www.jusletter-it.eu

Peter Leitner / Farsam Salimi / Leopold Löschl

Social Media Crime: Taxonomie zur Klassifizierung von Kriminalitätsphänomenen in sozialen Medien und rechtliche Empfehlungen

Dieser Beitrag beschreibt zentrale Ergebnisse des Projektes «Social Media Crime», der Entwicklung einer umfassenden Taxonomie zur effizienten Einordnung krimineller Handlungen in sozialen Medien. 15 Phänomene, zusammengefasst in 4 Hauptkategorien, bilden den Kern eines generischen Klassifizierungsmodells. Darüber hinaus wird auch ein standardisiertes und flexibles Social Media Crime Framework mit Aktionsraster vorgestellt, welches die Zusammenhänge zwischen den Phänomenen und den angewandten Vorgehensweisen durch kriminelle Einzeltäter oder Tätergruppen herstellt. Zudem liefert der Beitrag aktuelle Empfehlungen hinsichtlich zukünftiger Reformen der österreichischen Gesetzgebung.

Sammlung: Tagungsband IRIS 2015
Kategorie: Beiträge
Rechtsgebiete: IT-Recht
Region: Österreich

Zitiervorschlag: Peter Leitner / Farsam Salimi / Leopold Löschl, Social Media Crime: Taxonomie zur Klassifizierung von Kriminalitätsphänomenen in sozialen Medien und rechtliche Empfehlungen, in: Jusletter IT IRIS

Inhaltsübersicht

1 Einleitung

[Rz 1] Soziale Medien haben seit ihrer Entstehung unser Kommunikationsverhalten nachhaltig verändert und um neue Alternativen erweitert. Neben zahlreichen Vorteilen werden sie jedoch auch immer öfter Nährboden für kriminelle Aktivitäten. Unter der Bezeichnung Social Media Crime werden **kriminelle Aktivitäten gegen Personen oder Gruppen von Personen unter Nutzung oder zentraler Einbindung sozialer Medien, wie beispielsweise Social Networking, Microblogging oder Media Sharing Sites**[1]**,** zusammengefasst. Dazu zählen unter anderem die Bekanntmachung und Verbreitung illegaler Inhalte, Betrugsdelikte aber auch gezielte Diffamierung bzw. psychische Verletzung einzelner Personen oder Gruppierungen. Das KIRAS Projekt «Social Media Crime» setzte sich detailliert mit kriminalpolizeilich relevanten Phänomenen in sozialen Medien auseinander und entwickelte auf Basis einer umfassenden Fallanalyse erstmals eine einheitliche Taxonomie, die es ermöglicht, einzelne Phänomene aufgrund bestimmter Charakteristika zu isolieren.[2] Der vorliegende Beitrag präsentiert zentrale Projektergebnisse hinsichtlich der erstmaligen Klassifizierung der Phänomene sowie der rechtlichen Empfehlungen für die österreichische Gesetzgebung.

2 Taxonomie zur Klassifizierung von Social Media Crime

[Rz 2] Im Zuge der detaillierten Fallanalyse konnten insgesamt 15 Phänomene identifiziert werden. Wie folgende Abbildung zeigt, konnten diese aufgrund ihrer Ausrichtung und zugrundeliegenden Vorgehensweisen auf vier Cluster aufgeteilt werden.

---

1 Leitner, 2013, Social Media Crime: Towards a Common Understanding of an Emerging Phenomenon. Proceedings of the IADIS International Conference Internet Technologies & Society 2013, Kuala Lumpur, Malaysia, 29. November—1. Dezember 2013, IADIS Press, pp. 119—124.

2 Vgl. Weiss/Jäger/Leitner, 2014. A Flexible Categorization Model for Contemporary Crime Types in Social Media. In Proceedings of the IADIS WWW/Internet Conference 2014, Porto, Portugal, 25.—27. Oktober 2014, IADIS Press, pp. 391—393.

