STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Der Staatsminister

SÄCHSISCHES STAATSMINISTERIUM DES INNERN
01095 Dresden

Präsidenten des Sächsischen Landtages
Herrn Dr. Matthias Rößler
Bernhard-von-Lindenau-Platz 1
01067 Dresden

Aktenzeichen
(bitte bei Antwort angeben)
33-0141.50/8983

Dresden, 2. September 2015

Kleine Anfrage des Abgeordneten Enrico Stange, Fraktion DIE LINKE
Drs.-Nr.: 6/2376
Thema: Polizeiermittlungen in digitalen sozialen Netzwerken

Sehr geehrter Herr Präsident,

den Fragen sind folgende Ausführungen vorangestellt:

„Am 04.12.2013 berichtet die Sächsische Zeitung: ‚Die Ressortchefs sind sich offenbar einig, dass das Nutzen sozialer Netzwerke bei der Suche nach Tatverdächtigen prinzipiell rechtlich zulässig ist. Allerdings sollen die Justizminister dazu noch Richtlinien erarbeiten. Ab wann die Polizei in Sachsen per Facebook fahndet, ist noch unklar, wie es gestern aus dem Dresdner Innenministerium hieß. Unter dem Kürzel ‚DigiPol' diskutiert eine Arbeitsgruppe den Einsatz neuer Medien bei der Polizei und entwickelt Projekte dazu.' (Quelle: http://www.sz-online.de/sachsen/polizei-soll-ueber-facebook-ermitteln-2722811.html, letzter Zugriff 04.08.2015)"

Namens und im Auftrag der Sächsischen Staatsregierung beantworte ich die Kleine Anfrage wie folgt:

Frage 1:
Wurden bisher Richtlinien zum Einsatz digitaler Medien und digitaler sozialer Netzwerke in der Fahndungsarbeit der sächsischen Polizei erarbeitet und wenn ja welche?

Im Rahmen des in der Antwort auf die Frage 4 beschriebenen Projektes „DigiPol" wurde die als Anlage beigefügte Handlungsrichtlinie „Öffentlichkeitsfahndung unter Berücksichtigung des Einsatzes sozialer Medien" erarbeitet.

Hausanschrift:
Sächsisches Staatsministerium des Innern
Wilhelm-Buck-Str. 2
01097 Dresden

Telefon +49 351 564-0
Telefax +49 351 564-3199
www.smi.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den Straßenbahnlinien 3, 6, 7, 8, 13

Besucherparkplätze:
Bitte beim Empfang Wilhelm-Buck-Str. 2 oder 4 melden.

Frage 2:
Betreibt die sächsische Polizei Fahndungsarbeit über digitale soziale Netzwerke wie Facebook, Twitter etc. und aufgrund welcher Rechtsvorschriften?

Ja.

Die Rechtsgrundlagen ergeben sich aus dem Polizeigesetz und der Strafprozessordnung. Ergänzend kommen die Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) Anlage B - Richtlinien über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren zur Anwendung.

Frage 3:
Betreibt die sächsische Polizei anlassunabhängige Recherche in sozialen Medien, Blogs und Internetseiten, wenn nein warum nicht? (Bitte aufschlüsseln nach Dienststellen, Personalstellen und Art der Recherche!)

Die sächsische Polizei führt Recherchen im Netz vor allem verfahrensbezogen durch. Das heißt, dass eine Recherche in den Fällen vorgenommen wird, in denen bereits ein strafrechtlich relevanter Hinweis vorliegt, dem zur Aufklärung der Straftat und Verdichtung der Beweislage gezielt nachgegangen wird. Darüber hinaus führt die Polizei im Vorfeld und während planbarer Einsatzlagen verfahrensunabhängige Recherchen durch.

Im Zusammenhang mit der Lageentwicklung im Bereich „Asyl" wurde das Operative Abwehrzentrum (OAZ) aktuell beauftragt, die Zweckmäßigkeit und praktische Umsetzbarkeit verfahrensunabhängiger Recherchen für das Aufgabenfeld „PMK rechts mit Schwerpunkt Angriffe auf Asylbewerberunterkünfte" zu prüfen.

