Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Präsident des Deutschen Bundestages
– Parlamentssekretariat –
Reichstagsgebäude
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1117
FAX +49 (0)30 18 681-1019

INTERNET www.bmi.bund.de

DATUM 12. Juli 2011

BETREFF **Kleine Anfrage der Abgeordneten Ulla Jelpke u. a. und der Fraktion DIE LINKE.**
Nutzung Sozialer Netzwerke zu Fahndungszwecken
BT-Drucksache 17/6100

Auf die Kleine Anfrage übersende ich namens der Bundesregierung die beigefügte Antwort in 5-facher Ausfertigung.

Mit freundlichen Grüßen
in Vertretung

Dr. Christoph Bergner

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
VERKEHRSANBINDUNG S-Bahnhof Bellevue; U-Bahnhof Turmstraße
Bushaltestelle Kleiner Tiergarten

Kleine Anfrage der Abgeordneten Ulla Jelpke u. a. und der Fraktion DIE LINKE.

Nutzung Sozialer Netzwerke zu Fahndungszwecken

BT-Drucksache 17/6100

Vorbemerkung der Fragesteller:

Soziale Netzwerke im Internet wie Facebook, LinkedIn, MySpace, Twitter oder Studi VZ werden von Millionen Menschen genutzt. Von großem Interesse sind solche Netzwerke auch für Polizeibehörden, um etwa die Identität unbekannter tatverdächtiger Personen ausfindig zu machen oder das personelle Umfeld eines Verdächtigen zu erkunden.

In einem Aufsatz der Zeitschrift „Kriminalistik" (1/2010, S.30) nennen die Polizeidozenten Axel Henrichs und Jörg Wilhelm Soziale Netzwerke „wahre Fundgruben" für „allgemeine Ermittlungs- und Fahndungszwecke" ebenso wie für „präventionspolizeiliche Maßnahmen". Die Daten aus Sozialen Netzwerken seien von „hohem taktischen Nutzen".

In eine ähnliche Richtung hatte sich 2008 die von Wolfgang Schäuble inittierte „Zukunftsgruppe" einiger EU-Innenminister geäußert, die von einem „digitalen Tsunami" gesprochen hatte und hiermit keine Katastrophe meinte, sondern „gewaltige Informationsmengen", die sich Polizeien zukünftig zunutze machen sollten.

Am erfolgreichsten könnten laut „Kriminalistik" Recherchen sein, wenn „virtuelle Ermittler" zum Einsatz kommen. In einem im Frühjahr 2010 im Bundesinnenministerium erarbeiteten „Konzept zur Bekämpfung linker Gewalttaten" wird der Einsatz „virtueller Agenten" vorgeschlagen. Beamte könnten sich durch den Aufbau von Blogs in das linke Milieu einschleusen, Diskussionen anregen und Kontakte knüpfen. (http://www.spiegel.de/spiegel/print/d-70500966.html)

Der Vorsitzende des Bundes Deutscher Kriminalbeamter (BDK) Klaus Jansen forderte im Herbst 2010 „gesetzliche Befugnisse für offene und verdeckte Ermittlungen im Internet, speziell in Sozialen Netzwerken".

Auch der Bundesbeauftragte für Datenschutz hält es in seinem 23. Tätigkeitsbericht für die Jahre 2009 und 2010 aufgrund einer „Rechtsunsicherheit, in welchem Stadium der polizeilichen Recherchen im Internet von einem Eingriff in Grundrechte auszugehen ist", für geboten, „Inhalt und Grenzen derartiger Befugnisse spezialgesetzlich zu regeln". (Bundestagsdrucksache 17/5200, S.86)

Der Wert der erlangten Informationen könnte laut dem Artikel in der „Kriminalistik" insbesondere dann erhöht werden, wenn sie mit Informationen der Polizeidatenbanken und verdeckten Ermittlungen kombiniert würden. Hierfür fehlt allerdings die rechtliche Grundlage.

