DIGITALE | GESELLSCHAFT

Digitale Gesellschaft, CH-4000 Basel

Staatspolitische Kommission
3003 Bern

per E-Mail an: spk.cip@parl.admin.ch

4. Juni 2020

Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.)

Sehr geehrter Herr Nationalrat Glarner, sehr geehrte Damen und Herren

Am 11. Februar 2020 hat die Staatspolitische Kommission des Nationalrates (SPK) das Vernehmlassungsverfahren zur Mitwirkungspflicht im Asylverfahren (Überprüfungsmöglichkeit bei Mobiltelefonen; (17.423n Pa.Iv.)) eröffnet.

Die Digitale Gesellschaft ist eine gemeinnützige Organisation, die sich für Grund- und Menschenrechte, eine offene Wissenskultur sowie weitreichende Transparenz und Beteiligungsmöglichkeiten an gesellschaftlichen Entscheidungsprozessen einsetzt. Die Tätigkeit orientiert sich an den Bedürfnissen der Bürgerinnen und Konsumenten in der Schweiz und international. Das Ziel ist die Erhaltung und die Förderung einer freien, offenen und nachhaltigen Gesellschaft vor dem Hintergrund der Persönlichkeits- und Menschenrechte.

Wir bedanken uns für diese Möglichkeit zur Meinungsäusserung und möchten wie folgt Stellung beziehen.

Die Digitale Gesellschaft lehnt die Vorlage der Staatspolitischen Kommission des Nationalrates (SPK-N) zur Änderung des Asylgesetzes und des Ausländer- und Integrationsgesetzes zur Ergänzung der Mitwirkungspflicht und Überprüfungsmöglichkeit von elektronischen Datenträgern ab. Sie stellt einen schweren Eingriff in das Grundrecht auf Schutz der Privatsphäre dar. Aus Sicht der Digitalen Gesellschaft sind die Voraussetzungen für einen solchen Grundrechtseingriff nicht erfüllt (Art. 36 BV: gesetzliche Grundlage, Verhältnismässigkeit, Schutz des Kerngehalts).

Die SPK-N begründet die Einführung einer entsprechenden Rechtsgrundlage in der Schweiz unter anderem damit, dass andere europäische Länder ebenfalls entsprechende Regelungen kennen. Im erläuternden Bericht stellt sie die Praxis in den betreffenden Ländern jedoch nur sehr knapp und einseitig dar. In keiner Weise werden die kontroversen Diskussionen, die problematischen Aspekte und der äusserst beschränkte Nutzen erwähnt. Tatsächlich zeigen aber die nicht erwähnten Erfahrungen in Deutschland und anderen europäischen Ländern, die in den letzten Jahren ähnliche Regelungen eingeführt haben, wie komplex die Thematik ist. Sie machen deutlich, welche zahlreichen, noch ungeklärten Fragen und Probleme sich stellen bei fundamentalen Grundsätzen wie Rechtsstaatlichkeit, Grundrecht auf Schutz der Privatsphäre, Verhältnismässigkeit und Datenschutz. Die Erfahrungen insbesondere aus Deutschland dokumentieren, dass solche Massnahmen sehr hohe Kosten generieren, jedoch nur ein kleiner Teil der Auswertungen zu einem nennenswerten Nutzen führt. Von einer «effizienten Methode», von der die SPK-N in ihrem erläuternden Bericht spricht, kann somit keine Rede sein. Die Erfahrungswerte des Auslandes rechtfertigen aus Sicht der Digitalen Gesellschaft auch nicht die optimistische Haltung der SPK-N. Vielmehr müssen sie als Warnung angesehen werden, mit welchen Risiken die Einführung solch weitgehender Massnahmen verbunden ist.

Aus Sicht der Digitalen Gesellschaft darf keine entsprechende Rechtsgrundlage eingeführt werden, weil sie nicht mit den rechtsstaatlichen und grundrechtlichen Garantien vereinbar ist. Eine hinreichende Risiko- und Folgenabschätzung wurde augenscheinlich nicht vorgenommen. Für den geplanten schweren Grundrechtseingriff wären indes detaillierte, vertiefte Abklärungen und Erläuterungen zwingend, um überzeugend darlegen zu können, wie den verschiedenen Problemen und Fragen hinsichtlich Rechtsstaatlichkeit, Grundrecht auf Schutz der Privatsphäre, Verhältnismässigkeit und Datenschutz tatsächlich Rechnung getragen werden muss. Solche Ausführungen fehlen jedoch in der Vernehmlassungsvorlage.

Wir bedanken uns für die Berücksichtigung unserer Anmerkungen und Vorschläge.