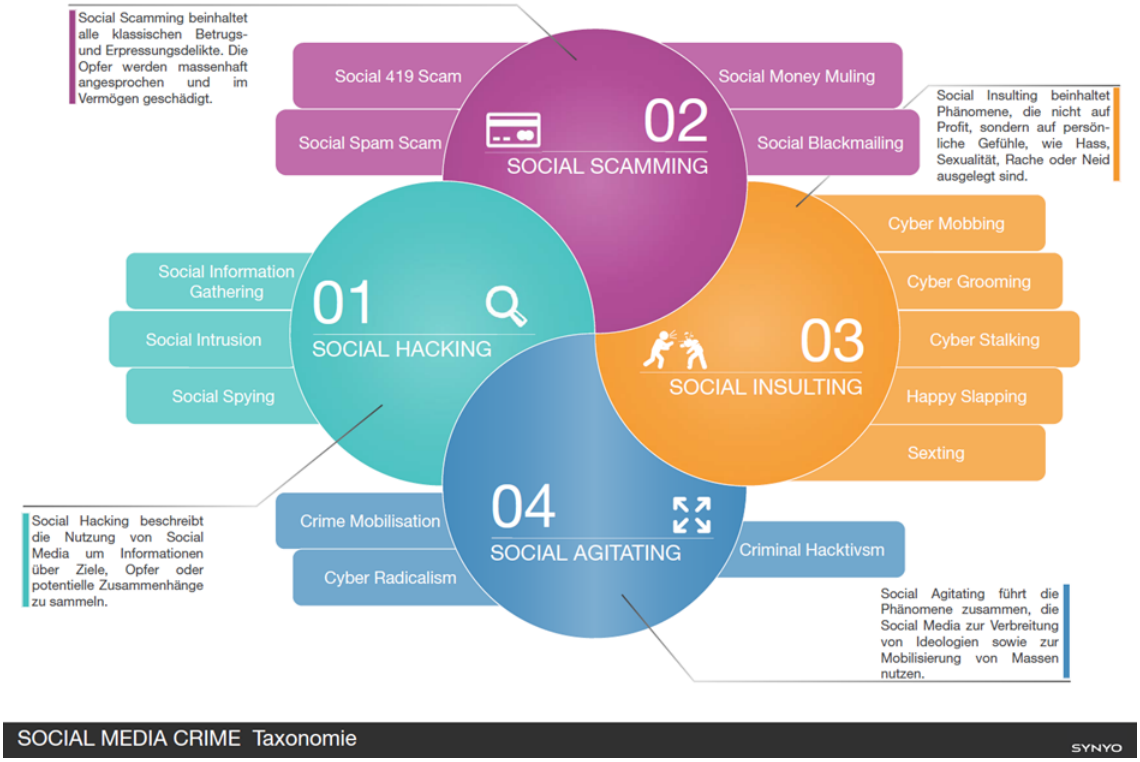

Abbildung 1: Social-Media-Crime-Taxonomie

[Rz 3] Die vier Cluster sowie die dazugehörigen Phänomene werden folgend kurz näher beschrieben:

[Rz 4] **Social Hacking:** Der Cluster beinhaltet Phänomene, die soziale Medien nutzen, um Informationen über Ziele, Opfer oder potentielle Zusammenhänge zu sammeln. Diese können in weiterer Folge für vielerlei Zwecke genutzt werden. Die verschiedenen Phänomene dieses Clusters unterscheiden sich in der Art der Datensammlung. Täter benutzen dabei sowohl legale als auch illegale Methoden.

[Rz 5] *Social Information Gathering:* Ziel ist es, Informationen und Daten über ein Opfer oder dessen Umgebung zu sammeln, um dieses Wissen später für weitere kriminelle Aktivitäten nutzen zu können. Sehr oft ist Social Information Gathering ein Phänomen, das vor der eigentlichen Straftat bzw. zu deren Vorbereitung ausgeführt wird.

[Rz 6] *Social Intrusion:* Definiert das Eindringen in Social Media Accounts, um Profildaten zu «minen», sprich auszulesen, um diese für weitere Zwecke (z.B. Versenden von Spam) nutzbar zu machen.

[Rz 7] *Social Spying:* Gezielte Angriffe auf Social-Media-Nutzer mit dem Ziel, Informationen zu erlangen bzw. vernetzte Systeme zu infiltrieren. Social Spying beinhaltet eine starke Hacking-Komponente und wird vor allem von professionell agierenden Tätern ausgeführt.

[Rz 8] **Social Scamming:** Das Hauptaugenmerk liegt hier auf klassischen Betrugs- und Erpressungsdelikten. Dabei werden potentielle Opfer zumeist per Massenverbreitung über soziale Medien angeschrieben oder angesprochen. Hauptsächlich geht es darum, möglichst schnell Geld zu erbeuten oder auf einfachem Wege kompromittierende Informationen/Fotos/Videos der Opfer zu erlangen, um damit Geld zu erpressen.

[Rz 9] *Social Spam Scam:* Basiert auf der Vortäuschung eines Angebotes oder eines Produkts. Um dieses zu erlangen, müssen User Beiträge oder Seiten teilen, liken oder kommentieren. Dies führt zu einer äuSSerst effektiven und schnellen viralen Verteilung der Spamquelle.

