# Verbotene Früchte und der Gesetzesvorbehalt in polizeilichen Ermittlungsverfahren

VB verfassungsblog.de/pimeyes-user-auf-raf-spuren/


Marc Bovermann

Johanna Fink

Jakob Mutter
22 March 2024

## PimEyes User auf den Spuren der RAF

„Die Staatsanwaltschaft Verden und das Landeskriminalamt Niedersachsen bitten um Ihre Mithilfe!“ So betitelt das Bundeskriminalamt seine Fahndungsaufrufe nach den Ex-RAF-Terroristen Garweg und Staub. Hinweise, die zu ihrer Ergreifung führen, sollen mit mindestens 150.000 Euro entlohnt werden. Die Ex-Komplizin Klette der beiden war bereits Ende Februar gefasst worden. Soweit bekannt hatten Private den Behörden die entscheidenden Hinweise gegeben. Hinweise, an die zuvor ein Journalist mittels der Gesichtserkennungssoftware “PimEyes” gelangt war – allerdings unter Verstoß gegen das Datenschutzrecht. Verfassungsrechtlich erscheint es außerdem problematisch, wenn die Polizei derart erhobene Informationen für ihre Ermittlungen verwendet, denn sie selbst dürfte PimEyes nicht einsetzen. Dazu bräuchte es wegen des Gesetzesvorbehalts eine hinreichende Ermächtigungsgrundlage. Eine solche fehlt derzeit. Und trotzdem ziehen diese problematischen Aspekte letztlich keinerlei Konsequenzen für die polizeilichen Ermittlungen nach sich. Die US-amerikanische Doktrin der „fruit of the poisonous tree”, die es Gerichten verbietet, rechtswidrig erhobene Beweise zu verwerten, wird hierzulande überwiegend abgelehnt, insbesondere von der Rechtsprechung. Entsprechendes gilt wegen des Verhältnismäßigkeitsgrundsatzes im Gefahrenabwehrrecht.

## PimEyes‘ problematisches Geschäftsmodell

PimEyes ist eine Gesichtserkennungssoftware, die mittels umgekehrter Bildsuche das Internet durchforscht, um den Namen der abgebildeten Person und andere Bilder von ihr zu finden. Zwar beschreibt das Unternehmen auf seiner Website lediglich, Nutzer:innen könnten eigene Bilder hochladen, um zu überprüfen, was für Bilder noch von ihnen im Internet

kursieren. Allerdings ist es problemlos möglich, auch Bilder anderer hochzuladen. Und das wird vermutlich auch nicht selten getan. Denn bei Erstellung eines kostenpflichtigen Kontos "Advanced" können unbegrenzt viele Suchaufträge durchgeführt werden. Und wer braucht das nur für die Suche nach eigenen Fotos?

PimEyes greift für die Bildsuche auf praktisch alle Bilder, die im Netz kursieren, zu. Hierdurch stellt die Gesichtserkennungstechnologie ein integriertes Informationssystem her, das biometrische Daten der Betroffenen aus unterschiedlichen Quellen umfassend zusammenfügt und sie ohne ihre Einwilligung in einer für sie nicht kontrollierbaren Weise online eindeutig erfassbar macht. Damit verstößt die Software gegen Art. 5 Abs. 1 lit. a-f, Art. 9 Abs. 1 i.V.m. Art. 4 Nr. 11 der Datenschutz-Grundverordnung (DSGVO). Da die Betroffenen wohl eher nicht damit rechnen, dass eine Software Bilder, die im Internet von ihnen kursieren, auswertet, liefern sie die biometrietauglichen Rohdaten meist unwissend. Deshalb liegt auch keine Erlaubnis nach Art. 9 Abs. 2 DSGVO durch willentliche, offensichtliche Veröffentlichung der Bilder für die biometrische Auswertung vor. Bereits die Datenerhebung, die private Nutzer:innen durch die Bildsuche in Gang setzen, ist somit rechtswidrig.