Mit freundlichen Grüssen

Erik Schönenberger
Geschäftsleiter

Das Wichtigste in Kürze

Die Digitale Gesellschaft lehnt die Vorlage der SPK-N zur Änderung des Asylgesetzes und des Ausländer- und Integrationsgesetzes zur Ergänzung der Mitwirkungspflicht und Überprüfungsmöglichkeit von elektronischen Datenträgern ab. Die Massnahme stellt einen schweren Eingriff in das Grundrecht auf Privatsphäre (Art. 13 BV, Art. 8 Ziff. 1 EMRK) dar, und die Voraussetzungen für einen solchen Eingriff sind nicht erfüllt:

- Die **gesetzliche Grundlage** ist unzureichend: Schwerwiegende Einschränkungen von Grundrechten erfordern ein Gesetz im formellen Sinn als Grundlage (Art. 36 Abs. 1 BV). Gemäss Vorentwurf sollen zentrale Aspekte, wie Triage der für die Identitätsabklärung relevanten Daten, Definition, welche Daten erhoben werden, Regelung des Zugriffs, jedoch erst auf Verordnungsstufe geregelt werden. Zudem ist die Grundlage nicht genügend bestimmt, denn sie umfasst mögliche Datenträger gemäss künftigen technischen Entwicklungen.
- **Verhältnismässigkeit**: Die Digitale Gesellschaft hält die Pflicht, von Asylsuchenden zwecks Identitätsfeststellung elektronische Datenträger auszuhändigen, für unverhältnismässig. Dasselbe gilt für das entsprechende Überprüfungsrecht des SEM.
    - Die Massnahme ist nicht erforderlich, weil der Zweck auch mit Massnahmen, die weniger stark in Grundrechte eingreifen, erreicht werden kann. Zudem fehlt im Vorentwurf der Vorbehalt der *ultima ratio*.
    - Der beschränkte Nutzen steht in keinem Verhältnis zum schweren Eingriff in die Privatsphäre.
    - Angesichts der schweren verfahrensrechtlichen Folgen einer Verletzung der Mitwirkungspflicht kann nicht von einer «freiwilligen» Herausgabe der Datenträger gesprochen werden.
- Es fehlt eine **gerichtliche Kontrolle** der Rechtmässigkeit und Verhältnismässigkeit, welche im Strafverfahren gegen Personen, die schwerer Straftaten verdächtigt werden, zwingend vorausgesetzt ist. Im Asylverfahren geht es nicht um potenzielle Straftäter, sondern um Schutzsuchende. Umso stossender ist, dass für sie nicht einmal dieselben verfahrensrechtlichen Garantien gelten sollen.
- **Datenschutz**: Im Asylverfahren sind sensible Daten betroffen. Bei allen Verfahrensschritten sind der Datenschutz der Betroffenen sowie die Verhältnismässigkeit zu wahren. Es sollen nur Regelungen eingeführt werden, die vom Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geprüft, beurteilt und gutgeheissen wurden. In anderen europäischen Ländern wurde in der Diskussion um die Einführung ähnlicher Regelungen von verschiedenen Seiten gewichtige datenschutzrechtliche Probleme angeführt.

- **Kosten**: Die vorgeschlagene Massnahme führt zu sehr hohen Kosten, welche in keinem Verhältnis zum beschränkten Nutzen stehen.
- Die Vorlage geht über den in der Parlamentarischen Initiative geforderten Zweck hinaus, indem sie den Zweck auf die Abklärung des Reisewegs ausdehnt, und die Mitwirkungspflicht auf das Wegweisungsvollzugsverfahren erweitert.

Gesetzliche Grundlage

Die geplante Gesetzesänderung stellt einen Eingriff in den Schutz der Privatsphäre dar (Art. 13 BV, Art. 8 Ziff. 1 EMRK), genauer in das Recht auf informationelle Selbstbestimmung. Dies stellt auch die SPK-N in ihrem erläuternden Bericht fest. Darin bezeichnet den Schutz der Privatsphäre als «wichtiges Grundrecht, das selbstverständlich auch im Asylverfahren gewährt werden muss». Aus Sicht der Digitalen Gesellschaft stellt die Auswertung von elektronischen Datenträgern im Asylverfahren einen **schwerwiegenden Eingriff in die Privatsphäre** dar. Gerade auf den Handys der Asylsuchenden sind eine Vielzahl persönlicher und teils höchst sensibler Daten gespeichert. Aber auch unbeteiligte Dritte würden durch die behördliche Auswertung erfasst. Mit dem Auslesen der Daten erhielten die Behörden Zugriff auf Daten von Familienmitgliedern und Unterstützern oder auf die Korrespondenz zwischen Schutzsuchenden und Anwältinnen oder Ärzten. Dies alles, ohne dass davon betroffene Dritten vorab eine persönliche Zustimmung dazu erteilt haben. Zwar dürfen Personendaten von Drittpersonen gemäss erläuterndem Bericht nicht ausgewertet werden. Angesichts der Fülle von möglichen auszuwertenden Daten, inklusive Korrespondenz, ist diese Abgrenzung in der Praxis jedoch schwierig. Im erläuternden Bericht wird nicht dargelegt, wie dies sichergestellt werden soll.