Untersuchungen haben ergeben, dass Beziehungen unter Personen, Sachverhalten und Dingen ein hoher Informationsgehalt innewohnt, der demnach sogar höher liegt als abgehörte Telefongespräche. Ein Beziehungsnetz einer Gruppe kann rekonstruiert werden, wenn nur 8% ihrer Beteiligten überwacht werden. Die Beispiele zeigen sowohl die hohe Relevanz polizeilicher Durchdringung sozialer Netzwerke wie auch die Notwendigkeit der öffentlichen Aufklärung über neue Ermittlungsmethoden. Insbesondere muss ausgeschlossen werden, dass Verfolgungsbehörden ein sogenanntes „Data Mining" betreiben, indem Daten sozialer Netzwerke mit anderen Datensätzen („Open Intelligence" oder Polizeidatenbanken) verknüpft werden. Durch dieses illegale Profiling würde sich der Informationsgehalt der fraglichen Daten beträchtlich erhöhen.

1. Welche Bedeutung misst die Bundesregierung Ermittlungen in Sozialen Netzwerken zur Kriminalitätsprävention- und kriminalpolizeilichen Ermittlungen bei?

Zu 1.
Ermittlungen in sozialen Netzwerken können im Rahmen der Gefahrenabwehr und Strafverfolgung von Bedeutung sein, denn auch Straftäter nutzen diese Plattformen für die Begehung von Straftaten und diesbezügliche Kommunikation.

2. Welche Abteilungen bei Polizeien und Geheimdiensten des Bundes befassen sich mit Ermittlungen in Sozialen Netzwerken?
a. Wie viele Mitarbeiter sind hierzu mit welchem Aufgabenbereich beschäftigt?
b. In welchen Bund-Länder-Arbeitsgruppen oder Kooperationen auch mit privaten Firmen, die sich unter anderem mit Ermittlungen in Sozialen Netzwerken wie auch verdeckten virtuellen Ermittlungen befassen, sind welche Behörden des Bundes eingebunden?

Zu 2.
Das Bundeskriminalamt (BKA), die Bundespolizei (BPOL) und der Zollfahndungsdienst nutzen bei der Kriminalitätsbekämpfung fallbezogen u. a. offen zugängliche Informationen aus sozialen Netzwerken. Es wird keine systematische und anlassunabhängige Recherche in sozialen Netzwerken durchgeführt.
BKA, BPOL und Zollfahndungsdienst verfügen über keine spezifischen Organisationseinheiten, die die Aufgabe haben, in sozialen Netzwerken zu ermitteln. Soweit Ermitt-

lungen in sozialen Netzwerken erforderlich sind, erfolgen diese nur im Einzelfall von den auch sonst mit Ermittlungen betrauten Organisationseinheiten.

Die Nachrichtendienste sind hingegen keine Ermittlungsbehörden. Mit Ermittlungen sind daher weder Mitarbeiter betraut, noch bestehen diesbezügliche Kooperationen.

a)
Da eine Recherche offen zugänglicher Informationen in sozialen Netzwerken nur anlassbezogen stattfindet, kann keine valide Berechnung der Personalbindung erfolgen. Spezielle Ermittlungs- und Fahndungseinheiten werden für diesen Zweck nicht vorgehalten.

b)
Die Thematik „Soziale Netzwerke" wurde bereits in nationalen polizeilichen Gremien behandelt. Sowohl die AG Kripo als auch der Arbeitskreis Innere Sicherheit (AK II) der Ständigen Konferenz der Innenminister und -senatoren der Länder befassten sich im Jahre 2009 insbesondere mit den Risiken und Gefahren im Zusammenhang mit Aktivitäten von Beschäftigten der Polizei in „sozialen Netzwerken". Die Kommission Kriminalitätsbekämpfung (KKB) der AG Kripo thematisiert seit 2010 die Möglichkeiten polizeilicher Recherchen in sozialen Netzwerken.
Neue Erkenntnisse und Entwicklungen in Sozialen Netzwerken werden außerdem in der AG KaRIN, bestehend aus BKA, Zollkriminalamt und 7 Landeskriminalämtern, in regelmäßigen Arbeitstagungen (mindestens zweimal pro Jahr) oder über einen elektronischen Verteiler ausgetauscht.
Polizeibehörden des Bundes unterhalten keine Kooperation mit privaten Firmen im Hinblick auf Ermittlungen in sozialen Netzwerken.