[Rz 10] *Social 419 Scam:* Hierbei handelt es sich um klassischen Vorschussbetrug über soziale Medien. Dabei werden Opfer unter Vorspiegelung falscher Tatsachen für eine ausstehende Gegenleistung zu willentlichen Geldtransaktionen bewegt. Diese Gegenleistung wird durch die Täter jedoch nie erbracht.

[Rz 11] *Social Money Muling:* Personen werden über soziale Netze als Kuriere für Geldwäsche angelockt. Missbrauchte Geldkuriere (Money Mules) sind Opfer organisierter Kriminalität und werden zumeist nur für kleine Beträge eingesetzt (Micro Laundering).

[Rz 12] *Social Blackmailing:* Beinhaltet das gezielte Erpressen von Opfern. Die Täter drohen oftmals mit Veröffentlichung von kompromittierenden Materialien (Bilder/Videos), sollten ihre Forderungen nicht erfüllt werden.

[Rz 13] **Social Insulting:** Dieser Cluster beinhaltet Phänomene, die vor allem auf die Beeinträchtigung der Freiheit, Ehre, körperlichen oder sexuellen Integrität und/oder Sicherheit einer einzelnen Person abzielen.

[Rz 14] *Cyber Mobbing:* Darunter versteht man das Beleidigen, Bedrohen, BloSSstellen oder Belästigen anderer Personen mit Hilfe moderner Kommunikationsmittel — meist über einen längeren Zeitraum hinweg.[3] Gruppendynamische Prozesse spielen beim Mobbing generell eine wichtige Rolle.

[Rz 15] *Cyber Stalking:* Das Phänomen bezieht sich auf das Nachspionieren, Belästigen, Ausspähen bis hin zum Bedrohen von Einzelpersonen im virtuellen Raum. Oft ist auch eine Verknüpfung mit dem klassischen Stalking in der «realen» Welt zu erkennen. Cyber Stalking führt durch dauerhaften und psychischen Druck zu einer massiven Beeinträchtigung der Lebensqualität des Opfers.

[Rz 16] *Cyber Grooming:* Hierbei handelt es sich um das gezielte Ansprechen von unmündigen Personen im Internet mit dem Ziel der Anbahnung sexueller Kontakte.[4]

[Rz 17] *Sexting:* Als Sexting wird grundsätzlich der Austausch eigener intimer Fotos (bzw. auch Texte) verstanden, wobei das Senden der Inhalte beabsichtigt und gewünscht ist. Problematisch wird Sexting vor allem dann, wenn die ausgetauschten Inhalte anderen Personen oder Personengruppen zugänglich gemacht werden oder wenn Bildmaterialien minderjährige Personen darstellen.

[Rz 18] *Happy Slapping:* Das Phänomen beinhaltet grundlose Angriffe auf dem Täter zumeist nicht bekannte Personen. Die Angriffe werden gefilmt und anschlieSSend über soziale Medien verbreitet.

[Rz 19] **Social Agitating:** Dieser Cluster bezieht sich vor allem auf die Nutzung von Social Media zur Verbreitung von ideologischen Inhalten, zur Mobilisierung von Massen und daraus folgend zur Störung der öffentlichen Ordnung/Sicherheit. Die Phänomene sind in den meisten identifizierten Fällen eher durch persönliche Einstellungen als durch Profitstreben motiviert.

---

3 Siehe http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das/ aufgerufen: 3. Februar 2015.

4 Vgl. Bundesministerium für Inneres — Bundeskriminalamt, 2013. Schutz vor Grooming. Abrufbar unter: http://www.bmi.gv.at/cms/BK/presse/files/Prventionstipps_Grooming.pdf aufgerufen: 3. Februar 2015.

[Rz 20] *Criminal Hacktivism:* Oftmals handelt es sich hier lediglich um Defacements (Veränderungen) von Webseiten, um dadurch auf gesellschaftspolitische Probleme aufmerksam zu machen. Nichts desto trotz werden dabei strafbare Aktionen gesetzt. In manchen Fällen werden auch gezielt Datensätze von Organisationen «gestohlen», um diese entweder zu veröffentlichen oder um die betroffenen Organisationen zu nötigen. Dahinter stehen in den meisten Fällen keine Geldforderungen, sondern Forderungen ideeller Natur.

[Rz 21] *Crime Mobilisation:* Bezeichnet eine gezielte Versammlung von Personen mit der Absicht, Straftaten wie z.B. Sachbeschädigung oder Diebstahl zu begehen. Die Verabredung und Mobilisierung der Personen findet über soziale Medien statt.