Auch das SEM bezeichnete die Massnahme anlässlich einer Medienanfrage nach der Auswertung des Pilotprojekts 2019 als «schweren Eingriff in das Grundrecht auf informationelle Selbstbestimmung». Die Gesellschaft für Freiheitsrechte in Deutschland hält in ihrer Studie zur Praxis in Deutschland fest (Seite 9): «Die Auswertung von Smartphones, in welchen sich eine Vielzahl sensibler Daten aus unterschiedlichsten Lebensbereichen bündeln, stellt unzweifelhaft einen gravierenden Grundrechtseingriff dar.»

Gemäss Art. 36 Abs. 1 BV muss ein schwerer Eingriff in das Recht auf Privatsphäre in einem **Gesetz im formellen Sinn** geregelt sein. Aus Sicht der Digitalen Gesellschaft erfüllt die Vorlage diese Anforderungen nicht. Zwar sollen die grundsätzlichen Punkte – Pflicht zur Aushändigung der Datenträger sowie Bearbeitungsrecht des SEM – im Asylgesetz geregelt werden. Mehrere zentrale Aspekte sollen hingegen erst auf Verordnungsstufe geregelt werden (Triage der für die Identitätsabklärung relevanten Daten, Definition welche Daten erhoben werden, Regelung des Zugriffs, nArt. 8a Abs.

5 AsylG). Auch die Ausführungen im erläuternden Bericht sind zu vage bezüglich der Frage, welche Daten genau erhoben werden sollen. Zudem fehlen in der Vorlage klare Informationen und konkrete Vorgaben zum Ablauf bezüglich Auslesen der Daten, Zwischenspeicherung und Auswertung. Diese relevanten Aspekte müssten aus Sicht der Digitalen Gesellschaft im Gesetz selbst enthalten sein.

Die gesetzliche Grundlage muss zudem hinreichend bestimmt sein. Die im Vorentwurf vorgeschlagene Liste von Datenträgern (nArt. 8a Abs. 2 AsylG) soll gemäss erläuterndem Bericht nicht abschliessend sein, um künftigen technischen Entwicklungen Rechnung zu tragen. Angesichts der noch völlig unbekannten Dimensionen, welche künftige technische Entwicklungen annehmen könnten, ist diese Bestimmung als gesetzliche Grundlage **zu unbestimmt**, um einen so weitgehenden Eingriff in die Privatsphäre zu erlauben. Auch in dieser Hinsicht sind die Anforderungen an die gesetzliche Grundlage nicht erfüllt.

Verhältnismässigkeit

Jede Massnahme, die in ein Grundrecht eingreift, muss geeignet und erforderlich (*ultima ratio*, keine milderen Massnahmen) sein. Zudem müssen Zweck und Wirkung des Grundrechtseingriffs im Verhältnis stehen (Verhältnismässigkeit im engeren Sinne). Aus Sicht der Digitalen Gesellschaft sind diese Voraussetzungen bei der vorgeschlagenen Pflicht von Asylsuchenden, elektronische Datenträger auszuhändigen, und dem entsprechenden Überprüfungsrecht des SEM, nicht erfüllt.

Fragliche Eignung: geringer Nutzen

Im Pilotprojekt in den Bundesasylzentren Chiasso und Vallorbe von November 2017 bis Mai 2018, bei welcher Asylsuchende auf freiwilliger Basis mobile Datenträger einreichen konnten, wurden gemäss Medienberichten aufgrund der Auswertung nur in 11 Prozent der Fälle (total wurden 565 Datenträger ausgewertet) «nützliche Hinweise» zur Identität und zur Herkunft gefunden. In 4 Prozent der Fälle fanden sich laut SEM dazu «nützliche Hinweise». Befremdend ist angesichts der Tragweite des Pilotprojekts und des grossen öffentlichen Interesses, dass weder der Schlussbericht noch die konkreten Resultate des Projekts durch das SEM publiziert wurden, sondern deren Bekanntwerden allein den Medien zu verdanken ist. Auch der erläuternde Bericht der SPK-N schafft die erforderliche Transparenz nicht. Er enthält nur sehr generelle Aussagen zum Pilotprojekt, und keine quantitativen Aussagen dazu, in wie vielen Fällen nützliche Hinweise gefunden werden konnten. Offen bleibt somit, auf welchen Daten welche Hinweise konkret beruhen, wonach deren Nützlichkeit beurteilt wird, welche Konsequenzen diese in jeweils wie vielen Fällen hatten (Bestätigung oder Widerlegung der gemachten Angaben der Asylsuchenden) und ob diese Hinweise nicht auch mit anderen, milderen Massnahmen hätten gewonnen werden können.

Kurzum: Der behauptete Nutzen der Datenauswertung kann mangels Transparenz weder überprüft werden noch ist er dadurch glaubhaft belegt.