3. Inwieweit ist es Beamtinnen und Beamten des BKA nach geltender Gesetzeslage erlaubt, als „virtuelle Ermittler" in Sozialen Netzwerken zu agieren (bitte Rechtsgrundlage benennen) und welche Einschränkungen existieren hierzu?
a. In welchen Fällen werden Ausgeforschte im Nachhinein von einer verdeckten polizeilichen Maßnahme in Kenntnis gesetzt bzw. aus welchen Gründen unterbleibt eine derartige Unterrichtung?
b. Ist die Bundesregierung in der Lage, eine Statistik oder wenigstens eine Näherung zu liefern, wie oft digital Ausgeforschte in den letzten fünf Jahren unterrichtet bzw. nicht unterrichtet wurden?
c. Wie bewertet die Bundesregierung die vom Bundesbeauftragten für Datenschutz im Tätigkeitsbericht Nr. 23 geäußerten „Zweifel, inwieweit die vom BKA angeführten Rechtsnormen den Eingriff in das informationelle Selbstbestimmungsrecht bei Ermittlungen in sozialen Netzwerken legitimieren können"?

Zu 3.

Das BKA kann, lediglich gestützt auf seine Aufgabenzuweisung, personenbezogene Daten aus offenen Quellen im Internet oder durch Beobachtung eines offenen Chats erheben, solange damit kein Eingriff in Grundrechte verbunden ist. Keinen Eingriff in Grundrechte stellt es nach der Rechtsprechung des Bundesverfassungsgerichts regelmäßig dar, wenn Beamte des BKA unter einer Legende an offener Kommunikation in sozialen Netzwerken teilnehmen, solange der Betroffene nicht schutzwürdig in die Identität des Kommunikationspartners vertraut (vgl. BVerfGE 120, 274, 346).

Trägt das BKA gezielt personenbezogene Daten zu polizeilichen Zwecken zusammen und wertet diese aus oder gleicht sie mit sonstigen Daten ab, so greift dies in das Recht auf informationelle Selbstbestimmung des Betroffenen ein und bedarf einer Rechtsgrundlage (vgl. BVerfGE 120, 274, 346). Das BKA verfügt über entsprechende Befugnisse in § 7 Absatz 2 des Bundeskriminalamtgesetzes (BKAG) zur Wahrnehmung der Aufgaben als Zentralstelle, in §§ 161, 163 der Strafprozessordnung (StPO) beim Tätigwerden als Ermittlungsbehörde im Strafverfahren und in § 20b des BKAG zur Abwehr von Gefahren des internationalen Terrorismus. Dieselben Rechtsgrundlagen sind maßgeblich, wenn Beamte des BKA unter einer Legende an Kommunikation in sozialen Netzwerken teilnehmen und der Betroffene auf die Identität des Kommunikationspartners vertraut. Bei der Beurteilung des Vertrauens des Betroffenen sind die äußeren Umstände maßgeblich, etwa, ob es sich um ein soziales Netzwerk handelt, in dem eine Anmeldung unter Pseudonym technisch problemlos möglich ist und von einer Vielzahl an Nutzern praktiziert wird.
Nehmen Beamte des BKA legendiert an einer Kommunikation in einer geschlossenen Benutzergruppe in einem sozialen Netzwerk teil und nutzen sie dabei Zugangsschlüssel, die sie ohne Zustimmung eines anderen Kommunikationsteilnehmers erhoben haben, kann dies nur unter den Voraussetzungen der §§ 100a, 100b, 110a ff. der StPO bzw. §§ 20l, 20g Absatz 2 Nummer 5 des BKAG zulässig sein.

