

Digitale Ermittlungsmaßnahmen¹

Ergänzende Informationen

Problem	Bislang gibt es in Deutschland keine Rechtsgrundlage, die den Strafverfolgungsbehörden den automatisierten Abgleich von Lichtbildern eines Tatverdächtigen aus einem Strafverfahren mit öffentlich zugänglichen Lichtbildern im Internet ermöglicht. Des weiteren erlauben die bestehenden Rechtsgrundlagen trotz immer größer werdenden Datenmengen nicht den Einsatz moderner Systeme zur Datenanalyse, um die rechtmäßig bei der Polizei gespeicherten Daten auf Zusammenhänge zu einem Strafverfahren zu analysieren. So können Ermittlerinnen und Ermittler derzeit nur unter viel Zeiteinsatz manuell einzelne Webseiten in Augenschein nehmen, um unbekannte Verdächtige zu identifizieren. Die verschiedenen Datenbanken bei der Polizei können gegenwärtig nur jeweils einzeln unter Einsatz sehr einfacher Programme nach Zusammenhängen zu einem konkreten Strafverfahren durchsucht werden. Die Ergebnisse der Suchen müssen hinterher händisch durch die Ermittlerinnen und Ermittler in Tabellen oder Diagrammen zusammengefasst werden. Das sind besonders personalaufwändige, fehleranfällige und ineffiziente Prozesse.
Vorschläge	Die Strafverfolgungsbehörden sollen mit neuen Befugnissen ausgestattet werden, um die Strafverfolgung effektiver zu machen. Der Gesetzentwurf sieht vor, dass Strafverfolgungsbehörden in bestimmten Fällen biometrische Daten aus einem Strafverfahren (z. B. ein Bild eines Verdächtigen) mit im Internet frei verfügbaren Daten automatisiert abgleichen können (biometrischer Internetabgleich). Außerdem soll unter engen Voraussetzungen der Einsatz von Recherche- und Analyseplattformen für bestehende Datenbanken der Polizei ermöglicht werden, um vorhandene Informationen aufzubereiten und einfacher auszuwerten (automatisierte Datenanalyse).
Verfahrensstand	Der Gesetzentwurf wurde in enger Abstimmung mit dem für die Polizeien des Bundes zuständigen Bundesministerium des Innern erarbeitet. Er wird derzeit innerhalb der Bundesregierung abgestimmt und wurde außerdem an die Länder und Verbände versandt. Interessierte Kreise haben nun Gelegenheit, bis zum 2. April 2026 Stellung zu nehmen.
Weitere Maßnahmen	Der Gesetzentwurf ist Teil der im Koalitionsvertrag für die 21. Legislaturperiode vorgesehenen Maßnahmen zur Stärkung der Sicherheits- und Strafverfolgungsbehörden. Parallel zu den für die Strafverfolgungsbehörden vorgesehenen Maßnahmen schlägt das Bundesinnenministerium in enger Abstimmung mit dem

¹ Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

I. Biometrischer Internetabgleich

1. Was schlägt das BMJV vor?

Um einen Sachverhalt aufzuklären, die Identität oder den Aufenthaltsort eines Beschuldigten oder Zeugen festzustellen, sollen Strafverfolgungsbehörden vorhandene biometrische Daten aus einem Strafverfahren mit im Internet öffentlich verfügbaren Daten automatisiert abgleichen können. Biometrische Daten sind alle Daten, die Rückschlüsse auf das Erscheinungsbild und andere physiologische Eigenschaften einer Person zulassen (zum Beispiel ein Foto oder eine Videoaufzeichnung). Damit soll es zum Beispiel möglich werden, ein Foto von einem Verdächtigen einer terroristischen Straftat mit öffentlich zugänglichen Social-Media-Bildern abzugleichen, um dessen Identität festzustellen.

2. Können Strafverfolgungsbehörden bisher keine Daten aus dem Internet abgleichen?

Bislang gibt es keine Rechtsgrundlage, die den automatisierten Abgleich von biometrischen Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten erlaubt. Nach geltender Rechtslage können im Internet öffentlich zugängliche biometrische Daten nur manuell, also ohne den Einsatz einer speziellen, für den Abgleich entwickelten Software, unter Einsatz gängiger Internet-Suchmaschinen mit vorhanden Daten aus einem Strafverfahren zur Sachverhaltsaufklärung abgeglichen werden.

