Bundeskriminalamt

BKA

Erforderliche Speicherfristen für IP-Adressen

Stand: 08.05.2023

I. Allgemeines

a) IP-Adressen

Sobald sich ein Telekommunikationsgerät (z.B. ein Smartphone, Tablet oder PC) in das Internet einwählt, vergibt der Telekommunikationsanbieter (TK-Anbieter) eine IP-Adresse (Zahlen-/Buchstabenkolonne), damit das Endgerät des Nutzers und die angerufene Website technisch miteinander kommunizieren können. Da die TK-Anbieter nur über eine begrenzte Anzahl von IP-Adressen verfügen, werden diese i.d.R. dynamisch vergeben: damit kann die IP-Adresse nach einem bestimmten Zeitintervall wieder einem anderen Anschluss zugeordnet werden. Hat ein Nutzer eine strafbare Handlung im oder mithilfe des Internets begangen, können Strafverfolgungsbehörden anhand der IP-Adresse (inkl. Zeitstempel) den TK-Anbieter um Auskunft bitten, wem die relevante IP-Adresse zum fraglichen Zeitpunkt zugewiesen war (Bestandsdatenabfrage z.B. gem. § 100j Absatz 2 StPO[1]). In der Strafverfolgung und Gefahrenabwehr kommt der IP-Adresse (inkl. Port[2] und Zeitstempel) bei Straftaten im oder mithilfe des Internets eine zentrale Rolle **zur Identifizierung von Tatverdächtigen** zu. In einer Vielzahl der Fälle ist sie der einzige Ermittlungsansatz.

b) Speicherpraxis der TK-Anbieter

In Deutschland ist die geltende Regelung zur Vorratsdatenspeicherung seit 2017 faktisch ausgesetzt. Der EuGH hat in seinem Urteil von 2022 die anlasslose Speicherung von IP-Adressen aufgrund geringerer Eingriffsintensität ausdrücklich zugelassen. Die TK-Anbieter speichern derzeit jedoch lediglich zu eigenen Geschäftszwecken (z.B. zu Abrechnungs- oder IT-Sicherheitszwecken) zeitlich begrenzt und zum Teil nicht vollständig die Telekommunikationsverkehrsdaten der Kunden. So unterbleibt insbesondere im Mobilfunkbereich häufig das Hinzuspeichern der vergebenen Portnummer zur IP-Adresse, die jedoch erforderlich wäre, um eine Identifizierung des Anschlussinhabers zu ermöglichen. Die gespeicherten Daten sind deshalb in vielen Fällen nur bedingt zur Identifizierung der Nutzer von TK-Anschlüssen geeignet, von denen strafbare Handlungen ausgehen.

Aktuelle Speicher-/Auskunfts-Praxis von IP-Adressen der fünf großen TK-Anbieter in Deutschland (nach Auskunft der TK-Anbieter[3]):

- Deutsche Telekom AG — bis zu 7 Tage
- Vodafone — bis zu 7 Tage
- Telefonica — bis zu 7 Tage
- 1&1 Versatel — zukünftig bis zu 7 Tage
- Freenet — für 0 Tage

[1] Für etwaige Gefahrenabwehrvorgänge die bereichsspezifische Norm im jeweiligen Polizeigesetz. Auf eine explizite Unterscheidung zwischen Straftäter und Störer wird lediglich aus Gründen der Übersichtlichkeit verzichtet.
[2] Für die Identifizierung des Anschlussinhabers ist insbesondere im Mobilfunkbereich das Hinzuspeichern der Portnummer zur IP-Adresse notwendig.
[3] Im Wesentlichen decken sich die Angaben der TK-Anbieter mit den Erfahrungen der Polizeibehörden, wenngleich in der Praxis kleinere Abweichungen von diesen Auskünften feststellbar waren. 1&1 Versatel hat in der Vergangenheit deutlich kürzer gespeichert.

c) Quick-Freeze bei IP-Adressen

Daten beim TK-Anbieter können nur zu bereits bekannten Anschlussinhabern eingefroren werden. Für die Identifizierung eines noch unbekannten Tatverdächtigen selbst bietet das Quick-Freeze-Verfahren keinen Nutzen, sofern die relevanten Daten zum Zeitpunkt des Auskunftsersuchens nicht mehr oder unvollständig gespeichert sind.

d) Ziel des Papiers

In diesem Papier soll die Frage beantwortet werden, für welchen Zeitraum IP-Adressen bei TK-Anbieter gespeichert werden müssten, um Tatverdächtige, die Straftaten im oder mithilfe des Internets begehen, identifizieren zu können.

II. Lageveränderungen

a) Verlagerung der Kriminalität in den digitalen Raum

In den letzten Jahren hat sich das gesellschaftliche Leben – damit einhergehend ebenfalls die Kriminalität – immer weiter ins Internet verlagert. Während die Straftaten der Polizeilichen Kriminalstatistik (PKS) zwischen 2015 bis 2022 um über 11% zurückgegangen sind, sind **„digitale“ Straftaten** deutlich **angestiegen**:

- Straftaten unter Nutzung des Tatmittels Internet + 62%
- Computerkriminalität bzw. Cybercrime (Tatmittel Internet) + 156%
- Verbreitung pornografischer Inhalte + 440%
- Verbreitung pornografischer Inhalte (Tatmittel Internet) + 598%
- Hasspostings (von 2019 zu 2022) + 122%

Diese Entwicklungen untermauern auch Ergebnisse aus Opferbefragungen

- 13,5% der Bevölkerung wurden zwischen November 2019 bis Oktober 2020 Opfer von Cybercrime[4]
- 34% hielten es in 2020 für wahrscheinlich, in den nächsten 12 Monaten Opfer von Betrug im Internet zu werden
- 11,4% der Kinder und Jugendlichen gaben 2022 an, dass Erwachsene bereits versucht haben, sie durch Drohung im Internet zu ungewollten Handlungen zu bewegen (Cybergrooming (Drohung))[5]
- 88% in 2021 und 84% in 2022 der Unternehmen in DEU wurden Opfer von Cyberangriffen (2017: 53%)
- 6,4% berichteten 2020, Opfer von Cybermobbing geworden zu sein (2014: 1%)
- 8,4% berichteten 2020, Opfer von Online-Warenbetrug geworden zu sein (2014: 3,9%)
- 20% aller Anfeindungen gegen Amtspersonen waren 2022 Hasspostings im Internet

[4] Die Angabe bezieht sich auf Cyberkriminalität im weiteren Sinne.
[5] Nicht umfasst sind andere Arten des Cybergroomings.

b) Sexueller Missbrauch von Kindern und Jugendlichen

Eine besondere Herausforderung der Kriminalitätsbekämpfung sind Abbildungen (z.B. Bilder oder Videos) von sexuell missbrauchten Kindern/Jugendlichen, die tausendfach im Internet geteilt werden – dies führt zu permanenter Reviktimisierung der Opfer. In den USA sind bestimmte Anbieter dazu verpflichtet, Darstellungen sexualisierter Gewalt, die sie bei freiwilligen Suchmaßnahmen auffinden, dem National Center for Missing & Exploited Children (NCMEC) zu melden, das seinerseits entsprechende Hinweise zum Zwecke der Strafverfolgung auch an das BKA als deutsche Zentralstelle übermittelt. Während 2017 noch **28.378** strafrechtlich relevante NCMEC-Hinweise mit Deutschlandbezug beim BKA eingingen, waren es **2022** bereits **89.844** – damit hat sich die Anzahl der NCMEC-Hinweise in 5 Jahren mehr als **verdreifacht**.

c) Ausblick

Mit Umsetzung der CSA-VO[6] schätzt das Statistische Bundesamt, dass künftig pro Jahr über **1.200.000** potentiell strafrechtlich relevante Hinweise über ein noch einzurichtendes EU-Zentrum im BKA eingehen werden. Damit würden sich die ohnehin schon sehr hohen Hinweiszahlen von 2022 noch einmal **mehr als verzehnfachen**. Anders als bei den Hinweisen im NCMEC-Prozess, die aus freiwilligen Suchmaßnahmen der Provider stammen und teilweise durch – freiwillig zusätzlich übermittelte – weitere Informationen angereichert sind, muss zukünftig bei Umsetzung der CSA-VO einkalkuliert werden, dass die mittels Aufdeckungsanordnung Verpflichteten **zunehmend** lediglich **IP-Adressen** und weniger/keinerlei andere Ermittlungsansätze (Telefonnummer oder E-Mail-Adressen) übermitteln werden.

Zugleich müssen sich die Polizeien des Bundes und der Länder darauf einstellen, dass sich mit der geplanten Umsetzung des **DSA (Digital Services Act)** die Zahl der Hinweise auf strafrechtlich relevante Sachverhalte im Internet insgesamt ab **dem Frühjahr 2024** weiter signifikant erhöht[7]. Die IP-Adresse wird daher für die Ermittlung der mutmaßlich Tatverdächtigen zwangsläufig weiter an Bedeutung gewinnen.

III. Heutige Erfolgsquoten ohne verpflichtende Speicherung für IP-Adressen

Vom NCMEC werden täglich Verdachtsmeldungen in drei- bis vierstelliger Höhe an das BKA übermittelt. Große Telemediendienstanbieter wie Meta und Google kooperieren neben der gesetzlichen Verpflichtung freiwillig mit dem NCMEC, sodass dem BKA neben der verpflichtenden Meldung der IP-Adresse in einem Teil der Fälle freiwillig weitere Ermittlungsansätze zur Verfügung gestellt werden (z.B. Telefonnummern oder Email-Adressen).

---

[6] Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern.

[7] Aktuell ist im DSA noch kein einheitlicher Standard der Ausleitung strafrechtlicher Hinweise festgelegt, wodurch sich der Prozess der Anlieferung der IP-Adresse zeitlich aufwändiger gestalten könnte.

Zur Analyse der heutigen Erfolgsquoten hat das BKA eine händische Auswertung zu 1000 strafrechtlich relevanten NCMEC-Vorgänge durchgeführt, die Ende 2021 / Anfang 2022 im BKA eingegangen sind. Als Ermittlungsansatz wurden mit den Hinweisen folgende Daten übermittelt:

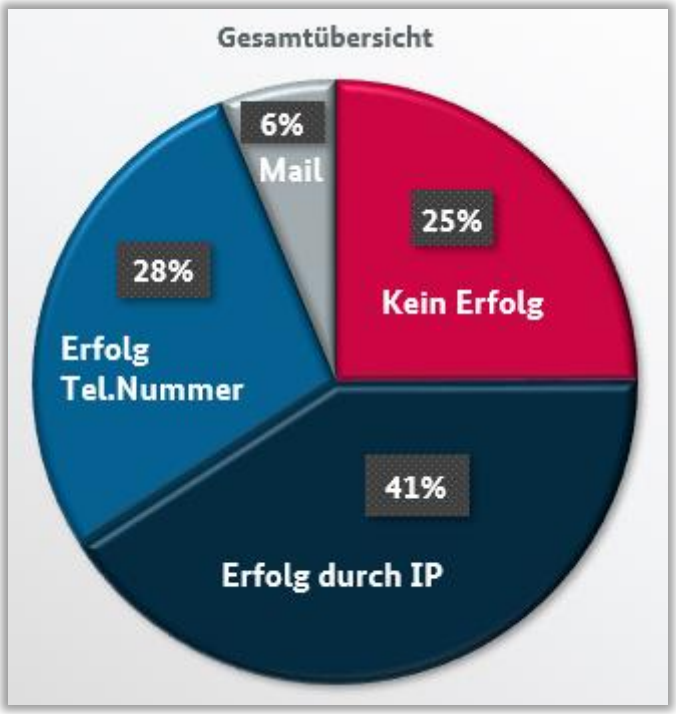
- 984 IP-Adressen,
- 484 Telefonnummern,
- 655 E-Mail-Adressen.

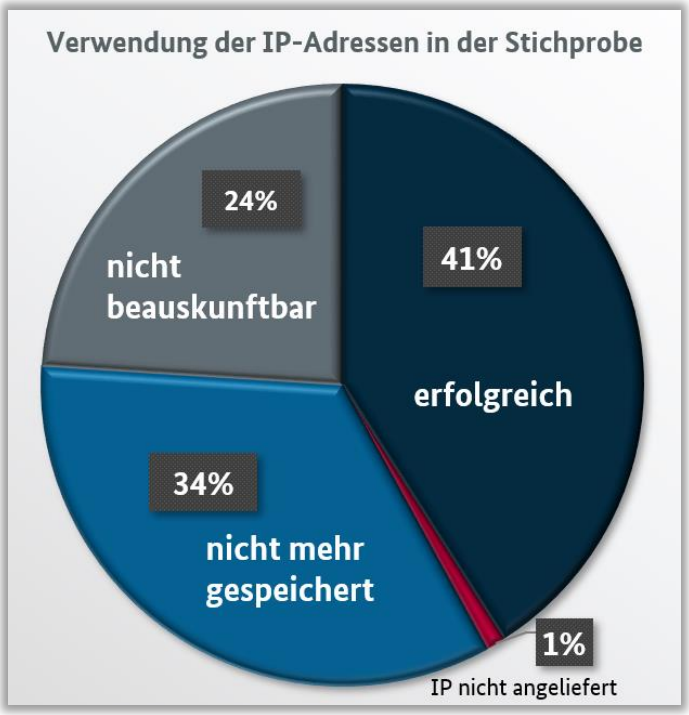
Die Analyse ergab, dass in **41% der Vorgänge** die IP-Adresse einem Nutzeranschluss für weitere Ermittlungen zugeordnet werden konnte (im nachfolgenden Schaubild als „erfolgreich“[8] gekennzeichnet) – etwa **34%** der angelieferten IP-Adressen waren beim TK-Anbieter nicht mehr gespeichert und weitere **24%** aus anderen Gründen (etwa aufgrund einer zusätzlich zur Identifizierung erforderlichen, aber nicht gespeicherten Portnummer) **nicht beauskunftbar.**

Führt eine IP-Adresse nicht zu Identifizierung des Täters, werden – sofern vorliegend – weitere Ermittlungsansätze (Telefonnummern und/oder E-Mail-Adressen) für die Ermittlungen genutzt. So konnten weitere 34% der bis dahin noch nicht aufgeklärten NCMEC-Vorgänge der weiteren Strafverfolgung zugeführt werden (in **28%** der Fälle über die **Telefonnummer** und in **6%** der Fälle über die **E-Mail-Adresse).** Damit erreichte das BKA eine Erfolgsquote von etwa 75% (für 2021 und 2022).

Die restlichen **etwa 25%** der NCMEC-Vorgänge wurden an die ZIT[9] zur Einstellung übermittelt und werden **nicht in der PKS erfasst**. Insofern ist die Aufklärungsquote in der PKS zumindest in diesem Kontext nur eingeschränkt aussagekräftig.

Schaubilder Erfolgsquoten im NCMEC-Prozess





[8] „Erfolgreich“ ist die Weiterleitung des NCMEC-Vorgangs an eine zuständige Länderdienststelle mit einem werthaltigen Ermittlungsansatz zur weiteren Strafverfolgung.
[9] Zentralstelle zur Bekämpfung der Internetkriminalität (GenStA Frankfurt am Main).

In diesem Zusammenhang wird auch nochmals darauf hingewiesen, dass die in der Antwort der Bundesregierung auf eine Schriftliche Frage dargestellten 2.150 NCMEC-Vorgänge aus dem Jahr 2021, bei denen die IP-Adresse nicht mehr gespeichert war, nur einen Ausschnitt des Problems darstellt. Nicht umfasst waren bei dieser Angabe die – mangels zusätzlicher Informationen wie etwa der Portnummer – „nicht beauskunftbaren" IP-Adressen und Fallkonstellationen, in denen die IP-Adresse nicht der einzige Ermittlungsansatz war. Die Anzahl der eingestellten Vorgänge war deshalb um ein Vielfaches größer. Im Jahr 2022 wurden **etwa 20.000 strafrechtlich relevante NCMEC-Vorgänge** mangels Möglichkeit der Identifizierung eines potentiellen Tatverdächtigen **zur Einstellung** an die ZIT übermittelt.

Die dargestellten Erfolgsquoten aus dem NCMEC-Prozess sind auf Ermittlungen in anderen Kriminalitätsbereichen nicht übertragbar, bei denen tatrelevante IP-Adressen z.T. erst später polizeilich bekannt werden oder durch (zeit-)aufwändige Maßnahmen zunächst ermittelt werden müssen.
Die unzureichende Speicherung von IP-Adressen bei TK-Anbietern kann insbesondere in (terroristischen) **Gefährdungsszenarien** ein **erhebliches Risiko** darstellen, wenn die relevante IP-Adresse zum Zeitpunkt der Übermittlung – bspw. durch eine ausländische Partnerbehörde – beim TK-Anbieter bereits nicht mehr gespeichert oder mangels gespeicherter Portnummer nicht beauskunftbar ist und weitere Ermittlungsansätze nicht vorliegen (siehe Parallelitäten zum Fall Castrop-Rauxel).

IV. Mögliche Erfolgsquoten mit Speicherverpflichtungen für IP-Adressen

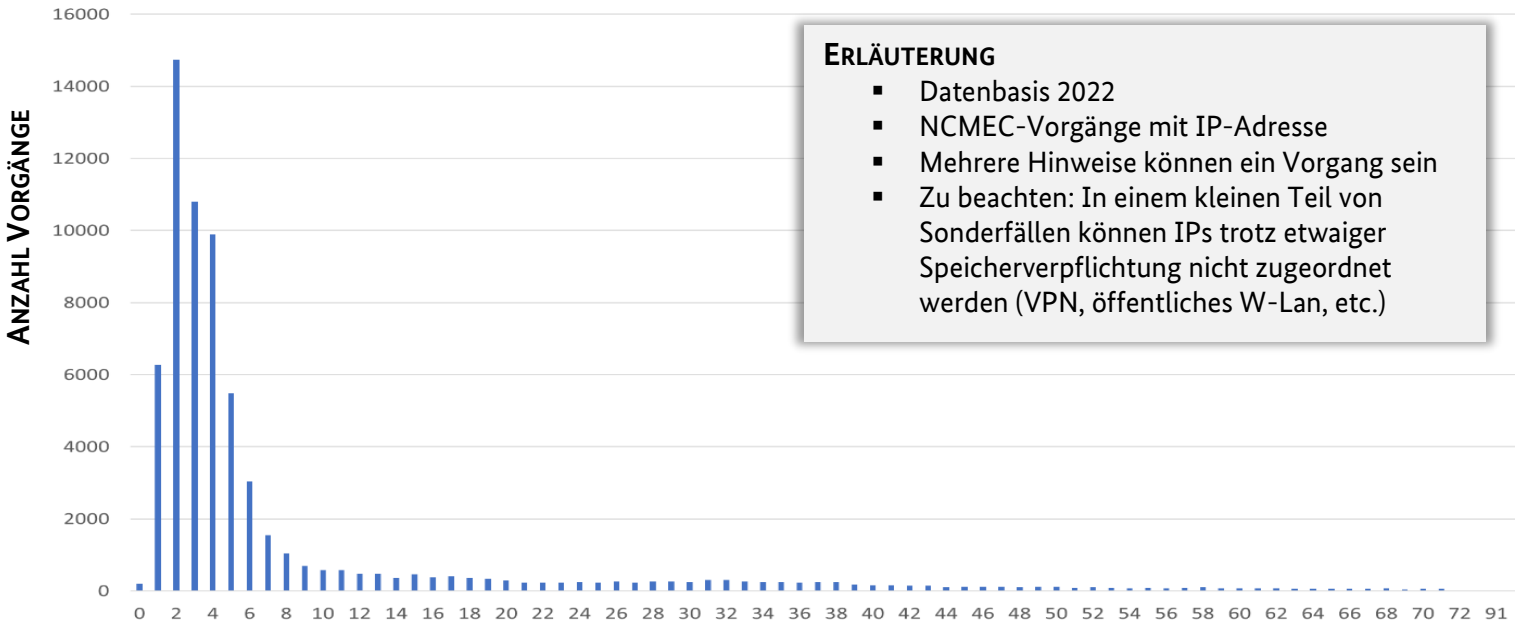
Zur Beantwortung der Frage, welche Erfolgsquote im NCMEC-Prozess erreicht werden könnte, wenn eine einheitliche Speicherverpflichtung (für IP-Adressen und Ports) umgesetzt würde, hat das BKA eine technische Auswertung von etwa 66.000 NCMEC-Vorgängen aus dem Jahr 2022 durchgeführt.

Das nachstehende Schaubild zeigt das Alter der IP-Adressen zum Zeitpunkt des Einganges des NCMEC-Hinweises im BKA (Vorgangsbeginn). Im NCMEC-Prozess wird die Strafbarkeitsprüfung durch das BKA ohne größeren Zeitverzug durchgeführt und die Bestandsdatenanfrage bei hinreichender Erfolgswahrscheinlichkeit unmittelbar gestellt. Das Alter der IP-Adressen gibt deshalb Aufschluss darüber, wie lange eine verpflichtende Speicherfrist für IP-Adressen bemessen sein müsste, um einen (hypothetischen) Identifizierungserfolg erreichen zu können. In einem zweiten Schaubild ist deshalb zur weiteren Veranschaulichung dargestellt, in wie vielen Vorgängen ein Identifizierungserfolg in Relation zur (hypothetischen) Speicherdauer beim TK-Anbieter möglich gewesen wäre. Dabei wird für den Zweck der Darstellung unterstellt, alle TK-Anbieter wären einheitlich zu einer Speicherung von der jeweiligen Dauer verpflichtet.

Bei Betrachtung dieser hypothetischen Erfolgsquote ist zu berücksichtigen, dass selbst dann, wenn die relevante IP-Adresse beim TK-Anbieter noch gespeichert ist, nicht in allen Fällen die Identifizierung eines konkreten Kundenanschlusses möglich ist. Bei Nutzung bspw. eines Virtual Private Networks (VPN) oder eines öffentlichen W-Lan-Netzwerkes verläuft eine Identifizierung einer konkreten Person in der Regel nicht erfolgreich. Dies betrifft zwar nur einen kleinen Anteil der Fälle, muss jedoch einkalkuliert werden. Umgekehrt könnte sich die hier wiedergegebene Erfolgsquote durch die Nutzung von weiteren Ermittlungsansätzen (Telefonnummern, E-Mail-Adressen) erhöhen.

Bundeskriminalamt

BKA



ALTER DER IP-ADRESSEN BEI EINGANG IM BKA (VORGANGSBEGINN) (IN TAGEN)

Hypothetische Speicherlänge der IP (in Tagen)	Hypothetischer Anteil mit Ermittlungserfolg (in Prozent)	Verbleibende Anzahl ohne Ermittlungserfolg (Vorgänge in absoluten Zahlen)
0	0,0 %	66.074
1	0,3 %	65.867
2	9,8 %	59.598
3	32,1 %	44.866
4	48,5 %	34.059
5	63,4 %	24.169
6	71,7 %	18.684
7	76,3 %	15.649
8	78,7 %	14.103
9	80,2 %	13.061
10	81,3 %	12.366
11	82,2 %	11.785
12	83,0 %	11.212
13	83,8 %	10.727
14	84,5 %	10.250
18	86,9 %	8.631
21	88,4 %	7.637
26	90,2 %	6.449