a)

Der Einsatz von Maßnahmen der Telekommunikationsüberwachung oder von verdeckten Ermittlern bedarf der nachträglichen Benachrichtigung des Betroffenen gemäß § 20w Absatz 1 Satz 1 Nummer 2, Nummer 7 des BKAG, §§ 101 Absatz 4 Satz 1 Nummer 3, Nummer 9 der StPO. Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, sowie ohne Gefährdung der Möglichkeit einer weiteren Verwendung des verdeckten Ermittlers möglich ist (vgl. § 101 Absatz 5 Satz 1 der StPO, § 20w Absatz 2 Satz 1 des BKAG). In den übrigen Fällen ist eine Benachrichtigung über die Maßnahme gesetzlich nicht vorgesehen. Beschuldigte in einem Strafverfahren erfahren

auch durch Wahrnehmung des Akteneinsichtsrechts durch den Verteidiger von den durchgeführten Maßnahmen der Datenerhebung.

b)
Nein. Eine Statistikpflicht existiert für die Datenerhebung in sozialen Netzwerken nicht.

c)
Die Bundesregierung teilt die Zweifel des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nicht. Zur Frage, wann polizeiliche Recherchen im Internet in das Grundrecht auf informationelle Selbstbestimmung eingreifen, hat sich das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung ausführlich geäußert (BVerfGE, 120, 274, 344-346).

4. Sieht die Bundesregierung die Notwendigkeit, besondere gesetzliche Befugnisse für offene und verdeckte Ermittlungen in Sozialen Netzwerken zu schaffen?
a. Wenn ja, welchen Handlungsbedarf sieht die Bundesregierung?
b. Wenn nein, aufgrund welcher gesetzlichen Grundlage sind offene und verdeckte Ermittlungen in Sozialen Netzwerken zulässig?
c. Wie bewertet die Bundesregierung die vom Bundesbeauftragten für Datenschutz im Tätigkeitsbericht Nr. 23 empfundene „Rechtsunsicherheit, in welchem Stadium der polizeilichen Recherchen im Internet von einem Eingriff in Grundrechte auszugehen ist"?

Zu 4.
Die Bundesregierung sieht derzeit keine Notwendigkeit, besondere gesetzliche Befugnisse für öffentlich zugängliche Quellen zu schaffen. Die Beantwortung der Frage 4 a) entfällt daher.

b)
Es wird auf die Antwort zu Frage 3 verwiesen. Weitere Rechtsgrundlagen zur Datenerhebung finden sich in den Fachgesetzen der jeweiligen Behörden.

c)
Die vom BfDI ausweislich seines 23. Tätigkeitsberichts empfundene Rechtsunsicherheit bezieht sich auf die Frage, in welchem Stadium der polizeilichen Internet-Recherche das schutzwürdige Vertrauen des Betroffenen in die Identität seines Kommunikationspartners ausgenutzt wird. Das schutzwürdige Vertrauen in die Identität des Kommunikationspartners markiert den Wechsel von der reinen Internetaufklärung, die keinen Grundrechtseingriff darstellt, hin zu einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung, der einer gesetzlichen Grundlage bedarf. Die in der Antwort zu Frage 3 angegebenen Rechtsgrundlagen setzen den Verdacht einer Straftat bzw. die Erfor-

derlichkeit zur Aufgabenerfüllung voraus. Im Übrigen wird auf die Antwort zu Frage 3c verwiesen.