Die Erfahrungswerte in Deutschland stützen die Zweifel am behaupteten Nutzen: Die Gesellschaft für Freiheitsrechte hält in ihrer Studie vom Dezember 2019 gestützt auf Antworten der deutschen Bundesregierung auf Anfragen von Abgeordneten fest (Seite 5): «In etwa einem Viertel der Fälle scheitern die Datenträgerauslesungen bereits technisch. Von Januar 2018 bis Juni 2019 wurden insgesamt etwa 17.000 Datenträger erfolgreich ausgelesen. Seit Beginn der Datenträgerauswertungen waren diese durchschnittlich nur in weniger als der Hälfte der Fälle brauchbar und nur in ein bis zwei Prozent der Fälle ergab sich aus der Auswertung ein Widerspruch zu gemachten Angaben. In allen übrigen Fällen bestätigte der Test das, was Asylsuchende vorgetragen hatten.»

Zudem gestand die deutsche Bundesregierung in der Antwort auf eine Kleine Anfrage ein, dass der anvisierte angebliche Nutzen empirisch schlicht nicht belegbar ist (Seite 26): «Da neben der Auswertung von Datenträgern auch viele andere Aspekte in die Bewertung einfliessen, lässt sich statistisch nicht ermitteln, in welchem Umfang die Auswertung von Datenträgern Asylsuchender durch das BAMF bislang dazu geführt oder massgeblich dazu beigetragen hat, Angaben der Asylsuchenden zu ihrer Herkunft / Identität / Staatsangehörigkeit zu widerlegen bzw. zu bestätigen. Auch wenn die ausgelesenen Daten gegen die angegebene Herkunft sprechen, kann es im Einzelfall sein, dass es andere Erkenntnisse gibt, die letztlich zu einer Bestätigung der Herkunftsangabe führen.»

Gemäss der Studie der Gesellschaft für Freiheitsrechte in Deutschland birgt die automatische Auswertung von Daten, u.a. die Analyse von Sprachen und Dialekten aufgrund von Sprach- oder Chatnachrichten, zudem ein grosses Fehlerpotenzial. Dies kann zu einer Diskriminierung von Asylsuchenden aus bestimmten Herkunftsländern führen. Aufgrund fehlender Daten zur Zuverlässigkeit der Spracherkennung seien Behördenmitarbeitende sowie Gerichte nicht in der Lage, den Beweiswert der automatischen Prüfung sachgerecht einzuschätzen, was rechtsstaatlich problematisch sei (Seite 20). In der Vernehmlassungsvorlage bleibt die Auswertungsmethode unklar. Fest steht: Würden bei der Auswertung gemäss Vorentwurf automatische Mechanismen eingesetzt, gelten die erwähnten rechtsstaatlichen Bedenken auch hierzulande. Sollte die Auswertung hingegen rein manuell durch Mitarbeitende des SEM vorgenommen werden, würde dies zu enormen Aufwand - und damit Kostensteigerungen - führen.

Angesichts dieser Erfahrungswerte ist mehr als fraglich, ob die Abgabepflicht und Auswertung elektronischer Datenträger überhaupt geeignet ist für den anvisierten Zweck. Jedenfalls kann der absehbare geringe Nutzen den schwerwiegenden Eingriff

in die Privatsphäre aus Sicht der Digitalen Gesellschaft nicht rechtfertigen, weshalb die Massnahme unverhältnismässig ist.

Erforderlichkeit und Verhältnis Zweck-Wirkung

Damit eine grundrechtsbeschränkende Massnahme verhältnismässig ist, muss sie erforderlich sein. Das ist nur der Fall, wenn derselbe Zweck nicht mit milderen Massnahmen erreicht werden kann, welche weniger stark in das Grundrecht eingreifen. Dieses Prinzip ist aus Sicht der Digitalen Gesellschaft in der Vorlage der SPK-N nicht erfüllt: Die Formulierung in nArt. 8 Abs. 1 Bst. g AsylG des Entwurfs «wenn ihre Identität, die Nationalität oder der Reiseweg weder gestützt auf Identitätsausweise noch mit zumutbarem Aufwand auf andere Weise» festgestellt werden kann, ist zu unbestimmt. Es fehlt eine Präzisierung, dass eine solche Massnahme nur als *ultima ratio* eingesetzt werden darf, also nur, wenn die Identität, die Nationalität oder der Reiseweg **nicht mit einem geringeren Eingriff in die Privatsphäre** festgestellt werden kann. Diese zentrale Voraussetzung fehlt auch im erläuternden Bericht. Die Feststellung, dass «der asylsuchenden Person immer zuerst die Gelegenheit eingeräumt werden muss, von sich aus Angaben zur Nationalität oder zum Reiseweg zu machen», sollte selbstverständlich sein. Weiter hält der erläuternde Bericht fest: «Eine Feststellung der Identität auf 'andere Weise' ist in Konkretisierung des Verhältnismässigkeitsprinzips immer dann zuerst angezeigt, wenn diese mit einem im Vergleich zur elektronischen Datenauswertung geringeren Aufwand möglich ist.» Die Durchführung einer LINGUA-Analyse sei aber nicht vor einer Auswertung eines elektronischen Datenträgers ins Auge zu fassen, «da ein solches Verfahren mit einem grossen zeitlichen und organisatorischen Aufwand verbunden» sei. Dieser Argumentation kann aus Sicht der Digitalen Gesellschaft nicht gefolgt werden, denn ausschlaggebend für die Verhältnismässigkeit *des Grundrechtseingriffs* ist nicht der (in erster Linie beim Staat anfallenden) Aufwand, sondern das *Ausmass des Grundrechtseingriffs*. Im deutschen Asylgesetz findet sich die entsprechende Voraussetzung: Die Auswertung eines Datenträgers ist nur zulässig, wenn dies zur Feststellung von Identität und Staatsangehörigkeit notwendig ist, und der Zweck der Massnahme nicht durch mildere Mittel erreicht werden kann (§ 15a deutsches Asylgesetz).