Frage 4:
Welche Projekte mit welchen Ergebnissen wurden in der Arbeitsgruppe „DigiPol" bisher entwickelt?

„DigiPol" ist selbst als Projekt angelegt und entwickelt keine weiteren Projekte. „DigiPol" ist noch nicht abgeschlossen. Wesentliche Zwischenergebnisse des Projekts sind die Inbetriebnahme der Facebookseiten
https://de-de.facebook.com/polizeisachsen.karriere und
https://www.facebook.com/polizeisachsen.info
sowie der testweise Einsatz des Twitterkanals https://twitter.com/PolizeiSachsen für Zwecke der Öffentlichkeitsarbeit bei Polizeieinsätzen.

Frage 5:
In welcher Form werden digitale soziale Netzwerke in der Arbeit der sächsischen Polizei eingesetzt? (Bitte aufschlüsseln nach sozialen Netzwerken!)

Im Bereich der Öffentlichkeitsarbeit werden die digitalen sozialen Netzwerke „Facebook" und „Twitter" von der sächsischen Polizei genutzt. Die sächsische Polizei nutzt die Facebookseite https://de-de.facebook.com/polizeisachsen.karriere zur Werbung geeigneten Nachwuchses für die jährlich zu vergebenden Ausbildungs- und Studien-

plätze und die Facebookseite https://www.facebook.com/polizeisachsen.info im Rahmen der allgemeinen Öffentlichkeitsarbeit.

Den Twitterkanal https://twitter.com/PolizeiSachsen nutzt die sächsische Polizei für die automatisierte Verbreitung der Pressemitteilungen einzelner Behörden.

In der Zeit von Februar 2015 bis Juli 2015 hat die sächsische Polizei den o. g. Twitterkanal testweise auch zur Öffentlichkeitsarbeit während größerer Polizeieinsätze genutzt; über die Fortführung ist noch nicht abschließend entschieden.

Mit freundlichen Grüßen

Markus Ulbig

Anlage

Öffentlichkeitsfahndung

unter besonderer Berücksichtigung des Einsatzes sozialer Medien

1 Ausgangslage

Eine Öffentlichkeitsfahndung ist die Suche nach Personen oder Sachen unter Inanspruchnahme der Bevölkerung. Sie erfolgt zu strafprozessualen Zwecken auf der Grundlage der §§ 131 ff. Strafprozessordnung (StPO). Sie wendet sich an eine bestimmte Zielgruppe oder an einen unbestimmten Teil der Bevölkerung. Darüber hinaus kann eine Öffentlichkeitsfahndung auch zum Zwecke der Gefahrenabwehr erfolgen.

Es wird deshalb zwischen der Sachfahndung (z. B. Suche nach speziellem Diebesgut) und der Personenfahndung unterschieden, wobei zu letzterer die Fahndungen nach vermissten Personen, nach Zeugen und nach Tatverdächtigen oder verurteilten Straftätern zählen.

Im Vordergrund steht hierbei die datenschutzrechtlich hervorstechende Personenfahndung. Die Sachfahndung hat regelmäßig keine personenbezogenen Daten und ist deshalb datenschutzrechtlich weniger relevant. Personenbezogene Daten spielen hier ggf. in der Nutzerreaktion eine Rolle. Insoweit kann auf die Ausführungen im Gesamtkonzept verwiesen werden, die sich mit dem Nutzerverhalten befassen: Wichtig ist der dringende Apell, für sachdienliche Hinweise nicht die von den sozialen Netzwerken selbst angebotenen Kommunikationswege[1] zu nutzen, sondern direkt die Polizei über angegebene Verbindungswege[2] zu informieren. Allgemeine Zeugenaufrufe (ohne Abbildung von Personen bzw. Personendaten) und die Fahndung nach Sachen werden hier nicht gesondert thematisiert.

Die Fahndung unter Einbeziehung der Öffentlichkeit hat sich seit der Einführung des polizeilichen Steckbriefes grundlegend weiterentwickelt. Heute kann zu Fahndungszwecken auf moderne Massenmedien zurückgegriffen werden, um den Aufenthaltsort von Personen zu ermitteln oder unbekannte Personen zu identifizieren.

