einer Definition sein. Hierbei wird es auch im Folgenden gehen, wann immer Daten gespeichert und/oder zusammengeführt werden.

2 Überwachungsmethoden

2.1 Telekommunikationsüberwachung

Die Telekommunikationsüberwachung (TKÜ) ist wahrscheinlich die am meisten mit Überwachung in Verbindung gebrachte Methode. Ziel ist es, Kommunikation zwischen Personen abzugreifen, ohne dass die Kommunikationsteilnehmer davon wissen. Schaut man im Duden nach, was Telekommunikation bedeutet, dann erhält man:

> Kommunikation, Austausch von Informationen und Nachrichten mithilfe der Nachrichtentechnik, besonders der neuen elektronischen Medien.[4]

Zu den erfassten Übertragungsmitteln gehören

1. Briefe
2. Telefongespräche
3. SMS
4. Fax
5. E-Mails
6. Internetverkehr.

Bei technischen oder auch rechtlichen Beschränkungen können auf dieser Grundlage auch "nur" Verkehrsdaten (Metadaten) erfasst werden[5]. Sie geben keinen direkten Aufschluss über die Inhalte der Kommunikation, ermöglichen aber die Zuordnung, wer, wann und wo an Kommunikation beteiligt war. Das wird später bei den *Bewegungsprofilen* eine Rolle spielen. Das Erfassen des Internetverkehres wird später von der Online-Überwachung abgegrenzt werden.
Die rechtlichen Rahmenbedingungen sind in der StPO § 100a *Telekommunikationsüberwachung* ausgeführt. Dort heißt es im ersten Absatz

[4] [3] Duden "Telekommunikation"
[5] Vgl. dazu weiter unten den Abschnitt zur *Vorratsdatenspeicherung*.

> Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn
>
> 1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
> 2. die Tat auch im Einzelfall schwer wiegt **und** [Hervorh. d. Verf.]
> 3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.[6]

Die rechtliche Ausgestaltung findet sich in den Polizeigesetzen der Länder wieder. Der Einsatz dieser Methode muss in jedem Falle vorher (!) von einem Richter genehmigt werden. Eine Ausnahme bildet die Formulierung *Gefahr im Verzug*, die den ermittelnden Behörden Spielräume lässt. In diesem Fall muss die Genehmigung nachgeholt und wenn nicht innerhalb von drei Tagen die Erlaubnis vorliegt, das Abhören unverzüglich eingestellt werden. Beispielhaft sei aus dem Polizeigesetz Baden-Württemberg zitiert, was so ein Antrag enthalten muss:

> 1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
> 2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes,
> 3. Art, Umfang und Dauer der Maßnahme,
> 4. im Fall des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
> 5. der Sachverhalt und
> 6. eine Begründung.[7]

Die Beantragung der Überwachung wird also durch Schriftstücke überwacht. So lässt sich später noch genau nachvollziehen wer, wann, womit und warum abgehört wurde. Zudem muss jeder *Einsatz des technischen Mittels*[8] protokolliert werden und die

[6] [4] StPO § 100a
[7] [5] PolG § 23b
[8] [4] Punkt 6

Datensicherheit und -integrität muss nach *dem Stand der Technik*[9] gewährleistet sein. Welche Straftaten nach § 100a StPO als Anlass für eine TKÜ gelten und welche von denen die meisten Abhörmaßnahmen hervorrufen, kann in den jährlich vom Bundesjustizamt herausgegebenen Statistiken nachgeschlagen werden.[10] Wer hier vielleicht an Terrorismus, organisierte Kriminalität oder Kindesmissbrauch denkt, liegt falsch. 2017 war es der Verstoß gegen das Betäubungsmittelgesetz. Etwa 35 Prozent aller Abhörmaßnahmen entfielen auf diese Rubrik. Erst mit großem Abstand folgen *Bandendiebstahl* (11 %), *Betrug und Computerbetrug* (10 %) und *Tötungsdelikte* (10 %). Das Thema Kinderpornographie spielt nur eine marginale Rolle von 0,1 Prozent, obwohl dieser Themenbereich medial stark vertreten ist.
Um noch etwas Polemisches hinzuzufügen: Bei *Straftaten gegen die öffentliche Ordnung* wurden 479 TKÜen angeordnet (von insgesamt 23204), während *Bestechlichkeit und Bestechung von Mandatsträgern* genau 0 TKÜen stattfanden. Es lässt sich nicht herausfinden, welche *Straftaten* es waren, die hier *gegen die öffentliche Ordnung* ausgeführt wurden. Mandatsträger werden gar nicht überwacht. Also die Menschen, die die Gesetze machen, sind von ihnen nicht betroffen. Das soll der Polemik genügen.
Vor zwei Jahren (2017) wurde ein neues Gesetz, das sogenannte *Quellen-TKÜ* verabschiedet. Dabei handelt es sich eigentlich nur um eine Erweiterung des Artikels 100a der StPO, die nötig wurde, da viele Daten inzwischen durch Kommunikationsdienste verschlüsselt werden.[11] Mit den gewöhnlichen Methoden der TKÜ lassen die sich nicht mehr auswerten. Deshalb musste eine besondere Form der TKÜ ausgearbeitet werden, die entweder die Daten abfangen kann, bevor sie verschlüsselt werden oder die eine Entschlüsselung der Daten ermöglicht.[12] Für diese Maßnahme muss oft heimlich Schadsoftware installiert werden, wobei die Methode von der Online-Durchsuchung zu unterscheiden ist, auf die wir weiter unten (im Anhang) zurückkommen. Hier sei aber schon einmal angemerkt, dass über diese Schadsoftware auch auf die Inhalte der Geräte (nicht nur die Kommunikation) zugegriffen werden kann, sowie die Fernsteuerung der Geräte möglich ist.
Der Chaos Computer Club (CCC) machte bereits 2011 darauf aufmerksam, dass diese Art von Programmen deutlich mehr können als bloß die Kommunikation zu überwa-

[9] [4] Punkt 5
[10] [6] Die Statistiken werden seit 2000 veröffentlicht.
[11] Vgl. Kapitel Ende-zu-Ende-Verschlüsselung
[12] Vgl. hierzu die Stellungnahme des Bundeskriminalamtes (BKA), die noch den rechtfertigenden Satz nachschieben: "Hierbei wird nur die Kommunikation erlangt, die auch durch eine „konventionelle“ TKÜ erlangt würden (sic!)." [7]

chen. Nach deren Darstellung können diese Programme das

- Nachladen beliebiger Programme aus dem Internet
- Erstellen von Bildschirmfotos
- Erfassen der Tastaturanschläge
- Ausspielen und Manipulieren von Daten

Was wir besorgniserregend daran finden, ist, dass die Programme nicht nur diese Fähigkeiten haben, die missbraucht werden können, sondern dass die Programme diese Fähigkeiten haben, obwohl sie offiziell einen ganz anderen Zweck erfüllen sollen. Nun kennen wir Informatiker alle die Anekdote, dass ein Kunde mit einer Idee kommt und mit einem völlig anderen Produkt geht, weil die Sichtweisen des Kunden und des Entwicklers nicht in Einklang zu bringen sind. Doch wenn ein Ziel so weit verfehlt wird, liegt die Vermutung nahe, dass andere Ziele anvisiert wurden, als rechtlich möglich sind. Hier stellt sich wieder die Frage nach der Verantwortung des Informatikers, aber diesmal unter dem Licht, dass ein anderes Programm entwickelt werden soll, als es die rechtliche Norm zulässt.
Bei der TKÜ ist unzweifelhaft, dass sie einen Eingriff in die Grundrechte darstellt. Befürworter argumentieren natürlich mit dem Nutzen solcher Methoden und auch wir können uns Situationen vorstellen, in denen eine Überwachung sinnvoll ist, besonders wenn es in den Bereich von organisierter Kriminalität geht. Überrascht hat uns allerdings schon, dass ein großer Teil wegen Drogendelikten überwacht wird. Hier stellt sich schon eher die Frage nach der Verhältnismäßigkeit. Es kommt noch ein ganz anderer Aspekt hinzu. Man mag argumentieren, dass man in einem demokratischen System darauf vertrauen sollte, dass diese Methoden nicht missbraucht werden. Doch die entwickelten System und das Wissen dahinter, werden zusätzlich in andere Länder exportiert, in denen bspw. Menschenrechte nicht geachtet werden. Da stellt sich die Frage nach Verantwortung in einer neuen Dimension.

2.2 Videoüberwachung

Über Kameras, die mit dem Internet verbunden sind, können private Wohnungen auch im Rahmen einer TKÜ-Maßnahme überwacht werden. Bei dem nun folgenden Thema geht es ganz allgemein um die Videoüberwachung. Dabei geht es um

> [d]ie Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung).[13]

Die bei der Videoüberwachung gewonnenen Daten werden meist aufgezeichnet und können auch zu einem späteren Zeitpunkt ausgewertet werden. Dabei können Algorithmen wie automatische Gesichtserkennung oder das automatische Auslesen von Nummernschildern beteiligt sein.
Wenn man die Videoüberwachung rechtlich betrachtet, muss man drei grundlegende Unterscheidungen treffen:

- Überwachung öffentlich zugänglicher Räume,
- Videoüberwachung von Beschäftigten,
- Videoüberwachung in nicht-öffentlich zugänglichen Räume.