Nutzt nun die Polizei selbst die Technologie, ist zwar die DSGVO nicht anwendbar (Art. 2 Abs. 2 lit. d DSGVO). Jedoch steht der Nutzung von privat kontrollierten Datenbanken durch die Polizeibehörden die speziellere JI-Richtlinie entgegen, namentlich ihre Art. 4 Abs. 1 lit. 1, d, e, f, Art. 10 lit. c. Dass die Richtlinie anwendbar wäre, ergibt sich aus ihrem Art. 3 Nr. 8: Denn wenn die Polizei Bildmaterial der Zielperson auf die Server von PimEyes hochlädt, verarbeitet sie als "Verantwortlicher" personenbezogene Daten.

Darüber hinaus bestehen auch verfassungsrechtliche Bedenken. Wer Bilder anderer auf PimEyes hochlädt, verletzt deren informationelles Selbstbestimmungsrecht (Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG) und ihr Recht auf Schutz personenbezogener Daten (Art. 8 Abs. 1 EU-Grundrechtecharta). Daneben birgt die Technologie aufgrund zuweilen auftretender Fehlerprognosen eine starke Diskriminierungsgefahr, weshalb auch Verstöße gegen Art. 3 Abs. 1 GG denkbar sind.

## Gesichtserkennungssoftware dennoch bereits im Einsatz

Eine Nutzung privater Gesichtserkennungsinternetsuchprogramme wie PimEyes durch deutsche Polizeibehörden wäre somit rechtswidrig und erfolgt aktuell (jedenfalls offiziell) noch nicht. Allerdings kooperiert PimEyes seit einigen Jahren mit dem schwedischen Unternehmen Safer Society. Dieses hat PimEyes in seine eigene Software Paliscope integriert, die Überwachungstechnik für Gefahrenabwehrbehörden bereitstellt. Zu den Kund:innen von Safer Society zählt auch die europäische Polizeibehörde Europol.

Zudem werden bereits nicht-internetbasierte, KI-gestützte Gesichtserkennungstechnologien erprobt. Die bekannteste ist wohl das Gesichtserkennungssystem des BKA, mit dem es seit 2007 unbekannte Täter identifiziert. Die Software vergleicht das Bildmaterial des Gesuchten

mit den im zentralen Informationssystem der Polizei schon aufgenommenen Porträtbildern von Straftätern. Danach werden die erzielten Ergebnisse allerdings noch von Menschen verifiziert. Im Gegensatz zu PimEyes läuft die Suche also nicht vollständig automatisiert ab. Zudem wird nur auf bereits vorhandene Bilder von Straftätern und nicht auf Bilder aus Internetquellen zugegriffen.

## Private Hinweise und Ermittlungen zur Gefahrenabwehr

Neben digitalen Hilfsmitteln nutzt die Polizei seit jeher Hinweise aus der Bevölkerung bei der erkennungsdienstlichen Suche. Tatsächlich scheint sie hierauf oft angewiesen zu sein, wie die Festnahme Klettes zeigt. Vor diesem Hintergrund erscheint es zunächst einmal sachgerecht, dass die Polizei private Hinweise zur Ermittlung nutzen kann. Gleichwohl verwendet die Polizei illegal erlangte Daten, die sie selbst so nicht erheben dürfte. Letztlich kann dies im Ergebnis aber regelmäßig keine Konsequenzen für die Verwendung dieser Hinweise in der gefahrenabwehrrechtlichen Ermittlung haben.