[Rz 22] *Cyber Radicalism:* Hier werden ideologische Botschaften und Propaganda durch den Einsatz von Online-Medien, einschlieSSlich sozialer Netzwerke wie Facebook, Twitter und YouTube verbreitet. Diese radikalen Ansichten können sowohl politisch als auch religiös motiviert sein.

3 Social Media Crime Framework und Aktionsraster

[Rz 23] Bisher gab es keine einheitliche Strukturierung von strafrechtlich relevanten Phänomenen in sozialen Medien. Um dieses Problem zu lösen, wurde das ein «Social Media Crime Framework» erstellt, welches eine nachvollziehbare Strukturierung von kriminalpolizeilich relevanten Phänomenen in sozialen Medien ermöglicht. Jedes identifizierte Phänomen besteht dabei aus einzelnen Aktionen, die vom Angreifer eingesetzt werden. Diese Aktionen des Täters können sowohl in den Bereich illegaler als auch legaler (z.B. Nutzung öffentlich einsehbarer Daten in Social Media, um eine Tat vorzubereiten) Handlungen fallen. Die Aktionen wurden anhand einer umfangreichen Fallerhebung (252 Fälle) und detaillierten Analyse (52 ausgewählte Fälle), identifiziert. Phänomene, die sich ähnlicher Aktionen bedienen und ähnliche Ziele aufweisen, können so zu gröSSeren Clustern zusammengefasst werden. Einzelne Phänomene waren bisher besonders deshalb schwer miteinander zu vergleichen, da Täter nicht immer exakt gleiche Vorgehensweisen nutzen bzw. unterschiedliche Aktionen kombinieren. Das vorliegende Framework ermöglicht es, festzustellen, welche Phänomene häufig in Kombination auftreten bzw. Ähnlichkeiten aufweisen. Aufgrund der hohen Entwicklungsdynamik im Bereich Social Media wurde das Framework so konstruiert, dass es in Zukunft einfach erweitert werden kann, sollte ein Phänomen auftreten, welches sich bisher nicht bekannter Aktionen bedient bzw. bestehende neu kombiniert.

[Rz 24] Folgende Abbildung stellt die 21 identifizierten Aktionen den 15 isolierten Social Media Crime Phänomenen gegenüber. Jede Aktion kann weitere Subkategorien enthalten (z.B. 8 — Verbreitung illegaler Inhalte in 8A — Verbreitung rechtsradikaler Inhalte und 8B — Verbreitung von Pornographie Minderjähriger). Durch diese Subunterteilung ist es möglich, eine Erweiterbarkeit des Rasters zu garantieren. Um eine bessere Übersicht zu gewährleisten, wird in der folgenden Abbildung jedoch lediglich die Hauptkategorie der jeweiligen Aktion angeführt und in Beziehung mit den einzelnen Phänomenen gesetzt.