Die Öffentlichkeitsfahndung richtet sich an die gesamte Bevölkerung, zumindest aber an regional oder thematisch eingrenzbare Teile der Bevölkerung. Sie erfolgt in offen zugänglichen Medien außerhalb des unmittelbaren Einflussbereiches der Polizeibehörden.

Neben den klassischen Massenmedien – Printmedien, Hörfunk und Fernsehen – zählt hierzu auch das Internet sowie die darin bestehenden sozialen Netzwerke. Außerdem bestehen weitere Informationsverbreitungskanäle wie u. a. der Kurznachrichtendienst „Twitter" mit rund 3,7 Mio. Nutzern oder Apps, welche für eine Öffentlichkeitsfahndung grundsätzlich nutzbar sind. So ist es möglich, mit der wachsenden Mobilität einzelner Täter und organisierten Kriminalitätsstrukturen Schritt zu halten.

---

[1] Nachrichten, Kommentare, Antworten etc.
[2] Post, Telefon, Telefax, E-Mail

2 Abwägung

2.1 Allgemeine Grundlagen

Angesichts des geänderten Kommunikationsverhaltens erreichen bislang genutzte und bewährte Instrumente der Öffentlichkeitsfahndung, die sich vor allem auf die „klassischen" Medien Hörfunk, Fernsehen, Fachzeitschriften und Tageszeitungen beschränkten, nur noch bedingt die geeigneten Adressaten. Insbesondere jüngere Bevölkerungsschichten nutzen intensiv die interaktiven Kommunikationsmöglichkeiten der sozialen Netzwerke; über herkömmliche Kommunikations- und Informationskanäle sind sie weniger bis kaum noch zu erreichen. Die alleinige Nutzung „klassischer" Medien reicht somit für eine adäquate Informationssteuerung im Zuge der Öffentlichkeitsfahndung nicht mehr aus. Es bedarf daher einer ergänzenden offensiven Nutzung der sozialen Netzwerke. Das interaktive Kommunikationsverhalten soll genutzt werden, um dadurch auch den Fahndungsdruck auf gesuchte Tatverdächtige zu erhöhen. Vorrangig geht es darum, dass die Aufmerksamkeit der Nutzer geweckt wird und sie die Fahndungsnachricht weiterverbreiten. Sie soll einem möglichst großen Kreis potentieller Zeugen bekannt werden.

Fahndung in sozialen Netzwerken bedeutet Fahndung im Internet. Die Fahndung im Internet stellt im Vergleich zu anderen Medien einen starken Eingriff in das Persönlichkeitsrecht des Betroffenen (Beschuldigter/Zeuge) dar und ist daher die sensibelste Form der Öffentlichkeitsfahndung.

Jeder bei Facebook eingestellte Beitrag wird automatisiert auf Server in die USA (Facebook ist ein soziales Netzwerk, das vom Unternehmen Facebook Inc. mit Sitz in Menlo Park, Kalifornien, betrieben wird; die europäischen Nutzer haben gleichwohl einen Vertrag mit der Facebook Ltd. in Irland)[3] transferiert, dort gespeichert und in verschiedenen Formen weiterverarbeitet. Fotos oder Personendaten, die auf Facebook gepostet werden, gelangen unweigerlich auf ausländische Server.

Die Polizei - als einstellende Behörde - gibt bei einer Einstellung die weitere Verwendung der Daten (Datenhoheit) an Facebook ab. Facebook kann durch deutsche Aufsichtsbehörden nicht wirksam beaufsichtigt werden. Einmal eingestellte Daten können zwar wieder gelöscht werden, doch können sie zu diesem Zeitpunkt längst viele Male "geteilt", weitergegeben oder kopiert worden sein und in den Weiten des Netzes weiter kursieren – möglicherweise mit weitreichenden Folgen für den Betroffenen.

Facebook Ltd. unterliegt dem (schwachen) irischen Datenschutzrecht und wird durch die (schwache) irische Datenschutzbehörde kontrolliert.[4] Auf Facebook greifen ausländische Nachrichtendienste zu und werten Geschehnisse aus. Die AGBs enthalten überraschende, verbraucherschädigende und unwirksame Klauseln (gem. §§ 305 ff. Bürgerliches Gesetzbuch). Die Pflicht zur vollständigen Löschung von Daten (gem. § 35 Abs. 2 Bundesdatenschutzgesetz) wird teilweise nicht umgesetzt.

