RechtsLage

<<TableOfContents>>

= Grundlegende Normen =

Der rechtliche Rahmen für Datenbanken von Staatsicherheits- und Repressionsbehörden wird abgesteckt von den staatlichen Interessen an Verfügung über und Kontrolle der Bevölkerung sowie an Repression unerwünschten Verhaltens auf der einen Seite und den Prinzipen des [[DatenSchutz]]es, die Einzelnen Schutzrechte gegenüber solchen Ansprüchen einräumen auf der anderen (mehr zu dieser Abwägung in <<Rellink(gc/html/burger.html,RHZ 3/14)>>.
Diese Abwägung wird jedenfalls in der Rechtstheorie durch das Verhältnismäßigkeitsprinzip vorgenommen.

Im Datenschutz werden aus grundrechtlichen Erwägungen hehre Prinzipien von Datensparsamkeit, Zweckbindung und Transparenz. Näher geregelt wird die Umsetzung dieser Prinzipien außerhalb des Sicherheitsbereichs in der Datenschutzgrundverordnung der EU (<<Ratsdokument(EU 2016/679V)>>) sowie in diversen nationalen Anpassungen (Bundes- und Landesdatenschutzgesetzen). Diese sind aber durchweg subsidiär. Ihre Garantien werden also von anderen Gesetzen überschrieben (z.B. G10-Gesetz, TKÜV, Melderegistergesetz usf).

== Repressiv vs. Präventiv ==

Im Sicherheitsbereich konnte sich die EU nicht auf direkt geltendes Recht einigen, hat aber, damit die Daten auch unter den entsprechenden Behörden frei fließen können, <<Ratsdokument(EU 2016/680)>> (kurz JI-Richtlinie oder JI-RL) verabschiedet; diese setzt einen Rechtsrahmen, der dann in nationale Gesetze umgesetzt werden muss. In der BRD geschieht das in erster Linie durch das Bundesdatenschutzgesetz, nachrangig aber auch durch die Polizeigesetze der Länder, das BKAG usf.

Ansprüche gegen den Datenschutz aus Strafverfolgungskreisen sind prototypisch in §484 StPO niedergelegt:

{{{#!blockquote (1) Strafverfolgungsbehörden dürfen für Zwecke künftiger Strafverfahren

1. die Personendaten des Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
2. die zuständige Stelle und das Aktenzeichen,
3. die nähere Bezeichnung der Straftaten, insbesondere die Tatzeiten, die Tatorte und die Höhe etwaiger Schäden,
4. die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften,
5. die Einleitung des Verfahrens sowie die Verfahrenserledigungen bei der Staatsanwaltschaft und bei Gericht nebst Angabe der gesetzlichen Vorschriften in Dateien

speichern, verändern und nutzen.

(2) Weitere personenbezogene Daten von Beschuldigten und Tatbeteiligten dürfen sie in Dateien nur speichern, verändern und nutzen, soweit dies erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder Tatbeteiligten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass weitere Strafverfahren gegen den Beschuldigten zu führen sind. Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Speicherung, Veränderung und Nutzung nach Satz 1 unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass der Betroffene die Tat nicht oder nicht rechtswidrig begange hat.

(3) Das Bundesministerium der Justiz und die Landesregierungen bestimmen für ihren jeweiligen Geschäftsbereich durch Rechtsverordnung das Nähere über die Art der Daten, die nach Absatz 2 für Zwecke künftiger Strafverfahren gespeichert werden dürfen. Dies gilt nicht für Daten in Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden. Die Landesregierungen können die Ermächtigung durch Rechtsverordnung auf die zuständigen Landesministerien übertragen.

(4) Die Verwendung personenbezogener Daten, die für Zwecke künftiger Strafverfahren in Dateien der Polizei gespeichert sind oder werden, richtet sich, ausgenommen die Verwendung für Zwecke eines Strafverfahrens, nach den Polizeigesetzen. }}}

Auch zur „Gefahrenabwehr” oder noch schlimmer dem praktisch unbestimmten „Schutz der öffentliche Sicherheit und Ordnung“ darf der Staat in die informationelle Selbstbestimmung eingreifen. Dies ist gemäß föderalistischer Arbeitsteilung in den Polizeigesetzen der Länder (dann und wann auch Sicherheits- und Ordnungsgesetz o.ä. genannt) geregelt (oder eben nicht). Durch BKA, Zoll, „Verfassungsschutz” und Co genehmigt sich aber auch der Bund einige Gefahrenabwehr. Dass die konkreten Regelungen kaum zu unterscheiden sind von denen zur Strafverfolgung darf als Hinweis gelten, dass die Normen weitgehend Wunschzetteln der Behörden entstammen.