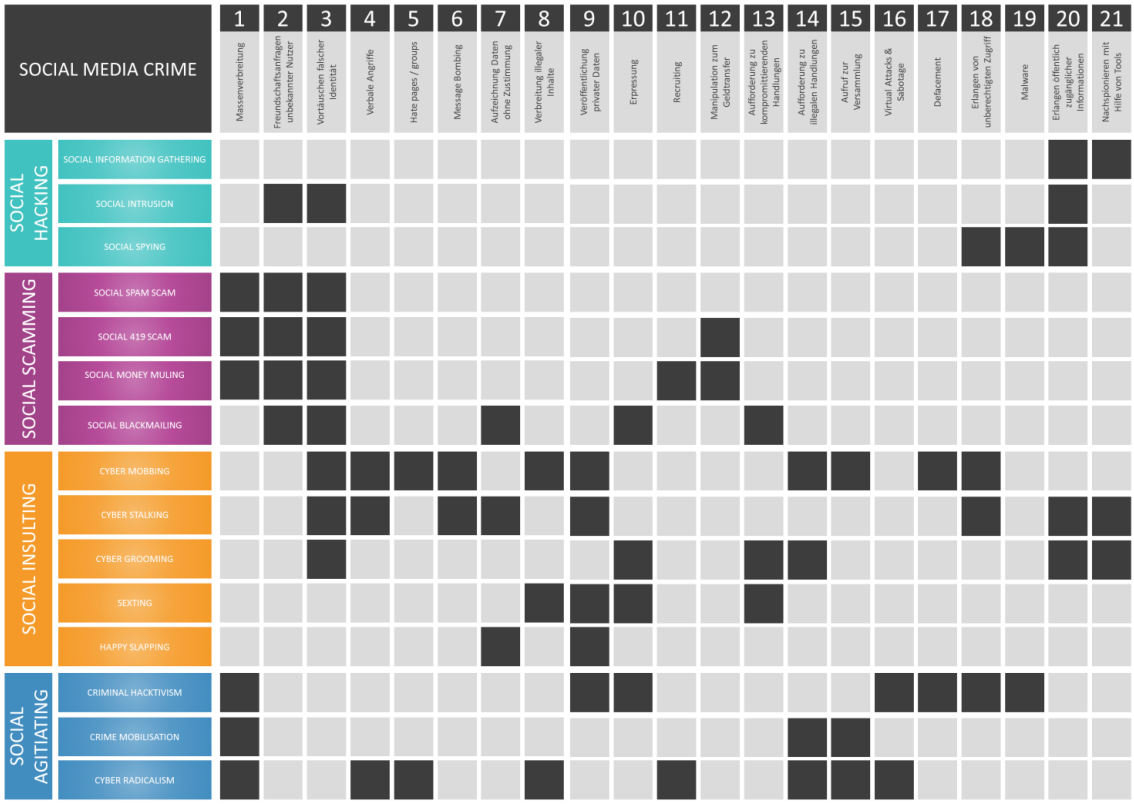

Abbildung 2: Social-Media-Crime-Aktionsraster

[Rz 25] In sozialen Medien können Nutzer unterschiedlichste Rollen einnehmen und dabei auf verschiedenste Art und Weise mit anderen Individuen oder Gruppen interagieren. Neben der Kontaktaufnahme zu anderen Nutzern, der zielgerichteten Verteilung von Informationen oder kollaborativen Handlungen bieten die diversen Social Media Sites (Microblogging, Media Sharing, Networking etc.) auch technische Möglichkeiten, eine groSSe Masse an Personen zeitnah zu erreichen. Dabei ist es aus analytischer Sicht zweckmäSSig, die unterschiedlichen Interaktionsebenen getrennt zu betrachten.

[Rz 26] Bezogen auf die identifizierten Phänomene im Bereich Social Media Crime wurde zur detaillierten Darstellung des Nutzungsverhaltens eine Gliederung gemäSS folgender vier Verwendungsformen vorgenommen:

> **Informationsmedium (I):** Social Media werden genutzt, um Informationen über eine Person/Gruppe /Bewegung/Organisation etc. zu erhalten. **Kontaktmedium (K):** Social Media werden genutzt, um in Kontakt mit einer Person/Gruppe /Bewegung/Organisation zu treten. **Ausführungsmedium (A):** Social Media werden genutzt, um Straftaten zu begehen. **Verbreitungsmedium (V):** Social Media werden genutzt, um Informationen an einen möglichst breiten Personenkreis zu verteilen.

[Rz 27] Unterscheidet man verschiedene Phänomene nach der jeweiligen Art der Social-Media-Nutzung, werden spezifische Eigenschaften der Cluster sowie Abgrenzungen voneinander deutlich erkennbar.

