Angelika Adensamer

Aspekte einer Überwachungs-Gesamtrechnung

Eine Überwachungs-Gesamtrechnung ist notwendig, weil die Betrachtung der einzelnen gesetzlichen Überwachungsbefugnisse alleine nicht ausreichend Aufschluss über die Lage der Freiheitsrechte und Achtung der Privatsphäre geben kann. Dies wird anhand von drei Beispielen konkretisiert: 1. technologische Neuerungen, 2. die Größe von Datensets und 3. private Speicherverpflichtungen. Die Ausweitung staatlicher Überwachung erfolgt nicht allein durch die Ausweitung der gesetzlichen Ermittlungsbefugnisse. Auch technische Entwicklungen und Speicherverpflichtungen und -praktiken müssen in der Evaluierung von Überwachungsbefugnissen eine Rolle spielen und unter Umständen zu ihrem Rückbau führen.

Als Grundrechtsorganisation ist epicenter.works die Kontrolle der staatlichen Überwachungsbefugnisse und ihre Beschränkung auf das absolut Notwendige ein großes Anliegen. Daher haben wir schon 2016 einen ersten Aufschlag für eine Anleitung zur Überwachungs-Gesamtrechnung im Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich (HEAT)[1] *gemacht. Drei Jahre später überarbeiten wir dieses nun, um es verständlicher und lesbarer als „Handbuch Überwachung" aufzubereiten. Das* Handbuch Überwachung *soll einen Überblick über alle polizeilichen Überwachungsbefugnisse geben: die Voraussetzungen ihres Einsatzes, ihre Geschichte, politische Kontroversen, die sich um sie entsponnen haben, ihren Grund- und Datenschutz- sowie EU-rechtlichen Rahmen, bis hin zu dem, was wir über die Häufigkeit ihres Einsatzes und ihre Effektivität wissen. Auch neuere Überwachungstechnologien, ihr Einsatz in Österreich und ein Ausblick darauf, was noch auf uns zu kommen könnte, werden darin Platz finden. Die Zielgruppe des Handbuchs sind einerseits alle interessierten Menschen, die sich mehr in die Debatte über staatliche Überwachung einbringen möchten, aber davor zurück schrecken, weil das Thema eher unübersichtlich und kompliziert ist. Andererseits soll es auch eine Hilfestellung sein für Menschen, die zu dem Thema arbeiten ohne Rechtswissenschaften studiert zu haben, beispielsweise Journalisten und Journalistinnen oder Politikerinnen und Politiker.*

Das Handbuch soll die Debatte über Überwachungsbefugnisse erweitern und mehr Menschen eine Informationsgrundlage geben, um sich an dieser zu beteiligen. Außerdem soll das Handbuch eine Grundlage für eine Überwachungs-Gesamtrechnung darstellen, um die Politik dazu zu bewegen, sich einen Überblick über das Ausmaß staatlicher Überwachung, ihre Notwendigkeit und ihre Grundrechtskonformität zu verschaffen. Dies soll geschehen, bevor Überwachungsbefugnisse immer weiter ausgeweitet werden, und soll letztendlich in Bereichen, wo sie überschießend und unverhältnismäßig sind, auch zu einem Abbau der Überwachungsbefugnisse führen.

Das Konzept der Überwachungs-Gesamtrechnung geht auf ein Urteil des deutschen Bundesverfassungsgerichts aus 2010 hervor, in dem der Gesetzgeber „in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung" angehalten wird.[2] Eine Überwachungs-Gesamtrechnung ist also deswegen notwendig, weil die Betrachtung der einzelnen gesetzlichen Überwachungsbefugnisse alleine nicht ausreichend Aufschluss über die Überwachungssituation und im Umkehrschluss über die Lage der Freiheitsrechte und Achtung der Privatsphäre geben kann. Ich möchte diesen Gedanken im Folgenden anhand von drei Problemfeldern konkretisieren: Das erste betrifft die Ausweitung von Überwachungsbefugnissen durch technologische Neuerungen, das zweite die Größe von verarbeiteten Datensets und das dritte Speicherverpflichtungen, die polizeiliche oder nachrichtendienstliche Abfragen ermöglichen.

