



**BfDI**

Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

Deutscher Bundestag  
Ausschuss für Inneres und Heimat

Ausschussdrucksache  
**19(4)732 A**

Bonn, den 18.02.2021

## **Stellungnahme**

**des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**

**zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat**

am 22. Februar 2021

zum Antrag der FDP-Fraktion

**„Freiheit und Sicherheit schützen – Für eine Überwachungsgesamtrechnung statt  
weiterer Einschränkungen der Bürgerrechte“**

BT-Drucksache 19/23695

Immer wieder werden Forderungen erhoben, Sicherheitsgesetze zu ändern und zu erweitern. Anlass sind zumeist einzelne Ereignisse, die große Aufmerksamkeit erregen. Vorschnelle Forderungen nach neuen Gesetzen sind aber abzulehnen. Zuerst ist eine Bestandsaufnahme notwendig. Abzulehnen sind insbesondere Maßnahmen, die in Grundrechte der Bürgerinnen und Bürger eingreifen, ohne wirklich die Sicherheitslage zu verbessern.

Der Gesetzgeber hat die Befugnisse der Sicherheitsbehörden in den letzten Jahrzehnten kontinuierlich erweitert. Die Zahl der nach 9/11 eingefügten neuen Befugnisse ist beachtlich. Dies macht die als Anlage beigefügte Liste mit Gesetzen bzw. Vorhaben deutlich, die zeigt, wie viele neue bzw. erweiterte Befugnisse die Sicherheitsbehörden mittlerweile erhalten haben (Anlage 1).

Immer wieder musste der Gesetzgeber Vorschriften enger fassen, nachdem das Bundesverfassungsgericht zum Schutze der Grundrechte betroffener Bürgerinnen und Bürger gegen eine ausufernde Gesetzgebungspraxis geurteilt hatte. Gerade die Sicherheitsgesetzgebung sollte stets einem Gesamtkonzept folgen. Dabei darf insbesondere nicht der Eindruck entstehen, die Politik wolle schnell einen Lösungsansatz präsentieren, um Diskussionen über mögliche Versäumnisse, Vollzugsdefizite oder vielschichtigeren Ursachen zu verhindern. Daher sollten Gesetzgebungsaktivitäten immer von einer in Ruhe durchgeführten, ergebnisoffenen und sorgfältigen politischen Diskussion begleitet sein.

Deshalb sind aus Sicht des Datenschutzes folgende Forderungen zu stellen:

### **1. Sicherheitsgesetz-Moratorium**

Wir benötigen eine Gesetzgebung und Behördenpraxis, die sich planvoll an sorgfältig durchdachten und die Grundrechte schützenden Konzepten orientiert. Sie sollte alle Zusammenhänge in den Blick nehmen und sich nicht nur mit der jeweils geforderten Einzelbefugnis beschäftigen. Deshalb ist es zu begrüßen, wenn der Bundestag sich dieses Themas annimmt und die Evaluierung von Gesetzen weiterentwickeln will.

Das Bundesverfassungsgericht hat dem Gesetzgeber in seiner Entscheidung zur Vorratsdatenspeicherung auferlegt, den Stand der eigenen Gesetzgebung regelmäßig zu beobachten. Insbesondere ist es dem Gesetzgeber verwehrt, mit neuen Vorschriften auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zu zielen. Er muss regelmäßig beobachten, keinen derartigen Zustand herbeizuführen. Er muss also regelmäßig eine Überwachungsgesamtrechnung durchführen, wie es Professor Alexander Roßnagel von der Universität Kassel treffend beschrieben hat.

Eine solche Überwachungsgesamtrechnung ist bislang noch nicht durchgeführt worden. Sie setzt voraus, dass die Wirkungen von Überwachungsmaßnahmen mit dem notwendigen Aufwand empirisch ausgeleuchtet werden. Eine solche Evaluierung sollte eine unabhängige Stelle durchführen und sie muss wissenschaftlich fundiert sein. Unzureichend sind Evaluierungen, bei denen nur allgemein Bewertungen oder Erfahrungen abgefragt werden. Vielmehr sind Evaluierungen nach wissenschaftlichen Methoden durchzuführen und sollten empirisch belastbar sein.

Die Evaluierung muss zunächst die gesetzgeberischen Ziele in den Blick nehmen. Sodann muss sie die Vollzugspraxis damit abgleichen und fragen, ob diese die Ziele erreicht und die gesetzlichen Möglichkeiten ausschöpft. Bei einer Überwachungsgesamtrechnung ist dabei das Entscheidende, die gesetzlichen Regelungen übergreifend in den Blick zu nehmen. Sie darf sich nicht nur isoliert mit wenigen Einzelregelungen beschäftigen.

Am wichtigsten ist es, dabei zu fragen, welche Auswirkungen die gesetzlichen Regelungen wie auch die Vollzugspraxis in ihrer Gesamtheit und in ihrem Zusammenwirken auf die Bürgerrechte und auf die Freiheit haben.

## **2. Vollzugsdefizite erkennen und beseitigen**

Bevor über neue Befugnisse nachgedacht wird, muss der Gesetzgeber prüfen, ob die verantwortlichen Behörden die vorhandenen Befugnisse hinreichend ausgeschöpft und die Schwerpunkte richtig gesetzt haben.

Der NSU-Untersuchungsausschuss des Bundestages ist in der vorletzten Legislaturperiode zu dem Ergebnis gekommen, die Gefahr rechtsextremistischer Gewalt im Bereich des Verfassungsschutzes sei unterschätzt und verharmlost worden (BT-Drs. 17/14600, 864). Er forderte einen Mentalitätswechsel. Es sei „nicht nachvollziehbar, wieso das Gefahrenpotential nicht höher eingeschätzt wurde und wieso seitens der Fachaufsicht diese Bewertungen nicht angezweifelt wurden.“ (S. 854 f.). Erst in jüngerer Zeit wird erkennbar, dass sich hier offenbar etwas ändert.

Es ist richtig und zu begrüßen, wenn die Bundesbehörden ihre Organisation an den aktuellen Sicherheitsanforderungen ausrichten. Dazu kann etwa gehören, Organisationseinheiten zu vergrößern oder einzurichten, die sich mit bestimmten Phänomenbereichen beschäftigen. So wurde etwa angekündigt, im Bundeskriminalamt die Kräfte zu verstärken, die für politisch motivierte Kriminalität im Bereich rechtsgerichteter Straftaten zuständig sind. Auch dass die Bundesregierung rechtsextremistische Gesinnung mittlerweile umfassend in den Blick nimmt und dabei auch die Bundesverwaltung und insbesondere die Sicherheitsbehörden nicht ausspart, zeigt die Notwendigkeit eines ganzheitlichen Ansatzes.

Das allein genügt aber nicht. Wer das große Ganze im Blick behalten will, muss sich auch die Sicherheit im Kleinen anschauen. Denn: Sicherheit wird vor Ort gemacht. Die stärkere Verschiebung der Kräfte hin zu den Bundesbehörden ist deshalb problematisch, gerade in einem föderalistisch organisierten Staat.

Wenn Bürgerinnen und Bürger in Not sind, dann hilft die Polizeiwache um die Ecke. Es ist dabei kurzsichtig, nur neue Befugnisse für die Datenverarbeitung zu fordern. Diese helfen nicht weiter, wenn diese Polizeiwache unzureichend ausgestattet ist. Fehler können sogar darin begründet sein, dass zu viele Polizeibeamtinnen und -beamte mit Datenspeicherungen und allgemeinen Datenauswertungen beschäftigt sind und damit zu wenige Beamte für die Ermittlungsarbeit, Gefahrenabwehr und Präsenz vor Ort zur Verfügung stehen. Nur vereinzelt und ausschnittsweise stehen hierfür statistische Informationen zur Verfügung. So betrug etwa in NRW die durchschnittliche Einsatzreaktionszeit für außenveranlasste Einsätze nach 110-Notrufen im Jahr 2016 durchschnittlich 16:14 Minuten (LT-Drucksache 16/14327, S. 3, abrufbar unter <https://landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMD16-14327.pdf>). Das ist deutlich länger als die etwa für den Rettungsdienst vorgeschriebene Hilfsfrist. Man muss also im Durchschnitt lange warten, bis der Streifenwagen vor Ort ist.

Und: Sicherheit wird nicht nur durch die Polizei gewährleistet. Am besten ist es, wenn Kriminalität gar nicht erst entsteht. Dies gilt für extremistische Kriminalität wie für alle anderen Straftaten. So ist beispielsweise zu fragen, ob vor Ort ausreichend Präventions-, Bildungs- und Sozialarbeit durchgeführt wird. Wer Sicherheit will, muss alles in den Blick nehmen.

### **3. Datenschutz ist Grundrechtsschutz**

Das Grundrecht auf informationelle Selbstbestimmung ist ein empfindliches Grundrecht. Deshalb benötigt es Schutz und Achtung.

Die Möglichkeiten, personenbezogene Daten mit neuen technischen Verfahren zu verarbeiten, sind inzwischen sehr umfassend und sie werden weiter wachsen. Die Daten können in international vernetzten Systemen ausgetauscht und mit hohen Geschwindigkeiten verknüpft und analysiert werden. Daraus ergeben sich unzählige Möglichkeiten, das Leben und die Entscheidungen einzelner Menschen zu beeinflussen. Maschinen oder Algorithmen, die entscheiden, ob jemand als Verdächtiger gilt oder nicht, sind technisch realisierbar. Einige aktuell bereits eingesetzte Algorithmen erfüllen diese Definition. Wenn die Daten zu einem falschen Verdacht führen, kann dies das Leben eines Menschen in seinem sozialen Gefüge nachhaltig verändern oder sogar zerstören.

Das Datenschutz-Grundrecht hat darüber hinausgehend eine sehr grundlegende Bedeutung für Demokratie und Gesellschaft: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“ Dies hat das Bundesverfassungsgericht schon in seinem bekannten Volkszählungsurteil prägnant beschrieben und ist unter dem Begriff „chilling effect“ sogar empirisch belegt.

#### **4. Sicherheit und Rechtssicherheit**

Sicherheit hat viele Facetten. Zu Recht erwarten die Bürgerinnen und Bürger, vor Gefahren und Kriminalität geschützt zu werden. Zu Recht muss der freiheitliche und demokratische Staat sich selbst erhalten und vor denen schützen, die Freiheit und Demokratie abschaffen oder einschränken wollen. Sicherheit ist aber nicht nur die „Bekämpfung“ von kriminellen Taten oder Verfassungsfeinden. Sicherheit bedeutet auch Rechtssicherheit. Diese prägt den Rechtsstaat. Jeder kann sich im freiheitlichen und demokratischen Rechtsstaat sicher sein, in seiner Freiheit nur dann eingeschränkt zu werden, wenn ein verhältnismäßig gestaltetes und demokratisches Gesetz dies regelt und er einen entsprechenden Anlass dafür gegeben hat. Willkür und anlasslose Maßnahmen soll es nicht geben. Damit ist klar: Wer von einem Rechtsstaat spricht, darf damit keinen Staat meinen, der unbegrenzte Möglichkeiten und Befugnisse zur vermeintlichen oder echten Strafverfolgung oder für nachrichtendienstliche Aktivitäten aller Art bietet. Sich zu begrenzen ist gerade das Wesen des Rechtsstaates. Bei politischen Forderungen nach einem „starken Rechtsstaat“ ist deshalb immer zu fragen, ob sie wirklich einen Rechtsstaat meinen.

#### **5. Datenschutz und Sicherheit**

In diesem Sinne dient der Datenschutz der Rechtssicherheit.

Datenschutz und die Interessen der Sicherheitsbehörden ergänzen sich gegenseitig. Pauschal einen Gegensatz zwischen Datenschutz und Sicherheit zu konstruieren, ist nicht akzeptabel. Beide verfolgen das Ziel, nur für die Sicherheit relevante Daten zu verarbeiten. Entscheidend ist es, zu differenzieren: Wenn Gefahren für gewichtige Rechtsgüter bestehen oder Straftaten begangen werden, dann darf und muss der Gesetzgeber effektive Mittel dafür bereitstellen, um diese abzuwehren. Gleichzeitig muss der Gesetzgeber aber ebenso die Grundrechte schützen. Er muss dazu Eingriffsschwellen und Verfahrenssicherungen festlegen und sich um deren rechtsstaatliche Kontrolle kümmern. Er hat dafür zum Beispiel die Speicherung vager Verdachtsmomente zu begrenzen, vor allem, wenn sie nicht bestätigt werden konnten. Diese müssen nach angemessener Zeit gelöscht werden,

insbesondere wenn sie nur weniger gewichtige Straftaten oder Gefahrenlagen tangieren. Zum Datenschutz gehört auch ein Recht auf Vergessen.

