

Dobrindts Lex Palantir

CSU-Innenminister legt Gesetzentwürfe zur Ermächtigung von BKA und Bundespolizei vor. Sie sollen massenhaft und automatisiert biometrische Daten aus dem Internet sammeln dürfen

Von Marc Bebenroth

Über die Vorstellungen der Bundesregierung zum nächsten Bundeshaushalt wurde und wird viel geschrieben und gesprochen. Der neueste Vorstoß zur Massenüberwachung glitt dabei im medialen Windschatten ebenfalls über den Kabinetttisch. Am Mittwoch vergangener Woche haben Gesetzentwürfe aus dem CSU-kontrollierten Innenministerium (BMI) die Zustimmung der Koalition aus CDU/CSU und SPD erhalten. Das Bundeskriminalamt (BKA) und die Bundespolizei sollen zum Einsatz von KI-Systemen für die Erfassung sämtlicher im Internet verfügbarer biometrischer Daten ermächtigt werden, wie das Ministerium gleichentags zur beabsichtigten »Stärkung der Sicherheitsbehörden im Kampf gegen Kriminalität und Terrorismus« mitteilte.

Der Referententwurf des »[Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit](#)« sieht vor, dem BKA das Kopieren von »öffentlich zugänglichen personenbezogenen Daten« aus dem Internet, die biometrische Merkmale enthalten, sowie den automatisierten biometrischen Abgleich mit Daten, »auf die es zur Erfüllung seiner Aufgaben zugreifen darf« zu erlauben. Zunächst ist dafür die Einschränkung vorgesehen, dass »bestimmte Tatsachen den Verdacht begründen« müssen, »dass eine Straftat von auch im Einzelfall erheblicher Bedeutung« begangen wurde oder »bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begehen wird«. Gemeint sind Delikte, wie sie in [Paragraph 2 Absatz 2 der Strafprozessordnung](#) gelistet sind.

Im Datenschleppnetz

Zu biometrischen Informationen können »die Form des Kopfes, die Fingerabdrücke, die Körpertemperatur oder die Beschaffenheit des Auges« zählen, wie das dem BMI unterstellte Bundesamt für Sicherheit in der Informationstechnik (BSI) [auf seiner Website erläutert](#). »Theoretisch lässt sich jedes körperliche Merkmal biometrisch verwerten.« Erfasst und verarbeitet werden bei biometrischen Verfahren beispielsweise »Fingerabdrücke, Iris, Handvenen oder das Gesicht«. Die Überwachung sei allerdings nicht auf Gesichter beschränkt, teilte die Linke-Abgeordnete Donata Vogtschmidt am Donnerstag mit. Sie umfasse auch biometrische Merkmale »wie Stimmen und Bewegungsabläufe«.

»Für die Bevölkerung ist wegen der weitgefassten Anwendbarkeit der Gesetzesvorschläge kaum vorhersehbar, in welchem Ausmaß sie der biometrischen Überwachung ausgesetzt sein wird«, kritisierte Vogtschmidt. »Der Anwendungsbereich geht deutlich über Terrorabwehr und nationale Sicherheit hinaus.« Deshalb habe die Linke-Fraktion einen Antrag eingebracht, »der ein generelles Verbot automatisierter biometrischer Überwachung im öffentlichen Raum fordert«. Mehr Überwachung könne »Ursachen von Kriminalität und sozialen Problemen nicht lösen«.

Dem BKA wird dabei freigestellt, ob es selbst das Datenschleppnetz auswirft oder andere damit beauftragt. Zulässig sein soll das Auslagern an »eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedstaats der Europäischen Union«. Das Auslagern an eine Stelle »in einem Drittstaat« inklusive Datenübermittlung dorthin soll erlaubt sein, wenn es wegen »nationaler Sicherheit« für erforderlich erklärt wird, wenn gewisse Voraussetzungen und Datenschutznormen eingehalten werden sowie niemand in der EU die Maßnahme angemessen umsetzen kann.

Schließlich soll das BKA auch die Erlaubnis erhalten, »bei ihm vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme« zu nutzen. Dem BMI zufolge ist der Missbrauch sämtlicher online verfügbarer biometrischer Daten als Futter für intransparente KI-Systeme »ein wichtiger Baustein zur (Weiter-)Entwicklung von polizeilichen Softwareanwendungen«.

»Der biometrische Internetabgleich ist erforderlich, um Personen zu identifizieren, zu lokalisieren sowie Tat-Täter-Zusammenhänge zu erschließen«, behauptet das BMI auch anlässlich des zweiten am Mittwoch beschlossenen [Gesetzesentwurfs zur »Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus«](#). Dieser enthält die Kernbestimmungen des ersten beschlossenen Papiers für den Fall, dass »eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat« begehen werde oder »das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet«, dass dies der Fall sei.

EU-Rechtsbruch mit Ansage

Ob die geplanten Befugnisse überhaupt mit dem Grundgesetz vereinbar sind, darf bezweifelt, muss aber – um sie zu kippen – gerichtlich festgestellt werden. Klar ist: Die Bundesregierung nimmt in Kauf, systematisch gegen die KI-Verordnung der Europäischen Union zu verstoßen. [Artikel 5 der Verordnung](#) benennt »verbotene Praktiken im KI-Bereich«. Dazu zählt »die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profilings einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen«. Verboten ist ebenso »die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern«.

