Aufsätze

Risiken einer polizeilichen „Facebook-Fahndung“

Der Autor widmet sich der inzwischen gängigen Fahndungspraxis der Polizei, mithilfe digitaler Bilder online „auf Verbrecherjagd“ zu gehen. Grundlage ist ein Beschluss der Justizministerkonferenz vom November 2013, nach dem die sogenannte „Öffentlichkeitsfahndung“ über soziale Netzwerke zulässig ist, falls sie „den datenschutzrechtlichen Anforderungen und rechtsstaatlichen Grundsätzen gleichermaßen genügt“. Ziel einer solchen digitalen Fahndung, so Schiffbauer, sei eine aktivere Bürgerpartizipation, insbesondere die „gesteigerte Wahrnehmung“ jüngerer Menschen. Dafür würden Fahndungen häufig auf Behörden-Webseiten veröffentlicht, zunehmend aber auch in Form von Pressemitteilungen über den externen Anbieter „na-presseportal“, ein Tochterunternehmen der Deutschen Presseagentur (dpa), was eine länderübergreifende Personensuche erleichtere. Parallel dazu fahndeten manche Behörden über eigene Facebook-Seiten, RSS-Feeds und Newsletter. Gestaltung und technische Umsetzung seien bei allen Erscheinungsformen vergleichbar: Zum Bild der Gesuchten erscheine ein Begleittext samt Aktenzeichen. Möglich sei die Partizipation des Bürgers über das schlichte Verlinken oder Teilen der Inhalte in soziale Netzwerke. Gerade Onlineredaktionen von Tageszeitungen griffen jedoch auf die weitere Möglichkeit zurück, die bereitgestellten Bilder herunterzuladen, um sie dann für eigene redaktionelle Zwecke zu nutzen. Der Autor weist zudem auf die Option des isolierten Herunterladens der Bilder (bloßer Rechtsklick – „Grafik speichert unter“) und die damit einhergehende Gefahr der uferlosen Verbreitung der Fahndungsbilder hin. Spätestens dann werde diese Praxis zu einem rechtlichen Problem.

Vor diesem Hintergrund erörtert Schiffbauer die Grundzüge des Rechts am eigenen Bild (§ 22 KUG), das sogar Phantomfotos einschließe. Ohne Einwilligung der abgebildeten Person stellten Verbreitung oder Veröffentlichung grundsätzlich eine Verletzung dieses Rechts dar. Während der Fahndung sei eine solche Abbildung zwar gesetzlich gerechtfertigt, wenn sie etwa zum Zwecke der Rechtspflege erfolge (§ 24 KUG). *Nach Beendigung* der Fahndung lebe allerdings das Recht am eigenen Bild wieder auf. Jeder, der – statt lediglich auf die Webseite der Behörde zu verweisen – das Fahndungsbild herunterlade und veröffentliche, müsse auch dafür Sorge tragen, das Bild wieder aus dem Netz zu entfernen. Ansonsten drohten Abmahnungen und Unterlassungsklagen. Parallel zu dieser Verpflichtung privater Nutzer sei die Polizei dazu verpflichtet, „die von ihr geschaffene Gefahrenlage unkontrollierter Bildverbreitung im Internet einzudämmen“.

Schiffbauer weist schließlich auf den unerwünschten Nebeneffekt der „digitalen Amtsanmaßung“ hin. Auf Facebook fänden sich vermehrt private Seiten, die sich im Gewand eines offiziellen behördlichen Webauftritts präsentierten, inklusiver Verwendung von Namen und Bildsymbolen der Polizeibehörden. Daraus könne schnell ein „digitaler Pranger“ werden. Die Betreiber solcher Seiten machten sich strafbar (u. a. wegen einer Fälschung beweiserheblicher Daten gemäß § 269 Abs. I Hs. 2 StGB), da ihre „gefakten“ Seiten die Zuverlässigkeit des Rechts- und Beweisverkehrs gefährdeten. Es werde suggeriert, dass auf diesem Weg sachdienliche Hinweise an die Polizei gegeben werden könnten, tatsächlich gingen sie jedoch nur dem „Hilfssheriff“ zu. Abschließend stellt Schiffbauer fest, der digitale Steckbrief eigne sich durchaus zu einer effektiven Strafverfolgung. Bürger und Staat seien aber angehalten, dafür Sorge zu tragen, sämtliche Bilddateien nach Beendigung der Fahndung aus dem Netz zu eliminieren. Zudem müsse darauf geachtet werden, einer neuen Ausprägung von Personenjagd in Wildwestmanier Einhalt zu gebieten.