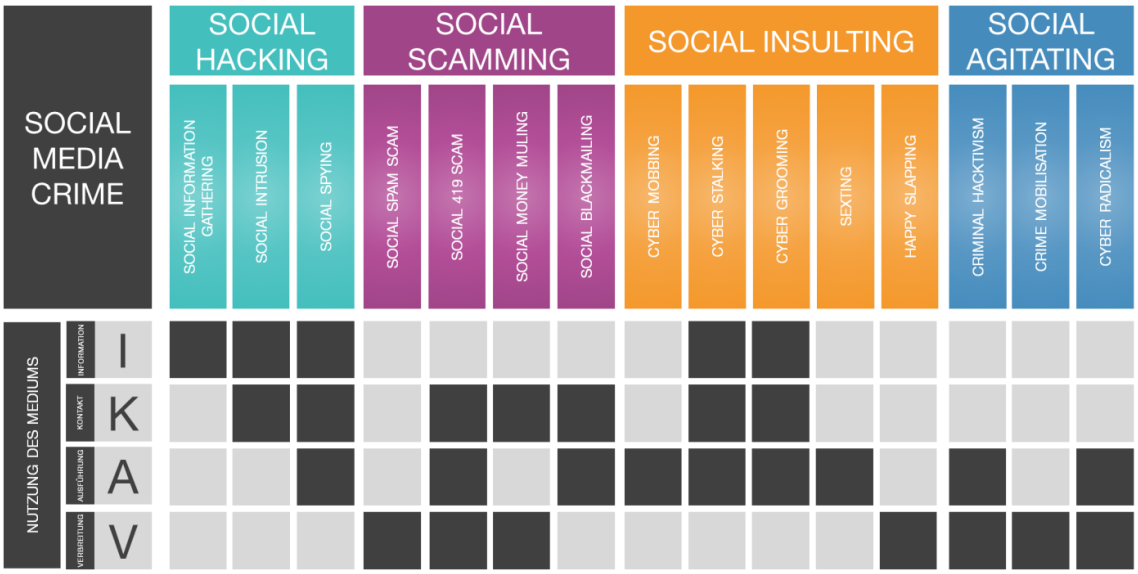

Abbildung 3: Nutzung von Social Media bezogen auf einzelne Phänomene

[Rz 28] *Social Hacking* zeichnet sich durch eine starke Nutzung des Mediums im Sinne der Informationsbeschaffung aus, wobei die jeweiligen Phänomene aufeinander aufbauend sind. *Social Scamming* ist der Cluster der klassischen Betrugsdelikte. Daher ist hier auch eine eindeutige Tendenz zur Nutzung des Mediums zur Kontaktaufnahme als auch zur Verbreitung erkennbar. Ganz deutlich identifizierbar ist auch die starke Ausführungskomponente des Clusters *Social Insulting*. Es gilt anzumerken, dass Happy Slapping sich hier zwar bezüglich der Mediennutzung klar von den anderen Phänomenen abhebt, jedoch die Kernkomponente der «Belästigung eines Individuums» wie bei den anderen Phänomenen im Cluster gegeben ist. *Social Agitating* Phänomene sind besonders auf die Erzeugung von Aufmerksamkeit ausgerichtet. Daher weisen sie hinsichtlich der Nutzung von Social Media eine starke Verbreitungskomponente auf.

4 Ergebnisse aus rechtlicher Sicht

[Rz 29] Im Rahmen der rechtlichen Fallanalyse wurden die realen Fälle mit Bezug zu sozialen Medien anhand der derzeit in Österreich geltenden Straftatbestände untersucht. Die umfassende Fallevaluierung hat gezeigt, dass es für viele kriminelle Phänomene in sozialen Medien nach geltendem Recht ausreichende Reaktionsmöglichkeiten gibt. In einigen Bereichen konnten aber Lücken im Strafrechtsschutz aufgezeigt werden. Der Projektbericht enthält daher eine Reihe von Empfehlungen an den Gesetzgeber, die dazu beitragen sollen, das österreichische Strafrecht an die Anforderungen des Zeitalters sozialer Medien anzupassen.

[Rz 30] So wurde vorgeschlagen, einen eigenen Tatbestand zur strafrechtlichen Erfassung des «**Cybermobbings**» zu schaffen. Die derzeitigen Straftatbestände erfassen nur die einzelnen Mobbing-Handlungen (Beleidigung, Üble Nachrede, Verletzung des Datenschutzrechts, gefährliche Drohung, Nötigung, Verleumdung u.ä.), nicht aber das Gesamtverhalten. Dieser neue Tatbestand soll den besonderen Unwert einer systematischen, über längere Zeit fortgesetzten Verletzung der Ehre oder der Privatsphäre durch ein eigenes Delikt erfassen, das von seiner Grundkonzeption an den

Tatbestand des «Stalkings» in § 107a StGB angelehnt ist.[5] Die Studie enthält konkrete legistische Vorschläge, die Grundlage für eine weitere Diskussion sein können.

[Rz 31] Ein zweiter Schwerpunkt liegt im Bereich des «**Identitätsmissbrauchs**». Die Vornahme von Handlungen im Internet unter fremdem Namen ist derzeit schon in vielen Fällen vom Tatbestand der Datenfälschung nach § 225a StGB erfasst, soweit es um die Erstellung von rechtserheblichen elektronischen Inhalten geht. Eine mögliche Strafbarkeitslücke wurde aber dort erblickt, wo im Namen einer Person im Internet für diese ehrrührige Inhalte verbreitet werden, sodass der Eindruck entsteht, diese Inhalte stammen vom Opfer selbst. Da in solchen Fällen die Einordnung unter den Tatbestand der Üblen Nachrede nach § 111 StGB nicht als gesichert gilt, sollte im Bereich der Ehrbeleidigungsdelikte eine legistische Klarstellung dahingehend erfolgen, dass auch die Unterstellung solcher Inhalte durch Verwendung der fremden Identitätsdaten unter § 111 StGB fallen kann.