== Verhältnismäßigkeit ==

Da die Gesetze die Behörden praktisch nicht mehr beschränken, ist das wesentliche Mittel gegen, nun, übermäßige Polizei-EDV das Übermaßverbot. Nach diesem muss, unabhängig von allen anderen legalen Erwägungen, ein Eingriff in ein Grundrecht (und angesichts des Gedanken des [[DatenSchutz]]es ist praktisch jeder EDV-Einsatz bei der Polizei über die Ausführung von Solitaire hinaus ein Grundrechtseingriff) zur Erreichung eines (hoffentlich überhaupt formulierten) Zwecks

1. ''geeignet'' sein, d.h. tatsächlich dazu führen, dass das Ziel erreicht wird. Daher ist nach allen ernstzunehmenden Untersuchungen etwa Videoüberwachung nicht verhältnismäßig zur Verbrechensreduzierung, da sich eine solche mit noch so viel Videoüberwachung nicht einstellt.
2. ''erforderlich'' sein. Das heißt, dass ohne den Eingriff das Ziel nicht erreicht werden kann. In Gesetzestexten wird meist noch ein "oder erheblich erschwert" hinzugefügt, womit Missbrauch Tür und Tor geöffnet ist. Beispielsweise sind Reihen-DNA-Tests nicht

verhältnismäßig, da auch ohne sie die Aufklärungsquote bei einschlägigen Verbrechen sehr hoch ist.
3. ''angemessen'' sein. Damit ist gemeint, dass die Schwere des Eingriffs in einem, nun, angemessenen Verhältnis zum intendierten Zweck steht. So ist beispielsweise die [["Anti-Terror-Datenbank"]] nicht verhältnismäßig, weil die Vertiefung eines geheimpolizeilichen Komplexes die Gesellschaft umkrempelt, während Terrorismus in der BRD verglichen mit z.B. Kettensägen, Trittleitern oder Ski eine praktisch vernachlässigbare Bedrohung für Leben und Gesundheit darstellt.

== Speichergründe ==

Wenn die Polizei Daten speichert, muss sie dafür Gründe angeben. Praktisch alle einschlägigen Gesetze folgen der StPO in der Angabe von zwei Kategorien:

- Gefahrenabwehr, "Prävention" (z.B. Anlegen von Terrorlisten, so dass die Leute nicht fliegen können; Listen von bekannten Linksradikalen, die dann vor Großereignissen mit "Gefährderansprachen" eingeschüchtert werden können; die berühmten Sport-Dateien zur Aufrechterhaltung von Stadionverboten; die meisten Speicherungen unter diesem Label sind allerdings kaum wirklich erklärbar)
- Aufklärung künftiger Straftaten (z.B. Fingerabdruck-, DNA-Datenbanken, aber auch Kram wie KAN, unter dem Motto „Round up the usual suspects“).

In beiden Fällen muss die Polizei eine „Negativprognose“ stellen, also belegen, dass Daten Personen betreffen, von denen tatsächlich eine Gefahr ausgeht, der durch die Speicherung wirksam begegnet werden kann bzw. die tatsächlich mit hoher Wahrscheinlichkeit eine Straftat begehen, bei deren Aufklärung die Daten helfen können.

Im <<Doclink(2015-bfdi-tb.pdf, 25. TB (2015))>> (S. 90) weist die BfD noch einmal darauf hin, dass diese Negativprognose nicht formal sein darf (dazu gibt es auch umfangreiche Rechtssprechung, die allerdings die Latte eher tief hängt).
Aber: "Ein bloßer fortbestehender Verdacht genügt für die Speicherung nicht" (BfDI). Sie fand bei ihrer Prüfung des [[KAN]] druchweg keine adäquate Dokumentation der Negativprogonose, auch wenn das BKA auf Nachfrage immer etwas produzieren konnte, das sie zufriedenstellte (sie sieht also "strukturellen Verbesserungsbedarf").