1. Ausweitungen von Überwachungsbefugnissen durch technologische Neuerungen

Technischen Fortschritt nutzen auch die Ermittlungsbehörden, und dies oftmals, ohne dass für den Einsatz neuer Überwachungstechnologien auch neue und eigene gesetzliche Befugnisse geschaffen werden. Die neuen Technologien werden auf Basis alt hergekommener Rechtsgrundlagen eingesetzt, obwohl die neuen Überwachungstechnologien die Grundrechtseingriffe massiv verstärken. Oft wird in diesem Zusammenhang von „Technologieneutralität" der Rechtsgrundlagen gesprochen, beispielsweise im Bezug auf die Strafprozessordnung in den Materialien zum Überwachungspaket, das 2018 die Überwachungsbefugnisse in Österreich massiv ausweitete[3]. Der Begriff der Technologieneutralität ist aber im Hinblick auf die veränderte Intensität der Grundrechtseingriffe irreführend.

Es ist eine durch die Menschenrechte garantierte Voraussetzung, dass bei der Einführung von Überwachungsbefugnissen eine Einschätzung darüber zu treffen ist, ob ihr Nutzen im Verhältnis zu ihrer Eingriffsintensität steht (Verhältnismäßigkeitsprüfung). Ändert sich im Nachhinein aber die Eingriffsintensität der Befugnis, kann sich auch das Ergebnis der Verhältnismäßigkeitsprüfung ändern und die Befugnis somit grundrechtswidrig werden. Aus diesem Grund wäre eine regelmäßige systematische Überprüfung der Recht- und Verhältnismäßigkeit der Überwachungsmaßnahmen notwendig. Unter Umständen müssen diese dann eingeschränkt, eingestellt oder abgeschafft werden. Die Ausweitung von Befugnissen durch neue Technologien lässt sich anhand folgender Beispiele illustrieren: 1. Automatische Gesichtserkennung, 2. Drohnen zur Videoüberwachung und 3. *Predictive Policing.*

Im April 2019 wurde bekannt, dass die österreichische Polizei plant, ab Dezember desselben Jahres, Software zur *automatischen Gesichtserkennung* einzusetzen.[4] Eine neue gesetzliche Grundlage ist dafür nicht vorgesehen, sondern die neue Analysesoftware soll auf Basis allgemeiner sicherheitspolizeilicher Bestimmungen verwendet werden.[5] Die Software soll Standbilder aus Videoüberwachungsmaterial berechnen, die das Gesicht einer verdächtigen Person zeigen und diese maschinell mit Bildern der polizeilichen erkennungsdienstlichen Datenbank abgleichen. Es wird davon ausgegangen, dass dieses Abgleichdatenset ein bis fünf Millionen Datensätze umfasst.[6] Es liegt auf der Hand,

dass ein automatischer Abgleich mit Millionen von Gesichtern eine andere Dimension eines Grundrechtseingriffs darstellt als die menschliche Datenauswertung.

In Österreich werden zur Zeit in einer Pilotphase erstmals 76 *Drohnen* zur polizeilichen Videoüberwachung – unter anderem zur Überwachung von Versammlungen – eingesetzt, und dies ohne neue Rechtsgrundlage[7]. Auch in Deutschland wird der Einsatz von Drohnen durch die Polizei diskutiert.[8] Der Einsatz von Drohnen verändert die polizeilichen Befugnisse zur Videoüberwachung maßgeblich. Drohnen sind beweglicher als heute noch üblichere Stand- und Mastkameras. Das bedeutet, sie können aus anderen Perspektiven filmen, beispielsweise in Privatwohnungen hinein. Außerdem ist es weitaus schwieriger, einer Drohne bewusst auszuweichen, als es bei weniger beweglichen Kameras möglich ist.