Seit dem Ausscheiden der FDP aus der Bundesregierung blockiert das Bundesjustizministerium nicht länger den vom BMI vorangetriebenen autoritären Staatsumbau. So begleitet ein [Referentenentwurf »zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen«](#) aus dem von Stefanie Hubig (SPD) geleiteten Justizressort die beiden Entwürfe des Innenministeriums. Die geplante Änderung der Strafprozessordnung sieht vor, dass »zur Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen« biometrische Daten »aus einem Strafverfahren mit im Internet öffentlich zugänglichen biometrischen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden« dürfen. Bei Fahndungen sollen auch »in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte personenbezogene Daten« automatisiert weiterverarbeitet werden dürfen. Der Zugriff soll sich dabei auf »Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen« erstrecken dürfen.

Dobrindts »Sicherheitspaket 2.0« sei aus der Sicht der Linke-Abgeordneten Vogtschmidt »in der Summe nichts weiter als der höchst zweifelhafte Versuch, durch ein Gefühl der ständigen Überwachung im öffentlichen Raum die Handlungsfreiheit der Menschen zu ersticken und KI auch dort zu entfesseln, wo sie gesellschaftlich besonders großen Schaden anrichten kann«. Worauf das in der Praxis hinausläuft, wissen Kritiker schon seit geraumer Zeit: Einschränkung von Grundrechten sowie lukrative Staatsaufträge zum Beispiel für das von Faschisten geführte US-Unternehmen Palantir, dessen Produkte bereits von einigen Landespolizeien erprobt werden.

Im vergangenen Sommer war bekanntgeworden, dass Dobrindt den bundesweiten Einsatz von Palantir-Software prüfe. Auf *dpa*-Anfrage teilte ein Sprecher des BMI mit, dass »verschiedene Optionen« in den Blick genommen würden, wie das Fachportal *Legal Tribune Online* am 30. Juli 2025 berichtete. Im europaweiten Vergabeverfahren habe zum damaligen Zeitpunkt nur das – erklärtermaßen antikommunistische sowie für extralegale Tötungen zur Verfügung stehende – Unternehmen eine marktverfügbare Softwarelösung angeboten, die den gestellten Ansprüchen entsprochen habe.

IP-Adressen auf Vorrat

Eine Woche vor den KI-Befugnissen hatten Dobrindt und Hubig den Entwurf für die geplante Vorratsdatenspeicherung von IP-Adressen durch das Kabinett gebracht. CDU/CSU und SPD planen derzeit eine »minimalinvasive Lösung«, die sich eng an die Vorgaben des Europäischen Gerichtshofs (EuGH) und des Bundesverfassungsgerichts halte, behauptete Hubig am 22. April. Der »große Unterschied« zu früheren Regelungen sei, dass »keine Bildung von digitalen Bewegungsprofilen« erlaubt sei.

Internetanbieter stellen ihren Kunden in der Regel für die Dauer von 24 Stunden eine bestimmte IP-Adresse zur Verfügung – und geben gegenüber Strafverfolgungsbehörden Auskunft über die Anschlussinhaber. So können beispielsweise Abmahnanwälte oder Justizbehörden gegen Personen vorgehen,

die eines mit dem »Tatmittel Internet« begangenen Vergehens beschuldigt werden.

Lobbyisten der Polizeien und Geheimdienste behaupten seit Jahren, dass die von den Internetanbietern vorgesehene Speicherfrist nicht ausreiche, um Tatverdächtige zu ermitteln, und fordern deshalb beständig eine längere gesetzlich vorgeschriebene Speicherfrist von mehreren Wochen oder gar Monaten.

Diese Unternehmen müssten allerdings das Geld und die Infrastruktur für größere Speicherkapazitäten stellen. Der Branchenverband Bitkom übte daher Kritik an den Plänen der Regierung, wenn auch verhalten. Sie seien »im Grundsatz richtig«, könnten aber rechtliche Konsequenzen nach sich ziehen. Der Gesetzentwurf sehe vor, dass die Daten drei Monate nach Ende der Zuweisung einer IP-Adresse gelöscht werden sollen und nicht drei Monate ab ihrer Entstehung, erklärte Verbandspräsident Ralf Wintergerst am 22. April.

Der sogenannten Deutschen Polizeigewerkschaft (DPolG) ging die dreimonatige Speicherung nicht weit genug. Dies reiche »in komplexen Ermittlungsverfahren, insbesondere bei banden- oder netzwerkartig organisierten Straftaten, regelmäßig nicht aus«, behauptete DPolG-Chef Heiko Teggatz gegenüber der *Rheinischen Post*. Teggatz zufolge sei eine Mindestspeicherfrist von sechs Monaten notwendig. Zu den härtesten Befürwortern einer solchen Form der anlasslosen Massenüberwachung zählt der Deutsche Richterbund (DRB). Dieser begrüßte entsprechend die am 22. April präsentierten Pläne der Bundesregierung. »Es ist höchste Zeit, dass die politische Hängepartie um die IP-Adressen-Speicherung endet« und eine »Regelungslücke schließt«, erklärte DRB-Bundesgeschäftsführer Sven Rebehn.

»Die Bundesregierung führt eine Massenüberwachung durch die Hintertür ein«, warnte dagegen die Linke-Abgeordnete Clara Büniger gleichentags. Die Speicherung erfolge aus technischen Gründen etwa bei Glasfaseranschlüssen »faktisch bis zu über einem Jahr«.

AF Info Hintergrund: ZF Hintergrund

<https://www.jungewelt.de/artikel/522028.massenueberwachung-in-der-brd-dobrindts-lex-palantir.html>