NIEDERSÄCHSISCHER LANDTAG
18. WAHLPERIODE

N i e d e r s c h r i f t

über die 18. - öffentliche - Sitzung
der Enquetekommission zur Verbesserung des Kinderschutzes und zur Verhinderung von Missbrauch und sexueller Gewalt an Kindern
am 27. September 2021
Hannover, Landtagsgebäude

Tagesordnung: Seite:

Anhörung zu den im Einsetzungsbeschluss genannten Aufgaben, Zielen und Fragestellungen, insbesondere zu Ziffer III Nrn. 2, 4, 5 und 11

Anhörung

Anwesend:

Mitglieder der Kommission:

Mitglieder des Landtags:

1. Abg. Lasse Weritz (CDU), Vorsitzender
2. Abg. Wiebke Osigus (SPD)
3. Abg. Claudia Schüßler (SPD) (per Videokonferenztechnik zugeschaltet)
4. Abg. Annette Schütze (SPD)
5. Abg. Ulrich Watermann (SPD)
6. Abg. Sebastian Zinke (SPD)
7. Abg. Marcel Scharrelmann (i. V. d. Abg. Christian Calderone) (CDU) (per Videokonferenztechnik zugeschaltet)
8. Abg. Petra Joumaah (CDU)
9. Abg. Clemens Lammerskitten (CDU)
10. Abg. Uwe Schünemann (CDU) (per Videokonferenztechnik zugeschaltet)
11. Abg. Editha Westmann (CDU)
12. Abg. Susanne Schütz (FDP)

Externe Sachverständige:

13. Prof. Dr. Anette S. Debertin
14. Henrike Krüsmann (per Videokonferenztechnik zugeschaltet)
15. Lisa Schmitz
16. Dr. Dirk Themann (DKSB) (per Videokonferenztechnik zugeschaltet)

Von der Landtagsverwaltung:

Regierungsrätin Lange,
Beschäftigter Ünal,
Beschäftigte Dr. Weingraber.

Niederschrift:

Beschäftigter Ramm, Stenografischer Dienst.

Sitzungsdauer: 13.50 Uhr bis 16.23 Uhr.

Tagesordnung:

Anhörung zu den im Einsetzungsbeschluss genannten Aufgaben, Zielen und Fragestellungen, insbesondere zu Ziffer III Nrn. 2, 4, 5 und 11 - Drs. 18/7604

SafeToNet GmbH

***Anwesend**:*

***Jesse Jeng,** Chief Investment Officer*

Jesse Jeng: Das Unternehmen SafeToNet befasst sich vor allem mit der Frage, wie man Kinder online vor denjenigen schützen kann, die sie in u. a. sexueller Hinsicht bedrohen können.

Kurz ein paar aufklärende Worte zu dem Ausmaß dieser Gefahr: Eine Studie der Charité - Universitätsmedizin Berlin hat untersucht, inwieweit pädophile Neigungen in der Bevölkerung vorhanden sind. Sie kam zu dem Schluss, dass bei 1 % bis 4 % aller Männer natürlicherweise eine Tendenz zu pädophilen Neigungen vorliegt.

Das Kriminologische Forschungsinstitut Niedersachsen hat in einer Untersuchung festgestellt, dass jede zweite Person im Laufe der Kindheit einen im weitesten Sinne sexuellen Vorfall erlebte. Das ist natürlich eine absolut besorgniserregende Erkenntnis.

Wir gehen daher davon aus, dass es in Deutschland unter den männlichen Personen ca. 275 000 - wenn man das so nennen möchte - aktive Pädophile gibt. 275 000 - ich möchte die Zahl wiederholen, um allen hier klarzumachen, wie groß das Potenzial an dieser Stelle ist.

Man kann aus diesen beiden Studien natürlich keine konkreten Fallzahlen ableiten. Es gibt in diesem Bereich ein sehr großes Dunkelfeld, weshalb es ja auch diese Enquetekommission gibt. Wenn man die Erkenntnisse der Studien gemeinsam betrachtet und nicht von dem Maximalwert 4 % ausgeht, sondern den Mittelwert annimmt, kommen Schätzungen zu dem Ergebnis, dass in Deutschland jährlich 45 845 kindliche Missbrauchsopfer gibt. Das sind also fast 46 000 Kinder jedes Jahr in Deutschland. Diese Zahl macht jedem die Größe des Problems klar.

