e-parl 01.11.2022 12:35

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

19. Oktober 2022

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Bericht des Bundesrates in Erfüllung des Postulats 21.3969, Kommission für Rechtsfragen des Nationalrates, vom 25. Juni 2021

BJ-D-15663401/110

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Inhaltsverzeichnis

1 Ausgangslage und Aufbau des Berichts ... 4
1.1 Postulat ... 4
1.2 Vorgeschichte und Einordnung ... 4
1.2.1 Parlamentarische Initiative Suter zum Cybermobbing ... 4
1.2.2 Vorstösse zum Thema «digitale Gewalt» ... 5
1.2.3 Rachepornografie in der Revision des Sexualstrafrechts ... 6
1.2.4 Vorstösse zum Thema «Rechtsdurchsetzung» ... 7
1.3 Auftrag ... 7
1.4 Aufbau des Berichts ... 8
2 Begriffsbestimmungen ... 8
2.1 Cybermobbing ... 8
2.1.1 Umschreibung des Phänomens ... 8
2.1.2 Fallgruppen ... 10
2.1.3 Strafrechtliche Definition ... 10
2.2 Weitere Formen «digitaler Gewalt» ... 11
2.2.1 Entstehung des Begriffs ... 11
2.2.2 Der Gewaltbegriff im Strafrecht ... 12
2.2.3 Die einzelnen Formen ... 12
3 Materielles Recht ... 13
3.1 Zivilrecht ... 13
3.2 Strafrecht ... 14
3.2.1 Cybermobbing ... 14
3.2.1.1 Einschüchterung ... 15
3.2.1.2 Belästigung ... 17
3.2.1.3 Blossstellung ... 19
3.2.2 Hassrede ... 21
3.2.3 Rachepornografie ... 22
3.2.4 Sextortion ... 24
3.2.5 Nicht erfasste Handlungen ... 24
3.3 Regelung in anderen Ländern ... 24
3.3.1 Österreich ... 24
3.3.2 Deutschland ... 26
3.3.3 Frankreich ... 27
3.3.4 Italien ... 27
3.4 Diskussion der Problematik in der Lehre ... 28
3.5 Analyse ... 28
3.5.1 Heterogenität der Verhaltensweisen ... 28
3.5.2 Bestimmtheitsgebot ... 29
3.5.3 Generalpräventive Wirkung ... 29
3.5.4 Beweisschwierigkeiten ... 29
3.5.5 Technologieneutralität des Strafrechts ... 30
3.5.6 Definition aufgrund der Perspektive der betroffenen Person ... 31
3.5.7 Mehrzahl von Handlungen ... 31

3.5.8 Mehrzahl von Personen ... 31
3.6 Handlungsmöglichkeiten des Gesetzgebers ... 32
3.6.1 Eigenständiger Tatbestand zum Mobbing ... 32
3.6.2 Verzicht auf einen eigenständigen Tatbestand ... 32
3.6.3 Strafbarerklärung der Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen ... 33
3.7 Fazit ... 33
4 Rechtsdurchsetzung ... 34
4.1 Ausgangslage ... 34
4.1.1 Problemstellung ... 34
4.1.2 Akteure im Internet ... 35
4.1.3 Cloud Computing als globalisiertes Datenmanagement ... 36
4.2 Zugriff der Strafverfolgungsbehörden auf Daten ... 37
4.2.1 Identifikation des Anschlusses ... 37
4.2.2 Das Territorialitätsprinzip bei der Erhebung von Beweismitteln ... 37
4.2.2.1 Grundsatz ... 37
4.2.2.2 Daten in der Schweiz ... 37
4.2.2.3 Aufforderung zur Datenherausgabe nur an den Dateninhaber ... 38
4.2.2.4 Anwendung des sog. Zugriffsprinzips ... 38
4.2.3 Schranke im StGB: Verletzung fremder Gebietshoheit ... 39
4.2.4 Rechtshilfe ... 40
4.2.4.1 Rechtshilfeersuchen an die USA ... 40
4.2.4.2 Rechtshilfeersuchen an europäische Staaten ... 42
4.2.4.3 Neue Rechtshilfeabkommen zur einfacheren Erhebung von Daten ... 42
4.2.5 Direkter Zugriff auf Grund des Übereinkommens des Europarates über die Cyberkriminalität ... 43
4.3 Strafrechtliche Verantwortlichkeit von Dienstanbietern ... 45
4.3.1 Strafbarer Ungehorsam und Rechtspflegedelikte ... 45
4.3.2 Gehilfenschaft des Dienstanbieters zur Haupttat eines Nutzers ... 45
4.3.3 Anwendbarkeit des Medienstrafrechts ... 46
4.4 Takedown und Sperren von rechtswidrigen Inhalten ... 47
4.4.1 Massnahmen auf strafrechtlicher Basis ... 47
4.4.2 Privatrechtliche Instrumente ... 48
4.4.3 Freiwillige Massnahmen durch Internetunternehmen ... 49
4.5 Gesetzgebungsauftrag: Pflicht zur Bezeichnung von Zustelldomizilen ... 49
4.5.1 Stand der Umsetzung ... 49
4.6 Fazit ... 50
5 Ergebnis ... 51
5.1 Materielles Recht ... 51
5.2 Rechtsdurchsetzung ... 52
6 Literatur- und Materialienverzeichnis ... 53

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

1 Ausgangslage und Aufbau des Berichts

1.1 Postulat

Das Postulat 21.3969 der Kommission für Rechtsfragen des Nationalrates (RK-N) «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch» vom 25. Juni 2021[1] hat folgenden Inhalt:

> **Wortlaut:** Der Bundesrat wird aufgefordert, einen Bericht zu erstellen, wie durch entsprechende Ergänzungen des Strafgesetzbuches (StGB) Cybermobbing und digitale Gewalt bestraft werden können.
>
> **Begründung:** Für betroffene Personen ist «Cybermobbing» unerträglich. Das Strafgesetzbuch (StGB) enthält bereits diverse Artikel, mit welchen «Cybermobbing» bestraft werden können (Art. 173 – Üble Nachrede, Art. 177 – Beschimpfung, Art. 180 – Drohung, Art. 181 – Nötigung, und viele weitere).
>
> Nur den Begriff «Cybermobbing» im Strafgesetzbuch (StGB) aufzuführen, löst die Nöte der Betroffenen nicht.

1.2 Vorgeschichte und Einordnung

1.2.1 Parlamentarische Initiative Suter zum Cybermobbing

Am 11. Juni 2020 hat Nationalrätin *Suter* die *parlamentarische Initiative 20.445 «Neuer Straftatbestand Cybermobbing»*[2] eingereicht. Diese verlangt, das Strafgesetzbuch[3] (StGB) um einen entsprechenden Straftatbestand zu ergänzen. Die Initiantin führt an, das soziale Phänomen des Cybermobbings (auch Cyberbullying, Internetmobbing oder E-Mobbing) habe in den letzten Jahren mit dem Aufkommen von Smartphones stark zugenommen. Im *Unterschied zum herkömmlichen Mobbing* könne die Täterschaft beim Cybermobbing anonym bleiben; die Inhalte könnten schnell und an einen grossen Personenkreis verbreitet werden und seien, einmal im Netz, rund um die Uhr zugänglich und kaum mehr löschbar. Dies setze die angegriffene Person einem äusserst grossen psychischen Leidensdruck aus. In der *Strafverfolgung* sei der Umgang mit Cybermobbing schwierig, da die klassischen Grundtatbestände auf *Einzelhandlungen* ausgelegt seien, die einen bestimmten Erfolg herbeiführen. Bei Cybermobbing wirke aber eher eine Vielzahl von Verhaltensweisen und Handlungen in ihrer Gesamtheit auf das Opfer ein. Die strafbaren Handlungen müssten im StGB so *genau und präzise* wie möglich umschrieben werden; dieses müsse allgemein verständliche Straftatbestände enthalten, die aktuellen sozialen Phänomenen entsprechen, um präventive Wirkung entfalten zu können.

Bei der Beratung der parlamentarischen Initiative am 25. Juni 2021 hielt es die RK-N für angebracht, zunächst *in einem Bericht abklären zu lassen*, wie dem Phänomen Cybermobbing auf strafrechtlichem Weg zielführend begegnet werden kann. Das StGB enthalte bereits verschiedene Artikel, mit welchen Cybermobbing bestraft werden könne; nur diesen Begriff im StGB aufzuführen, löse die Nöte der Betroffenen nicht. Sie weitete die Fragestellung zudem auf die *«digitale Gewalt»* im Allgemeinen aus. Zu diesem Zweck reichte die RK-N in derselben Sitzung das *Postulat 21.3969 «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch»* ein. Gleichzeitig hat sie der parlamentarischen Initiative 20.445 Suter mit 19 zu 0 Stimmen bei 4 Enthaltungen Folge gegeben, um ihrer Ansicht Ausdruck zu verleihen, dass die aktuellen Rechtsgrundlagen den Betroffenen keinen wirksamen Schutz bieten.[4] Der Bundesrat hat am 08. September 2021 die Annahme des Postulats beantragt, der Nationalrat hat es daraufhin am 27. September 2021 diskussionslos angenommen.[5]

---

1 www.parlament.ch > Geschäft 21.3969

2 www.parlament.ch > Geschäft 20.445

3 SR **311.0**

4 www.parlament.ch > Geschäft 20.445 > Medienmitteilung der RK-N vom 25.06.2021

5 AB **2021**1935

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Die Kommission für Rechtsfragen des Ständerates (RK-S) hat sich an ihrer Sitzung vom 20. Januar 2022 mit der parlamentarischen Initiative 20.445 zum Cybermobbing befasst. Sie hat mit 8 zu 5 Stimmen entschieden, der parlamentarischen Initiative vorerst keine Folge zu geben und zunächst den Bericht des Bundesrates in Erfüllung des Postulats abzuwarten. Sie erhofft sich, dass dieser eine breitere Auslegeordnung zu diesem Thema beinhaltet und einen allfälligen Handlungsbedarf klarer aufzeigt.[6]

1.2.2 Vorstösse zum Thema «digitale Gewalt»

In jüngster Zeit wurden verschiedene Vorstösse zur «digitalen Gewalt» eingereicht. Das *Postulat 22.3201 Bellaiche «Digitale Gewalt eindämmen»* vom 17. März 2022, welches der Bundesrat am 18. Mai 2022 zur Annahme empfohlen hat, verlangt einen Bericht über das Ausmass von digitaler Gewalt in der Schweiz und Massnahmen zu deren Bekämpfung.[7] Im Zusammenhang mit dem Untersuchungsgegenstand des vorliegenden Berichts ist zudem die *Interpellation 21.3684 Gysin Greta «Cybergewalt: Sind die rechtlichen Grundlagen angemessen?»* vom 10. Juni 2021 zu erwähnen. Auf die darin gestellte Frage, welche rechtlichen Grundlagen vor Phänomenen der Gewalt, des Hasses und des Mobbings im Netz schützen, verwies der Bundesrat auf verschiedene Tatbestände des StGB[8] sowie auf die Massnahmen gegen Persönlichkeitsverletzungen nach den Artikeln 28 ff. des Zivilgesetzbuches[9] (ZGB). Der Bundesrat betonte aber auch, dass bei der strafrechtlichen Verfolgung von Taten im Internet meistens nicht fehlende materielle Bestimmungen das Problem seien, sondern vielmehr die Rechtsdurchsetzung die grösste Schwierigkeit darstelle.[10] Mit dem *Postulat (Quadranti) Siegenthaler 19.411 «Kinder und Jugendliche vor der Handykamera nicht alleine lassen. Täter stoppen, die Kinder dazu anleiten oder erpressen, sexuelle Handlungen an sich selbst vorzunehmen»* vom 24. September 2019[11] wird ein Bericht zur Frage verlangt, welche rechtlichen, technischen und sonstigen Massnahmen nötig sind, damit Kinder und Jugendliche nicht ungehindert zur Herstellung von kinderpornografischem Material erpresst oder angeleitet werden können. Es wurde am 20. Dezember 2019 vom Nationalrat angenommen. Zu nennen sind ferner die *Interpellationen Gysin Greta 21.3683 «Prävention gegen Cybergewalt»* vom 10. Juni 2021[12] und *22.3156 «Verhütung und Bekämpfung von digitaler Gewalt gemäss den Empfehlungen der Expertengruppe Grevio zur Umsetzung der Istanbul-Konvention»* vom 16. März 2022.[13]

Andere Vorstösse beziehen sich auf *einzelne Formen* «digitaler Gewalt». So das *Postulat 21.3450 «Hassreden. Bestehen gesetzliche Lücken?»* vom 25. März 2021. Damit hat die *Sicherheitspolitische Kommission des Ständerates (SIK-S)* dem Bundesrat den Auftrag erteilt, bis Mitte 2023 einen Bericht zum Regulierungsbedarf vorzulegen. Der beim Bundesamt für Kommunikation (BAKOM) des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK) in Auftrag gegebene Bericht wird einerseits den gesetzgeberischen Handlungsbedarf in diesem Bereich abklären. Andererseits soll er Ausmass und Formen von Hassrede auf den Plattformen der Intermediäre erfassen.[14] Im Anschluss an den Bericht

---

6 www.parlament.ch > Geschäft 20.445 > Medienmitteilung der RK-S vom 20.01.2022

7 Dabei ist insbesondere zu prüfen, wieso digitale Gewalt sich grenzenlos ausbreiten kann, woran die Strafverfolgung gegen digitale Gewalt scheitert, wer besonders betroffen ist und welche Massnahmen ergriffen werden oder welche Anlaufstellen geschaffen werden müssen, um sie einzudämmen: www.parlament.ch > Geschäft 22.3201.

8 Aufgeführt werden namentlich Ehrverletzungsdelikte (Art. 173 ff. StGB), Drohung (Art. 180 StGB), Nötigung (Art. 181 StGB), Pornografie (Art. 197 StGB) oder Erpressung (Art. 156 StGB).

9 SR **210**

10 www.parlament.ch > Geschäft 21.3684; die Interpellation wurde mit der Stellungnahme des Bundesrates vom 01.09.2021 erledigt.

11 www.parlament.ch > Geschäft 19.4111.

12 www.parlament.ch > Geschäft 21.3683; die Interpellation wurde mit der Stellungnahme des Bundesrates vom 01.09.2021 erledigt.

13 www.parlament.ch > Geschäft 22.3156; die Interpellation wurde mit der Stellungnahme des Bundesrates vom 18.05.2022 erledigt.

14 www.parlament.ch > Geschäft 21.3450; der Ständerat hat das Postulat am 08.06.2021 angenommen.

des BAKOM unter Mitwirkung der Bundeskanzlei (BK) «Intermediäre und Kommunikationsplattformen»[15] hat der Bundesrat beim UVEK (BAKOM) ein Aussprachepapier in Auftrag gegeben, das aufzeigt, ob und wie Kommunikationsplattformen reguliert werden könnten. Dieses Aussprachepapier wird auch das Anliegen des Postulats untersuchen. Das BAKOM hat zudem über zwei Call for Projects Forschungsarbeiten im Bereich der digitalen Hassrede ausgeschrieben. Das *Postulat 21.4531 Gysin Greta «Transparenz über Hate-Speech-Vorfälle auf Social Media»* vom 16. Dezember 2021 wurde vom Nationalrat am 09. Mai 2022 entsprechend dem Antrag des Bundesrats angenommen.[16]

Die *parlamentarische Initiative 19.433 der RK-N «StGB-Tatbestände mit Stalking ergänzen»* vom 03. Mai 2019 bezieht sich gemäss Begründung auch auf Lösungsansätze in Bezug auf die Rechtsdurchsetzung bei Cyberstalking.[17] Die *parlamentarische Initiative 18.434 Amherd (Bregy) «Cybergrooming mit Minderjährigen endlich unter Strafe stellen»* vom 14. Juni 2018, welcher von den Räten Folge gegeben worden ist,[18] wird im Rahmen der Strafrahmenharmonisierung und Anpassung des Nebenstrafrechts an das neue Sanktionenrecht, Vorlage 3 zur Revision des Sexualstrafrechts,[19] beraten. Der Ständerat hat gemäss dem Antrag seiner vorberatenden Kommission die Einführung eines spezifischen Grooming-Tatbestandes abgelehnt. Denn das geltende Recht erfasst Grooming i.e.S.[20] bereits über den Versuch der entsprechenden Tathandlungen. Ein spezifischer Tatbestand ginge kaum über das hinaus, was bereits strafbar ist, und würde sich in seiner Wirkung primär auf symbolische Gesetzgebung beschränken. Ausserdem würden sich schwierige Konkurrenzprobleme zu den geltenden Tatbeständen stellen. Da für solche Vorbereitungshandlungen lediglich eine vage objektive Schwelle der Strafbarkeit festgelegt werden könnte, würde sich das Gewicht auf die subjektive Seite, d.h. die Absicht verlagern, womit ein solcher Tatbestand in die Nähe des verpönten Gesinnungsstrafrechts zu geraten droht. Die Vorlage wird nun noch vom Nationalrat beraten.[21]

1.2.3 Rachepornografie in der Revision des Sexualstrafrechts

Im Rahmen der *Revision des Sexualstrafrechts* schlug die RK-S mit 11 zu 1 Stimmen einen neuen Straftatbestand vor, der das Phänomen des *«Revenge Porn»* bzw. der *«Rachepornografie»* erfassen sollte.[22] In der Vernehmlassung zur Revision des Sexualstrafrechts hatten einzelne Teilnehmende die Auffassung vertreten, dass die geltenden Bestimmungen diesem Phänomen nicht ausreichend Rechnung zu tragen vermögen.[23] Der von der RK-S vorgeschlagene Tatbestand (Art. 197*a* E-StGB) kriminalisiert das unbefugte Weiterleiten von nicht öffentlichen sexuellen Inhalten. Als typisches Beispiel hierfür wird genannt, dass intime Fotos oder Videos, die ursprünglich in einer Paarbeziehung einvernehmlich aufgenommen wurden, später ohne Einverständnis der abgebildeten Person zugänglich gemacht werden.[24]

Eine Kommissionsminderheit beantragte, auf die Einführung eines neuen Artikels 197*a* E-StGB zu verzichten: Die Bestimmung sollte nicht bei den strafbaren Handlungen gegen die sexuelle Integrität eingeordnet werden, sondern eher bei den strafbaren Handlungen gegen die Ehre und den Geheim- oder Privatbereich. Zudem sollten auch weitere Verhaltensweisen mitumfasst werden, wie beispielsweise die Veröffentlichung von Fotos ohne sexuellen Inhalt, die

---

15 Bericht BAKOM Intermediäre und Kommunikationsplattformen.

16 www.parlament.ch > Geschäft 21.4531

17 www.parlament.ch > Geschäft 19.433

18 www.parlament.ch > Geschäft 18.434

19 www.parlament.ch > Geschäft 18.043. Die beiden anderen Vorlagen wurden am 17.12.2021 vom Parlament verabschiedet: BBl **2021** 2996 und 2997.

20 Als Grooming i.e.S. gilt, wenn jemand konkrete Handlungen für ein Treffen mit einem Kind vornimmt. Vgl. BBl **2022** 687, 71.

21 BBl **2022** 687, 72 f.

22 www.parlament.ch > Geschäft 18.043 > Medienmitteilung > Medienmitteilung RK-S vom 18.02.22; BBl **2022** 687, 57 ff.

23 Vernehmlassungsbericht Sexualstrafrecht, Ziff. 6.3

24 www.parlament.ch > Geschäft 18.043 > Medienmitteilung > Medienmitteilung RK-S vom 18.02.22.

aber kompromittierend sind.[25] Der Bundesrat unterstützte den Antrag der Minderheit mit denselben Argumenten. Er hält zudem die Formulierung des vorgeschlagenen Tatbestandes für problematisch. Insbesondere aber wies er darauf hin, dass es sich beim in Frage stehenden Phänomen um eine Erscheinungsform des Cybermobbings handle; der diesbezügliche Handlungsbedarf werde im Rahmen des vorliegenden Postulatsberichts abgeklärt.[26] Der Ständerat als Erstrat ist der Kommissionsmehrheit am 13. Juni 2022 dennoch mit 37 zu 6 Stimmen gefolgt und hat den Tatbestand zur Rachepornografie angenommen.[27]

1.2.4 Vorstösse zum Thema «Rechtsdurchsetzung»

Die *Motion 16.4082 Levrat «Den Strafverfolgungsbehörden den Zugang zu Daten von sozialen Netzwerken erleichtern»* vom 15. Dezember 2016 verlangte, dass soziale Netzwerke, die sich mit ihren Dienstleistungen an Schweizer Konsumentinnen und Konsumenten richten, über eine Vertretung in der Schweiz verfügen müssen. In seiner Stellungnahme vom 15. Februar 2017 wies der Bundesrat auf die Schwierigkeit der Durchsetzung einer solchen Verpflichtung hin und verwies zudem auf die Bestrebungen auf internationaler Ebene, die Kooperation zu verbessern. Die Motion wurde am 22. März 2018 zurückgezogen. Die *Motion 18.3379 RK-S «Zugriff der Strafverfolgungsbehörden auf Daten im Ausland»* vom 23. März 2018 wurde vom Bundesrat zur Annahme empfohlen und vom Parlament überwiesen.[28] Entgegen dem Titel geht es in der Motion um eine allgemeine Pflicht von Internetunternehmen, eine Zustellmöglichkeit zu schaffen. Auf entsprechenden Antrag des Bundesrates wurde auch die *Motion 18.3306 Glättli «Rechtsdurchsetzung im Internet stärken durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen»* vom 15. März 2018 überwiesen.[29] Sie beauftragt den Bundesrat, die Rechtsdurchsetzung im Internet durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen zu stärken. Die zuständige Bundesrätin hatte in den parlamentarischen Beratungen darauf hingewiesen, dass der Bundesrat die Motion in dem Sinne entgegennehme, dass zusammen mit der Motion 18.3379 nach umsetzbaren und wirkungsvollen Lösungen gesucht werde.[30]

1.3 Auftrag

Aus dem Postulat 21.3969 der RK-N «Ergänzungen betreffend Cybermobbing im Strafgesetzbuch» und dessen Auslegung im Lichte der parlamentarischen Initiative 20.445 Suter «Neuer Straftatbestand Cybermobbing» sowie dem Anliegen der RK-S bei Beratung der Revision des Sexualstrafrechts ergibt sich somit folgender Auftrag:

Der Bericht soll eine breite Auslegeordnung zu den Themen Cybermobbing und digitaler Gewalt enthalten und einen allfälligen Handlungsbedarf, d.h. mögliche Ergänzungen des rechtlichen Rahmens, klar aufzeigen.[31] Als besondere Erscheinungsform des Cybermobbings wird dabei insbesondere auch die Rachepornografie thematisiert.[32] Der Umgang mit Cybermobbing in der Praxis wird als schwierig angesehen, da die klassischen Tatbestände auf Einzelhandlungen ausgelegt sind, während bei Cybermobbing aber eine Vielzahl von Verhaltensweisen und Handlungen in ihrer Gesamtheit auf das Opfer einwirkten. Im Strafrecht seien die einzelnen

---

[25] BBl **2022** 687, 58.

[26] BBl **2022** 1011, 4 f.

[27] AB **2022** S 499 ff.

[28] www.parlament.ch > Geschäft 18.3379

[29] www.parlament.ch > Geschäft 18.3306

[30] AB **2018** N 1400.

[31] www.parlament.ch > Geschäft 21.3969 > Medienmitteilung > Medienmitteilung RK-S vom 21.01.22 > Bekämpfung von Cybermobbing: Bericht des Bundesrates abwarten.

[32] BBl **2022** 1011, S. 4 f.

strafbaren Handlungen zudem so genau und präzise wie möglich zu umschreiben. Straftatbestände müssten allgemeinverständlich sein und aktuellen sozialen Phänomenen entsprechen, um präventive Wirkung entfalten zu können.[33]

1.4 Aufbau des Berichts

Nach einer Annäherung an die *Begriffe Cybermobbing und «digitale Gewalt»* und dem Versuch einer Definition für das Strafrecht (Ziff. 2) wird die Strafbarkeit dieser sozialen Phänomene nach geltendem, *materiellem Recht* dargestellt. Dabei werden die Regelungen in ausgewählten Ländern vorgestellt, die Mängel des geltenden Rechts, aber auch dessen Vorzüge analysiert und schliesslich die Handlungsmöglichkeiten des Gesetzgebers aufgezeigt (Ziff. 3). Sodann widmet sich der Bericht der *Rechtsdurchsetzung* bei Cyberdelikten. Nach eingehender Darstellung der Problematik wird der Gesetzgebungsauftrag aufgrund hängiger Vorstösse dargelegt (Ziff. 4). Die *Ergebnisse,* welche aus den Untersuchungen zu ziehen sind, werden am Ende des Berichts zusammengefasst (Ziff. 5).

2 Begriffsbestimmungen

2.1 Cybermobbing

2.1.1 Umschreibung des Phänomens

Der Bundesrat hat am 26. Mai 2010 den *Bericht «Schutz vor Cyberbullying» in Erfüllung des Postulats Schmid-Federer 08.3050* verabschiedet. Das (synonyme) Cyberbullying liegt gemäss diesem Bericht vor, *wenn mit Hilfe moderner Kommunikationsmittel (…) diffamierende Texte, Bilder oder Filme veröffentlicht werden, um Personen zu verleumden, blosszustellen oder zu belästigen. Dabei erfolgen die Angriffe in der Regel wiederholt oder über längere Zeit und die Opfer zeichnen sich durch besondere Hilflosigkeit aus*».[34] Ähnlich wird der Begriff im *Bericht des Bundesrates vom 9. Oktober 2013 «Rechtliche Basis für Social Media»*[35] umschrieben. Die *parlamentarische Initiative 20.445* versteht unter Cybermobbing die *systematische Beleidigung, Bedrohung, Blossstellung oder Belästigung von Personen über digitale Kommunikationskanäle*.[36] Der *Bericht des BAKOM Intermediäre und Kommunikationsplattformen* nimmt ferner den Aspekt auf, dass das Opfer beim Cybermobbing nicht in der Lage ist, sich zu verteidigen.[37]

In der öffentlichen Wahrnehmung und auch in der juristischen Diskussion des Phänomens wird insbesondere Cybermobbing unter *Jugendlichen* thematisiert.[38] Cybermobbing kommt aber auch unter Erwachsenen vor, gerade auch gegenüber *in der Öffentlichkeit stehenden Personen*.

Beim Cybermobbing handelt es sich um ein *soziales Phänomen*, unter das eine *Vielzahl von Verhaltensweisen* fallen kann. Es definiert sich hauptsächlich über die Auswirkung, die es bei der betroffenen Person und in deren Wahrnehmung verursacht. Das Begriffselement Mobbing

---

[33] www.parlament.ch > Geschäft 20.445 > Begründung.

[34] www.parlament.ch > Geschäft 08.3050; Postulatsbericht Cyberbullying. Der Bericht widmet sich der Häufigkeit und Verbreitung des Phänomens sowie möglichen Massnahmen, insbesondere zur Prävention. Abgelehnt hatte der Bundesrat auch die in der Motion Freysinger 10.4054 «Mobbing-Strafnorm» geforderte Einführung eines neuen Mobbing-Straftatbestandes für das Arbeitsumfeld, da das geltende Recht die fraglichen Handlungen bereits weitgehend reguliere und die Einführung einer weiteren Strafnorm keinen zusätzlichen Nutzen in Anbetracht dessen bringeT, dass diese den zentralen Problemen der Beweisbarkeit sowie der Hemmung Betroffener gegen das betreffende Verhalten rechtlich vorzugehen, auch nicht begegne. Auch der Nationalrat lehnte die Einführung des Mobbing-Straftatbestandes mit 130 zu 33 Stimmen bei 11 Enthaltungen ab: www.parlament.ch > Geschäft 10.4054.

[35] Postulatsbericht Social Media 2013; siehe auch Nachfolgebericht Social Media 2017.

[36] www.parlament.ch > Geschäft 20.445 > Begründung.

[37] Bericht BAKOM Intermediäre und Kommunikationsplattformen, Ziff. 5.1, mit Verweis auf CAMPBELL/BAUMAN, 3.

[38] Zum Ausmass des Phänomens unter Jugendlichen bestehen keine belastbaren Daten. Der starke Anstieg gemäss JAMES-Studie, auf den in der Begründung zur parlamentarischen Initiative 20.445 Suter «Neuer Straftatbestand Cybermobbing» vom 11.06.2020 (www.parlament.ch > Geschäft 20.445 > Begründung) hingewiesen wird, bezieht sich auf sexuelle Belästigungen, die freilich im Rahmen von Cybermobbing vorkommen können, aber auch unabhängig davon. Vgl. aktuelle JAMES-Studie 2020 der Zürcher Hochschule für Angewandte Wissenschaften Postulatsbegründung zitiert wird, www.zhaw.ch > Forschung > Mediennutzung > JAMES > Ergebnisbericht JAMES-Studie 2020, 54.

leitet sich ab vom englischen *to mob*, was so viel bedeutet, wie über jemanden herfallen, jemanden angreifen oder schikanieren. Entsprechend dem Nomen *mob* (englisch für die Rotte, Bande) wird z.T. auch vorausgesetzt, dass sich mehrere Täter bzw. Täterinnen gegen dieselbe Person zusammenrotten müssen.[39] Mobbing beginnt dort, wo sich jemand *beleidigt, schikaniert, gequält oder herabgesetzt fühlt*.[40] Gerade jugendlichen Tätern und Täterinnen ist diese Auswirkung zumindest zu Beginn oftmals nicht bewusst. Es kann gar scherzhaft beginnen; der Übergang zu beleidigendem Verhalten ist oft fliessend.[41] Ferner muss es sich um *wiederholte Angriffe* handeln: Je nach Definition wird vorausgesetzt, dass die Angriffe über einen längeren Zeitraum[42] bzw. immer wieder,[43] systematisch und häufig[44] erfolgen. Mobbing kann dabei auch *dynamisch* sein, d.h. die Verhaltensweisen können sich im Verlauf der Zeit in ihrem Schweregrad steigern.