Asylsuchende haben bereits heute eine allgemeine gesetzliche Mitwirkungspflicht im Verfahren. Sie können dazu auch freiwillig Handy- und Computerdaten als Beweismittel geltend machen – etwa Fotos, die ihre Flucht dokumentieren, oder Korrespondenzen. Zudem nutzt das Staatssekretariat für Migration bereits jetzt niederschwelligere Prüfverfahren wie etwa die öffentlich zugänglichen Social-Media-Profile, die vollauf genügen und das Recht auf Privatsphäre weniger stark tangieren. Eine LINGUA-Analyse würde ebenfalls einen geringeren Eingriff darstellen. Der

genannte Zweck, die Abklärung von Identität und Nationalität, kann somit auch mit weniger einschneidenden Massnahmen ausreichend erfüllt werden, weshalb die **Voraussetzung der Erforderlichkeit nicht erfüllt** ist.

Da die Auswertung der Datenträger bereits zu Beginn des Verfahrens, gemäss erläuterndem Bericht in der Regel in der Vorbereitungsphase, vorgenommen werden soll, und angesichts der beschränkten Zeit im beschleunigten Verfahren, scheint zweifelhaft, ob tatsächlich gewährleistet ist, dass zuerst weniger einschneidende Massnahmen ausgeschöpft werden. Daher muss diese **Kaskade – die Ausschöpfung von Massnahmen, die weniger stark in die Grundrechte der Asylsuchenden eingreifen – verbindlich im Gesetz festgeschrieben** werden.

Der deutsche Anwaltverein hielt in seiner Stellungnahme die Einführung einer ähnlichen Regelung in Deutschland ebenfalls für klar unverhältnismässig (Seite 3f): «Die vorgesehene Mitwirkungspflicht des Asylbewerbers, die daran anknüpfende Durchsuchungsbefugnis und die Auswertungsbefugnis gehen zu weit. Sie erfassen nämlich sämtliche Datenträger – neben Mobiltelefonen und Smartphones z. B. Tablets, Notebooks, sonstige Computer, externe Festplatten oder USB-Sticks, und vor allem sämtliche darauf enthaltene Daten des Betroffenen – von Daten, die dem Kernbereich privater Lebensgestaltung zuzuordnen sind, einmal abgesehen. Dies geht im Hinblick auf die Verhältnismässigkeit des Eingriffs zu weit. Auch in tatsächlicher Hinsicht besteht kein Bedarf an einer Speicherung und Verwendung dieses Datenumfangs zur Feststellung von Identität und/oder Staatsangehörigkeit des Betroffenen. Es dürfen viel mehr Daten gespeichert und durchgesehen werden, als es für den verfolgten Zweck der Feststellung von Identität und/oder Staatsangehörigkeit erforderlich ist.»

Besonders schützenswerte Daten

Gemäss nArt. 8a Abs. 1 AsylG des Vorentwurfs beinhalten die Daten, welche das SEM bearbeiten darf, auch besonders schützenswerte Personendaten nach Art. 3 Bst. c DSG. Das sind Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten; die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; Massnahmen der sozialen Hilfe; administrative oder strafrechtliche Verfolgungen und Sanktionen. Es ist nicht ersichtlich, warum solche Daten für die Feststellung der Identität, der Nationalität oder des Reiseweges benötigt werden. Allerdings kann nicht ausgeschlossen werden, dass bei der Suche nach Informationen bezüglich Identität und Nationalität auch besonders schützenswerte Daten zu Tage treten, auch wenn nicht explizit nach diesen gesucht wird. Wie mit solchen «Zufallsfunden» umgegangen werden soll, ist unklar. Dies zeigt aus Sicht der Digitalen Gesellschaft gerade auf, wie heikel das Vorhaben ist, und wie unnötig stark es in den Schutz der Privatsphäre eingreift. Es ist fraglich, ob damit der Kerngehalt des Grundrechts auf Schutz der Privatsphäre respektiert werden kann i.S.v. Art. 36 Abs. 4

BV.