Fazit: Nachfragen bezüglich der Negativprognose sind sicher keine schlechte Idee; mensch muss bei den Antworten allerdings mit Bullshit rechnen.

= Realitäten bei der Polizei =

Natürlich sind diese Dinge in der "Verfassungspraxis" nur fromme Wünsche, aber es ist doch tröstend, um die Verfassungswidrigkeit polizeilichen Handelns zu wissen. Beispiele aus der Gesetzgebung dazu:

- Das Erforderlichkeitsprinzip wird mit großer Kreativität vom 2008er Polizeigesetz in BaWü verhöhnt. Es sieht vor, dass die Polizei für zwei Jahre ''beliebige'' Daten speichern darf, also nicht mal mehr probieren muss, irgendwelche "Gefahrenprognosen"

zusammenzustöpseln, aus denen der Zweck ([[Prävention]] oder Aufklärung d.h. Strafverfolgung) ableitbar wäre. Zwar kräht auch andernorts kein Hahn nach diesen Zwecken, aber dort stehts wenigstens nicht im Gesetz.
- Die Zweckbindung wird zu einer Farce, wenn z.B. Ausschreibungen in [[SIS]] "wenn es die Staatssicherheit verlangt" in nationale Datenbanken übernommen werden.
- Von Transparenz kann natürlich nicht mehr annähernd die Rede sein, wenn Bürger``Innen bei der [["Anti-Terror-Datenbank"]] anfangs rund 40 Behörden hätten fragen müssen, um rauszukriegen, ob sie gespeichert sind. Inzwischen übernimmt das zwar im Prinzip das BKA, viele Geheimdienste entziehen sich aber nach wie vor ihrer Auskunftspflicht (und haben dafür auch eine Rechtsgrundlage).
- Darüber hinaus dokumentieren rasche Blicke in Datenschutzberichte oder Pressemitteilungen der Innenministerien, dass selbst die schon verfassungswidrigen Gesetze von den Behörden häufig zuungunsten der Bevölkerung gebrochen werden. Immerhin lässt sich da dann aber manchmal noch was reparieren, wenn es rauskommt.
- Ein makaberes Beispiel zur Zweckbindung und ihrer Verletzung aus Opportunitätsgründen hat der [[LfDI]] [[Sachsen]] in seinem <<Doclink(2009-LfDSachsen-Bericht14.pdf,14. TB (2009))>>, 5.9.3: Eine HIV-positive Blutspenderin begeht Selbstmord, in ihrem Notizbuch finden sich Namen von acht Männern, mit denen sie in den vergangenen drei Monaten Sex hatte. Die lokale Blutbank fragt die Polizei nach diesen acht Namen; der [[LfDI]] sagt, die Änderung des "Speicherzwecks" (in dem Fall dürften die Namen noch nicht mal in der [[Vorgangsverwaltung]] aufgetaucht sein, aber grundsätzlich ist sowas ein klassischer Fall von "sonstiger Person") sei ok, aber im vorliegenden Fall (Daten zu Gesundheit und Sexualität) nur mit Zustimmung der Betroffenen.

= Verfahrensverzeichnisse =

Bis zur EU-DSGVO (und PIAV) war es in den meisten Ländern und Polizeien üblich, dass jede Datenbank eine Errichtungsanordnung hatte, aus der die Zweckbestimmung, die Typen der gespeicherten Daten, die Zielgruppe, die Lese- und Schreibberechtigten usf. hervorgingen. Mit der DSGVO dürfte das ein Ende haben; <<Ratsdokument(EU 2016/680)>> (JI-RL) sieht in Artikel 24 stattdessen die Führung eines Verfahrensverzeichnisses vor, und §70 BDSG (im dritten Teil, also für Sicherheitsbehörden gedacht) schließt sich dem an.

In Errichtungsanordnungen waren traditionell fast immer einzusehen, meist per IFG-Anfrage, gelegentlich auch mal per Klage (vgl. auch <<Rellink(/gc/html/errao.html, get connected 2/15)>>. Die Post-DSGVO-Regelungen sagen dazu nichts Explizites. §70 Abs. 4 BDSG lässt allerdings nichts Gutes ahnen: „Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Bundesbeauftragten zur Verfügung zu stellen.“

Im Sicherheitsbereich ist das ein deutlicher Rückschritt gegenüber der vorherigen Zustand; zwar wurden die Errichtungsanordnungen auch unter Ausschluss der Öffentlichkeit zwischen Polizei und Innenministerien ausgehandelt, doch war eine Beteiligung des [[BfDI]] oder [[LfDI]] in der Regel vorgeschrieben.

