Bundesministerium
Inneres

Sicherheitsakademie

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Büyükyorulmaz, Rifat

Öffentlichkeitsfahndung der Moderne – die Internetfahndung

SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1/2025), 66-77.

doi: 10.7396/2025_1_F

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Büyükyorulmaz, Rifat (2025). Öffentlichkeitsfahndung der Moderne – die Internetfahndung, SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 66-77, Online: https://dx.doi.org/10.7396/2025_1_F.

© Bundesministerium für Inneres – Sicherheitsakademie / Verlag Österreich, 2025

Hinweis: Die gedruckte Ausgabe des Artikels ist in der Print-Version des SIAK-Journals im Verlag Österreich (https://www.verlagoesterreich.at/) erschienen.

Online publiziert: 4/2025

Öffentlichkeitsfahndung der Moderne – die Internetfahndung

RIFAT BÜYÜKYORULMAZ,
Medienjurist in der Abteilung Öffentlichkeitsarbeit im BMI.

Der Artikel beleuchtet die Herausforderungen und rechtlichen Rahmenbedingungen, die mit der modernen Öffentlichkeitsfahndung, insbesondere der Internetfahndung, verbunden sind. Öffentlichkeitsfahndung bedeutet die aktive Einbindung der Bevölkerung bei der Suche nach Personen oder Gegenständen. In der heutigen Zeit nimmt die Nutzung digitaler Plattformen und sozialer Medien bei der polizeilichen Fahndung eine zentrale Rolle ein. Diese Methode ermöglicht eine schnelle und weiträumige Verbreitung von Informationen, birgt jedoch auch erhebliche Risiken für den Schutz der Persönlichkeitsrechte. Der Beitrag untersucht die rechtlichen Grundlagen der Internetfahndung in Österreich, die durch verschiedene Gesetze wie die Strafprozessordnung (StPO), das Datenschutzgesetz (DSG) und das Sicherheitspolizeigesetz (SPG) geregelt sind. Ein besonderer Fokus liegt auf dem Schutz personenbezogener Daten und der Abwägung zwischen dem öffentlichen Interesse und dem Schutz der betroffenen Personen. Die Veröffentlichung von Bildern oder persönlichen Informationen darf nur dann erfolgen, wenn sie für die Fahndung notwendig und verhältnismäßig ist. Zudem wird die Bedeutung von datenschutzkonformen Maßnahmen wie der „Link-Lösung“ betont, um die Kontrolle über die Verbreitung sensibler Informationen zu behalten. Der Artikel fordert eine sorgfältige Planung und strenge Einhaltung rechtlicher Vorgaben, um eine Balance zwischen der Effektivität der Fahndung und dem Schutz der individuellen Rechte zu gewährleisten.

EINLEITUNG

Öffentlichkeitsfahndung

In kaum einem anderen Zusammenhang ist der Umgang mit Persönlichkeitsschutz und der Übermittlung von Bilddateien so heikel wie bei einer Öffentlichkeitsfahndung. Dabei gilt es, mit verschiedenen Mitteln das gelindeste zum Ziel führende Mittel anzuwenden, um sowohl die öffentlichen Interessen als auch die Interessen des Einzelnen zu berücksichtigen. Eine besondere Herausforderung stellt bei der Polizeiarbeit die Internetfahndung dar.

Unter dem allgemeinen Begriff der Öffentlichkeitsfahndung versteht man die Einbindung der Öffentlichkeit, die zur Mithilfe aufgefordert wird. Es kann sowohl nach Personen als auch nach Sachen gefahndet werden. In diesem Artikel liegt das Hauptaugenmerk auf der Personenfahndung und der rechtlich ordnungsgemäßen Durchführung im Internet. Die StPO regelt die Fahndung nach

Personen in bestimmten strafrechtlichen Situationen. Eine Fahndung zur Ermittlung des Aufenthaltsortes einer Person ist demnach zulässig, wenn der Aufenthaltsort des Beschuldigten oder einer anderen Person, deren Identität festgestellt werden muss oder die als Zeuge vernommen werden soll, unbekannt ist.[1]

Sollte die Fahndung ohne die Zuziehung der Öffentlichkeit als wenig erfolgversprechend erscheinen, so darf in besonderen Fällen, unter der ausschließlichen Anordnung der Staatsanwaltschaft, eine öffentliche Bekanntmachung veranlasst werden. Dies ist insbesondere dann zulässig, wenn der Beschuldigte einer vorsätzlich begangenen Straftat, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, dringend verdächtig ist. Dabei dürfen Abbildungen von Personen nur dann veröffentlicht werden oder zur Veröffentlichung in den Medien sowie öffentlich zugänglichen Dateien freigegeben werden, wenn der damit angestrebte Vorteil den damit verbundenen Eingriff in die Privatsphäre deutlich überwiegt oder die Veröffentlichung zum Schutz der Rechte und Interessen von gefährdeten Personen erforderlich erscheint.[2]

Die Öffentlichkeitsfahndung ist somit ein wesentlicher Bestandteil der polizeilichen Ermittlungsarbeit. Sie bezeichnet die aktive Suche nach Personen oder Gegenständen mithilfe der breiten Öffentlichkeit. Dabei werden Informationen über gesuchte Personen, Vermisste oder wichtige Beweismittel an die Bevölkerung übermittelt, um Hinweise und Unterstützung zu erhalten. Diese Methode hat sich als äußerst effektiv erwiesen, da sie eine große Anzahl von Menschen erreicht und so die Chancen erhöht, relevante Informationen zu sammeln.[3]