Bewertung

Die Schaubilder zeigen, dass die Erfolgsquote im NCMEC-Prozess durch eine einheitliche gesetzliche Speicherverpflichtung von IP-Adressen (inkl. Portnummern) erheblich gesteigert werden könnte, wobei der Effekt **in den ersten Wochen besonders signifikant** wäre.

- So wäre die Erfolgsquote der Gewinnung von Identifizierungsansätzen allein anhand der IP-Adressen 2022 bei einer einheitlichen Speicherverpflichtung für 14 Tage von ca. 41% auf über **80%** gestiegen[10].

- Mithilfe von weiteren Ermittlungsansätzen (Telefonnummern, E-Mail-Adressen) ließe sich diese **Gesamterfolgsquote** noch **spürbar weiter steigern**.

Dieses Ergebnis dürfte im Wesentlichen auch auf die künftigen Meldungen nach der EU-VO CSA und DSA übertragbar sein, wenngleich aufgrund der noch unklaren Umsetzungsbedingungen der EU-VO CSA und DSA sowie dem zukünftigen Meldeverhalten der Verpflichteten keine exakten Voraussagen getroffen werden können.

Gemessen an den wahrscheinlichsten Fallkonstellationen wäre eine Speicherverpflichtung von 2 bis 3 Wochen auch bei besonderen (terroristischen) Gefahrenlagen regelmäßig ausreichend und damit ein signifikanter Sicherheitsgewinn.

Daneben existieren jedoch Bedarfslagen (bspw. Cybercrime, Organisierte Kriminalität, komplexe Ermittlungsverfahren im Bereich des sexuellen Missbrauchs von Kindern und Jugendlichen), bei denen eine Begrenzung der **Speicherfrist auf 2 bis 3 Wochen regelmäßig nicht ausreichend** sein dürfte. Dies trifft insbesondere auf komplexe Ermittlungsverfahren zu, bei denen tatrelevante IP-Adressen erst später bekannt werden oder zunächst aufwändig ermittelt werden müssen.

V. Schlussbemerkung

Die gravierend zunehmende Verlagerung der Kriminalität hin zu Delikten, die im oder über das Internet begangen werden, machen die Verfügbarkeit von IP-Adressen und Portnummern zur Täteridentifizierung wichtiger denn je und sind damit **der Anlass zur Einführung einer zumindest kurzzeitigen Speicherpflicht für IP-Adressen**: Gerade im Bereich der Bekämpfung von Darstellungen sexualisierter Gewalt gegen Kinder kommt den Meldungen vom NCMEC sowie den künftigen Meldeverpflichtungen nach der EU-VO CSA und dem DSA eine besondere Bedeutung zu.

Die durchgeführten Auswertungen der Daten im NCMEC-Prozess zeigen, dass durch eine einheitliche Speicherverpflichtung für IP-Adressen (inkl. Port) die signifikante Steigerung der Erfolgsquoten möglich wäre. Gleichzeitig gibt die Auswertung Hinweise darauf, wie lange die erforderliche Speicherfrist bemessen sein müsste, um die im NCMEC-Prozess angestrebte Erfolgsquote zu erreichen. Dieses Ergebnis lässt jedoch sich nicht ohne Weiteres auf andere Kriminalitätsbereiche übertragen, in denen die IP-Adressen i.d.R. deutlich älter als die im NCMEC-Prozess sind.

[10] Bei Berücksichtigung der o.g. Tatsache, dass bei Nutzung bspw. eines VPN oder eines öffentlichen W-Lan-Netzwerkes eine Identifizierung einer konkreten Person in der Regel dennoch nicht erfolgreich verläuft.