Gesetzliche Regelungen, die zwischen all dem nicht mehr differenzieren und Speicherdauer sowie Speicherzwecke entgrenzen, sind unverhältnismäßig. Sie schaden den Betroffenen und nützen niemandem. Auch nicht der Sicherheit und den Sicherheitsbehörden.

## **6. Personenkreis und Eingriffsschwellen**

Kein Datenschützer hat etwas dagegen, wenn Sicherheitsbehörden Daten zu Straftätern und Gefährdern als Einzelpersonen wie auch zu Organisationen speichern, damit sie diese beobachten und ihre Taten verfolgen und abwehren können. Wichtig ist aber: Nicht jede Person in den Datenbanken der Sicherheitsbehörden und Nachrichtendienste ist ein Straftäter oder Gefährder. Viele Speicherungen basieren lediglich auf einem Verdacht oder auf „tatsächlichen Anhaltspunkten“. Gerade im Bereich der Nachrichtendienste, deren Beobachtungsbefugnis deutlich eher ansetzt als die der Strafverfolgungs- und Gefahrenabwehrbehörden, werden auch Daten von Personen gespeichert, deren „Gefährdungspotential“ noch unklar ist. Es kann sich im Laufe der Zeit verdichten oder eben auch nicht.

Deshalb muss der Gesetzgeber klar definieren, welchen Personenkreis die Sicherheitsbehörden und Nachrichtendienste überhaupt erfassen dürfen und welche Parameter für das „Anreichern“ von Anhaltspunkten gelten. Die Eingriffsschwellen dürfen dafür nicht unverhältnismäßig abgesenkt werden. Je weniger „nah“ eine Person mit einer konkreten Straftat oder Gefahr im Zusammenhang steht, desto weniger darf sie gespeichert werden. Es ist deshalb zu differenzieren.

So regeln etwa die Nachrichtendienstgesetze nur sehr ungenau, welche Maßnahmen gegen welchen Personenkreis eingesetzt werden dürfen. Die Rechtsprechung lässt auf Grundlage der zu weit gefassten Rechtsvorschriften auch die Überwachung von Personen zu, die selbst überhaupt nicht wissen, dass sie von Dritten für extremistische Zwecke missbraucht werden. Sie hat dafür sogar einen eigenen Begriff geprägt und spricht von „nützlichen Idioten“. Dasselbe gilt für „Kontakt- und Begleitpersonen“. Der Gesetzgeber müsste hier viel stärker differenzieren.

Im Polizeibereich ist weiterhin zu fordern, Verdachtsfälle in den polizeilichen Datenbanken stärker zu beschränken.

Ein Kernanliegen des Datenschutzes ist es, die Unschuldsvermutung auch in polizeilichen Dateien zur Geltung zu bringen. Datenschutz ist rechtsstaatlicher Beschuldigtenschutz. Jeder muss die Chance haben, aus einem Ermittlungsverfahren am Ende auch als Unschuldiger herauszukommen. Bislang müssen Daten erst gelöscht werden, wenn die Unschuld erwiesen ist. Anderenfalls bedeutet das für die Betroffenen in der Regel: Sie werden

weiter gespeichert. Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Bei der Negativprognose ist daher der Grad des Tatverdachts zu berücksichtigen. Jeder gerichtliche Freispruch muss zur Löschung führen. Einen „Freispruch zweiter Klasse“ sollte es bei der Polizei nicht geben.

Gegenstand einer Überwachungs-Gesamtrechnung sollte deshalb auch die Frage sein, ob und inwieweit Gesetzgebung und Praxis das Ziel der Resozialisierung erreichen und im Blick haben. Denn für die Sicherheit geht es nicht darum, „Täter zu bekämpfen“, sondern (Straf-)Taten zu bekämpfen. Hinsichtlich des (potentiellen) Täters muss es das Ziel sein, ihn zum „Nicht-Täter“ zu machen. Das erreicht die Gesellschaft nicht allein mit „scharfen Sicherheitsgesetzen“. Deshalb sollte auch untersucht werden, ob und in welchem Umfang durch ein entsprechendes Labeling Menschen in polizeilichen Datenbanken oder Registern dauerhaft als „Täter“ abgestempelt werden und welche Folgen dies für ihren weiteren Lebensweg und letztlich auch für die Gesellschaft hat.

## **7. Analysen und Profilbildung**

Computergestützte Analysen und Profilbildung mit Data-Mining- und Maschinellen-Lernen-Methoden führen zu erheblichen Grundrechtseingriffen. Das Verknüpfen personenbezogener Daten ist deshalb gesetzlich zu begrenzen. Auch ein scheinbar harmloses Datum kann, wenn es in umfangreiche Datenbanken eingestellt und mit weiteren Daten verknüpft wird, tiefgreifende Aussagen zur Person des Betroffenen ermöglichen. Die fachliche Diskussion um die Verwendung von Metadaten durch Nachrichtendienste in Programmen wie PRISM und TEMPORA haben dies gezeigt. Durch die Zusammenstellung von Daten können umfassende Persönlichkeitsprofile angelegt werden. Dies betrifft nicht nur Datenanbieter wie Facebook und Google. Auch Sicherheitsbehörden arbeiten international daran, die Auswertemöglichkeiten zu erweitern. Mit ihren Datenbanken haben sie eine Grundlage geschaffen. Das ist ein erster Schritt. Weitere „polizeifachliche“ Forderungen nach weiteren technischen Erweiterungen werden kommen. Auswertungen auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht.

## **8. Verfahrenssicherungen**

Alle Gesetze müssen Verfahrenssicherungen vorsehen. Auch polizeiliche und nachrichtendienstliche Dateien müssen quasi einen „Notbremsassistenten“ und einen „Fehlerspeicher“ haben.

Dazu gehören klar geregelte Zugriffsrechte für alle Mitarbeitenden in den Sicherheitsbehörden. Diese müssen sich daran orientieren, ob die jeweilige Bearbeiterin oder der jeweilige Bearbeiter die Daten für die konkreten Zwecke tatsächlich benötigt. Pauschale Zu-

griffsberechtigungen erhöhen das Risiko. Zudem muss der Weg der Daten lückenlos protokolliert werden. Wenn etwa polizeiliche Daten in fremde Hände geraten oder für sachfremde Zwecke missbraucht werden, dann muss nachvollziehbar sein, woher sie stammen. Und auch solche Datenschutzverletzungen müssen konsequent geahndet werden.

## **9. Transparenz**

Transparenz ist in zweifacher Hinsicht notwendig. Zum einen muss die Arbeit der Sicherheitsbehörden allen Bürgerinnen und Bürgern in den Grundlagen bekannt gemacht werden. Zum anderen haben konkret betroffene Personen einen Anspruch auf Auskunft, welche Daten über sie gespeichert sind.

Das Auskunftsrecht hat eine doppelte Grundlage. Nämlich einerseits im Datenschutzgrundrecht, andererseits im Rechtsstaatsprinzip. Nur wenn ich weiß, was über mich gespeichert wird, kann ich dagegen vorgehen.

Sicherheitsbehörden dürfen in einem Rechtsstaat kein „Staat im Staate“ sein. Bürgerinnen und Bürger haben in einem freiheitlichen Staat grundsätzlich einen Anspruch darauf, zu wissen, was die Behörden tun. Das gilt auch für Polizeibehörden und für Nachrichtendienste. Ihre Arbeitsgrundlagen müssen deshalb transparent sein. Ausnahmen sind nur dort zulässig, wo sonst die Sicherheit gefährdet bzw. die Arbeit nicht möglich wäre. Dabei gilt: Polizeibehörden arbeiten grundsätzlich offen. Sie sind keine Nachrichtendienste. Ausnahmen bedürfen einer sachlichen Begründung. Diese Transparenz hat das Bundesverfassungsgericht in seinen Entscheidungen zum Bundeskriminalamtgesetz und zur Antiterrordatei ausdrücklich angemahnt.

## **10. Datenschutzkontrolle**

Wo es Gründe dafür gibt, kann nicht alles offen und transparent sein. Dies gilt etwa, wenn die Sicherheitsbehörden aus begründetem Anlass heimlich ermitteln. In solchen Fällen ist es schwierig, Rechtsschutz zu erhalten. Dieses Defizit müssen datenschutzrechtliche Kontrollen ausgleichen. Datenschutzkontrolle hat eine Kompensationsfunktion, die das Bundesverfassungsgericht sehr deutlich herausgearbeitet hat. Deshalb sind starke Kontrollbefugnisse für die Datenschutzbehörden unabdingbar. Dies gilt nicht nur für die Polizeibehörden, sondern gerade auch für die Nachrichtendienste.

Wirksame Kontrolle setzt voraus, dass festgestellte Verstöße gegen datenschutzrechtliche Vorschriften abgestellt werden. Dies ist aber nicht durchsetzbar, wenn den Datenschutzbehörden entsprechende Anordnungsbefugnisse fehlen. Die JI-Richtlinie schreibt dies für den Bereich der Strafverfolgung und Polizei sogar ausdrücklich und verbindlich vor. Für diese, aber auch für die Nachrichtendienste, ergibt sich dies zusätzlich aus der bereits angesprochenen Kompensationsfunktion.



Bislang kann der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) nur gegenüber dem Bundeskriminalamt anordnen, datenschutzrechtlich unzulässige Verarbeitungen einzustellen oder zu beseitigen. In allen anderen Sicherheitsgesetzen fehlt eine entsprechende Befugnis. Ich fordere deshalb, dies in der allgemeinen Vorschrift des § 16 Bundesdatenschutzgesetz einzufügen und damit insbesondere auch für die Nachrichtendienste festzulegen.

Im Bereich der Nachrichtendienste ist der Individualrechtsschutz zugunsten des staatlichen Sicherheitsinteresses besonders schwach ausgestaltet. Die Datenschutzkontrolle soll dies kompensieren. Wirksamer Individualrechtsschutz (im Zweifel auch ohne Kenntnis des Betroffenen) liegt aber nur dann vor, wenn sichergestellt ist, dass eine rechtswidrige Datenverarbeitung auch abgestellt werden kann. Im Streitfall bleibt es bislang bei der Rechtsauffassung des Nachrichtendienstes bzw. dessen Fachaufsicht. Es muss möglich sein, seitens der Datenschutzaufsicht eine Datenverarbeitung zu untersagen und diese Entscheidung dann der gerichtlichen Überprüfung zugänglich zu machen. Im Bereich des Bundesnachrichtendienstes (BND) hat die Bundesregierung dem BfDI im Jahr 2018 sogar noch mehr Steine in den Weg gelegt, seine Kritik überhaupt anderen Verfassungsorganen mitzuteilen. An den Bundestagsinnenausschuss darf sich der BfDI mittlerweile gar nicht mehr wenden (vgl. § 32a Nr. 1 b BNDG).

Zugleich ist die Kontrolllandschaft über die Nachrichtendienste in Deutschland mittlerweile so fragmentiert, dass eine umfassende Kontrolle sowie eine umfassende Kenntnis des Kontrollgegenstandes möglicherweise auf der Strecke bleiben. Außer von der jeweiligen Fachaufsicht werden die Nachrichtendienste vom BfDI, vom Parlamentarischen Kontrollgremium, von der G 10-Kommission und der BND zusätzlich voraussichtlich künftig noch vom Unabhängigen Kontrollrat kontrolliert, der das bisherige Unabhängige Gremium ersetzt. Die einzelnen Kontrollinstanzen haben partielle, zumeist nebeneinander stehende Kontrollaufträge. Eine durchgängige Kooperation und gegenseitige Information dieser Aufsichtsorgane findet bislang kaum statt, wird vom Gesetzgeber bislang kaum durch entsprechende Verpflichtungen unterstützt oder wird, wie im Fall des BND, durch die Novelle inhaltlich auf den Austausch von „allgemeinen Aspekten der Kontrolltätigkeit“ beschränkt. Die Gefahr von Kontrolllücken liegt auf der Hand.