Eine weitere technologische Veränderung althergebrachter Polizeibefugnisse stellt *Predictive Policing* dar. Um ihre Arbeit „vorhersehend" zu gestalten, verarbeitet die Polizei je nach Programm große Mengen personenbezogener Daten, Daten über Kriminalitätsaufkommen u. ä. In Österreich ist derzeit ein Programm in Betrieb, das der Vorhersage von Wohnraumeinbrüchen dienen soll.[9] In die Gebiete, die durch das Programm als besonders gefährdet gekennzeichnet werden, fahren Streifendienste öfter zur Prävention. Dadurch erlangt die einfache Befugnis des Streifendienstes eine völlig neue Bedeutung, die neue Fragen, wie nach Diskriminierung durch Algorithmen, Verantwortlichkeit, Transparenz und Kontrolle aufwirft. Solche Systeme wirken zurück auf die Datenbasis auf der sie funktionieren. Es kann beispielsweise sein, dass man aus den Gebieten, in denen öfter kontrolliert wird, mehr Daten über „verdächtige" Merkmale bekommt, die dann wiederum die Basis für weitere Kontrollen werden. Das würde eine Rückkoppelungs-Schleife erzeugen. Die Frage, was ein Streifendienst eigentlich bewirkt, und ob er das richtige Mittel zur Bekämpfung von Wohraumeinbruch ist, wird dabei überhaupt nicht mehr gestellt.

Auch das System der *Fluggastdatenverarbeitung,* die aufgrund einer EU-Richtlinie[10] für alle Mitgliedstaaten verpflichtend ist, birgt eine Form des *Predictive Policing*. Laut Erwägungsgrund 7 der Richtlinie sollen die Daten unter anderem dazu dienen, Personen zu ermitteln, die bis dahin nicht verdächtig waren. In diesen Datenbanken mit Daten von Millionen Menschen[11] wird also erstmals ohne vorherigen Verdacht mittels *Data Mining* erst Verdacht generiert, das heißt die Polizei wird völlig unabhängig davon tätig, ob ein Verbrechen geplant wird oder begangen wurde. So verändert sich die Polizeiarbeit durch den Einsatz von Algorithmen grundlegend.

Diese Ausweitungen von Überwachung durch neue technologische Möglichkeiten sind ohne demokratische Beschlüsse und damit weitgehend auch ohne breite gesellschaftliche Debatte nicht vertretbar.

2. Größe der Datensets und zunehmende Prävalenzfehler

Mit der zunehmenden Größe von Datensets im Zeitalter von Massenüberwachung und *Big Data* bei gleichbleibender (in Österreich aktuell sogar sinkender Kriminalitätsrate) nimmt auch die Gefahr für alle Menschen zu, selbst als falsche Treffer *(false positives)* eingestuft zu werden. Die Vergrößerung der Datensets mit denen gearbeitet wird, verschlechtert die Effizienz von Überwachungsmaßnahmen, statt sie zu verbessern oder auch nur neutral zu skalieren. Der für viele Menschen intuitiven Annahme, mehr Daten seien immer besser, liegt der sogenannte Prävalenzfehler *(Base Rate Fallacy)* zugrunde. Dieser Fehler besteht darin, dass einer relativen hohen Treffsicherheit vertraut wird, ohne die zugrunde liegende Wahrscheinlichkeit eines Treffers im gesamten *Sample* zu beachten.[12]

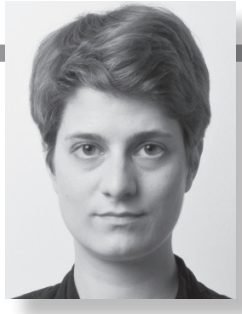
Auch bei guter Trefferquote wird es zu einer sehr hohen Rate an falschen Treffern kommen, wenn in einem sehr großen Datenset (wie den Fluggastdaten) nach einem sehr seltenen Ereignis gesucht wird (beispielsweise Terroranschlägen). Jeder falsche Treffer bedeutet, dass eine Person genauer überwacht wird, die sich nichts zu Schulden kommen hat lassen. Die Wahrscheinlichkeit wird also immer höher, ungerechtfertigt ins Visier zu kommen. In Österreich hielten in den ersten acht Monaten des Fluggastdatensystems nur 0,15 % aller 190.541 Treffer einer genaueren Überprüfung stand[13] und auch in Deutschland geht man nur von 0,1 % korrekten Treffern aus.[14]

Da wegen der fortschreitenden Digitalisierung immer mehr Daten über alle Lebensbereiche der Menschen vorliegen und diese immer häufiger gesamt und automatisch analysiert werden, um auf Basis von Algorithmen Entscheidungen zu treffen, werden auch die falschen Treffer zunehmen und mehr und mehr Menschen von den Folgen betroffen sein.