Später werden auch die Strafverfolgungsbehörden angehört. Ich weiß natürlich nicht, welche Inhalte deren Vorträge haben werden, womöglich wird aber die Differenz - das Dunkelfeld - zwischen dieser Schätzung und den tatsächlichen Ermittlungen ersichtlich werden.

Angesichts der Tatsache, dass viele Kinder „tatsächlich“ missbraucht werden, könnte man die sexuelle Bedrohung von Kindern im Online-Raum als eine Art Kavaliersdelikt bewerten. Ich möchte dem ganz deutlich widersprechen. Die Online-Welt ist ja kein abgeschlossener Raum ohne Auswirkungen auf die Offline-Welt. - Im Gegenteil! Die Online-Welt ist oftmals ein Vorbereitungsraum für Kindesmissbrauch und für andere Schäden an Kindern.

Der Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs der Bundesregierung hat den Begriff Cyber-Grooming definiert. „Grooming“ bedeutet übersetzt in etwa „anbahnen“ oder „vorbereiten“. Cyber-Grooming ist die Online-Vorbereitung von sexuellem Kindesmissbrauch.

Wie funktioniert Cyber-Grooming laut der entsprechenden Definition der Bundesregierung? - Es wird versucht, online Kontakt zu Kindern herzustellen. Es wird versucht, ihr Vertrauen zu gewinnen. Es wird versucht, ihre Wahrnehmung zu manipulieren und Abhängigkeitsverhältnisse zu schaffen. Natürlich wird auch versucht, dafür zu sorgen, dass sich Kinder niemandem anvertrauen.

Wie funktioniert das ganz konkret? Viele Kinder sind heutzutage auf Spieleplattformen aktiv, wo sie mit anderen Kindern aus der ganzen Welt spielen. Sie sehen diese anderen Kinder aber nicht, und sie kennen sie auch nicht außerhalb des Cyber-Raums.

Menschen mit pädophilen Neigungen versuchen, so Kontakt mit Kindern aufzunehmen, und geben sich oftmals auch selbst als Kinder aus. Sie suchen das Gespräch, stellen z. B. Fragen zur Schule oder zu Vorlieben. Sie spielen ihnen etwas vor und versuchen, einen „Vertrauensraum“ aufzubauen, zu dem die Eltern der Kinder keinen Zugang haben.

Das ist auch eine soziale Frage. Gerade diejenigen Kinder, die nicht mit den besten sozialen Voraussetzungen gesegnet sind, sind oftmals viel auf Spieleplattformen unterwegs, und den Eltern ist oft gar nicht klar, was dort passiert.

Cyber-Grooming passiert aber auch in Chatrooms und anderen Messengerplattformen. Kinder - insbesondere junge Mädchen - bekommen dort regelmäßig sexuell explizite Bilder zugesandt.

Cyber-Grooming passiert auch in den sozialen Netzwerken. Das sind natürlich Facebook und WhatsApp, das sind aber auch soziale Netzwerke, von denen hier vielleicht noch niemand gehört hat, z. B. Discord - eine Audioplattform -, Snapchat usw.

Wie gesagt, die Täter geben sich während der Annäherungsversuche oft als Kinder aus. Aus Vertrauensverhältnissen sind bereits Situationen entstanden, in denen Kinder explizite Fotos von sich verschickt haben. So können sie das Gefühl bekommen, erpressbar zu werden. Dann wird versucht, die Kinder aus dem Online- in den Offline-Bereich zu ziehen.

So wird versucht, Kinder beispielsweise durch Erpressung dazu zu bewegen, in einen Zug zu steigen und irgendwo anders wieder auszusteigen. Dort versuchen Täter dann, sexuelle Handlungen herbeizuführen. Kinder schämen sich dann oft für eine solche Situation und erzählen möglicherweise nichts davon. Das führt letztlich auch dazu, dass keine Anzeigen gestellt werden bzw. dass sich das Dunkelfeld vergrößert.

Eines möchte ich klarstellen: Es ist überhaupt nicht der Fall, dass der Onlinebereich keine Auswirkungen auf konkrete Missbrauchstaten hat. Im Gegenteil, er ist der Vorbereitungsraum. Wir müssen uns der Tatsache stellen, dass das eine riesige Gefahr für Kinder ist.

