Digitale Ermittlungsmaßnahmen: Häufige Fragen

I. Biometrischer Internetabgleich

1. Worauf zielt der Gesetzentwurf?

Der Gesetzentwurf sieht eine Anpassung der Strafprozessordnung vor: Strafverfolgungsbehörden sollen die Befugnis erhalten, unter gewissen Voraussetzungen einen sogenannten biometrischen Internetabgleich durchzuführen.

2. Was ist ein biometrischer Internetabgleich?

Bei einem biometrischen Internetabgleich werden biometrische Daten, die bei den Strafverfolgungsbehörden vorhanden sind, automatisiert mit im Internet öffentlich verfügbaren biometrischen Daten abgeglichen. Biometrische Daten sind alle Daten, die Rückschlüsse auf das Erscheinungsbild und andere physiologische Eigenschaften einer Person zulassen (zum Beispiel ein Foto oder eine Videoaufzeichnung).

Ein biometrischer Internetabgleich kann den Zweck haben, einen Sachverhalt aufzuklären, die Identität oder den Aufenthaltsort eines Beschuldigten oder Zeugen festzustellen. Ein biometrischer Internetabgleich liegt zum Beispiel vor, wenn ein Foto von einem Verdächtigen einer terroristischen Straftat mit öffentlich zugänglichen Social-Media-Bildern abgeglichen wird, um dessen Identität festzustellen.

3. Wie ist die geltende Rechtslage in Bezug auf den biometrischen Internetabgleich?

Bislang dürfen Strafverfolgungsbehörden keinen automatisierten biometrischen Internetabgleich durchführen: Es gibt bislang keine gesetzliche Regelung, die Strafverfolgungsbehörden den automatisierten Abgleich von biometrischen Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten erlaubt.

Nach geltender Rechtslage können Ermittler im Internet öffentlich zugängliche biometrische Daten nur manuell durchsuchen, beispielsweise unter Einsatz gängiger Internet-Suchmaschinen, um sie mit vorhanden Daten aus einem Strafverfahren abzugleichen.

4. Unter welchen Voraussetzungen soll der biometrische Internetabgleich künftig angeordnet werden dürfen?

Die Durchführung eines biometrischen Internetabgleich soll nur dann zulässig sein, wenn der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung besteht. Diese Voraussetzung gilt auch für andere Ermittlungsmaßnahmen im Strafverfahrensrecht, beispielsweise für die Erhebung von Verkehrs- oder Mobilfunkdaten (§§ 100g, 100i der Strafprozessordnung – StPO).

Die Durchführung des biometrischen Internetabgleichs soll darüber hinaus voraussetzen, dass die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre (Subsidiarität).

5. Auf welche Daten soll beim biometrischen Internetabgleich zugegriffen werden dürfen?

Für den Abgleich sollen nur solche Daten herangezogen werden dürfen, die im Internet öffentlich zugänglich sind: Also solche Daten, auf die jedermann zugreifen kann, beispielsweise aus sozialen Medien (je nach Privatsphäre-Einstellungen). Nicht umfasst sind hingegen Daten, die nur bestimmten Personengruppen zugänglich sind, beispielsweise Daten in sozialen Medien, die nur für die Kontakte einer Person bestimmt sind. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden. Auch Echtzeitdaten, wie beispielsweise Live-Streams, können und dürfen hierbei nicht erfasst werden.

6. Wer soll einen biometrischen Internetabgleich anordnen und 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), kann unter sehr engen Voraussetzungen über das Bundeskriminalamt als Zentralstelle

eine Zusammenarbeit mit Stellen im Ausland erfolgen; dies wird im parallelen Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit des Bundesministeriums des Innern geregelt.

7. 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. Das ist ein Vektordatensatz, aus dem sich die Abstände zwischen Gesichtsmerkmalen ergeben, die für die Identifikation wesentlich sind. Entsprechende Vergleichsdatensätze müssen von den Lichtbildern aus dem Internet erstellt werden. Diese können dann abgeglichen werden. Von den Strafverfolgungsbehörden werden überhaupt nur die Daten derjenigen Personen registriert, zu denen ein Treffer vorliegt.

8. Was passiert nach der Durchführung des Internetabgleichs mit den zum Abgleich herangezogenen öffentlichen Daten? Dürfen die Daten in einer dauerhaften Datenbank gespeichert werden?

Nein, die Erstellung einer dauerhaften Datenbank mit aus dem Internet erhobenen Daten (Lichtbildern und/oder zugehörigen Templates) ist ausgeschlossen. Der Gesetzentwurf schreibt ausdrücklich vor, dass die zum Abgleich erhobenen biometrischen Daten nach der Durchführung des Abgleichs unverzüglich gelöscht werden müssen. Erlaubt ist somit nur ein sogenannter Ad-hoc-Abgleich: Das heißt, dass die Vergleichsdatensätze für jeden Abgleich neu erstellt werden müssen.