Um einen Eindruck zu geben, was wir das so verloren haben (dürften): <<Doclink(IgaSt.pdf,Errichtunganordnung Igast)>> beim BKA (ist inzwischen aufgelöst und in [PMK

links-Z] aufgegangen); <<Doclink(FIT_anordnung.pdf,Errichtungsanordnung FIT)>> („Fundstellennachweis islamischer Terrorismus”, ebenfalls BKA).

= Merkwürdigkeiten =

- Wenn es kein Verfahrensverzeichnis gibt, ist nur das Datenschutzgesetz verletzt, was nach Ansicht des Hessischen Verwaltungsgerichtshofs (11 UE 2982/02, 16.12.2004) aber nicht schadet, wenn irgendwann mal ein Waschzettel nachgereicht wird.
- Eine parlamentarische Befassung findet nur dann statt, wenn die geltende Rechtslage die Einrichtung einer bestimmten Datenbank nicht hergibt; dies war etwa bei der [[DAD]] (DNA-Auskunftsdate) oder der [["Anti-Terror-Datenbank"]] der Fall.
- Dazu laufen Datenbanken gerne auch über lange Zeit im "Probebetrieb" ohne Errichtungsanordnung (vgl. z.B. [[AFIS]], Automatisierte Fingerabdruck-Indentifizierungssytem)
- Das BKA-Gesetz sieht vor, dass das Innenministerium (ggf. im [[Benehmen]] mit dem Bundesrat) die Natur der zu speichernden Daten per Rechtsverordnung (die veröffentlicht wird) genau spezifizieren muss. Unter Hinweis auf diese Regelung hat etwa das (typischerweise recht progressive) VG Hannover (10 A 2412/07) 2008 geurteilt, die Datei "Gewalttäter Sport" (analog wohl die übrigen Gewalttäter-Dateien) werde rechtswidrig betrieben. Leider stehen dem Urteile etwa des VG Mainz (1 K 363/08.MZ) ebenfalls von 2008 entgegen, die finden, die Rechtsverordnung sei "deklaratorisch" und nicht "konstitutiv" (also: Es braucht sie nur, damit was gesagt ist).

= Speicherfristen =

Grundsätzlich folgt aus der Zweckbindung, dass Daten zu löschen sind, wenn der Grund ihrer Erhebung und Speicherung nicht mehr besteht; dazu kommt eine Analogie zur Verjährung, die ihrerseits auf Artikel 1 und 2 des Grundgesetzes zurückgeführt wird – im Groben muss jedeR eine zweite, dritte, vierte und fünfte Chance bekommen, weil er/sie ein Mensch ist. Deswegen gibt es in allen Datenbanken "Aussonderungsprüfungsfristen" vorgesehen, nach denen ein Datensatz ''angesehen'' werden ''muss''. Er muss aber normalerweise nicht gelöscht werden, wenn ein Grund gefunden werden kann, warum der Zweck seiner Speicherung doch weiter besteht.

== Speicherfristen bei der Polizei ==

Für eine polizeiliche Datenbanken wie [[INPOL]] oder [[POLAS]] auf [[Datenbanken auf Länderebene|Länderebene]] werden je nach Fallgruppe Prüffristen festgelegt; typischerweise liegen sie bei fünf bis zehn Jahren. Im BKA-Gesetz ist für die Löschung und Sperrung von Daten [[http://www.gesetze-im-internet.de/bkag_1997/__32.html|§32 BKA Gesetz]] zuständig. Danach sind für Erwachsene in der Regel 10 Jahre Speicherdauer und 5 Jahre Speicherdauer bei Jugendlichen vorgesehen.