Aufsatz: Steckbrief 2.0 – Fahndungen über das Internet als rechtliche Herausforderung
Autor: Dr. Björn Schiffbauer, Habilitand am Institut für Völkerrecht und ausländisches öffentliches Recht der Universität zu Köln
Quelle: Neue Juristische Wochenschrift (NJW), 15/2014, S. 1.052 – 1.057

Cybermobbing – Plädoyer für einen Straftatbestand im Strafgesetzbuch

Ausgehend von zwei Fällen, in denen sich Jugendliche als direkte Folge von Bloßstellungen im Internet das Leben nahmen, zeigt der Autor auf, dass solche Fälle in Deutschland von der derzeitigen Rechtslage nur lückenhaft erfasst werden. Dabei habe das Problem inzwischen eine erschreckende Dimension angenommen: Aktuellen Studien zufolge sei etwa jeder Dritte 10- bis 18-jährige Deutsche Opfer von Cybermobbing, das den altbekannten Psychoterror gegen Einzelne vom Schulhof in die virtuelle Welt transportiere – mit der verheerenden Auswirkung, „dass der Öffentlichkeitsgrad enorm hoch ist, einmal online veröffentlichte Angriffe so gut wie nicht löschbar sind und es bei der Allgegenwärtigkeit sozialer Netze praktisch keinen Rückzugsraum mehr gibt“.

Cornelius definiert Cybermobbing als „die gezielte, wiederholte und damit anhaltende Bloßstellung, Belästigung oder Ausgrenzung eines Einzelnen durch mehrere andere Personen mittels Nutzung von Informations- und Kommunikationstechnologie“. Das Strafgesetzbuch werde den fatalen Folgen für die Opfer kaum gerecht, urteilt der Autor in seiner Analyse der gegenwärtigen Rechtslage. So seien zwar von den „Beleidigungstatbeständen“ (§§ 185 ff. StGB) ehrverletzende Äußerungen in Form von Unwahrheiten erfasst; reine Indiskretionen wie die Weitergabe wahrer Tatsachen blieben jedoch in der Regel straffrei. Auch der Straftatbestand der *Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen* (§ 201a StGB) erfasse das digitale Mobbing nicht gänzlich. Unter Strafe stehe hier „nur“ das Aufnehmen einer Person, die sich in einer Wohnung oder einem gegen Einblicke besonders geschützten Raum (Umkleide,

Toilette) befindet. Und auch der „Stalking-Paragraf“ (Nachstellung § 238 StGB) betreffe das Cybermobbing nur unzureichend, weil er sich gegen die beharrliche Kontaktaufnahme eines Einzelnen richte; die Dynamik der Beteiligung einer Vielzahl von zunächst Außenstehenden – wie beim Cybermobbing üblich – sei von diesem Straftatbestand nicht erfasst.

Auch weitere signifikante Aspekte des Cybermobbings wie die Reichweite der Verbreitung und die dauerhafte Verfügbarkeit der Informationen im Netz würden von der gegenwärtigen Rechtslage nicht berücksichtigt. Immerhin stehe, so Cornelius, der strafrechtliche Schutz vor Cybermobbing weit oben auf der politischen Agenda: Der Koalitionsvertrag 2013 von CDU/CSU und SPD sehe eine entsprechende Anpassung vor. Begrüßenswert sei dabei die Absicht, den Anwendungsbereich des § 201a StGB auf bloßstellende Bildaufnahmen oder Fotos einer unbekleideten Person zu erstrecken – unabhängig davon, an welchem Ort sie sich befinde (siehe oben).

Cornelius plädiert dafür, einen eigenständigen Straftatbestand für digitales Mobbing einzuführen – angelehnt an den Stalking-Paragrafen, aber unter Berücksichtigung der dynamischen Komponente grenzenlosen Cybermobbings. Dass sich das Strafrecht allein nicht eigne, jeglichen gesellschaftlichen Konflikt zu lösen, bemerkt der Autor abschließend. Insoweit sieht er das Urteil des Europäischen Gerichtshofs gegen Google zum „Recht auf Vergessenwerden“ vom Mai 2014 als Schritt in die richtige Richtung. Notwendig sei ferner eine Aufklärungskampagne in Schulen und in der breiten Öffentlichkeit.

Aufsatz: Plädoyer für einen Cybermobbing-Straftatbestand
Autor: Privatdozent Dr. Kai Cornelius LL.M., vertritt derzeit den Lehrstuhl für Strafrecht und Strafprozessrecht an der Universität Heidelberg
Quelle: Zeitschrift für Rechtspolitik (ZRP) 2014, S. 164 f.