Die Polizei darf private Indizien regelmäßig verwenden, wenn deren Kenntnis zur Aufgabenerfüllung erforderlich ist. Allerdings kann das verfassungsrechtlich normierte Verhältnismäßigkeitsgebot, an das staatliche Behörden stets gebunden sind (Art. 1 Abs. 3, 20 Abs. 3 GG), hier Grenzen setzen. Die Nutzung datenschutzwidrig erlangter Indizien, die Private erhoben haben, könnte polizeiliche Ermittlungsmaßnahmen daher von vornherein als unverhältnismäßig erscheinen lassen. Dabei ist auch zu bedenken, dass das Polizeirecht die Gefahrenabwehrbehörden auf präzise, eng gefasste Ermittlungsgrundlagen verweist. Wenn die Polizei mittels prämierter Fahndungsaufrufe die Bevölkerung zur Mithilfe anreizt, besteht die Gefahr, dass Private die Ermittlungsarbeit der Polizei „vom Sofa aus" unterstützen. Die parlamentarisch legitimierten, eng gefassten Voraussetzungen für staatliche Grundrechtseingriffe würden umgangen und sonst rechtlich unzulässige staatliche Ermittlungsmethoden könnten sich in ein "Recht der Privaten" flüchten – trotz der dortigen Verbote (s. o.).

Für die Verhältnismäßigkeit spricht indes, dass der polizeiliche Schutzauftrag (Art. 2 Abs. 2 GG) bei Vorliegen einer akuten Gefahr stets überwiegt. Wurde ein Indiz rechtswidrig erlangt, führt dies zudem *ipso iure* zur zivil- oder sogar strafrechtlichen Verantwortlichkeit des an der Ermittlung mitwirkenden Diensteanbieters oder Nutzers. Diejenigen, in deren Rechte durch die Bildsuche eingegriffen wurde, stehen somit nicht schutzlos da. Eine Abwägung des privaten Datenschutzverstoßes gegen die Abwehr von Gefahren für hochrangige Rechtsgüter wie Leib und Leben, z.B. bei einem möglichen Raubüberfall durch Ex-RAFler, führt daher regelmäßig zum Ergebnis, dass die Gefahrenabwehr angemessen ist.

## Private Hinweise in der strafprozessualen Ermittlung

Auch strafprozessual zeigt die Verwendung der von Privaten bei PimEyes abgerufenen Daten im Ermittlungsverfahren wohl keine Konsequenzen – sogar unter der Prämisse, dass die erlangten Daten in einem Hauptverfahren einem Beweisverwertungsverbot unterliegen.

Privat ermitteltes Material kann (und muss) die Staatsanwaltschaft nach § 160 Abs. 1, 2 StPO grundsätzlich verwenden. Ihre Ermittlungspflicht beginnt nach § 152 Abs. 2 StPO, wenn ein Anfangsverdacht vorliegt. Es müssen zureichende tatsächliche Anhaltspunkte vorliegen, die dafür sprechen, dass eine Straftat begangen wurde. Dieser Standard ist mit dem Polizeirecht vergleichbar (s. o.).

Wird ein Beweismittel rechtswidrig erlangt, wirkt sich dies nach herrschender Meinung prinzipiell nicht auf das Ermittlungsverfahren aus (s. etwa Bundesverfassungsgericht, Beschl. v. 30.06.2005, 2 BvR 1502/04). Deutsche Gerichte lehnen einen Ansatz, der mit der US-amerikanischen „fruit of the poisonous tree doctrine“ vergleichbar wäre, ab. Faktisch führt dies dazu, dass auch ein Beweismittel, das jemand in verbotener Weise erhoben hat, einen Anfangsverdacht begründen und Grundlage von Ermittlungsmaßnahmen sein kann.

Allerdings ist bei der Begründung eines Anfangsverdachts eine Abwägung zwischen der Schwere des Rechtsverstoßes und der Schwere der verfolgten Tat vorzunehmen (vgl. Bundesgerichtshof, Urt. v. 22.02.1978, 2 StR 334/77 oder *Peters* in MüKo-StPO, § 152 Rn. 48). Danach ist ein Anfangsverdacht zu verneinen, wenn die Schwere des Rechtsverstoßes die Schwere der verfolgten Tat überwiegt.

