



## **Stellungnahme der Gewerkschaft der Polizei (GdP)**

zum Referentenentwurf des  
Bundesministeriums der Justiz und für Verbraucherschutz

### **Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen**

Berlin, 01.04.2026  
Abt. Innenpolitik | 31, AL3

## I. - Vorbemerkung

Der Entwurf eines Gesetzes zur Änderung der Strafprozessordnung zu digitalen Ermittlungsmaßnahmen greift ein praktisches und sicherheitspolitisch nachvollziehbares Bedürfnis der Strafverfolgungsbehörden auf. Die fortschreitende Digitalisierung, die Verlagerung relevanter Spuren in den digitalen Raum sowie die zunehmende Bedeutung datenbasierter Ermittlungsansätze machen es erforderlich, den Strafverfolgungsbehörden Instrumente zur Verfügung zu stellen. Dies gilt sowohl für den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet als auch für die automatisierte verfahrensübergreifende Datenanalyse. Der Entwurf verfolgt damit ein legitimes Ziel: Schwere Straftaten wirksamer aufzuklären, Personen schneller zu identifizieren oder aufzufinden und bestehende polizeiliche Datenbestände im Interesse einer effektiven Strafverfolgung intelligenter und strukturierter nutzbar zu machen.

Für die Beschäftigten in Polizei und Strafverfolgung kommt es dabei nicht allein auf die Schaffung neuer Befugnisse an. Entscheidend ist vielmehr, dass diese Befugnisse im Vollzug rechtssicher, praxistauglich und gerichtsfest ausgestaltet werden. Unklare Eingriffsschwellen, unklare Begriffe, unzureichend strukturierte Verfahrensregeln oder technisch nicht hinreichend eingetragene Anwendungen führen in der Praxis nicht zu mehr Sicherheit, sondern zu Rechtsunsicherheit, zusätzlichem Rechtfertigungsdruck, erhöhtem Dokumentationsaufwand, Beweisverwertungsrisiken und letztlich auch zu Belastungen unserer eingesetzten Kolleg:innen. Die Aufgabe des Gesetzgebers besteht deshalb nicht nur darin, neue Ermittlungsinstrumente zu eröffnen, sondern diese so zu normieren, dass ihre Anwendung nachvollziehbar, kontrollierbar und in gerichtlichen Verfahren belastbar bleibt.

Die Gewerkschaft der Polizei (GdP) - mit über 210.000 Mitgliedern größte Polizeigewerkschaft hierzulande - begrüßt diesen richtigen und wichtigen Schritt und bedankt sich für die Gelegenheit zu diesem sicherheitspolitisch wichtigen Vorhaben Stellung zu nehmen.

## II. - Zum Vorhaben

Das Vorhaben betrifft aus Sicht der GdP einen Bereich von besonderer rechtlicher, tatsächlicher und sicherheitspolitischer Sensibilität. Soweit digitale Ermittlungsmaßnahmen den Umgang mit biometrischen Merkmalen sowie die Zusammenführung und Auswertung umfangreicher personenbezogener Datenbestände ermöglichen, geht es nicht um beliebige Informationen, sondern um Daten, die in besonderer Weise identitätsbezogen, persönlichkeitsrelevant und schutzbedürftig sind. Die diesem Vorhaben zugrunde liegende fachliche Diskussion weist zutreffend darauf hin, dass es sich bei biometrischen Daten um besonders geschützte Kategorien personenbezogener Daten handelt und dass ihr Einsatz mit einem erheblichen Grundrechtseingriff verbunden sein kann.

Diese besondere Sensibilität ist aus unserer Sicht ausdrücklich anzuerkennen und muss den weiteren gesetzgeberischen Umgang mit dem Vorhaben prägen. Eine Polizei, die sich für wirksame und moderne Ermittlungsbefugnisse einsetzt, verkennt nicht, dass der Staat hier in einen Bereich eingreift, in dem Datensicherheit, Vertraulichkeit, Integrität und strikte Zweckbindung keine bloßen Begleitfragen sind. Sie sind tragende Voraussetzungen staatlicher Legitimität. Je näher Daten an die Identität einer Person heranreichen und je umfassender sie technisch

verknüpft, ausgewertet oder für Folgemaßnahmen nutzbar gemacht werden können, desto höher sind die Anforderungen an ihren Schutz. Das gilt in besonderem Maße dort, wo aus einzelnen Treffern oder Datenfragmenten weitergehende Erkenntnisse gewonnen werden könnten.