2.2 Strafprozessuale Grundlagen

Die Nutzung der öffentlich zugänglichen elektronischen Kommunikationsmittel zu Fahndungszwecken stellt stets eine Öffentlichkeitsfahndung dar, die nur bei Vorliegen der gesetzlichen Voraussetzungen, insbesondere § 131 Abs. 3 sowie §§ 131a Abs. 3, 131b, 131c Abs. 1 Satz 1, 131 Abs. 2 StPO, in Betracht kommt.

[3] vgl. Vortrag Bannasch, RL beim SächsDSB, vom 26.11.2013
[4] Entscheidung des OVG Schleswig-Holstein vom 22.04.2013 (Az.: 4 MB 10/13 und Az.: 4 MB 11/13)

Grundlage der Öffentlichkeitsfahndung für die Polizei ist der staatsanwaltschaftliche bzw. richterliche Beschluss. Dieser richtet sich nach den Richtlinien für das Straf- und Bußgeldverfahren (RiStBV), Anlage B.

Nummer 3.2 der Anlage B zur RiStBV sieht zur Nutzung des Internets bislang vor, dass „private Internetanbieter grundsätzlich nicht eingeschaltet werden sollen". Zweck dieser Regelung ist die Vermeidung einer unkontrollierten Weitergabe sowie die Sicherstellung einer abschließenden Löschung von personenbezogenen Daten spätestens nach Abschluss einer Fahndung. Wenn Fahndungsmaßnahmen in sozialen Netzwerken aber künftig nicht nur – wie bislang – im Ausnahmefall zugelassen werden sollen, ist es angezeigt, die RiStBV an die neue Situation anzupassen. Die Justizministerkonferenz hat deshalb auf ihrer 84. Sitzung vom 24. November 2013 auch beschlossen, die RiStBV entsprechend zu überarbeiten. Die Änderung ist gegenwärtig in Vorbereitung. Insofern fehlen noch genau festgelegte Kriterien zum Einsatz sozialer Netzwerke bei einer Öffentlichkeitsfahndung.

In der Praxis enthält der staatsanwaltschaftliche/richterliche Beschluss regelmäßig keine konkreten Festlegungen und lässt mit der Anordnung einer Öffentlichkeitsfahndung das Medium und seine fest umrissene Anwendung offen.

Es ist der Verhältnismäßigkeitsgrundsatz zu beachten.

2.3 Grundsatzposition des Sächsischen Datenschutzbeauftragten

Der SächsDSB spricht sich im Hinblick auf diese besonderen datenschutzrechtlichen Risiken und auf die besonders sensiblen Personendaten dafür aus, dass für die substanziell stärkeren datenschutzrechtlichen Eingriffe besondere und speziell darauf ausgerichtete Vorkehrungen zu treffen sind.

Nach seiner Auffassung kommen die Vorschriften der Strafprozessordnung zur Öffentlichkeitsfahndung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) zwar grundsätzlich auch als Grundlage für Öffentlichkeitsfahndungen im Internet in Betracht, sind jedoch mit Blick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden, weshalb eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden könne. Er lehnt die Nutzung kommentarfähiger Seiten zur Unterstützung der Öffentlichkeitsfahndung grundsätzlich ab, da die Kommentare in der Praxis ein unbeherrschbares Risiko bergen würden. Jedenfalls müsste bereits der Antrag auf richterliche Anordnung einer solchen Maßnahme deren Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret angeben. Konkret festzulegen sei auch die begleitende Nutzung sozialer Netzwerke.