Vollends lückenhaft wird die Kontrolle, wenn es um Datenübermittlungen seitens deutscher Nachrichtendienste ins Ausland geht. Die Kontrolle endet hier quasi an der Grenze!

**Liste Bundesgesetze seit 2001\_National**

<b>Nr.</b>	<b>Bezeichnung</b>	<b>Wesentlicher Inhalt/Gegenstand</b>	<b>Fundstelle</b>
1.	<b>Luftverkehr-Zuverlässigkeitsüberprüfungsverordnung</b> vom 8.10.2001	Regelung des Verfahrens der Zuverlässigkeitsüberprüfung nach dem Luftverkehrsgesetz auf dem Gebiet des Luftverkehrs. Betroffen sind Personen, die Zugang zu nicht-öffentlichen Bereichen von Flughäfen haben sowie solche, die aufgrund Ihrer Tätigkeit, z.B. für ein Fracht- oder Cateringunternehmen unmittelbaren Einfluss auf die Sicherheit des Flugverkehrs nehmen können.	BGBl. I 2001, S. 2625
2.	<b>Terrorismusbekämpfungsgesetz</b> vom 9.1.2002	<p>1. Auskunftsbefugnisse des BfV gegenüber</p> <p>a. Kreditinstituten bzgl. Konten, Konteninhabern, Geldbewegungen u.a.</p> <p>b. Postdienstleistern bzgl. Postkunden</p> <p>c. Luftverkehrsunternehmen bzgl. pers. Daten von Kunden</p> <p>d. Telekommunikations und Telediensten bzgl. Telekommunikations und Teledienstedaten</p> <p>2. Befugnis zum Einsatz des IMSI-Catchers durch BfV</p> <p>3. Übermittlungspflichten für BAFL und Ausländerbehörden gegenüber BfV</p> <p>4. Einsatz des IMSI-Catchers durch MAD</p> <p>5. Auskunftsbefugnis des MAD gegenüber Telekommunikations und Telediensten</p> <p>6. Auskunftsbefugnis des BND gegenüber</p> <p>a. Kreditinstituten</p> <p>b. Telekommunikations und Telediensten</p> <p>7. Einführung des vorbeugenden personellen Selbstschutzes</p> <p>8. Eigenständige Datenerhebungsbefugnis des BKA in seiner Zentralstellenfunktion gegenüber öffentlichen und nicht-öffentlichen Stellen</p>	BGBl. I 2002 S. 361
3.	<b>Viertes Finanzmarktförderungsgesetz</b> vom 21.06.2002	§ 24c Kreditwesengesetz schafft Rechtsgrundlage für den automatisierten Abruf von Kontoinformationen durch die Bundesanstalt für Finanzdienstleistungsaufsicht, die auf Ersuchen Auskunft an die für die Verfolgung von Straftaten zuständigen Behörden erteilt.	BGBl. I 2002 S. 2010
4.	<b>Geldwäschebekämpfungsgesetz</b> vom 8. August 2002	Ausdehnung der Regelungen des Geldwäschebekämpfungsgesetzes auf die Finanzierung des Terrorismus, inkl Übermittlungsnorm zugunsten Polizei und Nachrichtendiensten des Bundes	BGBl. I 2002, Seite 3105
5.	<b>34. Strafrechtsänderungsgesetz</b> vom 22.08.2002	Einführung des § 129 b StGB, der die Tatbestände des §§ 129, 129 a StGB auf Vereinigungen im Ausland erweitert.	BGBl. I 2002, S. 3390

6.	<b>Telekommunikationsgesetz (TKG)</b> vom 22.06.2004	Gegenüber der Vorgängerregelung erlaubt das neue TKG den Abruf von Bestandsdaten durch Gerichte, Strafverfolgungsbehörden, Polizeibehörden und Nachrichtendienste auch unter Verwendung unvollständiger Abfragedaten und die Suche mittels Ähnlichfunktion im sog. automatisierten Auskunftsverfahren. Ferner wird die Auskunft über Daten, mittels derer der Zugriff auf Endgeräte oder Speichereinrichtungen geschützt wird (PIN oder PUK), erlaubt	BGBl. I 2004 S. 1190
7.	<b>Gesetz zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern</b> (Zuwanderungsgesetz) vom 30. Juli 2004	<ul style="list-style-type: none"> <li>• Grundlegende Neustrukturierung des Aufenthaltsrechts, u. a. Begrenzung des Zuzugs, Reduzierung der Zahl der Aufenthaltstitel auf zwei: (befristete) Aufenthaltserlaubnis und (unbefristete) Niederlassungserlaubnis.</li> <li>• Einrichtung eines Bundesamtes für Migration und Flüchtlinge (BAMF) anstelle des Bundesamtes für die Anerkennung ausländischer Flüchtlinge-</li> <li>• Umbenennung des Bundesinstituts für Bevölkerungsforschung in Bundesinstitut für Bevölkerungs- und Migrationsforschung,</li> <li>• Einschränkungen beim Zuzug von ausländischen Arbeitskräften: Kein Zuzug ohne Nachweis eines konkreten Arbeitsplatzes,</li> <li>• Verschärfung der Regelungen zur Ausweisung und Abschiebung gefährlicher Ausländer: Abschiebung bereits auf Grund einer auf Tatsachen gestützten Gefahrenprognose, Meldepflichten und Kommunikationsverbote, Einrichtung eines Registers zum vorübergehenden Schutz beim BAMF, Datenübermittlung durch das BAMF als nationale Kontaktstelle;</li> <li>• Übermittlungsgrundlage zugunsten der Nachrichtendienste des Bundes.</li> </ul>	BGBl. I 2004 S. 1950
8.	<b>Luftsicherheitsgesetz</b> vom 11.01.2005	Zuverlässigkeitsüberprüfung von Piloten, Flughafenpersonal u.a.	BGBl. I 2005, S. 78
9.	<b>Antiterrordateigesetz (ATD)</b> vom 22.12.2006	Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten zur Bekämpfung des internationalen Terrorismus beim BKA	BGBl. I 2006 S. 3409
10.	<b>Gemeinsame-Dateien-Gesetz</b> vom 30.12.2006	<ul style="list-style-type: none"> <li>• Errichtung einer gemeinsamen zentralen Antiterrordatei von Polizei und Nachrichtendiensten</li> <li>• gemeinsame Projektdateien von Polizei und Nachrichtendiensten</li> </ul>	BGBl. I 2006, S. 3409
11.	<b>Terrorismusbekämpfungsergänzungsgesetz</b> vom 05.01.2007	<p>Absenkung der bisher geltenden Verfahrenssicherungen (G-10-Voraussetzungen) bei den besonderen Auskunfts-befugnissen des BfV.</p> <p>Befugnis zur eigenständigen Ausschreibung von Personen und Sachen im SIS für BfV, BND, MAD</p> <p>Inhaltsgleiche Übertragung der besonderen Auskunfts-befugnisse des BfV</p> <ul style="list-style-type: none"> <li>• auf MAD</li> <li>• auf BND</li> </ul>	BGBl. I 2007, S. 2

12.	<b>Telemediengesetz (TMG)</b> vom 26.02.2007	Auf der Grundlage des außer Kraft getretenen Teledienstdatenschutzgesetzes (TDDSG) durften Diensteanbieter Auskünfte über Bestandsdaten nur für Zwecke der Strafverfolgung erteilen. Die Nachfolgevorschrift im TMG erweitert diese Auskunftsbefugnis gegenüber Polizeibehörden für Zwecke der Gefahrenabwehr sowie Nachrichtendiensten zur Erfüllung ihrer gesetzlichen Aufgaben.	BGBl. I 2007 S. 179
13.	<b>Gesetz zur Abwehr von Gefahren des internationalen Terrorismus</b> durch das BKA(BKATerrAbwG) m.W.v. 01.01.2009	Umsetzung der in Art. 73 Abs. 1 Nr. 9a GG geregelten Gesetzgebungskompetenz des Bundes für die Abwehr von Gefahren des internationalen Terrorismus	BGBl. I 2009 S. 3083
14.	<b>Gesetz zur Neuregelung der Telekommunikationsüberwachung</b> und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG v. 31.12.2007	Artikel 1: Neuregelung der heimlichen Ermittlungsmaßnahmen der StPO, u.a.: <ul style="list-style-type: none"> <li>• Erweiterung des Anlasstatenkatalogs der Telekommunikationsüberwachung</li> <li>• Ausweitung des Anwendungsbereichs des IMSI-Catchers: Einsatz nicht mehr nur zum Zwecke der Vorbereitung einer TKÜ oder der Lokalisierung einer festzunehmenden Person, sondern allgemein zur Sachverhaltserforschung oder zur Aufenthaltsermittlung des Beschuldigten und generell bereits bei Straftaten von erheblicher Bedeutung</li> <li>• Übermittlungsgrundlage zugunsten der Nachrichtendienste des Bundes und der Länder.</li> </ul>	BGBl. I 2007 S. 3198
15.	<b>Viertes Gesetz zur Änderung des Bundespolizeigesetzes</b> G v. 22. 12. 2007	Ausdehnung der Speicherfrist für Bilddaten von selbsttätigen Bildaufnahme- und Bildaufzeichnungsgeräten auf einen Monat	BGBl. I 2007 S. 3214
16.	<b>Änderung des Bundespolizeigesetzes II</b> zum 01.03.2008	Übermittlung von Fluggastdaten bei bestimmten Flügen (nach Maßgabe des BPolP) über die Schengen-Außengrenze in das Bundesgebiet (nach API-Richtlinie)	BGBl. I 2008 S. 250
17.	<b>SatellitendatensicherheitsG</b> 23.11.2007	Erweiterung der Mitwirkung der VerfSchbehörden auf Überprüfungen "sonstiger gesetzlich bestimmter Fälle", z.B. für Personen, die Zugang zu den Anlagen der Kommandierung eines hochwertigen Erdfernerkundungssystems haben Übermittlungsgrundlage zugunsten des BND; Subsidiäre Anwendung des Gesetzes für die Nachrichtendienste des Bundes.	BGBl. I 2007S. 259 0
18.	<b>Erstes Gesetz zur Änd. des Artikel 10-Gs</b> 31.7.2009	<ul style="list-style-type: none"> <li>• Speicherung und Übermittlung von Daten Minderjähriger durch BfV und BND</li> <li>• Auskunft von Finanzbehörden</li> <li>• Befugnis des BND, Mobiltelefone von Entführungsoffern abzuhören</li> </ul>	BGBl. I 2009 S. 2499
19.	<b>Zehntes Gesetz zur Änderung des Atomgesetzes v.</b> 17.03.2009	Neue Regelungen zur Zuverlässigkeitsüberprüfung von Personen vor dem Hintergrund der erhöhten Bedrohungslage durch internationalen Terrorismus. Betroffen sind als Verantwortliche benannte Personen in Genehmigungs-, Planfeststellungs- und Aufsichtsverfahren, Personen, die bei der Errichtung oder dem Betrieb von Atomanlagen tätig sind oder bei der Beförderung von radioaktiven Stoffen	BGBl. I 2009, S. 556