Das Begriffselement *Cyber-* soll verdeutlichen, dass das Mobbing *unter Nutzung der Informations- und Kommunikationstechnik (IKT)*[45] erfolgen muss. Als solche stehen heute *E-Mails, Messenger-Dienste, soziale Netzwerke, Chats, Foren, Blogs oder Videoportale* im Vordergrund. In unserer Zeit erfolgt ein beträchtlicher Teil der sozialen Interaktion über das Internet. Mit der grossen Verbreitung von Smartphones sind Viele ganztags vernetzt. Die Austragung von Konflikten findet mehr und mehr online statt.[46] Im Internet ist es dabei einfacher, anonym und unerkannt zu bleiben,[47] was die Hemmschwelle für Täter und Täterinnen senkt. Zudem sind die beispielsweise in Messenger-Gruppen, auf sozialen Medien, Foren oder Blogs erscheinenden Texte oder Aufnahmen einem grossen, z.T. gar unkontrollierbaren Personenkreis zugänglich. Da solche Nachrichten bei den Lesenden emotionales Engagement auslösen können, werden sie schnell weiterverbreitet.[48] Herabsetzung wirkt damit intensiver, da sie von Vielen wahrnehmbar ist. Sie wirkt schliesslich auch länger, da im Internet veröffentlichte und womöglich durch Dritte weiterverbreitete Daten nur schwer oder gar nicht kontrolliert werden können.[49]

Cybermobbing definiert sich somit gleich wie Mobbing im Allgemeinen – mit der zusätzlichen Voraussetzung, dass es unter Nutzung von IKT begangen werden muss.[50] Insbesondere sind auch *Mischformen* zwischen Offline- und Cybermobbing denkbar, das heisst, dass gewisse Verhaltensweisen in der realen, andere in der virtuellen Welt erfolgen, und diese in ihrer Gesamtheit herabsetzend wirken.

Es ist zu beachten, dass sich die *Verwendung des Begriffs im Laufe der Zeit gewandelt* hat. Während dieser früher zurückhaltender und nur für schwerwiegende Angriffe Verwendung fand, werden heute vermehrt auch leichtere Konfliktsituationen als Mobbing bezeichnet,

---

[39] Vgl. die Definition unter www.skppsc.ch > Fokus Internet > Cybermobbing; vgl. auch Bericht BAKOM Intermediäre und Kommunikationsplattformen, Ziff. 5.1, mit Verweis auf CAMPBELL/BAUMAN, 3: «Gruppe oder Einzelpersonen».

[40] Vgl. www.skppsc.ch > Fokus Internet > Cybermobbing > Opfer, Täterschaft und Ursachen > Das Verhältnis von Opfer und Täterinnen/Täter; www.jugendundmedien.ch > Themen > Cybermobbing > Gut zu wissen > Wie verbreitet ist Cybermobbing?

[41] www.jugendundmedien.ch > Themen > Cybermobbing > Gut zu wissen > Wie verbreitet ist Cybermobbing?

[42] BRUN, 101; www.skppsc.ch > Fokus Internet > Cybermobbing > Definition

[43] www.jugendundmedien.ch > Themen > Cybermobbing > Gut zu wissen > Wie verbreitet ist Cybermobbing?

[44] KUNZ, 8.

[45] Der Begriff IKT steht im weiteren Sinne für jegliche Kommunikationsanwendung, darunter Radio, Fernsehen, Handys, Smartphones, Hardware und Software für Computer und Netzwerke, Satellitensysteme, sowie für die verschiedenen Dienstleistungen und Anwendungen, die damit verbunden sind: www.wikipedia.org > IKT

[46] www.skppsc.ch > Fokus Internet > Cybermobbing > Opfer, Täterschaft und Ursachen > Verlagerung ins Internet, in Bezug auf Jugendliche: Das für diese Altersgruppe typische bewusste oder unbewusste Eingehen von Risiken und das Ausloten von Grenzen finden mehr und mehr online statt.

[47] Täter bzw. Täterinnen sind den Betroffenen aber oft bekannt: www.jugendundmedien.ch > Themen > Cybermobbing > Gut zu wissen > Was ist Cybermobbing?

[48] Vgl. etwa DEB ROY/SINAN ARAL, The spread of true and false news online, www.sience.org vom 09.03.2018.

[49] www.skppsc.ch > Fokus Internet > Cybermobbing > Opfer, Täterschaft und Ursachen > Verlagerung ins Internet

[50] Es geht also vorliegend nicht um Cyber-Delikte im engeren Sinn (Delikte, die nur mithilfe IKT begangen werden können), sondern um Delikte, welche als gewähltes Tatmittel IKT benutzen.

etwa alltägliche Auseinandersetzungen in der Arbeitswelt oder einmalige Herabsetzungen. Dies birgt die Gefahr, dass schweres Mobbing weniger ernst genommen wird, da es begrifflich mit solchen Situationen verschmilzt.[51] Gerade für den Bereich des Strafrechts, das an ein klar definiertes Verhalten die einschneidendste aller möglichen Rechtsfolgen knüpft, ist es wichtig, begrifflich an klaren Elementen festzuhalten.

2.1.2 Fallgruppen

In Anlehnung an BRUN[52] und die Schweizerische Kriminalprävention (SKP)[53] geht der vorliegende Bericht von folgenden drei Fallgruppen aus: *(1) Einschüchterung:* Der Täter oder die Täterin bedrängt die betroffene Person, ängstigt sie oder beeinträchtigt ihr Sicherheitsgefühl. *(2) Belästigung:* Der Täter oder die Täterin stört die Privatsphäre der betroffenen Person, indem er oder sie diese beispielsweise mit anstössigen Nachrichten oder Aufnahmen sexuellen Inhalts belästigt. *(3) Blossstellung:* Der Täter oder die Täterin verunglimpft die betroffene Person öffentlich, so etwa, indem er oder sie ehrverletzende Bekanntmachungen, falsche Informationen oder Gerüchte bzw. peinliche, verfälschte, freizügige oder pornografische Bild- oder Videoaufnahmen verbreitet, (beleidigende) Fake-Profile erstellt oder «Hassgruppen» gründet, in denen negative Äusserungen über sie gemacht werden.

Da es sich beim Mobbing um wiederholte Angriffe handelt, stehen die verschiedenen Fallgruppen nicht isoliert nebeneinander. Sie können sich vielmehr *mischen und ergänzen*. Dies zeigt beispielsweise der vielzitierte Begriff *«harassment»*, d.h. das wiederholte Versenden von bedrohenden, belästigenden oder beleidigenden Nachrichten.[54] Auch können die Verhaltensweisen, wie schon erwähnt, zum Teil unter Nutzung von IKT erfolgen, z.T. durch reale Angriffe (Ziff. 2.1.1.). Die Einteilung in die drei Fallgruppen dient lediglich einer Erleichterung der strafrechtlichen Annäherung und Erfassung des Phänomens.

2.1.3 Strafrechtliche Definition

Für eine strafrechtliche Definition von Cybermobbing ist von folgenden **Voraussetzungen** auszugehen:

- **Einschüchterndes, belästigendes oder blossstellendes Verhalten**
  Zu den Fallgruppen siehe Ziff. 2.1.2
- **Wiederholtes Verhalten**
  Die Einzelakte erfolgen über einen längeren Zeitraum und während diesem Zeitraum häufig.
- **Nutzung von IKT**
  Insbesondere E-Mails, Messenger-Dienste, soziale Netzwerke, Chats, Foren, Blogs oder Videoportale
- **Betroffene Person fühlt sich beleidigt, schikaniert, gequält oder herabgesetzt**
  Dabei ist vorauszusetzen, dass diese Auswirkung objektivierbar ist, d.h. eine besonnene Person in derselben Situation gleich reagieren würde.
- **Vorsätzliches Verhalten**
  Der Täter oder die Täterin muss mit Wissen und Willen handeln. Das heisst, er oder sie muss sich insbesondere auch der herabsetzenden Wirkung des Handelns bewusst sein und diese wollen bzw. zumindest in Kauf nehmen.

---

[51] KUNZ, 8.

[52] BRUN, 102. Diese Einteilung übernimmt auch WENK, 89.

[53] www.skppsc.ch > Fokus Internet > Cybermobbing > Definition.

[54] BRUN, 102.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Die Abgrenzung des Cybermobbings zum *Cyberstalking* ist schwierig und unklar. Stalking definiert sich als vorsätzliches Verhalten, das aus wiederholten Bedrohungen einer anderen Person besteht, die dazu führen, dass diese um ihre Sicherheit fürchtet.[55] Es geht mit anderen Worten um vorsätzliches, wiederholtes bedrohendes Verhalten, durch das bei der betroffenen Person Angst ausgelöst wird. Wie insbesondere aus der Darstellung möglicher Fallgruppen hervorgeht (Ziff. 2.1.2), können diese Voraussetzungen auch beim (Cyber-)Mobbing erfüllt sein. Auch (Cyber-)Stalking kann mittels Drohungen oder Belästigungen erfolgen, die die betroffene Person einschüchtern, indem sie sich ängstigt bzw. in ihrem Sicherheitsgefühl beeinträchtigt wird. Beim Mobbing geht es dem Täter oder der Täterin aber in der Regel um eine *Herabsetzung bzw. Erniedrigung* des Opfers.

2.2 Weitere Formen «digitaler Gewalt»

2.2.1 Entstehung des Begriffs

Die Begriffe «digitale Gewalt» und «Cybergewalt» sind *erst in den vergangenen Jahren* entstanden. Das Übereinkommen des Europarates über die Cyberkriminalität[56] (CCC) beispielsweise, abgeschlossen in Budapest am 23. November 2001 und für die Schweiz in Kraft getreten am 1. Januar 2012, spricht im Zusammenhang mit über IKT begangenen Delikten nicht von Gewalt.

Der Begriff der «digitalen Gewalt» hat erstmals mit einer *Empfehlung der Expertengruppe des Europarates für die Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (GREVIO)* vom 20. Oktober 2021 Einzug in die internationale Rechtssprache gefunden, die sich der digitalen Dimension von Gewalt gegen Frauen und häuslicher Gewalt widmet.[57] Es geht hier darum, dass Gewalt gegenüber Frauen und Gewalt im häuslichen Umfeld, insbesondere psychische Gewalt, sich auch über digitale Kommunikationskanäle manifestieren kann. Diesem Grundsatz legt GREVIO ein weites Begriffsverständnis zugrunde und erklärt zahlreiche über Internet begangene Taten als Formen von Gewalt gegen Frauen bzw. häuslicher Gewalt.[58] Dennoch bezeichnet GREVIO Cyberkriminalität auch in dieser Empfehlung nicht direkt als Gewalt. Für den vorliegenden Bericht, der nicht Formen der Gewalt an Frauen bzw. im häuslichen Umfeld im Fokus hat, ist das sehr breite Begriffsverständnis gemäss der GREVIO-Empfehlung nicht zielführend. Als Empfehlung, die zudem – wie in deren Vorwort ausdrücklich festgehalten – der offiziellen Auffassung des Europarats nicht zwingend entspricht,[59] kommt ihr keine Bindungswirkung für das schweizerische Recht zu.

Der Begriff der «digitalen Gewalt» hat auch Einzug in den öffentlichen Diskurs in der Schweiz gefunden. So versteht die bereits erwähnte Interpellation Gysin 21.3684 unter «Cybergewalt» Phänomene *der Gewalt, des Hasses und des Mobbings im Netz*. Vermehrt findet sich die Umschreibung, dass unter «digitaler Gewalt» Formen der Herabsetzung, der sozialen Isolation, der Rufschädigung, der Nötigung, der Erpressung bis hin zu Drohungen über IKT zu verstehen seien.[60]

---

[55] Bericht BJ Stalking, Ziff. 3, mit Verweis auf BBI **2017** 185, 239.

[56] SR **0.311.43**

[57] Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes vom 20.10.21, www.coe.int > Menschenrechte > Gewalt gegen Frauen und häusliche Gewalt GREVIO > Apropos du suivi > GREVIO > Recommandation générale > Recommandation générale No. 1.

[58] Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes vom 20.10.21, www.coe.int > Menschenrechte > Gewalt gegen Frauen und häusliche Gewalt GREVIO > Apropos du suivi > GREVIO > Recommandation générale > Recommandation générale No. 1, § 19 f.

[59] Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes vom 20.10.21, www.coe.int > Menschenrechte > Gewalt gegen Frauen und häusliche Gewalt GREVIO > Apropos du suivi > GREVIO > Recommandation générale > Recommandation générale No. 1, § 2.

[60] Vgl. FRASCH. Vgl. etwa Begriffsverständnis gemäss Postulat 22.3201 Bellaiche «Digitale Gewalt eindämmen» vom 17. März 2022, www.parlament.ch > Geschäft 22.3201: Cybermobbing, Cyberstalking, Hassrede, Gewaltandrohung oder Diskriminierung.

2.2.2 Der Gewaltbegriff im Strafrecht

Es ist unabdingbar, darauf hinzuweisen, dass ein neuer Begriff «digitale Gewalt» im Strafrecht nicht nur unpassend wäre, sondern gar Gefahren birgt. Dessen pauschalisierende Verwendung kann dazu führen, dass sich der strafrechtliche Gewaltbegriff auflöst.

Der strafrechtliche Gewaltbegriff deckt verschiedene Aspekte ab. Heute wird zwischen *physischer, sexueller und psychischer Gewalt* unterschieden. Während die strafbaren Handlungen gegen Leib und Leben (Art. 111 ff. StGB) sowie verschiedene strafbare Handlungen gegen die sexuelle Integrität (Art. 187 ff. StGB) offensichtlich Gewaltdelikte sind, enthalten auch andere Tatbestände Gewaltelemente (so insbesondere bei sogenannten zusammengesetzten Delikten wie Raub oder Erpressung, Art. 140 und 156 StGB, aber auch bei Menschenhandel oder Freiheitsberaubung und Entführung, Art. 182 f. StGB).

Artikel 33 des Übereinkommens des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt (Istanbul-Konvention) vom 11. Mai 2011[61], für die Schweiz in Kraft getreten am 1. April 2018, definiert psychische Gewalt als vorsätzliches Verhalten, durch das die psychische Unversehrtheit einer Person durch Nötigung oder Drohung ernsthaft beeinträchtigt wird. Insofern sind die Tatbestände der Drohung (Art. 180 StGB) und Nötigung (Art. 181 StGB) als Gewaltdelikte zu bezeichnen, auch wenn sie über IKT begangen werden. Bei anderen Delikten, die im öffentlichen Diskurs unter den Begriff der «digitalen Gewalt» subsumiert werden, ist dies nicht möglich. Die betroffene Person kann hier in anderer Hinsicht in ihrer Persönlichkeit angegriffen werden, etwa durch ehrenrührige Behauptungen oder Verbreitung intimer Bilder gegen ihren Willen, was zweifellos grosses Leid hervorrufen kann, ohne dass dies jedoch immer (psychische) Gewalt beinhaltet.

2.2.3 Die einzelnen Formen

Im Sinne des oben dargelegten Verständnisses behandelt der Bericht neben Cybermobbing die sozialen Phänomene der Hassrede, der Rachepornografie und der Sextortion.[62] Es handelt sich hierbei um digitale Angriffe gegen die Persönlichkeit, die auch psychische Gewalt enthalten können (so bei Sextortion). Ihre Definitionen überschneiden sich zum Teil.

Diese Phänomene werden zu einem grossen Teil bereits strafrechtlich erfasst (Ziff. 3.2.1.1 ff.). Sie können jeweils zugleich auch Einzelhandlungen des Cybermobbings darstellen.

- **Hassrede:** In Anlehnung an eine neue *Empfehlung des Ministerkomitees des Europarates*[63] kann Hassrede (auch «Hate-Speech») als jede Form von Äusserungen definiert werden, welche Hass, Diskriminierung oder Vorurteile gegenüber einer Person oder einer Personengruppe verbreiten, fördern, rechtfertigen oder hierzu anstacheln, unter Bezug auf eine wirkliche oder vermeintliche persönliche Eigenschaft der Person oder Personengruppe, beispielsweise Rasse, Ethnie, Hautfarbe, Religion, aber auch sexuelle Orientierung, Geschlecht, Alter, berufliche oder anderweitige Tätigkeiten oder körperliches oder geistiges Handicap.

---

61 SR **0.311.35**

62 Der Bericht klammert damit insbesondere die Phänomene des Cyberstalkings und des Cybergroomings aus. Cyberstalking meint Stalking unter Nutzung von IKT. Es wird im Rahmen der parlamentarische Initiative 19.433 der RK-N «StGB-Tatbestände mit Stalking ergänzen» behandelt. Als Cybergrooming i.e.S. gilt es, wenn jemand konkrete Handlungen für ein Treffen mit einem Kind vornimmt. Die Frage dessen Strafbarkeit ist Gegenstand der Revision des Sexualrechts. Der Ständerat als Erstrat hat abgelehnt, einen spezifischen Tatbestand zum Cybergrooming einzuführen. Vgl. BBl **2022** 687, 71.

63 Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022: «Le discours de haine est entendu comme tout type d'expression qui incite à, promeut, diffuse ou justifie la violence, la haine ou la discrimination à l'encontre d'une personne ou d'un groupe de personnes, ou qui les dénigre, en raison de leurs caractéristiques personnelles ou de leur statut réels ou attribués telles que la 'race', la couleur, la langue, la religion, la nationalité, l'origine nationale ou ethnique, l'âge, le handicap, le sexe, l'identité de genre et l'orientation sexuelle», www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres . Die Definition des Europarats bezieht auch Äusserungen mit ein, welche Gewalt verbreiten, fördern, rechtfertigen oder hierzu anstacheln.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

- **Rachepornografie:** Der Begriff der Rachepornografie (auch «Revenge Porn») wurde zunächst eng verstanden und bezog sich auf pornografisches Bild- oder Videomaterial,[64] das von oder im Einverständnis mit der darauf sichtbaren Person hergestellt wird – beispielsweise in einer Paarbeziehung –, später aber aus Rache gegen deren Willen weiterverbreitet wird. Im Zuge des Bedeutungszuwachses von IKT wird in der öffentlichen Wahrnehmung der Begriff weiter verstanden. Im Kern geht es nach heutigem Verständnis darum, dass intime Aufnahmen, die ohne Einverständnis der darauf sichtbaren Person hergestellt worden sind, oder die zwar mit deren Einverständnis hergestellt worden sind, aber nur für ganz bestimmte Personen bestimmt waren, weiterverbreitet werden, um sie blosszustellen, zu beleidigen oder zu diffamieren.
- **Sextortion:** Bei Sextortion wird einer Person angedroht, pornografische bzw. intime Bild- oder Videoaufnahmen weiterzuverbreiten, um dadurch entweder Geld zu erpressen oder diese zu nötigen, weitere pornografische bzw. intime Aufnahmen herauszugeben.

3 Materielles Recht

3.1 Zivilrecht

Eine Person, die Cybermobbing oder andere Formen digitaler Angriffe erfährt, ist in der Regel *in ihrer Persönlichkeit widerrechtlich verletzt*. Sie kann deshalb zu ihrem Schutz gegen jeden, der an der Verletzung mitwirkt, das Zivilgericht anrufen (Art. 28 Abs. 1 ZGB).

Auf diesem Weg kann die betroffene Person verlangen, dass eine *bestehende Persönlichkeitsverletzung beseitigt oder eine drohende Persönlichkeitsverletzung verboten* wird (Art. 28*a* Abs. 1 Ziff. 1 und 2 ZGB). Sie kann auch auf *Schadenersatz* und *Genugtuung* klagen (Art. 28*a* Abs. 3 ZGB). Zum Schutz gegen Gewalt, Drohungen oder Nachstellungen kann das Gericht dem Urheber der Persönlichkeitsverletzung dabei insbesondere *verbieten, mit der betroffenen Person Kontakt aufzunehmen, namentlich auf telefonischem, schriftlichem oder elektronischem Weg* (Art. 28*b* Abs. 1 Ziff. 3 ZGB). Dabei ist unerheblich, *wie* die Tatperson auf elektronischem Weg Kontakt aufnimmt.[65] Seit 1. Januar 2022 besteht die Möglichkeit, dass die Tatperson auf Antrag der betroffenen Person elektronisch überwacht wird (Art. 28*c* Abs. 1 ZGB), was aber primär bei räumlichen Verboten (Annäherungs- und Rayonverboten) und weniger bei einer Kontaktaufnahme auf elektronischem Weg Schutz vor weiteren Persönlichkeitsverletzungen verspricht.[66]

Das Gericht kann statt eines solchen Kontaktaufnahmeverbots aber auf Antrag auch *andere Massnahmen* anordnen, die geeignet sind, die betroffene Person vor Cybermobbing oder anderen digitalen Angriffen gegen ihre Persönlichkeit zu schützen – so etwa ein Verbot, Nachrichten auf Social Media Plattformen zu posten.

Gemäss den allgemeinen Regeln des Zivilprozessrechts muss die klagende Person, d.h. hier die vom Cybermobbing betroffene Person, vor Gericht den *Beweis dafür erbringen*, dass sie von einer bestimmten Person in ihrer Persönlichkeit widerrechtlich verletzt wird; sie hat nach Artikel 55 Absatz 1 der Zivilprozessordnung[67] (ZPO) die sogenannte Behauptungs- und Substantiierungslast. Gleichzeitig erlaubt der zivilrechtliche Weg ein *sehr rasches Einschreiten:* Die Massnahmen können auch *vorsorglich oder gar superprovisorisch,* d.h. auch ohne Anhörung der Gegenpartei, angeordnet werden. Über Artikel 268 ZPO ist eine jederzeitige *Modifikation und Anpassung* der angeordneten Massnahmen möglich. Das Gericht kann die Verfügung

---

[64] Vgl. Begriffsauslegung in der Interpellation 16.3162 Feri «Rachepornografie» vom 17. März 2016, www.parlament.ch > Geschäft 16.3162.

[65] Zum Ganzen: Botschaft zum Bundesgesetz über die Verbesserung des Schutzes gewaltbetroffener Personen vom 11.10.2017, BBl **2017** 7307, 7320; Interpellation 22.3157 Gysin Greta «Bietet das Rayon- und Kontaktverbot auch den Opfern von Cybergewalt genügend Schutz?», www.parlament.ch > Geschäft 22.3157.

[66] Zum Ganzen BBl **2017** 7307, 7344.

[67] SR **272**

zudem mit einer *Strafandrohung wegen Ungehorsams gegen amtliche Verfügungen* (Art. 292 StGB) verbinden, so dass die verletzende Person zusätzlich mit Busse bestraft werden kann.

3.2 Strafrecht

Das StGB enthält *keine spezifischen Straftatbestände* zum Cybermobbing und den anderen hier in Frage stehenden digitalen Angriffen gegen die Persönlichkeit. Dennoch bestehen die materiellen Möglichkeiten, die im konkreten Fall erfüllten herabsetzenden, drohenden, nötigenden oder anderweitig strafrechtlich relevanten Verhaltensweisen zu verfolgen und zu bestrafen.

Es gehört zu den Eigenheiten des schweizerischen Strafrechts, dass dieses *soweit möglich technologieneutral* ausgestaltet ist (Ziff. 3.5.5). Das bedeutet, dass die einzelnen Tatbestände *generell-abstrakt*, also unabhängig von der konkreten Art der Tatbegehung formuliert sind. So fallen Handlungen aus der realen und der virtuellen Welt unter ein und denselben Tatbestand. Entscheidend ist die Verletzung, die ein Verhalten bewirkt. Nur in Einzelfällen ist dies nicht möglich. So musste beispielsweise ein spezieller Tatbestand zur Datenbeschädigung (Art. 144bis StGB) geschaffen werden, da sich die Tatbestandselemente der Sachbeschädigung (Art. 144 StGB) nicht auf unkörperliche Daten übertragen lassen. Ein weiteres Beispiel für einen Tatbestand, der sachlich zwingend an eine Technologie anknüpfen muss, ist der im vorliegenden Zusammenhang relevante Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB).

3.2.1 Cybermobbing

Gemäss dem bereits erwähnten Bericht des Bundesrats zum *Postulat Schmid-Federer 08.3050 «Schutz vor Cyberbullying»* vom 26. Mai 2010 können die dem Cybermobbing zu Grunde liegenden belästigenden, drohenden oder verunglimpfenden Handlungen mit dem vorhandenen strafrechtlichen Instrumentarium wirksam verfolgt und angemessen bestraft werden.[68]

Auch nach dem *Bericht des Bundesrats zu Social Media von 2013 und dem Nachfolgebericht von 2017* bestehen keine Anhaltspunkte, wonach die geltenden Strafnormen nicht ausreichen würden. Die Social-Media-Berichte weisen jedoch darauf hin, dass die hauptsächlichen Schwierigkeiten im Bereich der Rechtsdurchsetzung liegen.[69]

Zuletzt hat die Kommission für Wissenschaft, Bildung und Kultur des Ständerates (WBK-SR) in ihrem *Bericht* vom 22. Juni 2015 *zur Motion 12.4161 Schmid-Federer «Nationale Strategie gegen Cyberbullying und Cybermobbing»* die Notwendigkeit zur Einführung von strafrechtlichen Normen verneint; die geltenden strafrechtlichen Bestimmungen genügten zur Verfolgung von Cybermobbing.[70]

Die geltenden Tatbestände, die beim Cybermobbing Anwendung finden können, werden im Folgenden je nach Fallgruppe (Ziff. 2.1.2) gesondert dargestellt.

---

[68] www.parlament.ch > Geschäft 08.3050; Postulatsbericht Cyberbullying, 21. Abgelehnt hatte der Bundesrat auch die in der Motion Freysinger 10.4054 «Mobbing-Strafnorm» geforderte Einführung eines neuen Mobbing-Straftatbestandes für das Arbeitsumfeld, da das geltende Recht die fraglichen Handlungen bereits weitgehend reguliere und die Einführung einer weiteren Strafnorm keinen zusätzlichen Nutzen in Anbetracht dessen bringe, dass diese den zentralen Problemen der Beweisbarkeit sowie der Hemmung Betroffener gegen das betreffende Verhalten rechtlich vorzugehen, auch nicht begegne. Auch der Nationalrat lehnte die Einführung des Mobbing-Straftatbestandes mit 130 zu 33 Stimmen bei 11 Enthaltungen ab: www.parlament.ch > Geschäft 10.4054.

[69] Postulatsbericht Social Media 2013, Ziff. 4.4.2.3 und Nachfolgebericht Social Media 2017, Ziff. 5.3.2.1. Die Berichte verweisen auch auf die zivilrechtlichen Möglichkeiten: Neben den Ansprüchen aus Art. 28*a* ZGB können Betroffene zum Schutz vor Persönlichkeitsverletzungen in Form von Gewalt, Drohung oder Nachstellungen auch bei einem Gericht geltend machen, Dritten sei der Kontakt mit ihnen – was elektronische Kommunikation explizit umfasst – zu verbieten (Art. 28*b* Abs. 1 Ziff. 3 ZGB)

[70] Bericht vom 22.06.2015 zur Motion 12.4161 Schmid-Federer «Nationale Strategie gegen Cyberbullying und Cybermobbing», www.parlament.ch > Geschäft 12.4161 > Ziff. 4. In seiner Antwort auf die Motion vom 27. Februar 2013 hatte der Bundesrat ausgeführt, im Anschluss an das Programm Jugend und Medien (…) sei zu evaluieren, ob und inwieweit Handlungsbedarf bestehe. Nach dessen Abschluss hat die WBK-SR im genannten Bericht die Schaffung einer nationalen Strategie gegen Cyberbullying und Cybermobbing verworfen. Das Förder- und Präventionsprogramm habe sich bewährt und Cybermobbing sei als zentrales Problem berücksichtigt worden. Insbesondere der Schutz der Kinder und Jugendlichen vor sozialem und kriminellem Fehlverhalten wurden dabei schwerpunktmässig behandelt. Im Bereich der Prävention konnten in den Kantonen bereits einige Erfolge festgestellt werden. Mittlerweile existiert ein breites Angebot an Beratung.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

3.2.1.1 Einschüchterung

Bei dieser Fallgruppe geht es darum, dass die mobbende Person jemanden unter Nutzung von IKT einschüchtert, indem sie diese bedrängt, ängstigt oder in ihrem Sicherheitsgefühl beeinträchtigt.

Drohung (Art. 180 StGB): Einschlägig ist hier zunächst der Tatbestand der Drohung. Danach wird bestraft, wer jemanden *durch schwere Drohung in Schrecken oder Angst versetzt*. Der Tatbestand schützt ein gewisses Mass an *innerer Freiheit*, auf das jede Person Anspruch hat und das ihr freie Entfaltung und psychisches Gleichgewicht garantieren soll. Es wird aber auch das *Sicherheitsgefühl* vor massiver Erschütterung durch andere geschützt.[71] Der Täter oder die Täterin muss der betroffenen Person einen *schweren Nachteil* ankündigen oder in Aussicht stellen,[72] dessen Eintritt als von seinem oder ihrem Willen abhängig scheint.[73] Beim Cybermobbing kann das beispielsweise eine Gewaltanwendung oder eine Bekanntmachung kompromittierender Art sein. Das Bundesgericht hat seine Rechtsprechung zur Frage, ob ein schwerer Nachteil im Sinne des Tatbestandes gegeben ist, in seiner neueren Rechtsprechung relativiert. Während es früher von einem *objektiven Massstab* ausging, gilt dieser heute nur noch als Grundsatz, der aber Ausnahmen zulässt. *In der Regel* ist somit «auf das Empfinden eines vernünftigen Menschen mit einigermassen normaler psychischer Belastbarkeit abzustellen».[74] Die Relativierung lässt es zu, die Umstände besonders schutzbedürftiger Personengruppen – gerade etwa Jugendlicher, die häufig von Cybermobbing betroffen sind – zu beachten.[75] Das Bundesgericht hat auch festgehalten, dass bei der Frage, ob die Drohung geeignet ist, *Angst hervorzurufen*, auf die gesamten Umstände abzustellen ist.[76] So hat es wiederholte Drohung bei mehreren Vorfällen unterschiedlicher Schwere bejaht, die sich über längere Zeit (i.c. ein Jahr) hinzogen: Dies mit der Begründung, dass die betroffene Person gegenüber dem Täter oder der Täterin ein ungutes Gefühl entwickelt und damit ihr inneres Sicherheitsgefühl verloren habe.[77] Die betroffene Person muss mit dem Eintritt des in Aussicht gestellten Nachteils rechnen bzw. diesen für möglich halten und andererseits durch die Schwere des Nachteils in Schrecken oder Angst versetzt worden sein.[78] Eine Drohung wird auf Antrag verfolgt[79] und mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Nötigung (Art. 181 StGB): Bei der Nötigung handelt es sich um ein Delikt gegen die Willensbildung, -entschliessung und -betätigung. Die betroffene Person wird durch Gewalt oder Androhung ernstlicher Nachteile oder durch eine andere Beschränkung ihrer Handlungsfreiheit dazu genötigt, etwas zu tun, zu unterlassen oder zu dulden. Der angekündigte «ernstliche» Nachteil, dessen Eintritt auch hier als vom Willen des Täters oder der Täterin abhängig dargestellt wird (jedenfalls nach der beim Opfer geweckten Vorstellung),[80] muss dabei nicht von gleicher Schwere sein wie bei der Drohung und insbesondere nicht zwingend Angst und Schrecken verursachen. Erforderlich ist aber eine Intensität, welche die betroffene Person entgegen ihrem eigenen Willen zu dem aufgenötigten Tun, Unterlassen oder Dulden bestimmen kann bzw. bestimmt. Um eine Überdehnung des Strafschutzes zu vermeiden, legt das Bundesgericht hier

---

[71] DELNON/RÜDY, BSK II StGB, Art. 180 N 5.