Das Bundesdatenschutzgesetz (BDSG) § 4 ff. regelt die Videoüberwachung im öffentlichen Raum. Dort sind die Zweckbindung, Datensparsamkeit und Transparenz, also wesentliche Aspekte des Datenschutzes, geregelt. Nach diesen Kriterien muss auf die Überwachung hingewiesen und Kontaktdaten des Verantwortlichen angegeben werden (durch bspw. Schilder) und es muss ein konkretes Interesse (bspw. die Wahrnehmung des Hausrechtes) vorliegen, bei der keine schutzwürdigen Interessen von Betroffenen überwiegen. Außerdem sind die Daten unverzüglich zu löschen, wenn der Zweck der Aufzeichnung erreicht wurde. [14]
Die staatliche Videoüberwachung liegt in der speziellen Kompetenz der Polizei, die an Landesrecht gebunden ist. Doch allgemein kann man sagen, dass für die Videoüberwachung hohe Hürden zu nehmen sind. Ein Grund für diese Hürden liegt nicht nur im Datenschutz der betroffenen Personen sondern auch in der Überlegung, dass Kriminalität nicht in andere Gebiete verdrängt werden soll. Da nicht überall überwacht werden kann, vertreibt man die Kriminalität von öffentlichen Plätzen in abgelegene Seitenstraßen. Mit diesem Argument führt man fast logisch zwingend auf den Weg, dass **alles** überwacht werden müsse, damit sich kein Verbrecher mehr verstecken kann. In einigen Bereichen wie Kassenräume von Banken, Sparkassen, Eingängen von Spielhallen oder speziellen Industrie-Anlagen (z. B. kerntechnische Anlagen) ist Videoüberwachung sogar rechtlich verbindlich.

[13] [9] BDSG § 4 ff.
[14] Vgl. [9] BDSG § 4, Punkte 1-5

Das Aufzeichnen von Bild und Ton führt zu einer ganzen Reihe von datenschutzrechtlichen Problemen. Es gilt, ist eine Person auf einem Bild identifizierbar (unabhängig ob sie tatsächlich identifiziert wird oder nicht), so unterliegen die Bildaufnahmen dem Datenschutz. Ein häufig gebrachtes Argument gegen öffentliche Videoüberwachung ist die einfache Tatsache, dass fast ausschließlich unverdächtige Menschen gefilmt werden. Dieser Generalverdacht gegen alle Personen widerspricht der Unschuldsvermutung des Einzelnen.
Durch zunehmende digitale Möglichkeiten entstehen Gefahren in ganz neuem Ausmaß. Die bei der Online-Durchsuchung bereits angesprochene Möglichkeit, Daten zu manipulieren, nimmt zu, insbesondere auch die Fähigkeit, Videoaufnahmen zu bearbeiten, ohne dass das später noch nachvollziehbar ist. Stellen wir uns nur vor, was passiert, wenn man in eine Videosequenz eine Person einfügen kann, die nie an diesem Ort war.[15]
Ein weiterer Aspekt digitaler Möglichkeiten ist das automatische Auswerten von Bildmaterial mittels Algorithmen. Besonders an diesem Punkt sind Informatiker involviert. Es ist dann nicht nur der Fall, Menschen in Echtzeit durch Gesichtserkennung zu identifizieren (oder gar Fehlverhalten festzustellen), sondern es kann auch Videomaterial der Vergangenheit nach und nach als neuer Datensatz ausgewertet werden.
Videoüberwachung ist ein kontrovers diskutiertes Thema. Immer wird die Frage der Nutzen/Kosten Abwägung eine Rolle spielen. Befürworter argumentieren, dass Videoüberwachung zur Aufklärung von Straftaten führe und außerdem eine präventive Wirkung habe, indem sie durch den "Beobachtungsdruck" Menschen von Fehlverhalten abhalten könne[16]. Außerdem gebe es auch das Opferrecht der Täterermittlung, für die die Videoüberwachung besonders hilfreich sei. Kritiker der Videoüberwachung ziehen deren Nutzen in Zweifel. Straftaten könnten damit nicht verhindert werden. Besonders terroristische Akte, mit denen Videoüberwachung häufig argumentativ gerechtfertigt wird, würden damit nicht aufgehalten. Diese bekommen ganz im Gegenteil durch das Videomaterial sogar *noch größere Aufmerksamkeit*. Eine Langzeitfolge der Überwachung könnte zudem ein Zwang zum Konformismus sein.

2.3 Vorratsdatenspeicherung (VDS)

Kommen wir zu einem Thema, das in den Medien sehr präsent ist - der Vorratsdatenspeicherung.

[15] Vgl. Deep-Fake
[16] Vgl. Benthams Panoptikum

> Die Vorratsdatenspeicherung (VDS [...]) ist ein kriminalpolitisches Instrument, das die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber eines öffentlichen Kommunikationsnetzes verpflichtet, bestimmte Daten, die von ihnen für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, zum Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten zur Verfügung zu stellen.[17]

Die Ausweisung als ein *kriminalpolitisches Instrument* deutet darauf hin, dass hier Daten von Behörden abgegriffen werden, die nicht für diese Zwecke bestimmt sind. Die Daten stammen aus Angaben von Nutzern und Nutzerinnen, die einen bestimmten Kommunikationsdienst nutzen wollen. Doch das Abgreifen der Daten hat mit der Speicherung noch nichts zu tun. Dies kommt im zweiten Abschnitt des Zitats.

> Dabei geht die erwünschte Speicherfrist deutlich über die für reine Vertragszwecke zulässige Dauer hinaus und ist weder durch Vertragszwecke veranlasst wie die Entgeltabrechnung oder die Erstellung eines Einzelverbindungsnachweises auf Wunsch des Kunden noch durch einen bestimmten Tatverdacht. Es werden deshalb die Daten sämtlicher Vertragspartner des Anbieters anlasslos „auf Vorrat“ gespeichert.[18]

In diesem Abschnitt steckt der Grund, warum das Thema Vorratsdatenspeicherung so kontrovers diskutiert wird. Daten können also auch, nachdem die Nutzung des Services beendet wurde, ausgelesen und verwendet werden. Das Schlüsselwort hier ist das Wort *anlasslos*. So wird eine ganze Gesellschaft unter Generalverdacht gestellt.
Mit den Daten kann das Kommunikationsverhalten (nicht die konkreten Inhalte der Kommunikation) von Personen nachverfolgt werden, woraus sich bspw. Bewegungsprofile (s. o.) erstellen lassen. Dabei ist der erklärte Zweck der VDS eine *verbesserte Möglichkeit der Verhütung und Verfolgung schwerer Straftaten*[19]. Man stellt sich die Frage, wie solch ein Instrument Straftaten *verhindern* könne, während andererseits einleuchtet, dass diese Informationen für eine Täterverfolgung wichtig sind.
An dieser Stelle sollen noch einmal zwei wichtige Abgrenzungen zur TKÜ hervorgehoben werden. Erstens wertet die VDS keine Inhalte von Kommunikation aus und

[17] [15] Wikipedia *Vorratsdatenspeicherung*
[18] [15] Wikipedia *Vorratsdatenspeicherung*
[19] [15] Wikipedia *Vorratsdatenspeicherung*

zweitens werden bei der TKÜ Informationen in Echtzeit überwacht, sofern die Erlaubnis vorliegt, während die VDS Daten aus der Vergangenheit, die bereits gesammelt wurden, auswertet. Der Knackpunkt hier ist eben, dass die Daten zunächst *anlasslos* gesammelt werden müssen, weil man noch nicht weiß, welche später relevant werden. Bei der TKÜ hingegen müssen Informationen zuerst ein gewisses Maß an Relevanz haben, bevor sie gesammelt werden.
Die rechtliche Situation ist durchwachsen, was hauptsächlich daran liegt, dass EU-Recht gegen deutsches Recht steht. Dabei ging die VDS 2006 aus einer EU-Richtlinie hervor, die alle EU-Mitgliedstaaten verpflichtete, ein entsprechendes Gesetz zu verabschieden. Anfang 2008 trat dann in Deutschland eine erste Version in Kraft, die nach Massenklagen im Jahr 2010 vom Bundesverfassungsgericht als verfassungswidrig und nichtig erklärt wurde. Zudem mussten alle bisher gesammelten Daten gelöscht werden. In der Begründung des Urteils hieß es dazu, dass in dem Gesetz keine konkreten Maßnahmen zur Datensicherheit stehen. Außerdem sei die Hürde für staatliche Zugriffe zu gering angesetzt, was gegen Artikel 10 Absatz 1 des Grundgesetzes (*Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.*[20]) verstoße.
Halten wir hier kurz inne: Der Gesetzgeber muss eine EU-Richtlinie umsetzen, die mit hochsensiblen Daten aller ihrer Bürger umgeht, und versäumt dann, für Datensicherheit und einen gerechtfertigten Zugang zu den Daten zu sorgen. Wenn man eine Debatte über den Überwachungsstaat führen will, könnte man hier ansetzen. Mit einer etwas anderen Sicht könnte man auch sagen, der Gesetzgeber habe sich nicht ausreichend Gedanken gemacht, was bedeuten würde, dass die Regierenden gegenüber Daten von Bürgern nicht genügend sensibilisiert sind.
Vier Jahre später (2014) erklärte dann auch der Europäische Gerichtshof die EU-Richtlinie zur VDS für ungültig, da sie mit den Grundrechten der Europäischen Union nicht vereinbar seien. Im gleichen Jahr stellt der Bundesgerichtshof fest, dass Verkehrsdaten vom Anbieter bis zu 7 Tagen gespeichert werden dürfen, allerdings nur für interne Zwecke.
Entgegen der Erklärung des EuGH beschloss 2015 die Bundesregierung ein neues Gesetz zur VDS. Ab dem 01. Juli 2017 musste die Speicherpflicht erfüllt werden, wogegen es viele Verfassungsbeschwerden gab. 2016 bekräftigte dann der EuGH seine Entscheidung, dass die VDS illegal sei und ein Jahr später entschied dann auch das Oberverwaltungsgericht von NRW, dass das Gesetz gegen EU-Recht verstoße. Damit ist die VDS ausgesetzt, was zu der absurden Situation führt, dass Daten vom Anbieter nun

[20] [**?**] Grundgesetz § 10

gespeichert werden können, aber nicht müssen.
Im Gesetzestext ist eine maximale Speicherdauer von zehn Wochen vorgesehen (s.u.).
Es ist verständlich, dass Menschen das Gefühl bekommen, immer mehr in einem Überwachungsstaat zu leben, wenn man die Handlungsweise der Bundesregierung betrachtet. Obwohl der EuGH sich klar positioniert, wird dennoch ein Jahr später ein Gesetz verabschiedet, das der Position zuwiderläuft.
Schauen wir uns doch mal konkret an, welche Daten nach dem Gesetz von 2015 gespeichert werden dürfen und diskutieren, ob wir damit einverstanden wären, wenn der Staat (und die Anbieter auch) diese Daten bekommen.[21]

- Standortdaten bei Beginn eines Telefonats oder bei Beginn einer mobilen Internetnutzung (4 Wochen Speicherfrist)
- Rufnummern, Zeit und Dauer aller Telefonate (10 Wochen Speicherfrist)
- Rufnummer, Sende- und Empfangszeit aller SMS-Nachrichten (10 Wochen Speicherfrist)
- zugewiesene IP-Adressen mit Zeit und Dauer der Internetnutzung (10 Wochen Speicherfrist).