Nun zu einem Bereich, den ich nur kurz streifen möchte, der aber ähnlich verheerende Auswirkungen haben kann, obwohl kein sexueller Kindesmissbrauch im Vordergrund steht. Es geht um Cyber-Mobbing. Hierfür gibt es eine Definition des Bundesministeriums für Familie, Senioren, Frauen und Jugend. Ich denke, Mobbing ist allen hier ein Begriff. Jede Person, die auf einer Schule gewesen ist, weiß, was Mobbing ist.

Es gibt aber einen entscheidenden Unterschied zu damals. Heute endet Mobbing nicht am Schultor, sondern ist 24/7 möglich. Es gibt Klassenchats, in denen das weitergeht. Da werden Bilder und Memes, die die Kinder lächerlich machen, verschickt. Es hat sich eine ganz andere Gruppendynamik gebildet, und es gibt eine viel größere Reichweite. Auch gibt es - das muss man ganz deutlich sagen - einen digitalen Fußabdruck. Auch diejenigen Kinder, die mobben oder beleidigen, werden das nie wieder los. Man muss tatsächlich beide Seiten des Problems betrachten.

8 % der jugendlichen Internetnutzer zwischen 12 und 19 Jahren sind Untersuchungen zufolge bereits Opfer von Cyber-Mobbing gewesen. 34 % der Befragten haben im Bekanntenkreis ein Opfer von Cyber-Mobbing. Auch diese Zahlen kommen vom Bundesministerium für Familie, Senioren, Frauen und Jugend. Es gibt also einen sehr bunten Strauß an Bedrohungen und Problemen für Kinder.

Ich möchte deutlich sagen, dass es hier natürlich nicht darum geht, das Internet schlechtzureden. Das Internet birgt für Kinder auch große Chancen, z. B. die Welt zu sehen oder sich zu vernetzen und zu organisieren. Das haben wir in den letzten Jahren ja erlebt. Das Internet ist aber eben auch ein Einfallstor für diejenigen, die Kindern schaden wollen.

Gerade der bestehende Generationenkonflikt - dass viele Eltern weniger digitalaffin sind -, stellt ein großes Problem dar. Dort beginnt die gesellschaftliche Verantwortung. Ich hoffe, dass die Politik hierbei eine noch stärkere Führungsrolle einnehmen kann.

Deswegen will ich abschließend auf die Möglichkeiten der Politik eingehen. Die Anhörungseinladung thematisierte auch Kinderschutz-Apps. Es gibt solche Apps. Ich möchte nicht auf einzelne Produkte eingehen, weil das dem Thema nicht gerecht würde, aber ich will auf generelle Möglichkeiten und auf den Existenzgrund dieser Apps eingehen.

Es gibt digitale Lösungen, die Kinder vor sexuellem Missbrauch oder Beleidigungen und Mobbing schützen sollen. Zum Beispiel verhindern sie mit Bilderkennungsmethoden, dass Nacktbilder oder -videos verschickt werden. Letzteres ist z. B. auch für Amokläufe, bei denen Videos direkt übertragen werden, relevant, wie es sie leider in der Vergangenheit gegeben hat.

Diese Anwendungen können zum Teil aber auch verhindern, dass z. B. schlimme Beleidigungen in Chatgruppen abgeschickt werden. Sie werden durch künstliche Intelligenz (KI) - im Grunde ist das eine algorithmenbasierte Mustererkennung - erkannt.

Zum Existenzgrund dieser Apps gibt es eigentlich nur eines zu sagen: Das Problem ist die Abwesenheit von Regulierungen. Ich bin Vertreter eines Privatunternehmens, aber ich möchte deutlich sagen: Am Ende des Tages gibt es diese digitalen Lösungen, weil es keine umfassende Regulierung zum Schutz von Kindern gibt.

Noch einmal kurz zu den Plattformen: Es muss verstanden werden, dass die Social-Media-Plattformen keinen ökonomischen Grund für Kinderschutz haben. Es gibt ihn schlicht und ergreifend nicht.