Das heißt natürlich nicht, dass eine vorherige Löschung ausgeschlossen ist; zu jeder Zeit muss die Polizei sagen können, welchen Zweck sie mit der Speicherung verfolgt und die Geeignetheit der Speicherung für diesen Zweck glaubhaft machen können. Die Maßstäbe sind da gewiss nicht streng, aber vorzeitige Löschungen sind nach Intervention nicht unüblich. Eine (etwas mickrige)

Statistik gibt es in <<BtDS(17/9003)>> (S. 9): So gab es für die (rund 250) Einträge der Bundespolizei in der [[Gewalttäter Sport]] zwischen 2005 und 2012 26 Löschersuchen, von denen 14, also über 50% ohne weiteres nachgekommen werden musste; das umfasst noch nicht Löschungen, die nach Gerichtsverfahren o.ä. vorgenommen werden mussten.

Hintergrund solcher Zahlen ist einerseits, dass die Polizei den (meist) offiziellen Begriff für Speicherfrist, „Aussonderungsprüffrist“, Ernst nimmt und vorher eben nicht nachsieht, ob sie die Daten noch braucht (ein Auskunftsersuchen sorgt allerdings auch dafür).

Andererseits liegt es natürlich auch an der Verachtung und Ignoranz in Datenschutzdingen auf Seiten der Polizei. Dies illustriert eine Anekdote aus dem 29 TB des LfD Bayern (S. 28):

{{{#!blockquote [Bei Gelegenheit] wurde ich bezüglich einer Speicherung von einem Polizeipräsidium mit der überraschenden Aussage konfrontiert, dass man „sofern“ die betroffene Person „zum heutigen Zeitpunkt eine Löschung beantragen sollte“ den Sachverhalt neu bewerten könne, da die Speicherung aus polizeilicher Sicht nicht mehr notwendig sei. }}}

(was leider nur eine milde Mahnung durch den LfD zur Folge hatte).

=== Sonderfall Zuspeicherung ===

Weiter laufen die Speicherfristen normalerweise bei "Zuspeicherung" (d.h. neuen Einträgen bei anderen Verfahren) neu an (das wurde dann und wann auch von Gerichten kritisiert, aber nie endgültig verurteilt).

Was genau eine Zuspeicherung darstellt, obliegt natürlich einem weiten Ermessenspielraum. Dass nun die Speicherfrist fürs Plakatieren neu anläuft, wenn Friedrich Schmidt in der Nähe eines AKWs wandernd aufgefunden wurde (um eine Speicherung zu ermöglichen, kann immer mal kurz ein 129a-Verfahren eröffnet werden), ist eigentlich nicht klar, wird aber üblicherweise so gehandhabt.

Die übliche Begründung dafür ist, dass all die mit Friedrich Schmidt zusammenhängenden Vergehen zur [[Prävention]] oder Aufklärung künftiger Straftaten hilfreich sein können (das ist ja der "Zweck", an den sie gebunden sind) und jede Zuspeicherung dokumentiert, dass dies auch weiter der Fall ist ("hätte Schmidt nicht weiter Staatsfeindliches im Sinn, wäre er woanders spazieren gegangen").

Eine besonders kafkaeske Variation der Fristverlängerung beschreibt der LfD BaWü im <<Doclink(2011-lfdbawue-tb30.pdf,30 TB (2011))>>, S. 92: Dabei hat das BKA die "Eigentümerschaft" eines erkennungsdienstlichen Datensatzes aus Baden-Württemberg übernommen, nachdem die entsprechenden Daten in Baden-Württemberg gelöscht worden waren (eine Praxis, die für sich schon sehr zweifelhaft ist). Als allerdings in Baden-Württemberg die Aussonderungsprüfung für andere Daten zum Betoffenen gekommen war, war der Umstand der Speicherung beim BKA Grund für den Sachbearbeiter, die Speicherung um drei Jahre zu verlängern.

=== Sonderfall PKS ===

Besonders kitzlig ist die Frage bei Speicherungen in der PKS (Polizeiliche Kriminalitäts-Statistik), wie sie im <<Doclink(2008-LfDBaWue-Bericht29.pdf,29. TB LfD BaWü)>>, 2.1/2.2.3, diskutiert werden. Diese Speicherungen dienen zur polizeilichen Kriminalstatistik, werden aber trotzdem im Auskunftssystem [[POLAS]] geführt.