[Rz 32] Weiters wurde durch die Studie deutlich, dass die Definition der **gefährlichen Drohung** in § 74 Abs. 1 Z 5 StGB zu eng ist. Eine gefährliche Drohung liegt demnach nur vor, wenn mit der Verletzung bestimmter, dort taxativ aufgezählter Rechtsgüter (Verletzung am Körper, Freiheit, Ehre, Vermögen) gedroht wird. In sozialen Medien wird — oftmals in Kombination mit anderen Phänomenen wie Cybermobbing oder Cyberstalking — die Verletzung anderer Rechtsgüter in Aussicht gestellt. Eine Drohung, intime Details zu veröffentlichen, ist bspw. derzeit strafrechtlich nicht relevant, wenn diese Details keine ehrrührigen Umstände betreffen, was bei Krankheiten oder der sexuellen Orientierung oftmals nicht der Fall ist.[6] Ebenso erscheint — entgegen der aktuellen Rechtsprechung des OGH[7] — die Drohung, Nacktbilder einer Person zu veröffentlichen, nicht in jedem Fall eine Drohung mit der Verletzung des Rechtsguts Ehre zu beinhalten. Vielmehr ist damit jedenfalls eine Verletzung der Privatsphäre angedroht, die aber derzeit nicht unter § 74 Abs. 1 Z 5 StGB fällt. Es wird daher im Projektbericht vorgeschlagen, das Rechtsgut Privatsphäre in den Rechtsgüterkatalog des § 74 Abs. 1 Z 5 StGB aufzunehmen oder alternativ dazu diesen Katalog gänzlich zu streichen.[8]

[Rz 33] Viele der analysierten Fälle betreffen den Missbrauch von **Bildaufnahmen** in sozialen Netzwerken. Damit sind auch Phänomene wie das sog. «Happy Slapping» angesprochen. Der Bildnisschutz ist im österreichischen Strafrecht verhältnismäSSig schwach ausgeprägt. So ist die unbefugte Bildaufnahme strafrechtlich gar nicht erfasst. Die unerlaubte Verwendung und Verbreitung von Bildaufnahmen setzt nach § 51 Datenschutzgesetz (DSG) u.a. voraus, dass die Bilder zuvor widerrechtlich verschafft oder aufgrund der berufsmäSSigen Stellung erlangt wurden.[9] Die Studie schlägt vor, einen eigenen Straftatbestand zu schaffen, der sowohl das Herstellen als auch

---

5 Dieser Vorschlag findet sich schon bei Reindl-Krauskopf, Cyberstrafrecht im Wandel, ALES-Tagung 2014 (in Druck). Ein ähnlich formulierter Vorschlag wurde auch in der Arbeitsgruppe zum StGB 2015 diskutiert, unterscheidet sich vom hier vorgelegten aber durch die Art der Bezugnahme auf die Cyberwelt (im Wege der Telekommunikation oder durch ein Computersystem); abrufbar unter: http://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf aufgerufen: 3. Februar 2015.

6 Vgl OGH 23. Februar 2014, 12 Os 90/13x = Schmoller, JBl 2014, 33; Anzenberger/Sprajc, ÖJZ 2014/49 [Anm.]; Birklbauer/Oberlaber, Drohungen mit Verletzungen der Privatsphäre im straffreien Raum?, JSt 2014, 26 f.; Smutny, juridikum 2014, 168 f. [Anm.].

7 OGH 3. Juli 2014, 12 Os 56/14y = JBl 2015 (in Druck) mit krit. Anm. Salimi; 25. September 2014, 12 Os 52/14k; anders noch OGH 23. Februar 2014, 12 Os 90/13x.

8 Dieser Vorschlag wurde auch von der Arbeitsgruppe zum StGB 2015 aus denselben Überlegungen, wie sie oben dargelegt wurden, erstattet (Bericht unter: http://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf aufgerufen: 3. Februar 2015).

9 Näher Salimi, WK^2 § 51 DSG Rz 21 ff.

das Verbreiten von den höchstpersönlichen Lebensbereich betreffenden Bildaufnahmen (Bilder des unbekleideten Körpers, Kontext zu Sexualleben oder Gesundheitszustand) strafrechtlich erfasst. Zudem wird ein Tatbestand empfohlen, der das Phänomen «Happy Slapping» eigens erfassen soll.[10] Alternativ dazu wird vorgeschlagen, den Anwendungsbereich des § 51 DSG auf all diese Phänomene zu erweitern.