Ich möchte das an einem konkreten Beispiel deutlich machen: Facebook hat 2,7 Milliarden Nutzer. Wenn wir davon die Frauen - nehmen wir generisch einen Anteil von 50 % an - abziehen, verbleiben immer noch 1,35 Milliarden Nutzer. Wenn 4 % dieser Männer pädophile Neigungen haben, wären das 54 Millionen Nutzer. Auf der gesamten Welt erzielt Facebook einen durchschnittlichen Umsatz in Höhe von 10,12 US-$ pro Nutzer. In den USA sind es 50 US-$, in Europa 17 US-$. Gehen wir von den durchschnittlichen 10,12 US-$ aus, macht Facebook mit diesen 4 % der Männer einen Umsatz in Höhe von 540 Millionen US-$. Es gibt für eine Social-Media-Plattform keinen ökonomischen Grund, gegen Kinderschutz vorzugehen bzw. sich für diesen zu engagieren.

Deswegen können wir diese Probleme nur als Gesellschaft lösen. Apps und Unternehmen wie wir können nur Unterstützer sein. Es wird nicht möglich sein, dass Strafverfolgungsbehörden alle Kinder schützen, und das Internet soll auch frei bleiben. Es ist klar, dass die Politik das Ganze natürlich nicht alleine lösen kann. Aber die Politik muss in den driver's seat, sie muss in die Führungsrolle! Es ist notwendig, dass soziale Medien in Bezug auf Kinderschutz deutlich stärker reguliert werden, damit das nicht ausschließlich bei anderen Unternehmen hängenbleibt, denn das wird nicht funktionieren. Dafür werbe ich.

Gerne stehe ich zur Beantwortung von Nachfragen zur Verfügung, möchte aber noch darauf hinweisen, dass ich kein ausgesprochener IT-Experte bin, aber aufgrund meiner Tätigkeit selbstverständlich über Einblicke in die Materie verfüge.

Abg. **Ulrich Watermann** (SPD) versicherte, seiner Überzeugung nach sei Kinderschutz wichtiger als Datenschutz. Die große Freiheit in der digitalen Welt, so Abg. Watermann, werde von vielen bejubelt. Er bejubele sie aber schon lange nicht mehr. Zu einer neuen Abwägung zwischen Kinder- und Datenschutz zu kommen, sei eine Aufgabe der Politik. Er bat um eine Einschätzung zu diesem Thema.

Jesse Jeng unterstrich die Wichtigkeit der Abwägungsfrage bei Daten- und Kinderschutz. Dass immer so getan werde, dass Kinder in der analogen Welt alle Freiheiten hätten, werde von sozialen Medien als Verteidigungsstrategie genutzt. Das entspreche aber nicht den Tatsachen. Bestimmte Kinofilme dürften Kinder nicht alleine oder nur in Begleitung von Erziehungsberechtigten sehen. Auch einem nächtlichen Besuch am Steintor würden Eltern sicherlich nicht zustimmen. Ebenso dürften Formate mit bestimmten Inhalten nicht zu jeder Zeit im Fernsehen ausgestrahlt werden.

Die Schutzmechanismen für Kinder, die in der analogen Welt selbstverständlich seien, müssten in gleicher Weise auch für das Internet gelten. Kinder hätten einen Anspruch auf einen solchen Schutz.

Ein Internetbrowser, führte Herr Jeng weiter aus, und auch Internetseiten können nicht ohne Weiteres die Mündigkeit der nutzenden Person feststellen. Für die Nutzung bestimmten Internetseiten - z. B. anhand eines Altersnachweises - die Identifizierung der nutzenden Person zu fordern. Aktuell könne ein 14-jähriges Kind problemlos jede beliebige Internetseite besuchen, indem es z. B. bei der Verifizierung ein falsches Alter angebe.

Die komplexen technischen Lösungen, die für eine effektive Kontrolle erforderlich seien, bräuchten Zeit für ihre Etablierung. Es sei daher politisch zu prüfen, bis wann diese Möglichkeiten Standard sein sollten, um entsprechend zu handeln. Bei wohl 46 000 Kindern, die in Deutschland jährlich Opfer würden, gebe es allerdings keinen großen zeitlichen Spielraum.

Abg. **Ulrich Watermann** (SPD) kam auf die Diskussionskultur in sozialen Medien zu sprechen. Die Unternehmer wiesen die Verantwortung für diese Nutzerinhalte auf ihren Plattformen von sich, aber er, Watermann, sehe das anders.