[72] STRATENWERTH/BOMMER, BT I, § 5 N 98.

[73] DELNON/RÜDY, BSK II StGB, Art. 180 N 14; TRECHSEL/MONA, PK StGB, Art. 181 N 4; BGE 120 IV 17, 19; 106 IV 125, 128 f.; 94 IV 111, 116; 81 IV 101, 105.

[74] Urteil des Bundesgerichts 6B_192/2012 vom 10.09.2012, E. 1.1 m.H. und 6B_307/2013 vom 13. 6. 2013, E. 5.1.

[75] DELNON/RÜDY, BSK II StGB, Art. 180 N 21; vgl. die Forderung bei BRUN, 103.

[76] BGE **99** IV 212, 215.

[77] Es ging hier um Drohungen des Ehemannes gegenüber seiner Frau: Urteil des Bundesgerichts 6B_1121/2013 vom 06.05.2014, E. 6.3 und E. 6 – 8.

[78] DELNON/RÜDY, BSK II StGB, Art. 180 N 24.

[79] Die Tat wird jedoch von Amtes wegen verfolgt, wenn sie in einer Paarbeziehung begangen wurde: Art. 180 Abs. 2 StGB.

[80] DELNON/RÜDY, BSK II StGB, Art. 181 N 26 und 25.

bzw. bei der Beurteilung, ob der angedrohte Nachteil ernstlich im Sinne der genannten Bestimmung ist, grundsätzlich einen *objektiven Massstab* an: Den Tatbestand erfüllen nur Androhungen, die geeignet sind, auch eine verständige bzw. besonnene Person in der Lage des Betroffenen gefügig zu machen.[81] Immerhin ist die «Absolutheit des Massstabs» in zweierlei Hinsicht zu relativieren: Einerseits bietet die spezifische Lage des Opfers Raum für eine gewisse Differenzierung; andererseits muss ein relativ geringfügiger Nachteil dann als «ernstlich» angesehen werden, wenn der Täter oder die Täterin eine besondere Schwäche des Opfers, z.B. eine Phobie, gezielt ausnützt.[82] Ein Teil der Lehre postuliert denn auch, wie bei der Drohung auf besonders schützenswerter Personengruppen einzugehen.[83] Auch bei der Generalklausel der *«anderen Beschränkung der Handlungsfreiheit»* muss die Einwirkung «das üblicherweise geduldete Mass der Beeinflussung in ähnlicher Weise eindeutig überschreiten, wie es für die vom Gesetz ausdrücklich genannte Gewalt oder die Androhung ernstlicher Nachteile gilt».[84] Die Intensität der Gewalt muss aber nicht so gross sein, dass das Opfer widerstandsunfähig wird. Der Massstab ist hier ein relativer: Es genügt die Gewalt, die erforderlich ist, um den Willen des konkreten Opfers zu brechen.[85] Bei der Nötigung handelt es sich um einen offenen Tatbestand, womit die Rechtswidrigkeit besonderer Begründung bedarf. Denn geschützt ist nicht die Freiheit des Individuums schlechthin; eine absolute Freiheit existiert nicht. Staats- und Rechtsordnung sowie das soziale Zusammenleben der Menschen auferlegen jedem Einzelnen von vornherein zahlreiche Sach- und Rechtszwänge. Das Gesetz schützt schon von daher nicht jegliche Freiheit der Willensbildung und -betätigung. Strafbar sein kann also nur eine unzulässige Freiheitsbeschränkung, womit ausschliesslich die «rechtlich geschützte» bzw. «rechtlich garantierte» Freiheit des Einzelnen geschützt wird.[86] Die Tat wird von Amtes wegen verfolgt und mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bedroht.

Im Zusammenhang mit der Nötigung durch *Stalking* hat das Bundesgericht die Rechtsprechung entwickelt, wonach sich bei einer Vielzahl von Belästigungen über längere Zeit die Einwirkungen kumulieren. Ist eine gewisse Intensität erreicht, kann damit jede einzelne Handlung, die für sich alleine den Anforderungen des Tatbestandes nicht genügen würde, geeignet sein, die Handlungsfreiheit des Opfers in ausreichendem Mass einzuschränken.[87] Angesichts dieser Rechtsprechung ist BRUN der Auffassung, dass Cybermobbing eine Nötigung darstellen kann, wenn der auf die betroffene Person ausgeübte Zwang (erst) angesichts der Intensität und Dauer zu einer Beschränkung der Handlungsfreiheit führt.[88]

Erpressung (Art. 156 StGB): Eine qualifizierte Form der Nötigung ist die Erpressung: Hier nötigt der Täter oder die Täterin die betroffene Person zu einer Vermögensdisposition, um sich oder einen anderen unrechtmässig zu bereichern. Entsprechend schützt der Tatbestand gleichrangig die Rechtsgüter der persönlichen Freiheit und des Vermögens.[89] Er ist unter dem zweiten Titel des Besonderen Teils des StGB unter den strafbaren Handlungen gegen das Vermögen eingereiht. Bestraft wird, wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, jemanden u.a. durch Androhung ernstlicher Nachteile zu einem Verhalten bestimmt, wodurch dieser sich selber oder einen andern am Vermögen schädigt. Bezüglich des

---

81 BGE 122 IV 325 f.; 120 IV 17, 19; 115 IV 207; 107 IV 38; 106 IV 125; 105 IV 122; 101 IV 48.

82 TRECHSEL/MONA, PK StGB, Art. 181 N 5.

83 DELNON/RÜDY, BSK II StGB, Art. 181 N 35 m.H.; zum Cybermobbing BRUN, 105.

84 BGE 119 IV 301, 305.

85 BGE 101 IV 42, 44; 101 IV 167, 169.

86 DELNON/RÜDY, BSK II StGB, Art. 181 N 8 m. w. Hinw.

87 BGE 141 IV 437, 441.

88 BRUN, 105.

89 WEISSENBERGER, BSK II, Art. 156 N 1.

Nötigungsmittels kann auf die entsprechenden Ausführungen verwiesen werden.[90] Bei der verlangten Vermögensdisposition kann es um die Gewährung eines beliebigen Vermögensvorteils gehen, als aktive Vermögensdisposition etwa um die Überweisung eines Betrags.[91] Dieses Offizialdelikt wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

Unter die eben dargestellten Tatbestände fallen auch *Sextortion* oder die *Androhung von Rachepornografie:* Um *Nötigung* würde es sich handeln, wenn der Täter oder die Täterin androht, eine kompromittierende Aufnahme zu veröffentlichen, falls die betroffene Person ihr beispielsweise nicht noch weitere solche Aufnahmen sendet. Eine *Erpressung* würde vorliegen, wenn mit der Veröffentlichung gedroht wird, falls die betroffene Person nicht einen bestimmten Betrag überweist. Eine *Drohung* liegt vor, wenn der Täter oder die Täterin androht, im Internet eine kompromittierende Aufnahme zu veröffentlichen (eingehend Ziff. 3.2.3 und 3.2.4).

Beschimpfung (Art. 177 StGB): Unter die direkte Einschüchterung fällt auch die Beschimpfung. Danach wird bestraft, wer jemanden zum Beispiel durch Schrift oder Bild (und «in anderer Weise» als durch üble Nachrede oder Verleumdung gemäss Art. 173 f. StGB) in seiner Ehre angreift, namentlich durch eine Tatsachenbehauptung unter vier Augen, d.h. nur gegenüber der betroffenen Person selbst, sowie durch ein Werturteil, welches gegenüber Dritten oder aber «unter vier Augen» geäussert wird. Es handelt sich bei Artikel 177 StGB also um einen zu Artikel 173 f. StGB subsidiären Tatbestand bzw. um einen Auffangtatbestand. Gegenstand der Beschimpfung ist entweder ein «reines Werturteil»[92] (d.h. ein blosser Ausdruck der Missachtung, ohne dass sich die Aussage erkennbar auf bestimmte, dem Beweis zugängliche Tatsachen stützt) oder aber eine üble Nachrede bzw. Verleumdung unter vier Augen.[93] Bei einem ehrverletzenden Vorwurf unter vier Augen ist das *subjektive persönliche Ehrgefühl* geschützt, d.h. das «Gefühl, ein achtbarer, ehrbarer Mensch zu sein und bei anderen als solcher bewertet zu werden».[94] Das Ehrgefühl kann neben dem direkten Vorwurf gegenüber der betroffenen Person auch mittelbar durch eine Rufschädigung bei Dritten verletzt sein, die der betroffenen Person zur Kenntnis gelangt.[95] Bei einer Beschimpfung wird der betroffenen Person durch den Täter bzw. die Täterin «jene Achtung versagt, die er bzw. sie dieser objektiv schuldet».[96] Aus der bundesgerichtlichen Rechtsprechung sind etwa die Äusserungen zu erwähnen, jemand sei ein Schwein, ein Luder,[97] ein Psychopath,[98] ein Halunke, [99] oder eine Hure[100]. Es handelt sich um ein auf Antrag verfolgtes Delikt, das mit Geldstrafe bis zu 90 Tagessätzen bestraft wird.

3.2.1.2 Belästigung

Unter dieser Fallgruppe werden Handlungen erfasst, mit denen der Täter oder die Täterin die Privatsphäre der betroffenen Person stört, etwa indem diese mit anstössigen Nachrichten oder Aufnahmen sexuellen Inhalts belästigt wird.

---

[90] WEISSENBERGER, BSK II, Art. 156 N 10.

[91] STRATENWERTH/BOMMER, BT I, § 17 N 6 ff.

[92] Auch als «Formalinjurie» oder «Verbalinjurie» bezeichnet.

[93] RIKLIN, BSK II StGB, Art. 177 N 1 und 4.

[94] RIKLIN, BSK II StGB, Vor Art. 173 N 9; vgl. RIKLIN, 33 f. m. w. Hinw.; in diesem Sinn auch BGE 77 IV 94, 98; 80 IV 159, 164 f.; 85 IV 182, 186; 92 IV 99, 101; 93 IV 20, 21; 96 IV 148, 149.

[95] RIKLIN, BSK II StGB, Vor Art. 173 N 9.

[96] RIKLIN, BSK II StGB, Art. 177 N 1.

[97] BGE 86 IV 81, 82

[98] BGE 93 IV 20, 21

[99] BGE 79 IV 20, 22

[100] BGE 92 IV 115

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Pornografie (Art. 197 StGB): *Pornografisch* ist eine grob vulgäre, besonders primitive Darstellung von auf sich selbst reduzierter Sexualität, die den Menschen zum blossen Sexualobjekt macht und die nach dem Gesamteindruck darauf abzielt, die betrachtende Person sexuell zu erregen.[101] Wird die vom Mobbing betroffene Person mit pornografischem Material belästigt, ist der Tatbestand Pornografie anwendbar. Danach wird bestraft, wer jemandem *«harte Pornografie»* weiterleitet, das heisst insbesondere pornografische Schriften, Ton- oder Bildaufnahmen oder Abbildungen, die sexuelle Handlungen mit Tieren oder nicht sexuelle Handlungen mit Minderjährigen zum Gegenstand haben. Dass auch Gewalttätigkeiten unter Erwachsenen als harte Pornografie gelten, soll mit der Revision des Sexualstrafrechts (Ziff. 1.2.3) aufgehoben werden.[102] Die Strafdrohung dieses von Amtes wegen verfolgten Delikts liegt bei Freiheitsstrafe bis zu drei Jahren oder Geldstrafe; geht es um tatsächliche sexuelle Handlungen mit Minderjährigen, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe (Art. 197 Abs. 4 StGB).

Ist eine *Person unter 16 Jahren* die Adressatin, so ist die Weiterleitung jeglicher Pornografie, auch sogenannter «weicher Pornografie», strafbar. Die Strafe ist diesfalls Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (Art. 197 Abs. 1 StGB). Mit Busse bestraft wird zudem, wer «weiche Pornografie» *einer erwachsenen Person unaufgefordert* anbietet bzw. zustellt (Art. 197 Abs. 2 StGB).

Sexuelle Belästigung (Art. 198 StGB): Handelt es sich nicht um pornografisches Material, kann der Tatbestand der sexuellen Belästigung erfüllt sein. Danach wird u.a. bestraft, wer jemanden in grober Weise durch Worte sexuell belästigt (Abs. 2). Auch hier ist die Revision des Sexualstrafrechts zu erwähnen: Entsprechend der (inzwischen abgeschriebenen) *Motion Reynard 18.4049 «Sexuelle Belästigung. Gravierende Lücken müssen geschlossen werden»* vom 28. September 2018,[103] soll der Tatbestand neu auch durch die Begriffe «Schrift» und «Bild» ergänzt werden. Das Bundesgericht hat in einem neueren Urteil[104] festgehalten, Artikel 198 Absatz 2 StGB umfasse nicht nur ausgesprochene Worte, sondern auch schriftliche oder bildliche Tatobjekte. Dies entspricht auch der neueren Entwicklung in der Lehre.[105] Unter Berücksichtigung des Bestimmtheitsgebots und in systematischer Anlehnung an die Artikel 177 und 261bis StGB soll im Gesetzestext von Artikel 198 StGB zum Ausdruck kommen, dass der Tatbestand auch durch geschriebene Worte erfüllt werden kann. Mit dieser Neuerung wird namentlich das Versenden sexuell konnotierter Bilder oder anzüglicher Nachrichten via IKT vom Tatbestand erfasst.[106] Die gesetzliche Voraussetzung, dass eine derartige sexuelle Belästigung durch Schrift oder Bild in grober Weise erfolgen muss, soll einen Ansatz von Bestimmbarkeit geben und meint (bezüglich dem Tatbestandselement des geltenden Rechts, den Worten), dass nur stark vulgäre Ausdrücke, welche eine grobe Zumutung darstellen, unter den Tatbestand fallen.[107] Die Tat wird, auf Antrag, mit Busse bestraft.

Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB): Als *Auffangtatbestand* für Belästigungen, die nicht unter die vorab genannten Tatbestände fallen, kann der Missbrauch einer Fernmeldeanlage dienen.[108] Es geht hier um den Schutz der Privatsphäre.[109] Nach diesem

---

[101] STRATENWERTH/BOMMER, BT I, § 17 N 4.

[102] BBl **2022** 687, 35.

[103] www.parlament.ch > Geschäft 18.4049. Der Vorstoss wurde am 25. September 2020 abgeschrieben.

[104] Urteil des Bundesgerichts 6B_69/2019 vom 4. November 2019, E. 2.3.2.

[105] DONATSCH, § 65 588.

[106] BBl **2022** 687, 60 f.

[107] ISENRING, BSK II, Art. 198 N 22.

[108] BRUN, 109.

[109] BRUN, 109: Gebrauch der modernen Kommunikationsmittel bzw. Kommunikationstechnologie; RAMEL/VOGELSANG, BSK I StGB, Art. 179^{septies} N 1a: Unter den Tatbestand fallen insbesondere E-Mails, Text- und Bildnachrichten.

Tatbestand wird bestraft, wer aus Bosheit oder Mutwillen eine Fernmeldeanlage zur Beunruhigung oder Belästigung missbraucht. Er ist also geradezu auf Belästigungen via IKT zugeschnitten. Die nach geltendem Recht noch vorausgesetzten subjektiven Elemente der Bosheit oder des Mutwillens wurden mit der Harmonisierungsvorlage (Ziff. 1.2.3) gestrichen. Damit fallen beispielsweise auch obszöne Belästigungen unter den Tatbestand. Massgebend ist, dass die Kontaktaufnahmen via IKT in objektiver Hinsicht lästig oder beunruhigend sind und eine gewisse minimale, quantitative Intensität und/oder qualitative Schwere erreichen.[110] Doch können auch weniger gravierende Äusserungen den Tatbestand erfüllen, die sich durch eine gewisse Häufung in ihrer Wirkung summieren, wie etwa beim Verschicken massenhafter E-Mail-Nachrichten.[111] Die Strafdrohung des Antragsdelikts wurde mit derselben Gesetzesvorlage auf Freiheitsstrafe bis zu einem Jahr oder Geldstrafe angehoben.[112]

3.2.1.3 Blossstellung

Bei dieser Fallgruppe verunglimpft der Täter oder die Täterin die betroffene Person öffentlich, beispielsweise, indem er oder sie ehrverletzende Bekanntmachungen, falsche Informationen oder Gerüchte verbreitet, peinliche, verfälschte, freizügige oder pornografische Bild- oder Videoaufnahmen weiterleitet, (beleidigende) Fake-Profile erstellt oder «Hassgruppen» gründet, in denen negative Äusserungen über die betroffene Person gemacht werden.

Üble Nachrede und Verleumdung (Art. 173 und 174 StGB): Der Tatbestand der *üblen Nachrede* (Art. 173 StGB) setzt voraus, dass der Täter oder die Täterin jemanden bei einem Dritten eines unehrenhaften Verhaltens oder anderer Tatsachen beschuldigt oder verdächtigt, die geeignet sind, den Ruf der betroffenen Person zu schädigen (Ziff. 1 Abs. 1). Bestraft wird auch, wer eine solche Beschuldigung oder Verdächtigung weiterverbreitet. (Ziff. 1 Abs. 2). Handelt der Täter oder die Täterin dabei wider besseres Wissen, handelt es sich um eine *Verleumdung* (Art. 174 StGB).

Kardinalsfrage dieser Tatbestände ist, *wann das Rechtsgut der Ehre verletzt ist*. Rechtsprechung und Lehre gingen hier lange Zeit überwiegend vom sogenannten *faktischen Ehrbegriff* aus.[113] Danach geht es um den *Ruf und die Wertschätzung einer Person als ehrbarer Mensch, ihre Geltung bei Dritten* – oder, wie es das Bundesgericht umschreibt, um den Ruf, «sich so zu benehmen, wie nach allgemeiner Anschauung ein charakterlich anständiger Mensch sich zu verhalten pflegt» (sog. faktische Ehre).[114] Vom Strafrecht erfasst wird gemäss Bundesgericht einzig die *sittliche Ehre*, also der Ruf als ehrbarer Mensch, welche die Persönlichkeit in ihrer menschlich-sittlichen Bedeutung berührt.[115] Damit ist insbesondere die Bezichtigung moralisch verwerflicher Handlungen strafbar.[116] Nicht vom Strafrecht erfasst wird dagegen die *gesellschaftliche Ehre*, also die sozialen Funktionen wie die geschäftliche und berufliche Geltung,[117] was in der Lehre von fast allen massgebenden Autoren und Autorinnen stark kritisiert worden ist.[118] In neuerer Zeit hat das Bundesgericht seine Rechtsprechung insofern relativiert, als es beispielsweise bei Vorwürfen, die das berufliche Verhalten berühren, die Möglichkeit der Mitbeeinträchtigung der sittlichen Ehre anerkennt. Sie können als «Schatten auf die Geltung als ehrbarer Mensch» fallen.[119] Damit sind Vorwürfe in Bezug auf die gesellschaftliche Ehre

---

[110] BGE 126 IV 216 E. 2.

[111] Urteil des Bundesgerichts 6B_75/2009 vom 02.06.2009, E. 3.2.1; BGE 126 IV 219; KINZIG, 3.

[112] BBl **2018** 2827, 2868; BBl **2021** 2997.

[113] RIKLIN, BSK II StGB, Vor Art. 173 N 12.

[114] BGE 93 IV 20, 21; 103 IV 157, 158; 105 IV 111, 112; 105 IV 194, 195; 117 IV 27, 28 f.; 131 IV 154, 157.

[115] BGE 115 IV 42, 44

[116] BGE 76 IV 29

[117] RIKLIN, 39

[118] RIKLIN, BSK II StGB, Vor Art. 173 N 18 mit Hinweisen.

[119] BGE 80 IV 159, 165; 99 IV 148, 150 u. a.; Schwander, StGB, Nr. 600a

dann relevant, wenn sie zugleich die Geltung der betreffenden Person als ehrbarer Mensch treffen können.[120]

In der Praxis wurden beispielsweise die Vorwürfe als ehrverletzend gewertet, jemand betätige sich als Hure,[121] pflege Kontakt zu Zuhältern und Prostituierten und sei in solchen Geschäften aktiv gewesen,[122] habe eine Geschlechtskrankheit,[123] sei in seiner politischen Gesinnung «nazihaft»,[124] leite als Anwalt Prozesse vor allem im eigenen Interesse ein[125] oder sei als Politiker Drahtzieher rechtswidriger Demonstrationen[126]. Eine Ehrverletzung begeht beispielsweise zudem, wer psychiatrische Fachausdrücke verwendet, um jemanden als verschroben, abnorm, charakterlich minderwertig oder als asozialen Sonderling hinzustellen,[127] also dann, wenn psychiatrische Fachausdrücke oder daran angelehnte Begriffe in diffamierender Absicht verwendet werden. Denn nach bundesgerichtlicher Rechtsprechung treffen Vorwürfe von Krankheit und Abnormität nämlich grundsätzlich nicht die Ehre.[128] Der Vorwurf psychischer Defekte ist insofern stets ehrenrührig, als damit die Fähigkeit zur Verantwortlichkeit abgesprochen wird; ausgenommen sind Äusserungen in einem diagnostischen oder therapeutischen Kontext.[129] Darauf, ob der physische oder psychische Defekt wirklich vorhanden ist, kommt es nicht an; so ist es besonders verwerflich, einen psychisch Kranken zum Beispiel als «Spinner» zu bezeichnen.[130]

Die üble Nachrede ist ein Antragsdelikt, das mit Geldstrafe bedroht ist. Bei der Verleumdung liegt die Strafdrohung bei Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (Art. 174 Ziff. 1 StGB). Ist der Täter oder die Täterin planmässig darauf ausgegangen, den guten Ruf einer Person zu untergraben, wird er oder sie mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe nicht unter 30 Tagessätzen bestraft (Art. 174 Ziff. 2 StGB).

Bei der *Hassrede* (eingehend Ziff. 3.2.2) als Verhaltensweise des Cybermobbings stehen ebenfalls die *Ehrverletzungsdelikte* (Art. 173 ff. StGB) im Zentrum, zudem auch die Tatbestände der *Drohung* (Art. 180 StGB) und *Nötigung* (Art. 181 StGB). Erfüllt sein können aber auch die *Antidiskriminierungs-Strafnorm* (Art. 261bis StGB)[131], oder die Tatbestände der *Gewaltdarstellung* (Art. 135) oder der *Aufforderung zu Verbrechen oder Gewalttätigkeit* (Art. 259 StGB) und weitere.

Identitätsmissbrauch (Artikel 179^{decies} nStGB): Mit der Totalrevision des Bundesgesetzes über den Datenschutz vom 19. Juni 1992[132] (DSG) wurde im StGB ein neuer Tatbestand eingeführt, der den sogenannten Identitätsmissbrauch unter Strafe stellt. Das Inkrafttreten des neuen Artikels 179^{decies} StGB ist auf den 1. September 2023 geplant. Danach wird bestraft, wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen. Der im Tatbestand vorausgesetzte Nachteil für die durch den Identitätsmissbrauch betroffene Person muss eine gewisse Schwere erreichen und kann materieller oder immaterieller Natur sein. Dabei

---

[120] BGE 71 IV 225, 230; 77 IV 94, 95; 80 IV 159, 164; 92 IV 94, 96; 98 IV 90, 92; 103 IV 157, 158; 105 IV 111, 112; 105 IV 194, 195; 116 IV 205, 206; 117 IV 27 ff.; 119 IV 44, 47; zum Ganzen RIKLIN, BSK II StGB, Vor Art. 173 N 18 f.

[121] BGE 92 IV 115, 117 f.

[122] Urteil des Bundesgerichts 6B_584/2016 vom 06.02.2017, E. 3.2 und 3.2.1.

[123] BGE 78 IV 32; 80 IV 159, 168 f.

[124] OGer BE, 10. 2. 1987, in SJZ 1988, 327, Nr. 54

[125] BGE 99 IV 148, 149

[126] BGE 108 IV 94, 95

[127] BGE 93 IV 20, 22; 96 IV 54, 55; 98 IV 90, 93; weitere Beispiele siehe bei RIKLIN, BSK II StGB, Vor Art. 173 N 20 ff.

[128] TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 8.

[129] TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 10.

[130] TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173 N 8.

[131] Urteil des Bundesgerichts B_627/2015 vom 04.11.2015, E. 2.8.

[132] **SR 235.1**

kann es bereits ausreichen, bei der betroffenen Person einen massiven Ärger auszulösen. Auf das Antragsdelikt wird Freiheitsstrafe bis zu einem Jahr oder Geldstrafe angedroht sein. Bei der Erstellung von Fake-Profilen wird die Tatsache der Verwendung einer fremden Identität also künftig durch diesen Tatbestand abgedeckt. Der damit einhergehende Reputationsverlust wird weiterhin über die Ehrverletzungsdelikte (Art. 173 ff. StGB) bestraft.[133] Weiter können im Zusammenhang mit der Schaffung von Fake-Profilen die Tatbestände des *unbefugten Eindringens in ein Datenverarbeitungssystem* (Art. 143bis StGB), des *betrügerischen Missbrauchs einer Datenverarbeitungsanlage* (Art. 147 StGB), der *Datenbeschädigung* (Art. 144bis StGB) oder des *unbefugtes Beschaffen von Personendaten* (Art. 179^{novies} StGB, ebenfalls eingefügt mit der Totalrevision des DSG und in Kraft voraussichtlich ab 1. September 2023) anwendbar sein.

Bei der *Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen* handelt es sich um eine Tatvariante der *Rachepornografie*. Geht es dabei um *pornografische Bild- oder Videoaufnahmen,* ist der Tatbestand der *Pornografie* (Art. 197 StGB) einschlägig (Ziff. 3.2.1.2). Die Frage, wann dagegen eine (nicht pornografische) Aufnahme als *peinlich* zu werten ist, scheint nicht einfach. Eine bildliche Darstellung aus dem Intimbereich der abgebildeten Person ist für sich allein nicht ehrverletzend.[134] Ist die Aufnahme aber ehrenrührig oder so verfälscht, dass aus den Umständen eine Verunglimpfung oder Blossstellung der betroffenen Person hervorgeht, können die Ehrverletzungsdelikte (insbesondere die üble Nachrede, Art. 173 StGB, Ziff. 3.2.1.2) erfüllt sein (eingehend Ziff. 3.2.3).

3.2.2 Hassrede

Auf die Strafbarkeit der Hassrede nach geltendem Recht wurde bereits bei den blossstellenden Einzelhandlungen des Cybermobbings eingegangen (Ziff. 3.2.1.3). Geht es um öffentliche Aufrufe zu Hass oder Diskriminierung gegen eine Person oder Personengruppe wegen ihrer Rasse, Ethnie, Religion oder sexuellen Orientierung (Abs. 1), das Verbreiten von Ideologien (Abs. 2), Teilnahme, Organisation und Förderungen von Propagandaaktionen (Abs. 3) sowie öffentliches Herabsetzen und Diskriminieren in einer gegen die Menschenwürde verstossenden Weise durch Wort, Schrift, Bild, Gebärden, Tätlichkeiten oder in anderer Weise (Abs. 4) ist die *Antidiskriminierungs-Strafnorm* (Art. 261bis StGB) einschlägig. Dieser Tatbestand schützt die Menschenwürde und (akzessorisch) den öffentlichen Frieden, indem er den öffentlichen Aufruf zu Hass oder die öffentliche Diskriminierung wegen bestimmter wesentlicher Merkmale der Persönlichkeit für strafbar erklärt. Damit wird für den Bereich des Strafrechts teilweise das Diskriminierungsverbot konkretisiert, das in Artikel 8 BV verankert ist. Artikel 261bis StGB wurde vor Kurzem gestützt auf die parlamentarische Initiative 13.407 Reynard «Kampf gegen die Diskriminierung aufgrund der sexuellen Orientierung» vom 7. März 2013 revidiert und um das Element der sexuellen Orientierung erweitert. Diese Änderung steht seit dem 1. Juli 2020 in Kraft. Wo es um Diskriminierungen aufgrund der Geschlechtsidentität geht,[135] greifen die Tatbestände zum Schutz der Ehre (Art. 173 ff. StGB), der körperlichen Unversehrtheit (Art. 111 ff. StGB) und der sexuellen Integrität (Art. 187 ff. StGB), jene des Zivilrechts zum Schutz der Persönlichkeit (Art. 28 ff. ZGB, Ziff. 3.1) und jene des Verwaltungsrechts zum Schutz vor Diskriminierungen aufgrund des Geschlechts nach dem Bundesgesetz über die Gleichstellung von Frau und Mann vom 24. März 1995[136].

---

[133] BBl **2020** 7639, 7687; BBl **2017** 6941, 7127 f.

[134] SJZ 2004, 95 f.