Rechtliche Grundlagen der Öffentlichkeitsfahndung

Die Fahndung wird im österreichischen SPG in § 24 geregelt. Gemäß dieser Bestimmung sind die Sicherheitsbehörden dazu verpflichtet, den Aufenthaltsort von Personen zu ermitteln, nach denen gefahndet wird. § 24 SPG definiert die Personen- und Sachfahndung als zentrale Aufgaben der Sicherheitsbehörden im Rahmen der Sicherheitspolizei zur Aufrechterhaltung der öffentlichen Sicherheit.[4] Die sicherheitspolizeiliche Personenfahndung ist auch ohne einen kriminalpolizeilichen Zusammenhang zulässig, insbesondere zur Suche nach abgängigen, hilflosen oder minderjährigen Personen. Da die Fahndung überwiegend eine Ermittlungstätigkeit darstellt, unterliegt sie den datenschutzrechtlichen Bestimmungen, da hierbei personenbezogene Daten verarbeitet werden.[5] Die Personenfahndung gemäß § 24 Abs 1 SPG umfasst die Ermittlung des Aufenthaltsortes einer Person, die aus den in Z 1 bis 4 der zitierten Bestimmung abschließend geregelten Gründen oder Anlässen gesucht wird. Im Gegensatz dazu definiert § 167 Z 1 StPO die Personenfahndung umfassender. Sie schließt nicht nur Maßnahmen zur Aufenthaltsermittlung ein, sondern auch Zwangsmaßnahmen, wie etwa die Festnahme eines Beschuldigten aufgrund einer Anordnung der Staatsanwaltschaft. Im strafprozessualen Kontext bildet somit ausschließlich eine solche Anordnung der Staatsanwaltschaft die rechtliche Grundlage für die Durchführung einer Personenfahndung.[6]

Gemäß § 53 Abs 1 SPG dürfen Sicherheitsbehörden und ihre Organe personenbezogene Daten im Rahmen des sicherheitspolizeilichen Ermittlungsdienstes nur zu den in der Bestimmung abschließend aufgezählten Zwecken ermitteln und verarbeiten. Einer dieser Zwecke, festgelegt in § 53 Abs 1 Z 5 SPG, ist die Fahndung.

Diese Ermächtigung erlaubt es den Sicherheitsbehörden, personenbezogene Daten gezielt für die Suche nach Personen zu verarbeiten, sofern dies zur Erfüllung ihrer Aufgaben im Bereich der öffentlichen Sicherheit erforderlich ist. Die Verarbeitung nach § 53 SPG erfolgt lokal durch eine Sicherheitsbehörde, die datenschutzrechtlich als Verantwortliche agiert, wobei ausdrücklich auch gesetzliche Ermächtigungen für eine Verarbeitung durch gemeinsam Verantwortliche vorgesehen sind. Zusätzlich ist aus § 52 SPG abzuleiten, dass jede Verarbeitung zur Erfüllung der vorgesehenen Zwecke erforderlich sein muss und gemäß § 51 SPG den Grundsatz der Verhältnismäßigkeit wahren muss.[7]

Polizeiliche Datenübermittlungen an Externe

Die Übermittlung von polizeilichen Daten an externe Stellen oder private Personen unterliegt in Österreich strengen rechtlichen Vorgaben, um die Sicherheit und den Schutz personenbezogener Daten zu gewährleisten.[8] Diese sind in der StPO, dem SPG und im Datenschutz (DSG, Datenschutz-Grundverordnung (DSGVO)) verankert. Je nach Übermittlung der Daten ist auch das Mediengesetz (MedienG) heranzuziehen.

Gemäß § 56 SPG ist die Übermittlung personenbezogener Daten durch Sicherheitsbehörden an Personen und Stellen außerhalb der eigenen Verwaltung nur unter spezifischen Bedingungen zulässig.[9] Dieser Paragraf enthält eine abschließende Aufzählung, in denen eine solche Datenübermittlung an Private erfolgen darf. Eine Datenübermittlung ist zulässig, wenn die betroffene Person ausdrücklich einwilligt und die Datenübermittlung für die Erfüllung einer gesetzlich übertragenen Aufgabe wesentlich ist. Die Daten an Interventions- oder Beratungsstellen für Gewaltprävention dienen bei Vorfällen im Zusammenhang mit Fußballsportgroßveranstaltungen dem Schutz gefährdeter Personen, deren Rechtsgut durch einen gefährlichen Angriff bedroht ist, lebenswichtige Interessen eines Menschen betroffen sind; für den Zweck der Veröffentlichung durch Sicherheitsbehörden oder Medienunternehmen, für wissenschaftliche Forschung und statistische Zwecke und im Rahmen einer sicherheitspolizeilichen Fallkonferenz dürfen Daten an die Teilnehmer übermittelt werden. Dies sind die einzigen Umstände, unter denen polizeiliche Daten mit Privaten geteilt werden dürfen. Es handelt sich dabei nicht um eine demonstrative, sondern eine abschließende taxative Aufzählung, da aus dem Gesetzeswortlaut eindeutig hervorgeht, dass nur unter diesen Umständen eine Datenübermittlung zulässig ist.[10]

Traditionell erfolgt die Öffentlichkeitsfahndung über Printmedien, Radio, Fernsehen und öffentliche Aushänge. Diese klassischen Medienkanäle haben jedoch ihre Grenzen, insbesondere was die Reichweite und die Geschwindigkeit der Informationsverbreitung betrifft. Durch das Internet und soziale Medien haben sich die Möglichkeiten der Öffentlichkeitsfahndung erheblich erweitert.[11] Angesichts der durch das Internet höheren Reichweite ist auch ein höheres Maß an Vorsicht geboten, um eine rechtskonforme verhältnismäßige Öffentlichkeitsfahndung durchzuführen.[12]

HAUPTTEIL

Internetfahndung

Die Internetfahndung stellt eine spezifische Form der Öffentlichkeitsfahndung dar, bei der digitale Plattformen wie soziale Netzwerke, Webseiten und Foren genutzt werden, um Informationen über gesuchte beziehungsweise vermisste Personen oder relevante Zeugenaussagen zu verbreiten. Diese Methode ist besonders

effektiv, um in kürzester Zeit eine breite Öffentlichkeit zu erreichen.[13]

Ein wesentlicher Vorteil der Internetfahndung liegt in der sofortigen Verfügbarkeit und der Reichweite der Informationen. Durch die Nutzung des Internets können Behörden und Ermittlungsorgane potenziell Millionen von Nutzerinnen und Nutzern erreichen, was die Chancen erhöht, dass relevante Informationen oder Hinweise gesammelt werden können. In einer zunehmend digitalisierten Welt ermöglicht die Internetfahndung eine schnelle Reaktion auf die Dynamik von Kriminalität und die Verbreitung von Informationen.