In diesem Zusammenhang interessiere ihn auch eine Einschätzung zur gesellschaftlichen Verantwortung für in der Vergangenheit getätigte Äußerungen Dritter, die digital konserviert seien. Abg. Watermann berichtete von einem Fall, bei dem

unverantwortliche Ausführungen eines Elternteils als Teil eines Interviews im Internet auffindbar seien. Es sei jedoch fraglich, ob die Kinder es guthießen, dass Äußerungen dieser Art unbeschränkt im Internet abrufbar seien.

Jesse Jeng sagte, häufig finde Cyber-Mobbing durch die Veröffentlichung bestimmter Bilder der kindlichen Opfer statt. Kinder würden z. B. in Klassenchats aufgrund ihres Aussehens verspottet, indem bestimmte Abbildungen von ihnen in großen, öffentlichen Verteilern verbreitet würden. Der Schmerz, der dadurch bei den Kindern entstehe, sei unvorstellbar. In solchen Fällen stelle sich die Frage nach den Möglichkeiten einer Löschung.

Hier müsse das gleiche Recht wie bei „klassischen Medien“ gelten. Falschmeldungen sollten genauso entfernt werden können wie bestimmte Abbildungen von Kindern.

Abg. **Editha Westmann** (CDU) wollte wissen, ob ein endgültiges Löschen von Inhalten im Internet technisch überhaupt möglich sei, oder ob der Spruch „Das Internet vergisst nicht“ den Tatsachen entspreche.

Jesse Jeng antwortete, ob eine vollständige Löschung möglich sei, hänge davon ab, auf welchen Servern sich die entsprechenden Daten befänden und ob die Betreiber der Server zu einer Löschung gezwungen werden könnten. Wenn es sich um eine deutsche Internetseite, die auf einem deutschen Server gehostet werde, handele, sei auch das deutsche Recht anwendbar. Bei rechtswidrigem Verhalten drohten den Betreibern auch wirtschaftliche Konsequenzen.

Es sei lange und ausgiebig diskutiert worden, ob es möglich sei, z. B. Falschmeldungen aus dem Internet zu löschen. Auch in Niedersachsen sei eine solche Maßnahme bereits von bestimmten Personen gefordert worden.

In diesem Zusammenhang kam Herr Jeng auf Google und das „Recht auf Vergessen“ zu sprechen. Er führte aus, per Formular könne bei Google ein Löschantrag gestellt werden. Hiernach seien die betreffenden Daten zumindest nicht mehr über die Suchmaschine auffindbar.

Im Darknet, wo Missbrauchsmaterialien größtenteils zu finden seien, sei eine Löschung hingegen nicht so einfach zu bewerkstelligen, da der Einfluss der Strafverfolgungsbehörden dort viel geringer sei. Um ins Darknet zu gelangen, werde ein Zugang über einen Tor-Browser sowie das Wissen über entsprechende Internetseiten benötigt.

In jedem Fall sei es möglich, den Schutz von Menschen durch aktives, gesetzgeberisches Handeln zu verbessern.

Abg. **Sebastian Zinke** (SPD) gab zu bedenken, dass die von Herrn Jeng vorgeschlagenen Maßnahmen - analog zu Regulierungen außerhalb des Internets - eine staatliche Regulierung des Internets voraussetzten, für die derzeit keine Strukturen existierten. Dies könne nicht allein auf Basis von Selbstverpflichtungen geschehen, denn in der Regel stünden private Unternehmen hinter Internetseiten, deren Nutzung erst über die Zustimmung zu den AGBs ermöglicht werde.

Nicht nur von der Landesbeauftragten für den Datenschutz, sondern auch von internetaffinen Kreisen, die Einschränkungen dieser Art strikt ablehnten, seien Widerstände gegen solche Maßnahmen zu erwarten. Insofern stelle sich die Frage, ob solch umfassende Eingriffe - das Internet müsse quasi „umgedreht“ werden - einerseits in technischer Hinsicht und andererseits in Anbetracht der beschriebenen Widerstände überhaupt umsetzbar seien.