Pro Asyl hat dazu in der Debatte in Deutschland festgehalten (Seite 20): «Gerade Smartphones fungieren als Speicher absolut privater Daten, seien es private Fotos oder intime Konversationen. Praktisch wird es für das Bundesamt kaum möglich sein eine Überprüfung der technischen Geräte vorzunehmen, ohne direkt auf höchstpersönliche Daten aus dem Kernbereich privater Lebensgestaltung zu stossen.» Pro Asyl kam zum Schluss (Seite 4): «Mit dem systematischen Auslesen der Handydaten schafft der Gesetzentwurf den «gläsernen Flüchtling», es gibt keine Grenze zum grundgesetzlich geschützten Kernbereich privater Lebensgestaltung. Damit erfolgt ein Ausspähen, das verfassungswidrig ist.»

Eine Bewertung der höchst sensiblen Personendaten auf informationstechnischen Systemen hat auch das Bundesverfassungsgericht in Deutschland bereits 2008 im Urteil gegen das Verfassungsschutzgesetz in Nordrhein-Westfalen vorgenommen: «Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.»

Das Bundesverfassungsgericht von Deutschland hat mit seinem Urteil ein neues **Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme** etabliert. Seit dem Richterspruch 2008 ist der Umfang der persönlichen Daten sowie der besonders schützenswerten Personendaten, die sich auf Computern, Datenträgern und Handys befinden und einen tiefen Einblick in die Privat- und Intimsphäre ermöglichen, durch die technische Entwicklung und die fortschreitende Digitalisierung und Vernetzung weiter dramatisch gewachsen.

Keine Freiwilligkeit

Die SPK-N hält den Vorschlag für verhältnismässig, und begründet dies u.a. damit, dass die Auswertung nur mit Einverständnis der Asylsuchenden geschehe. Diese könnten daher selber über die Verwertung ihrer Daten bestimmen, indem sie die Aushändigung verweigern. Eine Verweigerung der Herausgabe von elektronischen Datenträgern würde aber eine **Verletzung der Mitwirkungspflicht** darstellen. Eine

solche hat **gravierende verfahrensrechtliche Konsequenzen**:

- Negativer Einfluss auf die Glaubwürdigkeitsprüfung
- Formlose Abschreibung (Art. 8 Abs. 3bis AsylG)
- Ablehnung ohne Anhörung, somit nur mit rechtlichem Gehör, bei schuldhafter grober Verletzung der Mitwirkungspflicht (Art. 36 Abs. 1 lit. c i.V.m. Art. 31a Abs. 4 AsylG)
- Allenfalls Administrativhaft bei Verletzung der Mitwirkungspflicht im Wegweisungsverfahren (nArt. 76 Abs. 1 Bst. b Ziff. 3 AIG; wie im erläuternden Bericht erwähnt)

Angesichts dieser Konsequenzen kann nicht von einer «freiwilligen» Herausgabe von Datenträgern bzw. Mitwirkung bei der Bearbeitung von Personendaten gesprochen werden. Das Argument der SPK-N, dass aufgrund des «fehlenden Zwangs» die Verhältnismässigkeit gegeben sei, ist deshalb aus Sicht der Digitalen Gesellschaft nicht haltbar.

Die Anwesenheit der asylsuchenden Person bei der Auswertung bzw. die Gewährung des rechtlichen Gehörs kann die Schwere des Eingriffs nicht ausreichend abmildern. Nach Art. 4 Abs. 5 des Bundesgesetzes über den Datenschutz (DSG) ist eine Einwilligung der betroffenen Person in die Bearbeitung von Personendaten (wo diese erforderlich ist) erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen. Angesichts der Komplexität der Vorgänge – Auslesen von Daten, Zwischenspeicherung, Auswertung und Verwendung der Daten, welche Behörden erhalten Zugriff auf welche Daten – ist schwer vorstellbar, dass die Asylsuchenden im Zeitpunkt der Aushändigung der Datenträger ausreichend aufgeklärt sind, um in die Massnahme überhaupt informiert und damit gültig einwilligen zu können. Auch vor diesem Hintergrund kann nicht von Freiwilligkeit gesprochen werden. Zudem fällt auf, dass das Einverständnis nur im erläuternden Bericht, nicht aber im Vorentwurf selber erwähnt wird.

Vergleich zum Strafprozessrecht

Im Strafprozessrecht ist die Auswertung von Handydaten sehr restriktiv geregelt. Smartphones von mutmasslichen Straftätern dürfen nur bei **dringendem Tatverdacht auf schwere Delikte** überwacht und analysiert werden (Vgl. Art. 269ff Strafprozessordnung StPO sowie Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs BÜPF). Bei Asylsuchenden jedoch soll nun bereits der blosse Zweifel an deren Aussagen zum Auslesen der Handy- und Computerdaten genügen. Der Vorstoss stellt sie unter Generalverdacht. Faktisch findet eine Vorverurteilung statt: Einem Flüchtling ohne Pass wird unterstellt, seine Identität

absichtlich zu verschleiern und an der Identitätsklärung nicht mitwirken zu wollen. Es gibt jedoch vielfältige Gründe, warum Betroffene keinen Pass besitzen – oft nur schon deshalb, weil sie bereits im Herkunftsland keine Papiere hatten.