Die Internetfahndung ist in Österreich nicht eigens normiert, stattdessen kommt eine Reihe von rechtlichen Rahmenbedingungen zur Anwendung, die sowohl den Schutz personenbezogener Daten als auch die Wahrung der Persönlichkeitsrechte gewährleisten sollen. Die StPO, die Datenschutzgesetzgebung (DSG und DSGVO) sowie das SPG definieren die Voraussetzungen und Grenzen für die Veröffentlichung und Übermittlung von personenbezogenen Daten und legen fest, welche Täterschutzbestimmungen beachtet werden müssen.

Trotz der offensichtlichen Vorteile birgt die Internetfahndung erhebliche Risiken. Die Veröffentlichung von personenbezogenen Daten im Internet kann tiefgreifende Eingriffe in die Privatsphäre der betroffenen Personen mit sich bringen.[14] Es besteht die Gefahr der Stigmatisierung und der Verletzung der Unschuldsvermutung, insbesondere wenn die veröffentlichten Informationen unvollständig oder missverständlich sind.[15] Die Balance zwischen der Notwendigkeit, Informationen zu verbreiten, und dem Schutz der Persönlichkeitsrechte der Betroffenen ist daher eine zentrale Herausforderung.[16]

Dieser Artikel untersucht eingehend die rechtlichen Rahmenbedingungen und praktischen Herausforderungen der Internetfahndung in Österreich. Dabei wird analysiert, wie eine rechtmäßige und verhältnismäßige Nutzung dieser Fahndungsmethode sichergestellt werden kann. Besonderes Augenmerk liegt auf den Maßnahmen, die erforderlich sind, um die Rechte der betroffenen Personen zu wahren und den rechtlichen Anforderungen zu entsprechen. Durch die Auseinandersetzung mit aktuellen gesetzlichen Bestimmungen und praktischen Beispielen soll ein umfassendes Verständnis für die Balance zwischen der Effektivität der Fahndung und dem Schutz der individuellen Rechte vermittelt werden.

Rechtliche Grundlagen

Datenübermittlungen an Personen außerhalb der Verwaltung zu präventiv-polizeilichen Zwecken sind in Österreich in § 56 des SPG geregelt. Diese Vorschrift bestimmt einige besondere Anwendungsbereiche der polizeilichen Datenübermittlung an Private. Dies umfasst auch die präventive Öffentlichkeitsfahndung. Angesichts technischer Aspekte und der weiten Wortbedeutung unterliegen dem Bereich der „Übermittlungen“ somit auch die Übermittlung und Veröffentlichung von Daten im Internet.[17] Darüber hinaus deckt der Begriff auch die Internetfahndung ab. Eine Internetfahndung beziehungsweise eine gewisse mediale Aufbereitung der Berichterstattung durch das Innenressort, speziell im Zusammenhang mit der Exekutive, darf nur unter Einhaltung von datenschutzrechtlichen Bestimmungen, Persönlichkeitsrechten und unter Berücksichtigung anderer Grundrechte erfolgen.

Im Zweifelsfall hat der Schutz von personenbezogenen Daten Vorrang. Es ist Aufgabe der Sicherheitsbehörden, im Rahmen ihrer Medienarbeit keine Ansatzpunkte für Missachtungen der Rechte der Betroffenen durch die Medien zu schaffen.

Dies gilt insbesondere für den Schutz der Unschuldsvermutung und den Persönlichkeitsschutz, weshalb auch in Situationen, in denen ein Kriminalfall von den Sicherheitsbehörden als geklärt gilt, trotzdem nur von Tatverdächtigen zu sprechen ist. Auch das österreichische MedienG weist einen vergleichsweise hohen legistischen Standard zum Schutz der von Kriminalberichterstattung betroffenen Täter, Verdächtigen oder Opfer auf. Zu verweisen ist in diesem Zusammenhang auf § 7, § 7a und § 7b MedienG.[18]

Selbst wenn es keine genauen Datenübermittlungsvorschriften für das Internet als vermutlich wichtigstes Fahndungsmedium gibt, sind die genannten Vorschriften einzuhalten, um Risiken zu minimieren und Rechtsverletzungen zu vermeiden.

Grundrechtsschutz

Im Kontext der Internetfahndung spielt der Schutz der Grundrechte, vorwiegend des Persönlichkeitsrechts, eine zentrale Rolle. Personenbildnisse, häufig in Form von Fotos, dürfen nicht öffentlich ausgestellt oder zugänglich gemacht werden, wenn dadurch berechtigte Interessen der abgebildeten Personen verletzt werden.[19] Diese Regelung basiert auf einer objektiven Interessenabwägung, die sicherstellen soll, dass das Persönlichkeitsrecht vor Missbrauch und unangemessener öffentlicher Darstellung geschützt wird. Speziell sollen die abgebildeten Personen davor geschützt werden, bloßgestellt, in ihrem Privatleben preisgegeben oder in einer Weise dargestellt zu werden, die zu Missdeutungen oder Entwürdigungen führen kann.[20]