20.	Gesetz zu dem Protokoll vom 15. Mai 2003 zur Änderung <b>des Europäischen Übereinkommens vom 27. Januar 1977 zur Bekämpfung des Terrorismus</b> 03.09.2010	Schränkt die Möglichkeit ein, die Auslieferung von Personen, die eine schwere Straftat begangen haben, allein mit der Begründung zu verweigern, es handele sich um eine politische Straftat. Die in dem Übereinkommen vorgesehene Möglichkeit der Vertragsstaaten, gegen die genannte Einschränkung einen Vorbehalt einzulegen, bedarf ihrerseits einer Einschränkung, um Auslieferungen zu erleichtern und Ablehnungsmöglichkeiten zu verringern.	
21.	<b>Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten</b> vom 30. Juli 2009	Erweiterung des Staatsschutzstrafrechts zur Bekämpfung des Terrorismus. Strafbarkeit von festgelegten Vorbereitungshandlungen, von Kontaktaufnahme mit terroristischen Vereinigungen mit Ausbildungsabsicht sowie von Verbreitung oder Beschaffung von Anleitungen zur Tatbegehung	BGBI. I 2009, S. 2437
22.	<b>Änderung des Zollfahndungsdienstgesetzes</b>	Neuregelung der präventiven Telekommunikationsüberwachungsbefugnisse des ZKA infolge Urteil des BVerfG vom 27.07.2005 (Nds. SOG).	
23.	<b>Gesetz über den Zugang der Sicherheitsbehörden zum Visa-Informationssystem für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten (VIS-Zugangsgesetz - VISZG)</b>	Einrichtung „zentraler Zugangsstellen“ (ZZ) für Polizeibehörden und Nachrichtendienste des Bundes und der Länder.	BGBI. I 2009, S. 1034
24.	<b>Kontenstammdatenabruf</b> – Viertes Finanzmarktförderungsgesetz vom 21. Juni 2002	§ 24c Kreditwesengesetz (KWG) schafft die Rechtsgrundlage für den automatisierten Abruf von Kontostammdaten.  Nach seiner ursprünglichen Zielrichtung zielte die Vorschrift darauf ab, die Terrorismusfinanzierung, die Geldwäsche sowie das unerlaubte Betreiben von Bankgeschäften effektiver zu bekämpfen.  Durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 wurde der Anwendungsbereich des Kontenstammdatenabrufs auf Finanz- und Sozialbehörden erweitert (Inkrafttreten ab 1. April 2005).	BGBI. I 2002 S. 2010
25.	<b>Zweites Gesetz zur Änderung des Zollverwaltungsgesetzes</b> vom 31. Oktober 2003 nur hinsichtlich seines Artikels 2 (Änderung des Kre-	Einführung einer Ermächtigungsgrundlage in § 6a KWG für die BaFin auf der Grundlage der Resolution 1373 vom 27. September 2001 des VN-Sicherheitsrats, um Finanzinstituten verdächtige Verfügungen oder Finanztransaktionen zu untersagen.	

	ditwesengesetzes)		
26.	<b>Einrichtung gemeinsamer Zentren zur verstärkten Zusammenarbeit von Sicherheitsbehörden</b> (GASIM, GIZ, Nationales Cyberabwehrzentrum (NCAZ))	Gemeinsame Terror-Abwehrzentrum (GTAZ, seit Dezember 2004), Gemeinsamen Analyse- und Strategiezentrum Illegale Migration (GASIM, seit Mai 2006) und Gemeinsamen Internetzentrum (GIZ, seit Anfang 2007) arbeiten Polizei und Nachrichtendienste mit dem Ziel der Intensivierung des Informationsaustausches zwischen den Sicherheitsbehörden unmittelbar zusammen. Am NCAZ sind u.a. BSI, BKA, BfV, BND, BBK, BPol, ZKA und BW beteiligt. Es dient der Prävention, Information und Frühwarnung gegen sogenannte Cyber-Angriffe.	
27.	<b>Akkreditierungsverfahren</b> von Journalisten und ggf. anderen Personen bei Großveranstaltungen	Das „einmalige“ Verfahren der Akkreditierung von Journalisten und anderen Personen unter Abfrage nach Erkenntnissen bei Polizei und Nachrichtendiensten bei der Fußball WM 2006 wurde danach in gleicher oder ähnlicher Form wiederholt angewandt, z.B. beim Papstbesuch in Bayern 2006, und bei der Leichtathletik-WM 2009 in Berlin, Ski WM 2011, Frauen-Fußball-WM 2011.	
28.	<b>Einrichtung einer „Financial Intelligence Unit“ (FIU)</b> , zunächst beim Bundeskriminalamt, sodann beim Zollkriminalamt	Nationale Zentralstellen zur Entgegennahme und Auswertung von Geldwäscheverdachtsanzeigen und zur Bekämpfung der Finanzierung des Terrorismus.	
29.	Verschiedene <b>Finanzsanktionen</b> auf der Grundlage von Sanktionsmaßnahmen <ul style="list-style-type: none"> <li>• der Vereinten Nationen,</li> <li>• der Europäischen Union sowie</li> <li>• der nationalen Behörden.</li> </ul>	Beschränkungen des Kapital- und Zahlungsverkehrs durch umfassende wirtschaftliche Zwangsmaßnahmen gegen bestimmte Staaten oder natürliche bzw. juristische Personen. Bsp: Finanzsanktion gegen Al-Qaida, die Taliban und Osama bin Laden, gegen den Iran, gegen Birma / Myanmar u.s.w..	
30.	Zollrechtlicher Status des „Zugelassenen Wirtschaftsbeteiligten – AEO ( <b>Authorised Economic Operator</b> ) seit 1. Januar 2008	Rechtsgrundlage: EG-Durchführungsverordnung Nr. 1875/2006 zum Zollkodex.  Der AEO-Status berechtigt zu Vergünstigungen bei sicherheitsrelevanten Zollkontrollen und/oder Vereinfachungen gemäß den Zollvorschriften. Im Antragsverfahren haben die Unternehmen auf der Grundlage einer Dienstanweisung des BMF den Nachweis zu erbringen, dass sie ihre Mitarbeiter und Kunden regelmäßig mit den EG-Anti-Terrorlisten abgleichen	

31.	<b>Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung</b> (sog. Geldwäschebekämpfungsergänzungsgesetz, GwBekErgG) in Umsetzung der Dritten Geldwäsche-Richtlinie (2005/60/EG) und der sog. PeP-Richtlinie (2006/70/EG) 2008	Ausweitung der Geldwäschebekämpfung auf Terrorismusfinanzierung (insb.: spezifische Sorgfaltspflichten von Banken, Verpflichtung zum Datenabgleich zur Terrorismusbekämpfung, Identifizierungspflicht von wirtschaftlich Berechtigten)	BGBl. I 2008, Seite 1690
32.	<b>Körperscanner</b>	Der Körperscanner soll als Kontrolle vor dem Betreten des Sicherheitsbereichs an Flughäfen unter der Kleidung versteckte gefährliche Gegenstände - wie etwa Sprengstoff oder Keramikmesser - sichtbar machen.	
33.	<b>Gesetz zur Errichtung einer Visa-Warndatei</b> (Visa-Warndatei-Gesetz – VWDG) (v. 22.12.2011; Stand: 29.03.2017)	Errichtung einer zentralen, automatisierten Datenbank beim Bundesverwaltungsamt; sie betrifft in Visaangelegenheiten strafrechtlich aufgefallene Einlader, Verpflichtungsgeber und sonstige Referenzpersonen. Zugriffsbeschränkung auf die Visumbehörden; Einrichtung einer gesonderten Organisationseinheit beim Bundesverwaltungsamt zum automatisierten Abgleich der Visa-Warndatei mit der Antiterrordatei, Treffermeldung ausschließlich an die zuständige Sicherheitsbehörde.	BGBl. I 2011, Seite 3037
34.	<b>Gründung des GAR</b> (Gemeinsames Abwehrzentrum gegen Rechtsextremismus/Terrorismus im November 2011)	Nach dem Vorbild bestehender Zentren; geht ein Jahr später im neu gegründeten GETZ auf	
35.	<b>Gesetz zur Änderung des Bundesverfassungsschutzgesetzes</b> vom 7. 12.2011	Ausweitung der Auskunftsbefugnisse für BfV, BND, MAD: <ul style="list-style-type: none"> <li>· Möglichkeit der Abfrage von Passagierdaten nicht mehr nur von Luftfahrtunternehmen, sondern auch von Betreibern von Buchungssystemen für Flüge</li> <li>· Möglichkeit der Abfrage von Kontostammdaten beim BZSt und bei den Kreditinstituten</li> </ul> aber: Anhebung der Verfahrenssicherungen (G-10-Voraussetzungen § 8bBVerfSchG) bei den besonderen Auskunftsbefugnissen	BGBl. I 2011 S. 2576
36.	<b>Gesetz zur Optimierung der Geldwäscheschneidung</b> vom 22.12.2011	Umstrukturierung und Erweiterung der Regeln zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, um die Einhaltung der Anforderungen der Financial Action Task Force on Money Laundering (FATF) sicherzustellen (insb.: Erweiterung und Konkretisierung der Sorgfaltspflichten der geldwäscherechtlich Verpflichteten nach risikoorientiertem Ansatz; Ergänzung der verstärkten Sorgfaltspflichten in Bezug auf inländische „politisch exponierte Personen“; Anpassung des	BGBl. I S. 2959

		Verdachtsmeldewesens bei der beim BKA angesiedelten Zentralstelle für Verdachtsmeldungen (FIU) an die FATF-Standards, insb. Umbenennung von Verdachtsanzeige zu Verdachtsmeldung und damit de facto Absenkung der Schwelle zur Meldeverpflichtung bereits unterhalb des Straftatverdachts.	
37.	<b>Terrorismusbekämpfungsergänzungsgesetz</b>	Ausweitung der Auskunftsbefugnisse für BfV, BND, MAD	
38.	<b>Rechtsextremismustateigesetz, REDG</b> 20.08.2012	Kopie der ATD für den Rechtsextremismusbereich	BGLI IS.1798
39.	<b>Gründung des GETZ</b> (Gemeinsames Extremismus- und Terrorismus-Abwehrzentrum) im November 2012	Kommunikationsplattform für Polizei und Nachrichtendienste des Bundes und der Länder; das Ende 2011 gegründete GAR geht im GETZ auf	
40.	<b>VISA-Warndateigesetz</b> (VWDG) vom 22.12.2013, Inkraftreten zum 01.03.2013	VISA-Warndateigesetz (VWDG) - Datei zur Vermeidung des Missbrauchs von VISA, geführt beim BVA	BGBl. I 2011,Seite 3037
41.	<b>Gesetz zur Änderung des Antiterrorgesetzes und anderer Gesetze</b> (G.v.18.12.2014)	Einführung der erweiterten Datennutzung (Analysesysteme) in ATD und RED	BGBl. I 2014, Seite 2318
42.	<b>IT-Sicherheitsgesetz</b> (2015)	Erhöhung der Sicherheit informationstechnischer Systeme: <ul style="list-style-type: none"> <li>• Mindeststandards für Betreiber Kritischer Infrastrukturen</li> <li>• Meldung erheblicher IT-Sicherheitsvorfälle an das BSI (zentrale Rolle beim Schutz kritischer Infrastrukturen in Deutschland)</li> <li>• Anforderung an angemessene technische und organisatorische Vorkehrungen zum Schutz von IT-Systemen (mittels Standardisierungen und Auditierungen nachzuweisen)</li> <li>• Mitwirkung des BfDI bei Meldungen nach dem IT-Sicherheitsgesetz und die Kontrolle der Datenerhebungs- und -verwendungskonzepte</li> </ul>	
43.	<b>Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten</b> (GVVG-Änderungsgesetz – GVVG-ÄndG) vom 12.Juni 2015	Umsetzung der UN-Sicherheitsratsresolution zur Reduzierung der Gefahren "ausländischer terroristischer Kämpfer" durch Strafbarkeit des Reisens zum Zwecke der Vorbereitung schwerer staatsgefährdender Gewalttaten; Straftatbestände zur Terrorismusfinanzierung; Änderung der §§89a, 89c und 261 Strafgesetzbuch; Einschränkungen des Brief-, Post- und Fernmeldegeheimnisses und der Unverletzlichkeit der Wohnung	BGBl. I 2015, Seite 926