[Rz 34] Viele Fälle, die gemeinhin als «**Hacking**» bezeichnet werden, fallen nicht unter den entsprechenden Straftatbestand des StGB. Der Widerrechtliche Zugriff auf ein Computersystem nach § 118a StGB erfasst nur solche Sachverhalte, in denen der Täter mit der speziellen Absicht handelt, sich von nicht für ihn bestimmten und im System abgespeicherten Daten Kenntnis zu verschaffen, diese zu benützen oder zu verbreiten und sich dadurch zu bereichern oder dem Opfer dadurch einen Nachteil zuzufügen. Diese hohen subjektiven Anforderungen des Tatbestands erschwerten die Anwendung des § 118a StGB erheblich. Die Studie schlägt daher drei Varianten zur Reduzierung dieser Voraussetzungen in § 118a StGB vor.[11]

[Rz 35] Im Bereich des Social Scammings hat die rechtliche Fallanalyse gezeigt, dass die Definition der unbaren Zahlungsmittel in § 74 Abs. 1 Z 10 StGB viele **neue Zahlungsmodalitäten** im Internet nicht ausreichend erfasst. Unbare Zahlungsmittel sind nach geltendem Recht nur körperliche Zahlungsmittel. Zahlungsvorgänge im Internet kommen aber vielfach mit den Daten eines unbaren Zahlungsmittels aus (Kreditkartendaten) bzw. sind losgelöst von solchen körperlichen Zahlungsmitteln (z.B. e-money, Pay-Safe-Codes etc.). Um das Ausspähen und den Missbrauch solcher «unbarer Zahlungsdaten» — parallel zu den unbaren Zahlungsmitteln in den §§ 241a ff. StGB — strafrechtlich zu erfassen, wird eine Erweiterung der Definition in § 74 Abs. 1 Z 10 StGB vorgeschlagen.[12]

[Rz 36] Diese rechtlichen Empfehlungen an den Gesetzgeber könnten im Rahmen des Reformprozesses «StGB 2015» Berücksichtigung finden und sind sicherlich eine wertvolle Diskussionsgrundlage für grundlegende Reformen im Bereich der Cyberkriminalität.

5 Fazit und Ausblick

[Rz 37] Das entwickelte Framework sowie die daraus entstandene Taxonomie basiert auf der Analyse realer Fälle. Das dargestellte Aktionsraster erhebt dabei keinen Anspruch auf Vollständigkeit, sondern versteht sich als anpassungsfähiges Werkzeug, welches laufend anhand neuer Erkenntnisse erweitert werden kann. Aufgrund der hohen Entwicklungsdynamik des Social-Media-Bereiches wurde das Framework besonders flexibel konstruiert. Ziel ist ein fortlaufender wissenschaftlicher Diskurs zur Thematik Social Media Crime. Dieser soll vor allem zu einer genaueren Analyse der Phänomene führen, um so in Zukunft bessere Präventionsmethoden entwickeln zu können. Darüber hinaus haben die rechtliche Evaluierung der gesammelten Fälle sowie die Strukturierung der einzelnen Phänomene bereits dazu beigetragen, dass Lücken im Strafrechtsschutz aufgezeigt und entsprechende Vorschläge für zukünftige Reformprozesse ausgearbeitet werden

[10] Dieser Vorschlag findet sich auch bei Reindl-Krauskopf, Cyberstrafrecht im Wandel, ALES-Tagung 2014 (in Druck).

[11] Diese Varianten wurden auch in der Arbeitsgruppe StGB 2015 diskutiert, Bericht unter: http://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf aufgerufen: 3. Februar 2015).

[12] Auch die Arbeitsgruppe zum StGB 2015 hat dieses Problem erkannt, allerdings keine Erweiterung der Legaldefinition, sondern einen Tatbestand hinsichtlich des Ausspähens von Zahlungsdaten vorgeschlagen (Bericht unter: http://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf aufgerufen: 3. Februar 2015).

konnten.

[Rz 38] Das Projekt «Social Media Crime — Strukturierte Analyse kriminalpolizeilich relevanter Aktivitäten in sozialen Medien und Ableitung eines Methodenrasters» wurde innerhalb des Sicherheitsforschungs-Förderprogramm KIRAS durch das Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT) gefördert und unter Leitung der SYNYO GmbH gemeinsam mit dem Austrian Center for Law Enforcement Sciences (ALES) und dem Bundeskriminalamt (.BK) als Bedarfsträger durchgeführt.

Peter Leitner, Head of Research and Development, SYNYO GmbH, Otto-Bauer-Gasse 5/14, 1060 Wien, AT, peter.leitner@synyo.com; http://www.synyo.com
Farsam Salimi, Wissenschaftlicher Mitarbeiter, Austrian Center for Law Enforcement Sciences (ALES), Universitätsassistent (Post-Doc), Institut für Strafrecht und Kriminologie, Universität Wien, SchenkenstraSSe 4, 1010 Wien, AT, farsam.salimi@univie.ac.at; http://ales.univie.ac.at/
Leopold Löschl, Leiter Cybercrime-Competence-Center C4, Bundeskriminalamt (.BK), Josef-Holaubek-Platz 1, 1090 Wien, AT, leopold.loeschl@bmi.gv.at; http://www.bmi.gv.at/cms/bk/