3. Interaktion von Speicherverpflichtungen mit polizeilichen Abfragen

Speicherverpflichtungen Privater, insbesondere von Telekommunikationsbetreibern und -betreiberinnen, können die Eingriffsintensität von polizeilichen Abfragebefugnissen stark be-

Angelika Adensamer



Angelika Adensamer beschäftigt sich als Juristin und Kriminologin vor allem mit Kriminalpolitik, Überwachungsbefugnissen der Polizei und der Wahrung von Grundrechten in diesen Bereichen. Sie arbeitet bei der Grundrechts-NGO epicenter.works in Wien als Policy Advisor.

einflussen. So ist die österreichische Polizei befugt, ohne weitere Voraussetzungen Stammdaten von Telekommunikationsbetreibern und -betreiberinnen zu verlangen. Auch die Auskunft über Verkehrs- und Standortdaten ist unter bestimmten Voraussetzungen möglich. Üblicherweise speichern die Betreiber Verkehrs- und Standortdaten nur zu Verrechnungszwecken und löschen sie, sobald die Rechnungen unwidersprochen bezahlt wurden. Die Daten darüber hinaus zu speichern, ist nicht im Interesse der Anbieter und Anbieterinnen, sehr wohl aber in dem der Polizei, wie die nicht enden wollende Debatte um die Vorratsdatenspeicherung zeigt.

Mit der *Vorratsdatenspeicherung* sollte 2006 die EU-weite Verpflichtung geschaffen werden, die betreffenden Daten für sechs Monate zu speichern, um den Zugriff von Ermittlungsbehörden länger zu ermöglichen. Sie wurde vom EuGH jedoch 2014 für grundrechtswidrig erklärt. Dennoch gibt es auf EU-Ebene aktuell Bestrebungen, sie wieder einzuführen.[15] Hier wird eine Überwachungsmaßnahme nicht als polizeiliche Befugnis geregelt, sondern über den Umweg einer Speicherverpflichtung.

Mit dem Überwachungspaket wurde 2018 in Österreich unter anderem die *Anlassdatenspeicherung* (auch *Quick Freeze)* eingeführt. Nun können die Sicherheitsbehörden bei Bedarf eine Speicherpflicht von Verkehrs- Standort-, und Zugangsdaten von bis zu einem Jahr anordnen. Es handelt sich also quasi um eine – „Vorratsdatenspeicherung light".

Ähnlich ist es bei der *SIM-Karten-Registrierung,* welche in Österreich ebenfalls mit dem Überwachungspaket 2018 eingeführt wurde und seit 1.9.2019 in Kraft ist. Seither muss die Identität aller Personen registriert werden, die SIM-Karten oder Guthaben kaufen. Neu ist nicht nur eine Speicherverpflichtung sondern die Pflicht, die Käuferdaten überhaupt zu erheben.

Ermittlungstechnische Speicherverpflichtungen sind aber nicht die einzigen, die das Potenzial haben, Überwachung auszuweiten, ohne die gesetzlichen Grundlagen der Polizeiarbeit zu verändern. In dieser Hinsicht wurden beispielsweise Entwürfe zur Einführung einer *Digitalsteuer* der letzten österreichischen Bundesregierung kritisiert.[16] Eine Speicherverpflichtung von Browserhistorien zur Steuerberechnung würde dazu führen, dass die Sicherheitsbehörden auf diese Zugriff erlangen.

Eine Evaluierung von Überwachungsbefugnissen muss daher besonderes Augenmerk auf Auskunftsbefugnisse der Polizei legen und mit Erhebungen darüber einhergehen, welche und wie viele Daten von diesen Auskunftsbefugnissen betroffen sind. Verändern sich die privat gespeicherten Daten in Umfang und Qualität, verändert sich auch die Eingriffsintensität der polizeilichen Befugnisse. So kommen immer mehr Daten von vernetzten Geräten, dem *Internet of Things,* dazu, die alle Lebensbereiche der Menschen in noch nie dagewesener Kleinteiligkeit abdecken.

Fazit

Ich hoffe, anhand dieser Beispiele überzeugend demonstriert zu haben, dass die Ausweitung von staatlicher Überwachung nicht nur durch die Ausweitung der gesetzlichen Ermittlungsbefugnisse geschieht, sondern auch durch neue Technologien und den

Bei epicenter.works wird gebaut.