44.	<b>Gesetz zur Änderung des Personalausweisgesetzes zur Einführung eines Ersatz-Personalausweises und zur Änderung des Passgesetzes (G.v.20.6.2015 )</b>	Ausstellung eines Ersatz-Personalausweises bei gleichzeitiger Einziehung/ Versagung des Personalausweises insbes. für sog. Dschihadisten. Ersatz-Dokument enthält in mehreren Sprachen den Hinweis, dass es nicht zur Ausreise aus Deutschland berechtigt. Problematisch auch die Voraussetzungen, unter denen das Gesetz zur Anwendung kommt (strafrechtliche Verlagerung weit in allg. Unterstützungs- und Vorbereitungs-handlungen).	BGBl. I S. 970
45.	<b>Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutz (G.v. 17.11.2015,)</b>	Einführung eines neuen nachrichtendienstlichen Informationsverbundes, Absenkung gesetzlicher Schwellen, problematische Regelung zu V-Personen u.a.	BGBl I S. 1938
46.	<b>Gesetz zur Einführung einer Speicherpflicht und einer Höchst-speicherfrist für Verkehrsdaten (2015)</b>	Vorratsdatenspeicherung II	BGBl I 2015 S. 2218
47.	<b>Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen (G.v. 3.12.2015)</b>	Umsetzung der Ergebnisse der Evaluierung befristeter Befugnisse der Nachrichtendienste des Bundes zur Terrorismusbekämpfung: Verlängerung der durch die Terrorismusbekämpfungsgesetze geschaffenen Regelungen im Bundesverfassungsschutz, MAD-, BND- und Sicherheitsüberprüfungsgesetz bei neuerlicher Befristung zum 10.01.2021, Ausnahmeregelung zum vorbeugenden personellen Sabotageschutz, Regelung verdeckter Einsichtnahme der Nachrichtendienste in Grundbücher und Grundakten; Einschränkung des Grundrechts des Fernmelde-geheimnisses; erneute Evaluierung unter Einbeziehung wissenschaftlicher Sachverständiger	BGBl I S. 2161
48.	<b>Datenaustauschverbesserungsgesetz (G.v. 5.2.2016)</b>	Schaffung eines zentralen Kerndatensystems für die Registrierung Asyl- und Schutzsuchender im Ausländerzentralregister (AZR); Ergänzung bisher zu speichernder Grundpersonalien um weitere Daten; Erfassung im Kerndatensystem bei erstmaligem behördlichem Kontakt, Sicherheitsabgleich, Verpflichtung aller zur Registrierung befugten Stellen zur Datenübermittlung an das AZR, Ermächtigung öffentlicher Stellen zum Datenabruf aus dem Kernsystem im Rahmen der Aufgabenerfüllung; Übermittlungsbefugnis des BAMF für im AZR gespeicherte Daten an Forschungseinrichtungen; Einfügung eines § 34 a AZR-Gesetz zu Prüfpflichten des BfDI und der LfD.	BGBl. I S. 130

49.	<p><b>Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (G.v. 30.6.2016,)</b></p>	<p><b><u>Im Bereich Polizei und Justiz:</u></b></p> <ul style="list-style-type: none"> <li>- keine zusätzlichen Abhilfebefugnisse des BfDI entgegen Art. 47 Abs. 2 JI-RL;</li> <li>- keine gerichtlichen Überprüfungsmöglichkeiten für BfDI entgegen Art. 47 Abs. 5 JI-RL;</li> <li>- unzureichende Umsetzung der Verwendung besonderer Kategorien personenbezogener Daten (ergänzendes Fachrecht erforderlich);</li> <li>- unzureichende Umsetzung der Zulässigkeit von Zweckänderungen (ergänzendes Fachrecht erforderlich)</li> </ul> <p><b><u>Im Bereich der Nachrichtendienste:</u></b></p> <ul style="list-style-type: none"> <li>- weiterhin keine Sanktions- bzw. Abhilfemöglichkeiten der BfDI bei Rechtsverstößen durch die Nachrichtendienste,</li> <li>- erhebliche Einschränkung der Rechte des BfDI sowie des Bundestages und des Bundesrates durch Änderung des BND-Gesetzes: Durch Art. 4 wird § 32a ins BND-Gesetz eingefügt: danach darf sich der BfDI den BND betreffend künftig nur an die Bundesregierung sowie an die für die Kontrolle des BND zuständigen Gremien wenden. Bislang durfte er sich (entsprechend §§ 24, 26 BDSG-alt bzw. § 14 Abs. 2 BDSG-neu) zur Erfüllung seiner Aufgaben zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an den Bundestag oder einen seiner Ausschüsse, den Bundesrat, die Bundesregierung sowie sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten.</li> </ul>	BGBl. I S. 2097
50.	<p><b>Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus (G.v. 26.7. 2016,)</b></p>	<ul style="list-style-type: none"> <li>• Einrichtung gemeinsamer Dateien mit ausländischen Partnerdiensten (BfV),</li> <li>• Verlängerung gemeinsamer Projektdateien der Sicherheitsbehörden auf nationaler Ebene;</li> <li>• keine hinreichende Datenschutzkontrolle (BVerfG: Kompensationsfunktion), insbesondere im Hinblick auf die Prüfung von deutschen Daten in ausländischen Dateien</li> <li>• Möglichkeit präventiven Einsatzes Verdeckter Ermittler der Bundespolizei zur Bekämpfung der Schleusungskriminalität,</li> <li>• Verifizierung der Identität der Nutzer von im Voraus bezahlten Mobilfunkdiensten (Prepaid-Tarife),</li> <li>• - Einschränkung von Grundrechten (Fernmeldegeheimnis).</li> </ul>	BGBl. I S. 1818
51.	<p><b>Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes (G.v. 30.11.2016)</b></p>	<p>Einrichtung eines Ständigen Bevollmächtigten, der das PKGr unterstützt</p>	

52.	<b>Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes</b> (G.v. 23.12.2016,)	<p>Legalisierung der Ausland-Ausland-Überwachung:</p> <ul style="list-style-type: none"> <li>- keine Regelung der Ausland-Ausland-FMA vom Ausland aus;</li> <li>- Datenschutzkontrolle nicht hinreichend gewährleistet (BVerfG: Kompensationsfunktion);</li> <li>- Fernmeldegeheimnis nicht gewährleistet (Verwendung untauglicher Filtersysteme);</li> <li>- maximale Anordnungsfrist 9 Monate (G 10: 3 Monate),</li> <li>- weitere Zersplitterung Kontrolllandschaft;</li> <li>- Heilung rechtswidriger Datenerhebungen vorgesehen;</li> <li>- verfassungswidriger Eingriff in Art. 10 GG durch Eignungsprüfung incl. zweckändernder Nutzung;</li> <li>- Kooperation mit AND: unzureichende Prüfkompetenz BfDI</li> </ul>	BGBl. I S. 3346
53.	<b>Videoüberwachungsverbesserungsgesetz (2017)</b>	Änderung des § 6b Absatz 1 und 3 BDSG mit dem Ziel der Ausweitung der Videoüberwachung durch private Betreiber öffentlich zugänglicher, großflächiger Anlagen (z.B. Sport- und Versammlungsstätten, ÖPNV)	BGBl. I S. 968
54.	<b>Gesetz zur Änderung des Zollverwaltungsgesetzes</b> vom 10. März 2017	Anpassung der Regelungen des Zollverwaltungsgesetzes an die Verordnung (EU) Nr. 952/2013 vom 09. Oktober 2013 zur Festlegung des Zollkodex der Union; u.a. Verschärfung von Regeln zur Überwachung und Bekämpfung von Geldwäsche durch den Zoll (z.B. Verschärfung der Anmelde- und Mitwirkungspflichten bei grenzüberschreitendem Verkehr mit Barmitteln).	BGBl. I S. 425
55.	<b>Gesetz zur Neuregelung des Bundesarchivrechts</b> (G.v. 10.3.2017)	Problem/ Gefahr des Unterlaufens datenschutzgerechter Regelungen in bereichsspezifischen Fachgesetzen durch das Gesetz zur Neuregelung des Bundesarchivrechts, insbesondere hinsichtlich elektronischer Unterlagen, die der fortlaufenden Aktualisierung unterliegen (IT-basierte Register). Mit der Begründung von Methoden- oder Quellenschutz kann sich der BND umfänglich der grundsätzlich bestehenden Anbieterspflicht gegenüber dem Bundesarchiv entziehen.	BGBl. I S. 410
56.	<b>Gesetz zur Änderung des Soldatengesetzes und weiterer soldatenrechtlicher Vorschriften</b> vom 27. März 2017	Einführung einer Soldateneinstellungsüberprüfung (Ü1 bei erstmaliger Berufung in ein Dienstverhältnis als Berufssoldat oder Soldat auf Zeit).	BGBl. I 2017 S. 562
57.	<b>Gesetz zur Verbesserung der Fahndung bei besonderen Gefahrenlagen und zum Schutz von Beamtinnen und Beamten der Bundespolizei durch den Einsatz von mobiler Videotechnik</b> ( G. v. 05.05.2017)	Änderung BPolG: Einfügung § 27a ( Mobile Bild- und Tonaufzeichnungsgeräte), § 27b ( Anlassbezogene automatische Kennzeichenerfassung), § 27c ( Gesprächsaufzeichnung)	BGBl. I S. 1066
58.	<b>Gesetz zur Umsetzung der Vierten Geldwäscherichtlinie</b> (Richtlinie (EU))	Neufassung des bestehenden Geldwäschegesetzes; Schaffung der Zentralstelle für Finanztransaktionsuntersuchungen (FIU) bei der Generalzolldirektion als zentrale Meldestelle für geldwäscherechtliche Meldungen. Nähere Regelungen zur Geld-	

	2015/849), zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen	transferverordnung	
59.	<b>Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681</b> (Fluggastdatengesetz – FlugDaG)(2017)	Umsetzung der Fluggastdatenrichtlinie (PNR-Records)	
60.	<b>Gesetz zur besseren Durchsetzung der Ausreisepflicht</b> vom 20. Juli 2017	Regelungen im Ausländerrecht und im Asylrecht werden angepasst, um die Durchsetzung einer Verpflichtung, auszureisen, effektiver durchzusetzen.	BGBl. I S. 2780
61.	<b>Dreiundfünfzigstes Gesetz zur Änderung des Strafgesetzbuches–Ausweitung des Maßregelrechts bei extremistischen Straftätern</b> vom 11. Juni 2017	Ausweitung von elektronischer Aufenthaltsüberwachung (EAÜ, "elektronische Fußfessel") und fakultativer Anordnung der Sicherungsverwahrung auf Vorbereitung einer schweren staatsgefährdenden Straftat, Terrorismusfinanzierung sowie Mitgliedschaft in bzw. Werbung für eine inländische oder ausländische terroristische Organisation; Absenkung der erforderlichen Mindestvollverbüßungszeit für die Anordnung einer EAÜ auf 2 Jahre; Änderung §§ 66 und 68b Strafgesetzbuch, Einfügung Art. 316 Einführungsgesetz zum Strafgesetzbuch sowie Änderung § 463a Strafprozessordnung	BGBl I 2017 S. 1612
62.	<b>Gesetz zur Förderung des elektronischen Identitätsnachweises</b> (G. v. 7.7.2017, )	Zugriffsmöglichkeit für Polizeibehörden des Bundes und der Länder, MAD, BND, Verfassungsschutzbehörden des Bundes und der Länder, Steuerfahndungsdienststellen der Länder, Zollfahndungsdienst und Hauptzollämter auf die biometrischen Fotos von Personalausweis und Pass im automatisierten Verfahren zur Erfüllung ihrer Aufgaben. Gefahr des Aufbaus faktischer Biometrie-Datenbanken bei diesen Behörden	BGBl. I S. 2310
63.	<b>Fünfundfünfzigstes Gesetz zur Änderung des Strafgesetzbuches–Wohnungseinbruchdiebstahl</b> vom 17. Juli 2017	Anpassung des Strafrahmens, Anhebung der Mindeststrafe von Einbrüchen in eine dauerhaft genutzte Privatwohnung, Aufnahme in den TKÜ-Katalog schwerer Straftaten; Einschränkung von Grundrechten betr. Brief-, Post- und Fernmeldegeheimnis; Änderung § 244 Strafgesetzbuch sowie §§ 100g und 395 Strafprozessordnung.	BGBl I 2017 S. 2442
64.	<b>Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens</b> vom 18.7.2017	Quellen-TKÜ und Online-Durchsuchung in der Strafprozessordnung (als Formulierungshilfe im Nachtrag!). Leichtere Datenübermittlungen von Bewährungshelfern an die Polizei unter Umgehung der Führungsaufsicht.	BGBl I 2017 S. 3202