=== Vorgangsverwaltungen ===

[[Länderübergreifende Software#Vorgangsverwaltungen|Vorgangsverwaltungen]] speichern alles, was beim Polizeialltag so passiert, d.h. auch Ordungswidrigkeiten oder ggf. sogar Personenkontrollen. Dafür gibt es in der Regel (d.h.je nach Bundes- oder Länderregelung) eine Speicherfrist von ein bis fünf Jahren. Danach sollten die Daten in gelöscht werden. Bei einer Neueröffnung eines alten Vorganges können damit verbundene Daten länger gespeichert werden (siehe [[http://www.datenschutz-bayern.de/tbs/tb21/k7.html#7.2|21. Tätigkeitsbericht LfD Bayern, 7.2]]).

Fristverlängerungen bei Zuspeicherung sollte es bei Vorgangsverwaltungen nicht geben; es wäre aber überraschend, wenn es sie nicht trotzdem gäbe.

=== 170 (2)-Einstellungen ===

Im Prinzip sollen Daten, die nach [[http://www.gesetze-im-internet.de/stpo/__170.html|§170 (2) StPO]] eingestellt wurden, gelöscht werden. Da nach §170 (2) die Staatsanwaltschaft vor einer Klageerhebung vor Gericht abgesehen hat. Bei [[http://www.gesetze-im-internet.de/stpo/__153.html|§153 StPO]] ist das schon schwieriger, denn dort wurden die Verfahren erst vor dem Gericht eingestellt.

Mehr dazu bei [[Eingestellte Verfahren]].

== Staatsanwaltschaften ==

In Strafverfahren, die mit einem Urteil (ohne Freispruch) enden, erfolgt die Löschung aus dem [[ZStV]] bei gleichzeitiger sofortiger Eintragung der Urteilsdaten in das [[Bundeszentralregister]]. Wird der Beschuldigte freigesprochen oder die Eröffnung des Hauptverfahrens abgelehnt, sind sie Daten nach zwei Jahren zu löschen. Wird in dieser Zeit jedoch ein weiteres Verfahren eröffnet, bleiben die alten Daten bis zur Löschung auch der neueren erhalten ([[http://www.gesetze-im-internet.de/stpo/__493.html|§ 493 StPO]]).

== Verfassungsschutz ==

In der Regel sollen die Daten 5 Jahre (Prüffrist), 10 Jahre (Zwingende Löschung, Weiterspeichung nur dbei OK des Chefs) oder 15 Jahre (Zwingende Löschung bei Agententätigkeit oder islamischen Terrorismus) nach [[http://www.gesetze-im-internet.de/bverfschg/__12.html|§12 Bundesverfassungsschutzgesetz]] nach dem letzten Eintrag gelöscht werden. D.h. nach den 5, 10 oder 15 Jahren wird der [[Datenbanken der Dienste/NADIS|NADIS]]-Eintrag gelöscht, die korrespondierenden Sachakten werden in der Regel nicht vernichtet (denn da stehen noch andere Personen drin). Sogar die korrespondierenden Personenakten werden nur als Sachakten umbenannt, falls dort noch andere Personen erwähnt werden (zumindestens nach dem

[[http://www.deutschesfachbuch.de/info/detail.php?isbn=3415037738|Handbuch des Verfassungsschutzrechts]] geschrieben von einer ehemaligen leitenden Mitarbeiterin des [[Datenbanken der Dienste|BfV]]).

= Auskunftsrecht =

Vgl. [[RechtsLage/Auskunftsrecht|Auskunftsrecht]].

= Datensammeln =

Die Strafprozessordnung, die Polizeigesetze, die Außenwirtschafts- und Zollgesetze, die Geheimdienstgesetze und das Gesetz zu Artikel 10 GG bieten eine Vielzahl von Gesetzenvorschriften zum [[/Datensammeln]], aufgrund derer Sicherheitsbehörden und Geheimdienste nicht nur Täter, sondern auch Personen, die vermeintlich dem Täterumkreis zugeordnet werden, (auch [[Prävention|präventiv]]) überwacht werden können. Die Überwachung geschieht dabei mit technischen Hilfsmitteln (siehe [[Überwachungstechnik]]) oder klassisch durch [[Observation]], [[Verdeckte Ermittler]] und [[V-Leute]]. Ganz besonders viele Rechte haben die Repressionsbehörden bei angeblichem Terrorismus, d.h. [[129a Verfahren]].

Version #1
Erstellt: 2025-10-27 22:32:00 UTC von Datenschmutz Migration Bot
Zuletzt aktualisiert: 2025-10-27 22:32:00 UTC von Datenschmutz Migration Bot