In Österreich regelt § 7a des MedienG den Identitätsschutz von Opfern, Verdächtigen und Täterinnen oder Tätern im Zusammenhang mit gerichtlich strafbaren Handlungen. Unter einer gerichtlich strafbaren Handlung versteht man alle Verhaltensweisen, die nach österreichischem Recht strafbar sind.[21] Für Opfer, Verdächtige und Täterinnen oder Täter besteht ein Anspruch auf Identitätsschutz, sofern schutzwürdige Interessen einer betroffenen Person unverhältnismäßig beeinträchtigt beziehungsweise verletzt werden oder eine solche Gefahr besteht. Das MedienG definiert diesen Begriff zwar nicht allgemein, jedoch vertritt die Rechtsprechung[22] die Auffassung, dass es grundsätzlich auf eine konkrete Gefährdung oder Verletzung schutzwürdiger Interessen ankomme. Bei Verdächtigen werden schutzwürdige Interessen durch eine identifizierende Berichterstattung (im weiteren Sinne auch Fahndung) jedenfalls dann verletzt, wenn die verdächtige Person das 18. Lebensjahr noch nicht vollendet hat.[23] Weiters werden schutzwürdige Interessen verletzt, wenn dadurch das Fortkommen der oder des Betroffenen unverhältnismäßig gefährdet wird. Unter dem Fortkommen einer Person sind die privaten und beruflichen Entwicklungsmöglichkeiten zu verstehen. Ob eine derartige Eignung zu einer unverhältnismäßigen Beeinträchtigung des Fortkommens vorliegt, bestimmt sich unter anderem nach folgenden Kriterien:

Je weniger eingreifend die Maßnahmen der Strafverfolgung sind und je mehr sie am Beginn stehen, desto eher ist eine identifizierende Berichterstattung oder Fahndung unverhältnismäßig.[24] Berichte über den Verdacht eines Verbrechens sind in der Regel geeignet, das Fortkommen der oder des Betroffenen unverhältnismäßig zu gefährden.[25] Ein Anspruch nach § 7a MedienG ist umso eher zu verneinen, je fortgeschrittener das Verfahrensstadium und je gewichtiger die angelastete Straftat ist.[26]

Zufolge § 7a Abs 1 zweiter Halbsatz MedienG besteht kein Identitätsschutz, wenn wegen der Stellung des Verdächtigen oder eines sonstigen Zusammenhangs mit dem öffentlichen Leben oder aus anderen

Gründen ein überwiegendes Interesse der Öffentlichkeit an der Veröffentlichung besteht. Damit ordnet der Gesetzgeber eine Interessenabwägung an.

Eine solche Verletzung würde etwa dann stattfinden, wenn personenbezogene Informationen über den Zweck hinaus an die Öffentlichkeit übermittelt werden, oder etwa, wenn bei einem Fahndungsfoto eine unverhältnismäßig hohe Reichweite eingesetzt wird.

Die globale Reichweite des Internets, die permanente Zugriffsmöglichkeit und die oft schwer nachvollziehbaren Möglichkeiten zur Weiterleitung und Speicherung von Daten führen dazu, dass Informationen online eine dauerhafte Verfügbarkeit erlangen können. Dies stellt eine besondere Herausforderung für den Grundrechtsschutz dar, da die Daten in der digitalen Welt weit verbreitet und langfristig zugänglich bleiben können.

Datenschutz im Kontext der Internetfahndung

Auch der Datenschutz ist eine wichtige Säule der Internetfahndung. In Österreich sind die wesentlichen Datenschutzregelungen im DSG und in der DSGVO verankert. Diese Regelungen definieren die Grundsätze, unter denen personenbezogene Daten verarbeitet werden dürfen. Ein zentraler Grundsatz ist die Datenminimierung, die vorschreibt, dass nur die für den jeweiligen Zweck unbedingt erforderlichen Daten erhoben und verarbeitet werden dürfen.[27] Dies bedeutet, dass bei der Internetfahndung nur solche Informationen veröffentlicht werden sollten, die für die Erreichung des Fahndungsziels notwendig sind.

Des Weiteren gewährt die DSGVO den betroffenen Personen verschiedene Rechte, wie das Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung. Im Rahmen der Internetfahndung müssen Maßnahmen getroffen werden, um diese Rechte zu wahren.[28] Dadurch soll verhindert werden, dass die Fahndungsbilder auf unbestimmte Zeit abgespeichert werden oder im Internet öffentlich für jeden zugänglich sind. Dies würde über den Rahmen der Verhältnismäßigkeit hinausgehen.

Zulässigkeit einer Internetfahndung

Die Zulässigkeit einer Internetfahndung setzt voraus, dass sowohl strafrechtliche als auch datenschutzrechtliche Anforderungen eingehalten werden. Dabei spielen mehrere Faktoren eine entscheidende Rolle, um sicherzustellen, dass die Rechte der betroffenen Personen gewahrt bleiben, während gleichzeitig die öffentliche Sicherheit und das Interesse an der Strafverfolgung berücksichtigt werden.[29]

Für die rechtmäßige Durchführung einer Internetfahndung sind die Schwere der vorgeworfenen Straftat und die Intensität des Verdachts von zentraler Bedeutung. Handelt es sich um eine besonders schwere Straftat, wie etwa ein Verbrechen, bei dem eine erhebliche Gefahr für die Öffentlichkeit besteht, kann eine Internetfahndung gerechtfertigt sein. In solchen Fällen überwiegt das öffentliche Interesse an der Aufklärung der Straftat und der Ergreifung der Täterin oder des Täters oft die Persönlichkeitsrechte der betroffenen Person.[30]

Allgemein kann das öffentliche Interesse an der Aufklärung einer Straftat eine Internetfahndung rechtfertigen, insbesondere wenn eine akute Gefahrenlage besteht oder die Straftat die Gesellschaft in besonderem Maße betrifft. Dabei muss jedoch stets die Verhältnismäßigkeit gewahrt bleiben. Die Internetfahndung darf nicht über das zur Erreichung des Fahndungszieles notwendige Maß hinausgehen. Dies beinhaltet auch eine Abwägung zwischen dem öffentlichen Interesse und den schutzwürdigen Interessen der betroffenen Per-

son, wie etwa dem Fortkommen im privaten und beruflichen Leben.[31]