Smart-TV darf Zuschauer nicht grenzenlos ausspähen

Nach Erwartungen der Industrie, denen die Autoren Schmidtmann und Schwiering folgen, wird die Verbreitung internetfähiger Smart-TV-Empfänger in deutschen Haushalten sprunghaft weiter zunehmen. Den Grund sehen sie in der attraktiven Kombination von Fernsehprogrammen mit nicht linearen und interaktiven Onlineangeboten. Als technischer Standard für den neuen System-Mix gilt inzwischen HbbTV („Hybrid broadcast broadband TV“), der Rundfunk- und Breitbandinhalte miteinander verbindet. Ähnlich dem althergebrachten Videotext werden damit zusätzliche Informationen des Programmanbieters angezeigt, nur ließen sich jetzt Fernsehprogramme und Internetinhalte gemeinsam auf einem TV-Bildschirm darstellen.

Blieb der Zuschauer beim klassischen Fernsehen anonym, wird er jetzt identifizierbar, was unter Umständen sein Persönlichkeitsrecht gefährdet. Denn den Anbietern eröffne der neu geschaffene HbbTV-Rückkanal (siehe Anmerkungen) gleichzeitig die Möglichkeit, Nutzerdaten hinsichtlich der Fernsehgewohnheiten/-zeiten oder des Surfverhaltens zu erheben und zu verarbeiten, stellen die Autoren fest. Bei den entsprechenden Datenübermittlungen handle es sich um Telemedien, sodass das Telemediengesetz (TMG) greife. Die Nutzung von Smart-TV produziere eine Vielzahl personenbezogener Daten – schon allein durch die Registrierung für HbbTV-Anwendungen, aber auch zum Nutzungsverhalten von Lieblingsprogrammen, Internetdiensten, Suchbegriffen oder Sehdauer. Laut Gesetz dürfe ein Anbieter derartige (personenbezogene) Daten nur erheben, wenn sie einerseits „zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telemedien erforderlich sind“ (§ 14 TMG Bestandsdaten) oder wenn deren Erhebung *erforderlich ist*, „um die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen“ (§ 15 TMG Nutzungsdaten). Die Abrechnung eines Kaufs mehrerer Kameraperspektiven bei einem Liveevent könnte ein solcher Grund sein. Eindeutig keinem dieser beiden Zwecke dienten jedoch Daten hinsichtlich des Medienverhaltens. Der Anbieter müsse zudem umfassend und transparent über die Datenverarbeitung, also über Art, Umfang und Zweck der Erhebung informieren. Unterbliebe das und missachte der Anbieter die Grenzen der rechtlich zulässigen Datenerhebung, drohten nicht nur Reputationsschäden. Denn die entsprechende Aufsichtsbehörde könne Maßnahmen wie Unterlassungsverfügungen oder Bußgelder in Höhe von bis zu 50.000 Euro erlassen.

Sofern Datenerhebungen dennoch zur Auswertung des Nutzer-/Zuschauerverhaltens erfolgen sollten (z. B. ein sogenanntes Profiling im Interesse der Werbeindustrie), müsse der Anbieter dem Nutzer zumindest ein Opt-out einräumen – also eine technische Option, die Verwendung von Cookies auszuschalten. Des Weiteren müsse ihm ein Widerrufsrecht eingeräumt werden. Auf Nummer sicher gehe der Anbieter jedoch, wenn er ausdrücklich die Einwilligung seiner entsprechend informierten Nutzer einhole (ein sogenanntes Opt-in). Diese Vorgehensweise sei ihm auch bis zur Klärung sämtlicher künftiger Rechtsfragen (Inkrafttreten der neuen EU-Datenschutzgrundverordnung [DS-GVO]) anzuraten.

Anmerkungen:

HbbTV-Rückkanal:
Er ermöglicht einen Kontakt des Nutzers zum Programm- oder Diensteanbieter, der in der Regel über das Internet hergestellt wird. Er kann aktiv für die Teilnahme an Quizsendungen, Feedback und Abstimmungen (Votings) genutzt werden, aber auch passiv zum Messen von Sehgewohnheiten, Zuschauerzahlen und zur Übermittlung personenbezogener Daten.
Cookies:
Diese „Nutzer-Fußabdrücke“ sammeln in Computern oder Smart-TVs automatisch Daten über besuchte Seiten. So können Cookies dem Anwender ersparen, sich beim wiederholten Besuch einer Webseite erneut anzumelden. Allerdings speichern sie auch komplexe Details zum privaten Internetverhalten. Normalerweise können Nutzer ihre Cookies löschen.

Aufsatz: Datenschutzrechtliche Rahmenbedingungen bei Smart-TV. Zulässigkeit von HbbTV-Applikationen
Autoren: Karin Schmidtmann, Rechtsanwältin in Köln; Sebastian Schwiering, Rechtsanwalt in Aachen
Quelle: Zeitschrift für Datenschutz (ZD), 2014, S. 448 f.