Technisch ist nach Auffassung der Datenschützer weiter sicherzustellen, dass

- die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern privater Anbieter,
- die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch sog. „Web-Crawler" o.ä. so weit als technisch möglich verhindert wird und
- die fahndungsbezogene Kommunikation zwischen Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

2.4 Allgemeine Abwägungsgesichtspunkte

Der Einsatz des Mittels Facebook im Zusammenhang mit der Öffentlichkeitsfahndung ist dann zulässig, wenn er sich als verhältnismäßig darstellt, also einem legitimen Zweck dient, dabei so rechtsschonend und risikovermeidend wie möglich eingesetzt wird und die angewendeten Mittel in einem angemessenen Verhältnis zum verfolgten Ziel stehen.

Bei der Öffentlichkeitsfahndung stehen sich zwei gegensätzliche Intentionen mit den entsprechenden Vorgehensweisen gegenüber, die es auszugleichen gilt. Auf der einen Seite sollen die Vorteile eines sozialen Netzwerks, nämlich die schnelle und umfassende Verfügbarkeit und Verbreitung von Informationen für die polizeiliche Arbeit genutzt werden, um so insbesondere gesuchte Straftäter mit Hilfe der Nutzer finden zu können. Auf der anderen Seite stehen die oben dargestellten (Nr. 2.1 und Nr. 2.3) erheblichen zusätzlichen datenschutzrechtlichen Risiken bei besonders sensiblen Personendaten.

Wenn nach einem Straftäter öffentlich gefahndet wird, ist zusätzlich zu berücksichtigen, dass der datenschutzrechtliche Löschungsanspruch in seiner speziellen Ausprägung des Straftatentilgungsanspruches nach §§ 45, 46 Bundeszentralregistergesetz nicht umgangen wird. In diesem Zusammenhang kommt auch der weltweiten und nicht mehr rückholbaren Datenverbreitung besondere Bedeutung zu, weil die Auswirkungen von existenziellem Charakter sein können, erst recht wenn Unschuldige, z. B. durch Namens- oder Personenverwechslungen oder falsche Schreibweisen, betroffen sind.

2.5 Konkrete Abwägungen / Maßnahmen

Die Grundentscheidung, dass eine Fahndung mit der öffentlichen Darstellung personenbezogener Daten etwa eines Tatverdächtigen verbunden werden kann, wurde vom Gesetzgeber getroffen. Dies schließt ein, dass der mit der Fahndung öffentlich gemachte Verdacht Gegenstand öffentlicher Erörterung wird. Die Öffentlichkeitsfahndung mit ihren Voraussetzungen wird in den §§ 131 ff. StPO geregelt. Die RiStBV konkretisiert dies dahingehend, dass zum Zwecke einer Öffentlichkeitsfahndung auch das Medium Internet genutzt werden kann.

Wenn die Strafverfolgungsbehörden einem geänderten gesellschaftlichen Kommunikationsverhalten folgen und die Öffentlichkeitsfahndung auch auf die Nutzung neuer Medien erstrecken, verfolgen sie hierbei weiterhin einen legitimen Zweck und wählen mit Facebook als dem Unternehmen mit dem größten Nutzerkreis auch ein geeignetes Mittel (zur grundsätzlichen Kritik an Facebook siehe Gesamtkonzept).

Derzeit wird durch Justizministerkonferenz eine Konkretisierung der RiStBV in Bezug auf die Öffentlichkeitfahndung unter Nutzung sozialer Netzwerke verhandelt. Die Novelle soll verfahrensmäßig sicherstellen, dass eine solche Öffentlichkeitsfahndung so rechtsschonend und risikovermeidend wie möglich geschieht. Angestrebt wird zunächst, dass künftig die Antragstellung bereits Konkretisierungen in Bezug auf Art, Umfang und Dauer der Öffentlichkeitsfahndung im Internet enthält. Nach dem derzeitigen Stand ist weiter davon auszugehen, dass geänderte Regelungen der RiStBV

1. die Einbindung sozialer Netzwerke bei der Öffentlichkeitsfahndung zu im Einzelfall schwerwiegenden Straftaten einräumen werden, aber

2. gleichwohl in Fällen, in denen in besonderem Maße die Gefahr diskriminierender Äußerungen oder tätlicher Angriffe besteht, die Erforderlichkeit einer Öffentlichkeitsfahndung im Internet besonders kritisch zu prüfen ist und bei der Gestaltung des Fahndungsaufrufes geeignete Vorkehrungen zur Verringerung solcher Gefahren zu treffen sind, und

3. der Fahndungsaufruf die Aufforderung enthalten soll, sachdienliche Hinweise unmittelbar (z.B. per Telefon oder E-Mail) an die Strafverfolgungsbehörden zu richten und **nicht** in das soziale Netzwerk oder auf Seiten privater Anbieter einzustellen sind.