Das überwiegende Interesse der Öffentlichkeit ist auch unter räumlichen Gesichtspunkten zu prüfen. Ein regionales Interesse, beispielsweise in einer kleinen Gemeinde, könnte eine weniger intensive Form der Fahndung rechtfertigen, während eine österreichweite oder gar internationale Veröffentlichung nur in Fällen von erheblichem öffentlichen Interesse gerechtfertigt ist. Ein Zuwiderhandeln könnte insbesondere auch das Fortkommen der oder des Betroffenen im Hinblick auf die dadurch bewirkte überdimensionale Publizität unverhältnismäßig beeinträchtigen und wäre daher unzulässig.[32]

Aus datenschutzrechtlicher Sicht ist eine Internetfahndung nur dann zulässig, wenn die Verarbeitung personenbezogener Daten auf einer klaren Rechtsgrundlage beruht und die Prinzipien der Datenminimierung und Zweckbindung eingehalten werden.[33] Die Veröffentlichung von Fotos oder anderen identifizierenden Informationen darf nur erfolgen, wenn sie für den Zweck der Fahndung unerlässlich sind. Sämtliche Datenverarbeitungen, die über den Rahmen der Zweckmäßigkeit hinausgehen, sind zu unterlassen und es müssen geeignete technische und organisatorische Maßnahmen zum Schutz der Daten ergriffen werden.[34]

Risiken der Internetfahndung

Die Veröffentlichung von Personenbildern oder persönlichen Informationen im Rahmen einer Internetfahndung kann zu einer erheblichen Verletzung der Persönlichkeitsrechte führen. Sie birgt das Risiko, dass diese Daten im Internet unkontrolliert verbreitet und gespeichert werden, wodurch die Gefahr eines verstärkten Reputationsverlusts besteht.[35] Einmal veröffentlichte Daten lassen sich nur schwer zurückziehen und die Kontrolle über ihre Weiterverbreitung ist praktisch unmöglich. Dadurch können die Daten auch nach der Klärung des Falls weiterhin im Umlauf bleiben, was zu langanhaltenden negativen Konsequenzen für die betroffene Person führen kann. Daher ist es umso wichtiger, vor der Veröffentlichung eine genaue Prüfung der Erforderlichkeit[36] und Verhältnismäßigkeit[37] durchzuführen.[38]

Den Risiken der Internetfahndung steht jedoch das Allgemeininteresse an einer effektiven Gefahrenabwehr gegenüber, für die das Internet eine Vielzahl fahndungstechnischer Vorteile bietet. Durch die hohe Zahl von Informationsempfängern im Internet und die zahlreichen Datenweiterleitungen ist eine schnellere und höhere Reichweite im Vergleich zu klassischen Fahndungen gegeben. Dadurch erhöhen sich auch die Erfolgschancen einer Fahndung vehement. Die Verwendung von klassischen Fahndungsmitteln wie Rundfunk, Printmedien und dergleichen stellen hingegen das mildere Mittel dar, jedoch mit dem Nachteil, dass sie nicht gleich effektiv sind.

Fahndung über interne Internetseiten

Die Internetfahndung unterscheidet sich von traditionellen Fahndungsmethoden insbesondere durch ihre erhöhte Grundrechtsrelevanz. Diese resultiert aus der unkontrollierten und dauerhaften Verbreitung von Inhalten sowie der ständigen und überörtlichen Zugriffsmöglichkeit. In einem digitalen Raum, in dem Informationen potenziell weltweit und unbegrenzt abrufbar sind, besteht die Gefahr, dass personenbezogene Daten unrechtmäßig weiterverbreitet oder missbraucht werden.[39] Dieses Risiko kann erheblich reduziert werden, wenn die Fahndung auf polizeieigenen Internetseiten stattfindet.

Bei der Nutzung eigener Kanäle[40] behält die zuständige Behörde die Kontrolle über die Dauer und den Umfang der Verbrei-

tung der Informationen. Im Gegensatz zu öffentlichen, nicht behördlichen Plattformen, auf denen Inhalte unkontrolliert weiterverbreitet werden können, bietet eine zentrale Verwaltung auf polizeieigenen Seiten die Möglichkeit, Fahndungsaufrufe gezielt und zeitlich befristet zu steuern. Dies reduziert die Gefahr, dass die betroffenen Personen langfristig oder unnötigerweise stigmatisiert werden.

Zudem ist der Zugriff auf solche Inhalte auf das Interesse einer spezifischen Nutzergruppe beschränkt. Personen, die sich bewusst auf die Suche nach Fahndungsinformationen begeben, besuchen die entsprechenden Seiten. Dadurch wird vermieden, dass unbeteiligte Dritte zufällig auf sensible Inhalte stoßen, was das Risiko eines unverhältnismäßigen Grundrechtseingriffs weiter senkt. Der Verhältnismäßigkeitsgrundsatz, der ein zentrales Prinzip im Datenschutz und in der Wahrung der Persönlichkeitsrechte darstellt, kann somit besser gewährleistet werden.

Darüber hinaus ermöglicht die Zentralisierung der Informationen auf behördlichen Plattformen eine verbesserte Überwachung und Kontrolle der Daten. So können etwa missbräuchliche Verwendungen oder unerwünschte Weiterverbreitungen schneller erkannt und unterbunden werden. Dies trägt dazu bei, das Vertrauen der Bevölkerung in die Maßnahmen der Strafverfolgungsbehörden zu stärken und gleichzeitig die Rechte der betroffenen Personen zu schützen.

Fahndung über externe Internetseiten

Die Nutzung externer Internetseiten zur Unterstützung polizeilicher Fahndungsmaßnahmen birgt spezifische Herausforderungen, insbesondere in Bezug auf die Kontrolle und den Schutz personenbezogener Daten. Sobald sie personenbezogene Daten, wie Fahndungsfotos oder Informationen über gesuchte Personen, an Dritte übermittelt, verliert die Polizei die direkte Kontrolle über diese Daten. Dies führt zu einem erheblichen Risiko: Weder die Dauer der Speicherung noch der Umfang der Verbreitung kann von der Polizei beeinflusst werden, was zu einem potenziellen Missbrauch oder einer unkontrollierten Weitergabe der Daten führen kann. Der absolute Kontrollverlust, der hier entsteht, stellt eine ernsthafte Gefahr für die Wahrung der Persönlichkeitsrechte und den Datenschutz dar.[41]

Um diesem Problem entgegenzuwirken, empfiehlt sich die „Link-Lösung“.[42] Bei dieser Methode übermittelt die Polizei den Betreibern externer Internetseiten nicht die Daten selbst, sondern lediglich einen Link, der auf eine polizeieigene Seite verweist, auf der die relevanten Informationen bereitgestellt werden. Der wesentliche Vorteil dieser Lösung liegt in der Beibehaltung der Datenkontrolle durch die Polizei. Die eigentlichen Informationen verbleiben auf internen Servern, wodurch die Polizei jederzeit die Möglichkeit hat, diese Daten nach Abschluss der Fahndung zu entfernen. Sobald die Daten von der polizeieigenen Seite gelöscht werden, wird der Link ungültig und die Informationen sind nicht mehr abrufbar. Somit wird mit der Deaktivierung des Links gleichzeitig dafür Sorge getragen, dass diese spezifische Fahndung auch für alle externen Internetseiten unzugänglich wird.

Dieser Ansatz ermöglicht es, die große Reichweite externer Internetseiten effektiv zu nutzen, ohne dabei die Kontrolle über sensible Informationen zu verlieren. Gleichzeitig wird der Aufwand, der durch die Einhaltung datenschutzrechtlicher Verpflichtungen entsteht, erheblich reduziert. So muss die Polizei nicht jeden Betreiber externer Seiten individuell auffordern, Daten zu löschen oder Links zu deaktivieren, wie es in der DSGVO vorgesehen ist.[43] Die Link-Lösung bietet somit eine effiziente

und datenschutzkonforme Alternative, die den Schutz der Daten von betroffenen Personen gewährleistet und gleichzeitig die Effektivität der Fahndungsmaßnahmen unterstützt.

Darüber hinaus trägt diese Methode zur Vertrauensbildung in der Öffentlichkeit bei, da sie zeigt, dass die Polizei auch in digitalen Räumen verantwortungsvoll mit personenbezogenen Daten umgeht. Indem sie die Kontrolle über die Verbreitung der Informationen behalten, können die Behörden sicherstellen, dass die Daten nach Ablauf der Fahndung nicht unnötig oder unrechtmäßig im Internet verbleiben, was den Datenschutz und die Persönlichkeitsrechte der betroffenen Personen stärkt.

Fahndung über soziale Medien

Soziale Medien und die offiziellen Social-Media-Accounts von Polizeibehörden[44] sind zu einem zentralen Instrument in der Öffentlichkeitsfahndung geworden. Diese Kanäle ermöglichen es, Fahndungsaufrufe schnell und weitreichend zu verbreiten. Allerdings geht dies auch mit erheblichen Risiken einher. Insbesondere verliert die Polizei nach Veröffentlichung eines Fahndungsaufrufs auf Plattformen wie Facebook oder X (ehemals Twitter) weitgehend die Kontrolle über die Verbreitung und Speicherung der Informationen.[45] Sobald eine Fahndung über Social-Media-Kanäle veröffentlicht wird, ist nicht nur von einer österreichweiten, sondern potenziell von einer weltweiten Bekanntgabe der Identität der gesuchten Person auszugehen. Jede Person mit Zugang zu diesen Plattformen kann auf die Fahndung und die damit verbundenen Identitätsdaten zugreifen.

Darüber hinaus besteht die Gefahr, dass durch automatisierte Algorithmen und Verknüpfungen ungewollt Verbindungen zwischen dem Fahndungsaufruf und den Profilen anderer Nutzer hergestellt werden.[46] Dies erhöht das Risiko eines Eingriffs in die Grundrechte erheblich, insbesondere wenn dadurch falsche oder missverständliche Assoziationen entstehen.[47]

Ähnlich wie bei der Nutzung externer Internetseiten bietet auch hier die Link-Lösung eine sicherere Alternative zur direkten Veröffentlichung von Identitätsdaten. Anstatt die Identität der Täterin oder des Täters oder Verdächtigen direkt zu posten, empfiehlt es sich, einen Beitrag zu veröffentlichen, der die Umstände der Fahndung erläutert, ohne ein Bildnis von der oder vom Tatverdächtigten anzuhängen. Dies könnte beispielsweise so erfolgen: „Es wird nach einer Person in [Ort] gefahndet, wegen [Tatvorwurf]." In den Kommentaren oder im Text des Beitrags könnte ein weiterführender Link zur offiziellen Homepage der Polizei bereitgestellt werden, auf der die vollständigen Informationen zu finden sind.

Dieser Ansatz bietet den Vorteil, dass nur Personen, die tatsächlich Interesse an der Fahndung haben, weil sie sich zum Beispiel am selben Ort aufhalten oder relevante Informationen besitzen, auf den Link zugreifen. Dadurch wird verhindert, dass unbeteiligte Nutzerinnen und Nutzer, die lediglich beiläufig durch ihre Social-Media-Feeds scrollen, unnötig mit der Fahndung konfrontiert werden. So kann das Risiko einer Grundrechtsverletzung der betroffenen Person deutlich reduziert und eine übermäßig räumliche Veröffentlichung eingeengt werden.

Um eine verhältnismäßige und datenschutzkonforme Fahndung in sozialen Medien zu gewährleisten, sollten solche Methoden und Vorsichtsmaßnahmen stets berücksichtigt werden. Nur durch eine sorgfältige Planung und eine differenzierte Herangehensweise kann sichergestellt werden, dass die Rechte der betroffenen Personen gewahrt bleiben, während die Polizei gleichzeitig die notwendige Unterstützung aus der Bevölkerung erhält.

Ausnahmefälle

In bestimmten Ausnahmefällen wie Sittlichkeitsdelikten kann die Offenlegung der Identität einer Täterin oder eines Täters im überwiegenden Interesse der Öffentlichkeit liegen. In solchen Situationen erfüllt die Veröffentlichung eine wichtige Warn- und Schutzfunktion, indem sie potenzielle Opfer informiert und dazu beiträgt, weitere Straftaten zu verhindern.[48]

Allerdings stellen diese Fälle eine Ausnahme dar. Selbst in solchen Situationen müssen Verhältnismäßigkeit und Erforderlichkeit vorab geprüft werden. Es ist entscheidend, sicherzustellen, dass die Veröffentlichung der Identität der Täterin oder des Täters tatsächlich notwendig ist und dass die potenziellen Vorteile für die Öffentlichkeit die möglichen Nachteile für die Betroffene oder den Betroffenen deutlich überwiegen.[49]

RESÜMEE

Unter Berücksichtigung der strengen Tatbestandsvoraussetzungen ist eine Öffentlichkeitsfahndung im Internet grundsätzlich zulässig. Dabei ist es jedoch unerlässlich, die Risiken so gering wie möglich zu halten und ausschließlich verhältnismäßige sowie erforderliche Maßnahmen zu ergreifen.

Besonders wichtig ist, dass die Fahndung primär über polizeieigene Plattformen erfolgt. Sollten die Daten zusätzlich auf externen Webseiten oder sozialen Medien verbreitet werden, sollte dies ausschließlich mittels der Link-Lösung geschehen. Es ist sicherzustellen, dass Nutzerinnen und Nutzer informiert werden, dass eine Weiterverbreitung der Fahndungsmeldung nur durch das Teilen des Links auf das offizielle Fahndungsportal erfolgen darf.

Zusätzlich müssen bei der Veröffentlichung sämtliche technisch möglichen Maßnahmen getroffen werden, um den Grundrechtsschutz der betroffenen Person zu gewährleisten.[50] Nach Abschluss der Fahndung ist die entsprechende Meldung unverzüglich zu entfernen und die Öffentlichkeit muss in derselben Form über den Abschluss informiert werden wie es bei der ursprünglichen Bekanntmachung des Falles gewesen ist.[51]

Auch wenn die Internetfahndung eine immer wichtigere Rolle bei der Unterstützung der polizeilichen Arbeit darstellt, ist eine klare gesetzliche Normierung bisher noch nicht ausreichend gegeben. Es ist daher entscheidend, die beschriebenen Maßnahmen und Vorgaben strikt einzuhalten, um sowohl den Schutz der Persönlichkeitsrechte als auch die Effektivität der Fahndung zu gewährleisten.

[1] *Siehe § 168 StPO.*

[2] *Siehe dazu § 169 StPO, vgl Online: https://www.parlament.gv.at/dokument/XXII/AB/1018/fnameorig_013626.html (17.08.2024).*

[3] *Vgl Online: https://www.bka.de/SharedDocs/FAQs/DE/Oeffentlichkeitsfahndung/oeffentlichkeitsfahndungFrage01.html (17.08.2024); Heuer, Datensicherheit im GTelG 2012: die „Übermittlung" im Sinne von § 3 Abs 1 GtelG 2012, jusIT 3/2024, 99.*

[4] *Vgl Vogl, § 169 StPO Festnahme, Fuchs/Ratz (Hrsg), StPO Wiener Kommentar zur Strafprozessordnung (2024) Rz 14f.*

[5] *Vgl Leitner, Aufgaben der Sicherheitsbehörden auf dem Gebiet der Sicherheitspolizei, Thanner/Vogl (Hrsg), SPG – Sicherheitspolizeigesetz³ (2024) 245.*

[6] *Vgl Vogl, § 169 StPO Festnahme, Fuchs/Ratz (Hrsg), StPO Wiener Kommentar zur Strafprozessordnung (2024) Rz 2–4.*

[7] *Vgl Weiss, Verarbeiten personenbezogener Daten im Rahmen der Sicherheitspolizei, Thanner/Vogl (Hrsg), SPG – Sicherheitspolizeigesetz[3] (2024) 648f.*

[8] *Vgl Divjak, Datenschutz und Strafprozess (2024) 157f.*

[9] *Vgl Weiss, Verarbeiten personenbezogener Daten im Rahmen der Sicherheitspolizei, Thanner/Vogl (Hrsg), SPG – Sicherheitspolizeigesetz[3] (2024) 648f. 769f.*

[10] *Siehe dazu § 56 SPG; Prange, Verfassungsrechtliche Möglichkeiten und Grenzen polizeilicher Datenübermittlungen an Private (2023) 74f.*

[11] *Vgl Wohlers, Hooliganismus-Bekämpfung: kann die Schwein von England lernen?, Causa Sport 2011, 176.*

[12] *Vgl Divjak, Datenschutz und Strafprozess (2024) 80f; vgl Soyer, Verhältnismäßigkeit einer Personenfahndung durch Lichtbildveröffentlichung, JSt 2/2021, 178.*

[13] *Vgl Prange, Verfassungsrechtliche Möglichkeiten und Grenzen polizeilicher Datenübermittlungen (2023) 156f.*

[14] *Vgl Holzer, Der Rechtsmissbrauch als Grenze der Betroffenenrechte nach der DSGVO, jusIT 3/2024, 103.*

[15] *Vgl Divjak, Datenschutz und Strafprozess (2024) 154f.*

[16] *Vgl Soyer, Verhältnismäßigkeit einer Personenfahndung durch Lichtbildveröffentlichung, JSt 2/2021, 178.*

[17] *Vgl Prange, Verfassungsrechtliche Möglichkeiten und Grenzen polizeilicher Datenübermittlungen (2023) 74f.*

[18] *Siehe § 7, § 7a und § 7b MedienG; Höpfel/Ratz (Hrsg), WK² (2019); vgl Divjak, Datenschutz und Strafprozess (2024) 154f.*

[19] *Vgl Soyer, Verhältnismäßigkeit einer Personenfahndung durch Lichtbildveröffentlichung, JSt 2/2021, 178.*

[20] *Siehe OGH 4 Ob 26/95.*

[21] *Siehe OLG Wien 18 Bs 72/03, MR 2003, 293.*

[22] *Siehe OGH 15 Os 36, 37/96; OLG Wien 18 Bs 277/95.*

[23] *Siehe § 1 Z 2 JGG.*

[24] *Siehe OGH 15 Os 95/09y.*

[25] *Vgl Divjak, Datenschutz und Strafprozess (2024) 154f.*

[26] *Siehe OLG Wien 17 Bs 110/06k.*

[27] *Vgl Jahnel/Pallwein-Prettner, Datenschutzrecht (2021) 34f.*

[28] *Siehe dazu drittes Kapitel der DSGVO Art 13–21.*

[29] *Vgl Divjak, Datenschutz und Strafprozess (2024) 201f.*

[30] *Vgl Röggla/Zöchbauer, Identitätsschutz – Informationsinteresse der Öffentlichkeit, MUR 6/2014, 285; siehe OGH 15 Os 161/10f, MR (2011) 62; OGH 15 Os 99/14v, MR (2014) 285.*

[31] *Vgl Ratz, Mediale Warnung, ÖJZ 4/2015, 181; OGH 15 Os 99/14v.*

[32] *Vgl Frohner/Haller, MedienG[6] (2016) 55.*

[33] *Vgl Jahnel/Pallwein-Prettner, Datenschutzrecht (2021) 33f; Haidinger, Grundsätze der Datenverarbeitung, in Knyrim (Hrsg), Praxishandbuch Datenschutzrecht[4] (2020) 53.*

[34] *Vgl Thiele, EuGH: Widerrechtliche Datenweitergabe durch Europol – Schadenersatz, jusIT 3/2024, 111.*

[35] *Vgl Janisch, Zu Unterlassungsansprüchen gegen Social-Media-Plattformen wegen Persönlichkeitsrechtsverletzung durch Nutzer aus Anlass der Entscheidung OGH 30.08.2023 6 Ob 166/22p (furchtundunruhe), jusIT 3/2024, 90.*

[36] *Siehe dazu OGH Os99/14v; Ratz, Mediale Warnung, EvBl 4/2015, 181.*

[37] *Vgl Rohrer/Gruber, Die identifizierende Kameraüberwachung, ÖJZ 16/2020, 732; OGH 6 Ob 150/19f; Wittmann, Videoüberwachung des Zugangsbereichs zur Wohnung, MUR 3/2020, 138.*

[38] *Vgl Divjak, Datenschutz und Strafprozess (2024) 80f.*

[39] *Vgl Melz, Öffentlichkeitsfahndung im Internet (2020) 215f; Leupold, Google und der Streisand-Effekt: Das Internet vergisst nicht, MR-Int 1-2/2024, 3.*

[40] *Siehe dazu Online: https://www.bmi.gv.at/fahndung/ (18.08.2024); und weiters Online: https://www.polizei.gv.at/wien/lpd/fahndung/fahndung.aspx (18.08.2024).*

[41] *Vgl Flörl, Veröffentlichung von Personenbildnissen im Internet, Dako 1/2021 (7).*

[42] *Vgl Online: https://rdb.manz.at/document/1574_1_datenschutzbeauftragte_kap17 (18.08.2024); Bajmel, Datenschutz in sozialen Netzwerken – Die Öffentlichkeitsfahndung im Rahmen der Nutzung des sozialen Netzwerks Facebook, 181.*

[43] *Vgl Online: https://rdb.manz.at/document/1223_10_datkomm_dsg_p0046 (19.08.2024); EuGH 5.12.2023, C-807/21, EWS 1/2024 (37).*

[44] *Siehe dazu Online: https://www.facebook.com/WienerPolizei.at/?locale=de_DE (20.08.2024).*

[45] *Vgl Bajmel, Datenschutz in sozialen Netzwerken – Die Öffentlichkeitsfahndung im Internet, 134; Jahnel, Datenschutz im Internet – Rechtsgrundlagen Cookies und Web-Logs, ecolex 1/2001 (84).*

[46] *Vgl Bajmel, Datenschutz in sozialen Netzwerken – Die Öffentlichkeitsfahndung im Internet, 107f.*

[47] *Vgl Anderl/Woltran, 20. Kapitel: Social Media, in Zankl (Hrsg), Rechtshandbuch der Digitalisierung (2021) Rz 20.3f.*

[48] *Vgl Röggla/Zöchbauer, Opfereigenschaft iS des § 7a MedienG – Bloßstellung nach § 7 MedienG, MUR 3/2019 (107); Online: https://rdb.manz.at/document/1253_1_stgb_medieng_p0007a (20.08.2024); siehe OGH 4 Ob 275/98i.*

[49] *Vgl Online: https://rdb.manz.at/document/1223_10_datkomm_dsg_p0046 (19.08.2024); EuGH 5.12.2023, C-807/21, EWS 1/2024 (37).*

[50] *Online: https://rdb.manz.at/document/1211_2_dsg_p0054 (20.08.2024).*

[51] *Vgl Melz, Öffentlichkeitsfahndung im Internet (2021) 363.*