Dies hat Konsequenzen für die Zulässigkeit jener Ermittlungsmaßnahmen, die auf Beweise gestützt werden, die Private rechtswidrig erhoben haben. Die Ermittlungsmaßnahmen setzen nämlich mindestens einen Anfangsverdacht voraus. Wiegt der Rechtsverstoß, den die Privatperson bei der Beweiserhebung begangen hat, schwerer als die verfolgte Tat, dürfen sich an den Verdachtsmoment keine Ermittlungsmaßnahmen anschließen. Gleiches gilt allerdings auch für den Fall, in dem ein Anfangsverdacht zwar bereits aus anderen Gründen besteht, jedoch nur das rechtswidrig erhobene Beweismittel eine sich hieran anschließende Ermittlungsmaßnahme zu begründen vermag. Spürt eine Privatperson Garweg und Staub mithilfe von PimEyes auf, gelten dieselben Maßstäbe wie für den Fall, dass ein Privater CDs mit illegal erlangten Nachweisen über die Steuerhinterziehung an die Polizei verkauft.

Freilich ist die Frage, inwieweit die Strafverfolgungsbehörden rechtswidrig erhobene Beweise im Ermittlungsverfahren verwenden dürfen letztlich von der Auflösung der obigen Prämisse, dass ein Beweisverwertungsverbot besteht, abhängig. Hier ist jedenfalls die Rechtsprechung sehr lax, da Rechtsverstöße Privater nur in Extremfällen (etwa bei Folter) zu Beweisverwertungsverboten führen (siehe instruktiv Verfassungsgerichtshof Rheinland-Pfalz, Urt. v. 24.02.2014, VGH B 26/13 zur Verwertbarkeit von Steuerdaten-CDs). Die Verwendung von Informationen, die PimEyes auswirft, stellt vor diesem Hintergrund eher keinen Fall eines Beweisverwertungsverbotes dar. Ein anderes Ergebnis lässt sich allerdings mit verfassungs- und unionsrechtlichen Gründen gut vertreten (s. hier).

## Fazit

Letztlich spricht vieles dafür, dass im gefahrenabwehrrechtlichen wie im strafprozessualen Ermittlungsverfahren mit Beweisen, die Private erhoben haben, ähnlich umzugehen ist: Ein Datenschutzverstoß seitens privater Hinweisgeber „infiziert“ die Informationsverwertung der staatlichen Behörden in aller Regel nicht. Ob dies in Extremfällen genauso gilt, kann man aber gerade bei der (repressiven) Strafverfolgung durchaus in Frage stellen. Dass die Polizei einen Hinweis zu einer gegenwärtigen Gefahr für ein besonders gewichtiges Rechtsgut einfach ignorieren muss, scheint allerdings schwer hinnehmbar.

In jedem Fall wirft der Fall Klette wichtige Fragen zur Mitwirkung Privater in sicherheitsrechtlichen Abläufen auf. Dieser in der Polizeipraxis sehr wichtige Bereich muss rechtlich besser eingehegt werden. Die Digitalisierung bewirkt, dass es auch Privatpersonen möglich ist, die Rolle eines polizeilichen Ermittlers einzunehmen. Kommen noch Anreize wie die ausgeschriebenen Belohnungen hinzu, droht ein Szenario, das an die funktionale Privatisierung erinnert: Privatpersonen übernehmen staatliche Übermittlungen, während der Staat in eine koordinierende Rolle gedrängt wird. Die Digitalisierung darf nicht zur Makulatur des Gesetzesvorbehalts im Ermittlungsverfahren werden.


SUGGESTED CITATION  Bovermann, Marc, Fink, Johanna; Mutter, Jakob: *PimEyes User auf den Spuren der RAF: Verbotene Früchte und der Gesetzesvorbehalt in polizeilichen Ermittlungsverfahren, VerfBlog,* 2024/3/22, https://verfassungsblog.de/pimeyes-user-auf-raf-spuren/, DOI: 10.59704/ee5e12eaf02c1341 .

Explore posts related to this: