

Liliane Mollet, Jens Klopp, Thomas Walther

Cyberkriminalität: Bekämpfung von Kinderpornografie

Neue technische Möglichkeiten sollen polizeiliche Ermittlungen erleichtern

Polizeiliche Ermittlungen im Bereich der Kinderpornografie sind für die zuständigen Beamten meist äußerst belastend. Zusätzlich stellen der unaufhaltsame technische Fortschritt, die zunehmende internationale Verflechtung sowie die steigende Anzahl Bilder und Filme immer neue Herausforderungen an effiziente polizeiliche Ermittlungen. Mit der Nationalen Datei- und Hashwertesammlung (NDHS) hat die Schweizerische Koordinationsstelle KOBİK einen Lösungsansatz gefunden, welcher die kantonalen IT-Ermittler maßgeblich bei der Bekämpfung von Kinderpornografie unterstützen wird.

1 Einleitung

Die hochentwickelte Infrastruktur, die weite Verbreitung der Internetnutzung¹ sowie der in zunehmendem Masse internetgestützte Handel und die entsprechenden Zahlungssysteme bieten in der Europäischen Union wie in der Schweiz einen teils äußerst lukrativen Nährboden für Cyberkriminalität². Mit einem Klick können nicht nur Landesgrenzen, sondern auch ethische wie moralische Grenzen überschritten werden, die viele Internetnutzende im „realen Leben“, wo die Anonymität des Internets³ keinen Schutz bietet, niemals überschreiten würden.

Mit der Evolution des Internets steigen auch die Anforderungen an die internationale Gemeinschaft, im Internet verübte Delikte über Landesgrenzen hinweg effizient zu bekämpfen⁴. Unterschiedliche Rechtsordnungen und -auffassungen sowie die aufgrund technischer wie wirtschaftlicher Globalisierung schwindende Durchsetzungsmacht stellen die Staaten vor große Herausforderungen⁵.

Konsumenten von Kinderpornografie verkennen oft, dass hinter jedem Bild oder Film das Schicksal eines Kindes steht und dieses ein stiller „Zeuge“ teils schwerer sexueller Misshandlungen dar-



Liliane Mollet

Master of Law, CAS Information Security, Geschäftsführerin und Inhaberin des Beratungsunternehmens insecor gmbh und externe Beraterin der aktuellen NDHS.
E-Mail: l.mollet@insecor.ch



Jens Klopp

Diplom Ingenieur (FH), Geschäftsführer und Inhaber des Beratungsunternehmens insecor gmbh und externer Projektleiter der aktuellen NDHS.

E-Mail: j.klopp@insecor.ch



Thomas Walther

Kommissariatsleiter der bei der Bundeskriminalpolizei angesiedelten Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBİK) des Bundesamtes für Polizei (fedpol).

E-Mail: cybercrime@fedpol.admin.ch

¹ Zur steigenden Internetnutzung in der Schweiz siehe Bundesamt für Statistik (Hrsg.), Internet in den Schweizer Haushalten, Ergebnisse der Erhebung Omnibus IKT 2010, Neuchâtel 2012, S. 21 ff.

² Vgl. Mitteilung der Kommission an das Europäische Parlament und den Rat, Erster Jahresbericht über die Durchführung der EU-Strategie der inneren Sicherheit, Brüssel 25.11.2011, KOM (2011) 790, S. 8 f.

³ Siehe Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBİK (Hrsg.), Jahresbericht 2011, S. 4; Schwarzenegger, Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht. Zeitschrift für Schweizerisches Recht (ZSR) 127 (2008) II, Heft 2, 399-503, S. 410.

⁴ Siehe dazu etwa Botschaft vom 18. Juni 2010 des Schweizerischen Bundesrates über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, BBl 2010 4697, S. 4701; zum Problem der Strafhoheit bei der Aufklärung mittels Internet verübter Delikte siehe auch Eidgenössisches Polizei- und Justizdepartement (Hrsg.), Netzwerk-Kriminalität, Bericht der Expertenkommission „Netzwerkriminalität“, Bern 2003, S. 68 ff.

⁵ Vgl. dazu Schwarzenegger, S. 417 ff.

stellt⁶. Bei jedem Klick im Internet wird dieses Kind, zumindest virtuell, ein weiteres Mal missbraucht. Zugleich wird damit die Nachfrage und Produktion neuer kinderpornografischer Darstellungen gefördert. Für Außenstehende meist nicht direkt erkennbar, nutzen pädophil und pervers veranlagte Personengruppen oft die Aussage, dass sie „nur Bild- und Filmmaterial im Internet konsumieren und niemanden direkt schädigen“. Das Bewusstsein, ob strafrechtlich relevant oder nicht, ist oft nicht gegeben oder im Vergleich zum „Unterhaltungswert“ aufgrund der Anonymität des Internets und des scheinbaren Gefühls von Straffreiheit zweitrangig⁷.

Mit diesen Entwicklungen und den moralisch äußerst bedenklichen Sichtweisen einzelner Internetnutzer steigt auch der Handel von kinderpornografischem Material im Internet⁸. Die geschlossen partnerschaftliche Vorgehensweise der Polizeibehörden bei der effizienten und nachhaltigen Bekämpfung von Cyberkriminalität ist unabdingbar geworden⁹.

Die Schweiz, welche das föderalistische System kennt, etablierte zu diesem Zweck eine Einrichtung, welche die entsprechende Zusammenarbeit und Koordination der Polizeikräfte im Inland und mit ausländischen Behörden gewährleistet und den Anforderungen zur Bekämpfung der Internetkriminalität gewachsen ist. Bereits im Juni 2000 wurden dazu konkrete Bestrebungen für eine nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBİK) aufgenommen¹⁰.

Das jüngste und wohl wichtigste Ergebnis dieser Zusammenarbeit ist die Nationale Datei- und Hashwertesammlung (NDHS) zur effizienteren Bekämpfung der Kinderpornografie. Die Schweiz hat damit eine Fachanwendung ins Leben gerufen, welche die Auswertungen und Beurteilungen von strafrechtlich relevantem Material nach den Art. 135 (Gewaltdarstellungen) und 197 (Pornografie) des Schweizerischen Strafgesetzbuches (StGB)¹¹ beschleunigt und den Kantonspolizeien eine zusätzliche technische Unterstützung bietet.

Nachfolgend soll aufgezeigt werden, wie die NDHS in der Schweiz entstanden ist, insbesondere mit Blick auf die Vorgehensweise bei der Entscheidungsfindung, Konzeption und Umsetzung dieses forensischen Hilfsmittels.

2 Rechtliche Definition der Kinderpornografie

2.1 Internationales Recht

International wird der Begriff Kinderpornografie juristisch unterschiedlich definiert¹². Dies hat seine Ursache unter anderem in den unterschiedlichen rechtlichen Definitionen von „Kind“

6 Siehe Koller, Cybersex, Die strafrechtliche Beurteilung von weicher und harter Pornographie im Internet unter Berücksichtigung der Gewaltdarstellungen, Bern 2007, S. 14.

7 Viele Delikte bleiben von den Betroffenen unbemerkt oder werden nicht als strafbar „eingestuft“; siehe dazu auch Pfister, Hacking in der Schweiz im Spiegel des europäischen, des deutschen und des österreichischen Computerstrafrechts, Berlin u.a. 2008, S. 62 f.

8 Vgl. zur Phänomenologie des Cybersex Koller, S. 7 ff.; siehe auch Jenssen, Filme sind an Widerwärtigkeit kaum zu überbieten, Die Welt, 24. Oktober 2012 sowie von Dohnanyi, Hässliche Wachstumsindustrie, Die Weltwoche, 31. Oktober 2012.

9 Siehe dazu auch die Literaturhinweise unter Fußnote 5.

10 Siehe zur Entstehungsgeschichte von KOBİK in KOBİK (Hrsg.), Jahresbericht 2003, S. 3 f.

11 Vgl. Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, abrufbar unter: http://www.admin.ch/ch/d/sr/c311_0.html.

12 Vgl. dazu unter <http://www.cybercrime.admin.ch/content/kobik/de/home/themen/kinderpornografie.html>.

und „Pornografie“¹³. In internationalen Übereinkommen wie der Lanzarote-Konvention¹⁴ findet sich in Art. 20 folgende Definition: jedes Material mit der bildlichen Darstellung eines Kindes bei wirklichen oder simulierten eindeutig sexuellen Handlungen oder jede Abbildung der Geschlechtsteile eines Kindes zu vorwiegend sexuellen Zwecken. Konkreter wird die Kinderpornografie im Übereinkommen über die Cyberkriminalität (Cybercrime Convention)¹⁵ umschrieben. Nach dessen Art. 9 macht sich strafbar, wer mittels eines Computersystems vorsätzlich Kinderpornografie anbietet, zugänglich macht, verbreitet, übermittelt, sich verschafft, besitzt oder für die Verbreitung mittels Computer herstellt. Dabei liegt das Schutzalter bei 18 Jahren.

2.2 Schweizerisches Recht

Die Schweiz hat sich bereits vor Abschluss einer Reihe internationaler Abkommen zur konsequenten Bekämpfung der Kinderpornografie verpflichtet¹⁶. Obschon die schweizerische Rechtsordnung den Anforderungen der Lanzarote-Konvention weitgehend genügt, werden einzelne Anpassungen des geltenden StGB nötig sein¹⁷. Dies betrifft im Bereich der Kinderpornografie die Anhebung des Schutzalters von 16 auf 18 Jahre. Dabei sollen Kinder in der Schweiz künftig bis zum vollendeten 18. Lebensjahr vor der Mitwirkung bei sexuellen Darstellungen geschützt werden.

Die geltende Schweizerische Pornografiestrafnorm Art. 197 StGB lässt sich in zwei Kategorien unterteilen: die weiche und harte Pornografie. Man spricht von „harter Pornografie“, wenn eines der abschließend aufgezählten Merkmale „Kind“, „Tier“, „menschliche Ausscheidung“ oder „Gewalt“ zur weichen Pornografie hinzukommt¹⁸. Das gemeinsame Kennzeichen der in Art. 197 Ziff. 3 und 3^{bis} StGB abschließend aufgezählten Fälle besteht offensichtlich in der Darstellung schwerer sexueller Perversionen bzw. besonders abartiger oder abscheuerregender sexueller Praktiken¹⁹. Diese beiden Ziffern sind als absolute Verbote zu verstehen²⁰. Im Zentrum der Bekämpfung der Kinderpornografie steht dabei immer der Schutz der Kinder, die bereits zur Herstellung solcher Produkte missbraucht worden sind²¹.

13 Vgl. Koller, S. 218 ff.; siehe jedoch Bestrebungen des International Centre for Missing & Exploited Children (ICMEC) in Kooperation u.a. mit INTERPOL zur internationalen Harmonisierung gesetzlicher Bestimmungen betreffend Ausbeutung und Misshandlung von Kindern, Child Protection Model Law, Best Practices: Protection of Children from Exploitation, 6th Draft, March 2012.

14 Vgl. Übereinkommen des Europarates vom 25. Oktober 2007 zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, SEV-Nr.: 201.

15 Vgl. Übereinkommen des Europarates vom 23. November 2001 über die Cyberkriminalität, SEV-Nr.: 185. Dieses Übereinkommen ist bis anhin die erste und einzige internationale Konvention, die sich mit Computer- und Netzwerkkriminalität befasst. Am 1. Juli 2004 ist es für die Schweiz in Kraft getreten.

16 Dieses Übereinkommen ist das erste und bisher einzige internationale Instrument, das die verschiedenen Formen sexuellen Kindsmisbrauchs umfassend strafbar erklärt. Siehe dazu Botschaft vom 4. Juli 2012 des Schweizerischen Bundesrates zur Genehmigung des Übereinkommens des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (Lanzarote-Konvention) sowie zu seiner Umsetzung (Änderung des Strafgesetzbuchs), BBl 2012 7571, S. 7578.

17 Siehe dazu in der Botschaft des Schweizerischen Bundesrates zur Lanzarote-Konvention, a.a.O., S. 7581 ff.

18 Vgl. Koller, S. 217 f.

19 Vgl. Urteil des Schweizerischen Bundesgerichts, BGE 121 IV 128, E. 2.

20 Siehe Schwaibold/Meng, Kommentar zu Art. 197 StGB, in: Niggli/Wiprächtinger (Hrsg.), Basler Kommentar, StGB II, 3. Auflage, Basel 2012.

21 Vgl. BGE 131 IV 64, E. 11.4.

3 Bewältigung föderalistischer Herausforderungen

3.1 Allgemeines

Im föderalistischen System der Schweiz erfolgt die Erfüllung gesetzlicher Aufgaben im Rahmen des *kooperativen Föderalismus*²². Darunter sind alle Formen von Zusammenarbeit unter den Kantonen oder zwischen den Kantonen und dem Bund zu verstehen. Diese Zusammenarbeit kann auf freiwilliger Basis oder aufgrund einer Norm des Bundesrechts erfolgen. Der kooperative Föderalismus dient der Erkenntnis, dass komplexe Aufgaben der Kantone und die starke Interdependenz in allen Bereichen eine weitgehende Koordination und Kooperation erfordern.

Polizeiaufgaben werden in erster Linie durch die kantonalen Polizeibehörden wahrgenommen (kantonale Polizeihochheit, Art. 57 BV)²³. Jedoch koordinieren nach Art. 57 Abs. 2 BV Bund und Kantone ihre Anstrengungen im Bereich der internen Sicherheit²⁴. Wichtigste Behörden in der Schweiz zur Bekämpfung der Kinderpornografie im Internet sind die kantonalen Polizeibehörden, KOBİK und die kantonalen Staatsanwaltschaften.

Die kantonsübergreifende Zusammenarbeit bei der Beurteilung von sichergestelltem, teils sehr umfangreichem strafrechtsrelevantem Material im Bereich der Kinderpornografie²⁵ gestaltet sich oft als schwierig. Dies nicht nur aufgrund unterschiedlicher rechtlicher Kompetenzen der kantonalen Behörden, sondern etwa auch aufgrund verschiedener Vorgehensweisen oder Beurteilungskriterien²⁶. Mit der Schaffung der nationalen Koordinationsstelle KOBİK und damit neuen organisatorischen, rechtlichen wie technischen Möglichkeiten konnten diese föderalistischen Herausforderungen entschärft werden.

3.2 KOBİK als nationale Koordinationsstelle

Die im Schweizerischen Bundesamt für Polizei (fedpol) angesiedelte KOBİK ist eine von Bund und Kantonen gemeinsam betriebene und finanzierte Einrichtung. Sie wurde 2001 durch Vertreter des Bundes und der Kantone zum koordinierten Vorgehen bei der Bekämpfung der Internetkriminalität ins Leben gerufen²⁷.

Die strategische Führung von KOBİK obliegt dem paritätischen Leitungsausschuss mit je einem Delegierten der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), der Konferenz der Strafverfolgungsbehörden der Schweiz (KSBS), der Konferenz der kantonalen Polizeikom-

mandanten der Schweiz (KKPKS) und der Geschäftsleitung des Bundesamtes für Polizei (fedpol). Der Leitungsausschuss legt die Geschäftsordnung fest, garantiert die Umsetzung des Mandats und überwacht die Leistungserbringung.

Als nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität ist KOBİK das Kompetenzzentrum für Schweizerische Behörden, Internet Service Provider und Private für rechtliche, technische und kriminalistische Fragen sowie der Ansprechpartner für ausländische Behörden im Bereich der Bekämpfung der Internetkriminalität.

3.3 Arbeitsgruppe IT-Ermittler

Zur Bearbeitung komplexer, kantonsübergreifender Polizeiaufgaben werden verschiedene Arbeitsgruppen durch die KKPKS eingesetzt, welche sich jeweils intensiv mit einem bestimmten Thema auseinandersetzen und gemeinsam nach Lösungen suchen. Die Spezialisten mit Vertretern aus Kantonen und dem Bund sind bemüht, jeweils gemeinsam einen größtmöglichen Nenner einer bestimmten Problemstellung zu erarbeiten. Diese Entscheide sind nicht rechtsverbindlich, doch entfalten sie regelmäßig Signalwirkung für die Mitglieder dieser Arbeitsgruppen und damit auch der anderen Kantone.

Im Gebiet der Internetkriminalität findet sich die Arbeitsgruppe IT-Ermittler. Diese Arbeitsgruppe hat eine *Unterarbeitsgruppe IT* unter der Leitung von KOBİK ins Leben gerufen. Sie hat den Auftrag, die bis anhin in den Kantonen gesammelten Erkenntnisse und Erfahrungen im Bereich der Umsetzung des Art. 197 StGB auszutauschen und bestmögliche Synergien zu nutzen. Weiter werden die unterschiedlichen Ebenen und Kompetenzen sowie Bedürfnisse und Sichtweisen von Kantonen und Bund berücksichtigt, sowie verschiedene Standpunkte, Verantwortlichkeiten, Aufgabenteilungen und Prozessabläufe ausgetauscht. Eine entsprechende Rücksichtnahme und Toleranz gegenüber unterschiedlichen Arbeitsweisen und Auffassungen der verschiedenen Sprach- und Kulturgebiete der Schweiz ist unabdingbar²⁸. Hier spielt die KOBİK wiederum eine wichtige Rolle, welche dank ihrer zentralen und koordinierenden Funktion eine einheitliche Entscheidung unter den Kantonen herbeiführen kann.

4 Problematik bei der Beurteilung von Kinderpornografie

Hohe zeitliche Aufwände, physischer und psychischer Ressourcenverbrauch bestimmen die täglichen Arbeiten zur Auswertung und Beurteilung von sichergestelltem strafrechtsrelevantem Material nach Art. 197 StGB²⁹. Die zuständigen IT-Ermittler müssen teilweise sehr große Datenmengen von Bildern und Filmen mit Bezug zur Kinderpornografie untersuchen³⁰. Eine exakte und korrekte Auswertung sowie Beurteilung nach den gesetz-

22 Siehe Häfelin/Haller/Keller, Schweizerisches Bundesstaatsrecht, 8. Auflage, Zürich 2012, N 1242 ff.

23 Siehe Biaggini/Gächter/Kiener (Hrsg.), Staatsrecht, § 19, N 48; Ehrenzeller, St. Galler Kommentar zu Art. 57, N 6 und 12.

24 Siehe Ehrenzeller, a.a.O., Kommentar zu Art. 57, N 2; zur Übersicht der Bundeskompetenzen im Bereich der inneren Sicherheit vgl. N 7 ff.

25 Siehe KOBİK (Hrsg.), Jahresbericht 2011, S. 17 f. wobei es sich bei dem in den Jahren 2003 bis 2011 im Rahmen von Hausdurchsuchungen beschlagnahmten Material in 94% der Fälle um Kinderpornografie handelte.

26 Vgl. beispielsweise Frey/Omlin, „Genesis“ – Pornographie & Internet, Eine Würdigung der neuen Rechtslage gestützt auf die Erfahrungen im Kanton Luzern, in: AJP 2003, S. 1378-1390, S. 1383 ff.; siehe auch Eidgenössisches Polizei- und Justizdepartement (Hrsg.), Netzwerk-Kriminalität, Bericht der Expertenkommission „Netzwerkriminalität“, Bern 2003, S. 75 ff. sowie S. 133.

27 Vgl. dazu die Verwaltungsvereinbarung zum koordinierten Vorgehen bei der Bekämpfung der Internetkriminalität vom 19. Dezember 2001 und die Geschäftsordnung für die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBİK) vom 30. März 2011. Weitergehende Informationen zu KOBİK siehe unter www.kobik.ch.

28 Vgl. auch Brühl-Moser, Schweizerischer Föderalismus: Ausgestaltung, Neugestaltung und Herausforderungen, in: Härtel (Hrsg.), Handbuch Föderalismus – Föderalismus als demokratische Rechtsordnung und Rechtskultur in Deutschland, Europa und der Welt, Bd. IV, 2012, § 99, 112 ff.

29 Exemplarisch: 10'000 unbekannte Dateien strafrechtsrelevanten Materials bei einer Sichtszeit je Datei von erfahrungsgemäß etwa fünf Sekunden ergibt eine Gesamtmenge von etwa 19.5 Gbyte und eine Bearbeitungszeit von etwa 13.8 Stunden. Eine detaillierte Auswertung und Beurteilung von Filmen ist nicht mitberücksichtigt.

30 Häufig werden mehrere Terrabyte an Dateien sichergestellt.

lichen Grundlagen und damit eine zweifelsfreie Einordnung der sichergestellten Daten ist hierbei zwingend. Dies bedeutet, dass jede Datei gesichtet und entsprechend beurteilt werden muss. Beurteilungen und Einordnungen erfolgen über alle sichergestellten Dateien je Fall und Kanton. Partiiell werden durch die zuständigen kantonalen Polizeibehörden bereits beurteilte Dateien, aus früheren Kinderpornografie-Fällen, erneut ausgewertet, was einen erheblichen, unnötigen und nicht haltbaren Zustand darstellt. Weiter können aufgrund fehlender einheitlicher Prozesse und Instrumente Synergien unter den kantonalen Polizeibehörden nur wenig genutzt werden.

Was sich auf den ersten Blick leicht umsetzbar anmuten lässt, bedarf sehr guter Kenntnisse und vertiefter Erfahrungen in der Beurteilung und Sachlage der Thematik von kinderpornografischem Material. Als Beispiele seien hierbei die Interpretationsspielräume bei der Beurteilung des Alters eines Kindes oder spezifischen Darstellungen der potentiellen Opfer genannt³¹.

5 Forensische Hilfsmittel

5.1 Einsatz von Hashwert-Listen

Von sichergestellten Dateien werden Hashwerte³² gebildet, die unter anderem zur Analyse großer Datenmengen genutzt werden. Um einen Rückschluss auf strafrechtsrelevantes Material zu erhalten, werden die generierten Hashwerte mit bereits bekannten Hashwert-Listen³³ verglichen. Entscheidende Vorteile durch den Einsatz von Hashwert-Listen sind Zeitersparnis und Wegfall aufwändiger und belastender Sichten.

5.2 Black- und White-Listen Ansätze

Grundsätzlich kann zwischen zwei Verwendungsansätzen von Hashwert-Listen unterschieden werden³⁴:

- **Black-Listen:** Listen, die Hashwerte von strafrechtsrelevanten Dateien enthalten und die dazu dienen, aus der sichergestellten Datenmenge verbotene Inhalte zu erkennen;
- **White-Listen:** Hashwert-Listen, die nicht strafbare Inhalte (z.B. Icons von Betriebssystemen oder Applikationen) enthalten. Diese Listen dienen zur Reduktion der Datenmenge.

5.3 Abwägungen bei der Verwendung von Hashwert-Listen

Zur Datenreduktion können unter Umständen etablierte Hashwert-Listen³⁵ eingesetzt werden. Der Einsatz solcher Listen sollte jedoch vorgängig hinsichtlich Übereinstimmung mit den entsprechenden nationalen Strafnormen geprüft werden. Dies bestä-

31 Zur Schwierigkeit der Beurteilung kinderpornografischer Darstellungen vgl. beispielsweise Koller, S. 218 ff.

32 Vgl. Steinebach, FORBILD Forensische Bilderkennung findet illegales Material, Projektblatt, abrufbar bei Fraunhofer-Institut für Sichere Informationstechnologie SIT: http://www.sit.fraunhofer.de/content/dam/sit/de/projektblaetter/ForBild_de.pdf.

33 Vgl. etwa die Listen des NIST abrufbar unter <http://www.nsl.nist.gov/RDS/> oder jene des NFI abrufbar unter <http://www.forensicinstitute.nl/>.

34 Vgl. etwa Baier/ Dichtelmüller, Datenreduktion mittels kryptographischer Hashfunktionen in der IT-Forensik: Nur ein Mythos?, in: Schartner/Taeger (Hrsg.), Tagungsband D-A-CH Security 2012, Frechen 2012, S. 279 ff.

35 Siehe unter Fußnote 33; die weltweit verbreitetste Whitelist ist das Reference Data Set (RDS) des US-amerikanischen NIST.

tigte sich u.a. im Austausch mit den kantonalen Vertretern in der *Unterarbeitsgruppe IT*. Deshalb empfiehlt es sich zusätzlich landesspezifische Referenz-Hashwert-Listen wie jene der NDHS von KOBİK zu verwenden.

6 Idee eines nationalen Systems NDHS

Im Zuge der eben genannten Herausforderungen einer zweifelsfreien Einordnung strafrechtsrelevanter Dateien und effizienter wie korrekter Aufarbeitung immenser Datenmengen im Bereich der Kinderpornografie, hat die Schweiz eine Fachanwendung ins Leben gerufen, welche die Ermittlungen beschleunigen soll und den kantonalen Polizeibehörden eine zusätzliche Unterstützung bietet.

6.1 Kategorisierung in der NDHS

Um eine Standardisierung bei der Beurteilung und Einordnung der Dateien zu erreichen, einigten sich die Mitglieder der *Unterarbeitsgruppe IT* auf entsprechende Kategorien, welche ihre Grundlage u.a. in Art. 197 Ziff. 3 und 3^{bis} StGB finden. Exemplarisch wurden etwa Kategorien wie *Gewalt*, *KiPO* oder *Zoophilie* gebildet und entsprechende Beschreibungen zur eindeutigen Zuordnung solcher Bilder und Filme erarbeitet. Je Kategorie lassen sich spezifische Hashwert-Listen generieren, die seitens der kantonalen Polizeibehörden als Referenz dienen oder zur Datenreduktion genutzt werden können.

6.2 Qualitätssicherung und Akzeptanz durch Rating

Das Hauptaugenmerk gilt der inhaltlichen Korrektheit und Verifizierbarkeit der Hashwert-Listen. Somit erscheint eine Datei erst dann in den Hashwert-Listen der NDHS, wenn eine dreifache identische Beurteilung (Rating) und abschließende Qualitätskontrolle durch KOBİK erfolgt ist.

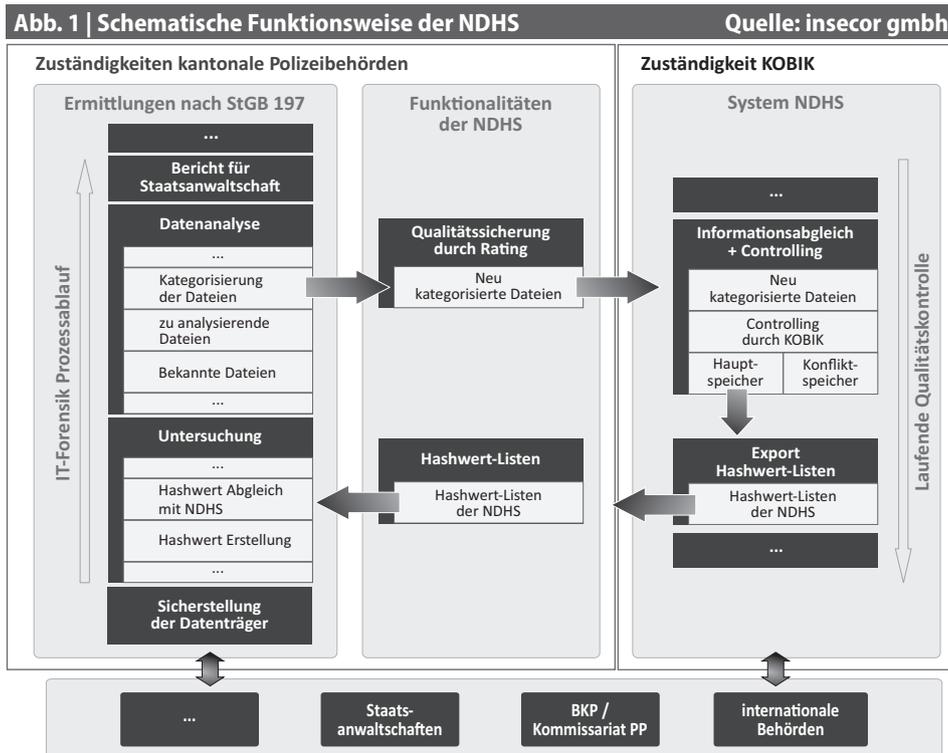
Dateien, die nicht identisch gewertet worden sind, werden in einen sogenannten Zwischenspeicher (Konfliktspeicher) verschoben, der im Zuge von Schulungen und wiederkehrenden Arbeitsgruppensitzungen mit kantonalen Polizeibehörden und Bundesbehörden gemeinsam und abschließend beurteilt wird. Infolge einheitlicher Kategorisierung und qualitativer Anforderungen lassen sich strafrechtsrelevante und nicht strafrechtsrelevante Dateien Schweiz weit einheitlich einordnen, beurteilen und vergleichen.

6.3 Effiziente Aufarbeitung der Datenmenge

Nebst einer einheitlich definierten Kategorisierung und hohen Qualität von Hashwerten ist das Vorgehen bei der Beurteilung großer Datenmengen innerhalb eines vertretbaren Zeitaufwandes zu bestimmen. Hierzu existieren grundsätzlich zwei Umsetzungsvarianten:

- **Zentraler Ansatz:** Auswertung und Kategorisierung der Dateien je Strafnorm durch eine zentrale Stelle wie z.B. der KOBİK; oder
- **Dezentraler Ansatz:** Auswertung und Kategorisierung der Dateien durch die kantonalen Polizeibehörden während der Fallanalyse.

Eine zentrale Auswertung kam für alle Beteiligten (Kantone, KOBIK) insbesondere aus folgenden Gründen nicht in Frage: erhebliche Mehraufwände für die zentrale Stelle und hohe personelle Ressourcen sowie zu starke Abhängigkeit einer zweifelsfrei kategorisierten Hashwert-Liste und entsprechender Qualität von der Akzeptanz der im Fall zuständigen kantonalen Polizeibehörden. Aufgrund dessen und im Sinne einer solidarischen Zusammenarbeit zwischen kantonalen Ermittlungsbehörden und Bundesbehörden erfolgt die Auswertung und Beurteilung dezentral. Ziel ist, die NDHS mit eindeutig strafrechtsrelevantem Material (Bilder und Filme) zu speisen und durch das abschließende Controlling der KOBIK Referenz-Hashwert-Listen mit hoher Qualität zu erreichen.



7 Schematische Funktionsweise der NDHS

8 Fazit

Anhand eines exemplarischen IT-Forensik Prozessablaufs wird nachstehend das Zusammenspiel zwischen IT-Forensik und dem System NDHS aufgezeigt (vgl. dazu Abb. 1).

Die kantonalen Polizeibehörden verwenden wie bis anhin ihre standardisierten IT-Forensik Prozesse³⁶ und erstellen verschiedene Hashwert-Listen. Diese Hashwert-Listen können nun mit den Hashwert-Listen derselben Strafnorm aus der NDHS verglichen werden. Das Ergebnis in den IT-Forensik Prozessschritten *Untersuchung* und *Datenanalyse* ist eine Aussage über die Anzahl strafrechtsrelevanter Dateien. Die verbleibende Restmenge unbekannter Dateien ist durch die kantonalen IT-Ermittler und Forensiker entsprechend der NDHS-Kategorisierung zu beurteilen. Diese erste Kategorisierung der Dateien stellt das erste Rating von dreien dar. Sobald ein Bild oder Film ein drittes Mal durch einen Kanton identisch kategorisiert worden ist, werden diese Hashwerte in die finale NDHS Hashwert-Liste übernommen.

Diese Liste von Hashwerten wird wiederum den Kantonen über die JANUS-Community³⁷ zur Verfügung gestellt. Mittels Vergleich dieser Hashwerte können umfangreiche Dateien miteinander auf Übereinstimmungen geprüft werden, ohne das strafrechtsrelevante Material ein weiteres Mal visuell prüfen zu müssen.

³⁶ Vgl. zum Beispiel IT-Forensik Prozess des BSI (Hrsg.), Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), S. 60 ff.; zur Abgrenzung der strafprozessualen Ermittlungshandlungen nach der Schweizerischen Strafprozessordnung (StPO; SR 312.0) von den sogenannten Vorermittlungshandlungen der kantonalen Polizeibehörden vgl. Albertini, in: Albertini/Fehr/Voser (Hrsg.), Polizeiliche Ermittlung, Zürich/Basel/Genf, 2008, S. 543 ff.

³⁷ Bei der JANUS-Community handelt es sich um das Intranet, welches schweizweit den Polizeibehörden Informationen zur Verfügung stellt.

Den Auftrag, welchen KOBIK von der *Unterarbeitungsgruppe IT* erhalten hat, konnte durch die NDHS und der guten Zusammenarbeit mit den kantonalen Polizeibehörden in kurzer Zeit erreicht werden. Folgende Verbesserungen in der Auswertung und Beurteilung kinderpornografischer Fälle können verzeichnet werden:

- Referenz-Hashwert-Listen: die NDHS Hashwert-Listen entsprechen der Strafnorm Art. 197 Ziff. 3 und 3^{bis} StGB und können durch die Ermittler als Referenzliste bei der Auswertung weiterer Fälle genutzt werden;
- Effizienzsteigernd: aufgrund der Verlässlichkeit und der Qualität der NDHS Hashwert-Listen kann größtenteils auf weitere Sichtung des kinderpornografischen Materials verzichtet werden;
- Gemeinschaftswerk: Mit der NDHS ist ein Gemeinschaftswerk entstanden, welches dem föderalistischen Gedanken in der Schweiz und der gemeinsamen Verantwortung Rechnung trägt sowie die Wirksamkeit dieser Organisationsform aufzeigt³⁸;
- Nutzen und Erfahrungen: Die NDHS ist im Verlaufe des Jahres 2012 in Betrieb genommen worden. Einen wichtigen Beitrag leisten dabei die kantonalen Polizeibehörden, welche die im Rahmen der Projektarbeiten definierten Prozesse auch in der Praxis solidarisch und möglichst einheitlich im Interesse einer gemeinsamen Bekämpfung der Cyberkriminalität und Durchsetzung der entsprechenden Rechtsnormen, verwenden;
- Standardisierung: Ein Beitrag zu einer standardisierten Beurteilung leisten die auf nationaler Ebene durchgeführten Schulungen zu den einheitlichen Kategorisierungskriterien. Als „Schulungsunterlagen“ dienen Dateien aus dem Konflikt-speicher.

³⁸ Vgl. statt vieler Härtel, a.a.O., Vorwort.