Auf diese Daten darf zugegriffen werden nach einer vorher erteilten richterlichen Anordnung oder bei Gefahr im Verzug.
Wollen wir als Nutzer und Nutzerinnen wirklich, dass jedesmal unser Standort gespeichert wird, sobald wir ins Internet gehen? Sooft wie wir ins Internet gehen, dürfte sich sehr einfach ein genaues Bewegungsprofil von jedem von uns erstellen lassen.
Das Gesetz enthält aber auch ganz klar ein Verbot, dass Inhalte der Kommunikation nicht gespeichert werden dürfen.

> Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.[22]

Zudem muss die *irreversible* Löschung der Daten spätestens eine Woche nach Ablauf der Frist vom Betreiber sichergestellt werden.[23]

[21] Vgl. § 113b TKG Punkte 1-4. [17]
[22] [17] § 113b TKG Punkte 1-4.
[23] Vgl. § 113b TKG Punkte 8. [17]

Befürworter der VDS argumentieren mit der Kriminalitäts- und Terrorismusbekämpfung und es wird wohl kaum Menschen geben, die etwas dagegen haben, dass organisierte Kriminalität oder Kindesmissbrauch aufgeklärt und gestoppt werden kann. Das Argument ist also so gestrickt, dass sich dagegen nicht argumentieren lässt. Deshalb berufen sich Kritiker auf die Verhältnismäßigkeit und stürzen sich auf die Frage, ob eine Bekämpfung von Verbrechen damit überhaupt effektiv erfolgen kann.

> Eine Vorratsdatenspeicherung würde die durchschnittliche Aufklärungsquote von bisher 55 % im besten Fall auf 55,006 % erhöhen.[24]

Das Max-Planck-Institut für ausländisches und internationales Strafrecht zeigt in einer Studie, dass in der Aufklärungsquote mit dem Wegfall der Vorratsdatenspeicherung keine Veränderung im Trend feststellbar ist. [25]
Befürworter führen dagegen Beispiele an wie die Anschläge in Madrid 2004. Außerdem argumentieren sie, dass die Daten ohnehin für Abrechnungszwecke gespeichert würden und der staatliche Zugriff auf diese Daten nur im Einzelfall erfolge und hohen Hürden unterliege. Der Preis, den wir allerdings zahlen würden, so die Kritiker, sei der Eingriff in unsere geschützten Grundrechte (wie das Fernmeldegeheimnis oder Recht auf informationelle Selbstbestimmung). Wollen wir wirklich, dass **alle** unsere Aktionen im Internet auf unseren Anschluss zurückgerechnet werden können, sodass jeder Klick dadurch verfolgbar wird? Außerdem werde der Informationsschutz von bestimmten Personenkreisen gefährlich eingeschränkt. Das betrifft vor allem Journalisten, Ärzte, Juristen, Seelsorger usw.
Die Kritiker der VDS haben noch ein Argument, welches mit dem geringen statistischen Nutzen korreliert, nämlich dass es zu effektive Umgehungsmöglichkeiten (Proxy-Server, VPN) gäbe. Es ist klar, dass besonders schwere Kriminalität (Terrorismus, Bandenkriminalität) diese Möglichkeiten nutzen werden. Das wiederum bedeutet, dass sich mit den erhobenen Daten nur kleinere Delikte aufklären lassen, was dem ursprünglichen Argument der Befürworter widerspricht.
Es ergibt sich die allgemeine Frage, ob Menschen ein Recht haben, im Internet anonym zu sein? (Die Frage kann natürlich noch dahingehend zugespitzt werden, zu fragen, ob ein Mensch, der an Gesellschaft teilnimmt (teilnehmen will) überhaupt das Recht auf Anonymität hat.) Fest steht: Journalisten müssen ihre Quellen schützen können,

[24] [44] Arbeitskreis Vorratsdatenspeicherung, Netzwerk Neue Medien e.V., Neue Richtervereinigung e.V
[25] [45] Max-Planck-Instituts für ausländisches und internationales Strafrecht

Menschen mit kritischen Ideen müssen ihre Meinung äußern können, ohne Angst zu haben, dass man sie verfolgen kann.

3 Beispiel Demo-Überwachung

Das nun folgende Beispiel soll illustrieren, was mit der zunehmenden Technik und den Überwachungsmethoden möglich ist.
Was war geschehen[26] : Am 19. Februar 2011 erfasste die Polizei sämtliche Anrufe und SMS-Nachrichten der Dresdner Südvorstadt. Betroffen waren vermutlich mehr als 30000 Menschen, die mindestens viereinhalb Stunden überwacht wurden.
Offiziell war diese großangelegte Überwachungsaktion dafür geplant, Personen zu finden, die zuvor Polizisten angegriffen hatten. Allerdings demonstrierten an diesem Tag in Dresden 20000 Menschen gegen eine Nazidemonstration (ca. 3000 Teilnehmer). Unter den Demonstranten fanden sich neben Anwohnern auch Journalisten, Anwälte und Politiker.
Das Abgreifen der Daten war von offiziellen Behörden erlaubt worden, aber nur für den vorher bestimmten Zweck.[27] Doch die Daten wurden später auch für andere Ermittlungen verwendet.
So zum Beispiel die von Christian Leye, der ein Mitarbeiter des Bundestagsabgeordneten Sevim Dagdelen (Linkspartei) war.

> In seiner Ermittlungsakte sind rund 15 Handyverbindungen vom 19. Februar zwischen 13.00 und 17.30 Uhr aufgelistet, versehen mit der genauen Angabe des Orts, wo er sich jeweils befand. Aufgeführt sind auch die Namen der Personen, mit denen er Kontakt hatte. "Es wurde ein genaues Bewegungsprofil erstellt", sagt Leye.[28]

Als die Polizei um 16 Uhr seine Personalien aufnahm, ermittelte sie alle auf ihn zugelassenen Telefonnummern. Als seine Mobilfunknummer später in der Funkzellenauswertung auftauchte, ermittelte die Polizei die zugehörigen Namen der Gesprächsteilnehmer. Diese Daten wurden später bei Ermittlungen gegen ihn wegen Behinderung einer angemeldeten Demonstration verwendet.

[26] Vgl. zu den Angaben den Taz-Artikel "Mal eben ausgespäht", [18]
[27] Vgl. oben das Antragsformular für die TKÜ-Überwachung
[28] [18] Taz-Artikel "Mal eben ausgespäht"

Auch der Bundestagsabgeordnete Hans-Christian Ströbele (Bündnis 90/Die Grünen) war bei der Demonstration. Er fügt hinzu, dass Mandatsträger besonders geschützte Personen seien, deren Daten nicht gespeichert werden dürften. Trotzdem finden sich von ihm in Ermittlungsakten Aufenthaltsorte samt Uhrzeiten.
Ob diese Aktion der Verhältnismäßigkeit entspricht ist umstritten. Klar allerdings ist (wir hatten das oben auch im Gesetzestext nachgewiesen), dass die Daten nur für den angegebenen Zweck verwendet werden dürfen. Dies bestätigte dann auch die Staatsanwaltschaft, indem sie untersagte, *weiterhin Handydaten in entsprechende Ermittlungsakten zu übernehmen.*[29] Nachdem die *taz* über diesen Vorfall recherchiert und berichtet hatte, verbot die Staatsanwaltschaft zudem die Verwendung der Daten für Ermittlungen, die nicht mit dem beantragten Zweck übereinstimmten.

4 INDECT

Die EU hat von 1984-2013 sieben Forschungsrahmenprogramme gestartet, die europaweite Fördermaßnahmen beinhalten. Dafür können Projekte eingereicht werden, die dann von verschiedenen Institutionen in Europa gemeinsam bearbeitet werden.

> Primäres Ziel des Forschungsrahmenprogramms ist, die wissenschaftlichen und technologischen Grundlagen in der Gemeinschaft zu stärken und die Entwicklung ihrer internationalen Wettbewerbsfähigkeit zu fördern sowie alle Forschungsmaßnahmen zu unterstützen, die aufgrund anderer Politiken der Gemeinschaft für erforderlich gehalten werden. [30]

Im Rahmen dieser Fördermaßnahme wurde ein Projekt mit dem Namen INDECT genehmigt bzw. angestoßen. Dieses lief unter der Rubrik *Sicherheit* von Anfang 2009 bis Ende 2013. INDECT steht für *Intelligent information system supporting observation, searching and detection for security of citizens in urban environment.* In der Projektbeschreibung stehen folgende Ziele:

- Schaffung einer Plattform, die Daten aus unterschiedlichen (kriminologischen) Quellen zusammenführt
- Automatische Erkennung von Straftaten

[29] [18] Taz-Artikel "Mal eben ausgespäht"
[30] [20] Wikipedia *Forschungsrahmenprogramm*

- Wahrnehmen von abnormalem Verhalten
- Prototyp eines Systems zur Unterstützung der Polizei bei Überwachung von beweglichen Objekten
- Entwicklung einer Suchmaschine, die Bild- und Videomaterial zusammen mit anderen Metadaten analysieren kann
- Entwicklung von Techniken, die das Internet überwachen können und kriminelle Aktivitäten und Verbrechen erkennen.[31]

Die einzelnen Ziele werden in dem Projekt so zusammengefasst, dass es eine zentrale Station gibt, wo die Daten zusammenlaufen, automatisch ausgewertet und ggfs. an Behörden weitergeleitet werden können.