Neue digitale Ermittlungsmaßnahmen können nur dann Akzeptanz beanspruchen, wenn gesetzlich und organisatorisch sichergestellt ist, dass sensible Daten ausschließlich anlassbezogen, streng zweckgebunden, nachvollziehbar und in einem auf das absolut Erforderliche beschränkten Umfang verarbeitet werden. Gerade aus Sicht der GdP ist dies kein Hemmnis effektiver Strafverfolgung, sondern ihre Voraussetzung.

Der vorliegende Entwurf enthält insoweit wichtige Ansatzpunkte, die aus unserer Sicht in ihrer Bedeutung ausdrücklich hervorgehoben werden sollten. Positiv ist, dass die erhobenen Inter- netdaten nur temporär als Referenzdaten für das konkrete Ermittlungsverfahren gespeichert werden dürfen und eine weitergehende Nutzung ausgeschlossen sein soll. Ebenso ist es sachgerecht, dass Daten nach Durchführung des Abgleichs unverzüglich zu löschen sind, soweit sie keinen konkreten Ermittlungsansatz aufweisen, und dass die Löschung aktenkundig zu machen ist. Hinzu treten Protokollierungspflichten sowie die vorgesehene Unterrichtung der für die Datenschutzkontrolle zuständigen Stelle.

Aus Sicht der GdP ist hervorzuheben, dass digitale Ermittlungsinstrumente stets nur unterstützende Werkzeuge sein dürfen. Sie können polizeiliche Bewertung und Entscheidungsfindung vorbereiten, strukturieren und erleichtern, sie aber nicht ersetzen. Am Ende muss die Verantwortung für die Bewertung eines Sachverhalts und für daraus folgende Maßnahmen immer bei dem handelnden Menschen verbleiben.

Für Polizei und Strafverfolgung ist dies auch aus praktischen Gründen von erheblicher Bedeutung. Ein unzureichend abgesicherter Umgang mit hochsensiblen Daten schafft nicht nur Risiken für Betroffene, sondern auch erhebliche Belastungen für die vollziehenden Behörden selbst. Wo Datensicherheit und klare Verarbeitungsgrenzen nicht hinreichend gewährleistet sind, entstehen Rechtsunsicherheit, zusätzlicher Legitimationsdruck und die Gefahr späterer Beanstandungen durch Gerichte oder Aufsichtsstellen. Umgekehrt stärkt ein datensicher ausgestalteter Rechtsrahmen die Verlässlichkeit polizeilichen Handelns und das Vertrauen in den Rechtsstaat. Er schützt sensible Informationen vor unkontrollierter Verwendung, stärkt die Verfahrenssicherheit und sichert zugleich die Akzeptanz moderner Ermittlungsmaßnahmen in einer rechtsstaatlichen Ordnung. Gerade deshalb sollte das Vorhaben erkennbar von dem Leitgedanken getragen sein, dass mit besonders sensiblen Daten nur unter besonders hohen Anforderungen an Schutz, Sicherheit und Begrenzung gearbeitet werden darf.

Aus Sicht der GdP gehört zur rechtssicheren und praxistauglichen Ausgestaltung digitaler Ermittlungsbefugnisse jedoch nicht nur eine klare gesetzliche Ermächtigungsgrundlage, sondern auch eine belastbare, souveräne und sicherheitsgerechte technische Umsetzungsarchitektur. Wo der Gesetzgeber auf digitale Ermittlungsinstrumente und Analyseplattformen abstellt, muss zugleich sichergestellt sein, dass diese Systeme dauerhaft unter behördlicher Kontrolle stehen, höchsten Anforderungen an Datensicherheit und Vertraulichkeit genügen und nicht in technische oder organisatorische Abhängigkeiten führen, die dem Anspruch staatlicher Souveränität widersprechen.

### III. - Im Einzelnen

#### Artikel 1 – Änderung der Strafprozessordnung

##### **98d StPO-E: Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet**

Die vorgesehene Regelung zum automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet ist aus Sicht der GdP zu begrüßen. Der Gesetzgeber trägt damit dem praktischen Bedarf Rechnung, moderne technische Möglichkeiten zur Sachverhaltsaufklärung, Identitätsfeststellung und Aufenthaltsortermittlung nutzbar zu machen. Gerade bei schweren Straftaten kann ein solches Instrument Ermittlungen wirksam unterstützen.