[135] Die Verhaltensweisen, welche gemäss Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022 (www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres) strafrechtlich verfolgt werden sollen, werden mehrheitlich, jedoch nicht vollumfänglich vom StGB erfasst werden. So umfasst der Schutzbereich von Art. 261bis StGB entgegen dieser Empfehlung weder das Geschlecht an sich, noch sämtliche LGBTI-Personen. Das Parlament hat auf Vorschlag des Bundesrates explizit darauf verzichtet, auch das Element der Geschlechtsidentität in die Strafnorm aufzunehmen: BBl **2018** 5231. Vgl. aber die parlamentarischen Initiativen 21.527 Bertschy, 21.522 Studer, 21.516 Arslan, 21.515 De Quattro, 21.514 Binder-Keller und 21.513 Marti mit den gleichlautenden Titeln «Aufrufe zu Hass und Gewalt aufgrund des Geschlechts müssen strafbar werden» vom Dezember 2021. Die RK-N hat diesen parlamentarischen Initiativen am 23.06.2022 Folge gegeben.

[136] RS **151.1**.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Im Zusammenhang mit dem Untersuchungsgegenstand des vorliegenden Berichts stehen Äusserungen im Vordergrund, welche zu *Hass gegen Personen oder Personengruppen aufrufen*, sowie öffentliches Herabsetzen und Diskriminieren in einer gegen die Menschenwürde verstossenden Weise durch Wort, Schrift, Bild, Gebärden, Tätlichkeiten oder in anderer Weise (Abs. 4). Hass- oder Hetzkampagnen sind ohne Begehung von Ehrverletzungsdelikten kaum denkbar.[137] Hier sind damit wiederum die *Beschimpfung* (Art. 177), die *üble Nachrede* (Art. 173 StGB) und die *Verleumdung* (Art. 174 StGB) zentral (Ziff. 3.2.1.1 und 3.2.1.3). Gemäss der Lehre genügen diese Tatbestände, um auf das neue Phänomen angemessen zu reagieren.[138] Bei der Frage, was als «ehrverletzend» im strafrechtlichen Sinn zu gelten hat, kann das Bundesgericht seine Rechtsprechung den Fragen unserer Zeit anpassen.[139] Nach der heutigen bundesgerichtlichen Rechtsprechung genügt es dabei bereits, wenn jemand «eines Mangels an Pflichtgefühl, Verantwortungsbewusstsein und Zuverlässigkeit oder sonst einer Eigenschaft bezichtigt [wird], die geeignet wäre, ihn als Mensch verächtlich zu machen oder seinen Charakter in ein ungünstiges Licht zu rücken».[140] Einschlägig kann dabei insbesondere auch Artikel 174 Ziffer 2 StGB sein, die *planmässige Rufuntergrabung*. Es handelt sich um eine Qualifikation der Verleumdung.[141] Der konkrete Erfolg eines solchen Vorgehens braucht nicht einzutreten; die blosse Gefahr der Rufzerstörung genügt.

Im Einzelfall können zudem auch die Tatbestände der *Erpressung* (Art. 156 StGB), *Drohung* (Art. 180 StGB), *Nötigung* (Art. 181 StGB), der *Gewaltdarstellung* (Art. 135 StGB) der *Aufforderung zu Verbrechen oder Gewalttätigkeit* (Art. 259 StGB), der *Ausübung von Gewalt und Drohung gegen Behörden und Beamte* (Art. 285 StGB) oder der *Kriminellen oder terroristischen Organisationen* (Art. 260ter StGB) anwendbar sein.

Viele als Hassrede bezeichnete Äusserungen dürften aber die Schwelle der Strafbarkeit nicht erreichen. Gemäss der *Empfehlung des Ministerkomittees des Europarats zur Bekämpfung der Hassrede* vom 20. Mai 2022[142] sollen nur schwerwiegende Formen der Hasssrede strafrechtlich sanktioniert werden. Weniger gravierenden Hassreden soll mittels zivil- bzw. verwaltungsrechtlicher Instrumente begegnet werden. Der Europarat und die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) definieren dabei nicht genau, wann eine schwerwiegende Hassrede vorliegt. Es werden jedoch Faktoren genannt, welche bei der Beurteilung der Schwere zu berücksichtigen sind: So der Inhalt der Hassrede; der politische und soziale Kontext im Moment der Äusserung; die Absichten des Täters; dessen Rolle und Status in der Gesellschaft; die Art, wie die Hassrede verbreitet und verstärkt worden ist; die Möglichkeit schädlicher Auswirkungen; die Art und Grösse des Publikums und die Merkmale der Zielgruppe.[143]

3.2.3 Rachepornografie

Als Rachepornografie gilt es nach weitem Begriffsverständnis, wenn intime Aufnahmen, die ohne Einverständnis der darauf sichtbaren Person hergestellt worden sind, oder die zwar mit deren Einverständnis hergestellt worden sind, aber nur für ganz bestimmte Personen bestimmt waren, weiterverbreitet werden, um sie blosszustellen, zu beleidigen oder zu diffamieren.

---

[137] SELMAN/SIMMLER, 257; SALMINA, 217.

[138] SELMAN/SIMMLER, 228 ff. sowie SALMINA, 218, der allerdings eine Straferhöhung fordert.

[139] SALMINA, 218.

[140] BGE **105** IV 112, 113

[141] SALMINA, 219, der kritisiert, dass sich diese Qualifikation nicht auch bei der üblen Nachrede findet.

[142] Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022, www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres.

[143] Recommandation CM/Rec(2022)16 du Comité des Ministres aux États membres sur la lutte contre le discours de haine du 20.05.2022, www.coe.int > droits de l'homme > Promouvoir les droits de l'homme > Liberté d'expression > Textes adoptés > Comité des Ministres, Ziff. 4.1; Exposé des motifs CM(2022)43, Rz. 32 f. mit Hinweisen auf Entscheide des EGMR.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Handelt es sich um *pornografische Bild- oder Videoaufnahmen*, ist der Tatbestand der Pornografie (Art. 197 StGB) einschlägig. Zum Pornografietatbestand ist auf die obigen Ausführungen (Ziff. 3.2.1.2) zu verweisen. Eine Weiterverbreitung ist strafbar, wenn es sich um «harte Pornografie» handelt (Art. 197 Abs. 1 StGB) oder wenn jegliche, auch «weiche Pornografie» einer Person unter 16 Jahren zugänglich gemacht wird (Art. 197 Abs. 4 StGB). Letzteres ist einerseits der Fall, wenn die betroffene Person in diese Alterskategorie fällt, andererseits aber generell bei einer Publikation im Internet. Denn hier muss der Täter oder die Täterin davon ausgehen, dass auch Personen unter 16 Jahren die Aufnahme ansehen können. Schliesslich ist es auch strafbar, wenn «weiche Pornografie» einer erwachsenen Person unaufgefordert angeboten, d.h. zugestellt wird (Art. 197 Abs. 2 StGB).

Die Eingrenzung, wann eine andere (nicht pornografische) Aufnahme als *peinlich* zu werten ist, scheint nicht einfach. Ist die Aufnahme ehrenrührig oder so verfälscht, dass aus den Umständen eine Verunglimpfung oder Blossstellung der betroffenen Person hervorgeht, können die *Ehrverletzungsdelikte* (insbesondere die üble Nachrede, Art. 173 StGB, Ziff. 3.2.1.2) erfüllt sein. Ist die Aufnahme dagegen lediglich freizügig, lässt sich deren Weiterleitung nicht unter die Ehrverletzungsdelikte subsumieren. Eine bildliche Darstellung aus dem Intimbereich der abgebildeten Person ist für sich allein nicht ehrverletzend.[144] Gerade im Rahmen von Cybermobbing könnte aber eine genügende Verunglimpfung aus den die Veröffentlichung begleitenden Umständen hervorgehen.

Die *Drohung* mit der Veröffentlichung der Aufnahmen, mit welcher der Täter oder die Täterin der betroffenen Person einen schweren Nachteil in Aussicht stellt und diese in Schrecken oder Angst versetzt, wäre nach Artikel 180 StGB zu bestrafen. Was die Herstellung solcher Aufnahmen ohne Wissen bzw. Einverständnis der betroffenen Person betrifft, ist zudem die *Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte* (Art. 179^{quater} StGB) anwendbar. Nach diesem Tatbestand wird bestraft, wer eine Tatsache aus dem Geheimbereich eines andern oder eine nicht jedermann ohne weiteres zugängliche Tatsache aus dem Privatbereich eines andern ohne dessen Einwilligung mit einem Aufnahmegerät beobachtet oder auf einen Bildträger aufnimmt (Abs. 1). Strafbar ist es ferner, eine Aufnahme, die – wie der Täter oder die Täterin weiss oder annehmen muss – auf diese Art hergestellt wurde, aufbewahrt oder einem Dritten zugänglich macht (Abs. 3). Diese Taten werden auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Wie dargelegt, schlägt der Ständerat einen neuen *Artikel 197a StGB* vor, um das Phänomen in einem Spezialtatbestand zu kriminalisieren (Ziff. 1.2.3):

> **Unbefugtes Weiterleiten von nicht öffentlichen sexuellen Inhalten**
>
> [1] Wer einen nicht öffentlichen sexuellen Inhalt, namentlich Schriften, Ton oder Bildaufnahmen, Abbildungen, Gegenstände oder Vorführungen, ohne Zustimmung der darin erkennbaren Person einer Drittperson weiterleitet, wird, auf Antrag, mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.
>
> [2] Hat der Täter den Inhalt öffentlich gemacht, so wird er mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Der Bundesrat erachtet die *Formulierung* des vorgeschlagenen Tatbestandes für *problematisch*. Daraus würden *Schwierigkeiten in der praktischen Anwendung* des Tatbestandes resultieren, was in der Regel den Effekt hat, dass dieser selten als erfüllt erachtet würde. Die vom Parlament geforderte strafrechtliche Verfolgung solcher Phänomene könnte damit nicht durchgesetzt werden. So ist beispielsweise die Formulierung «sexueller Inhalt» wenig klar. Nacktbil-

[144] SJZ 2004, 95 f.

der beispielsweise dürften wohl nur dann darunterfallen, wenn zusätzlich etwa über die Körperhaltung oder die Darstellung ein sexueller Bezug hergestellt wird. Rechtliche Unsicherheiten könnten sich z.B. bei einem Bild ergeben, das eine Frau mit einem übergrossen, betonten Ausschnitt zeigt. Ebenfalls unklar ist die Zuordnung von Bildern, auf denen die betroffene Person nicht erkennbar ist (weil nur gewisse Körperteile abgebildet sind oder sie entsprechend bearbeitet wurden), die Bilder aber mit ihrem Namen versehen sind. Schliesslich ist unklar, was das Merkmal «nicht öffentlich» umfassen soll.

Ein Tatbestand, der sich *auf sexuelle Inhalte beschränkt*, würde zudem nur einen Teil des Phänomens erfassen. Peinliche, verfälschte oder einfach freizügige Aufnahmen würden nur unter der Voraussetzung erfasst, dass sie einen sexuellen Inhalt haben. Soll das Phänomen bestraft werden, müsste der Tatbestand entsprechend anders formuliert werden.

Er sollte auch nicht unter den *strafbaren Handlungen gegen die sexuelle Integrität* eingeordnet werden. Kern des Ganzen ist, dass die betroffene Person durch die Weiterleitung einer nicht für die Augen Dritter gedachten Aufnahme in ihrem Geheim- oder Privatbereich verletzt wird, dass sie eine ehrenrührige Blossstellung erfährt oder dass ihr unter Androhung der Weiterleitung gedroht wird bzw. sie durch eine solche Androhung zu etwas genötigt oder gar erpresst werden soll. Freilich ist, wo es um sexuelle Inhalte geht, auch die sexuelle Scham der betroffenen Person tangiert. Dennoch geht es in der Hauptsache nicht um eine Verletzung der sexuellen Integrität oder um eine sexuelle Belästigung.[145]

3.2.4 Sextortion

Sextortion ist durch das geltende Strafrecht erfasst: Hier sind die Tatbestände der Nötigung (Art. 181 StGB) und der Erpressung (Art. 156 StGB), allenfalls auch der Drohung (Art. 180 StGB) anwendbar. Um *Nötigung* würde es sich handeln, wenn jemand androht, eine kompromittierende Aufnahme zu veröffentlichen, falls die betroffene Person ihm beispielsweise nicht noch weitere solche Aufnahmen sendet. Und eine *Erpressung* würde vorliegen, wenn mit der Veröffentlichung gedroht wird, falls die betroffene Person ihm nicht einen bestimmten Betrag überweist. Eine reine *Androhun*g der Veröffentlichung, mit welcher der betroffenen Person einen schweren Nachteil in Aussicht gestellt und diese dadurch in Schrecken oder Angst versetzt wird, wäre nach Artikel 180 StGB zu bestrafen.

3.2.5 Nicht erfasste Handlungen

Nach geltendem Recht ist damit insbesondere *Cybermobbing* dann nicht strafrechtlich erfasst, wenn die einzelnen Handlungen aufgrund ihres isoliert gesehen geringen Unrechtsgehalts die Schwelle der geltenden Tatbestände nicht erfüllen, das Verhalten in seiner Gesamtheit aber beleidigend, schikanierend, quälend oder herabsetzend auf die betroffene Person wirkt und als strafwürdig scheint. Die bundesgerichtliche Rechtsprechung insbesondere zur Nötigung und zum Missbrauch einer Fernmeldeanlage würde es zulassen, das Verhalten in seiner Gesamtheit zu werten (Ziff. 3.2.1); allerdings ist die Anwendung dieser Rechtsprechung auf Mobbing-Fälle vom Bundesgericht soweit ersichtlich noch nicht geprüft worden.

Nicht strafbar ist nach geltendem Recht auch die *Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen*, wenn es sich *nicht um pornografisches Material* handelt und aus den Umständen auch *kein Vorwurf der Ehrenrührigkeit* hervorgeht.

3.3 Regelung in anderen Ländern

3.3.1 Österreich

Das österreichische Strafgesetzbuch (A-StGB) enthält einen spezifischen Straftatbestand gegen *Cybermobbing*. Er steht seit dem 1. Januar 2016 in Kraft.

[145] Vgl. zum Ganzen BBl **2022** 1011, 4 f.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Art. 107c A-StGB
Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems

(1) Wer im Wege einer Telekommunikation oder unter Verwendung eines Computersystems in einer Weise, die geeignet ist, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen,

1. eine strafbare Handlung gegen die Ehre einer Person für eine größere Zahl von Menschen für eine längere Zeit wahrnehmbar begeht oder
2. eine Tatsache oder Bildaufnahme des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung für eine größere Zahl von Menschen für eine längere Zeit wahrnehmbar macht,

ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(2) Hat die Tat den Selbstmord oder einen Selbstmordversuch der im Sinn des Abs. 1 verletzten Person zur Folge, begeht der Täter innerhalb eines ein Jahr übersteigenden Zeitraums fortgesetzt gegen die verletzte Person gerichtete Tathandlungen im Sinne des Abs. 1 oder übersteigt die Dauer der Wahrnehmbarkeit nach Abs. 1 ein Jahr, so ist der Täter mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Nach diesem Tatbestand muss entweder eine *strafbare Handlung gegen die Ehre einer Person* begangen oder eine *Tatsache oder Bildaufnahme des höchstpersönlichen Lebensbereiches einer Person ohne deren Zustimmung wahrnehmbar* gemacht worden sein. Die zweite Variante betrifft die *Rachepornografie* in ihrem weiten Begriffsverständnis. Er betrifft nur die Cybervariante dieser Delikte, die Tat muss also unter Verwendung der *Telekommunikation oder eines Computersystems* erfolgt sein. Zudem setzt der Tatbestand voraus, dass die strafbare Handlung gegen die Ehre oder die zustimmungslose Verwendung einer Tatsache oder Bildaufnahme einer *grösseren Zahl von Menschen* (worunter mindestens 10 Personen zu verstehen sind)[146] für eine *längere Zeit* wahrnehmbar gemacht wurde. Die Tat muss *fortgesetzt* begangen worden sein, eine einmalige Tathandlung reicht daher nicht, erst wiederholte Tathandlungen erfüllen den Tatbestand. Eines der wohl wichtigsten Elemente des Tatbestandes, das diesen zu einem *abstrakten Gefährdungsdelikt* macht ist, dass die Tat *geeignet sein muss, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen*. Dies ist eine notwendige Eingrenzung. Sie bedeutet, dass das fragliche Verhalten derart unerträglich sein muss, dass sich womöglich selbst ein «Durchschnittsmensch» veranlasst gesehen hätte, seine Lebensgestaltung zu ändern. Das ist beispielsweise bei einem Wechsel der Schule, dem Bruch mit dem Freundeskreis oder dem Ausstieg aus den sozialen Medien zu bejahen.[147] Nach Absatz 2 ist die Strafdrohung insbesondere höher, wenn es als Folge der Handlungen zu einem *Suizid oder Suizidversuch* kommt. Sie ist zudem höher, wenn die Tathandlungen während mehr als einem Jahr begangen wurden oder die Dauer der Wahrnehmbarkeit ein Jahr übersteigt.

Auch die Rachepornografie wird damit nur als Einzelhandlung im Rahmen von Cybermobbing für strafbar erklärt. Zudem geht die Strafbarkeit einschüchternder, blossstellender Verhaltensweisen nicht unter die Schwelle, welche die schon vormals geltenden Ehrverletzungsdelikte des «Beschimpfens, Schmähens, Verspottens oder Herabwürdigens» setzen.[148] Damit kann mit aller Vorsicht gesagt werden, dass der Unterschied zum schweizerischen Recht sich kaum auf die Grenze der Strafbarkeit bezieht, sondern einzig auf *symbolische Gesichtspunkte*.

---

[146] WENK, 93, m.H.

[147] WENK, 93, m.H.

[148] WENK, 93 f., m.H.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Was die Anwendung des Tatbestandes in der Praxis betrifft, zeigt sich aufgrund der Kriminalstatistik,[149] dass sehr viele Anzeigen wegen Artikel 107c A-StGB eingegangen sind, aber nur wenige Verurteilungen erfolgt sind. So waren es *2017* 359 Anzeigen aber nur 16 Verurteilungen und *2019* 330 Anzeigen aber nur 11 Verurteilungen. Zumindest mit Blick auf diese Zahlen kann damit aktuell noch nicht von einer grossen Praxisrelevanz gesprochen werden; da die Norm aber erst seit Kurzem in Kraft steht, ist bezüglich dieser Aussage Zurückhaltung geboten.[150]

Das österreichische Strafgesetzbuch pönalisiert auch die Hassrede, bezeichnet als *Verhetzung*. Artikel 283 A-StGB schützt Gruppen oder Mitglieder von Gruppen, welche sich durch ihre Hautfarbe, Sprache, Religion oder Weltanschauung, Staatsangehörigkeit, Abstammung oder nationale oder ethnische Herkunft, Geschlecht, Behinderung, Alter oder sexuelle Ausrichtung auszeichnen. Mögliche Handlungen sind die Aufforderung oder Aufstachelung zum Hass gegenüber einer bestimmten Gruppe oder einem Mitglied dieser Gruppe, die Beleidigung einer Person oder Gruppe sowie Billigung, Leugnung, gröbliche Verharmlosung oder Rechtfertigung bestimmter Verbrechen. Bei der Beleidigung ist zusätzlich gefordert, dass der Täter oder die Täterin in der Absicht gehandelt hat, die Menschenwürde der Gruppe oder der Person zu verletzen, sowie dass die Beleidigung dazu geeignet ist, die Gruppe oder die Person in der öffentlichen Meinung verächtlich zu machen oder herabzusetzen. Damit ist auch hier – wegen der Ausgestaltung des Tatbestandes als Sonderdelikt, unter das nur bestimmte Personen oder Gruppen fallen, sowie durch die zusätzlichen Tatbestandsvoraussetzungen einer Beleidigung – die einfache Herabsetzung, welche nicht ehrenrührig ist und auch keine weiteren Tatbestände erfüllt, nicht erfasst.

3.3.2 Deutschland

Das deutsche Strafgesetzbuch (D-StGB) enthält *keinen eigenständigen Tatbestand zum Mobbing oder Cybermobbing*. Die einzelnen Handlungsweisen werden gestützt auf die für die einzelnen Handlungen einschlägigen Tatbestände bestraft.

Mit dem Netzwerkdurchsetzungsgesetz (NDG), das am 1. Oktober 2017 in Kraft trat, soll erreicht werden, dass die Betreiber sozialer Netzwerke auf entsprechende Meldung hin selbständig und rasch Löschungen vornehmen. Es verpflichtet die Betreiber gewinnorientierter sozialer Netzwerke dazu, «offensichtlich strafbare Inhalte» binnen 24 Stunden nach Eingang einer Beschwerde zu löschen. Das NDG begründet keine neuen Löschpflichten, die nicht schon nach bestehenden straf- oder zivilrechtlichen Vorschriften bestehen würden. Eine kürzlich erfolgte Revision des NDG soll die Bekämpfung von Rechtsextremismus und Hasskriminalität verbessern und die Rechte der Nutzer von sozialen Netzwerken stärken.

In diesem Zusammenhang ist insbesondere der *Tatbestand der Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen* nach § 201a D-StGB zu nennen. Im deutschen Recht fällt die Verletzung der Persönlichkeit durch Aufnahmen unter das Strafrecht, während im schweizerischen Recht hierbei das Zivilrecht greift (Ziff. 3.1). § 201a D-StGB bestraft insbesondere auch die *Rachepornografie:* Strafbar ist die wissentlich unbefugte Veröffentlichung von ursprünglich befugt hergestellten Bildaufnahmen (§ 201a Abs. 1 Ziff. 5 D-StGB). Damit sind insbesondere Aufnahmen gemeint, die in einer Beziehung einvernehmlich hergestellt bzw. verschickt wurden und nach dem Ende der Beziehung aus Rache veröffentlicht wurden.[151] Bestraft wird zudem, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht

[149] www.statistik.gv.at > Statistiken > Bevölkerung und Soziales > Kriminalität und Sicherheit > Verurteilungs- und Wiederverurteilungsstatistik, Publikationen > Gerichtliche Kriminalstatistik 2017 und 2018, 82 sowie Gerichtliche Kriminalstatistik 2019 und 2020, 86; Polizeiliche Kriminalstatistik 2017, www.bundeskriminalamt.at > Grafiken & Statistiken > Broschüre Sicherheit 2017, 17; WENK, 94.

[150] WENK, 94.

[151] WENK, 97 m.H.

(§ 201a Abs. 2 D-StGB). Diese Begehungsvariante wurde explizit mit Blick auf eine Veröffentlichung im Rahmen von Cybermobbing eingeführt.[152] Die *Volksverhetzung* wird in Deutschland mit § 130 D-StGB unter Strafe gestellt. Auch dieser Tatbestand ist als Sonderdelikt ausgestaltet: Betroffen muss eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe sein, Teile der Bevölkerung oder ein Einzelner wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung. Strafbar ist es, zum Hass aufzustacheln oder zu Gewalt- oder Willkürmassnahmen aufzufordern (Abs. 1 Ziff. 1). Strafbar ist es sodann, die Menschenwürde dadurch anzugreifen, dass der Täter oder die Täterin eine vorbezeichnete Gruppe bzw. Einzelne wegen ihrer Zugehörigkeit zur vorbezeichneten Gruppe beschimpft, böswillig verächtlich macht oder verleumdet. Auch hier knüpft der Tatbestand damit an die bestehenden Ehrverletzungsdelikte des D-StGB an.

3.3.3 Frankreich

Das französische Strafgesetzbuch (F-StGB) kennt Tatbestände, die explizit die Handlungsweisen des Mobbings unter Strafe stellen. Pönalisiert wird die Belästigung einer Person durch wiederholte Äusserungen oder Verhaltensweisen, welche eine Verschlechterung ihrer Lebensbedingungen bezwecken oder bewirken und sich in einer Beeinträchtigung ihrer körperlichen oder geistigen Gesundheit äussern (Art. 222-33-2-2 F-StGB). Die Handlung kann auch durch mehrere Personen gemeinsam an einem Opfer begangen werden, sofern in abgestimmter Weise oder auf Anweisung einer der Personen gehandelt wird. Hierbei ist es nicht notwendig, dass eine einzelne Person wiederholt gehandelt hat. Die Äusserungen oder Verhaltensweisen können demselben Opfer auch nacheinander von mehreren Personen ohne Absprache aufgezwungen werden, welche wissen, dass sie durch eine Wiederholung gekennzeichnet sind. *Cybermobbing* stellt eine qualifizierte Tatvariante dar.

Rachepornografie wird in Artikel 226-2-1 F-StGB unter Strafe gestellt. Der Tatbestand knüpft an Bestimmungen gegen den Geheim- und Privatbereich (Art. 226-1 und 226-2 F-StGB) und erhöht deren Strafdrohung, sofern diese sich auf sexuelle Äusserungen oder Bilder beziehen, welche an einem öffentlichen oder privaten Ort aufgenommen wurden. Nach Artikel 226-2-1 Absatz 2 F-StGB wird sodann bestraft, wer der Öffentlichkeit oder einem Dritten Aufnahmen oder Dokumente mit sexuellem Text oder sexuellen Bildern, welche mit der ausdrücklichen oder mutmasslichen Zustimmung der betroffenen Person erlangt wurden, zur Kenntnis bringt, obwohl die betroffene Person nicht mit der Verbreitung einverstanden ist.

Als *Hassrede* gilt nach Artikel R. 625-7 F-StGB die nichtöffentliche Aufstachelung zu Diskriminierung, Hass oder Gewalt gegen eine Person oder eine Gruppe von Personen aufgrund ihrer Herkunft oder ihrer tatsächlichen oder vermuteten Zugehörigkeit oder Nichtzugehörigkeit zu einer bestimmten Ethnie, Nation, Rasse oder Religion (Abs. 1) oder aufgrund ihres Geschlechts, ihrer sexuellen Orientierung oder Geschlechtsidentität oder einer Behinderung (Abs. 2). Die reine Herabsetzung oder Blossstellung ist damit auch hier nicht erfasst.

3.3.4 Italien

Italien kennt keine explizite Strafnorm gegen Mobbing oder Cybermobbing. Es gibt jedoch eine zivilrechtliche Grundlage, welche eine Definition von Cybermobbing beinhaltet und das Recht auf Löschung von Inhalten mit Cybermobbing-Charakter sowie eine Beschwerdemöglichkeit bei Missachtung des Rechts auf Löschung gewährleistet.

Das Verbreiten herabsetzender Ideologien sowie das Aufreizen zu Diskriminierungen und gewalttätigen Akten werden gemäss Artikel 3 Buchstabe a und b des Spezialgesetzes zum Rassismusübereinkommen bestraft. Die Handlung muss hierbei aus rassistischen, ethnischen, na-

[152] WENK, 97 f. m.H.

tionalen oder religiösen Gründen erfolgen. Auch hier geht das Gesetz bezüglich der Strafbarerklärung blossstellender und herabsetzender Hassrede nicht über die Ehrverletzungsdelikte hinaus.

3.4 Diskussion der Problematik in der Lehre

In der Schweizer Lehre haben sich bisher insbesondere BRUN und WENK zur Frage geäussert, ob es eines spezifischen *Cybermobbing-Tatbestandes* im StGB bedarf. Ein solcher wird von beiden Autoren übereinstimmend als *nicht erforderlich* und nicht sachlich begründbar angesehen.[153] Die typischen Formen von Cybermobbing könnten *mit den bestehenden Tatbeständen grundsätzlich sanktioniert* werden.[154] Es wird als problematisch erachtet, nur Cybermobbing unter Strafe zu stellen, vergleichbar schwerwiegende Fälle des *klassischen Mobbings* jedoch nicht.[155] Zudem wird auf die *Konkurrenzprobleme* bei der Schaffung einer solchen Norm hingewiesen.[156]

WENK ortet allerdings dennoch einen gewissen *Reformbedarf*. Da Cybermobbing-Handlungen im Wesentlichen bereits durch bestehende Tatbestände erfasst würden, schlägt er punktuelle Anpassungen bei den entsprechenden Tatbeständen vor. So könnten nach seiner Auffassung beispielsweise die Ehrverletzungsdelikte durch einen Absatz ergänzt werden, der eine höhere Strafdrohung aufnimmt für den Fall, dass die Tat durch IKT begangen wurde und dadurch für eine grössere Anzahl von Menschen wahrnehmbar war.[157] Eine Strafbarkeitslücke bestehe zudem hinsichtlich der (böswilligen) Veröffentlichung von intimen, peinlichen oder entwürdigenden Bildern.[158]

Sämtliche Autoren und Autorinnen weisen zudem auf die Wichtigkeit der *Prävention* zur Verhinderung von Cybermobbing hin.[159]

3.5 Analyse

3.5.1 Heterogenität der Verhaltensweisen

Die dargestellten Verhaltensweisen *können konkret auf höchst vielfältige Art begangen werden*. Das zeigt sich insbesondere beim Cybermobbing, das definitionsgemäss aus wiederholten Einzelhandlungen besteht, aber auch bei den weiteren, im Rahmen dieses Berichts behandelten digitalen Angriffen.

Die von den Einzelhandlungen tangierten *Rechtsgüter* sind unterschiedlicher Art. Es kann sich etwa um Verletzungen der Ehre, der (Handlungs-)Freiheit, des Geheim- oder Privatbereichs, des Vermögens oder der sexuellen Integrität handelt. Angesichts der Vielfalt der beeinträchtigten Rechtsgüter stellt sich somit das Problem, wo ein allfälliger eigenständiger Tatbestand gegen Cybermobbing einzuordnen wäre.

Ein weiterer Punkt, der in diesem Zusammenhang zu beachten ist, sind die *Konkurrenzen*. Wenn man einen eigenständigen Tatbestand gegen Cybermobbing einführte, wären auf ein und dieselbe Tat einerseits dieser, andererseits die bereits geltenden Tatbestände anwendbar, die für die jeweiligen Einzelhandlungen greifen. Der Cybermobbing-Tatbestand müsste aber als *lex specialis* vorgehen. Ein solcher, übergreifender Cybermobbing-Tatbestand müsste einen weiten Fächer möglicher Verhaltensweisen abdecken, die von kaum strafwürdigen bis zu

---

[153] BRUN, 111; WENK, 99 f.; zum deutschen Recht PREUSS, 104.