3. Unter welchen Voraussetzungen soll der biometrische Internetabgleich möglich sein?

Der biometrische Internetabgleich soll nur bei dem Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung erlaubt sein. Diese Voraussetzung gilt auch für andere Ermittlungsmaßnahmen im Strafverfahrensrecht, beispielsweise für die Erhebung von Verkehrs- oder Mobilfunkdaten (§§ 100g, 100i der Strafprozessordnung – StPO). Dabei handelt es sich in der Regel um Straftaten mindestens des mittleren Kriminalitätsbereichs, die aufgrund der Umstände des Einzelfalls ein derartiges Gewicht aufweisen müssen, dass sie die mit der Maßnahme verbundenen Grundrechtseingriffe rechtfertigen. Dies ist insbesondere bei schweren Straftaten der Fall,

² Referentenentwurf des Bundesministeriums des Innern eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit und Referentenentwurf des Bundesministeriums des Innern eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus.

bei denen auch Maßnahmen wie die Telekommunikationsüberwachung nach § 100a StPO möglich wären. Der biometrische Internetabgleich soll nur zulässig sein, wenn die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre (Subsidiarität).

4. Wer soll einen biometrischen Internetabgleich durchführen dürfen?

Der Gesetzentwurf sieht vor, dass ein biometrischer Internetabgleich grundsätzlich nur durch eine Staatsanwältin oder einen Staatsanwalt angeordnet werden darf. In Eilfällen darf auch die Polizei selbst die Maßnahme anordnen, muss aber innerhalb von 48 Stunden eine Entscheidung der Staatsanwaltschaft einholen. Der biometrische Internetabgleich soll dann von der Strafverfolgungsbehörde selbst durchgeführt werden, d. h. in der Regel von der Polizei. Kann die Strafverfolgungsbehörde den automatisierten Internetabgleich technisch nicht selbst durchführen (zu den Anforderungen siehe Frage 5), können unter sehr engen Voraussetzungen im Wege der polizeilichen Rechtshilfe auch Stellen im Ausland um Unterstützung gebeten werden; dies wird im parallelen Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit des Bundesministeriums des Innern geregelt.

5. Wie soll der biometrische Internetabgleich durchgeführt werden?

Für die Durchführung des biometrischen Internetabgleichs muss aus dem Lichtbild der gesuchten Person zu deren biometrischen Merkmalen ein Template generiert werden. Entsprechende Vergleichsdatensätze müssen von den Lichtbildern aus dem Internet erstellt werden. Diese können dann abgeglichen werden. Nur ein sogenannter Ad-hoc Abgleich soll zulässig sein. Das heißt, dass die Vergleichsdatensätze nicht dauerhaft gespeichert werden dürfen, sondern für jeden Abgleich neu erstellt werden müssen. Die Erstellung einer dauerhaften Datenbank, die aus dem Internet erhobene Lichtbilder und/oder zugehörige Templates vorhält, ist damit ausgeschlossen.

II. Automatisierte Datenanalyse

1. Was schlägt das BMJV vor?

Strafverfolgungsbehörden sollen zukünftig zur Aufklärung einer Straftat in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte Daten mittels einer Software zur automatisierten Datenanalyse auswerten können. Bisher unverbundene Datenbanken der Polizei, die zum Beispiel Angaben aus anderen Strafverfahren oder polizeilichen Maßnahmen enthalten, sollen so mittels Suchfunktionen vernetzt und analysiert werden können.

2. Können Strafverfolgungsbehörden bisher nicht auf vorhandene Daten der Polizei zugreifen?

Gegenwärtig gibt es keine Rechtsgrundlage für den Betrieb von verfahrensübergreifenden Recherche- und Analyseplattformen zur Strafverfolgung. Bei der Polizei vorhandene Dateien und Datenquellen müssen für die Strafverfolgung im Rahmen einer aufwendigen Suche in einzelnen Datenbanken jeweils einzeln mit einer bestimmten Angabe abgeglichen werden. Dies bindet zum einen personelle Ressourcen, zum anderen birgt dies ein Risiko von Übertragungsfehlern, Informationsverlusten und paralleler Datenhaltung. Dies kann im Einzelfall dazu führen, dass wesentliche Anhaltspunkte für die Aufklärung der konkreten Straftat entweder nur mit hohem Personal- und Zeitaufwand gewonnen werden können oder dass sie überhaupt nicht erkannt werden. Dies soll der Einsatz verfahrensübergreifender Analyseplattformen verbessern.