65.	<b>Neues BKAG</b> (2017, Inkrafttreten Juni 2018)	Neuregelung der Datenverarbeitung im BKAG. Insb. neuer Informationsverbund und Informationssystem für das BKA (Aufhebung der bisherigen Trennung in logische Dateien). Neuregelung von Prüffalldateien u.a.  Daneben Umsetzung der Vorgaben des Bundesverfassungsgerichts vom 20. April 2016 (BVerfGE 141, 220) und der EU-Richtlinie 2016/680).	BGBl I 2017 S. 1354
66.	<b>Zweites Gesetz zur besseren Durchsetzung der Ausreisepflicht</b> (Geordnete-Rückkehr-Gesetz)	Erweiterung der Möglichkeiten zur Datenübermittlung zwischen BAMF und BPol/BKA sowie mit dem BfV.	
67.	<b>Zweites Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu Aufenthalts- und asylrechtlichen Zwecken (Zweites Datenaustauschverbesserungsgesetz - 2. DAVG)</b> vom 04.08.2019	<ul style="list-style-type: none"> <li>• Umfassende Möglichkeit des automatisierten Abrufs von Daten aus dem Ausländerzentralregister für BfV und MAD</li> <li>• Protokollierung nachrichtendienstlicher Datenabrufe aus dem Ausländerzentralregister durch den jeweiligen Nachrichtendienst selbst</li> <li>• Einbeziehung der BPol in den Sicherheitsabgleichs und Vorsehen des Sicherheitsabgleichs auch in Widerrufs-/Rücknahmeverfahren bei Flüchtlingschutz und subsidiärem Schutz, bei Übernahmeersuchen nach der Art. 21 Verordnung (EU) Nummer 604/2013 und nationalen Neuansiedlungsverfahren sowie bei sonstigen humanitären Aufnahmeverfahren von Drittstaatsangehörigen und der Umverteilung von Asyltragstellern aufgrund von Maßnahmen nach Artikel 78 Absatz 3 AEUV</li> </ul>	BGBl. I 2019 S. 1131
68.	<b>Entwurf IT-Sicherheitsgesetz 2.0</b> (2019)	<ul style="list-style-type: none"> <li>• BSIG-Änderungen, vor allem Erweiterung der Befugnisse des BSI</li> <li>• TKG-Änderungen, insb. Benachrichtigungspflichten und Pflicht zur Nutzung von Angriffserkennungssysteme</li> <li>• StGB-Änderung, insb. Kriminalisierung von Verschlüsselungs- und Anonymisierungsdiensten</li> <li>• StPO-Änderung, insb. Ausweitung Katalog für TKÜ und Online-Durchsuchung sowie Account-Übernahmen und –Nutzung auch der Identität bei Kontakt ggü. Dritten</li> <li>• IRG-Änderung, insb. Erweiterung von Speicherfristen</li> </ul>	
69.	<b>Entwurf eines Gesetzes zur Neustrukturierung des Zollfahndungsdienstgesetzes</b> (2019)	Nachfolgend aufgeführte Punkte sollen u.a.durch eine konstitutive Neufassung des Zollfahndungsdienstgesetzes umgesetzt und aufgenommen werden. <ul style="list-style-type: none"> <li>• die Schaffung der Möglichkeit zum Einsatz Verdeckter Ermittler</li> <li>• die Befugnis zur Identifizierung und Lokalisierung von Mobilfunkkarten und Telekommunikationsendgeräten, bspw. durch IMSI-Catcher oder WLAN-Catcher im Rahmen der Gefahrenabwehr</li> <li>• die Erweiterung der Auskunftspflichten von Betroffenen und Dritten</li> </ul>	

70.	<b>Drittes Gesetz zur Änderung des Staatsangehörigkeitsgesetzes</b> vom 04.08.2019	Mit dem Änderungsgesetz wird eine neue Verlustregelung in das Staatsangehörigkeitsgesetz eingeführt. Danach verlieren Deutsche mit Doppelpass, die sich an Kampfhandlungen einer terroristischen Vereinigung im Ausland beteiligen, die deutsche Staatsangehörigkeit. Das Gesetz ist am 9. August 2019 in Kraft getreten. Die Verlustregelung findet keine Anwendung auf Minderjährige.	BGBl. I 2019 S. 1124
71.	<b>Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679</b> vom 20. November 2019	- Neugestaltung der bereichsspezifischen Sonderregeln und Nutzung vorgesehener Ausnahmen und Öffnungsklauseln für das Strafverfahrensrecht und das Justizverwaltungsrecht einschl. der bereichsspezifischen Vorschriften für den grenzüberschreitenden Datenaustausch im Rechtshilfeverkehr neben den allgemeinen Regelungen des Bundesdatenschutzgesetzes;  - Einschränkung von Grundrechten betr. Fernmeldegeheimnis; Änderung, Neufassung und Einfügung zahlr §§ Strafprozessordnung, Zivilprozessordnung, Schuldnerverzeichnisabdruckverordnung, Strafvollzugsgesetz, Grundbuchordnung und Gesetz über internationale Rechtshilfe in Strafsachen,	BGBl. I 2019 S. 1724
72.	<b>Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU-2. DSAnpUG-EU)</b> vom 20. November 201	Nachfolgend bereichsspezifische Datenschutzregelungen des Bundes mit folgenden Schwerpunkten den EU-Vorgaben wurden angepasst: <ul style="list-style-type: none"> <li>• Anpassung von Begriffsbestimmungen und Verweisungen</li> <li>• Anpassung von Rechtsgrundlagen für die Datenverarbeitung</li> <li>• Regelungen zu den Betroffenenrechten</li> <li>• Anpassungen aufgrund unmittelbar geltender Vorgaben der DSGVO zu technischen und organisatorischen Maßnahmen, zur Auftragsverarbeitung, zur Datenübermittlung an Drittländer oder an internationale Organisationen sowie zu Schadenersatz und Geldbußen.</li> </ul>	BGBl. I 2019 S. 1626
73.	<b>Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie</b> vom 12. Dezember 2019	Umsetzung der erweiterten EU-Vorgaben zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, z.B. Zugang zu im Transparenzregister gespeicherten Daten grundsätzlich für die gesamte Öffentlichkeit, Erweiterung des Personenkreises der geldwäscherechtlich Verpflichteten, Kompetenzerweiterung der FIU	BGBl I 2019, S. 2602
74.	<b>Drittes Gesetz zur Änderung des Waffengesetzes und weitere Vorschriften</b> vom 17.02.2020	- Die zuständige Behörde hat künftig im Rahmen der Zuverlässigkeitsprüfung bei der (nach Wohnort) zuständigen Verfassungsschutzbehörde (im Zweifel beim BfV) abzufragen, ob dort Tatsachen bekannt sind, die gegen die Zuverlässigkeit der betreffenden Person sprechen, sog. „Regelabfrage“. - „Nachberichts“-Pflicht der Verfassungsschutzbehörden, wenn im Nachhinein bedeutsame Erkenntnisse für die Zuverlässigkeit bekannt werden. Zu diesem Zweck wird der Name, Vorname, Geburtsdatum, Geburtsname, Geburtsort, Wohnort und Staatsangehörigkeit der betroffenen Person gespeichert (gleiches gilt nach dem SprengG).	BGBl I 2020, S. 166

		<ul style="list-style-type: none"> <li>- Das Bedürfnis für den Besitz von Waffen wird künftig alle fünf Jahre von der zuständigen Waffenbehörde überprüft.</li> <li>- Als in der Regel waffenrechtlich unzuverlässig, gelten Personen, die Mitglied / Unterstützer einer verfassungsfeindlichen Vereinigung sind, unabhängig davon, ob diese verboten ist (gleiches gilt nach dem SprengG).</li> <li>- Die Länder werden ermächtigt, an belebten Orten und Bildungseinrichtungen Waffen- und Messerverbotzonen einzurichten.</li> <li>- Das nationale Waffenregister wird so ausgebaut, dass künftig der gesamte Lebenszyklus einer Waffe – von der Herstellung bis zur Vernichtung – behördlich nachvollziehbar ist.</li> </ul>	
75.	<b>Gesetz zur Stärkung der Sicherheit im Pass-, Ausweis- und ausländerrechtlichen Dokumentenwesen</b> 12.12.2020	<ul style="list-style-type: none"> <li>- Künftig wird die Speicherung von zwei Fingerabdrücken im Speichermedium des Personalausweises verpflichtend</li> <li>- Ab Mai 2025 sind nur noch digitale Passbilder möglich, die elektronisch an die Passbehörde übermittelt werden.</li> </ul>	BGBl, I S. 2744
76.	<b>Gesetz zur Entfristung von Vorschriften zur Terrorismusbekämpfung</b> vom 3. Dezember 2020	<ul style="list-style-type: none"> <li>- die durch TBG und TBEG geschaffenen Befugnisse der NDe waren befristet eingeführt und mit einer Pflicht zur Evaluierung versehen worden</li> <li>- die durch oder im Auftrag der Bundesregierung durchgeführten Evaluierungen wurden unzureichend durchgeführt – dennoch erfolgte nunmehr die Entfristung</li> <li>- es handelt sich insbesondere um Auskunftspflichten von Unternehmen der Branchen Luftverkehr, Finanzdienstleistungen, Telekommunikation und Telemedien zur Netzwerkaufklärung sowie Regelungen zum IMSI-Catcher-Einsatz zur Feststellung genutzter Mobiltelefonnummern und zur Ausschreibung im Schengener Informationssystem zur Nachverfolgung internationaler Bezüge</li> </ul>	BGBl. I 2020, S. 2667
77.	<b>Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme</b>	<ul style="list-style-type: none"> <li>- Unter anderem soll es Daten künftig über einen längeren Zeitraum speichern können.</li> <li>- Das Bundesamt wird als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit etabliert.</li> </ul>	
78.	<b>Entwurf: Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität</b>	<p>Als zentrale Neuerung im Netzwerkdurchsetzungsgesetz ist die Verpflichtung sozialer Netzwerke vorgesehen, dem Bundeskriminalamt als Zentralstelle bestimmte strafbare Inhalte zu melden, die den sozialen Netzwerken durch eine Beschwerde bekannt und von ihnen entfernt oder gesperrt wurden.</p>	

79.	<b>Entwurf eines Gesetzes zur Stärkung der Integrität in der Wirtschaft</b> Entwurf vom 21.10.2020	<ul style="list-style-type: none"> <li>- Schaffung eines Verbandssanktionenregister</li> <li>- auf Ersuchen erhalten u.a. Auskunft: <ul style="list-style-type: none"> <li>- Gerichte und Staatsanwaltschaften für Zwecke der Rechtspflege</li> <li>- Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst und der Militärische Abschirmdienst für die diesen Behörden übertragenen Aufgaben,</li> <li>- Kriminaldienst verrichtende Dienststellen der Polizei für Zwecke der Verhütung und Verfolgung von Straftaten,</li> </ul> </li> </ul>	BT-Drs. 19/23568 vom 21.10.2020 (Gesetzesentwurf)
80.	Entwurf eines <b>Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts</b> vom 27. Mai 2020	<ul style="list-style-type: none"> <li>- Zugriff auf Passwörter und IP-Adressen durch Sicherheitsbehörden</li> <li>- neben dem BKA künftig auch die Bundespolizei und die Zollfahndung bei Telemedienanbietern Passwörter abfragen</li> <li>- Zugriff auf Sicherheitscodes wie PINs und PUKs bei Telekommunikationsfirmen</li> </ul>	
81.	Entwurf eines <b>Gesetzes zur Stärkung der Finanzmarktintegrität</b>	Durch Anpassungen im Geldwäschegesetz und der Abgabenordnung werden die Befugnisse der FIU erweitert. Die FIU wird in die Lage versetzt sowohl steuerliche Grunddaten bei den Finanzbehörden als auch dem Steuergeheimnis unterliegende Daten bei dem Bundeszentralamt für Steuern (BZSt) automatisiert abzurufen.	
82.	<b>Entwurf eines Gesetzes zur intensivierte erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen von Soldatinnen und Soldaten und zur Sicherheitsüberprüfung von Reservistinnen und Reservisten</b> (Kabinettsbeschluss am 10.2.2021)	Einführung einer inhaltlich und zeitlich intensivierten Sicherheitsüberprüfung mit Sicherheitsermittlungen (verschärfte Ü3) für Soldatinnen und Soldaten in Verwendungen mit besonders hohen Sicherheitsanforderungen; Ausweitung der Ü1 bei Reservisten	
83.	<b>Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts</b> Entwurf vom 27. November 2020	<ul style="list-style-type: none"> <li>- Befugnis zur Quellen-Telekommunikationsüberwachung</li> <li>- Verpflichtung zur Mitwirkung der TK-Diensteanbieter zur "Umleitung" von Verkehren mit dem Ziel, Quellen-TKÜ zu ermöglichen</li> <li>- Informationsaustausch zwischen den Verfassungsschutzbehörden und dem Militärischen Abschirmdienst durch erweiterte Möglichkeiten gemeinsamer Datenhaltung</li> </ul>	BT-Drs 19/24785 (Gesetzesentwurf)
84.	<b>Entwurf Telekommunikationsmodernisierungsgesetz</b> Entwurf vom	- Erweiterung der Pflichten der Betreibern von Telekommunikationsanlagen zur Duldung der Aufstellung und des Betrieb von technischen Mitteln in eigenen Räumen durch die zur Überwachung der Telekommunikation berechtigten Stellen	BT-Drs 19/26108 vom 25.01.2021