> The INDECT concept of the multimedia platform assumes the elaboration of a distributed system whose principal element is an autonomous node station designed for the purposes defined in the project. The automatic data acquisition station will be used to acquire data, signals and images from the surveyed area, then to pre-process the data intelligently and transmit the gathered information to the remote servers. The distributed data processing system, provided with huge computational power and a vast repository of knowledge connected also to a spatial information system, will be programmed in a way that will allow the automatic detection of behaviours that could pose a potential threat to security and safety.[32]

Mehrmals wird in der Projektbeschreibung von *security and safety* gesprochen, die wegen *terrorism*, *threats* und *criminal activites* in Gefahr sind. Doch besondere Kritik erfuhr das Projekt kurz nach seinem Start wegen einer anders klingenden Formulierung. Nach den Plänen von INDECT war ein entscheidender Ansatzpunkt

> monitoring of various people clusters and detection of abnormal behaviour and situations of danger.[33]

[31] Vgl. die Ziele des Projekts in der Projektbeschreibung. [21] S. 52
[32] [21] Projektbeschreibung *INDECT* S. 52
[33] [21] Projektbeschreibung *INDECT* S. 52

Von verschiedenen Seiten kam die Frage auf, was denn unter *abnormalem Verhalten* zu verstehen sei.[34] In einem Fernsehbericht von *kla.tv* wird das Szenario geschildert: Jemand habe sein Auto auf einem großen Parkplatz am Flughafen geparkt und vergessen, wo es stehe. Als er es dann am Abend sucht und zwischen den Autoreihen scheinbar orientierungslos hin und her eilt, nimmt eine Kamera ein abnormales Verhalten war. Könnte es sich hierbei um einen Autodieb handeln? Die Polizei wird alarmiert.[35]
Diese Beispiele zeigen, dass es bei weitem nicht trivial ist, *abnormales Verhalten* zu definieren. Und es wird noch gefährlicher, wenn man bedenkt, dass mit einem bereits installierten System es jeder Zeit möglich wäre, diesen Begriff zu redefinieren.
Die allgemeine Kritik an INDECT bezog sich aber natürlich auf die fundamentalen Eingriffe in die Grundrechte. So schrieb die von der Piratenpartei mitgetragenen Initiative *STOPP INDECT*

> INDECT ist das umfassendste Überwachungsprogramm, das je installiert werden sollte. [...] INDECT verbindet sämtliche Daten aus Foren, Social Networks (z. B. Facebook), Suchmaschinen des Internets mit staatlichen Datenbanken, Kommunikationsdaten und Kamerabeobachtungen auf der Straße. INDECT wird wissen, wo wir sind, was wir tun, weshalb wir es tun und was unsere nächsten Schritte sein werden. INDECT wird unsere Freunde kennen und wissen, wo wir arbeiten. INDECT wird beurteilen, ob wir uns normal oder abnormal verhalten.[36]

Was hier nicht betrachtet wird, ist, dass INDECT zunächst *nur* ein *Forschungs*projekt ist. Dieses ist, zumindest bei seriöser Forschung, auch dazu in der Lage, Konsequenzen abzuschätzen und einen Einsatz der Technik unter alles Perspektiven gesellschaftlichen Handelns zu betrachten. Es ging in erster Linie noch nicht um den Einsatz[37], der später von Politik umgesetzt werden müsste. Es ist allerdings beängstigend, dass an so einem sensiblen Projekt nicht nur Forschungseinrichtungen sondern auch private Unternehmen beteiligt sind.[38]
Die massenhafte Kritik hatte zur Folge, dass 2011 eine Ethikkommission überprüfte, ob ethische Grundsätze in dem Projekt verletzt wurden. Sie kam zu dem Schluss, dass dies nicht der Fall sei. In ihrer Stellungnahme schrieb sie:

[34] So etwa in dem oben genannten Videobericht des ZDF.
[35] Vgl. Youtube Video *Indect – die neue Generalüberwachung?*, [23]
[36] [46] Piratenpartei Deutschland Landesverband Bayern
[37] Man mag hier die Frage aufwerfen, ob Wissenschaft unabhängig von der Praxis forschen darf.
[38] Vgl. die Auflistung in der Projektbeschreibung. [21] S. 53]

> The algorithms and methodologies underlying the project rely primarily on previously available, usually public, information sources. These include monitoring cameras, public Web pages, etc. The research covered by the INDECT grant, will not consider processing of highly sensitive material, such as telephone intercept, VoIP, etc.[39]

Die Arbeit des Projektes ziele darauf ab, öffentlich zugängliche Daten (wie Überwachungskameras und Internetseiten) automatisiert auszuwerten, um Informationen zusammenzuführen und der Polizei im operativen Einsatz zur Verfügung zu stellen. Es wurde allerdings kritisiert, dass die Ethikkommission hauptsächlich aus Polizei und Industrie zusammengesetzt war. So bleibt die Frage, wie objektiv ihre Einschätzung ist.
Das deutsche Bundeskriminalamt jedenfalls gab in einer Stellungnahme bekannt, dass sie *aufgrund des umfassenden Überwachungsgedankens* eine Zusammenarbeit ablehne. Auch eine Folge der massenhaften Kritik dürfte sein, dass 2010 die Geheimhaltungsvorschrift verschärft wurde. Seitdem entscheidet ein Ethikrat, welche Informationen über das INDECT-Projekt veröffentlicht werden. Man fragt sich als demokratischer Bürger, der möglicherweise später mal über öffentliche Kameras permanent beobachtet und analysiert wird, wie es sein kann, dass die Entwicklung solcher Projekte im Geheimen ablaufen. Sind das nicht ganz klare Zeichen für *abnormales Verhalten*?
Zum Abschluss soll uns noch eine andere Frage beschäftigen: Würden wir uns als Informatiker an einer Universität, an so einem Forschungsprojekt beteiligen? Kann man hier zwischen Forschung und Praxis unterscheiden? Würden wir daran mit forschen, in Videomaterial automatisch Gesichter zu identifizieren, so wie es schon Bestandteil der Methoden der (gelehrten) *Bildverarbeitung* ist?

5 Smartphone

Ein Smartphone sei hier vereinfacht ein sehr handlicher Computer mit Sensoren, wie Kamera und Mikrofon, Akku und Transmitter für verschiedene Frequenzen. Welche Programme auf dem Computer laufen, auf welche Sensoren oder Daten sie zugreifen und was sie versenden, ist für den Nutzer, wie bei den meisten modernen Computern, nicht ersichtlich. Ihre Nutzer speichern auf diesen Geräten viele persönliche Daten wie Bilder, Nachrichten, Termine und Kontaktdaten, aber auch Zugangsschlüssel zu

[39] [47] Indect Ethikkommission

verschiedenen Diensten. Nutzt man zum Beispiel die Instagram-App, so wird auf dem Smartphone ein Schlüssel abgelegt, welcher den Zugang zum Account ermöglicht. Die Daten auf einem Smartphone geben einen intimen Einblick in das Leben des Nutzers, obwohl technisch gesehen nur Daten aus einem Datenträger gelesen werden. Unserer Ansicht nach ist das Smartphone ein ähnlich sensibler „Raum“ wie die Wohnung. Die eigene Wohnung ist nach Deutschem Grundgesetz Artikel 13 besonders geschützt.

> „Die Wohnung ist unverletzlich.“

Es bedarf einem richterlichen Beschluss sie dennoch zu verletzen.[40] Mit den ähnlich sensiblen Daten auf dem Smartphone wird jedoch eher grob gearbeitet. Folglich sollte dieser Raum ähnlich gesetzlich ähnlich stark geschützt werden und Eingriffe in diesen Raum ähnlich schwierig sein.

[40] [25] Grundgesetz Artikel 13

5.1 Auslesen der Daten bei der Einreise

Eine neue Entwicklung ist, dass dieser höchstpersönliche Datenspeicher nun immer öfter beim Grenzübergang ausgelesen wird. Sobald physischer Zugang zum Gerät besteht, können alle Daten ausgelesen werden, sofern es nicht durch besondere Maßnahmen geschützt ist.[41] Neben dem auswerten der verschickten Nachrichten, Bilder, Standorten und weiterem, würde dies den Zugang zu allen Accounts ermöglichen, die auf dem Gerät genutzt werden.