5. Inwieweit nutzt das Bundeskriminalamt bereits Soziale Netzwerke zu Ermittlungszwecken?
a. In wie vielen Fällen waren Ermittlungen in Sozialen Netzwerken ausschlaggebend bei der Aufklärung von Straftaten? (bitte nach Jahren und Art bzw. Phänomenbereich der Straftaten aufschlüsseln)
b. In wie vielen Fällen waren Ermittlungen in Sozialen Netzwerken ausschlaggebend bei der Verbrechensprävention? (bitte nach Jahren und Art bzw. Phänomenbereich der Straftaten aufschlüsseln)

Zu 5.
Eine Recherche in sozialen Netzwerken dient dem Erkenntnisgewinn über Beschuldigte in den beim BKA geführten Ermittlungsverfahren unter Sachleitungsbefugnis der Staatsanwaltschaft. Werden in diesem Rahmen Benutzerkonten zu Beschuldigten in sozialen Netzwerken festgestellt, können in einem zweiten Schritt die Echtpersonalien über die Provider (z. B. facebook, Studi-VZ, WKW) erhoben werden.
Im Bereich der Internationalen Fahndung/Rechtshilfe erfolgen Abfragen bei (Personen-) Suchmaschinen. Im Bereich der Gefährdungsermittlungen im Personenschutz werden anlassbezogen frei zugängliche, personenbezogene Informationen aus sozialen Netzwerken zur Verdichtung bereits vorhandener Erkenntnisse genutzt.

a)
Die Ermittlungen in sozialen Netzwerken dienen lediglich als zusätzliche Erkenntnisquellen. Es ist kein Fall bekannt, in dem ausschließlich die Ermittlungen in diesen Netzwerken für die Aufklärung maßgeblich waren.

b)
Es wird auf die Antwort zu Frage 5 a) verwiesen.

6. In wie vielen und welchen Fällen sind „virtuelle Ermittler" des BKA bereits zum Einsatz gekommen?
a. Dürfen „virtuelle Ermittler" zu Straftaten aufrufen, Texte mit strafbaren Inhalt verfassen oder Dateien mit strafbarem Inhalt weitergeben?
b. Kann die Bundesregierung mit Sicherheit ausschließen, dass „virtuelle Ermittler" in der Vergangenheit jemals zu Straftaten aufgerufen oder Texte mit strafbarem Inhalt verfasst oder Dateien mit strafbarem Inhalt weitergegeben haben?
c. Legen „virtuelle Ermittler" sogenannte „Honigtöpfe" aus, wie es etwa bei Ermittlungen des BKA gegen die „militante gruppe" mit dem Protokollieren von Zugriffen auf der BKA-Webseite als illegale Praxis offenkundig wurde?
d. In welchen und wie vielen Fällen haben „virtuelle Ermittler" selbst Webseiten oder Blogs angelegt? In welchen und wie vielen Fällen haben „virtuelle Ermittler" unter falschen Identitäten Profile in Sozialen Netzwerken angelegt?
e. Inwieweit wurden entsprechend den Überlegungen des „Konzepts zur Bekämpfung linker Gewalttaten" bereits „virtuelle Agenten" der Sicherheitsbehörden in das linke Online-Milieu eingeschleust?

Zu 6.
Das BKA setzt für eine längerfristige, gezielte Teilnahme an der Kommunikation in sozialen Netzwerken nach Anordnung der Staatsanwaltschaft sogenannte „virtuelle" Verdeckte Ermittler ein. Die Einsätze finden auf der Rechtsgrundlage und nach Maßgabe der §§ 110a ff. der StPO statt.
Im Rahmen der Strafverfolgung wurden innerhalb der zurückliegenden 24 Monate in sechs Ermittlungsverfahren „virtuelle" Verdeckte Ermittler durch das BKA eingesetzt.

a)
§§ 110a ff. der StPO enthalten keine Befugnis zur Begehung milieubedingter Straftaten. Damit kommen die in Frage 6 a) genannten Handlungsweisen für „virtuelle" Verdeckte Ermittler regelmäßig nicht in Betracht, ausnahmsweise dann, wenn sie nach den allgemeinen Regelungen rechtmäßig sind.