	25.01.2021	nunmehr auch bei Individualmaßnahmen der TKÜ durch BfV und BAMAD - die entsprechende Erweiterung der Kontrollrechte der G10-Kommission fehlt bislang!	(Gesetzesentwurf)
85.	<b>Entwurf Gesetz zur Änderung straßenverkehrsrechtlicher Vorschriften – Gesetz zum autonomen Fahren</b>	geplant ist eine Datenübermittlungsregelung zur Weitergabe von beim autonomen Fahren generierten Daten durch das Kraftfahrt-Bundesamt an BfV und BKA	noch im Ressortverfahren, noch keine BT-Drs.
86.	<b>Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts– Gesetz über den Bundesnachrichtendienst</b>	Das BNDG ermöglicht weitreichende Eingriffe. Dazu gehören unter anderem:  - Befugnis zur strategischen Ausland-Fernmeldeaufklärung zur Gefahrenfrüherkennung und zur politischen Unterrichtung,  - Befugnis zum Eingriff in informationstechnische Systeme mittels Computer-Network-Exploitation („Hacking“) samt der Ermächtigung zur Durchführung einer Quellen-TKÜ von Ausländern im Ausland zur Gefahrenfrüherkennung und zur politischen Unterrichtung,  - Weitgehende Übermittlungsbefugnisse für Daten aus der strategischen Ausland-Fernmeldeaufklärung und der Computer-Network-Exploitation an in- und ausländische Stellen.  - Überwachtes Internetaufkommen wird nominell auf 30 % der weltweiten Netzkapazität festgesetzt; dies entspricht eher einer 100%igen Überwachungserlaubnis der effektiven Datenströme der erreichbaren Telekommunikationsnetze,  - Unkenntlich gemachte Verkehrsdaten von inländischen Grundrechtsträgern können repersonalisiert werden,  - Keine inhaltsbezogene Kooperation der Kontrollorgane.	BT-Drs. 19/26103 vom 25.01.2021  (Gesetzesentwurf)

<b>Liste Gesetze EU und International</b>			
<b>Nr.</b>	<b>Bezeichnung</b>	<b>Wesentlicher Inhalt/Gegenstand</b>	<b>Fundstelle</b>
1.	<b>Gesetz zum Internationalen Übereinkommen vom 15. Dezember 1997 zur Bekämpfung</b>	Ratifikation des von der VN-Generalversammlung am 15. Dezember 1997 angenommenen, von der Bundesrepublik Deutschland am 26. Januar 1998 in New York unterzeichneten Übereinkommens: Sicherstellung der weltweiten Verfolgung von Gewaltakten in Form von Bombenanschlägen, Verpflichtung	BGBI. II 2002, Seite 2506

	<b>terroristischer Bombenanschläge</b> vom 5. Oktober 2002	tung der Vertragsstaaten zur Einstufung als Straftat und zur Strafverfolgung oder Auslieferung, Begründung einer diesbezüglichen Gerichtsbarkeit	
2.	<b>Gesetz zum Internationalen Übereinkommen der Vereinten Nationen vom 9. Dezember 1999 zur Bekämpfung der Finanzierung des Terrorismus</b> vom 19. Dezember 2003	Ratifikation des am 20. Juli 2000 von der Bundesrepublik Deutschland unterzeichneten Abkommens: Strafbarkeit des Sammelns und Bereitstellens finanzieller Mittel, die der Finanzierung terroristischer Akte dienen; Verpflichtung der Mitgliedstaaten zur Schaffung von Möglichkeiten der Beschlagnahme und Einziehung, Regelungen zur Begründung der internationalen Gerichtsbarkeit sowie zur Rechtshilfe und Auslieferung.	BGBl. II 2003, Seite 1923
3.	<b>Gesetz zur Umsetzung des EU-Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze</b> vom 22. Dezember 2003	EU-einheitliche Definition der terroristischen Straftaten sowie Festlegung von Strafsanktionen für bestimmte Delikte; Änderung §§129a und 261 StGB, §120 GVG sowie von §112 StPO.	BGBl. I 2003, Seite 2836
4.	Gesetz zum Abkommen vom 3. März 2003 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Türkei über die Zusammenarbeit bei der Bekämpfung von Straftaten mit erheblicher Bedeutung, insbesondere des Terrorismus und der organisierten Kriminalität vom 23. Juli 2004	Ratifikation des am 3. März 2003 in Ankara unterzeichneten Abkommens: Zusammenarbeit der Behörden bei der Bekämpfung des Terrorismus, der Organisierten Kriminalität und anderer Straftaten außerhalb der Rechtshilfe, u.a. Entsendung von Verbindungsbeamten und Austausch von Fachleuten, Regelungen für die Verwendung personenbezogener Daten.	BGBl. II 2004, Seite 1059
5.	Gesetz zum Abkommen vom 7. April 2003 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Tunesischen	Zusammenarbeit bei der Bekämpfung der Organisierten Kriminalität und des Terrorismus.	BGBl. II 2004, Seite 1570

	Republik über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung, Gesetz vom 02.Dezember 2004		
6.	Gesetz vom 20.Dezember 2007 zu dem Abkommen zwischen der Europäischen Union und den USA über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records -PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security vom 26.Juli 2007	Ratifikation des am 23.Juli 2007 in Brüssel von der EU und am 26.Juli 2007 in Washington von den USA unterzeichneten Abkommens nebst begleitendem Briefwechsel: Arten und Umfang der übermittelten Daten, Übermittlungsverfahren und Verwendungszweck, Datenspeicherung und Datenschutzmaßnahmen durch das DHS, Rechtsmittel und Rechtsbehelfe.	BGBl. II 2007, Seite 1978
7.	Gesetz zu dem Abkommen vom 24.September 2005 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Arabischen Emirate über die Zusammenarbeit im Sicherheitsbereich vom 29.Juli 2008	Ratifikation des in Abu Dhabi am 24.September 2005 unterzeichneten Abkommens zur Erhöhung der Inneren Sicherheit in den Vertragsstaaten durch verbesserte Zusammenarbeit bei der Terrorismusbekämpfung und der grenzüberschreitenden Kriminalität.	BGBl. II 2008, Seite 758
8.	Gesetz zu dem Abkommen vom 31.August 2006 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Sozialistischen Republik Vietnam über die Zusammenarbeit bei der Bekämpfung von	Ratifikation des in Berlin am 31.August 2006 unterzeichneten Abkommens zur Erhöhung der Inneren Sicherheit in den Vertragsstaaten durch verbesserte Zusammenarbeit bei der Bekämpfung schwer-wiegender Straftaten und Organisierter Kriminalität	BGBl. II 2008, Seite 1182 BGBl. II 2009, Seite 964b

	schwerwiegenden Straftaten und der organisierten Kriminalität, Gesetz vom 23.Oktober 2008		
9.	Gesetz zu dem Abkommen vom 1.Oktober 2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität vom 1.September 2009	Annahme einer EntschlieÙung: Bedeutung der partnerschaftlichen Zusammenarbeit mit den USA zur Verhinderung und Bekämpfung schwerwiegender Kriminalität, insbesondere des internationalen Terrorismus; besondere Anforderungen an die Übermittlung personenbezogener Daten, keine Notwendigkeit für die Datenkategorie Mitgliedschaft in einer Gewerkschaft beider Terrorismusbekämpfung, Bekräftigung des besonderen verfassungsrechtlichen Schutzes der Gewerkschaften.	BGBI. II 2009, Seite 1010
10.	Gesetz zur Umsetzung des Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika vom 1.Oktober 2008 über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität vom 11.September 2009	Umsetzung des Abkommens mit den USA über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität in nationales Recht: Bundeskriminalamt (BKA) als nationale Kontaktstelle; Vertretung der völkerrechtlichen Ansprüche Betroffener auf Auskunft, Berichtigung, Sperrung und Löschung personenbezogener Daten gegenüber den USA durch das BKA; Ergänzung der Regelungen zur Verwendung von DNA-Daten nach dem Bundeskriminalamtgesetz, Schaffung rechtlicher Regelungen für den automatisierten Abruf von DNA-Daten.	BGBI. I 2009, Seite 2998
11.	Gesetz zu dem Abkommen vom 30.August 2010 zwischen der Regierung der Bundesrepublik Deutschland und dem Ministerkabinett der Ukraine über die Zusammenarbeit im Bereich der Be-	Zustimmung zu dem am 30.August 2010 in Berlin unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von Organisierter Kriminalität, Terrorismus und anderen Straftaten von erheblicher Bedeutung: Formen und Verfahren der Zusammenarbeit sowie zuständige Stellen, Datenübermittlung und Datenschutz	BGBI. II 2012, Seite 435

	kämpfung der Organisierten Kriminalität, des Terrorismus und anderer Straftaten von erheblicher Bedeutung vom 3.Mai 2012		
12.	Gesetz zu dem Abkommen vom 14.April 2010 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Kosovo über die Zusammenarbeit im Sicherheitsbereich vom 3.Mai 2012	Zustimmung zu dem am 14.April 2009 in Berlin unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von organisierter Kriminalität, schwerer Kriminalität und Terrorismus: Formen und Verfahren der Zusammenarbeit, Verhütung und Bekämpfung der Betäubungsmittelkriminalität, zuständige Stellen, Datenschutz, Fälschungssicherheit von Reisedokumenten.	BGBI. II 2012, Seite 427
13.	Gesetz zu dem Abkommen vom 27.Mai 2009 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung des Königreichs Saudi-Arabien über die Zusammenarbeit im Sicherheitsbereich vom 3.Mai 2012	Zustimmung zu dem am 27.Mai 2009 in Riad unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von grenzüberschreitender organisierter Kriminalität und Terrorismus: Bereiche, Mittel und Formen der Zusammenarbeit, Datenschutz, zuständige Behörden.	BGBI. II 2012, Seite 415
14.	Gesetz zu dem Abkommen vom 10.März 2009 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Kroatien über die Zusammenarbeit bei der Bekämpfung der Organisierten und der schweren Kriminalität vom 3.Mai 2012	Zustimmung zu dem am 10. März 2009 in Berlin unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von organisierter Kriminalität, schwerer Kriminalität und Terrorismus: Formen und Bereiche der Zusammenarbeit, Informationsübermittlung und Datenschutz, zuständige Stellen.	BGBI. II 2012, Seite 408
15.	Gesetz zu dem Abkommen vom 22.Februar 2009	Zustimmung zu dem am 22.Februar 2009 in Doha unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von Terrorismus und grenzüberschreitender Kriminalität: Formen	BGBI. II 2012, Seite 421

