Deutscher Bundestag **Drucksache 20/3759**

20. Wahlperiode 29.09.2022

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Eugen Schmidt, Barbara Lenk, Joana Cotar, Edgar Naujok und der Fraktion der AfD
– Drucksache 20/3433 –

Aktivitäten im Bereich sogenannter Digitaler Identitäten der Bundesregierung, Datenschutz und Datensouveränität und elektronischem Personalausweis

Vorbemerkung der Fragesteller

Die Bundesregierung wirbt in verschiedenen Publikationen für ihr „Projekt Digitale Identitäten“ (https://www.bmi.bund.de/Webs/PA/DE/verwaltung/projekt_digitale_identitaeten/projekt_digitale_identitaeten_node.html). Dabei solle nicht nur die Identifizierung vor staatlichen Stellen und in herkömmlichen Szenarien ermöglicht werden, sondern ein gesamtes „Ökosystem“ entstehen (ebd.). Nach Ansicht der Fragesteller handelt es sich bei Digitalen Identitäten zwar um eine technisch interessante Technologie, die Gefahr von Totalüberwachung, besonders durch nach Meinung der Fragesteller bestehende linkextrem unterwanderte Stellen, wohnt ihr aber nach Auffassung der Fragesteller inne. Die Gefahren wachsen nach Lesart der Fragesteller insbesondere dann, wenn immer weitere Pflichten zur Identitätsfeststellung geschaffen werden oder sich die Praxis auf andere Weise etabliert.

Die Bundesregierung gibt als Nutzungsbeispiel von Digitalen Identitäten auch „Packstationen“ und „Konzerttickets“ an (https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124; https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf). Die Präsidentin der Europäischen Kommission, Dr. Ursula von der Leyen, pries sogar das Mieten von Fahrrädern als Anwendungsgebiet an (https://web.archive.org/web/20210603210849/https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de). Offen bleibt nach Auffassung der Fragesteller bislang, in welchen Fällen nach Ansicht der Bundesregierung eine streng personengebundene Identifizierung überhaupt notwendig sei und ob entsprechende Pflichten und Anreize vor privaten und staatlichen Stellen zurückgefahren statt ausgeweitet werden müssten.

Die Nutzung Digitaler Identitäten solle laut Bundesregierung angeblich „selbstbestimmt“ und „souverän“ erfolgen (https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf, S. 1 f.). Die Fragesteller wollen ermitteln, ob die Begriffspaare „selbstbestimmtes Teilen“ und „selbstsouveräne Identität“ (ebd., S. 2) in der Praxis so aussieht, dass Bürger trotzdem faktisch häufiger Daten an durch die Regierung direkt oder indirekt

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 28. September 2022 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

kontrollierte Stellen herausgeben. Gerade für oppositionelle Gruppen in der Bundesrepublik Deutschland ergäben sich nach Ansicht der Fragesteller vor diesem Hintergrund erhebliche Gefahren durch die Möglichkeit zur Erstellung von Bewegungs- und Verhaltensprofilen und deren Nutzung durch die 19 staatlichen Geheimdienste.

Auf einer Informationsseite schreibt die Bundesregierung zum elektronischen Personalausweis, es sei „nicht möglich, die Daten im Chip ohne [das] Wissen [des Inhabers] auszulesen. Hierfür ist ein spezielles Lesegerät notwendig, das nur bestimmten staatlichen Stellen (zum Beispiel Ausweis-, Polizei-, Grenz- und Zollbehörden) zur Verfügung steht“ (https://web.archive.org/web/20211101194727/https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/2_biometrie_faq/biometrie-liste.html). Vor dem Hintergrund, dass bei einem mutmaßlichen Mitglied einer kriminellen Vereinigung aus dem Spektrum des Linksextremismus (sogenannte Gruppe E.) ein Ausweisdrucker mit behördlicher Kennzeichnung festgestellt worden sei, ergeben sich für die Fragesteller weitere Fragen (https://www.welt.de/politik/plus231390455/Linksextremismus-Generalbundesanwalt-erhebt-Anklage-gegen-Lina-E.html).

1. Schließt die Bundesregierung aus, dass sie zukünftig (etwa über das Einbringen von Gesetzentwürfen) Versuche unternehmen wird, Bürger rechtlich zu verpflichten, Digitale Identitäten, die über die Sicherheitsstufe der Anmeldung mit Nutzername und Kennwort hinausgehen, einzusetzen, und wenn nein, plant die Bundesregierung Verpflichtungen einzuführen, und wenn ja, in welchen Fällen erwägt sie eine Verpflichtung?