Seit 2017 können die Daten auf Handys zur „Feststellung der Identität und Staatsangehörigkeit des Ausländers“ [26] genutzt werden. Die Daten werden schon bei der Einreise ohne Anlass ausgelesen und gespeichert. Wenn sich die Notwendigkeit dazu ergibt, werden sie vom Bundesamt für Migration und Flüchtlinge (BAMF) ausgewertet. [27]

> „Der Ergebnisbericht listet Ländercodes der gespeicherten Kontakte, Ländercodes der angerufenen und angeschriebenen Nummern, Ländercodes der eingehenden Anrufe und Nachrichten, Lokationsdaten und die in den Nachrichten verwendeten Sprachen auf.“ [28]

Seit 2018 können Grenzbeamten in Neuseeland bei Verdacht auf Verstoß gegen Ein- und Ausfuhrregeln das Smartphone eines Reisenden durchsuchen. Der Reisende ist verpflichtet an der Durchsuchung mitzuwirken und muss auch Passwörter herausgeben. Tut er dies nicht kann eine Geldstrafe bis zu 5000 $ verhängt werden. Das Gerät kann zur Untersuchung oder zur späteren Untersuchung auf unbestimmte Zeit eingezogen werden. [29] Der Verdacht könne ohne Angabe von Gründen ausgesprochen werden. [30] Ob erhobene Daten wieder gelöscht werden ist unklar. Bei der Einreise in die U.S.A. haben die Grenzbeamten sogar ohne Anfangsverdacht die Möglichkeit die Herausgabe von Passwörtern zu verlangen. Weigert man sich, kann das Gerät eingezogen werden und der Zutritt in die U.S.A. verweigert werden. Wenn es nach Ansicht des Grenzbeamten eine Sache der nationalen Sicherheit ist, kann eine Kopie der auf dem Smartphone liegenden Daten angefertigt werden. [31] [32]

[41] Seit dem iPhone 3GS wird die Verschlüsselung durch das setzen eines Passworts für den Sperrbildschirm wirksam. [40] Bei Android-Geräten ist muss die Verschlüsselung manuell gestartet werden und erfordert ein weiteres Passwort bei jedem Start des Gerätes. Für beide gilt die Verschlüsselung schützt nur solange das Passwort nicht weiter gegeben wird und ist am effektivsten, wenn das Gerät ausgeschaltet ist.

Seit 2019 ist bekannt, dass an wenigstens einer Grenze von China jeder Einreisende anlasslos sein Smartphone durchsuchen lassen muss. Dazu muss das Smartphone entsperrt werden. Anschließend wird von den Grenzbeamten eine Software installiert, welche „alle Kurznachrichten, das komplette Adressbuch und die Nutzerkennungen für eine Reihe chinesischer Social-Media-Seiten“ [34] auf einen anderen Computer kopiert. Außerdem wird das Smartphone nach ca. 73000 Dateien durchsucht. [34]

5.2 Überwachung durch W-LAN

Überwachung findet auch ohne physischen Zugang zum Smartphone statt. Denn sobald das Smartphone zur Kommunikation genutzt wird, werden Signale ausgesendet, die sich unbemerkt mitschneiden lassen. Dies ist nicht nur beim Mobilfunk der Fall. Auch Bluetooth und W-LAN[42] lassen sich von anderen Geräten empfangen.
Ist W-LAN aktiviert, sendet das Smartphone ständig Funksignale aus. Diese Signale enthalten die Namen der bekannten W-LAN-Netze und eine Kennung des Smartphones. Man kann sich diese Signale als Bitte um Rückruf vom entsprechenden Netzwerk vorstellen. Diese Signale sind unverschlüsselt und können von jedem empfangen werden. Allein die Kennung reicht aus, um ein Smartphone zu verfolgen. [37] Aber auch die W-LAN-Netze enthalten relevante Informationen. Denn die gleiche Person nutzt meist auch gleichen W-LAN-Netze. Misst man welche W-LAN-Netze ein Smartphone um Rückruf bittet, lässt sich ein Profil über den Nutzer erstellen. Zum Beispiel die Namen der Netzwerke vom letzten Urlaub, das Heimnetz, und das Gastnetz eines Freundes. So lässt nicht nur das Smartphone, sondern auch alle anderen W-LAN-Geräte des Nutzers verfolgen. Wenn man genug dieser Signale aufnimmt, kann sehr genau in Echtzeit die Bewegungen des Smartphones festgestellt werden. Diese Systeme werden derzeit in Läden genutzt, um den Weg durch den Laden zu verfolgen, aber auch um Stoßzeiten vorherzusagen [38], zum Beispiel an der University of California San Diego [39].

6 Smartmeter

Im Jahr 2016 ist das neue Messstellenbetriebsgesetz in Kraft getreten. Es sieht vor, dass bis 2032[43] alle Strommessgeräte gegen „intelligente Messgeräte“ ausgetauscht werden. Sie messen den Stromverbrauch über eine Zeit von meist 15 Minuten und übermitteln

[42] W-LAN kurz für Wireless-Local-Area-Network, auf Englisch of mit Wi-Fi bezeichnet.

[43] sofern es sich um einen Neubau handelt, oder das gemessene Gebäude einer größeren Renovierung unterzogen wurde

dem Messtellenbetreiber diese Informationen. [49] [50] So kann das typische Nutzungsverhalten eines Nutzers ermittelt werden. Eine Veränderung der Lebensgewohnheiten bildet sich dann auch im Stromverbrauch ab. In Xinjiang in China werden diese Daten der Polizei zur Verfügung gestellt. Sie hat ein Programm entwickelt, um Beamten auf ungewöhnlichen Verbrauch hinzuweisen. [51]

7 Ende-zu-Ende-Verschlüsselung

Zu Beginn des 21. Jahrhunderts war die Kommunikation im Internet noch zum Großteil unverschlüsselt. Jede Nachricht, verschickt über das Internet, konnte unbemerkt mitgelesen werden oder verändert werden. Während Snowden Veröffentlichungen haben viele Dienste eine verschlüsselte Verbindung zum Standard gemacht. [52] Bei der Nutzung von aktuellen Verschlüsselungsalgorithmen ist die Verschlüsselung nach heutigen Standards nicht zu brechen.[44] Diese Verschlüsselung findet zwischen dem Client, also der Software auf einem Gerät des Nutzers, und dem Server, auf dem der Dienst angeboten wird, statt. Die Verbindung zwischen Client und Server ist abhörsicher und vor Manipulation geschützt. Allerdings laufen auf dem Server die Nachrichten aller Nutzer zusammen. Die schiere Menge an Informationen gesammelt an einem Punkt weckt das Interesse bei verschiedensten Gruppen[45]. Entsprechend wurden Gesetze erlassen, um die Anbieter zur Mitwirkung zu zwingen. Um dennoch abhörsicher zu kommunizieren, folgte der nächste logische Schritt: Die Verschlüsselung findet nicht mehr zwischen dem Client und einem Server statt, sondern zwischen dem sendenden Client und dem empfangenden Client. Dies nennt man Ende-zu-Ende-Verschlüsselung (E2EE). Ein Anruf zwischen zwei WhatsApp-Nutzern wird auf diese Art und Weise verschlüsselt. Die einzigen bleibenden Schwachpunkte ist die Verschlüsselung und die Software auf den Geräten der Kommunizierenden.

7.1 Funktionsweise

In E2EE wird in modernen Nachrichtendiensten[46] ein Verfahren basierend auf asynchroner Verschlüsselung verwendet. [54] Dabei hat jeder Client einen privaten und einen öffentlichen Schlüssel. Verschlüsselt man einen Text mit dem privaten Schlüssel, kann dieser nur mit dem öffentlichen Schlüssel entschlüsselt werden. Um eine Nachricht zu versenden, wird diese mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.[47] Halten die Clients die privaten Schlüssel geheim und geben sie an niemanden weiter, kann nur der designierte Empfänger die Nachricht mit seinem privaten Schlüssel entschlüsseln. Will ein Dritter Nachrichten entschlüsseln, benötigt er Zugang zu einem der

[44] Zum Beispiel RSA mit 2048bit [53]

[45] Zum Beispiel Staaten, Versicherungen, Werbeunternehmen, Kriminelle

[46] ein Dienst, um Nachrichten zu versenden und zu empfangen, zum Beispiel: WhatsApp, Telegram, Signal

[47] Dies ist eine starke Vereinfachung. Dies ist das Minimum. Meist werden durch komplexere Verfahren noch mehr kryptografische Eigenschaften wie Perfect-Forward-Secrecy erzeugt.

Clients.

7.2 Verbieten?

Ein Staat könnte dort operierenden Unternehmen verbieten, E2EE einzusetzen. Anbieter könnten die Nachrichten ihrer Nutzer mitlesen und ausleiten. Verbietet man E2EE, verliert man die Sicherheit, dass niemand anderes die Nachricht entschlüsseln kann. Den Einsatz von E2EE durch Gesetze zu verbieten, richtet sich immer gegen die Zivilbevölkerung. Denn Kriminelle halten sich per Definition nicht an Gesetze und würden von einem Verbot kaum getroffen werden.

7.3 Hintertür

Die aktuelle Gesetzgebung konzentriert sich daher darauf, die Anbieter von Software zur Kooperation zu verpflichten. [55]
Es gibt verschiedene Möglichkeiten, dies umzusetzen. Eine ist alle Nachrichten beim Versenden auch an eine weitere speichernde Entität zu schicken.[48] Eine solche zentrale Entität wäre ein sehr lukratives Ziel für Hackerangriffe. Der Anbieter könnte aber auch einzelne Clients dazu anweisen, oder staatlichen Akteuren eine Schnittstelle bieten, um diese Anweisung automatisch zu versenden. Damit wäre jeder Client nur eine Anweisung entfernt, die Geheimnisse seines Nutzers zu verraten. Insbesondere Journalisten, Ärzte, Rechtsanwälte und Politiker arbeiten mit Daten, die einen besonderen Schutz bedürfen. Datenschützer stehen gemeinsam mit zivilen Verbänden und Unternehmen gegen Forderungen nach einem solchen Gesetz ein. [59] Ein solcher Eingriff ist sehr schwierig zu detektieren.[49] Um einen Nachweis für eine Überwachung zu erbringen, müsste der Client untersucht werden. Er müsste in einer kontrollierten Umgebung gestartet werden, um zu beobachten, ob im Vergleich zu einem Referenzclient andere Instruktionen von der Software an das Gerät gesendet werden. Der hohe Ressourcenaufwand macht einen solchen Nachweis in der Praxis unwahrscheinlich. Ein Nutzer kann sich also nicht sicher sein, ob er derzeit überwacht wird. Ein ähnlicher Angriff ist auch mit Hilfe der Anbieter des Betriebssystems denkbar. Statt der Ausleitung von Nachrichten würde ein Zugang zum Betriebssystem des Nutzers erstellt werden, um dann die Programme auf dem Gerät nach Bedarf zu verändern. Sollte dieser Zugang gewährt werden, könnte kein Programm auf dem Betriebssystem eine sichere Kommunikation gewährleisten.