b)
Die Preisgabe von Informationen zu konkreten verdeckten Einsätzen bei der Verfolgung von Straftaten im Internet an die Öffentlichkeit würde das schützenswerte Interesse der Bundesrepublik Deutschland an einer wirksamen Bekämpfung der gewerbs- oder gewohnheitsmäßigen, organisierten oder schweren Kriminalität und damit das Staatswohl erheblich beeinträchtigen. Die Veröffentlichung dieser internen Vorgänge würde die Offenlegung sensibler polizeilicher Vorgehensweisen und Taktiken bedeuten. Die Frage tangiert polizeitaktische Maßnahmen, die als ultima ratio im Einzelfall in Kriminalitätsfeldern angewandt werden, bei denen von einem besonderen Maß an Konspiration ausge-

gangen werden muss. Die Kenntnisnahme von Informationen aus dem angeforderten Bereich durch kriminelle Kreise würde sich auf die polizeiliche Aufgabenwahrnehmung außerordentlich nachteilig auswirken. Nach sorgfältiger Abwägung mit den Informationsrechten des Deutschen Bundestages und seiner Abgeordneten kann in der Sache daher keine Auskunft in der für Kleine Anfragen nach § 104 i.V.m. § 75 Absatz 3, 76 Absatz 1 der Geschäftsordnung des Deutschen Bundestages (GO BT) vorgesehenen, zur Veröffentlichung in einer Bundestagsdrucksache bestimmten Weise erfolgen. Die Antwort der Bundesregierung auf diese Frage ist daher als „Verschlusssache - Vertraulich" eingestuft werden und kann bei der Geheimschutzstelle des Deutschen Bundestages eingesehen werden.

c)
Nein.

d)
Auf die Antwort zu Frage 6 b wird verwiesen.

e)
Auf die Antwort zu Frage 6 b wird verwiesen.

7. An welchen Kooperationen im Bereich Forschung und Entwicklung von Software zur Analyse nicht frei zugänglicher Informationen im Internet (social networks, geschlossen Foren, etc.) auf EU-Ebene sind Stellen des Bundes beteiligt, und mit welchen Partnern? Welchen finanziellen Umfang haben diese Kooperationen, und wie sind die einzelnen Partner daran beteiligt?

Zu 7.
BKA, BPOL und Zollfahndungsdienst unterhalten keine entsprechenden Kooperationen auf EU-Ebene.

8. In wie vielen und welchen Fällen hat sich das BKA von Anbietern Sozialer Netzwerke Zugang zu nicht-öffentlichen Profilen bzw. Nachrichten geben lassen?

Zu 8.
Das BKA hat in insgesamt vier Fällen zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person (Suizidankündigung, Morddrohungen sowie Erpressung/Androhung einer Sprengstoffexplosion) Bestands- und Inhaltsdaten erhoben und an die sachbearbeitenden Dienststellen der Bundesländer weitergeleitet.

9. Teilt die Bundesregierung die Ansicht der Fragesteller, dass eine per Software vorgenommene Verknüpfung der in Sozialen Netzwerken aufgespürter Beziehungen unter Personen und Ereignissen mit Informationen aus Polizeidatenbanken und verdeckten Ermittlungen ein unzulässiges Profiling darstellt?

Zu 9.

Die von den Fragestellern beschriebene Verfahrensweise einer automatisierten Verknüpfung mittels spezieller Software findet bei Bundesbehörden keine Anwendung. Zu der Funktionsweise von Software zur Verknüpfung der in sozialen Netzwerken aufgespürten Beziehungen unter Personen und Ereignissen mit Informationen aus Polizeidatenbanken und verdeckten Ermittlungen liegen der Bundesregierung keine Erkenntnisse vor.