[154] BRUN, 111, der aber nicht ausschliesst, dass sich dies aufgrund zukünftiger Entwicklungen ändern könnte.

[155] PREUSS, 104.

[156] WENK, 99.

[157] WENK, 95.

[158] WENK, 99.

[159] BRUN, 111; WENK, 100; PREUSS, 104.

schwerwiegenden Verhaltensweisen reichen. Insofern müsste er eine sehr weite Strafdrohung vorsehen. Es könnte sein, dass eine Bestrafung nach den einzelnen, bereits geltenden Tatbeständen unter Anwendung der Regeln der Konkurrenz mit entsprechender Erhöhung gleichartiger Strafen (Art. 49 StGB) im Einzelfall zu einer höheren Sanktion führen würde.

3.5.2 Bestimmtheitsgebot

Das Bestimmtheitsgebot besagt, dass das *strafbare Verhalten im Gesetz bestimmt umschrieben sein muss.* Denn der Rechtsadressat oder die Rechtsadressatin muss erkennen, welches Verhalten strafbar ist; nur so kann er oder sie sich danach richten. Es handelt sich hierbei um eine Ausprägung des Legalitätsprinzips. Dieses ist in Artikel 1 StGB verankert, was auch systematisch die Wichtigkeit dieses Grundsatzes demonstriert.

Ein Tatbestand, in welchem eine *generell-abstrakte Formulierung für höchst unterschiedliche Tathandlungen* gefunden werden müsste – wie bei einem Cybermobbing-Tatbestand, aber auch etwa bei der Umschreibung der Hassrede oder der Rachepornografie – könnte diesem Prinzip kaum genügen. Die *Grenzziehung zwischen nicht strafwürdigen und strafbaren Einzel- bzw. Gesamthandlungen* hinge von unbestimmten Rechtsbegriffen ab, die den rechtsanwendenden Behörden einen rechtsstaatlich heiklen Spielraum belassen. Dieser Spielraum wäre vor allem auch *in der Praxis schwer zu handhaben*.

3.5.3 Generalpräventive Wirkung

Von einem symbolischen Tatbestand gegen Cybermobbing erhofft man sich eine generalpräventive Wirkung. Der Gedanke der Generalprävention geht davon aus, dass der oder die Tatgeneigte durch das Bewusstsein des Verbots und seiner Durchsetzung demotiviert (negative Generalprävention) oder dass dadurch gar der Entstehung einer Tatneigung entgegengewirkt wird (positive Generalprävention).[160]

Was die negative Generalprävention betrifft, wird es für die potentielle Rechtsbrecherin oder den potentiellen Rechtsbrecher nicht entscheidend sein, ob die Tat durch einen speziellen oder durch die Anwendung mehrerer Tatbestände bestraft wird. Es gilt in der Lehre als gesichert, dass auch die Höhe der angedrohten Strafe auf den Entschluss des potentiellen Täters oder der potentiellen Täterin nicht entscheidend wirkt. Die Geltung einer Norm scheint mit anderen Worten nicht von Art und Mass der gesetzlich angedrohten Sanktion abzuhängen. Vielmehr kommt es darauf an, ob deren Missachtung überhaupt strafrechtlich geahndet wird.[161]

Dieser Schluss bedeutet in seiner Umkehr aber auch, dass ein Straftatbestand, der aufgrund seiner zwingend unbestimmten Formulierung (Ziff. 3.5.2) und damit verbundener Beweisschwierigkeiten (Ziff. 3.5.4) kaum zu Verurteilungen führt, auch eine gegenteilige Wirkung haben könnte: Wenn ein bestimmtes Verhalten trotz (spezifischer) Formulierung im Gesetz kaum zu Verurteilungen führt, kann dies fast schon als «Einladung» für Tatgeneigte gelten. Dieser Aspekt sollte davor warnen, spezifische Tatbestände mit weitgehend symbolischer Wirkung in das StGB aufzunehmen.

3.5.4 Beweisschwierigkeiten

Von einem spezifischen Cybermobbing-Tatbestand wäre *nur schwerlich eine Erleichterung der Beweissituation* zu erwarten. Ein solcher Tatbestand müsste *zwingend wiederholte Einzelakte voraussetzen, die zu einem bestimmten Erfolg führen*. Auch diese müssten konkret nachgewiesen werden, wie es beim Beweis der Umstände der Fall wäre, welche die heute geltenden und ebenfalls anwendbaren Tatbestände erfüllen. Freilich können diese beim Cybermobbing

[160] WENK, 99.

[161] STRATENWERTH, AT I, § 2 N 21.

etwa mittels Screenshots oder Chatverläufe einfacher dokumentiert werden als bei offline-Mobbing.

Auch darf nicht vergessen gehen, dass *Tatbestandselemente, die einen grossen Interpretationsspielraum lassen* – und insofern mit Blick auf das Bestimmtheitsgebot heikel sind (Ziff. 3.5.2) – oftmals nur schwer zu beweisen sind. Im österreichischen Tatbestand ist dies beispielsweise der Nachweis, dass das Cybermobbing geeignet war, eine Person in ihrer Lebensführung unzumutbar zu beeinträchtigen. So kann es sein, dass die Subsumtion unter die einzelnen anwendbaren Tatbestände gelingen würde, die Subsumtion unter den spezifischen Tatbestand dagegen höhere Hürden setzt.

3.5.5 Technologieneutralität des Strafrechts

Die grundsätzliche Technologieneutralität der Straftatbestände im StGB hat *verschiedene Vorzüge*. Die generell-abstrakte Umschreibung der Strafbarkeitsvoraussetzungen macht die Tatbestände offen für Entwicklungen, die zum Erlasszeitpunkt noch nicht voraussehbar waren – gerade auch im technologischen Bereich. Wo immer möglich sind die Tatbestände daher so formuliert, dass sowohl Handlungen aus der realen als auch der virtuellen Welt darunterfallen.

Dem Grundsatz der Technologieneutralität folgte das Parlament beispielsweise auch beim neuen Tatbestand zum *Identitätsmissbrauch* (Art. 179^{decies} StGB, in Kraft per 1. September 2023). Der Bundesrat führte in der Botschaft dazu aus, das Phänomen und die Problematik des Missbrauchs einer fremden Identität hätten sich zwar durch den verbreiteten Gebrauch elektronischer Medien und entsprechender Kommunikationsmittel akzentuiert und verschärft. Die Strafbestimmung solle jedoch unabhängig vom Tatmittel und Medium, mit dem die Tat begangen wird, Anwendung finden. Daher erfasse diese auch den herkömmlichen Missbrauch einer Identität. Es werde davon abgesehen, lediglich den mittels eines Computers oder eines Telefons begangenen Identitätsmissbrauch unter Strafe zu stellen.[162]

Auch beim *Mobbing* fragt sich, ob tatsächlich ein Tatbestand nur für die Begehung per IKT geschaffen werden soll. Zweifelsohne ist Cybermobbing von seinen Auswirkungen her besonders schwerwiegend für die betroffene Person. Dennoch scheint es problematisch, wenn für Cybermobbing ein Spezialtatstand geschaffen würde, für vergleichbar schwerwiegende Fälle des klassischen Mobbings dagegen nicht.[163] Dies mutet inkonsequent an und ist sachlich nicht zu begründen.

Zudem darf nicht vergessen gehen, dass es *Mischformen* gibt: In ein und demselben Mobbingfall können manche Tathandlungen in der virtuellen, andere in der realen Welt erfolgen (Ziff. 2.1). Bei einem speziellen Cybermobbing-Tatbestand würde sich die Frage stellen, wie mit solchen Fällen umzugehen ist.

Vor diesem Hintergrund vermag auch der Vorschlag nicht zu überzeugen, von einem speziellen Cybermobbing-Tatbestand abzusehen, dafür aber bei einzelnen anwendbaren Tatbeständen (beispielsweise den Ehrverletzungsdelikten, Art. 173 ff. StGB) eine *Qualifikation* vorzusehen, wenn die Tat mittels IKT begangen und dadurch für eine grössere Anzahl von Menschen wahrnehmbar wird (Ziff. 3.4).[164] Eine solche Änderung könnte e contrario so gewertet werden, dass solche Umstände nur bei diesen Tatbeständen zu beachten sind, bei anderen jedoch nicht.

Die Regeln der *Strafzumessung* erlauben es bereits, der erhöhten kriminellen Energie bei Begehung der Tat mittels IKT Rechnung zu tragen. Andererseits könnte eine solche Änderung zu einem uferlosen Revisionsbestreben führen, wonach bei weiteren Tatbeständen ein entsprechender, wohl weitgehend *deklaratorischer* Absatz eingefügt werden soll.

---

[162] PREUSS, 104.

[163] BBl **2017** 6941, 7127 f.

[164] WENK, 95.

3.5.6 Definition aufgrund der Perspektive der betroffenen Person

Die Definition des Mobbings und Cybermobbings erfolgt schwergewichtig aufgrund der Wahrnehmung und des Gefühls der betroffenen Person. Sie setzt voraus, dass *sich die betroffene Person beleidigt, schikaniert, gequält oder herabgesetzt fühlt* (Ziff. 2.1.3).

Dies stellt eine *grosse Herausforderung bei der Formulierung des Tatbestandes* dar. Ein strafrechtlicher Schutz des subjektiven Gefühls ist dezidiert abzulehnen. Die Umschreibung des strafrechtlich relevanten Verhaltens muss sich daher an der Betrachtung eines Durchschnittsmenschen in derselben Situation orientieren. Der spezifische Cybermobbing-Tatbestand müsste als *Erfolgsdelikt* konzipiert sein und eine Veränderung der Lebensumstände auch bei einer besonnenen Person voraussetzen – oder (wie im österreichischen Strafrecht) als *abstraktes Gefährdungsdelikt*, das die *Eignung* zu einer solchen Veränderung auch bei einer besonnenen Person genügen lässt. Nur dadurch wird die strafbare Handlung objektiviert. Und nur dadurch wird die Schwelle der *Strafwürdigkeit* genügend hoch angesetzt.

Dies löst allerdings nicht das Problem, wie die Eignung zur Veränderung der Lebensumstände beweisbar ist und wie sich der Tatbestand somit in der Praxis bewähren kann.

3.5.7 Mehrzahl von Handlungen

Die Tatsache, dass sich beim Cybermobbing mehrere Verhaltensweisen summieren, findet nach geltendem Recht durch die Konkurrenzregeln bzw. auf Strafzumessungsebene Berücksichtigung.[165] Ein spezifischer Mobbing- oder Cybermobbing-Tatbestand könnte aber insofern eine Änderung bewirken, als damit *auch Mobbingfälle erfasst würden, bei denen sich für die betroffene Person gravierende Folgen ergeben, während die Einzelhandlungen für sich alleine die Strafbarkeitsschwelle der einzelnen Straftatbestände nicht erreichen*.

Das Bundesgericht hat bereits verschiedentlich zugelassen, bei der Frage der Erfüllung eines Tatbestandes auf das gesamte Verhalten des Täters oder der Täterin abzustellen (so bei der Nötigung durch Stalking, Art. 181 StGB und beim Missbrauch einer Fernmeldeanlage, Art. 179^{septies} StGB; Ziff. 3.2.1). Dies würde durch die Schaffung eines spezifischen Tatbestandes lediglich noch gesetzlich festgehalten.

3.5.8 Mehrzahl von Personen

Beim (Cyber-)Mobbing summieren sich nicht nur die Verhaltensweisen; es handelt sich oftmals auch um ein *dynamisches Zusammenwirken mehrerer Personen*. So setzte insbesondere das *frühere Begriffsverständnis* bei Mobbing *per definitionem* ein Handeln mehrerer Personen gegen denselben Betroffenen voraus (Ziff. 2.1).

Diesem Umstand kann sowohl bei Anwendung mehrerer Tatbestände als auch eines speziellen Cybermobbing-Tatbestandes Rechnung getragen werden. Beim Mobbing können insbesondere mehrere Täter und Täterinnen in *Mittäterschaft* handeln. Als Mittäter gilt, «wer bei der Entschliessung, Planung oder Ausführung eines Deliktes vorsätzlich und in massgebender Weise mit anderen Tätern zusammenwirkt, so dass er als Hauptbeteiligter dasteht; dabei kommt es darauf an, ob der Tatbeitrag nach den Umständen des konkreten Falles und dem Tatplan für die Ausführung des Deliktes so wesentlich ist, dass sie mit ihm steht oder fällt».[166] Fassen also mehrere Personen zusammen den Vorsatz, eine bestimmte Person (über IKT) einzuschüchtern, zu belästigen oder blosszustellen bzw. führen sie eine solche Tat je in sogenannter Tatherrschaft aus, sind beide wegen der begangenen Taten strafbar.

Der *Anstifter* bestimmt einen anderen vorsätzlich zu einem Delikt, ruft mit anderen Worten dessen Tatentschluss hervor. Das wäre beispielsweise der Fall, wenn jemand eine Hassgruppe

---

[165] PREUSS, 104.

[166] BGE 135 IV 152, 155 E. 2.3.1; 133 IV 76, 82 E. 2.7; 130 IV 58, 66 E. 9.2.1; 126 IV 84, 88 E. 2c/aa; 125 IV 134, E. 3a; 120 IV 265, 271 f. E. 2c/aa.

gründet und andere überredet, auch teilzunehmen, wobei sich diese beispielsweise ebenfalls ehrverletzend äussern. Der Anstifter wird nach derselben Strafdrohung bestraft, die für den Täter oder die Täterin gilt (Art. 24 Abs. 1 StGB).

Der *Gehilfe* leistet vorsätzlich Hilfe zum verübten Delikt. Beim Cybermobbing ist insbesondere die *psychologische* Gehilfenschaft relevant, die etwa darin bestehen könnte, dass jemand in der Hassgruppe mitmacht, sich aber nicht aktiv beteiligt. Für die Bestrafung der Gehilfenschaft greift ex lege eine *Strafmilderung* (Art. 25 StGB).

3.6 Handlungsmöglichkeiten des Gesetzgebers

3.6.1 Eigenständiger Tatbestand zum Mobbing

Dem Gesetzgeber stehen verschiedene Handlungsvarianten zur Verfügung. Insbesondere mit Blick auf den *Grundsatz der Technologieneutralität* wäre es nicht angebracht und auch nicht sachlich begründbar, einen Tatbestand speziell für die Cybervariante des Mobbings einzuführen. Wenn man einen spezifischen Tatbestand schaffen will, sollte dieser technologieneutral ausgestaltet werden und sowohl online als auch offline begangenes Mobbing erfassen. Man könnte sich dabei allenfalls überlegen, eine *Qualifikation* einzuführen, d.h. eine höhere Strafandrohung vorzusehen, wenn der Täter oder die Täterin unter Nutzung von IKT handelt und die Einschüchterungen bzw. Blossstellungen für einen grossen Personenkreis wahrnehmbar sind. Die Rechtsprechung wird zu entscheiden haben, wie mit Mischformen zwischen on- und offline-Mobbing umzugehen ist.

Ein solcher Tatbestand liesse es insbesondere zu, Mobbing zu erfassen, bei dem die *einzelnen Handlungen* aufgrund ihres isoliert gesehen geringen Unrechtsgehalts die Schwelle der geltenden Tatbestände nicht erfüllen, das Verhalten in seiner Gesamtheit aber beleidigend, schikanierend, quälend oder herabsetzend auf die betroffene Person wirkt und als strafwürdig scheint.

Die *systematische Einordnung* eines solchen Tatbestandes wirft Probleme auf. Am ehesten könnte er bei den strafbaren Handlungen gegen die Freiheit (Einschüchterung) oder gegen die Ehre (Blossstellung) eingeordnet werden. Eine Herausforderung wird es sein, die Tatbestandselemente mit genügender Bestimmtheit zu formulieren. Der Tatbestand sollte als Erfolgsdelikt oder abstraktes Gefährdungsdelikt konzipiert sein und ähnlich dem österreichischen Tatbestand voraussetzen, dass die Verhaltensweisen geeignet sind, eine besonnene Person in derselben Lage zu einer Veränderung der Lebensumstände zu drängen.

3.6.2 Verzicht auf einen eigenständigen Tatbestand

Zahlreiche Gründe sprechen dafür, auf einen speziellen Tatbestand zum Mobbing bzw. Cybermobbing zu verzichten. So der Grundsatz, dass das *Strafrecht als schärfstes Schwert des Staates* nur dort eingesetzt werden sollte, wo dies nötig ist. Von einer *rein symbolischen* Gesetzgebung sollte abgesehen werden.

Mobbing ist aufgrund der heute geltenden Tatbestände weitestgehend in ähnlichem Umfang strafbar, wie es nach einem speziellen Tatbestand wäre. Auch Mobbing, bei dem die einzelnen Handlungen aufgrund ihres isoliert gesehen geringen Unrechtsgehalts die Schwelle der geltenden Tatbestände nicht erreichen, das Verhalten in seiner Gesamtheit aber beleidigend, schikanierend, quälend oder herabsetzend auf die betroffene Person wirkt: Hier könnte allenfalls eine Übernahme der Rechtsprechung zur Nötigung betreffend Stalking (Art. 181 StGB)[167] und zum Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB)[168] durch das Bundesgericht dazu

[167] BGE 129 IV 262, 265 ff.; 141 IV 437, 441.

[168] Urteil des Bundesgerichts 6B_75/2009 vom 02.06.2009, E. 3.2.1; BGE 126 IV 219.

führen, das Verhalten in seiner Gesamtheit zu würdigen und entsprechend bestrafen zu können.

3.6.3 Strafbarerklärung der Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen

Die Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen fällt zum Teil nicht unter die geltenden Straftatbestände, namentlich wenn es sich *nicht um pornografisches Material handelt* (Art. 197 StGB), aus den Umständen *kein Vorwurf der Ehrenrührigkeit* hervorgeht (Art. 173 ff. StGB) und es sich *nicht um ohne Einwilligung der betroffenen Person aufgenommene Tatsachen aus dem Geheimbereich* handelt oder um Tatsachen aus dem *Privatbereich, die nicht jedermann zugänglich sind* (Art. 179^{quater} Abs. 3 StGB).

Solches Verhalten könnte – soweit es als strafwürdig erachtet wird und die zivilrechtlichen Möglichkeiten des Persönlichkeitsschutzes als ungenügend angesehen werden – für strafbar erklärt werden. Dies könnte mittels eines (technologieneutralen) spezifischen Tatbestandes oder auch als Tatvariante eines Mobbing-Tatbestandes erfolgen. Im Rahmen der Revision des Sexualstrafrechts schlägt der Ständerat einen neuen Tatbestand vor, der das *unbefugte Weiterleiten von nicht öffentlichen sexuellen Inhalten* bestrafen soll (Art. 197*a* E-StGB; Ziff. 3.2.3). Im Gegensatz zu diesem Vorschlag sollte ein allfälliger neuer Tatbestand allerdings *nicht auf sexuelle Inhalte beschränkt* sein, sondern *auch anderweitig kompromittierende Aufnahmen* erfassen. Er sollte entsprechend auch nicht unter den strafbaren Handlungen gegen die sexuelle Integrität eingeordnet werden, sondern bei jenen gegen die Ehre und den Geheim- oder Privatbereich (Dritter Titel des zweiten Buches).

3.7 Fazit

Nach geltendem Recht ist *Cybermobbing dann nicht strafrechtlich erfasst, wenn die einzelnen Handlungen aufgrund ihres isoliert gesehen geringen Unrechtsgehalts die Schwelle der geltenden Tatbestände nicht erfüllen, das Verhalten in seiner Gesamtheit aber beleidigend, schikanierend, quälend oder herabsetzend auf die betroffene Person wirkt*. Die bundesgerichtliche Rechtsprechung zur Nötigung durch Stalking (Art. 181 StGB) und zum Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB) würde es zulassen, das Verhalten in seiner Gesamtheit zu werten (Ziff. 3.2.1). Allerdings wurde diese Rechtsprechung soweit ersichtlich in Mobbing-Fällen bisher nicht angewendet.

Von den umliegenden Ländern kennt einzig das *österreichische Strafrecht* einen *speziellen Tatbestand zum Cybermobbing*. Hierzulande wäre ein solcher insbesondere mit Blick auf die *grundsätzliche Technologieneutralität des Strafrechts* nicht angebracht und auch nicht sachlich begründbar. Die Lehre spricht sich denn auch gegen einen solchen Tatbestand aus, fordert aber z.T. punktuelle Anpassungen.

Es wäre denkbar, einen eigenständigen *Tatbestand zum Mobbing* vorzusehen. Evtl. könnte dieser eine *Qualifikation,* d.h. eine höhere Strafandrohung für eine Begehung des Mobbings unter Nutzung von IKT enthalten, wenn die Einschüchterungen bzw. Blossstellungen für einen grossen Personenkreis wahrnehmbar sind.

Mit einem spezifischen Mobbing-Tatbestand wären aber verschiedene Probleme verbunden:

- Ein Mobbing-Tatbestand müsste die Vielfalt möglicher Mobbing-Handlungen umfassen (sog. *Heterogenität der Verhaltensweisen*). Mit anderen Worten müsste eine generell-abstrakte Formulierung für höchst unterschiedliche Tathandlungen gefunden werden. Ein solcher Tatbestand könnte kaum vor dem *Bestimmtheitsgebot* standhalten. Die Grenzziehung zwischen nicht strafwürdigen und strafbaren Einzel- bzw. Gesamthandlungen hinge von unbestimmten Rechtsbegriffen ab, die den rechtsanwendenden Be-

hörden einen rechtsstaatlich heiklen und schwer zu handhabenden Spielraum belassen. Aufgrund der sehr weiten Strafdrohung, die ein solcher Tatbestand vorsehen müsste, könnte es sein, dass eine Verfolgung gestützt auf die einzelnen, in concreto erfüllten und bereits geltenden Tatbestände im Einzelfall in Anwendung der *Konkurrenzregeln* zu einer höheren Sanktion führen würde. Zudem wäre es in Anbetracht der unterschiedlichen, von den einzelnen Handlungen tangierten *Rechtsgüter* fraglich, wo ein solcher Tatbestand *systematisch einzuordnen* wäre.

- Was die *negative Generalprävention* betrifft, scheint entscheidend, ob ein Verhalten überhaupt strafrechtlich geahndet wird (gestützt auf die geltenden Tatbestände oder einen spezifischen Mobbing-Tatbestand), während es auf Art und Mass der angedrohten Sanktion in weitem Mass nicht anzukommen scheint. Der Gesetzgeber sollte sich somit nicht von *symbolischen Überlegungen* leiten lassen.
- Von einem spezifischen Cybermobbing-Tatbestand wäre nur schwerlich eine Erleichterung der *Beweissituation* zu erwarten. Auch die wiederholten Einzelakte, die ein solcher Tatbestand zwingend voraussetzen müsste, müssten je einzeln bewiesen werden. Gerade Tatbestandselemente, die einen grossen Interpretationsspielraum lassen – und insofern mit Blick auf das Bestimmtheitsgebot heikel sind – sind oftmals nur schwer zu beweisen, insbesondere betreffend Tatvorsatz.

Bei der übrigen *«digitalen Gewalt»* bzw. übrigen *digitalen Angriffen gegen die Persönlichkeit* lässt sich lediglich strafloses Verhalten ausmachen, was die *Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen* betrifft. Nach geltendem Recht ist dies dann nicht strafbar, wenn es sich *nicht um pornografisches Material* handelt (Art. 197 StGB), aus den Umständen *kein Vorwurf der Ehrenrührigkeit* hervorgeht (Art. 173 ff. StGB) und es sich *nicht um ohne Einwilligung der betroffenen Person aufgenommene Tatsachen aus dem Geheimbereich* handelt oder um Tatsachen aus dem *Privatbereich, die nicht jedermann zugänglich sind* (Art. 179^{quater} Abs. 3 StGB). Solches Verhalten könnte – soweit es als strafwürdig erachtet wird und die zivilrechtlichen Möglichkeiten des Persönlichkeitsschutzes als ungenügend angesehen werden – für strafbar erklärt werden. Anders als der Vorschlag des Ständerates im Rahmen der *Revision des Sexualstrafrechts* (Unbefugtes Weiterleiten von nicht öffentlichen sexuellen Inhalten, Art. 197*a* E-StGB) sollte ein allfälliger neuer Tatbestand jedoch nicht auf sexuelle Inhalte beschränkt sein, sondern auch *andere Aufnahmen kompromittierender Art* erfassen. Er sollte entsprechend auch nicht unter den strafbaren Handlungen gegen die sexuelle Integrität eingeordnet werden, sondern bei jenen gegen die Ehre und den Geheim- oder Privatbereich (Dritter Titel des zweiten Buches).

4 Rechtsdurchsetzung

4.1 Ausgangslage

4.1.1 Problemstellung

Bei der *strafrechtlichen Verfolgung von Taten, die über IKT begangen werden,* sind meistens nicht fehlende materielle Bestimmungen das Problem. Werden solche Taten von einer *anonymen Täterschaft* begangen, ist vielmehr die *Rechtsdurchsetzung die grösste Schwierigkeit*. Für die Identifikation der Täterschaft und auch den Nachweis anderer Sachverhaltselemente sind die Strafverfolgungsbehörden *auf Daten als Beweismittel angewiesen, die oft im Ausland gespeichert sind*. Die Beweissicherung ist somit technisch und rechtlich anspruchsvoll.

Im Folgenden werden die Möglichkeiten des Zugriffs von Strafverfolgungsbehörden auf Daten im Ausland generell dargestellt. Ein Blick auf Möglichkeiten des Entfernens (Takedown) und Sperrens von rechtswidrigen Daten rundet die Darstellung ab.

4.1.2 Akteure im Internet

Der Bundesrat hat im ersten Social Media-Bericht die Akteure rund um Social Media-Plattformen eingehend erläutert.[169] In Bezug auf den vorliegenden Bericht ist von folgenden Akteuren auszugehen, die über Beweismittel verfügen können:

Plattformbetreiber: Plattformbetreiber stellen Nutzenden einen *Rahmen zum Austausch selbst geschaffener oder aufgegriffener Inhalte* zur Verfügung. Sie machen den Nutzenden *Vorschriften* für den Umgang mit anderen Nutzenden oder unbeteiligten Dritten sowie für die Herstellung, Verwendung oder Verbreitung von Inhalten. Sie können darin festlegen, welche Inhalte oder Verhaltensweisen nicht erlaubt sind. Sie üben aber in der Regel eine im Vergleich zu traditionellen Medien geringere redaktionelle Kontrolle aus. Inhalte, welche den Nutzungsbestimmungen widersprechen, können entfernt werden *(«Notice and Takedown»)*.

Die meisten der in der Schweiz stark genutzten[170] Plattformen haben ihren Sitz im Ausland. Die Nutzenden können dort unter echtem Namen oder unter einem Pseudonym auftreten. Zu diesen meist in den USA domizilierten Anbietern gehören Facebook, Instagram, YouTube, Snapchat, Pinterest, Twitter oder TikTok:

- Die Plattform **Facebook** ermöglicht die Erstellung von privaten Profilen und Unternehmensseiten, welche untereinander vernetzt und einer unbeschränkten Anzahl von Abonnenten und Abonntentinnen zugänglich gemacht werden können. Facebook wird vom Unternehmen Meta Platforms Inc. (USA; bis im Jahr 2021 Facebook Inc.) betrieben. Das Bundesgericht hielt fest, dass Facebook eine ausländische Programm- und Applikations-Anbieterin sei.[171] Die schweizerische Tochtergesellschaft von Meta befasst sich mit der Entwicklung des schweizerischen Marktes für Werbeauftritte. Sie ist im Gegensatz zu Meta Platforms Ireland Limited bzw. Meta Platforms Inc. (USA) nicht die Inhaberin der Facebook-Daten.[172]
- **Instagram** ist ein kostenloser Dienst, auf dem Fotos und Videos geteilt, bewertet und kommentiert werden können. Er gehört zu Meta Platforms Inc. (USA).
- **YouTube**, eine Tochtergesellschaft von Google LLC (USA), ist ein kostenloses Videoportal, auf das sich Videos hochladen lassen, bzw. auf dem diese angeschaut, geteilt, bewertet und kommentiert werden können. Nutzende können einen eigenen YouTube-Kanal erstellen.
- **Snapchat** ist ein kostenloser Instant-Messaging-Dienst und wird von Snap Inc. (USA) betrieben.
- Auf der Plattform **Pinterest** können die Nutzenden Bilderkollektionen mit Beschreibungen an virtuelle Pinnwände heften. Pinterest wird von Pinterest Inc. (USA) betrieben.
- **Twitter** ist ein soziales Netzwerk für Microblogging, auf dessen Plattform die Nutzenden Kurznachrichten veröffentlichen. Die Nachrichten richten sich meist an ein unbeschränktes Publikum und nur ausnahmsweise an einen geschlossenen, vom Sender festgelegten Empfängerkreis. Die Nutzenden wollen typischerweise möglichst viele Follower generieren.[173] Twitter wird vom US-Unternehmen Twitter Inc. betrieben.

---

[169] Postulatsbericht Social Media 2013, Ziff. 2.3.

[170] Zur Nutzung in der Schweiz vgl. etwa www.mcschindler.com > Studien > Digital 2022 Report zur Entwicklung der globalen Nutzung von Internet, Social Media und Mobile vom 15.02.2022, Zahlen und Fakten in Kürze. Für die Mediennutzung von Jugendlichen vgl. etwa die JAMES-Studie 2020 der Zürcher Hochschule für Angewandte Wissenschaften, www.zhaw.ch > Forschung > Mediennutzung > JAMES > Ergebnisbericht JAMES-Studie.

[171] BGE 143 IV 270, 277.

[172] BGE 143 IV 21.

[173] Urteil des Bundesgerichts 5A_195/2016 vom 4.7.2016, E. 5.3.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

- **TikTok** ist eine Video-Plattform, auf der Nutzende kurze Videos hochladen und diese dann mit anderen teilen bzw. bewerten können. TikTok wird vom chinesischen Unternehmen ByteDance betrieben.