4. Soweit in sozialen Netzwerken die Kommentierungsfunktion freigeschaltet sei, sind entsprechende Kommentare der Nutzer durch die Strafverfolgungsbehörden rund um die Uhr zu überwachen. Kommentare mit diskriminierendem, strafrechtlich relevantem oder gefährlichem Inhalt seien unverzüglich zu entfernen.

5. Gefordert wird weiter, durch geeignete technische Maßnahmen sicherzustellen, dass die zur Öffentlichkeitsfahndung benötigten personenbezogenen Daten ausschließlich auf Servern im Verantwortungsbereich der Strafverfolgungsbehörden gespeichert/gesichert werden und nicht an private Internetdienstanbieter übermittelt werden.

6. Zur Wahrung der Datenhoheit seien geeignete technische Vorkehrungen nach dem Stand der Technik zu treffen, die eine Weitergabe und einen automatisierten Abruf der personenbezogenen Fahndungsdaten im Internet zumindest erschweren.

Diese Maßgaben sind eine geeignete Basis für ein rechtsschonendes und risikominimierendes sächsisches Vorgehen. Darüber hinaus gilt:

Für die Beurteilung, ob eine schwerwiegende Straftat vorliegt, kann § 35 Abs. 2 Sächsisches Polizeigesetz als Richtschnur herangezogen werden.

In Fällen, in denen aufgrund der Fahndung in besonderem Maß die Gefahr diskriminierender Äußerungen oder tätlicher Übergriffe besteht (z.B. mögliche Aufrufe zur „Lynchjustiz"), ist im Zweifel von einer Öffentlichkeitsfahndung im Internet abzusehen.

Zur verfahrensrechtlichen Absicherung hat die Anordnung in dem staatsanwaltschaftlichen/richterlichen Beschluss konkretisierende Angaben zur Art (genaue Einzelbenennung des Mediums bzw. der Medien, z. B. im Internet mit/ohne Hilfe sozialer Netzwerke), zum Umfang (Benennung der Anzahl der Veröffentlichungen) und zur Dauer der beabsichtigten Öffentlichkeitsfahndung zu enthalten. Die Polizei hat dies – unabhängig von den (neuen) Regelungen zur RiStBV – vor Einleitung einer Öffentlichkeitsfahndung zu prüfen und gegebenenfalls nachzufordern.

Es sind folgende konkrete Sicherheitsvorkehrungen zu treffen, um eine größtmögliche Rechtsschonung und Risikominimierung zu erreichen:

- Die zur Öffentlichkeitsfahndung genutzten personenbezogenen Daten sind nicht auf Facebook selbst einzustellen. Es ist die (im Gesamtkonzept dargestellte) „Link"-Technik anzuwenden. Diese Lösung favorisiert auch der SächsDSB.

  (Danach wird der Sachverhalt auf einer Internetseite der Polizei Sachsen eingestellt. Auf der Fanpage bei Facebook wird dann ein Hinweis auf die Fahndung erstellt, der eine Kurzbeschreibung des zugrunde liegenden Delikts sowie eine sachliche und örtliche Zuordnung enthält. Personenbezogene Daten werden auf Facebook nicht eingestellt. Unter dem Fahndungshinweis/Facebook-Post wird ein „Link" eingesetzt, der den Nutzer durch Anklicken auf die polizeieigene Internetseite führt. Um das Interesse beim Nutzer für den eigentlichen Fahndungssachverhalt auf der Polizei-Seite zu wecken, wird es vom SächsDSB mitgetragen, wenn auf der Facebook-Seite gepixelte Fotos, z. B. zu einem Banküberfall eingestellt werden.)