[48] auch bekannt als Ghost-Proposal

[49] Da alle Daten verschlüsselt verschickt werden, würden überwachte Clients nur mehr Daten versenden. Allerdings könnte der Anbieter auch bei unüberwachten Clients mehr Daten als nötig versenden.

7.4 Sicherheitslücke

Solche Angriffe können auch ohne die Kooperation der Anbieter erfolgen. Dazu wird eine Sicherheitslücke genutzt, um einen Zugang zum Gerät zu erhalten und beliebige Programme auszuführen. Eine Sicherheitslücke muss zunächst gefunden oder eingekauft werden. Sicherheitslücken haben eine begrenzte Lebenszeit, bevor sie entdeckt und geschlossen werden. Indem diese Sicherheitslücken nicht gemeldet werden, bleiben sie nicht nur für staatliche Akteure in Deutschland länger offen, sondern auch für Kriminelle und Diktaturen. EnternalBlue ist der Name einer Sicherheitslücke in Windows, die, bevor sie an die Öffentlichkeit drang, seit Jahren bei der National Security Agency (NSA) bekannt war. [56] Sie wurde 2017 in einer Malware names WannaCry genutzt. [57]
WannaCry verschlüsselt alle Daten auf einem infizierten Computer und verlangt für die Entschlüsselung ein Lösegeld. Es hat in zivile Organisationen wie Krankenhäusern enormen Schaden erzeugt. Auch die Deutsche Bahn war betroffen. [58]

7.5 Metadaten statt Inhalte

Seit der Wiedereinführung der Vorratsdatenspeicherung[50] ist ein Internetdienstleister, auch genannt Internet-Service-Provider (ISP), verpflichtet, Daten über die Verbindung zu speichern. Durch die Analyse der verschickten Daten kann festgestellt werden, welche Art der Kommunikation stattfindet. Diese Metadaten können einen sehr tiefen Einblick in die Gewohnheiten der Nutzer geben. Wann befindet man sich wo? Welche Dienste und Webseiten werden genutzt? Mit wem wird über das Internet telefoniert? Diese Fragen können schon mit Metadaten beantwortet werden. Solche Analysen werden auch von nicht staatlichen Akteuren durchgeführt. Unternehmen sammeln diese Daten und verkaufen sie weiter. [60] [51] Durch Metadaten können auch Anonymisierungsmaßnahmen umgangen werden. Dazu wird eine Aktivität, die mit Hilfe von Anonymisierungsdiensten erfolgte, mit den Nutzer der entsprechenden Anonymisierungstechnik verglichen. In Harvard hatte ein Student über das TheOnionRouter-Netzwerk[52] (TOR-Netzwerk) eine Bombendrohung geschrieben. Er konnte identifiziert werden, indem alle Studenten verhört wurden, die zum Zeitpunkt des Versands das TOR-Netzwerk

[50] siehe Kapitel 2.3

[51] Die Quelle bezieht sich auf das Plugin „Web of Trust“. Dies hat nicht nur Zeit und Ziel der Verbindung aufgezeichnet, sondern auch die gesamte URL. Die URL enthält oft sensible Daten. Cloudspeicher können über solche erreicht werden. Die URL dient als Schlüssel.

[52] Dieses Netzwerk dient der Anonymisierung im Internet.

nutzten. [61] Es können auch Korrelationen mit anderen Nutzern bestimmt werden. Angenommen ein Verdächtiger hat jede Woche zur gleichen Zeit das Internet über einen bestimmten Netzwerkknoten verwendet. Möchte man erfahren, wer auch da war, könnte in den Metadaten aller nach diesem Muster gesucht werden. Wir halten fest: Metadaten können in den richtigen Händen sehr mächtig sein.

8 Gedankenexperiment

Um die Frage zu beantworten „Was macht dieses Wissen mit uns?“ wollen wir ein kleines Gedankenexperiment wagen. Dabei wird nur eines vieler möglicher Szenarien skizziert. Stellen wir uns vor, wir gehören zu einer friedlichen religiösen Minderheit in einem Staat mit totalem Machtanspruch. Das Nachgehen einer Religion ist verboten, deshalb treffen wir uns im Geheimen regelmäßig jede Woche. Nur Wenige trauen sich an diesen Veranstaltungen teilzunehmen. Eines Tages wird einer der Teilnehmer wegen einer Bagatelle festgenommen. In der automatischen Überprüfung fällt er durch abnormales Verhalten auf. Er schweigt, aber die Spuren sind schon vorhanden. Mit Hilfe der durch die Kameraüberwachung dokumentierten Ein- und Ausgänge, stellt man fest, dass er jede Woche zur etwa gleichen Zeit das Haus verlassen und wenige Minuten später sein Handy abgeschaltet hat. Er tat dies, um den Ort der Treffen nicht zu verraten. So wie er, taten es auch einige der anderen Teilnehmer. Dank der Vorratsdaten können die Handys ermittelt werden, die ein ähnliches Verhalten aufwiesen. Wir werden gemeinsam mit den Anderen inhaftiert. Noch liegen keine konkreten Beweise gegen uns vor. Doch bei der Abfrage der Stromverbräuche in genau dieser Zeit, konnten einige wenige Orte ausfindig gemacht werden, die genau zum Zeitpunkt unserer Treffen einen ungewöhnlich hohen Stromverbrauch auswiesen. Diese wenigen Orte werden durchsucht. Nach einigen Minuten wurde unser Rückzugsort entdeckt.

9 Fazit

Ob wir in einem Überwachungsstaat leben, ist diskutabel. Wir (die Autoren) haben das Gefühl, dass es (noch) nicht so ist.
Klar ist aber auch, dass die neuen technischen Möglichkeiten, die sich erst im letzten Jahrzehnt ergeben haben, eine totale Überwachung stark vereinfachen. Nicht nur können Daten effizient erhoben, gespeichert und international abgerufen, sondern auch mittels automatisierter Algorithmen durchforstet und ausgewertet werden. Jedoch ist

jeder Algorithmus der aus Daten mehr Daten generiert, immer nur so gut, wie die Daten, mit denen er gefüttert wird.[53]
In Zukunft wird es außerdem wichtiger werden, für Datenintegrität zu sorgen. Es muss nachvollziehbar bleiben, woher welche Daten kommen und wie sie zu verstehen sind. Werden Täter etwa aufgrund von Datenbankeinträgen ermittelt, muss sichergestellt sein, dass niemand die Daten der Datenbank manipulieren kann. Dass dies besonders dann gefährlich wird, wenn der Staat die Macht über diese Daten hat, erscheint auch logisch. Staatskritische Denker können mit gefälschten Daten belastet werden, um sie aus den Weg zu räumen. Es muss also auch dafür gesorgt werden, dass die Datensammler nicht diejenigen sind, die verurteilen.

10 Anhang

10.1 Online-Überwachung

Die Online-Überwachung muss von der TKÜ abgegrenzt werden. Sie ist die heimliche Überwachung staatlicher Behörden über das Internet. Soweit es die (unverschlüsselte) Kommunikation über Netzwerke betrifft, handelt es sich um die aus der TKÜ bekannte Internetüberwachung, die nun ihrerseits über das Internet abgegriffen wird. Aber auch die Videoüberwachung von Privatwohnungen oder des Arbeitsplatzes mit Kameras, die an das Internet angeschlossen sind, zählt zur Onlineüberwachung. Davon abgegrenzt werden muss noch die Online-Durchsuchung. Diese Methode benutzt Schadsoftware (aus den Medien bekannt als "Bundestrojanern"), um mittels Internetverbindung auf Daten der Festplatte zuzugreifen. Diese Daten können also unabhängig von Kommunikation ausgelesen werden.
Wie bei der TKÜ schon beschrieben, erlaubt die Online-Durchsuchung nicht nur das Abrufen der Daten sondern auch deren Manipulation, weshalb die Schadsoftware ein hohes Potential für Betrug hat. Jedem von uns könnte kompromittierendes Material (wie kinderpornographische Dateien) untergeschoben werden, ohne dass wir je beweisen könnten, dass es nicht von uns ist. Dieses Szenario beschreibt nur die Gefahr, und wir glauben nicht, dass deutsche Behörden an solchen Aktionen beteiligt sind. Wenn man aber bedenkt, dass diese Software in Länder geliefert werden, in denen ein Diktator seine Macht um jeden Preis erhalten will und in denen staatskritische Journalisten (wie

[53] Zur Illustration ist die berühmte Geschichte Neural Network Follies [48] von Neil Fraser sehr empfehlenswert.

in Medien zu verfolgen) immer wieder in Gefängnissen landen, dann kann man sich nicht mehr so sicher sein, woher das belastende Beweismaterial kommt. Und wer garantiert, dass sich das deutsche politische Klima nicht so zuspitzt, dass auch hierzulande kritische Stimmen ausgeschaltet werden?[54]

10.2 Großer Lauschangriff

Im Rahmen des sogenannten *Großen Lauschangriffs* sind Polizei und Staatsanwaltschaft auch befugt, Wohnung zu überwachen. Diese Maßnahme muss von der Staatsanwaltschaft angeordnet werden.
Vom Großen Lauschangriff ist der *Kleine Lauschangriff* zu unterscheiden, der sich nur auf Gespräche außerhalb der Wohnung, also auf öffentliche Orte oder allgemein zugängliche Büro- und Geschäftsräume, bezieht. Damit grenzt sich der Begriff Wohnung ab, als der Bereich, die der Berechtigte der allgemeinen Zugänglichkeit entzogen und zur Stätte seines Lebens und Wirkens gemacht hat.
Gleichbedeutend kann auch der Terminus *akustische Wohnraumüberwachung* verwendet werden.
Momentan im Gespräch ist der sogenannte Lauschangriff 4.0. Ermittelnde Behörden wollen den Zugriff auf Daten aus smarten Geräten wie Alexa und Siri bekommen dürfen. Nach einer Studie der Postbank[55] nutzen zur Zeit etwa 32 Prozent der Deutschen Sprachassistenten wie Alexa und Siri. Es ist klar, dass hier eine enorme Informationswolke vorhanden ist, die Behörden bei der Aufklärung von Straftaten helfen kann. Das wird dadurch prekärer, dass man in den Zeitungen liest: Zur Serviceverbesserung werden die Daten von Sprachassistenten teilweise ausgewertet und bei diesem Abhören werden auch Straftaten belauscht, die nicht geahndet werden können, weil es dafür keine rechtliche Grundlage gibt.