Positiv ist, dass der Entwurf die Maßnahme an qualifizierte Voraussetzungen bindet und sie auf gewichtige Sachverhalte beschränkt. Ebenso ist es sachgerecht, dass sie subsidiär ausgestaltet ist und damit nur dann zur Anwendung kommt, wenn andere Ermittlungsansätze wesentlich erschwert oder aussichtslos wären.

Zu begrüßen ist ferner die Begrenzung auf öffentlich zugängliche Internetdaten. Damit wird deutlich, dass zwischen allgemein zugänglichen digitalen Inhalten und geschützten privaten Kommunikations- und Rückzugsräumen unterschieden wird. Auch der Ausschluss von Echtzeitdaten unterstreicht den eng begrenzten Charakter der Vorschrift.

Von besonderer Bedeutung ist schließlich, dass die Regelung den Umgang mit biometrischen Daten betrifft und damit mit Daten von besonderer Sensibilität. Umso wichtiger ist es, dass der Entwurf auf Zweckbindung, Begrenzung, Löschung und Protokollierung abstellt. Die vorgesehene verfahrensbezogene Nutzung der Referenzdaten sowie die unverzügliche Löschung nicht weiter benötigter Daten sind vor diesem Hintergrund richtige und wichtige Ansätze.

##### **§ 98e StPO-E: Automatisierte verfahrensübergreifende Datenanalyse**

Auch die vorgesehene Regelung zur automatisierten verfahrensübergreifenden Datenanalyse ist aus Sicht der GdP zu begrüßen. Moderne Strafverfolgung ist gerade in schweren und komplexen Verfahren zunehmend darauf angewiesen, rechtmäßig vorhandene Datenbestände strukturiert, sachverhaltsbezogen und technisch unterstützt auszuwerten. Recherche- und Analyseplattformen können dabei helfen, verfahrensübergreifende Zusammenhänge früher zu erkennen, relevante Hinweise zusammenzuführen und Ermittlungen zielgerichteter zu führen.

Zugleich ist hervorzuheben, dass es sich auch hierbei um einen besonders sensiblen Bereich handelt. Die Zusammenführung und Auswertung unterschiedlicher Datenbestände kann die Eingriffsintensität erheblich steigern und macht deshalb einen klaren rechtlichen, technischen und organisatorischen Rahmen erforderlich. Positiv ist insoweit, dass der Entwurf die Datenanalyse an qualifizierte Voraussetzungen knüpft, sie auf rechtmäßig gespeicherte Daten bezieht, offene anlasslose Suchen ausschließt und verdeutlicht, dass die Analyseplattform die Arbeit der Strafverfolgungsbehörden unterstützen, aber nicht eigenständig ersetzen soll.

Von besonderer Bedeutung ist aus unserer Sicht der Schutz sensibler Daten. Gerade bei verfahrensübergreifenden Analyseplattformen sind Datensicherheit, Zweckbindung, Zugriffsbe-

grenzung, Protokollierung und organisatorische Absicherung von zentraler Bedeutung. Es ist daher ausdrücklich zu begrüßen, dass der Entwurf Begründungs- und Protokollierungspflichten vorsieht, die Rechte der Betroffenen und die geltenden datenschutzrechtlichen Verwendungsregelungen unberührt lässt und deren Einhaltung technisch und organisatorisch sicherstellen will. Auch die ausdrückliche Zielsetzung, diskriminierende Algorithmen weder herauszubilden noch zu verwenden, ist im Hinblick auf die rechtsstaatlich verantwortbare Ausgestaltung hervorzuheben.

Zentral ist aus unserer Sicht zudem, dass die praktische Nutzbarkeit entscheidend davon abhängt, dass auf Seiten der Länder und des Bundes spiegelbildliche Befugnisse in den jeweiligen Polizeigesetzen geschaffen werden. Nur wenn die gesetzlichen Grundlagen dort entsprechend ausgestaltet werden, können für Zwecke der Gefahrenabwehr zusammengeführte Daten unter den vorgesehenen Voraussetzungen auch für Zwecke der Strafverfolgung nutzbar gemacht werden.