- Es ist mit klaren und deutlichen Hinweisen darauf hinzuwirken, dass sachdienliche Mitteilungen nicht an/über Facebook, sondern unmittelbar an bestimmte dafür vorge-

sehene Polizeidienststellen zu richten sind, deren Adressen und Telefonnummern benannt werden. Mit diesen hat sich der Hinweisgeber dann ausschließlich außerhalb der Kommunikationsstrukturen sozialer Netzwerke (z. B. per Telefon, Telefax oder E-Mail) in Verbindung zu setzen, auch wenn dies umständlich erscheinen mag.

- In Fällen, bei denen sich Nutzer nicht daran halten und Hinweise im Internet geben, sollten diese Mitteilungen (nach Weiterleitung an die zuständigen Polizeidienststellen) schnell gelöscht werden. Dies erfordert eine einzelne „händische" Herausnahme durch die Polizei.

- Der Appell, dass es nicht um Kommentierung der Fahndung, sondern um sachdienliche Hinweise zu ihr geht, ist sowohl im Kontext der Verlinkung wie bei der Individualkommunikation aufzugreifen. Bei der Öffentlichkeitsfahndung ist es deshalb besonders wichtig, eine polizeiliche Dauerpräsenz (24/7-Prinzip) zu gewährleisten, um zeitnah auf Kommentare und Einträge reagieren zu können.

- Die polizeiliche Dauerpräsenz ist auch deshalb zu gewährleisten, um sicherzustellen, dass fälschlicherweise auf diesem Weg gegebene sachdienliche Hinweise nicht einem größeren Nutzerkreis bekannt werden und auf diese Weise gegebenenfalls Ermittlungsansätze verloren gehen.

- In Bezug auf die von der Polizei geführte „Fahndungsseite", zu der der in Facebook eingebettete Link führt, ist an dieser Stelle auf besondere Sicherungsmaßnahmen hinzuweisen, da ihre Frequentierung aufgrund des viral verbreitbaren Links deutlich erhöht werden soll. Für sie gilt insbesondere das Gebot, dass die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch sog. „Web-Crawler" und ähnliche Dienste so weit als technisch möglich verhindert werden soll.

- Bei der Fahndung im Internet muss die Authentizität des Fahndungsaufrufs gewährleistet sein. Durch geeignete technische Maßnahmen ist deshalb sicherzustellen, dass unberechtigte Veränderungen der Fahndungsaufrufe auf der Polizei-Seite ausgeschlossen sind.

- Von großer Bedeutung sind gerade bei der Öffentlichkeitsfahndung Sicherungsmaßnahmen gegen eine unkontrollierte Weitergabe und eine zweckwidrige Speicherung von (Personen-)Daten sowie einen automatisierten Datenabruf im Internet. Hier kommt in Betracht, Klarnamen und Texte durch Einstellung als Grafiken für Textcrawler unlesbar zu machen und Bilder in verschiedene Einzelbilder aufzuteilen und einzustellen. Die Aufteilung ist beim Betrachten der Bilder nicht sichtbar, kann aber ein vollständiges Scannen und Speichern des Gesamtbildes (etwa zur Erfassung biometrischer Daten) verhindern.

- Auf der Polizeiseite sollte weiter durch technisch-administrative Maßnahmen die Fertigung von Kopien erschwert werden.

- Ein sog. „Screenshot" (Bildschirmfotografie) ist technisch nicht zu verhindern und deshalb immer möglich. Um jedoch auch eine darauf fußende Weiterverbreitung von (Personen-)Daten zumindest etwas einzuschränken, ist eigenhändige Verbreitung von Namen und Bild in Zusammenhang mit der Tat zu untersagen.

3 Spezielles Sollkonzept

3.1 Layout

Der Fahndungsbeitrag wird mit einer signifikanten Überschrift sowie einer kurzen Sachverhaltsschilderung (ähnlich einer Pressemitteilung) dargestellt und beinhaltet den „Link", der zur entsprechenden Fahndungsveröffentlichung auf der Homepage der Polizei Sachsen führt.

Die einzelnen Fahndungsbeiträge fügen sich in das Gesamtlayout der Polizei Sachsen-Fanpage ein.