Ausbau privater Datenspeicher. Diese, sowie die Größe der Datenbanken, die automatischen Analysen unterzogen werden, müssen in der Evaluierung von Befugnissen eine Rolle spielen und unter Umständen zu ihrem Rückbau führen. Das bedeutet auch, dass es nicht genug ist, sich als kritische Öffentlichkeit mit Gesetzesvorhaben zu beschäftigen, sondern dass es auch gilt technische Entwicklungen im Auge zu behalten sowie Speicherverpflichtungen und -praktiken Privater, die oft nicht in polizeirechtlichen Regelungsmaterien geändert werden.

Anmerkungen

1 *https://epicenter.works/sites/default/files/heat_v1.2.pdf.*
2 *1 Bvr 256/08 vom 2. März 2010, Rz 218. Vgl. auch Bieker/Bremert/Hagendorff, Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in Roßnagel et al. (Hrsg.) Die Fortentwicklung des Datenschutzes (2018).*
3 *Vgl. Erläuterungen zum Strafprozessänderungsgesetz 2018 (17 d. B.) XXVI. GP, S. 2, https://www.parlament.gv.at/PAKT/VHG/XXVI/I/I_00017/fname_682032.pdf.*
4 *Wimmer, Polizei startet im Dezember mit Gesichtserkennung, futurezone.at vom 18.4.2019, https://futurezone.at/netzpolitik/polizei-startet-im-dezember-mit-gesichtserkennung/400469524.*
5 *Vgl. Bundesministerium für Inneres, Anfragebeantwortung vom 25.9.2019, https://fragdenstaat.at/anfrage/gesichtserkennung/.*
6 *Bundesministerium für Inneres, Anfragebeantwortung vom 11.6.2019, https://fragdenstaat.at/anfrage/ankauf-einer-gesichtserkennungs-software-durch-das-bundeskriminalamt/.*
7 *Bundesministerium für Inneres, Anfragebeantwortung vom 22.8.2019, https://fragdenstaat.at/anfrage/drohneneinsatze-durch-die-polizei/.*
8 *Blees, Polizei testet Drohnen, Neues Deutschland vom 3.9.2019, https://www.neues-deutschland.de/artikel/1125253.berlin-polizei-testet-drohnen.html.*
9 *Bundesministerium für Inneres, Anfragebeantwortung vom 5.9.2019, https://fragdenstaat.at/anfrage/predictive-policing/.*
10 *Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.*
11 *Allein in Deutschland wird von bis zu 180 Millionen betroffenen Personen pr Jahr ausgegangen (laut Anfrage der Abgeordneten Andrej Hunko, Martina Renner, Jan Korte u. a. http://dipbt.bundestag.de/doc/btd/19/095/1909536.pdf). In Österreich, mit einer Gesamtbevölkerung von ca. 8,5 Millionen, waren im nicht voll ausgebauten Betrieb in den ersten acht Monaten schon 11,9 Millionen Menschen betroffen*

(Bundesministerium für Inneres, Anfragebeantwortung vom 8.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutz-rechtliche-aspekte/).

12 *Zur ausführlichen Erklärung des Prävalenzfehlers und seiner Auswirkungen auf Systeme der Massenüberwachung sei McDermott, An Explainer On The Base Rate Fallacy empfohlen (https://en.epicenter.works/content/an-explainer-on-the-base-rate-fallacy-and-pnr).*

13 *Siehe die Zahlen des Bundesministerium für Inneres, Anfragebeantwortung vom 8.10.2019, https://fragdenstaat.at/anfrage/fluggastdatenanalyse-datenschutzrechtliche-aspekte/.*

14 *https://nopnr.eu/pnr/.*

15 *Vgl. z. B. Rat der EU, Vorratsdatenspeicherung zum Zweck der Kriminalitätsbekämpfung: Rat verabschiedet Schlussfolgerungen, https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/.*

16 *Epicenter.works, Digitalsteuergesetz schreibt bis dato unerlaubte Datenspeicherung vor, Blogpost vom 9.5.2019, https://epicenter.works/content/digitalsteuergesetz-schreibt-bis-dato-unerlaubte-datenspeicherung-vor.*

David Leeuwestein

Die wundersame Kreativität der GesetzgeberInnen

Haben Sie sich schon einmal gefragt, was der Staat eigentlich alles über Sie weiß? Welche verschiedenen Behörden Daten über Sie erheben, verknüpfen und analysieren? Waren sie schon mal verärgert oder verunsichert darüber, dass Sie nicht mehr wissen, welchen digitalen Fingerabdruck sie bei einer Verkehrskontrolle hinterlassen, einer Flugreise, einem Website-Aufruf?