Hosting-Provider: Viele Plattformbetreiber nehmen die Dienste sog. Hosting-Provider in Anspruch, welche ihnen *technische Infrastruktur* wie z.B. Speicherplatz, Rechenkapazität oder Übermittlungskapazität zur Verfügung stellen. Wie die meisten Plattformbetreiber hat auch die Mehrzahl der grossen Hosting-Provider ihren Sitz im Ausland. Sie haben in der Regel zwar keine eigene redaktionelle Verantwortung, sind aber *technisch oftmals in der Lage, Inhalte auf ihren Systemen zu löschen*. Ausländische Dienste sind auch im Bereich der *reinen Speicherdienste* weit verbreitet, beispielsweise Google docs, Apple iCloud, Microsoft office.live.com oder dropbox.

Access-Provider: Die *Verbindung zwischen den Nutzenden und den Plattformen* wird durch Zugangsdienstleister hergestellt (Access-Provider). Schweizerische Nutzende nehmen in der Regel die Dienste eines in der Schweiz ansässigen Access-Providers in Anspruch. Access-Provider sind typischerweise *nicht in der Lage, unerwünschte Inhalte zu löschen,* da sie nicht auf ihren Servern gespeichert sind. Denkbar ist allerdings, dass sie den *Zugang zu bestimmten Inhalten blockieren*.[174]

E-Mail-Provider: Relevant für die Strafverfolgung sind auch die zahlreichen ausländischen E-Mail-Dienste wie z.B. gmail von Google. Die Mails stehen aber nicht im Herrschaftsbereich der schweizerischen Niederlassung von Google.[175]

4.1.3 Cloud Computing als globalisiertes Datenmanagement

Der Begriff Cloud Computing suggeriert, dass die Kommunikation sich in virtuellen Wolken abspielt und sich von Hardwareinfrastrukturen ablöst. Cloud Computing basiert aber auf realen Hardwareinfrastrukturen. Gemeint ist damit die *Bereitstellung von IKT-Infrastruktur* wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet. Cloud Computing umschreibt den Ansatz, IKT-Ressourcen *online* zur Verfügung zu stellen, ohne dass diese bei den Nutzenden auf dem lokalen Rechner installiert sein müssen. Bekannte Beispiele von Cloud-Diensten sind Amazon Web Services, Apple iCloud, Dropbox, Google Docs oder Microsoft Office 365.

Grosse Internetunternehmen sind weltweit tätig und folgen bei Planung und Aufbau ihrer Infrastrukturen in erster Linie ökonomischer Rationalität. Zur Erbringung ihrer Dienstleistung bedarf es z.T. mehrerer, grosser Datencenter. So betreibt beispielsweise Facebook/Meta – soweit bekannt – drei Data Center in Europa (Schweden, Dänemark und Irland).

Die *Plattformbetreiber* haben zwar in den einzelnen Ländern oft *Niederlassungen*. Diese haben aber einzig zur Aufgabe, dort die entsprechende Plattform zu *vermarkten*. Sie haben keinen Einfluss auf die technische Konzeption und den Betrieb der Plattform oder auf die Speicherung der Daten.

Diese Konstellation führt dazu, dass *selbst Kommunikation, die sich von einem Sender aus der Schweiz an Adressaten in der Schweiz richtet, über ausländische Infrastrukturen abgewickelt wird und die entsprechenden Daten im Ausland gespeichert sind.* Fragen zum Zugriff auf strafrechtlich relevante Daten erhalten vor diesem Hintergrund oft eine internationale Dimension, selbst wenn die Kommunikation an sich zwischen Endpunkten in der Schweiz stattfindet.

[174] So in Art. 86. Abs. 1 des Bundesgesetzes über Geldspiele vom 29.09.2017 (Geldspielgesetz [BGS], SR 935.51); dazu Urteil des Bundesgerichts 2C_336/2021 vom 18.05.2022, E. 7 und 8.

[175] Urteil des Bundesgerichts 1B_142/2016 vom 16.11.2016, E. 3.

4.2 Zugriff der Strafverfolgungsbehörden auf Daten

4.2.1 Identifikation des Anschlusses

Personen kommunizieren im Internet oft unter einem *Pseudonym*. Im Strafverfahren wegen einer IKT-Straftat ist deshalb die *Identifikation der unbekannten verdächtigen Person der erste und entscheidende Ermittlungsschritt*. Erforderlich hierfür ist i.d.R. die *Internet Protokoll-Adresse,*[176] unter der die verdächtige Person mit dem Internet verbunden war. IP-Adressen sind ein Teil der Daten, die ein Mail- oder Plattform-Server bei jedem Zugriff speichert. Mit dieser Information ist freilich nur der Anschlussinhaber identifizierbar. Zur Ermittlung der effektiv handelnden Person sind *weitere Schritte* erforderlich (z.B. Beschlagnahme von IKT-Geräten).

4.2.2 Das Territorialitätsprinzip bei der Erhebung von Beweismitteln

4.2.2.1 Grundsatz

Das Territorialitätsprinzip besagt, dass alle Personen, die sich auf schweizerischem Territorium befinden, auch den schweizerischen Gesetzen unterworfen sind. Die Regeln der Strafprozessordnung[177] (StPO) und des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016[178] (BÜPF) richten sich also an Personen in der Schweiz. Daraus folgt, dass *Beweismittel von schweizerischen Behörden grundsätzlich nur erhoben werden dürfen, wenn sie sich im Inland befinden* (Art. 1 und Art. 54 StPO i.V.m. Art. 1 Abs. 1 Bst. b des Bundesgesetzes über internationale Rechtshilfe in Strafsachen vom 20. März 1981[179] [IRSG] und Art. 3 StGB).[180]

4.2.2.2 Daten in der Schweiz

Benötigen die Strafverfolgungsbehörden Daten als Beweismittel, können sie den *Inhaber zur Herausgabe auffordern* (Art. 265 StPO, vgl. auch Art. 264 StPO), die *IT-Systeme von Privaten durchsuchen* (Art. 246 StPO) und Daten bzw. die *Datenträger beschlagnahmen* (Art. 263 ff. StPO[181]). Die Behörden können diese Massnahmen auch bei einer Hausdurchsuchung unmittelbar durchsetzen (Art. 244 und Art. 265 Abs. 4 StPO). Der Inhaber kann die Siegelung der Daten verlangen (Art. 248 StPO).[182] Heute spielt die Beschlagnahme und Durchsuchung von Smartphones eine grosse Rolle. Das Bundesgericht stellt dabei relativ hohe Anforderungen an die Geltendmachung von Geheimhaltungsinteressen (z.B. Berufsgeheimnisse), die einer Entsiegelung der Daten entgegenstehen können.[183]

Die *Pflicht zur Aufbewahrung der Daten des Internetverkehrs* ist nicht einheitlich geregelt und hängt massgeblich davon ab, ob der Server-Betreiber in den Anwendungsbereich des BÜPF fällt. Die Überwachung des Internetverkehrs ist eine Massnahme aus dem Bereich der Überwachung des Fernmeldeverkehrs (FMÜ). Sie ist ein Sonderfall der Beschlagnahme und es gelten strengere Regeln, namentlich weil die Beweise heimlich erhoben werden (Art. 269 ff. StPO).[184] Die Modalitäten der Durchführung einer FMÜ sind im BÜPF geregelt.

---

[176] Zur Funktion von IP-Adressen vgl. BGE 136 II 508, E. 3.3.

[177] SR **312.0**.

[178] SR **780.1**.

[179] SR **351.1**.

[180] BGE 141 IV 108.

[181] Vgl. BOMMER/GOLDSCHMID, BSK StPO II, Art. 263 N 27. Die Behörden können die Daten vorläufig sicherstellen, wenn die Gefahr besteht, dass Beweismittel unterdrückt werden oder wenn andere Verdunkelungshandlungen drohen (Art. 263 Abs. 3 und Art. 265 Abs. 4 StPO). Werden Beweise bei Behörden erhoben, ist gemäss Urteil des Bundesgerichts 1B_26/2016 vom 29. November 2016, E. 4.1, nicht nach Art. 263 ff. StPO vorzugehen, sondern nach den Regeln über die nationale Rechtshilfe (Art. 43 ff. StPO).

[182] Gegebenenfalls muss ein Gericht entscheiden, vgl. Art. 248 Abs. 3 oder Art. 264 Abs. 3 StPO.

[183] Vgl. Urteil des Bundesgerichts 1B_342/2017 vom 11.12.2017, E. 3.3 (Beschwerde gegen Entsiegelungsgesuch abgelehnt); allgemein dazu THORMANN/BRECHBÜHL, BSK StPO II, Art. 248 N 22 ff. m.w.H.

[184] Es gilt insbesondere ein Richtervorbehalt für die Genehmigung von FMÜ-Massnahmen.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Die *Beweisbeschaffung mittels GovWare* ist ein Spezialfall der FMÜ. Die GovWare ist ein Informatikprogramm, mit dem sich der verschlüsselte Fernmeldeverkehr direkt – d.h. an der Quelle – überwachen lässt (Art. 269ter StPO).[185] Der Einsatz von GovWare ist im Strafverfahren nur unter restriktiven Voraussetzungen genehmigungsfähig. So ist insbesondere der Katalog der Anlasstaten deutlich enger als bei einer normalen FMÜ. Zur Aufklärung der meisten Äusserungsdelikte – wie Ehrverletzungen, Rassendiskriminierung sowie Aufforderung zu Verbrechen oder zur Gewalttätigkeit – und von Verletzungen des Urheberrechts ist der Einsatz von GovWare nicht zulässig (Art. 269ter i.V.m. Art. 286 Abs. 2 StPO).

4.2.2.3 Aufforderung zur Datenherausgabe nur an den Dateninhaber

Wer von den Strafverfolgungsbehörden in der Schweiz aufgefordert wird, Daten herauszugeben, muss die *Herrschaftsmöglichkeit* über die verlangten Daten haben, um prozessual mitwirkungspflichtig zu sein. Die *schweizerischen Niederlassungen* von Google und Facebook/Meta sind nach der Rechtsprechung des Bundesgerichts nicht Inhaber der Daten der Nutzenden, da sie die Dienste lediglich vermarkten, aber nicht betreiben.[186] Die Mitarbeitenden solcher Unternehmen sind deshalb in dieser Hinsicht *nicht mitwirkungspflichtig*. Die Strafverfolgungsbehörden müssen somit die Daten, die nicht in der Schweiz gespeichert sind, auf dem *Rechtshilfeweg* beschaffen.

4.2.2.4 Anwendung des sog. Zugriffsprinzips

Wer über einen Internetzugang im Inland einen Dienst benutzt, der von einem ausländischen Unternehmen angeboten wird, handelt nach der Rechtsprechung des Bundesgerichts nicht «im Ausland». Der blosse Umstand, dass die Daten des betreffenden Internetdienstes auf Servern im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche *nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium* (im Sinne der Praxis des Bundesgerichts) erscheinen.[187]

Wenn die Zugangsdaten also in einer prozessual zulässigen Form erhoben worden sind,[188] dürfen die Strafverfolgungsbehörden in der Schweiz über das Nutzerkonto auf die so verfügbaren Daten zugreifen und sie verwerten.[189] Weil nicht heimlich zugegriffen wird, kann die beschuldigte Person zur Wahrung von Geheimnissen die Siegelung der Daten verlangen.[190]

Diese Praxis des Bundesgerichts wird etwa kritisiert mit dem Argument, sie verletze das Territorialitäts- und das Souveränitätsprinzip.[191] Dem kann man entgegenhalten, dass der Zugriff über das Nutzerkonto ohne Mitwirkung einer Person im Ausland möglich ist. Es wird insbesondere kein Zwang auf Personen im Ausland ausgeübt.[192] Das ist ein wichtiger Unterschied zu Beispielen, die zur Begründung der Auffassung angeführt werden, dass der Zugriff auf die Daten das Territorialitäts- bzw. das Souveränitätsprinzip verletze und u.U. sogar strafbar sei.[193]

---

[185] Eingehend dazu die BBl **2013** 2683, 2771 ff. und HANSJAKOB, Rz. 10 ff.

[186] BGE 143 IV 21, 25 f. und Urteil des Bundesgerichts 1B_142/2016 vom 16.11.2016, E. 3.

[187] BGE 143 IV 270, 287 f.

[188] Z.B. Beschlagnahme von PC/Smartphone oder Unterlagen wegen Kollusionsgefahr bei der Aufklärung schwerer Straftaten, dazu BGE 143 IV 270, 279 ff.

[189] BGE 143 IV 270, 285 f.

[190] BGE 143 IV 270, 280.

[191] GRAF, Rz. 21 ff. Allg. dazu AEPLI, 130 f. Eingriffe in fremde Souveränitätsrechte bei grenzüberschreitenden Ermittlungen in sozialen Netzwerken nimmt für das deutsche Recht BAUER, S. 62 ff. an; anders WICKER, 356. Zur Diskussion in Deutschland vgl. IHWAS, 289 ff.

[192] Dieselbe völkerrechtliche Frage stellt sich spiegelbildlich (aus schweizerischer «Opferperspektive») bei Art. 271 StGB: In diesem Kontext zum Zwangselement bzw. der Freiwilligkeit und dem Erfordernis der Rechtshilfe vgl. den Entscheid des Bundesstrafgerichts (BStGer) RR.2015.196-198 vom 18.11.2015, E.2.2.1 f. und HUSMANN, BSK StGB II, Art. 271 N 15 f.; zum Ganzen auch Ziff. 4.2.3.

[193] GRAF, Rz. 22 f., 25 f.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Von der technologischen Seite her betrachtet scheinen bei Beweiserhebungen im Internet *neue Differenzierungen bei der Auslegung des Territorialitätsprinzips* nicht abwegig: Bei Applikationen und Fileservern, die auf einer Cloud-Computing-Architektur aufbauen, ist häufig nicht klar, in welchem Land die Daten gespeichert werden. Der Speicherort kann zudem technisch bedingt rasch ändern, ohne dass die Nutzenden dies bemerken. Deshalb lässt sich oft nicht eindeutig sagen, an wen man ein Rechtshilfeersuchen richten müsste.[194] Der Befund, dass die Beweisverwertung zulässig ist, sofern in der Schweiz eine gesetzeskonforme Herrschaftsmöglichkeit über die fraglichen Daten besteht und Straftaten von einer gewissen Schwere verfolgt werden, ist somit naheliegend.[195]

Bei einer restriktiven Anwendung des Territorialitätsprinzips bleibt der Strafverfolgung meist nur das zeitraubende Rechtshilfeverfahren (Ziff. 4.2.4). Das wiederum kann dazu führen, dass gesetzliche Fristen ablaufen und eine Strafverfolgung allenfalls eingestellt werden muss.[196] Der vom Bundesgericht nun als zulässig beurteilte Fernzugriff ist demgegenüber eine effiziente Art der Beweismittelbeschaffung, deren Bedeutung noch zunehmen dürfte.[197]

Beim Zugriff aus der Schweiz auf Daten im Ausland besteht freilich ein Risiko für Mitarbeitende von Strafverfolgungsbehörden, sich nach der ausländischen Gesetzgebung strafbar zu machen.[198] Dieses Risiko lässt sich bei einem einseitigen Vorgehen nie ausschliessen. Es lässt sich nur regulieren, wenn eine bilaterale oder multilaterale Vereinbarung besteht, welche den grenzüberschreitenden Zugriff der Vertragsparteien regelt.

4.2.3 Schranke im StGB: Verletzung fremder Gebietshoheit

Werden Beweise im Ausland abseits eines Rechtshilfeverfahrens erhoben, kann dies nicht nur im Ausland strafrechtlich relevant sein, sondern auch in der Schweiz. Ein direktes Vorgehen der schweizerischen Strafverfolgungsbehörden, wie das der belgischen Behörden gegen Yahoo Inc. in USA oder Skype Communications SARL in Luxembourg,[199] wäre nach schweizerischem Recht mindestens problematisch.[200] Die Anwendung oder Androhung von Zwang gegen Unternehmen oder Personen im Ausland ist nämlich auch nach schweizerischem Recht strafbar.

Mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe wird bestraft, wer die Gebietshoheit eines fremden Staates verletzt, insbesondere durch unerlaubte Vornahme von Amtshandlungen auf dem fremden Staatsgebiet (Art. 299 Ziff. 1 Abs. 1 StGB). Artikel 299 StGB ist das Gegenstück zur verbotenen Handlung für einen fremden Staat (Art. 271 Ziff. 1 StGB).[201] Die möglichen Tathandlungen sind deshalb spiegelbildlich-identisch. Dazu gehört auch die Zustellung von verpflichtenden Prozessverfügungen, insb. wenn darin Zwang angedroht wird (z.B. Verfügungen von CH-Gerichten an US-Internetunternehmen).[202] Diese Straftat kann nur mit Ermächtigung des Bundesrates verfolgt werden (Art. 302 Abs. 1 StGB).

---

[194] Vgl. dazu Urteil des Bundesgerichts 1B_142/2016 vom 16.11.2016, E. 3.3 und BGE 143 IV 21, 25. Zum sog. «loss of location» vgl. SIEBER/NEUBERT, 249.

[195] Grundlegend SCHMID, 108 f.; eingehend BANGERTER, 280 ff.

[196] Z.B. die Frist für die Aufbewahrung und Verwertung von IP-Adressen, welche Randdaten nach Art. 273 Abs. 3 StPO sind; dazu auch BGE 139 IV 98 (vollständiger Sachverhalt im Urteil des Bundesgerichts 1B_481/2012 vom 22.01.2013, E. 2 und 3).

[197] GRAF, Rz. 3, 9 ff.; IHWAS, 263. Generell zur Beschlagnahme von Mobiltelefonen vgl. Urteil des Bundesgerichts 1B_342/2017 vom 07.12.2017 (insb. E. 6.1 f.).

[198] GRAF, Rz. 32; siehe auch das Fallbeispiel bei SIEBER/NEUBERT, 248 f.

[199] Hof van cassatie van België, 01.12.2015, Arrest Nr. P.13.2082.N (Yahoo Inc., USA) und Hof van beroep Antwerpen, 15.11.2017, C/1288/2017 (Skype Communications SARL, Luxembourg).

[200] Dazu GRAF, Rz. 28. Vgl. auch Verwaltungspraxis der Bundesbehörden (VPB) 1985 51.5, E. III. (Fall Marc Rich): Ein direkt an CH-Unternehmen gerichteter, mit Beugestrafen verbundener Herausgabebefehl von US-Behörden ist völkerrechtswidrig, das Befolgen des Befehls verstösst gegen schweizerische Gesetze (Art. 273 StGB); Ermächtigung zur Strafverfolgung i.c. nicht erteilt.

[201] STRATENWERTH/BOMMER, BT II, § 51 N 12.

[202] STRATENWERTH/BOMMER, BT II, § 47 N 14. Zum spiegelbildlichen Problem bei Art. 271 StGB vgl. Entscheid des BStGer RR.2015.196-198 vom 18.11.2015, E. 2.2.1 f. und VPB 2016.3, Ziff. II 9.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Im Gegensatz zu den verbotenen Handlungen für einen fremden Staat (Art. 271 StGB) spielt die Verletzung fremder Gebietshoheit in der Praxis bisher keine Rolle. In prozessualer Hinsicht muss jedoch betont werden, dass in strafbarer Weise erhobene Beweise grundsätzlich nicht verwertbar sind (Art. 141 Abs. 2 StPO). Zu bedenken ist weiter, dass die Vornahme einer Amtshandlung auch nach ausländischem Recht strafbar sein kann, falls dort eine mit Artikel 271 StGB vergleichbare Norm existiert.

4.2.4 Rechtshilfe

Falls die schweizerischen Strafverfolgungsbehörden Daten von Anbietern mit Sitz im Ausland nicht selber direkt erheben dürfen, können sie diese allenfalls mittels Rechtshilfe beschaffen. Bei der Rechtshilfe in Strafsachen werden im ersuchten Staat strafrechtliche Untersuchungsmassnahmen durchgeführt wie für ein eigenes Strafverfahren – nur, dass die erhobenen Beweismittel in einem ausländischen Strafverfahren (im ersuchenden Staat) verwendet werden. Die Rechtsgrundlagen dafür sind in der Regel völkerrechtlicher[203] oder verwaltungsrechtlicher Natur. Das Verfahren richtet sich dabei nach dem IRSG.[204] Rechtshilfeverfahren sind aufwändig und es kann je nachdem mehrere Monate dauern, bis die Strafverfolgungsbehörden die Daten erhalten. Je nach ausländischem Rechtssystem erfolgt auch keine unmittelbare provisorische Sicherung bzw. Sperre der Daten, was die Arbeit der Strafverfolgungsbehörden zusätzlich erschwert. Für viele Strafverfolger ist der Weg über die Rechtshilfe zu lang und zu beschwerlich.[205]

4.2.4.1 Rechtshilfeersuchen an die USA

Eine grosse Anzahl der Internet-Unternehmen hat ihren Hauptsitz in den USA. Die Datenherrschaft wird von den Konzernen oft an ihrem Hauptsitz behauptet, weshalb die rechtshilfeweise Erhebung von Beweismitteln häufig auf der Grundlage des Staatsvertrages zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vom 25. Mai 1973[206] (RVUS) erfolgt.

Eine zentrale Voraussetzung zur zwangsweisen Anordnung von Beweiserhebungen ist die beidseitige Strafbarkeit (Art. 4 Ziff. 2 RVUS). Diese ist gegeben, wenn die nach schweizerischem Recht strafbare Handlung nach US-Recht ebenfalls strafbar ist. Der Tatbestand muss zudem in der Liste der Straftaten aufgeführt sein, für welche gemäss bilateralem Staatsvertrag Zwangsmassnahmen angewendet werden können. Ehrverletzungsdelikte (Art. 173 ff. StGB), aber auch Widerhandlungen gegen das Verbot der Rassendiskriminierung (Art. 261bis StGB) sind darin nicht aufgeführt. Demnach besteht bei diesen Delikten im Verhältnis zu den USA kein Anspruch auf rechtshilfeweise Anordnung von Zwangsmassnahmen.

Richten Strafverfolgungsbehörden bei solchen Delikten dennoch Rechtshilfeersuchen an die USA, so beurteilen sich diese ausschliesslich nach US-Recht, insb. in Bezug auf die Voraussetzungen für die Anordnung von Zwangsmassnahmen. Praktisch alle Rechtshilfeersuchen, welche im Rahmen von Ehrverletzungsdelikten oder Widerhandlungen gegen die Antirassismus-Strafnorm gestellt werden, werden von den US-Behörden nicht vollzogen. Die US-Verfassung schützt nämlich unter dem Titel der Redefreiheit viele Äusserungen, welche in der Schweiz einen Straftatbestand erfüllen. Mangels beidseitiger Strafbarkeit sind die US-Behörden somit oft nicht in der Lage, bei den betroffenen Unternehmen die entsprechenden Beweismittel zu erheben, da diese auch in einem innerstaatlichen Verfahren nicht erhältlich gemacht werden könnten.

---

[203] Multi- oder bilaterale Staatsverträge.

[204] Zum Zugriffsprinzip Ziff. 4.2.2.4. und zum Direktzugriff gemäss CCC Ziff. 4.2.5.

[205] Dazu SIEBER/NEUBERT, S. 246 und «Die Schweiz zapft Google und Apple an», Aargauer Zeitung vom 06.12.2017, S. 2.

[206] SR **0.351.933.6**

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Die Unternehmen haben die Möglichkeit, die Herausgabe von Daten im Rahmen ihrer Allgemeinen Geschäftsbedingungen (AGB) zu regeln. Diese sehen die Herausgabe jedoch meist nur gestützt auf eine richterliche Anordnung vor, welche in diesen Konstellationen vor den US-Gerichten eben nicht erwirkt werden kann. Eine freiwillige Herausgabe von Daten – auf der Grundlage einer direkten Anfrage seitens der schweizerischen Strafverfolgungsbehörde – hängt somit von der Kooperationsbereitschaft der Unternehmen ab. Insbesondere, wenn es viele Nutzer hat, ist diese Bereitschaft aus betriebswirtschaftlichen Gründen eingeschränkt: Die Bearbeitung einer grossen Menge von Anfragen bindet teure Ressourcen. Die freiwillige Herausgabe muss notabene die nationalen Gesetze zum Daten- und Persönlichkeitsschutz einhalten.

Bei anderen Delikten, z.B. Vermögensdelikten und Pornografie, können zwar gemäss RVUS rechtshilfeweise Zwangsmassnahmen angeordnet werden. Das massgebende US-Recht stellt jedoch hohe Anforderungen an Rechtshilfeersuchen. Die US-Behörden lehnen Ersuchen teilweise mit der Begründung ab, dass die Sachverhaltsdarstellung nicht den Anforderungen des US-Rechts entspreche. Aber nicht nur der Sachverhalt muss sehr präzise dargestellt sein, sondern auch der begründete Tatverdacht sowie der enge Bezug zwischen der strafbaren Handlung und den verlangten Daten.

Bei einem geringen Deliktsbetrag (Vorschussbetrug bei Ferienwohnungen, Kaufverträge über elektronische Geräte des täglichen Bedarfs etc.) werden Rechtshilfeersuchen aus Ressourcengründen ebenfalls oft nicht vollzogen.

Da auch die US-Strafverfolgungsbehörden selbst zunehmend mit Problemen im Bereich der grenzüberschreitenden Erhebung von Daten als Beweismittel im Rahmen von Strafverfahren konfrontiert waren,[207] erliess der US-amerikanische Gesetzgeber 2018 den Clarifying Lawful Overseas Use of Data Act (**CLOUD Act**). Dieser verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, den US-Strafverfolgungsbehörden im Rahmen von US-Strafverfahren Zugriff auf Daten zu gewähren, auch wenn diese im Ausland gespeichert sind. Dies gilt grundsätzlich auch dann, wenn die Daten bei ausländischen Tochtergesellschaften der US-Unternehmen liegen und unabhängig vom geltenden Recht am Lageort der Daten. Der CLOUD Act knüpft nicht am für das Strafrecht üblichen Kriterium der Territorialität an, sondern schlicht an der Frage der Zugriffsmöglichkeit: Wenn die US-Strafverfolgungsbehörde in den USA den Zugriff auf ein Datum erzwingen kann, soll der Dienstanbieter diesen Zugriff grundsätzlich vornehmen. Der Rechtsschutz richtet sich dabei ausschliesslich nach US-Recht. Der betroffene Dienstanbieter, also z.B. die Schweizer Tochter eines US-Dienstanbieters, kann sich nach US-Recht und vor dem zuständigen US-Gericht gegen die Herausgabe der Daten wehren, indem sie z.B. vorbringt, der Herausgabe stünde das Recht am Lageort der Daten entgegen. Schweizerisches Datenschutzrecht, schweizerische Grundrechte oder auch Berufs- oder Bankgeheimnisse werden damit zu Abwägungsgründen in einem US-amerikanischen Comity-Verfahren.[208]

Die USA bieten ausländischen Staaten, welche aus US-Sicht gewisse Standards im Bereich von Rechtsstaatlichkeit und Grundrechten erfüllen, den Abschluss eines sog. «executive agreement» gemäss Teil II des CLOUD Act an. Mit dem Abschluss eines solchen Agreements toleriert der Partnerstaat die US-Zugriffe auf Daten auf seinem Territorium, dafür erhalten seine Strafverfolgungsbehörden ebenfalls Zugriff auf Daten, die bei Dienstanbietern in den USA gespeichert sind. Ausführlich zu Chancen und Risiken des Abschlusses eines «executive agreements» vgl. Bericht des Bundesamtes für Justiz zum US CLOUD Act.[209]

---

[207] Vgl. United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

[208] Dazu DODGE, 2071 ff.

[209] Bericht BJ US CLOUD Act, Ziff. 5.6.

4.2.4.2 Rechtshilfeersuchen an europäische Staaten

Die Rechtshilfe zwischen der Schweiz und europäischen Staaten stützt sich grundsätzlich auf das Europäische Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen und dessen Zusatzprotokolle.[210] Dieses lässt den Vertragsstaaten die Möglichkeit, die Anordnung von Zwangsmassnahmen von der Voraussetzung der beidseitigen Strafbarkeit abhängig zu machen. Davon hat neben der Schweiz auch Irland – wie die Schweiz ein bedeutender europäischer Standort von Datenzentren – Gebrauch gemacht.

Ungeachtet der konkreten Ausgestaltung nationaler (z.B. irischer) Strafbestimmungen zur Ehrverletzung oder zu rassistischen Äusserungen, unterliegen diese Tathandlungen einer von lokalen gesellschaftlichen Vorstellungen geprägten Wertung von Freiheitsrechten; die Grenze bildet dabei das nationale (z.B. irische) Strafrecht. Posts oder Kommentare, welche in der Schweiz ehrverletzend oder diskriminierend beurteilt werden, fallen in anderen Ländern unter den Schutz der Meinungsäusserungsfreiheit. Diese unterschiedliche Wertung hat direkten Einfluss auf die Beurteilung der beidseitigen Strafbarkeit.

Diese Tatsache – verbunden mit der verbreiteten Qualifikation dieser Delikte als Bagatellen, bei denen sich eine aufwändige Strafverfolgung nicht lohnt – führt dazu, dass der rechtshilfeweise Zugriff auf Daten für schweizerische Strafverfolgungsbehörden auch innerhalb Europas teilweise nur eingeschränkt möglich ist.