10. Wie ist ein „Data Mining" bzw. die Verknüpfung von im Internet ermittelten Informationen mit anderen Datensätzen geregelt?
a. Welche Bestimmungen existieren für Polizeien und Geheimdienste des Bundes zum Erstellen eines Personenprofils anhand im Internet ermittelter Informationen bzw. mit einer Verknüpfung anderer Datensätze?
b. Welche Unterschiede machen entsprechende Bestimmungen hinsichtlich unterschiedlicher Kriminalitätsphänomene sowie bezüglich Strafverfolgung und Gefahrenabwehr?
c. Welche Rolle spielt die Einbindung von Geodaten und welche Bestimmungen existieren hierzu?
d. Wie oft hat das BKA in den letzten fünf Jahren Ermittlungen geführt, in die Geodaten aus Sozialen Netzwerken eingeflossen sind?
e. Welche weiteren Datensätze können unter technischen Gesichtspunkten eingebunden werden?

Zu 10.

Das in der Fragestellung genannte „Data Mining" findet im BKA und bei der BPOL nicht statt. Auch für Recherchen durch den Zollfahndungsdienst werden keine automatisierten Tools genutzt. Es gibt keinen automatisierten Abgleich mit Fahndungsdatenbanken. Die Nutzung und Verwendung von erhobenen Daten durch Polizeibehörden des Bundes im Übrigen richtet sich nach den jeweils einschlägigen gesetzlichen Vorschriften.
Für "Data Mining" bzw. die Verknüpfung von im Internet ermittelten Informationen mit anderen Datensätzen durch Nachrichtendienste gelten die allgemeinen datenschutzrechtlichen Vorgaben, die für die Nachrichtendienste zum Teil durch die entsprechenden Fachgesetze wie z. B. das Gesetz über den Bundesnachrichtendienst modifiziert werden, das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) sowie weitere rechtliche Vorgaben wie beispielsweise das Straf- oder

das Urheberrecht. Behördenabhängig sind darüber hinaus Arbeitsanweisungen zu beachten.

a)
Auf die Antwort zu Frage 10 wird verwiesen.

b)
Unterschiedliche Kriminalitätsphänomene haben keine Auswirkungen auf die Rechtmäßigkeit einer polizeilichen Maßnahme. Die Zweckrichtung der polizeilichen Maßnahme (Strafverfolgung oder Gefahrenabwehr) ist entscheidend für die anzuwendende Ermächtigungsgrundlage. Insoweit wird auf die Beantwortung zu Frage 10 verwiesen.

c)
Die Polizeibehörden und Nachrichtendienste des Bundes nutzen personenbezogene Geodaten bzw. Standortdaten, sofern dies im Einzelfall im Rahmen ihrer jeweiligen Aufgabenerfüllung erforderlich ist. Es gelten die eingangs genannten rechtlichen Vorgaben.

d)
Die von den Fragestellern erbetene Auswertung sämtlicher Ermittlungsverfahren aus den letzten fünf Jahren ist nicht möglich, da zur Verwendung von Standortdaten aus sozialen Netzwerken keine Statistiken geführt werden.

e)
Grundsätzlich sind aus technischer Sicht Verknüpfungen denkbar und möglich, wenn entsprechende Verknüpfungskriterien existieren.

11. Kommt beim BKA spezielle Software zu Online-Ermittlungen oder zur präventiven Aufhellung von deliktspezifischen Milieus bzw. Netzwerken zur Anwendung und wenn ja, welche?
a. Welche Software zu Online-Ermittlungen oder Data Mining haben Bundesbehörden in den letzten zwei Jahren getestet?
b. Haben Bundesbehörden Software der Firmen rola Security, HBGary, In-Q-Tel, IBM (insbesondere „Criminal Reduction Utilising Statistical History") oder TEMIS (auch zu Testzwecken) beschafft und falls ja, wofür wurden diese eingesetzt?

Zu 11.