Zudem braucht es im Strafverfahren für eine Überwachung des Fernmeldeverkehrs eine **gerichtliche Genehmigung** (Genehmigungspflicht: Art. 272 Abs. 1 StPO, Genehmigungsverfahren: Art. 274 StPO). D.h. die Rechtmässigkeit der Überwachung (darunter die Verhältnismässigkeit) muss innert 24h durch ein Gericht geprüft werden. Eine Durchsuchung elektronischer Datenträger kann neben dem Gericht zwar auch die Staatsanwaltschaft anordnen, der Durchsuchungsbefehl muss aber auf jeden Fall (abgesehen von dringlichen Ausnahmefällen) schriftlich erfolgen (Art. 198 StPO und Art. 241 Abs. 1 StPO). Eine systematische und präventive Durchsuchung ist ausgeschlossen (BGer, Urteil 6B_998/2017 vom 20.04.2018, E. 2.1.1.). Entsprechende Voraussetzungen wie im Strafprozessrecht, insbesondere eine gerichtliche Kontrolle, fehlen im vorliegenden Vorschlag bezüglich Mitwirkungspflicht im Asylverfahren gänzlich. Mängel könnten höchstens nachträglich im Beschwerdestadium vor dem Bundesverwaltungsgericht geltend gemacht werden; dies wäre jedoch zu spät, da dann die Auswertung der Daten bereits vorgenommen wurde. **Asylsuchende sind keine straftatverdächtigen Personen**. Dass eine breite Auswertung ihrer Datenträger ermöglicht werden soll ohne **(mindestens) dieselben grundlegenden Verfahrensgarantien** wie für Strafverdächtige, ist nicht haltbar. Die Anwesenheit bzw. der Einbezug der Rechtsvertretung der Asylsuchenden sowie die Gewährung des rechtlichen Gehörs vermögen diesen gravierenden Mangel nicht zu beheben. Es ist daher eine gerichtliche Überprüfung vorzusehen.

Mit Blick auf die Einführung der Regelung in Deutschland hat Pro Asyl gestützt auf die Rechtsprechung des deutschen Bundesverfassungsgerichts ebenfalls festgehalten, dass für den Zugriff auf Verbindungsdaten in Strafverfahren ein richterlicher Beschluss notwendig sei. Und (Seite 21): «Die Klärung der Identität ist auch nicht ansatzweise mit der Situation bei Ermittlungen wegen Straftaten von erheblicher Bedeutung vergleichbar. Wenn schon dort der Richter sprechen muss, gilt dies erst Recht bei unschuldigen, keiner Straftat verdächtigten und bloß ausweislosen Flüchtlingen.»

Datenschutz

Im Asylverfahren sind sensible Daten betroffen. Bei allen Verfahrensschritten sind der Datenschutz der Betroffenen sowie die Verhältnismässigkeit zu wahren. Es sollen nur Regelungen eingeführt werden, die vom Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) geprüft, beurteilt und gutgeheissen wurden.

Im Hinblick auf die Einführung einer ähnlichen Regelung in Deutschland äusserte die deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

erhebliche datenschutzrechtliche Bedenken. Aus Sicht der Gesellschaft für Freiheitsrechte steht die Datenverarbeitung durch das BAMF (Seite 6) «im Widerspruch zu diversen datenschutzrechtlichen Grundsätzen, insbesondere der Datenminimierung und der Zweckangemessenheit der Massnahmen, aber auch der Transparenz und Nachvollziehbarkeit von Datenverarbeitung.» In drei Fällen haben Asylsuchende gegen die Auswertung ihrer Mobiltelefone Beschwerde eingereicht, diese sind noch hängig. In Österreich wurde die entsprechende gesetzliche Grundlage bisher unter anderem aus datenschutzrechtlichen Gründen nicht angewendet (Seite 44). In Belgien wurde eine ähnliche gesetzliche Grundlage entgegen der Stellungnahme der Datenschutzbehörde eingeführt. Verschiedene Organisationen haben eine Beschwerde gegen die Regelung eingereicht, die beim belgischen Verfassungsgerichtshof hängig ist. Gemäss den beschwerdeführenden Organisationen wurde die Regelung bisher nicht umgesetzt.