Innerhalb der EU hat sich in den letzten Jahren ein System mit gegenseitiger Anerkennung von Justizentscheidungen durchgesetzt.[211] Die EU hat dabei eine Reihe von Instrumenten geschaffen, welche die Prüfung der beidseitigen Strafbarkeit erübrigen und auf gegenseitigem Vertrauen in die Justizsysteme beruhen (z.B. EU-Haftbefehl, EU-Ermittlungsanordnung). Im Unterschied zu den EFTA-Staaten Norwegen und Island beteiligt sich die Schweiz bislang nicht an diesen Zusammenarbeitsformen. Beruhend auf diesen Grundsätzen entwickelt die EU derzeit ihr System im Bereich des grenzüberschreitenden Zugriffs auf Daten als Beweismittel im Rahmen von Strafverfahren. Die sog. EU-E-Evidence-Vorlage befindet sich zurzeit im Trilog und soll noch im Jahr 2022 verabschiedet werden.[212] Die EU-Regelung zielt dabei nicht eigentlich auf «Drittstaaten» ab, sondern auf gegenseitige Zugriffsrechte zwischen den EU-Mitgliedstaaten. Jedoch ist es das erklärte Ziel der EU, auf Daten aller Dienstanbieter zugreifen zu können, welche auf dem EU-Binnenmarkt ihre Dienste anbieten. Gemäss den Entwürfen der Verordnung würde der Marktzugang an die Errichtung eines «legal seat» in der EU geknüpft. Mittels der neuen EU-Herausgabeanordnung könnten die Strafverfolgungsbehörden in den EU-Mitgliedstaaten sodann ihre Verfügungen fortan direkt an diesen «legal seat» auf EU-Gebiet richten. Das EU-E-Evidence-System hat voraussichtlich auch Auswirkungen auf Dienstanbieter aus der Schweiz, zumindest solange diese ihre Dienste auch an Kundinnen und Kunden in der EU richten.

4.2.4.3 Neue Rechtshilfeabkommen zur einfacheren Erhebung von Daten

Die Revision des RVUS ist bei Konsultationen zwischen den Rechtshilfebehörden der Schweiz und der USA regelmässig ein Thema. Die USA wären grundsätzlich daran interessiert, den RVUS zu revidieren, wie auch am Abschluss eines «executive agreement» unter dem CLOUD Act mit der Schweiz. Die Pflicht zur Speicherung von Vorratsdaten für Strafverfahren ist in der Schweiz und in den USA jedoch völlig unterschiedlich: In der Schweiz sind bestimmte Fernmeldedienstanbieterinnen (FDA) gemäss BÜPF verpflichtet, die Daten, welche eine Teilnehmeridentifikation erlauben, während mindestens sechs Monaten aufzubewahren. In den

---

[210] SR **0.351.1**

[211] Vgl. dazu z.B. das Factsheet des EU-Parlaments, www.europarl.europa.eu\factsheets > citizens > 4.2. An area of freedom, security and justice > 4.2.6. Judicial cooperation in criminal matters.

[212] Vgl. dazu die Informationen auf der Webseite der EU-Kommission, www.ec.europa.eu > Topics A-Z > Justice and fundamental rights > Policies > Criminal justice > E-evidence - cross-border access to electronic evidence.

USA gibt es jedoch keine entsprechende gesetzliche Aufbewahrungspflicht. Auch sind Standards und Verfahren im Bereich von Daten- und Rechtsschutz sehr unterschiedlich. Es ist somit herausfordernd, eine konsensfähige Lösung für direktere Zusammenarbreitsformen ausserhalb der souveränitäts- und territorialitätsorientierten Rechtshilfe zu finden, deren Verfahren zwar schwerfällig sein mögen, den Schutz hiesiger Rechtsprinzipien aber auch bei grenzüberschreitender Zusammenarbeit gewährleisten.

Auch in der EU kennen nicht alle Staaten eine dem BÜPF entsprechende Aufbewahrungspflicht. Ob und inwiefern ein Anschluss an das E-Evidence-System der EU für die Schweiz überhaupt eine Option wäre, hinge von den derzeit nicht bekannten Möglichkeiten und Interessen beider Parteien ab.

Da das EU-System im Unterschied zum CLOUD Act nicht auf extraterritoriale Zugriffe setzt, sondern im Gegenteil durch die (erzwungene) Anwesenheit des Dienstanbieters auf Herstellung der Territorialität abzielt, scheint es auf den ersten Blick besser vereinbar mit schweizerischen Prinzipien im Bereich des Daten- und Rechtsschutzes.

4.2.5 Direkter Zugriff auf Grund des Übereinkommens des Europarates über die Cyberkriminalität

Das CCC ist das *wichtigste internationale Übereinkommen im Bereich der Computer- und Netzwerkkriminalität*. Im ersten Teil verpflichtet es die Mitgliedstaaten, bestimmte Verhaltensweisen unter Strafe zu stellen.[213] Im zweiten Teil werden Regelungen für das Strafverfahren aufgestellt; dabei geht es vorrangig um Fragen der Beweiserhebung und Beweissicherung von elektronischen Daten. Der dritte Teil regelt die internationale Zusammenarbeit zwischen den Vertragsparteien. Diese soll im Interesse einer erfolgreichen Strafverfolgung schnell und effizient gestaltet werden, jedoch unter Wahrung rechtsstaatlicher Prinzipien.

Unter den 66 Vertragsstaaten[214] befinden sich neben der Schweiz fast alle Mitgliedstaaten des Europarates und Länder wie die USA, Kanada, Japan, Australien oder Israel – Länder, die für die gemeinsame Bekämpfung der Cyberkriminalität bedeutsam sind. Weitere Staaten haben ihr Interesse an einem Beitritt signalisiert.[215]

Das Übereinkommen regelt zwei Fälle, in denen die Vertragsstaaten grenzüberschreitend auf Computerdaten zugreifen dürfen, **ohne** dass eine **Rücksprache mit dem Staat**, in welchem sich die Daten befinden, erfolgen oder formell die internationale Rechtshilfe in Anspruch genommen werden muss:

- Zum einen den Fall, dass ein Vertragsstaat auf *öffentlich zugängliche Daten* zugreift.[216] Solche Daten, die von einem ausländischen Server abgerufen werden, dürfen – auch wenn eine Registrierung als Benutzer erforderlich ist – ohne Zustimmung des anderen Vertragsstaates verwendet werden.
- Zum anderen den Fall, dass ein Vertragsstaat auf *im Ausland gespeicherte Daten* zugreift und diese als *Beweismittel* verwendet, wenn er vorher die *rechtmässige und freiwillige Zustimmung* der Person einholt, welche befugt ist, die Daten (an eine Strafverfolgungsbehörde) weiter zu geben (Art. 32 Bst. b CCC). Ein solcher Fall liegt etwa vor, wenn eine Person ihren E-Mail-Account bei einem ausländischen Provider unterhält und sie diese Daten der inländischen Staatsanwaltschaft für Ermittlungs- oder Beweiszwecke zur Verfügung stellt.[217]

---

[213] U.a. Hacking, Computerbetrug und Kinderpornografie.

[214] Stand 01.06.2022.

[215] Weitere Informationen unter www.coe.int > Explore > Treaty Office > Full list > Convention on Cybercrime (ETS No. 185).

[216] Sog. open source data, siehe Art. 32 Bst. a CCC.

[217] Vgl. BBl **2010** 4697, 4737 f.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Das **2. Zusatzprotokoll** zum CCC bezweckt eine *verstärkte internationale Kooperation* im Bereich der Cyberkriminalität und einen *erleichterten und raschen Austausch von elektronischen Informationen und Beweismitteln* unter den Vertragsstaaten.

In der Zwischenzeit konnten die Arbeiten zur Ausarbeitung des 2. Zusatzprotokolls abgeschlossen werden. Die Auflage zur Unterzeichnung ist am 12. Mai 2022 erfolgt. Die Unterzeichnung durch einen Mitgliedstaat des Europarates (oder auch eine direkte Umsetzung des Inhalts mit Ratifikation) bleibt auch zu einem späteren Zeitpunkt stets möglich.

Das neue, noch nicht in Kraft getretene 2. Zusatzprotokoll wird durch die Schweiz vor einer Unterzeichnung in zahlreichen Punkten **vertieft evaluiert** werden. Es geht dabei vor allem darum, seine *Erfolgschancen* punkto breiter Umsetzung durch die Staatengemeinschaft, seinen *Mehrwert* in praktischer Hinsicht (insbesondere für die Strafverfolgungsbehörden) sowie die daraus resultierenden *Gefahren* (etwa für den Datenschutz und die staatliche Souveränität) zu eruieren. Zur Beurteilung dieser Fragen ist es wichtig, vorgängig Erfahrungen zu sammeln: *Inwieweit gewährleisten die zukünftigen Vertragsstaaten eine schnelle, aber regelkonforme und sichere Zusammenarbeit?*

Bei einer weitgehenden Umsetzung des 2. Zusatzprotokolls werden in der Hauptsache folgende grundlegenden **Gesetzesanpassungen** im schweizerischen Recht zu prüfen sein:

- Eine neue gesetzliche Bestimmung, gemäss welcher die Schweizer Strafverfolgungsbehörden für Auskünfte *direkt Ersuchen an Registerbetreiberinnen (von Domains) in einem anderen Vertragsstaat stellen können*.
- Eine Rechtsgrundlage, damit *schweizerische Registerbetreiberinnen (Domains) die ersuchten Auskünfte direkt an ausländische Behörden liefern dürfen.*
- Eine neue gesetzliche Bestimmung, gemäss welcher Schweizer Strafverfolgungsbehörden für Auskünfte betreffend Teilnehmerdaten (*subscriber information*) *direkt Ersuchen an Provider in einem anderen Vertragsstaat stellen können*.
- Eine Rechtsgrundlage, damit *schweizerische Provider die ersuchten Auskünfte betreffend Teilnehmerdaten (subscriber information) direkt an ausländische Behörden liefern dürfen.*

Ein **erhebliches Dilemma** besteht in jedem Fall: Diese Weiterentwicklung des Instrumentariums für eine verstärkte grenzüberschreitende Zusammenarbeit und Vertrauensbildung wird stets in einem *Widerspruch zur angestrebten Globalisierung der Cybercrime-Konvention* stehen. Der absehbare Verzicht auf nationale Garantien im Einzelfall kollidiert mit der Ausweitung des Geltungsbereiches des Vertrages auf Staaten, welche in der Praxis nicht für die Werte des Europarates (*insb. Datenschutz, fair trial, Einhaltung von strafprozessualen Garantien*) einstehen können oder wollen.

Die **heute bestehenden rechtlichen Möglichkeiten** des direkten grenzüberschreitenden Datenzugriffs durch Strafverfolgungsbehörden werden zurzeit als *unbefriedigend und nicht zeitgemäss* erachtet. Entsprechend werden **erhebliche Anstrengungen** unternommen, damit die internationale Zusammenarbeit den Herausforderungen der technologischen Entwicklung und des gesellschaftlichen Wandels entspricht und eine effiziente Strafverfolgung im Cyber-Bereich zulässt.

4.3 Strafrechtliche Verantwortlichkeit von Dienstanbietern

4.3.1 Strafbarer Ungehorsam und Rechtspflegedelikte

Personen, welche den Behörden die in einem Strafverfahren zu Beweiszwecken benötigten Daten trotz behördlicher Aufforderung vorenthalten, machen sich strafbar (Art. 265 Abs. 3 StPO).[218]

Wer eine strafprozessuale Mitwirkungspflicht verletzt,[219] kann wegen Ungehorsams gegen amtliche Verfügungen (Art. 292 StGB) bestraft werden. Für Personen, die Mitwirkungspflichten gemäss BÜPF haben,[220] gilt eine analoge Spezialbestimmung (Art. 39 Abs. 1 Bst. a BÜPF).[221]

Die Delikte im 17. Titel des StGB schützen die Rechtspflege vor ungerechtfertigten Einwirkungen. Wer jemanden der Strafverfolgung entzieht, wird wegen Begünstigung (Art. 305 StGB) mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Das Bundesgericht[222] hat die Strafbarkeit des Geschäftsführers eines Providers wegen Begünstigung bejaht: Durch das Löschen von IP-Adressen sei er seiner Auskunftspflicht (Art. 22 BÜPF) nicht nachgekommen. Er sei zudem verpflichtet gewesen, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren (Art. 26 Abs. 5 BÜPF). Auf welchen gesetzlichen Bestimmungen eine Aufbewahrungspflicht der IP-Adressen beruhe, erscheine letztlich unerheblich: Entscheidend sei, dass der Geschäftsführer die Benutzer seiner Website einer allfälligen Strafverfolgung entziehen wolle.

Befinden sich der beweisrelevante Gegenstand und sein Besitzer im Ausland, kann weder die Herausgabe, noch die Beschlagnahme, noch die Ahndung einer Pflichtverletzung direkt angeordnet oder durchgesetzt werden. Für solche Fälle kommt das IRSG zur Anwendung (Ziff. 4.2.4).

4.3.2 Gehilfenschaft des Dienstanbieters zur Haupttat eines Nutzers

Wer eine technische Infrastruktur zur Verfügung stellt, mit der die Nutzenden Straftaten begehen, kann nach der Rechtsprechung des Bundesgerichts grundsätzlich wegen Gehilfenschaft[223] zur Haupttat des Nutzers bestraft werden. Im konkreten Fall wurde der Generaldirektor der PTT wegen Gehilfenschaft zur Veröffentlichung von strafrechtlich verbotener Pornografie bestraft: Er stellte die technische Einrichtung zur Verfügung und wusste, dass damit konkrete Straftaten begangen wurden.[224]

Im Fall «Appel au peuple»[225] entschied das Obergericht des Kantons Waadt in einem nicht offiziell publizierten Entscheid vom 2. April 2003, der Zwang zur Sperrung des Zugangs zu einer Internetseite durch Access Provider sei strafprozessual unzulässig, weil dafür keine gesetzliche Grundlage besteht: Die Provider seien aber darüber zu informieren, dass sie sich der Gehilfenschaft zur Haupttat (i.c. Ehrverletzungsdelikte) strafbar machen könnten, falls sie die Sperrung nicht vornähmen.

Von Bedeutung sind in diesem Zusammenhang Regelwerke wie z.B. der Code of Conduct Hosting (CCH) der Interessenvertretung der ICT- und Internetbranche (swico).[226] Der CCH

---

[218] Die beschuldigte Person hat keine Mitwirkungspflicht (nemo tenetur-Grundsatz, Art. 113 StPO); auch Zeugnisverweigerungsrechte können eine Ausnahme begründen, vgl. Art. 264 f. StPO.

[219] Insb. Zeugnispflicht (Art. 163 Abs. 2 StPO) oder Herausgabepflicht (Art. 265 StPO).

[220] Insb. Fernmeldedienstanbieterinnen (FDA), aber auch Mail-Provider und Plattformbetreiber etc.

[221] Die fahrlässige Begehung ist hier ebenfalls strafbar (Art. 39 Abs. 3 BÜPF).

[222] Urteil des Bundesgerichts 6B_766/2009 vom 08.01.2010, E.3.

[223] Art. 25 StGB.

[224] BGE 121 IV 109, E. 3 („Telekiosk“).

[225] Dazu Urteil des Bundesgerichts 1B_242/2009 vom 21.10.2009.

[226] Abrufbar unter www.swico.ch > Wissen > Normen und Standards > Code of Conduct Hosting (CCH). Für Einzelheiten des CCH (vormals Simsa-Code) vgl. die Ausführungen in BBl **2018** 591, Ziff. 1.2.1.1.

ist eine freiwillige Selbstregulierungsmassnahme von schweizerischen Internetunternehmen, die im Bereich Data-Hosting tätig sind, und gibt eine Anleitung für den Umgang mit Hinweisen auf möglicherweise rechtswidrige Inhalte.[227] Er regelt ein Notice-and-Takedown-Verfahren, gibt aber keinen Anspruch auf Löschung des beanstandeten Inhalts.[228] Ein Provider, der den CCH einhält, ist strafrechtlich kaum zu belangen.

In Anwendung der vorstehend dargelegten Gerichtspraxis könnte somit gegen den CEO einer unkooperativen Social Media-Plattform im Ausland ein Strafverfahren wegen Gehilfenschaft zu einem Äusserungsdelikt eines Plattformnutzers oder einer Plattformnutzerin eröffnet werden. Voraussetzung wäre, dass der CEO Kenntnis hat, dass auf der Plattform seines Unternehmens bestimmte Delikte begangen werden, und dass er trotzdem nichts dagegen unternimmt. Die Rechtsverletzung gegen ein Schweizer Opfer kann strafrechtlich auch dann in der Schweiz abgeurteilt werden, wenn sich die beschuldigte Person im Ausland befindet und nicht zur Hauptverhandlung in der Schweiz erscheint (Abwesenheitsverfahren nach Art. 366 StPO). Die schweizerische Strafgerichtsbarkeit ergibt sich aus dem Individualschutzprinzip (passives Personalitätsprinzip).[229] Im Verfahren gegen den Teilnehmer einer Haupttat kann summarisch festgestellt werden, dass die Haupttat tatbestandsmässig und rechtswidrig begangen worden ist – sogar dann, wenn der Haupttäter (d.h. der Plattformnutzer) unbekannt ist.

4.3.3 Anwendbarkeit des Medienstrafrechts

Das Medienstrafrecht ist ein Sonderstrafrecht und stellt diejenigen Personen besser, die an der Publikation eines Medienerzeugnisses beteiligt sind. In Abweichung von den normalen Regeln ist hier immer nur der Autor oder die Autorin allein strafbar (Art. 28 Abs. 1 StGB). Dieses Privileg ist freilich auf typische Medieninhaltsdelikte beschränkt (Ehrverletzungen, Geheimnisverletzungen). Nach der Rechtsprechung des Bundesgerichts gelten bei Rassendiskriminierung, harter Pornografie und Gewaltdarstellungen die normalen Regeln (Gehilfenschaft, ev. auch Anstiftung und Mittäterschaft).[230]

Kann der Autor oder die Autorin nicht ermittelt oder in der Schweiz nicht vor Gericht gestellt werden, greift eine besondere strafrechtliche Kaskadenhaftung: Strafbar sind danach der Redaktor oder die Redaktorin und ersatzweise die für die Veröffentlichung verantwortliche Person (Publikator; Art. 28 Abs. 2 StGB). Bestraft werden sie freilich nicht wegen des Äusserungsdeliktes des Autors oder der Autorin, sondern wegen vorsätzlicher oder fahrlässiger Nichtverhinderung der strafbaren Veröffentlichung (Art. 322bis StGB).

Soziale Netzwerke wie Twitter oder Facebook können grundsätzlich zu Medien i.S.v. Artikel 28 Absatz 1 StGB gezählt werden.[231] Freilich ist nur die öffentliche Kommunikation auf Social Media-Plattformen vom Medienprivileg gedeckt, nicht aber die private.[232] Bei Netzwerken, bei denen die Privacy individuell und stufenweise festgelegt werden kann, fragt es sich, wo die private Kommunikation aufhört und wo die öffentliche beginnt.[233] Bei E-Mail-Anbietern ist das Medienstrafrecht mangels Veröffentlichung nicht anwendbar. Dasselbe dürfte für Plattformen zutreffen, die reine Speicherdienstleistungen erbringen, ohne dass die Informationen i.S.d. Medienstrafrechts veröffentlicht werden.

---

[227] Ziff. 1 CCH.

[228] Ziff. 7.1 CCH.

[229] POPP/KESHELAVA, BSK StGB I, Vor Art. 3 N 21.

[230] ZELLER, BSK StGB I, Art. 28 N 64 ff. (insb. N 68) m.w.H.; TRECHSEL/JEAN-RICHARD, PK StGB, Art. 28 N 7.

[231] Urteil GG150250 des Bezirksgerichts Zürich vom 26. Januar 2016, wiedergegeben in forum poenale 2017, 290 ff. (mit Anm. ROTH SIMON); vgl. auch ZELLER, BSK StGB I, Art. 28 N 96 ff. Ablehnend SCHWAIBOLD, 113 ff. Siehe weiter BGE 136 IV 145: Quellenschutz für Blog-Kommentar auf Internetseite des Schweizer Fernsehens bejaht.

[232] ZELLER, BSK I, Art. 28 N 49.

[233] Illustrativ BGE 141 IV 215 zur Schreckung der Bevölkerung (Art. 258 StGB) auf Facebook sowie BGE 126 IV 176 und 130 IV 111 zum Erfordernis der Öffentlichkeit bei der Rassendiskriminierung (Art. 261bis StGB).

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Wird ein Äusserungsdelikt über eine Social Media-Plattform begangen, kommt in Anwendung der Kaskadenhaftung eine Strafbarkeit des Plattformbetreibers in Frage. Vorausgesetzt ist, dass der Plattformbetreiber eine Überwachungspflicht und Verhinderungsmacht hat.[234] Lässt sich der Autor oder die Autorin einer Veröffentlichung auf einer Plattform nicht identifizieren – z.B. weil die Rechtshilfe verweigert wird – kann der Verantwortliche der Plattform nach den Regeln des Medienstrafrechts wegen vorsätzlicher oder fahrlässiger Nichtverhinderung einer strafbaren Veröffentlichung bestraft werden. Ein Abwesenheitsverfahren ist auch hier möglich (Art. 366 StPO).

4.4 Takedown und Sperren von rechtswidrigen Inhalten

4.4.1 Massnahmen auf strafrechtlicher Basis

Liegt ein rechtskräftiger Entscheid vor, müssen die rechtswidrigen Inhalte[235] im Internet entfernt werden. Dieser sog. Takedown von Daten in der Schweiz wird im Strafrecht auf die Regeln der Einziehung gestützt. Während die «harte Pornografie» und die Gewaltdarstellungen eine spezifische Grundlage für die Einziehung haben (Art. 197 Abs. 6 und Art. 135 Abs. 2 StGB), muss bei «weicher Pornografie» (Art. 197 Abs. 1 und 2 StGB), bei Rassendiskriminierung (Art. 261bis StGB) und bei Ehrverletzungsdelikten (Art. 173 ff. StGB) die Grundnorm von Artikel 69 StGB (Sicherungseinziehung) herangezogen werden. Der Wortlaut des Gesetzes beinhaltet jedoch nur «Gegenstände» und nennt «Daten» nicht ausdrücklich. Folglich gibt der strafrechtliche Datenbegriff Anlass zu Diskussionen und auch das Analogieverbot wirft Fragen hinsichtlich der Anwendbarkeit dieser Norm auf.[236]

Der Takedown ist schwierig oder sogar unmöglich, wenn der Hosting Provider seinen Sitz im Ausland hat und sowohl er als auch der Täter oder die Täterin die Kooperation verweigern. Es werden deshalb Sperrverfügungen an die Access Provider in der Schweiz erwogen, um Internet-Inhalte für das schweizerische Publikum zu sperren. Es gibt zwei Arten von *Zugangssperren*:

- Mittels *IP-Sperre* wird der Zugriff auf einen bestimmten Server gesperrt, indem der Access Provider den Weg zu diesem Server (bzw. zu dessen IP-Adresse) für seine Kunden löscht.
- Mittels *DNS-Sperre* blockiert der Access Provider die Zuordnung eines Domain Namens zur dazugehörigen IP-Adresse.[237]

Beide Massnahmen sind nur bedingt wirksam, da sie relativ leicht umgangen werden können. Vor allem bei der IP-Sperre besteht zudem die Gefahr des sog. Overblocking: Sämtliche unter derselben IP-Adresse erreichbaren Inhalte werden nämlich blockiert, nicht nur die rechtswidrigen.[238] Bei solchen Massnahmen ist deshalb die Frage der Verhältnismässigkeit von zentraler Bedeutung.[239] Im Bereich der Pornografie-Delikte des StGB wurde die freiwillige Sperrung am 1. Januar 2021 auf eine verpflichtende gesetzliche Grundlage gestellt (Art. 46*a* Abs. 2 des Fernmeldegesetzes vom 30.04.1997[240]).[241]

---

[234] TRECHSEL/JEAN-RICHARD, PK StGB, Art. 28 N 14.

[235] Z.B. Pornografie, Ehrverletzung oder Rassendiskriminierung.

[236] TRECHSEL/JEAN-RICHARD, PK StGB, Art. 69 N 1; eingehend BOMMER, 172 f. und 178 f. Zum Analogieverbot vgl. POPP/BERKEMEIER, BSK StGB I, Art. 1 N 31 ff., insb. N 42.

[237] Eine DNS-Sperre wirkt, als ob der Access Provider die zu einem Personennamen zugehörige Telefonnummer in *seinem* Exemplar des Telefonbuchs streichen würde. In anderen Exemplaren ist sie u.U. noch verfügbar.

[238] Dazu eingehend Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider, 46 f. und Urteil des Bundesgerichts 1B_294/2014 vom 19.3.2015, E. 4.5.

[239] Zu Funktion und Zulässigkeit der Sperre gem. Art. 86. Abs. 1 BGS siehe Urteil des Bundesgerichts 2C_336/2021 vom 18. Mai 2022 (zur Publikation vorgesehen), E. 7 und 8.

[240] **SR 784.10**

[241] Dazu BBl **2017** 6559 ff.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Das deutsche NDG (Ziff. 3.3.2) soll den Kampf gegen Hass und Hetze im Internet verbessern. Es begründet keine neuen Löschpflichten, die nicht schon nach bestehenden straf- oder zivilrechtlichen Vorschriften bestehen würden. Der Zweck dieses Erlasses besteht notabene ebenfalls primär im Takedown von Inhalten. Die Rechtmässigkeit der Inhalte wird freilich nicht vom Staat, sondern von den Unternehmen beurteilt. Ob die Strafverfolgung durch die Massnahmen des Netzwerkdurchsetzungsgesetzes gestärkt wird, scheint jedoch fraglich (vgl. auch Ziff. 3.3.2).

4.4.2 Privatrechtliche Instrumente

Gemäss Artikel 28 Absatz 1 ZGB kann, wer in seiner Persönlichkeit widerrechtlich verletzt wird, zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen. Der Kläger oder die Klägerin kann, wie oben dargelegt (Ziff. 3.1), unter anderem beantragen, eine bestehende Verletzung zu beseitigen (Beseitigungsklage nach Art. 28*a* Abs. 1 Ziff. 2 ZGB). Diese Regelung ist technologieneutral. Es ist deshalb denkbar, dass gestützt darauf sowohl das Löschen als auch das Sperren von rechtswidrigen Inhalten im Internet angeordnet wird. In Fällen, in denen der rechtsverletzende Nutzer oder die rechtsverletzende Nutzerin selbst nicht bekannt ist, kommt der Möglichkeit einer Klage gegen Mitwirkende grosses Gewicht zu. Der Bundesrat hat im Bericht «Die zivilrechtliche Verantwortlichkeit von Providern» vom 11. Dezember 2015 deshalb unter anderem die Möglichkeit von Beseitigungsklagen gegen verschiedene Internetakteure untersucht.

Im Bericht wurde dargelegt, dass der Kreis derjenigen, gegen die Beseitigungsansprüche grundsätzlich bejaht werden können, nicht uferlos sein kann. Selbst wenn für die Bejahung eines Beseitigungsanspruchs ein untergeordneter Tatbeitrag genügt, kann der Tatbeitrag nur rechtlich relevant sein, wenn er adäquat kausal ist.[242] Auch der Grundsatz der Verhältnismässigkeit ist stets zu beachten. Bei der Frage der zivilrechtlichen Verantwortlichkeit für Inhalte im Internet sollte nach Ansicht des Bundesrates das Kriterium der Inhaltsnähe des betreffenden Providers massgebend sein.[243] Um den Rechtsschutz der Betroffenen zu gewährleisten, ist es erwünscht, dass inhaltsnahe Anbieter wie die Betreiber von Social Media-Plattformen – unter Berücksichtigung des Grundsatzes der Verhältnismässigkeit – zur Beseitigung von rechtsverletzenden Inhalten angehalten werden können. Internetzugangsanbieter (Access Provider) haben dagegen keine Möglichkeit, von den transportierten, in aller Regel verschlüsselten Inhalten Kenntnis zu nehmen. Man kann von ihnen vernünftigerweise nicht verlangen, auf den Transport der gespeicherten Inhalte direkt Einfluss zu nehmen. Ansprüche gegen Access Provider dürften daher in der Regel schon mangels adäquat kausalen Tatbeitrags zu einer Rechtsverletzung ausscheiden.[244] Zu beachten ist auch, dass Access Provider den Zugang zu rechtsverletzenden Inhalten im Grunde – wie bereits erwähnt – nur mittels Sperren (IP- oder DNS-Blocking) verhindern können, wobei die Verhältnismässigkeit der technischen Massnahmen in jedem Einzelfall besonders sorgfältig zu prüfen ist (Ziff. 4.4.1).[245]

Schliesslich ist die Rechtsdurchsetzung im Ausland auch im Bereich des Privatrechts oftmals mit Schwierigkeiten verbunden. Im Rahmen der Erstellung des erwähnten Berichts wurde vertieft geprüft, ob es möglich wäre, bestimmte Provider zu verpflichten, ein Zustellungsdomizil in der Schweiz zu bezeichnen, um die zivilrechtliche Rechtsdurchsetzung ihnen gegenüber zu erleichtern. Der Bundesrat ist in diesem Bericht zum Schluss gekommen, die Frage eines Zustelldomizils im Zivilrecht vorerst nicht prioritär weiterzuverfolgen. Vielmehr sei der Abschluss von Rechtshilfeabkommen oder Vereinbarungen, welche die direkte postalische Zustellung

---

[242] Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider, Ziff. 3.2.2; vgl. zur Notwendigkeit eines Kausalzusammenhangs zwischen dem Verhalten des Mitwirkenden und der Persönlichkeitsverletzung auch BGE 141 III 513, E. 5.3, zur Relevanz des Tatbeitrags weiter Urteil des Bundesgerichts 5A_658/2014 vom 06.05.2015 E. 4.2.

[243] Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider, Ziff. 3.2.2 und 7.1.

[244] Vgl. zum Urheberrecht: BGE 145 III 72.

[245] Vgl. Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider, Ziff. 7.1.2.

von Schriftstücken in Zivilsachen vorsehen, voranzutreiben. Die Möglichkeit der direkten postalischen Zustellung besteht heute bereits bei einigen Staaten, in denen bekannte Plattformbetreiber ihren Rechtssitz haben.[246]

4.4.3 Freiwillige Massnahmen durch Internetunternehmen

Unternehmen wie Google, Facebook/Meta und Twitter bieten freiwillige Notice-and-Takedown-Verfahren an, damit man Rechtsverletzungen länderübergreifend melden, sperren[247] oder löschen lassen kann. Jedermann ist grundsätzlich berechtigt, entsprechende Hinweise zu machen, die zu einem Takedown führen können.