Vermeintliche SicherheitspolitikerInnen erlassen immer mehr Gesetze, um unser digitales und analoges Leben bestmöglich zu überwachen. Polizeigesetze, Vorratsdatenspeicherung und Staatstrojaner bilden nur die Spitze des Eisbergs. Schon längst ist es für Einzelne unmöglich geworden, zu überblicken wie genau sie oder er von wem unter welchen Umständen überwacht werden darf.

Das hat das Bundesverfassungsgericht bereits vor Jahren als Problem erkannt. In seinem Urteil [illegible] 2010 hielt das Gericht fest, dass [illegible] zwar nicht per se verfassungswid[illegible] Kontext bereits bestehender Über[illegible] für die Demokratie gefährliches Maß erreiche. Aus diesem Urteil entstand der Begriff der Überwachungs-Gesamtrechnung.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Wir von Digitalcourage sind überzeugt, dass das für eine Demokratie verträgliche Maß an Überwachung schon lange überschritten ist. Um das zu belegen, pflegen wir schon seit Längerem eine Materialsammlung *(https://digitalcourage.de/ueberwachungsgesamtrechnung)* für eine Überwachungs-Gesamtrechnung, in der wir möglichst alle entstehenden und verabschiedeten Überwachungsgesetze erfassen. Als Absolvent eines Freiwilligen Sozialen Jahres bei Digitalcourage gehörte es zu meinem Aufgabenbereich, diese Übersicht aktuell zu halten.

Kein gutes Jahr

Schon die Gesetze, die in diesem einen Jahr dazugekommen sind, schaden unserer Demokratie empfindlich. Das sind unter Anderem:

- Das *Zensusvorbereitungsgesetz,* das zur Folge hatte, dass sensible Informationen wie Name, Geschlechtsidentität, Familienstand oder Religionszugehörigkeit von allen BundesbürgerInnen im Rahmen eines Testlaufs für den Zensus 21 im Statistischen Bundesamt zentral zusammengeführt wurden – ohne sie vorher zu anonymisieren oder pseudonymisieren. Das Gesetz sieht eine maximale Aufbewahrungsfrist von bis zu zwei Jahren vor.

- Das *Neunte Gesetz zur Änderung des Straßenverkehrsgesetzes,* das Autofahrer mit Überwachung für den Dieselskandal straft, anstatt die Autokonzerne in die Verantwortung zu nehmen.

- Das *European Travel Information and Authorisation Sys-* [illegible]*hreibt,* dass alle Menschen, die [illegible]*en möchten,* sofern sie kein Vi- [illegible]*enehmigung* (ETIAS Genehmi- [illegible]*erhobenen* Daten wie Alter, Geschlecht, Nationalität, Gesundheitszustand und vorherige Reisen sollen durch einen Algorithmus auf Risikoindikatoren untersucht und gegen diverse Datenbanken abgeglichen werden.

- Die Ausweitung der EU-weiten Fahndungsdatenbank *SIS II,* die vorgibt, dass bei allen Treffern, die im Zusammenhang mit Terrorismus stehen, ab Ende 2019 die Behörde Europol informiert werden muss. Zusätzlich können nun auch Ermittlungsanfragen gestellt werden. Diese legen Fragen oder Informationen fest, auf deren Grundlage die betroffene Person bei einer Polizeikontrolle befragt wird. Zudem wird der Eintrag von „Rückführentscheidungen abgelehnter AsylantragstellerInnen" verpflichtend.

- Die *Verordnung zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern,* welche nahezu alle EU-BürgerInnen zur Abgabe von Fingerabdrücken zwingt. *(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1157)*

- Das Zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen *(ECRIS-TCN),* in dem biometrische Daten (Fingerabdrücke und Passbild) sowie biographische Informationen über alle in der