3. Unter welchen Voraussetzungen soll die automatisierte Datenanalyse möglich sein?

Zum Einsatz soll die automatisierte Datenanalyse nur kommen dürfen, wenn der Verdacht einer auch im Einzelfall schwerwiegenden Straftat im Sinne von § 100a Absatz 2 StPO besteht. Das entspricht den Voraussetzungen der Telekommunikationsüberwachung (§ 100a Absatz 2 StPO).

Dazu zählen schwere Delikte wie Mord, Totschlag, bandenmäßiger Drogenhandel, schwere Steuerrückziehung, Raub oder Erpressung. Zudem dürfen Daten aus besonders sensiblen Ermittlungsmaßnahmen, wie zum Beispiel der Telekommunikationsüberwachung, nur in die Suche miteinbezogen werden, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die einzubeziehenden Daten in Verbindung zum konkreten Suchanlass stehen könnten. Die besonders sensiblen Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen dürfen gar nicht in die automatisierte Datenanalyse einbezogen werden.

4. Wer soll eine automatisierte Datenanalyse durchführen dürfen?

Die Strafverfolgungsbehörden sollen die automatisierte Datenanalyse unter den dargelegten Voraussetzungen selbstständig durchführen dürfen. Zur Gewährleistung von Kontrolle und Transparenz ist jeder Einsatz unter Darlegung der Voraussetzungen im Einzelfall zu begründen und zu protokollieren.

5. Wie soll die automatisierte Datenanalyse durchgeführt werden?

Der Gesetzentwurf enthält strenge Vorgaben für die Methodik, die bei der Software zur Recherche und Analyse angewendet werden darf. Die automatisierte Datenanalyse hat sich dabei darauf zu beschränken, in Datei- und Informationssystemen der Polizei gespeicherte Daten aufzuberei-

ten und bereitzustellen. Das Ergebnis der Weiterverarbeitung muss immer erkennen lassen, welche in den Datei- und Informationssystemen der Polizei gespeicherten Daten ihm aus welchem Grund zugrunde liegen, sodass von den ermittelnden Beamtinnen und Beamten eigene Bewertungen und Entscheidungen getroffen werden können. Die Anwendung darf auch nur aufgrund eines konkreten Anlasses erfolgen und anhand von Suchkriterien, die sich aus dem konkreten Sachverhalt ergeben. Offene Suchen nach Zusammenhängen „ins Blaue hinein“ sind damit ausgeschlossen. Der Einsatz der Software dient dazu, den Rechercheaufwand zu reduzieren, damit die Ermittlerinnen und Ermittler sich vorwiegend auf die eigentliche Analyse konzentrieren können. Die Ermittlerinnen und Ermittler sollen in die Lage versetzt werden, mittels einer einheitlichen Software die rechtmäßig in den Datei- und Informationssystemen der Polizei gespeicherten Daten umfassend, schnell und effizient durch eine Vielzahl zeitgleich ausgeführter Datenabgleiche auf Querverbindungen zum eigenen Strafverfahren zu untersuchen. Bewertungen und Entscheidungen auf Grundlage dieser Erkenntnisse werden ausschließlich von den Beamtinnen und Beamten getroffen.

6. Soll auch der Einsatz von Künstlicher Intelligenz (KI) ermöglicht werden?

Im Rahmen der in dem Gesetzentwurf definierten Grenzen für den Einsatz einer Recherche- und Analysesoftware (siehe Frage 5) ist grundsätzlich auch der Einsatz von KI-Anwendungen möglich. Die Methodik der automatisierten Anwendung zur Datenverarbeitung muss sich aber weiterhin darauf beschränken, in Datei- und Informationssystemen der Polizei gespeicherte Daten aufzubereiten und bereitzustellen, die es den Strafverfolgungsbehörden ermöglichen, eigene Bewertungen und Entscheidungen zu treffen. Das Ergebnis der Weiterverarbeitung muss immer erkennen lassen, welche in den Datei- und Informationssystemen der Polizei gespeicherten Daten ihm aus welchem Grund zugrunde liegen. Eine ausschließlich auf der Datenanalyse beruhende automatisierte Entscheidungsfindung ist ausgeschlossen.