Die Nutzung von Digitalen Identitäten wird stets freiwillig erfolgen. Insoweit ist nicht geplant, dass es eine gesetzlich geregelte Verpflichtung zur Nutzung Digitaler Identität geben wird.

2. Hat die Bundesregierung konkrete Schritte unternommen, um die verpflichtende Nutzung von digitalen Identitäten zu verhindern, und wenn ja, welche?

Eine gesetzlich zwingende Nutzung von Digitalen Identitäten wurde bisher nicht erwogen oder verfolgt und musste insoweit nicht durch die Bundesregierung verhindert werden.

3. Aus welchem Grund führt die Bundesregierung „Packstationen“ und „Konzerttickets“ als Beispiele für die Nutzung Digitaler Identitäten an statt, wie es nach Ansicht der Fragesteller denkbar wäre, bei Anbietern dafür zu werben, eine anonyme Nutzung der Dienste zu ermöglichen (siehe Vorbemerkung der Fragesteller)?

Die zitierte Passage entstammt einer Veröffentlichung der vorherigen Bundesregierung, die sich die aktuelle Bundesregierung unter dem Gesichtspunkt der Diskontinuität nicht zu eigen macht.

Dessen ungeachtet handelt es sich bei den zitierten Anwendungsfällen um privatwirtschaftliche Anwendungen. Der These, dass die genannten Beispiele sich auch mit anonymer Nutzung verwirklichen lassen dürften, tritt die Bundesregierung im Grundsatz nicht entgegen. Weiterhin teilt die Bundesregierung die in der Vorbemerkung dargestellte Auffassung, dass digitale Identitäten „selbstbestimmt“ und „souverän“ nutzbar sein müssen.

4. Geht die Bundesregierung davon aus, dass Bürger sich zukünftig bei großflächiger Nutzung von Digitalen Identitäten häufiger als bisher mit staatlich beglaubigten Identitäten – in herkömmlicher oder digitaler Form – bei privaten oder staatlichen Stellen identifizieren werden, und wenn ja, in welchen Lebensbereichen?

Es wird nicht davon ausgegangen, dass eine Nutzung der Online-Ausweisfunktion dazu führt, dass Bürger sich mittels staatlich beglaubigter Identitäten häufiger bei privaten oder staatlichen Stellen identifizieren.

5. Wie begegnet die Bundesregierung der aus Sicht der Fragesteller bestehenden Gefahr der Kriminalisierung von Personen etwa über § 281 des Strafgesetzbuchs (StGB), die, wie im Wirtschaftsverkehr üblich, mit Einwilligung und bevollmächtigt in fremdem Namen handeln, sobald staatlich ausgegebene digitale Identitäten genutzt werden?

Die Bundesregierung teilt die in der Frage zum Ausdruck gebrachte Sorge nicht. In Betracht kommende Straftatbestände setzen ein Handeln zur Täuschung im Rechtsverkehr, eine Täuschung oder eine unbefugte Verwendung von Daten voraus. Handelt eine Person mit Einwilligung und bevollmächtigt in fremdem Namen, dürften allein dadurch die genannten Tatbestandsvoraussetzungen in aller Regel nicht erfüllt sein.

6. Hat die Bundesregierung Studien durchgeführt, durchführen lassen oder ausgewertet über die Auswirkungen von ständiger Identifizierung vor staatlichen oder nichtstaatlichen Stellen auf die Gesellschaft und den Einzelnen, und wenn ja, welche sind dies, und welche wesentlichen Schlussfolgerungen leitet die Bundesregierung daraus ab?

Die Bundesregierung hat keine entsprechenden Studien durchgeführt, durchführen lassen oder ausgewertet.

7. Plant die Bundesregierung, einem Regelungsgedanken der Fragesteller folgend einen Katalog von Typen nichtstaatlicher Stellen einzuführen, die eine Identifizierung mittels Digitaler Identitäten oder herkömmlicher Verfahren stets oder grundsätzlich rechtlich verbieten, und wenn nein, wie soll das von der Bundesregierung betonte Grundrecht auf informationelle Selbstbestimmung vor dem Hintergrund angemessen verwirklicht werden können?