9. Wie ist sichergestellt, dass die Grundrechte von Bürgerinnen und Bürgern durch den vorgesehenen Datenabgleich nicht verletzt werden?

Der vorgesehene Internetabgleich soll nur unter strengen Voraussetzungen zulässig sein: Es muss der Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung bestehen; zudem darf es im konkreten Fall keine praktikable Alternative geben zum Datenabgleich. Darüber hinaus ist vorgeschrieben, dass die für den Datenabgleich herangezogenen öffentlichen Daten nach Durchführung des Datenabgleichs sofort gelöscht werden müssen, wenn es keinen Treffer gibt. Von den Strafverfolgungsbehörden werden überhaupt nur diejenigen Daten registriert, zu denen ein Treffer vorliegt.

10. Besteht das Risiko, dass ein Datenabgleich „falsche Treffer“ produziert – und es somit zu Fehlurteilen kommt?

Wenn der Datenabgleich einen Treffer ergibt, dann ist das zunächst lediglich der Anlass für die Strafverfolgungsbehörden, den Treffer zu verifizieren. Nur wenn die Staatsanwaltschaft hinreichend überzeugt von der Identität ist, wird sie Anklage erheben. Damit es zu einer Verurteilung kommen kann, muss am Ende das Strafgericht überzeugt sein, dass die durch einen Abgleich identifizierte Person tatsächlich der Täter der angeklagten Straftat ist. Es gilt – wie in jedem Strafverfahren – der Grundsatz „im Zweifel für den Angeklagten“.

II. Automatisierte Datenanalyse

1. Worauf zielt der Gesetzentwurf?

Der Gesetzentwurf sieht eine Anpassung der Strafprozessordnung vor: Strafverfolgungsbehörden sollen die Befugnis erhalten, unter gewissen Voraussetzungen und innerhalb bestimmter Grenzen eine automatisierte Datenanalyse vorzunehmen.

2. Was ist ein automatisierte Datenanalyse im Sinne des Gesetzentwurfs?

Bei der automatisierten Datenanalyse geht es um die Auswertung von rechtmäßig gespeicherten Daten durch die Strafverfolgungsbehörden: Bisher unverbundene Datenbanken der Polizei sollen mit einer speziellen Software vernetzt und analysiert werden können. Es geht zum Beispiel um Angaben aus Strafverfahren oder polizeilichen Maßnahmen. Der Einsatz der Software dient dazu, den Rechercheaufwand zu reduzieren; die Ermittlerinnen und Ermittler sollen in die Lage versetzt werden, die vorhandenen Daten auf Querverbindungen zum eigenen Strafverfahren zu untersuchen. Die automatisierte Datenanalyse soll dem Zweck der Aufklärung von Straftaten dienen. Bewertungen und Entscheidungen auf Grundlage dieser Erkenntnisse werden ausschließlich von den Beamtinnen und Beamten getroffen.

3. **Wie ist die geltende Rechtslage in Bezug auf automatisierte Datenanalyse?**

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 bestimmen 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.

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

Die automatisierte Datenanalyse soll nur eingesetzt werden 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 beispielsweise schwere und besonders schwere Delikte wie Mord, Totschlag, bandenmäßiger Drogenhandel, schwere Steuerhinterziehung, 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.

5. 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.

6. 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 ge-

speicherte Daten aufzubereiten 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. So können die ermittelnden Beamtinnen und Beamten auf Grundlage der aufbereiteten Daten eigene Bewertungen und Entscheidungen treffen. 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.

7. 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 vorangegangene Frage) 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, um so den Strafverfolgungsbehörden zu 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.

8. Wie wird sichergestellt, dass der Datenschutz gewahrt bleibt?

Die rechtlichen Grenzen der Speicherung und Durchsuchbarkeit von Daten bleiben unverändert, weil die gesetzlichen Vorgaben für die Verarbeitung personenbezogener Daten trotz der Zusammenführung fortgelten und zwingend technisch in das verwendete System zur Datenanalyse zu implementieren sind.

9. Welche Software soll für die automatisierte Datenanalyse zum Einsatz kommen?

Es darf nur solche Software zum Einsatz kommen, die den gesetzlichen Vorgaben genügt. Mit der Schaffung der Rechtsgrundlage ist noch nicht die Entscheidung über den Einsatz bestimmter Software verbunden.

III. Änderungen im Regierungsentwurf

Was hat sich gegenüber dem Referentenentwurf geändert?

Die wenigen Änderungen betreffen im Wesentlichen technische Aspekte. Insbesondere die Protokollierungspflichten wurden noch weiter konkretisiert. Zur Transparenz sollen die Bezeichnung der automatisierten Anwendung zur Datenverarbeitung und der Zeitpunkt ihres Einsatzes, die einbezogenen Daten und die Organisationseinheit, die die Maßnahme durchführt, protokolliert werden.