	zwischen der Regierung der Bundesrepublik Deutschland und der Regierung des Staates Katar über die Zusammenarbeit im Sicherheitsbereich, Gesetz vom 3.Mai 2012	und Verfahren der Zusammenarbeit sowie zuständige Stellen, Datenübermittlung und Datensicherheit, Fälschungssicherheit von Reisedokumenten	
16.	Gesetz zu dem Abkommen vom 13.Februar 2007 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung des Staates Kuwait über die Zusammenarbeit im Sicherheitsbereich, Gesetz vom 3.Mai 2012	Zustimmung zu dem am 13.Februar 2007 in Berlin unterzeichneten Abkommen zur Zusammenarbeit bei Bekämpfung von Terrorismus und grenzüberschreitender Kriminalität: Formen und Verfahren der Zusammenarbeit sowie zuständige Stellen, Datenübermittlung und Datensicherheit, Fälschungssicherheit von Reisedokumenten.	BGBl. II 2012, Seite 402
17.	Prümer Vertrag (2006) und dessen Überführung in den Rechtsrahmen der EU (2009)	Datenaustausch von DNA-, Fingerabdruck und Kfz-Registerdaten zwischen den Unterzeichnerstaaten und der im Nachgang beigetretenen Staaten (Teil der EU-Staaten und seit 06/2019 auch Schweiz), Datenaustausch über terroristische Gefährder sowie im Zusammenhang von Großveranstaltungen.	BGBl. II 2006, Seite 626
18.	VN-EU-Terrorlisten	Infolge Urteils des EuGH muss das Listing-Verfahren der Aufnahme von Personen in die sog. Terrorlisten der EU (in Anlehnung der entspr. Listen der VN) überarbeitet werden. Insbesondere muss betroffenen Personen eine Möglichkeit der Anhörung und des Rechtsschutzes eingeräumt werden.	
19.	Übermittlung von Fluggastdaten aus und nach Europa gemäß PNR-Abkommen mit Drittstaaten	Übermittlung verschiedener Kategorien personenbezogener Daten von Fluggästen (PNR – Passenger Name Records) an Behörden der USA, Kanada und Australiens.	
20.	D-USA-Abkommen vom 1. Oktober 2008 über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender	Teilautomatisierter Austausch von daktyloskopischen und DNA-Daten mit US-Stellen, Austausch von personenbezogenen Daten zur Bekämpfung des internationalen Terrorismus	

	Kriminalität		
21.	<b>Abschluss eines TFTP-Abkommen zwischen der EU und den USA</b> (2010/412/EU)	Übereinkommen zwischen der EU und den USA zur Übermittlung von auf europäischen Servern liegenden Finanztransaktionsdaten nach sog. „requests“ der USA, die von Europol vor Übermittlung der Daten zu überprüfen sind. Innereuropäische Überweisungen sind nur dann ausgeschlossen, wenn sie über das SEPA-System (Single European Payment Area – Einheitlicher Euro-Zahlungsverkehrsraum) abgewickelt werden.	Amtsblatt der Europäischen Union L 195/3
22.	Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den <b>Strafverfolgungsbehörden der Mitgliedstaaten der EU („Schwedische Initiative“)</b> RAHMENBESCHLUSS 2006/960/JI DES RATES	Für den Informationsaustausch von Strafverfolgungsbehörden innerhalb der EU sollen keine höheren Anforderungen gelten als für den innerstaatlichen Informationsaustausch	Amtsblatt der Europäischen Union L 386/89
23.	<b>Europol-Verordnung (EU) 2016/794 (2017)</b>	Vollständige Überführung Europols in den Rechtsrahmen der EU, Berechtigung der Behörden der Bundespolizei und des Zollfahndungsdienstes zum unmittelbaren Datenaustausch mit Europol-Verbindungsbeamten sowie dem Europol-Informationssystem.	Amtsblatt der Europäischen Union L 135/53
24.	<b>Schengener Informationssystem der zweiten Generation (SIS II)</b>  BESCHLUSS 2007/533/JI DES RATES	Dient der Personen- und Sachfahndung innerhalb der EU. Gespeichert werden unerwünschte, zur Fahndung ausgeschriebene oder vermisste Personen und zu überwachende Sachen (z. B. Kfz). Zugriffsberechtigung besteht für die europäischen Sicherheitsbehörden, Europol und Eurojust. Die Betreuung des europäischen Zentralsystems erfolgt durch die IT-Agentur der EU (eu-LISA).	Amtsblatt der Europäischen Union L 205/63
25.	<b>Verordnung für eine Europäische Ermittlungsanordnung</b> RICHTLINIE 2014/41/EU DES EUROPÄISCHEN PARLAMENTES UND DES RATES	Gegenseitige Anerkennung und Vollstreckbarkeit von Ermittlungsanordnungen in der EU (z.B. Wohnungsdurchsuchungen, Lauschangriffe).	Amtsblatt der Europäischen Union L 130/1

26.	Richtlinie (EU) 2016/681 über die Verwendung von <b>Fluggastdatensätzen</b> (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität	Einführung eines eigenen EU-PNR-Systems. Danach werden PNR-Daten von Flugpassagieren bei Flügen nach oder von Drittstaaten und ggfs. auch von EU-internen Flügen zu Zwecken der Risikobewertung und Strafverfolgung genutzt und für 5 Jahre gespeichert. Die nationale Umsetzung erfolgte durch das FlugDaG	Amtsblatt der Europäischen Union L 119/132
27.	<b>Eurodac-Verordnung</b> (EU) Nr. 603/2013 (2013)	Räumt seit 2015 den Zugriff der Sicherheitsbehörden auf das EURODAC-Informationssystem ein.	Amtsblatt der Europäischen Union L 180/1
28.	<b>Schengener Informationssystem SIS III</b> Verordnung (EU)2018/1860, Verordnung (EU)2018/1861 und Verordnung (EU)2018/1862 (jeweils 28.11.2018)	Ausbau von SIS II. Verpflichtet die teilnehmenden nat. Behörden in Fällen, die mit Terroristischen Straftaten in Verbindung stehen, eine Warnmeldung zu erstellen. Neue Ausschreibungskategorie „Ermittlungsanfrage“ (Befragung anhand spezifischer Informationen der Fragen des ausschreibenden Mitgliedstaates). Ausschreibung unbekannter Personen in Verb. mit schweren oder terror. Straftaten (auch anhand von Fingerabdrücken). Künftig auch Bildabgleiche.	
29.	<b>Entry-Exit-System Verordnung</b> (EU)2017/2226 (30.11.2017)	An den EU-Außengrenzen werden die Daten des Grenzübertritts erfasst. Zweck der Erfassung ist die (automatische) Berechnung der Aufenthaltszeit im Schengenraum und im Fall der Überschreitung des erlaubten Zeitraums die Benachrichtigung der Mitgliedstaaten. Erfasst werden Stamm- und biometrische Daten.	



30.	<p><b>ETIAS</b>  <b>European Travel Information and Authorization System</b>  - Europäisches Reiseinformations- und Reisegenehmigungssystem –  (Voraussichtliche Inbetriebnahme 2021)  Die Verordnung (EU) 2018/1240</p>	<p>Wird ein elektronisches Reisegehmigungssystem ähnlich dem US-amerikanischen ESTA-System.</p> <p>Zielergruppe sind von der Visumpflicht befreite Drittstaatsangehörige. Diese müssen sich vorab registrieren und es erfolgt ein Sicherheitscheck durch Abgleich mit EU- und Interpol Datenbanken zur Feststellung ob ein Antragsteller in den Schengenraum einreisen darf.</p> <p>Erfasst werden sollen:</p> <ul style="list-style-type: none"> <li>• Vorname</li> <li>• Familienname</li> <li>• Geburtsname</li> <li>• Geburtsdatum</li> <li>• Geburtsort</li> <li>• Informationen bezüglich der Staatsangehörigkeit</li> <li>• Adresse</li> <li>• E-Mailadresse und Telefonnummer</li> <li>• Ausbildung und Arbeitserfahrung</li> <li>• erstes EU-Land, in das der Antragsteller beabsichtigt zu reisen</li> <li>• Fragen zu Berechtigung und Hintergrund, die auf den Gesundheitszustand, Reisen in Kriegsgebiete oder Regionen, in denen der Antragsteller abgeschoben oder ausgewiesen wurde, oder Strafregister abzielen</li> <li>• bei Minderjährigen muss der Erziehungsberechtigte den Antrag für ETIAS stellen</li> <li>• Familienmitglieder von EU-Bürgern aus einem anderen Land müssen Beweise für die Beziehung, die Aufenthaltsgenehmigung und weitere Hintergrundinformationen einreichen.</li> </ul>	
31.	<p><b>Interoperabilität</b>  (in Planung; Annahme der entsprechenden Verordnungen durch den Rat ist bereits erfolgt)</p>	<p>Ziel ist ein erleichterter Austausch zwischen den (bestehenden) Eu-Informationssystemen im Bereich Justiz und Inneres. Vorgesehen sind folgende Interoperabilitätskomponenten:</p> <ul style="list-style-type: none"> <li>• ein europäisches Suchportal, das den zuständigen Behörden parallele Abfragen in mehreren EU-Informationssystemen ermöglichen würde, und zwar sowohl mit biografischen als auch mit biometrischen Daten,</li> <li>• einen gemeinsamen Dienst für den Abgleich biometrischer Daten, der die Abfrage und den Abgleich biometrischer Daten (Fingerabdrücke und Gesichtsbilder) aus mehreren Systemen ermöglichen würde,</li> <li>• einen gemeinsamen Speicher für Identitätsdaten, der biografische und biometrische Daten von Drittstaatsangehörigen aus mehreren EU-Informationssystemen enthalten würde,</li> <li>• einen Detektor für Mehrfachidentitäten, mit dem sich nachprüfen lässt, ob die abgefragten biografischen Identitätsdaten auch in anderen angeschlossenen Systemen vorhanden sind, um Mehrfachidentitäten aufzudecken, die mit ein und demselben Satz biometrischer Daten verknüpft sind.</li> </ul>	

32.	<b>Vorschlag einer E-Evidence-Verordnung</b> (COM (2018) 225 final)	Grenzübergreifender Direktzugriff der Sicherheitsbehörden auf bei Providern im Ausland gespeicherte Daten unter Umgehung der rechtsstaatlichen Rechtshilfavorschriften.	
33.	<b>Planung des Antrags auf Vollmitgliedschaft des Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)</b>	Insbesondere Übermittlungen und Weiterübermittlungen personenbezogener Daten aus/in EU-Mitgliedstaaten, Schengen-assozierten und nicht Schengen-assozierten Staaten, Drittstaaten, Internationalen Organisationen und an NGOs. Die Drittstaaten sind größtenteils solche mit problematischer Menschenrechtslage	
34.	<b>EU-Verordnung zur Verhinderung der Verbreitung von terroristischen Online-Inhalten (TCO) politisch ausverhandelt</b>	- terroristische Inhalte im Internet auf behördliche Anordnung von den Internet-Unternehmen innerhalb einer Stunde zu löschen- Möglichkeit der Verpflichtung von Unternehmen zur Ergreifung von Maßnahmen, um die Verbreitung terroristischer Inhalte im Netz zu verhindern. Über die Wahl der Maßnahmen entscheiden die Unternehmen. Mit der Verordnung werden nationale Behörden ermächtigt, die Löschung terroristischer Inhalte anzuordnen, unabhängig vom Sitz des Unternehmens in der EU. Die Behörden des Staates, in dem das Unternehmen seinen Sitz hat, werden hierbei einbezogen.	
35.	<b>Erste unabhängige Staatsanwaltschaft der EU</b>	<p>Mit Errichtung der Europäischen Staatsanwaltschaft wird erstmals eine unabhängige und dezentrale Staatsanwaltschaft der Europäischen Union geschaffen. Ziel ist die Bekämpfung von Straftaten zum Nachteil der finanziellen Interessen der EU in den Mitgliedstaaten. Zu solchen Straftaten gegen den Finanzhaushalt der Europäischen Union gehören zum Beispiel Fälle von Subventionsbetrug, Korruption oder grenzüberschreitender Mehrwertsteuerbetrug.</p> <p>Die Europäische Staatsanwaltschaft wird die Ermittlungen und Strafverfolgungsmaßnahmen in den teilnehmenden EU-Ländern als zentrale Behörde beaufsichtigen und koordinieren, um einen einheitlichen Ansatz zu gewährleisten.</p> <p>“COUNCIL REGULATION (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor’s Office (‘the EPPO’)”</p>	