10.3 Rasterfahndung

Bei der Rasterfahndung werden automatisiert personenbezogene Daten mit verschiedenen Datenbeständen abgeglichen, um Personen(-gruppen) ausfindig zu machen. Dabei geht es nicht darum einzelne Personen zu finden, sondern mithilfe der Merkmale der

[54] Einen sehr guten rechtlichen und auch kritischen Überblick über Möglichkeiten und Grenzen der Onlineüberwachung bietet der Aufsatz *Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme - Rechtsfragen von Online-Durchsuchung und Quellen-TKÜ* von Albrecht/Dienst. [8]
[55] Vgl. den Artikel der FAZ [11]

gesuchten Person die Zielgruppe einzuschränken. Entstanden ist die Methode in den 70er Jahren bei der Fahndung nach RAF-Terroristen.[56].

> Damals wollten die Ermittler in Erfahrung bringen, ob jemand seine Stromrechnung bar und unter falschem Namen bezahlte - weil sie annahmen, dass sich ein Terrorist, der untergetaucht ist, so verhält. Also wurden die Kundendateien von Stromwerken beschlagnahmt, alle Barzahler herausgesucht und dann mit Melderegistern, Versicherungsunterlagen und anderen Datensätzen verglichen. [...] Einer wurde tatsächlich auf diese Art entdeckt.[57]

An diesem Beispiel sieht man sofort, wie aufwändige Methoden der 70er Jahre durch Computer beschleunigt und verselbstständigt werden können. Ein Algorithmus könnte, vorausgesetzt die Daten sind zugänglich, diese Art der Suche in wenigen Sekunden lösen. Und gerade in dieser Beschleunigung liegt die Gefahr, dass solche Algorithmen leichtfertig und zweckentfremdet eingesetzt werden. Denn wenn eine Untersuchung weder Zeit noch Geld kostet, so kann zuerst eine Antwort eingeholt und anschließend geprüft werden, ob etwas mit dem Ergebnis anzufangen ist und ob die Verhältnismäßigkeit gewahrt bleibt.
Wir werden im nächsten Unterpunkt darauf eingehen, mit welchen Daten (s. Vorratsdatenspeicherung, Datenbanken) hier ein Abgleich stattfinden könnte. Aber das Beispiel aus den 70er Jahren zeigt, dass ganz allgemeine Daten (wie das Begleichen der Stromrechnung) notwendig sind, wenn man ein bestimmtes Täterprofil hat. Hier mag also die Gefahr liegen, dass Daten wegen möglicher strafrechtlicher Verfolgungen über Menschen (Stromkunden) gespeichert werden, nur für den Fall, dass sie mal gebraucht werden. In den 70er Jahren hat diese Methode noch keine wesentliche Rolle gespielt, da sich der Aufwand nur in extremen Fällen, wie dem Finden der RAF-Terroristen, lohnte.
Die Rasterfahndung wird in den Bundesländern inhaltlich unterschiedlich umgesetzt. Zusätzlich gibt es aber seit 1992 auch eine Regelung in der Strafprozessordnung. Zum konkreten Ziel dieser Methode heißt es dort: Es

> dürfen, unbeschadet §§ 94, 110, 161, personenbezogene Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit anderen Daten maschinell abgeglichen werden, um Nicht-

[56] Vgl. Wikipedia *Rasterfahndung* [12]
[57] [14] Zeit

> verdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen.[58]

Problematisch ist die Rasterfahndung schon deshalb, weil unschuldige Personen allein aufgrund allgemeiner Merkmale zu Verdächtigen werden. Diese Merkmale können das Geschlecht, Alter, aber auch die Hautfarbe sein. Es ist klar, dass es deshalb genaue Regeln dafür geben muss, wie die Rasterfahndung eingesetzt wird.
Nach § 98 der StPO müssen denn auch *tatsächliche Anhaltspunkte dafür vor[liegen], daß (sic!) eine Straftat von* ***erheblicher*** *[Hervorh. d. Verf.] Bedeutung.*[59] begangen worden ist. Teilgebiete dafür sind:

1. Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. Gebiet des Staatsschutzes
3. Gebiet der gemeingefährlichen Straftaten

Man kann hier also schon erkennen, dass diese Methode nur in schweren Fällen angewendet werden kann. Hinzu kommt im Gesetz folgender Zusatz, der zeigt, dass die Rasterfahndung nicht leichtfertig eingesetzt werden kann:

> Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.[60]

10.4 Bewegungsprofile

Wie bei der Rasterfahndung werden beim Anlegen von Bewegungsprofilen auch Daten aus ganz unterschiedlichen Quellen verknüpft, um Bewegungen (und teilweise auch Handlungen) einer Person nachzuvollziehen.
Die Informationsquellen können sein:

1. Handyortung (Funkzellen, GPS, WLAN, Bluetooth)

[58] [13] StPO § 98a
[59] [13] StPO § 98a
[60] [13] StPO § 98a

2. Kaufverhalten mittels Kundenkarten
3. RFID-Chips (auf Kaufhauswaren, elektronischen Tickets)
4. Zusammenfügen von Aufenthaltsorten (mittels Kreditkartenrechnungen, Handyortung)
5. Echtzeitverfolgung mittels positionssendender GPS-Ortungsgeräte

Gerade durch die GPS-Ortung kann heutzutage nicht nur ein Bewegungsprofil erstellt werden, das etwas über einen vergangenen Zeitraum der betreffenden Person aussagt, sondern es ist auch Echtzeitverfolgung möglich. Dafür müssen die Personen selbst solche Geräte besitzen, die GPS-Daten senden können, aber wer von uns besitzt heute nicht ein Smartphone, welches das kann?

10.5 Datenbanken

Wenn wir bei der Speicherung von Daten sind, können wir noch eine weitere Frage hinzufügen: Sollte der Staat berechtigt sein, sich Datenbanken aufzubauen? Es ist klar, dass für eine Strafverfolgung Daten benötigt werden und irgendwo müssen diese Daten herkommen. Aber dürfen Daten *anlasslos* gespeichert werden oder dürfen nur in einer konkreten Ermittlung erhobenen Daten verwendet und gespeichert werden. Wir versuchen die Frage noch zu konkretisieren: Sollten Fingerabdrücke von verurteilten Verbrechern gesammelt werden dürfen oder von niemanden oder von allen Menschen? Konkret geht es um die Gendatenbank. In dieser können genetische Informationen über Personen (wie der Fingerabdruck) gespeichert werden, sodass Menschen anhand von DNA-Spuren eindeutig bestimmt werden können.
Das Problem, was wir hier nochmal aufmachen wollen, ist die Frage, was soll gespeichert werden, um bei (konkreten) Ermittlungen zu helfen. Gehen wir also mal davon aus, dass wir alle wollen, dass (schwere) Straftaten aufgeklärt und verhindert werden. Wie weit wollen wir dafür gehen? Denn mit dem Argument der Aufklärung von Straftaten können beliebig viele Daten gesammelt werden. Also wo würden Befürworter eine Grenze ziehen und wo würden Kritiker Zugeständnisse machen?
Es liegt in der Natur der Fragen, dass sie nicht abschließend beantwortet werden können, aber sie müssen diskutiert werden. Und das Seminar *Informatik und Gesellschaft* bietet dafür einen idealen Rahmen.

Literatur

[1] Wikipedia. Überwachungsstaat.
https://de.wikipedia.org/wiki/%C3%9Cberwachungsstaat (abgerufen am 22.05.2019)

[2] Duden. überwachen.
Online verfügbar unter
https://www.duden.de/rechtschreibung/ueberwachen (abgerufen am 16.05.2019)

[3] Duden. Telekommunikation.
Online verfügbar unter
https://www.duden.de/suchen/dudenonline/telekommunikation
(abgerufen am 15.06.2019)

[4] Strafprozessordnung § 100a.
Online verfügbar unter
https://dejure.org/gesetze/StPO/100a.html (abgerufen am 15.06.2019)

[5] Polizeigesetz NRW § 23b. Online verfügbar unter
https://dejure.org/gesetze/PolG/23b.html (abgerufen am 15.06.2016)

[6] Bundesamt für Justiz : Referat III 3.
Übersicht Telekommunikationsüberwachung. Online verfügbar unter
https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html
(abgerufen am 15.06.2019)

[7] Bundeskriminalamt. Quellen-TKÜ und Online-Durchsuchung : Notwendigkeit, Sachstand und Rahmenbedingungen. Online verfügbar unter
https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html
(abgerufen am 16.06.2019)

[0]Für Webseiten wurde die Verlinkung, wenn möglich, über das WebArchive getätigt. Dies fertigt einen Schnappschuss der Website zu einem bestimmten Zeitpunkt an. So kann auch später noch nachvollzogen werden wie die Website zum Zeitpunkt des Verfassens aussah, beziehungsweise auf welche Version der Webseite sich der Inhalt bezieht. Sollte die Webseite nicht mehr erreichbar sein, bleibt der Schnappschuss erhalten.

[8] Albrecht F.; Dienst S. Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme - Rechtsfragen von Online-Durchsuchung und Quellen-TKÜ. In: JurPC Web-Dok. 5/2012, Abs. 1-65. Der Beitrag ist auch online verfügbar unter https://www.jurpc.de/jurpc/show?id=20120005 (abgerufen am 15.06.2019).