Hinweise von bestimmten Institutionen werden privilegiert behandelt. Bekannt ist etwa das Trusted Flagger-Programm von YouTube. Ein Trusted Flagger ist ein besonders vertrauenswürdiger Nutzer, auf dessen Hinweise und Warnungen das Unternehmen schneller reagiert als bei gewöhnlichen Nutzenden. Insbesondere Videos, in denen es um Terrorismus oder Dschihadismus geht, werden so rasch gelöscht. fedpol besitzt den Status eines Trusted Flaggers.[248]

4.5 Gesetzgebungsauftrag: Pflicht zur Bezeichnung von Zustelldomizilen

Die *Motion 18.3379 RK-S «Zugriff der Strafverfolgungsbehörden auf Daten im Ausland»* vom 23. März 2018 wurde vom Bundesrat zur Annahme empfohlen und vom Parlament überwiesen.[249] Der Titel der Motion ist irreführend bzw. unvollständig: Es geht um eine allgemeine Pflicht von Internetunternehmen, eine Zustellmöglichkeit zu schaffen. Die Motion verlangt u.a. die Schaffung einer gesetzlichen Grundlage, damit soziale Netzwerke verpflichtet werden können, eine Vertretung oder ein Zustellungsdomizil in der Schweiz zu bezeichnen. Dies soll die Kommunikation mit den Behörden sowie mit Konsumentinnen und Konsumenten vereinfachen. Wenn sich ein Unternehmen im Ausland weigert, eine Vertretung in der Schweiz zu bezeichnen, kann diese Pflicht jedoch nicht durchgesetzt werden, da die schweizerischen Behörden in einem fremden Staat keine Zwangsmittel anwenden dürfen.

Die *Motion 18.3306 Glättli «Rechtsdurchsetzung im Internet stärken durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen»* vom 15. März 2018[250] beauftragt den Bundesrat, die Rechtsdurchsetzung im Internet durch ein obligatorisches Zustellungsdomizil für grosse kommerzielle Internetplattformen zu stärken. Im Gegensatz zur heutigen Kann-Vorschrift in Artikel 140 ZPO sollen grosse kommerzielle Internetplattformen neu obligatorisch ein Zustellungsdomizil bezeichnen müssen. Auch in der StPO soll die Bezeichnung eines Zustellungsdomizils für grosse kommerzielle Internetplattformen obligatorisch sein. Auch diese Motion hat der Bundesrat zur Annahme empfohlen. Allerdings hatte die zuständige Justizministerin schon bei der Debatte im Rat darauf hingewiesen, dass der Bundesrat die Motion in dem Sinne entgegennehme, dass zusammen mit der Motion 18.3379 nach Lösungen gesucht werde, die tatsächlich auch umsetzbar seien und auch eine Wirkung zeigten.[251]

4.5.1 Stand der Umsetzung

Bei den vom Parlament Ende September 2020 abgeschlossenen Beratungen zur Revision des DSG hat das Parlament eine neue Regelung eingefügt, wonach private Datenbearbeiter mit Sitz im Ausland verpflichtet sind, eine Vertretung in der Schweiz zu bezeichnen, wenn sie Per-

---

[246] USA, Irland, vgl. Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider, Ziff. 6.2.4.

[247] Im Sinne von Geo-Blocking (Sperrung von Inhalten für bestimmte Regionen).

[248] Bericht BAKOM Intermediäre und Kommunikationsplattformen, Ziff. 10.2.2; BÜHLER STEFAN, So stoppt der Bund Jihad-Videos, NZZ am Sonntag vom 14. August 2016.

[249] www.parlament.ch > Geschäft 18.3379

[250] www.parlament.ch > Geschäft 18.3306

[251] AB **2018** N 1400.

sonendaten von Personen in der Schweiz bearbeiten und sie weitere Voraussetzungen erfüllen (Art. 14 nDSG). Diese Vertretung hat bestimmte Pflichten (Art. 15 nDSG). Diese Regelung überschneidet sich mit den Anliegen der Motionen 18.3306 und 18.3379.

Private Datenbearbeiter, die Personen in der Schweiz Waren oder Dienstleitungen anbieten oder das Verhalten von Personen in der Schweiz beobachten (z.B. Targeting von Kunden), werden mit Artikel 14 nDSG verpflichtet, eine Vertretung in der Schweiz zu bezeichnen, wenn die Datenbearbeitung umfangreich[252] ist und regelmässig[253] stattfindet sowie ein hohes Risiko für die Persönlichkeit der betroffenen Person mit sich bringt[254]. Davon betroffen sind voraussichtlich insbesondere grosse Internetplattformen und soziale Netzwerke. Dabei soll die Vertretung als Ansprechpartner für den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und die betroffenen Personen in der Schweiz dienen (Art. 14 Abs. 2 nDSG).

Der ausländische Datenbearbeiter muss den Namen und die Adresse seiner Vertretung veröffentlichen (Art. 14 Abs. 3 nDSG). Gemäss Artikel 15 nDSG hat diese Vertretung drei Pflichten: Erstens führt sie ein Verzeichnis der Bearbeitungstätigkeiten, zweitens gibt sie dem EDÖB auf Anfrage Einsicht in das Verzeichnis[255] und drittens erteilt sie betroffenen Personen Auskünfte darüber, wie diese ihre Rechte ausüben können.

Der EDÖB kann einen ausländischen Datenbearbeiter, der die Voraussetzungen von Artikel 14 nDSG erfüllt, mittels Verfügung dazu verpflichten, eine Vertretung in der Schweiz zu bezeichnen (Art. 51 Abs. 4 nDSG). Da es sich dabei um ein amtliches Dokument handelt, muss die Verfügung des EDÖB allerdings auf diplomatischem Weg zugestellt werden (ausser, ein internationales Abkommen würde die direkte Zustellung vorsehen). Der EDÖB kann dem ausländischen Datenbearbeiter zusammen mit seiner Anordnung auch eine Strafe wegen Missachtung von Verfügungen androhen (Art. 63 nDSG). Wird dieser gestützt darauf zu einer Busse verurteilt, kann diese grundsätzlich nur rechtshilfeweise vollstreckt werden bzw. muss auf diplomatischem Weg um Hilfe bei der Vollstreckung der Busse ersucht werden.

4.6 Fazit

Bei Äusserungsdelikten auf Internetplattformen operiert die Täterschaft oft anonym, und die Identifikation der Täterschaft ist diesfalls nur über Beweiserhebungen im Ausland möglich.

Wegen der Territorialität der Gesetze und dem völkerrechtlichen Souveränitätsprinzip dürfen schweizerische Strafverfolgungsbehörden solche Beweise nur ganz ausnahmsweise direkt erheben. In solchen Fällen kann das schweizerische Strafrecht deshalb regelmässig nur mit grossem Aufwand (über die internationale Rechtshilfe in Strafsachen) und oft auch gar nicht durchgesetzt werden (so z.B., wenn es am Erfordernis der gegenseitigen Strafbarkeit mangelt). Neue materielle Bestimmungen ändern nichts an diesem Manko und können falsche Erwartungen wecken.

Auch unilaterale Massnahmen sind nur beschränkt wirksam: Die grenzüberschreitende Beweiserhebung ist vorzugsweise mit völkerrechtlichen Verträgen zu verbessern.

---

[252] Die Datenbearbeitung muss mit anderen Worten eine grosse Zahl von Personen in der Schweiz oder einen grossen Bestand von Personendaten betreffen.

[253] Diese Voraussetzung dürfte z.B. im Bereich des Online-Handels erfüllt sein. Auch wenn Personendaten sozusagen den «Rohstoff» einer Tätigkeit bilden – wie z.B. für soziale Netzwerke – liegt eine regelmässige Datenbearbeitung vor. Keine regelmässige Datenbearbeitung ist es dagegen, wenn die Daten nur während einer beschränkten Zeitdauer oder nur gelegentlich bearbeitet werden.

[254] Ob eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich bringt, ist jeweils im Einzelfall zu prüfen. Das hohe Risiko kann sich insbesondere aus der Menge und der Art der bearbeiteten Daten (namentlich bei besonders schützenswerten Personendaten), dem Zweck der Datenbearbeitung, der Art und Weise der Datenbearbeitung (z.B. beim Einsatz neuer Technologien), einer allfälligen Datenbekanntgabe ins Ausland sowie der Zugriffsberechtigung auf die Daten (z.B. bei Zugriffen durch eine grosse oder gar unbegrenzte Anzahl Personen) ergeben.

[255] Um das Souveränitätsprinzip zu respektieren, darf der EDÖB die Vertretung nicht um Angaben oder Personendaten ersuchen, die im Ausland gespeichert sind. Solche Informationen dürfen nur über die internationale Rechtshilfe beschafft werden.

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Das Entfernenlassen von ehrenrührigen Posts auf Internetplattformen soll für die betroffenen Personen jedoch leichter werden: Die Regelung im künftigen DSG, wonach private Datenbearbeiter mit Sitz im Ausland eine *Vertretung in der Schweiz* zu bezeichnen haben, wenn sie Personendaten von Personen in der Schweiz bearbeiten und gewisse andere Voraussetzungen erfüllen (Art. 14 f. nDSG), soll es ermöglichen, direkt mit den Betreibern von Internetplattformen in Kontakt zu treten. Somit kann eine betroffene Person direkt beim Betreiber verlangen, dass z.B. ein ehrenrühriger Post entfernt wird. Allein damit besteht freilich noch kein Anspruch auf Löschung, der auch international durchgesetzt werden könnte.

Es ist zudem darauf hinzuweisen, dass der Bundesrat nun den konkreten Handlungsbedarf im Bereich der Rechtsdurchsetzung im Zusammenhang mit dem Postulat 21.3450 SIK-S «Hassreden. Bestehen gesetzliche Lücken?» und dem Aussprachepapier zur Regulierung von Kommunikationsplattformen untersucht. Während Letzteres nach aktuellem Stand Ende 2022 vorliegen wird, kann der Postulatsbericht voraussichtlich im 2. Quartal 2023 verabschiedet werden.

5 Ergebnis

5.1 Materielles Recht

Aufgrund der vorangehenden Ausführungen ist ein *Handlungsbedarf im materiellen Recht* zu verneinen:

Cybermobbing – d.h. vorsätzlich begangenes, einschüchterndes, belästigendes oder blossstellendes Verhalten unter Nutzung von IKT, das aus wiederholten Einzelakten über einen längeren Zeitraum besteht und dazu führt, dass sich die betroffene Person beleidigt, schikaniert, gequält oder herabgesetzt fühlt – kann nach geltendem Strafrecht aufgrund verschiedener Tatbestände verfolgt und bestraft werden. Dies grundsätzlich auch, wenn die einzelnen Handlungen aufgrund ihres isoliert gesehen geringen Unrechtsgehalts die Schwelle der geltenden Tatbestände nicht erreichen, das Verhalten in seiner Gesamtheit aber beleidigend, schikanierend, quälend oder herabsetzend auf die betroffene Person wirkt: Hier könnte allenfalls eine Übernahme der Rechtsprechung zur Nötigung betreffend Stalking (Art. 181 StGB)[256] und zum Missbrauch einer Fernmeldeanlage (Art. 179^{septies} StGB)[257] durch das Bundesgericht dazu führen, das Verhalten in seiner Gesamtheit zu würdigen und entsprechend bestrafen zu können. Damit böte das geltende Recht insgesamt bereits einen Rahmen, um auf Cybermobbing strafrechtlich angemessen reagieren zu können.

Wollte man dennoch einen *spezifischen Tatbestand* einführen, müsste dieser nach Auffassung des Bundesrates *technologieneutral* ausgestaltet sein. Denn es ist zu beachten, dass gravierende Formen des Mobbings auch in der *realen Welt* vorkommen. Einen spezifischen Tatbestand nur für die Cybervariante des Mobbings zu schaffen und letztere weiterhin durch die jeweils in concreto erfüllten Tatbestände zu bestrafen, liesse sich sachlich nicht begründen. Zudem gibt es auch Mischformen: In ein und demselben Mobbingfall können bestimmte Einzelakte online und andere offline begangen werden. Bei einem spezifischen Cybermobbing-Tatbestand wäre es für die Praxis schwierig, mit solchen Fällen umzugehen. Wie ein Blick auf die Regelung anderer Länder zeigt, kennt denn auch *einzig das österreichische Strafrecht* einen speziellen Tatbestand zum Cybermobbing.

Es ist zu beachten, dass die *Erwartungen an einen solchen Tatbestand nicht allzu hoch gesteckt werden dürfen*. Angesichts der Vielfalt möglicher Mobbing-Handlungen (sog. *Heterogenität der Verhaltensweisen*) wäre es schwierig, eine Formulierung zu finden, die vor dem *Bestimmtheitsgebot* standhält und in der Praxis zu handhaben ist. Auch wäre von einem solchen Tatbestand *nur schwerlich eine Erleichterung der Beweissituation* zu erwarten. Denn auch

[256] BGE 129 IV 262, 265 ff.; 141 IV 437, 441.

[257] Urteil des Bundesgerichts 6B_75/2009 vom 02.06.2009, E. 3.2.1; BGE 126 IV 219.

die wiederholten Einzelakte, die ein solcher Tatbestand zwingend voraussetzen müsste, müssten je einzeln bewiesen werden, auch betreffend subjektivem Tatbestand. Gerade Tatbestandselemente, die einen grossen Interpretationsspielraum lassen – und insofern mit Blick auf das Bestimmtheitsgebot heikel sind – sind oftmals nur schwer zu beweisen. Auch darf man von der *negativen Generalprävention* bzw. abschreckenden Wirkung eines solchen Tatbestandes nicht viel erwarten, scheint doch entscheidend, ob ein Verhalten überhaupt strafrechtlich geahndet wird (gestützt auf die geltenden Tatbestände oder einen spezifischen Mobbing-Tatbestand). Die Lehre spricht sich denn auch grundsätzlich gegen einen solchen Tatbestand aus.[258]

Bei der übrigen *«digitalen Gewalt»* bzw. übrigen *digitalen Angriffen gegen die Persönlichkeit* lässt sich lediglich strafloses Verhalten ausmachen, was die *Weiterverbreitung peinlicher, verfälschter oder freizügiger Bild- oder Videoaufnahmen* betrifft: Nach geltendem Recht ist dies dann nicht strafbar, wenn es sich *nicht um pornografisches Material* handelt (Art. 197 StGB), aus den Umständen *kein Vorwurf der Ehrenrührigkeit* hervorgeht (Art. 173 ff. StGB) und es sich *nicht um ohne Einwilligung der betroffenen Person aufgenommene Tatsachen aus dem Geheimbereich* handelt oder um Tatsachen aus dem *Privatbereich, die nicht jedermann zugänglich sind* (Art. 179^{quater} Abs. 3 StGB). Solches Verhalten könnte – soweit es als strafwürdig erachtet wird und die zivilrechtlichen Möglichkeiten des Persönlichkeitsschutzes als ungenügend angesehen werden – für strafbar erklärt werden. Dies könnte mittels eines (technologieneutralen) spezifischen Tatbestandes oder auch als Tatvariante eines Mobbing-Tatbestandes erfolgen. Im Gegensatz zum Tatbestand, welcher der Ständerat im Rahmen der *Revision des Sexualstrafrechts* vorschlägt (Unbefugtes Weiterleiten von nicht öffentlichen sexuellen Inhalten, Art. 197*a* E-StGB) sollte ein allfälliger neuer Tatbestand *nicht auf sexuelle Inhalte beschränkt* sein, sondern *auch anderweitig kompromittierende Aufnahmen* erfassen. Er sollte entsprechend auch nicht unter den strafbaren Handlungen gegen die sexuelle Integrität eingeordnet werden, sondern bei jenen gegen die Ehre und den Geheim- oder Privatbereich (Dritter Titel des zweiten Buches).

5.2 Rechtsdurchsetzung

Es darf nicht vergessen gehen, dass die geltenden materiellen Straftatbestände bzw. auch die Einführung neuer, spezifischer Tatbestände keine Wirkung entfalten können, wenn sich das Strafrecht nicht durchsetzen lässt. Die *Rechtsdurchsetzung bei über IKT begangenen Straftaten ist schwierig und oft sogar unmöglich:* Bei Äusserungsdelikten auf Internetplattformen operiert die *Täterschaft oft anonym*. Für die Identifikation der Täterschaft und auch den Nachweis anderer Sachverhaltselemente sind die Strafverfolgungsbehörden *auf Daten als Beweismittel angewiesen, die oft im Ausland gespeichert sind*. Die Beweissicherung ist somit technisch und rechtlich anspruchsvoll.

Ein wichtiger Schritt zur Verbesserung der Situation ist hier bereits mit der *Regelung im künftigen DSG* erfolgt, wonach private Datenbearbeiter mit Sitz im Ausland eine *Vertretung in der Schweiz* zu bezeichnen haben, wenn sie Personendaten von Personen in der Schweiz bearbeiten und gewisse andere Voraussetzungen erfüllen (Art. 14 f. nDSG). Damit soll die einfache Kontaktaufnahme mit Betreibern von Internetplattformen ermöglicht werden, um beispielsweise das Entfernen von ehrenrührigen Inhalten zu verlangen.

Der Bundesrat untersucht zudem den konkreten Handlungsbedarf im Bereich der Rechtsdurchsetzung weiter im Zusammenhang mit dem *Postulat 21.3450 SIK-S «Hassreden. Bestehen gesetzliche Lücken?»* und dem *Aussprachepapier zur Regulierung von Kommunikationsplattformen*. Somit besteht auch bezüglich der Problematik der Rechtsdurchsetzung zurzeit kein Handlungsbedarf; die Arbeiten zur Untersuchung und Verbesserung der Situation sind bereits im Gange.

---

[258] WENK schlägt jedoch punktuelle Änderungen vor. So könnten nach seiner Auffassung beispielsweise die Ehrverletzungsdelikte durch einen Absatz ergänzt werden, der eine höhere Strafdrohung aufnimmt für den Fall, dass die Tat durch IKT begangen wurde und dadurch für eine grössere Anzahl von Menschen wahrnehmbar war: WENK, 95.

6 Literatur- und Materialienverzeichnis

Literatur

AEPLI MICHAEL, Die Sicherstellung von elektronisch gespeicherten Daten, Zürich/Basel/Genf 2004 (zit. AEPLI)

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht: unter vergleichender Berücksichtigung der StPO, Zürich 2014 (zit. BANGERTER)

BAUER SEBASTIAN, Soziale Netzwerke und strafprozessuale Ermittlungen, Berlin 2018 (zit. BAUER)

BOMMER FELIX, Löschung als Einziehung von Daten, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, 172 f. und 178 f. (zit. BOMMER)

BOMMER FELIX/GOLDSCHMID PETER, in: NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196–457 StPO, 2. Aufl., Basel 2014, Art. 263 StPO (zit: BOMMER/GOLDSCHMID, BSK StPO II, Art. 263)

BRUN MARCEL, Cyberbullying – aus strafrechtlicher Sicht, recht 2016 S. 100 ff. (zit. BRUN)

CAMPBELL MARILYN/BAUMAN SHERI, Cyberbullying: Definition, consequences, prevalence, in: Reducing Cyberbullying in Schools, 2018, 3 ff. (zit. CAMPBELL/BAUMAN)

DELNON VERA/RÜDY BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 180 StGB (zit. DELNON/RÜDY, BSK II StGB, Art. 180)

DELNON VERA/RÜDY BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 181 StGB (zit. DELNON/RÜDY, BSK II StGB, Art. 181)

DODGE WILLIAM S., International Comity in American Law, in: Columbia Law Review, Vol. 115, No. 8, 2071 ff.

DONATSCH ANDREAS, Strafrecht III, 11. Aufl., Zürich 2018 (zit. DONATSCH)

FRASCH DENNIS, Cybermobbing ohne Konsequenzen – warum Straftäter der Justiz oft entkommen, www.watson.ch > Digital (zit. FRASCH)

GRAF DAMIAN K., Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, in: Jusletter IT vom 21. September 2017 (zit. GRAF)

HANSJAKOB THOMAS, Was ist GovWare?, Jusletter vom 11. September 2017 (zit. HANSJAKOB)

HANSJAKOB THOMAS, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16. Dezember 2016, in forum poenale 2017, 252 ff. (zit. HANSJAKOB BGer 6B_656/2015)

HUSMANN MARKUS, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht II, Art. 137–392 StGB, 4. Aufl., Basel 2019, Art. 271 StGB (zit. HUSMANN, BSK StGB II, Art. 271)

IHWAS SALEH RAMADAN, Strafverfolgung in sozialen Netzwerken, Baden-Baden 2014 (zit. IHWAS)

ISENRING BERNHARD, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht II, Art. 137–392 StGB, 4. Aufl., Basel 2019, Art. 198 StGB (zit: ISENRING, BSK StGB II, Art. 198)

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

KINZIG JÖRG, Die Strafbarkeit von Stalking in Deutschland – Vorbild für die Schweiz?, in: recht 2011, 1 ff. (zit. KINZIG)

KUNZ HAENNES, ZEPRA Prävention und Gesundheitsförderung, Mobbing in der Schule, St. Gallen 2016, in: Sicher! Gsund!, abrufbar unter www.sichergsund.ch > Themen > Mobbing in der Schule (zit. KUNZ)

POPP PETER/BERKEMEIER ANNE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 1 StGB (zit. POPP/BERKEMEIER, BSK StGB I, Art. 1)

POPP PETER/KESHELAVA TORNIKE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Vor Art. 3 StGB (zit. POPP/KESHELAVA, BSK StGB I, Vor Art. 3)

PREUSS TAMINA, Erforderlichkeit der Kriminalisierung des Cybermobbings – Sinnvolle Schliessung einer Gesetzeslücke oder blosses Symbolstrafrecht?, KriPoZ 2/2019, 97 ff. (zit. PREUSS)

RAMEL RAFFAEL/VOGELSANG ANDRÉ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 179^{septies} StGB (zit. RAMEL/VOGELSANG, BSK II StGB, Art. 179^{septies})

RIKLIN FRANZ, Der Straf- und zivilrechtliche Ehrenschutz im Vergleich, ZStrR 1983, 29 ff. (zit. RIKLIN)

RIKLIN FRANZ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Vor Art. 173 StGB (zit. RIKLIN, BSK II StGB, Vor Art. 173)

RIKLIN FRANZ, NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 177 StGB (zit. RIKLIN, BSK II StGB, Art. 177 StGB)

SELMAN/SIMMLER, Shitstorm – strafrechliche Dimension eines neuen Phänomens, ZStrR 136 (2018), 228 ff. (zit. SELMAN/SIMMLER)

SALMINA EDY, Der Preis der Ehre, forumpoenale 3/2020, S. 215 ff. (zit. SELMINA)

SCHMID NIKLAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im Allgemeinen, Schweizerische Zeitschrift für Strafrecht (ZStrR) 1993, S. 81 ff. (zit. SCHMID)

SCHWAIBOLD MATTHIAS, Warum «Twitter» kein Medium im Sinne des Strafrechts ist, sui generis 2017, S. 113 ff. (zit. SCHWAIBOLD)

SIEBER ULRICH/NEUBERT CARL-WENDELIN, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty, in: LACHENMANN FRAUKE/RÖDER TILLMANN/WOLFRUM RÜDIGER (Hrsg), Max Planck Yearbook of United Nations Law, Volume 20 (2016), Leiden/Boston 2017, S. 249 ff. (zit. SIEBER/NEUBERT)

SMAHEL DAVID/MACHACKOVA HANA/MASCHERONI GIOVANNA/DEDKOVA LENKA/STAKSRUD ELISABETH/ÓLAFSSON KJARTAN/LIVINGSTONE SONIA/HASEBRINK UWE, 2020, EU Kids Online 2020, Survey results from 19 countries, 2020, unter: www.eukidsonline.ch > Internationaler Ergebnisbericht (zit. SMAHEL/MACHACKOVA/MASCHERONI/DEDKOVA/STAKSRUD/ÓLAFSSON/LIVINGSTONE/HASEBRINK)

STRATENWERTH GÜNTER, Schweizerisches Strafrecht, Allgemeiner Teil I: Die Straftat, 4. Aufl., Bern 2011 (zit. STRATENWERTH, AT I)

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022 (zit. STRATENWERTH/BOMMER, BT I)

STRATENWERTH GÜNTER/BOMMER FELIX, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7. Aufl., Bern 2013 (zit. STRATENWERTH/JENNY/BOMMER, BT II)

THORMANN OLIVIER/BRECHBÜHL BEAT, in: NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196–457 StPO, 2. Aufl., Basel 2014, Art. 248 (zit.THORMANN/BRECHBÜHL, BSK StPO II)

TRECHSEL STEFAN/JEAN-RICHARD-DIT-BRESSEL MARC, Praxiskommentar Schweizerisches Strafgesetzbuch, Zürich/St. Gallen 2018, Art. 28 StGB (zit. TRECHSEL/JEAN-RICHARD, PK StGB, Art. 28)

TRECHSEL STEFAN/LEHMKUHL MARIANNE JOHANNA in: TRECHSEL STEFAN/PIETH MARK (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. Aufl., Zürich/St. Gallen 2021, Vor Art. 173 StGB (zit. TRECHSEL/LEHMKUHL, PK StGB, Vor Art. 173)

TRECHSEL STEFAN/MONA MARTINO, in: TRECHSEL STEFAN/PIETH MARK (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. Aufl., Zürich/St. Gallen 2021, Art. 181 StGB (zit. TRECHSEL/MONA, PK StGB, Art. 181)

WEISSENBERGER PHILIPPE, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 156 StGB (zit. WEISSENBERGER, BSK II, Art. 156)

WENK JAN, #opfer, Bedarf es eines Cybermobbing-Tatbestands?, recht 2021, 88 ff. (zit. WENK)

WICKER MAGDA, Cloud Computing und staatlicher Strafanspruch, Baden-Baden 2016 (zit. WICKER)

ZELLER FRANZ, in: NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht I, Art. 1–136 StGB, 4. Aufl., Basel 2019, Art. 28 StGB (zit. Zeller, BSK StGB I, Art. 28)

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Materialien

Schutz vor Cyberbullying, Bericht des Bundesrates vom 26. Mai 2010 in Erfüllung des Postulats Postulat Schmid-Federer 08.3050, www.fedpol.admin.ch > Aktuell > Cyberbullying (zit. *Postulatsbericht Cyberbullying*)

BBl **2010** 4697, Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010

BBl **2013** 2683, Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013

Bericht des Bundesrates «Rechtliche Basis für Social Media» vom 09. Oktober 2013 in Erfüllung des Postulats Amherd 11.3912 «Rechtliche Basis für Social Media» vom 29 September 2011, www.bakom.admin.ch > Digitalisierung und Internet > Digitale Kommunikation > Intermediäre und Kommunikationsplattformen > Rechtliche Basis für Social Media (zit. *Postulatsbericht Social Media 2013*)

Die zivilrechtliche Verantwortlichkeit von Providern, Bericht des Bundesrates vom 11. Dezember 2015, www.bj.admin.ch > Publikationen & Service > Berichte, Gutachten und Verfügungen > Berichte und Gutachten > Zivilrechtliche Verantwortlichkeit von Providern (zit. *Bundesratsbericht zivilrechtliche Verantwortlichkeit Provider*)

BBl **2017** 185, Botschaft zur Genehmigung des Übereinkommens des Europarats zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vom 2. Dezember 2016

Nachfolgebericht des Bundesrates vom 10. Mai 2017 zum Postulatsbericht Rechtliche Basis für Social Media: Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011, www.bakom.admin.ch > Digitalisierung und Internet > Digitale Kommunikation > Intermediäre und Kommunikationsplattformen > Rechtliche Basis für Social Media (zit. *Nachfolgebericht Social Media 2017*)

BBl **2017** 6559, Botschaft zur Revision des Fernmeldegesetzes vom 6. September 2017

BBl **2017** 6941, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017

BBl **2017** 7307, Botschaft zum Bundesgesetz über die Verbesserung des Schutzes gewaltbetroffener Personen vom 11. Oktober 2017

BBl **2018** 591, Botschaft vom 22. November 2017 zur Änderung des Urheberrechtsgesetzes sowie zur Genehmigung zweier Abkommen der Weltorganisation für geistiges Eigentum und zu deren Umsetzung

BBl **2018** 2827, Botschaft zur Harmonisierung der Strafrahmen und zur Anpassung des Nebenstrafrechts an das geänderte Sanktionenrecht vom 25. April 2018

Bericht des Bundesamtes für Justiz zur Frage der Kodifizierung eines Straftatbestands «Stalking» vom 12. April 2019, www.parlament.ch > Geschäft 19.433 (zit. *Bericht BJ Stalking*)

BBl **2020** 7639, Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) vom 25. September 2020

Bundesgesetz zu einer Revision des Sexualstrafrechts, Bericht über das Ergebnis des Vernehmlassungsverfahrens vom 8. August 2021, www.parlament.ch > Geschäft 18.043 > Vernehmlassung zu Entwurf 3 > Vernehmlassungsergebnisse (zit. *Vernehmlassungsbericht Sexualstrafrecht*)

Ergänzungen betreffend Cybermobbing im Strafgesetzbuch

Bericht des Bundesamtes für Justiz zum US CLOUD Act vom 17. September 2021, www.bj.admin.ch > Publikationen & Service > Berichte und Gutachten und Verfügungen > Berichte und Gutachten (zit. *Bericht BJ US CLOUD Act*)

Bericht des Bundesamtes für Kommunikation Intermediäre und Kommunikationsplattformen, Auswirkungen auf die öffentliche Kommunikation und Ansätze einer Governance, vom 17. November 2021, www.bakom.admin.ch > Digitalisierung und Internet > Digitale Kommunikation > Intermediäre und Kommunikationsplattformen (zit. *Bericht BAKOM Intermediäre und Kommunikationsplattformen*)

BBl **2021** 2997, Bundesgesetz vom 17. Dezember 2021 über die Harmonisierung der Strafrahmen

BBl **2022** 687, Bundesgesetz über eine Revision. des Sexualstrafrechts. Bericht der Kommission für Rechtsfragen des Ständerates vom 17. Februar 2022

BBl **2022** 1011, Strafrahmenharmonisierung und Anpassung des Nebenstrafrechts an das neue Sanktionenrecht, Vorlage 3: Bundesgesetz über eine Revision des Sexualstrafrechts, Bericht der Kommission für Rechtsfragen des Ständerates vom 17. Februar 2022, Stellungnahme des Bundesrates vom 13. April 2022