Die Bundesregierung misst dem Recht auf informationelle Selbstbestimmung besondere Beachtung bei. So soll auch bei einer Weiterentwicklung des bestehenden eID-Systems stets gewährleistet sein, dass ein Erstellen von Verhaltens- und Bewegungsprofilen ausgeschlossen ist.

8. Plant die Bundesregierung, einem Regelungsgedanken der Fragesteller folgend, die Kodifizierung eines Katalogs von Datenarten (zum Beispiel Name oder Adresse), die von privaten Stellen bei bestimmten Anwendungsszenarien nicht erhoben werden dürfen?

   a) Wenn ja, welche konkreten Überlegungen bestehen dahin gehend?

   b) Wenn nein, warum nicht?

Die Fragen 8 bis 8b werden gemeinsam beantwortet.

Bezogen auf die Onlineausweisfunktion ist die Kodifizierung eines Katalogs von Datenarten nicht erforderlich. Die Nutzung der Onlineausweisfunktion erfolgt im Sinne des Datenschutzes bezüglich personenbezogener Daten stets nur in einem Umfang, der für den jeweiligen Anwendungsfall erforderlich ist.

9. Sind staatliche Stellen beim eID (elektronische Identität)-System, das beim Personalausweis zum Einsatz kommt (siehe die Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/4987), technisch in der Lage, die darauf befindliche Digitale Identität zu jeder Zeit für ungültig zu erklären, zurückzurufen oder zu sperren, sodass das das Online-Ausweisen und das Vor-Ort-Auslesen unter allen Umständen ab dem Zeitpunkt des Sperrwunsches unmöglich wird, und wenn nein, hängt die Wirksamkeit an weiteren Bedingungen (etwa einem Abruf aktueller Sperrlisten von Lesegeräten, die nur periodisch erfolgen), und wie wird die Sperrung technisch umgesetzt?

Die Frage 9 wird so verstanden, dass der Sperrwunsch vom Personalausweisinhaber ausgeht. Ein Sperren der eID-Funktion (Online-Ausweisfunktion) für Personalausweisinhaber, bei beispielsweise Verlust des Personalausweises (nPA), erfolgt im Regelfall über die Sperr-Hotline und ist somit technisch möglich. Voraussetzung ist, dass das Sperrkennwort vorliegt. Wenn das Sperrkennwort nicht vorliegt, ist ein persönliches Erscheinen bei der Ausweisbehörde inklusive einer Identitätsfeststellung aus Sicherheitsgründen nötig.

10. Können staatliche Behörden auch kontaktlos ohne PIN auf Daten des Personalausweises mit eID-Funktion zugreifen, wenn sich ein entsprechendes Lesegerät in der Nähe eines Ausweises befindet, und wenn ja, auf welche Daten?

Die im Chip der Personalausweise gespeicherten Daten der Online-Ausweisfunktion sind durch besondere Sicherheitsmechanismen vor unberechtigtem Zugriff geschützt. Diese Sicherheitsmechanismen sehen vor, dass ein Lesegerät nur dann die im Chip gespeicherten Informationen der Online-Ausweisfunktion lesen kann, wenn die PIN eingegeben wurde und die lesende Stelle sich mit einem Berechtigungszertifikat autorisieren kann. Nur wenn dem Chip der richtige Schlüssel übermittelt wird, gibt er die in ihm gespeicherten Daten gegenüber dem Lesegerät frei (sog. Extended Access Control).

11. Erlangen staatliche Stellen bei einem Identifizierungsvorgang eines Bürgers gegenüber einer nichtstaatlichen Stelle mittels der eID-Funktion des Personalausweises Kenntnis

    a) von dem Ob des Identifizierungsvorganges,

    b) von Daten der natürlichen Person oder einer Kennung, die direkt auf die sich identifizierende natürliche Person rückführbar ist,

    c) von der nichtstaatlichen Stelle, die um die Identifizierung gebeten hat, sei es nur vorübergehend und ohne menschliche Kenntnisnahme, und wenn ja, wie konkret, welche staatlichen Stellen sind das, und welche der dabei anfallenden oder daraus abgeleiteten Daten werden durch staatliche Stellen für welche Dauer gespeichert?

Die Fragen 11 bis 11c werden gemeinsam beantwortet.