[9] Bundesdatenschutzgesetz § 4.
Online verfügbar unter https://dejure.org/gesetze/BDSG/4.html.

[10] Abus August Bremicker Söhne KG Rechtliche Grundlagen der Videoüberwachung in Deutschland. Online verfügbar unter
https://www.abus.com/ger/Ratgeber/Recht/Rechtliche-Grundlagen/Videoueberwachung (abgerufen am 16.06.2019)

[11] FAZ. Jeder dritte Deutsche nutzt Sprachassistenten. Online verfügbar unter https://m.faz.net/aktuell/wirtschaft/diginomics/jeder-dritte-deutsche-nutzt-sprachassistenten-16229830.html (abgerufen am 18.06.2019)

[12] Wikipedia. Rasterfahndung. https://de.wikipedia.org/wiki/Rasterfahndung (abgerufen am 22.06.2019)

[13] Strafprozessordnung § 98a.
Online verfügbar unter
https://beck-online.beck.de/Dokument?vpath=bibdata%2Fges%2Fstpo%2Fcont%2Fstpo.p98a.htm&pos=2&hlwords=on (abgerufen am 15.06.2019)

[14] Biermann, Kai. Für Algorithmen ist jeder verdächtig. In: Zeit 19.06.2013.
Online verfügbar unter
https://www.zeit.de/digital/datenschutz/2013-06/mustererkennung-algorithmen-terror
(abgerufen am 15.06.2019)

[15] Wikipedia. Vorratsdatenspeicherung.
https://de.wikipedia.org/wiki/Vorratsdatenspeicherung (abgerufen am 22.06.2019)

[16] Grundgesetz § 10.
Online verfügbar unter
https://www.gesetze-im-internet.de/gg/BJNR000010949.html
(abgerufen am 15.06.2019)

[17] Telekommunikationsgesetz § 113b. Online verfügbar unter https://dejure.org/gesetze/TKG/113b.html (abgerufen am 16.06.2019)

[18] Wrusch, Paul. Mal eben ausgespäht: Demo-Überwachung per Mobilfunk. In TAZ 19.06.2011. Online verfügbar unter: https://taz.de/!5118324/

[19] ZDF. INDECT - Das EU-Überwachungsprojekt. Abrufbar auf Youtube unter https://www.youtube.com/watch?v=38tqDAapA-8 (abgerufen am 18.06.2019).

[20] Wikipedia. Forschungsrahmenprogramm. https://de.wikipedia.org/wiki/Forschungsrahmenprogramm (abgerufen am 18.06.2019)

[21] European Commission. Security Research : Towards a more secure society and increased industrial copetitiveness. Online verfügbar unter http://rp7.ffg.at/de/rp7.ffg.at/upload/medialibrary/towards-a-more-secure_en.pdf
(abgerufen am 18.06.2019)

[22] Wikipedia. INDECT. https://de.wikipedia.org/wiki/INDECT
(abgerufen am 18.06.2019)

[23] Kla.tv. Indect - Die neue Generalüberwachung?. Abrufbar auf Youtube unter https://www.youtube.com/watch?v=qlgV3uFt6bk

[24] Statista Research Department. Umfrage zum Vertrauen in die Institutionen in Deutschland 2018. Online verfügbar unter https://de.statista.com/statistik/daten/studie/814334/umfrage/vertrauen-in-die-institutionen-in-deutschland/ (abgerufen am 16.05.2019)

[25] Grundgesetz Artikel 13

[26] . Asylgesetz (AsylG) § 15a Auswertung von Datenträgern, Stand: 2019 August.

[27] 18. Deutscher Bundestag. Deutscher Bundestag Drucksache18/13551 Seite 12 8. ff.

[28] 18. Deutscher Bundestag. Deutscher Bundestag Drucksache18/13551 Seite 11

[29] State of New Sealand. Customs and Excise Act 2018, 228 - Data in electronic devices that are subject to control of Customs

[30] Radio New Zealand. Interview mit dem Sprecher der Council for Civil Liberties, Thomas Beagle https://web.archive.org/web/20181011104241/https://www.radionz.co.nz/news/national/367642/travellers-refusing-digital-search-now-face-5000-customs-fine, 2018

[31] The Canadian Press. https://www.cbc.ca/news/technology/usa-border-phones-search-1.4494371, 2018

[32] Alex Hern. https://web.archive.org/web/20190701214747/https://www.theguardian.com/us-news/2017/apr/09/uk-tourists-to-us-may-get-asked-to-hand-in-passwords-or-be-denied-entry, 2017

[33] The Associated Press. https://apnews.com/c96a215355b242e58107c2125c18fc4a, 2019

[34] Svea Eckert und Jan Lukas Strozyk. Überwachung an der Gremnze. Chinesische App späht Smartphones aus. Auf tagesschau.de vom 02.07.2019. https://web.archive.org/web/20190705191935/https://www.tagesschau.de/investigativ/ndr/china-ueberwachung-103.html, 2019

[35] 18. Deutscher Bundestag Deutscher Bundestag Drucksache 18/5088 Seite 12

[36] Bundesnetzagentur. Speicherdauer von Vorratsdaten. https://web.archive.org/web/20190503085439/http://wiki.vorratsdatenspeicherung.de/images/BNetzA_Speicherdauer.pdf

[37] Latanya Sweeney. My Phone Your Service. Federal Trade Commission. https://web.archive.org/web/20190618011736/https://www.ftc.gov/news-events/blogs/techftc/2014/02/my-phone-your-service, 2014

[38] Tracking with Wifi. https://www.waitz.io/index.html

[39] Tracking with Wifi in UC, San Diego https://waitz.io/geisel-live?fbclid=IwAR18n-SmB2hZ-VBqbeA0pkGZf8109Vra3TJcp83HS5ppUsuZP71nI6zEZ34,

[40] How to: Encrypt your iPhone. https://ssd.eff.org/en/module/how-encrypt-your-iphone, 2018

[41] Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG)

[42] Deutscher Bundestag Drucksache 19/881 Seite 9

[43] Jannis Brühl. Passanger-Name-Record für Zug, Schiff und Bussreisen. Süddeutsche Zeitung https://www.sueddeutsche.de/digital/pnr-ueberwachung-eu-zuege-schiffe-busse-1.4526751, 2019

[44] Arbeitskreis Vorratsdatenspeicherung, Netzwerk Neue Medien e.V. und Neue Richtervereinigung e.V.. Stellungnahme zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG https://web.archive.org/web/20181125201409/http://www.vorratsdatenspeicherung.de/images/stellungnahme_vorratsdatenspeicherung.pdf Seite 32, 2007

[45] Max-Planck-Institut für ausländisches und internationales Strafrecht. Schutzlücken durch Wegfall der Vorratsdatenspeicherung?. https://web.archive.org/web/20151013205824/http://vds.brauchts.net/MPI_VDS_Studie.pdf, Seite 120, 2011

[46] Piratenpartei Deutschland Landesverband Bayern. STOPP INDECT. https://web.archive.org/web/20120525225850/http://www.stopp-indect.info/?page_id=2&lang=de

[47] Indect Ethikkommission. Abschlussbericht. https://web.archive.org/web/20190202040920/http://www.indect-project.eu/approach-to-ethical-issues

[48] Neil Fraser. Neural network follies. https://web.archive.org/web/20190719160829/https://neil.fraser.name/writing/tank/, 1998.

[49] E.ON. Smart Meter Pflicht in Deutschland. https://web.archive.org/web/20190816181636/https://www.eon.de/de/eonerleben/smart-meter-pflicht-in-deutschland.html

[50] Messstellenbetriebsgesetz §29 Absatz 3

[51] Steffen Wurzel. Polizei-App iüberwacht Millionen Chinesen. Auf tagesschau.de. https://web.archive.org/web/20190703005114/ https://www.tagesschau.de/ausland/china-polizei-app-101.html, 2019

[52] Anna Mulrine. New encryption technology is aiding terrorists intelligence director says. https://web.archive.org/web/20180214112410/https://www.csmonitor.com/USA/ Politics/monitor_breakfast/2016/0425/New-encryption-technology-is-aiding-terrorists-intelligence-director-says

[53] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-02102-1 Version:2019-01 Stand:22. Februar 2019 - Seite 38

[54] Moxie Marlinspike, Trevor Perrin. The X3DH Key Agreement Protocol. https://web.archive.org/web/20190719032338/https://signal.org/docs/specifications/x3dh/, 2016.

[55] Australia data encryption laws explained. https://www.bbc.com/news/world-australia-46463029, BBC News, 2018.

[56] Ellen Nakashima, Craig Timberg. NSA officials worried about the day its potent hacking tool would get loose. Then it did. https://web.archive.org/web/20190810000504/ https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html, 2017

[57] Fabian A. Scherschel. Bluescreen als Retter: Windows XP zu instabil für WannaCry. https://www.heise.de/security/meldung/Bluescreen-als-Retter-Windows-XP-zu-instabil-fuer-WannaCry-3730059.html, 2017

[58] Volker Briegleb. WannaCry: Was wir bisher über die Ransomware-Attacke wissen. https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, 2017

[59] Geplanter Eingriff in Verschlüsselung von Messenger-Diensten hätte fatale Konsequenzen. Offener Brief an das Bundesministerium des Innern, für Bau und Heimat. https://cyber-peace.org/wp-content/uploads/2019/06/Offener-Brief-Geplanter-Eingriff-in-Verschl%C3%BCsselung-von-Messenger-Diensten-Google-Docs.pdf

[60] Nackt im Netz: Millionen Nutzer ausgespäht. https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

[61] Runa A. Sandvik. Harvard Student Receives F For Tor Failure While Sending 'Anonymous' Bomb Threat.
In Forbes. https://www.forbes.com/sites/runasandvik/2013/12/18/harvard-student-receives-f-for-tor-failure-while-sending-anonymous-bomb-threat/, 2013.