3.2 Zuständigkeiten, organisatorischer Ablauf

Die Nutzung der Web-2.0-Anwendungen sollte in einen ganzheitlichen Geschäftsprozess integriert werden, in dem die Kanäle der klassischen und neuen Medien für eine Öffentlichkeitsfahndung gleichermaßen und komplementär bedient werden. Dabei sollte ein ineinandergreifendes Zusammenspiel der tangierten Bereiche Ermittlung, Fahndung sowie Presse- und Öffentlichkeitsarbeit erfolgen.

Die zentrale und fachliche Zuständigkeit für die Fahndungsseite auf der Homepage der Polizei Sachsen liegt bei der zuständigen Organisationseinheit des Landeskriminalamts Sachsen (LKA) in der Kernarbeitszeit, danach beim Führungs- und Lagezentrum des LKA. Das LKA ist verantwortlich für die Maßnahmen zum Schutz der auf der Fahndungsseite enthaltenen personenbezogenen Daten vor Weitergabe, Speicherung und automatisierten Abruf sowie für Maßnahmen zum Schutz der Authentizität des Fahndungsinhaltes.

Die für die Öffentlichkeitsfahndung im Internet zuständige Stelle im LKA nimmt eine Beratungsfunktion sowohl für die sachbearbeitenden Dienststellen als auch für das Social Media-Team der sächsischen Polizei nach entsprechender Prüfung der formalen Voraussetzungen wahr.

Ein optimaler Geschäftsprozess sollte wie folgt gestaltet werden:

1. Die sachbearbeitende Polizeidienststelle betreibt das Verfahren und führt den entsprechenden justiziellen Beschluss für die Öffentlichkeitsfahndung im Internet, ggf. einschließlich der Nutzung von Facebook, herbei.

2. Der Beschluss wird mit den einzustellenden Inhalten in Form eines Ersuchens (gemäß VwV-Fahndung) an das LKA gesandt, das den Fahndungssachverhalt ins Internet einstellt.

3. Nach erfolgter Einstellung informiert das LKA per E-Mail das Social Media-Team über die Internetveröffentlichung und leitet diesem zeitgleich den Inhalt und die Linkadresse für die Facebook-Veröffentlichung zu.

4. Eine für Facebook geeignete Fahndung sollte zeitnah auch auf Facebook veröffentlicht werden, um den Nutzern die Möglichkeit zu bieten, diese Polizeifahndungen zur Kenntnis zu nehmen und darauf zu reagieren.

5. Das Social Media-Team erstellt die Bewerbung der Internetveröffentlichung einschließlich Link und übernimmt sodann die Kontrolle und Bearbeitung der Kommentare.

6. Sachdienliche Hinweise sollen außerhalb der sozialen Netzwerke übermittelt werden, damit personenbezogene Daten nicht offengelegt werden. Sollten derartige Informationen dennoch eingehen, sind diese zu sichern/dokumentieren und an die sachbearbeitende Dienststelle weiterzuleiten. Der Inhalt eines solchen Kommentares ist dann zu löschen und in allgemeiner Form zu beantworten (erneuter Hinweis, Verweis etc.).

7. Bei Fahndungserledigung informiert die sachbearbeitende Dienststelle unverzüglich die zentrale Stelle im LKA, sodass von dort eine sofortige Fahndungslöschung im Internet erfolgen kann. Gleichzeitig wird das Social Media-Team per E-Mail von der Löschung in Kenntnis gesetzt, damit die unverzügliche Deaktivierung des Fahndungsaufrufes auf der Facebookseite (Abschlussmeldung) erfolgen kann.

8. Kommentare, die personenbezogene Daten des Tatverdächtigen oder dritter Personen beinhalten oder die diskriminierenden oder ehrverletzenden Charakter haben, sind unverzüglich zu löschen.

9. Aus polizeitaktischen Gründen sind keine Informationen darüber zu erheben und insbesondere in den medialen Raum zu transportieren, wie ein Fahndungserfolg zustande kam. Dazu gehören auch Aussagen darüber, ob eine Fahndung ausschließlich durch die Facebooknutzung erfolgreich war oder nicht.

10. Es ist eine ständige polizeiliche Betreuung des Facebook-Accounts mit den Fahndungslinks nach dem 24/7-Prinzip einzurichten.