Bei einem Identifizierungsvorgang eines Bürgers gegenüber einer nicht staatlichen Stelle (mittels der eID-Funktion des Personalausweises) erhalten staatliche Stellen keine Informationen über die online ausweisende Person. Es ist

technisch nicht möglich, dass direkt auf die sich identifizierende natürliche Person rückführbare Informationen erhoben werden.

12. Unter welchen technischen und rechtlichen Bedingungen und in welchem Zeitraum sind staatliche Stellen in der Lage, die staatlich erteilte Berechtigung für private oder andere staatliche Stellen, die eine Identifizierung mit der eID-Funktion des Personalausweises einfordern, zurückzurufen oder zu sperren, sodass der elektronische Personalausweis den Identifizierungsvorgang abbricht?

Das Sperren einer Berechtigung für Diensteanbieter erfolgt, wenn ein Missbrauch durch die Vergabestelle für Berechtigungszertifikate festgestellt oder bestätigt wird. Diese prüft zunächst vorliegende Hinweise im Rahmen eines Verwaltungsverfahrens. In diesem Zusammenhang können auch die zuständigen Datenschutzaufsichtsbehörden beteiligt werden.

13. Hat die Bundesregierung ausländischen Staaten die technische Möglichkeit eingeräumt, über die eID-Funktion des Personalausweises diesen kontaktlos auszulesen, und wenn ja, welchen?

Gemäß § 21 Absatz 7 des Personalausweisgesetzes (PAuswG) sind öffentliche Stellen anderer Mitgliedstaaten der Europäischen Union berechtigt, Daten im Wege des elektronischen Identitätsnachweises anzufragen und können diese bei Zustimmung und PIN-Eingabe der Nutzerin oder des Nutzers auslesen. Gemäß Verordnung (EU) 910/2014 stellt die Bundesrepublik Deutschland den anderen Mitgliedstaaten eine entsprechende Software zur Anbindung an das deutsche eID-System bereit.

Zudem dürfen Inspektionssysteme von Kontrollbehörden in der Europäischen Union im Rahmen ihrer Kontrollaufgaben nach einer erfolgreichen Authentisierung unter Verwendung der MRZ oder der Card-Access Number (CAN) auf Daten der eID-Funktion zugreifen.

14. Sind der Bundesregierung Fälle von Lesegeräten für elektronische Personalausweise bekannt, die staatlichen Stellen abhandengekommenen sind, und wenn ja, wann, und wo sind solche Fälle aufgetreten?

Kontaktlos-Lesegeräte sind u. a. NFC-fähige Smartphones oder sogenannte Visualisierungs-Änderungsterminals in den Personalausweisbehörden. Ein Abhandenkommen dieser Geräte ist für den Schutz der Identitäten unbeachtlich, da der Personalausweisinhaber vor jedem Online-Ausweisen seine PIN eingeben muss. Zudem müssen sich Visualisierungs-Änderungsterminals täglich bei dem Ausweishersteller mit einer Smartcard elektronisch autorisieren; in Verlust geratene Geräte werden unmittelbar gesperrt.

15. Sind die staatlich ausgegebenen Lesegeräte für elektronische Personalausweise an Datennetze angeschlossen, und wenn ja, in welcher Form (beispielsweise zwingend dauerhaft oder periodisch), und für welche Funktionen wird diese Verbindung zu Datennetzen genutzt?

Hierbei ist zwischen Änderungsterminals, welche in den Pass- und Ausweisbehörden eingesetzt werden, und hoheitlichen Inspektionssystemen, welche im Rahmen der Grenzkontrolle verwendet werden, zu unterscheiden.

Die Änderungsterminals sind über eine Online-Verbindung an die durch den Ausweishersteller betriebenen Hintergrundsysteme angebunden. Über diese werden durch die Änderungsterminals Softwareaktualisierungen, aktuelle TLS-Kommunikationszertifikate, CSCA-Zertifikate und -Masterlisten, sowie die Zertifikate aus der CVCA-eID-PKI bezogen, die für den Zugriff der Terminals auf die Ausweisdokumente notwendig sind. Die Kommunikation erfolgt hierbei nur authentisiert und verschlüsselt durch PKI basierte Protokolle (TLS) und stets nur initiiert durch die Firmware des Geräts. Darüber hinaus erfolgt keine Kommunikation über externe Datennetze.

Die hoheitlichen Inspektionssysteme laufen im Netz der Bundespolizei und beziehen im Bedarfsfall elektronisches Zertifikatsmaterial als Grundlage der Prüfung der Dokumentenechtheit und der biometrischen Verifikation des Ausweisinhabers.