Der Vorentwurf wirft bezüglich Datenschutz verschiedene Fragen auf, etwa mit Blick auf die Information und Einwilligung der betroffenen Person (siehe dazu oben), die vorgesehene Zwischenspeicherung (nArt. 8a Abs. 3 AsylG), die Weiterleitung an andere Behörden (Sicherheitsbehörden gemäss Art. 22a BPG / Art. 20 Abs. 3 und 4 NDG; kantonale Behörden, nArt. 47 Abs. 3 AsylG), den Einbezug von Dritten für den Einzug von Datenträgern (Art. 26 Abs. 5 AsylG), sowie die Tangierung von Daten von Drittpersonen. Demgegenüber sind die Ausführungen im erläuternden Bericht zum Datenschutz zu knapp, um die datenschutzrechtlichen Bedenken auszuräumen. Dazu bräuchte es eine detailliertere Analyse und Begründung.

Gemäss nArt. 8a Abs. 1 AsylG des Vorentwurfs beinhalten die Daten, die das SEM bearbeiten darf, auch besonders schützenswerte Personendaten nach Art. 3 Bst. c DSG. Das sind Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten; die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; Massnahmen der sozialen Hilfe; administrative oder strafrechtliche Verfolgungen und Sanktionen. Die Bearbeitung und Verwendung dieser Daten geht weit über das Ziel der Identitätsklärung hinaus und untergräbt damit eines der zentralen Datenschutzprinzipien: den Grundsatz der Zweckbindung. Dies ausgerechnet in einem Bereich, in dem ein besonderes Bedürfnis nach Datenschutz besteht (Vgl. Peter Uebersax: Zur Revision des Ausländergesetzes gemäss der Botschaft des Bundesrates vom März 2018, in: Jusletter 9.7.2018; Caroline Gloor Scheidegger, Adrian Lobsiger: Rechtliche Fragen bei der Bearbeitung von Migrationsdaten, in: Stephan Breitenmoser, Otto Lagodny, Peter Uebersax (Hrsg.): Schengen und Dublin in der Praxis – aktuelle Herausforderungen, Zürich 2018, S. 317-338). Die Digitale Gesellschaft fordert daher eine explizite Beschränkung der Verwendung und Auswertung jener Daten, die tatsächlich und ausschliesslich dem anvisierten Zweck der Identitätsklärung dienen.

Der Vorentwurf (nArt. 8a Abs. 5 AsylG) sieht vor, dass der Bundesrat festlegt, welche Daten erhoben werden und den Zugriff sowie die Einzelheiten der Auswertung der Personendaten regelt. Er bestimmt insbesondere die verschiedenen elektronischen Daten, die ausgewertet werden können. Die Delegation der Rechtsetzungsbefugnisse hinsichtlich Datensicherheit und Datenschutz an den Bundesrat ist aus Sicht der Digitalen Gesellschaft ungenügend, da die Anforderungen an die Normdichte bei Datenbearbeitungsvorgängen mit einem derart grossen Gefährdungspotenzial wie im vorliegenden Fall besonders hoch sind. Nach Ansicht der Digitalen Gesellschaft sollten daher die Grundzüge der Materie ins Gesetz aufgenommen werden.

Kosten

Der erläuternde Bericht der SPK-N enthält nur vage Angaben bezüglich der zu erwartenden Kosten. Der Personalaufwand sowie die Kosten für Beschaffung, Einrichtung und Betrieb neuer Informatikkomponenten sowie Dolmetscher und Einbezug der Rechtsvertretung können demnach noch nicht beziffert werden. Gemäss informeller Anfragen des SEM an verschiedene Anbieter von in Frage kommender «Auswertungssoftware» würden sich die entsprechenden Anschaffungskosten in einem Bereich zwischen 100'000 und 200'000 Franken bewegen. Es ist fraglich, ob aufgrund dieser ungenauen Angaben eine verlässliche Kostenprognose erstellt werden kann.

Zum Vergleich: In Deutschland fielen die Kosten für die notwendige Hard- und Software sowie die Analyse der Daten bisher deutlich höher aus als geplant (Seite 34): von 2017 bis April 2018 waren die Kosten mit 7.6 Millionen Euro mehr als doppelt so hoch wie ursprünglich veranschlagt. Die Gesellschaft für Freiheitsrechte führt weiter aus (Seite 35): «Laut Angaben des Bundesinnenministerium aus dem Dezember 2018 sind für das System bis Ende des Jahres 2019 Gesamtkosten in Höhe von 11,2 Millionen Euro vorgesehen. Die Gesamtkosten werden weiter steigen, für Support ist mit jährlich etwa 2,1 Millionen Euro zu rechnen. Ausserdem wurden entsprechend der Gesetzesbegründung 300.000 Euro pro Jahr für Lizenzen erwartet.» Die Gesellschaft für Freiheitsrechte zieht den Schluss (Seite 47): «Es profitieren damit in erster Linie die Hersteller von Überwachungstechnologie, die mit ihren Angeboten gut verdienen.»

Die voraussichtlich hohen Kosten sind mit Blick auf den erwartungsgemäss beschränkten Nutzen nicht gerechtfertigt. Siehe dazu oben «Fragliche Eignung: geringer Nutzen. Auch aus diesem Grund ist die vorgeschlagene Änderung aus Sicht der Digitalen Gesellschaft unverhältnismässig und unnötig.