Das BKA nutzt für seine Internetrecherchen herkömmliche Recherchetools (z. B. im Internet allgemein verwendete Suchmaschinen).

a)

Spezielle Software wird im BKA nicht eingesetzt. Ein „Data Mining" im Sinne der Fragestellung (Recherche im Internet) findet im BKA nicht statt.

b)

Das BKA nutzt zur Auswertung und Analyse von sichergestellten, großen Datenmengen Anwendungen der Hersteller rola Security und - gegenwärtig zu Testzwecken - IBM. Mit Hilfe dieser Software werden einzelfallabhängig unterschiedliche kriminalistische Fragestellungen bearbeitet.

12. Welche Aus- und Fortbildungsangebote setzen Bundesbehörden für „virtuelle Ermittlungen" ein?
a. Welche Bundesbehörden haben hierzu eigene Module entwickelt und welchen konkreten Inhalt haben diese?
b. In welchen EU-weiten oder internationalen Institutionen oder Projekten (auch Interpol oder CEPOL) werden Angehörige deutscher Behörden in „virtuellen Ermittlungen" unterrichtet?

Zu 12.

Für die in der Frage genannten „virtuellen Ermittlungen" bestehen im BKA, bei der BPOL und im Zollfahndungsdienst keine eigenen Fortbildungsveranstaltungen.
Die Europäische Polizeiakademie CEPOL und die Mitteleuropäische Polizeiakademie MEPA bieten Seminare zum Bereich Cybercrime und IuK-Kriminalität an, die auch Ermittlungen im Internet zum Gegenstand haben. Bei den Seminaren von CEPOL steht der deutschen Polizei in der Regel ein Teilnehmerplatz zur Verfügung.
Nachrichtendienste des Bundes nutzen Aus- und Fortbildungsangebote im Bereich der Internetrecherche an der Schule für Verfassungsschutz.

13. An welchen Kooperationen im Bereich Forschung und Entwicklung von Software zur Analyse nicht frei zugänglicher Informationen im Internet (social networks, geschlossen Foren, etc.) auf EU-Ebene sind Stellen des Bundes beteiligt, und mit welchen Partnern? Welchen finanziellen Umfang haben diese Kooperationen, und wie sind die einzelnen Partner daran beteiligt?

Zu 13.

Stellen des Bundes sind an Kooperationen im Sinne der Fragestellung nicht beteiligt. Im Übrigen wird auf die Beantwortung der Frage 7 verwiesen.

14. In welchen Arbeitsgruppen, privaten oder öffentlichen Institutionen sind Stellen des Bundes bezüglich „virtueller Ermittlungen" innerhalb der EU und international beteiligt oder beziehen dort ermittelte Ergebnisse, wie es etwa heise online bereits am 19.11.2008 über Interpol berichtete? Sind der Bundesregierung Aktivitäten des US-Militärs bekannt, mittels maschinell angelegter falscher Identitäten (sogenannte „sock puppets") gefälschte Mehrheitsmeinungen im Internet vorzuspiegeln (Guardian 17.3.2011) und falls ja, welche Stellen des Bundes forschen hierzu bzw. haben sich mit Ergebnissen anderer Forschungen befasst?

Zu 14.

Das Thema Soziale Netzwerke wurde in der Sitzung der EU-Ratsarbeitsgruppe "Strafverfolgung" (Law Enforcement Working Party - LEWP) am 13.05.2011 angesprochen. Die ungarische Ratspräsidentschaft stellte einen „Vorschlag zu Leitlinien für die Nutzung ‚sozialer Netzwerke' durch Strafverfolgungsbehörden und ihre Mitarbeiter vor. Für weitere Einzelheiten wird auf den Bericht der Bundesregierung zu dieser Sitzung verwiesen, der dem Bundestag vorliegt.

Zu den von den Fragestellern benannten angeblichen Aktivitäten des US-Militärs liegen der Bundesregierung keine Erkenntnisse vor.