16. Können Lesegeräte zum Auslesen des elektronischen Personalausweises, die staatliche Stellen nutzen (siehe Vorbemerkung der Fragesteller), ohne physischen Zugriff auf die Lesegeräte gesperrt werden, sodass ein Auslesen von Personalausweisen damit nicht mehr möglich ist, und wenn ja, wie wird die Sperrung technisch umgesetzt, und wie schnell nachdem eine staatliche Stelle eine Sperrung veranlasst, wird diese technisch wirksam?

Der Betrieb der Änderungsterminals ist nur unter Verwendung einer Bedienerkarte sowie der zugehörigen PIN möglich, welche nur den Mitarbeiten in den Pass- und Ausweisbehörden vorliegen. Diebstahl allein reicht nicht aus, um das Gerät unbefugt zu verwenden. Im Falle eines Diebstahls, bei dem das Gerät vom Strom getrennt wird, ist der Schlüsselspeicher des Terminals in Form einer zertifizierten Chipkarte stromlos und erwartet bei späteren Neustarts eine erneute Authentisierung durch einen Bediener. Zudem ist der Betrieb des Änderungsterminals nur in Verbindung mit dem Behörden-PC möglich, mit deren Software es bei der initialen Einrichtung kryptographisch abgesichert gekoppelt wurde.

17. Sind der Bundesregierung länderübergreifende und vergleichende Studien über die tatsächliche Häufigkeit der Aufforderung nichtstaatlicher Stellen, sich bei wirtschaftlichen Aktivitäten vor nichtstaatlichen Stellen auszuweisen, bekannt, oder hat sie solche Studien in Auftrag gegeben, und wenn ja, welche?

Entsprechende Studien sind nicht bekannt und nicht von der Bundesregierung in Auftrag gegeben.

18. Plant die Bundesregierung, einem Regelungsgedanken der Fragesteller folgend, für Verbraucher vor privaten Stellen ein Recht auf eine Hinterlegung eines Pfandes (etwa in Form von Bargeld) einzuführen statt Identifizierungsdokumente vorlegen zu müssen, und wenn nein, warum plant die Bundesregierung vor dem Hintergrund des von ihr proklamierten Rechtes auf informationelle Selbstbestimmung ein solches Recht nicht?

Allgemein darf vom Inhaber oder der Inhaberin eines Personalausweises gemäß § 1 Absatz 1 Satz 3 PAuswG grundsätzlich nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam daran aufzugeben. Die Regelung soll sicherstellen, dass der Ausweis stets in der Einfluss- und Kontrollsphäre des Ausweisinhabers bzw. der Ausweisinhaberin verbleibt. Eine Ausnahme vom Hinterlegungsverbot gilt gemäß § 1 Absatz 1 Satz 4

PAuswG für zur Identitätsfeststellung berechtigte Behörden. Zur Identitätsfeststellung berechtigte Behörden sind nach § 2 Absatz 2 PAuswG öffentliche Stellen, die befugt sind, zur Erfüllung ihrer gesetzlichen Aufgaben als hoheitliche Maßnahme die Identität von Personen festzustellen. Die Ausnahmevorschrift des § 1 Absatz 1 Satz 4 PAuswG deckt u. a. die Fälle ab, in denen Polizeibehörden Einlasskontrollen vornehmen.

§ 1 Absatz 1 Satz 3 PAuswG verbietet jedoch nicht die freiwillige Abgabe des Personalausweises. Der für die Hinterlegung angebotene Service/Dienstleistung/Zugang muss jedoch freiwillig sein. Das Bundesministerium des Innern und für Heimat empfiehlt, den Ausweis aus den zuvor geschilderten Erwägungen nicht abzugeben, sondern den Service/die Dienstleistung/den Zugang mit Hilfe alternativer Hinterlegungsgegenstände zu erlangen bzw. persönlich vorzunehmen.

Dem Bundesministerium des Innern und für Heimat ist bekannt, dass die rechtlichen Vorgaben zur Hinterlegung des Personalausweises insbesondere im nicht-öffentlichen noch nicht flächendeckend umgesetzt werden, z. B. durch die jederzeit bestehende Möglichkeit der Hinterlegung alternativer „Pfand“-Gegenstände im Rahmen des Einlassverfahrens.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333