Jesse Jeng stellte klar, dass ein 100-prozentiger Schutz unmöglich sei. Allerdings gebe es mit einem pragmatischen Vorgehen viele Möglichkeiten zur Verbesserung des Kinderschutzes, die keine so starke Einschränkung des Internets bedingten.

In Indien sei Kindern z. B. der Erwerb von SIM-Karten verboten, weshalb ihr Zugang zum Internet - verglichen mit Kindern in Deutschland - eingeschränkt sei. Herr Jeng betonte, dieses Beispiel solle die theoretischen Möglichkeiten herausstellen und nicht als Vorbild verstanden werden.

Es gehe nicht darum, das Internet insgesamt zu ändern, sondern - ähnlich wie in Kinos - Zugangsbeschränkungen zu schaffen. Es sei z. B. denkbar, den Herstellern von Smartphones oder den Telekommunikationsunternehmen bestimmte Bedingungen aufzuerlegen. Auf diese Weise könnten Kinder, die in Besitz eines internetfähigen Endgeräts seien, besser geschützt werden

Entsprechend trainierte Algorithmen - eine KI - seien nach aktuellem Stand der Technik in der Lage, Inhalte, die nicht kindgerecht seien, zu identifizieren. In der Praxis könnte auf entsprechend präparierten Geräten z. B. die Darstellung

pornografischen Material oder das Senden bzw. Empfangen entsprechender Texte unterbunden werden. Das Material zum Training der Algorithmen - dessen Besitz schließlich strafbar sei - müsste allerdings von den Strafverfolgungsbehörden zur Verfügung gestellt werden.

Auf diese Weise käme großen Konzernen wie Vodafone, Telekom, Apple und Samsung mehr Verantwortung im Kinderschutz zu, während sich zugleich ein profitables neues Marktsegment für sie auftäte. Natürlich seien die Eltern dann dafür verantwortlich, dass ihre Kinder nur die entsprechenden „Kinderschutz-Handys“ erhielten. Die Grundlagen hierfür müssten aber von der Politikgeschaffen werden.

Abg. **Sebastian Zinke** (SPD) führte aus, Apple habe aufgrund eines weltweiten Aufschreis und der Forderung zahlreicher Verbände seine Foto-Scan-Pläne zur Eindämmung von Kindesmissbrauchsdarstellungen nicht weiterverfolgt. Daran zeige sich die Dimension des Problems, das, so die Worte des Abg. Zinkes, mit Erziehungstipps und kleinen App-Lösungen nicht zu lösen sei.

Jesse Jeng versicherte, Handys mit den beschriebenen Funktionen könnten einen wichtigen Beitrag leisten. Dort, wo es möglich sei, die Herstellerfirmen stärker in die Verantwortung zu nehmen, sollten entsprechende Lösungen auch vorangebracht werden.

Staatsanwaltschaft Hannover
Abteilung „Sexualdelikte“
Sonderdezernat Misshandlung von Schutzbefohlenen

Schriftliche Stellungnahme: Vorlage 45

***Anwesend**:*

- ***Katrin Ballnus**, Leitende Oberstaatsanwältin*
- ***Dr. Bianca Vieregge**, Oberstaatsanwältin, Abteilungsleiterin des Sonderdezernats*
- ***Daniela Hermann**, Oberstaatsanwältin, Leiterin der Zentralstelle zur Bekämpfung gewaltdarstellender, pornografischer oder sonst jugend-gefährdender Schriften*

Dr. Bianca Vieregge: Bei der Staatsanwaltschaft Hannover wurde 2008 ein Sonderdezernat für die Bearbeitung von Verfahren wegen Misshandlung von Schutzbefohlenen, die zur Tatzeit nicht älter als vier Jahre sind, eingerichtet. Manchmal nehmen wir auch etwas ältere Kinder auf. Es kommt dabei vor allen Dingen darauf an, ob die Kinder bereits zeugentüchtig sind.

Die langjährige Erfahrung mit der Bearbeitung dieser Verfahren hat gezeigt, dass der Datenaustausch zwischen den Institutionen grundsätzlich gut funktioniert, was ich vor allem auf eine gute, kontinuierliche Netzwerkarbeit zurückführe. Ich nenne beispielsweise den jährlich tagenden Runden Tisch Kinderschutz, der von dem Koordinierungszentrum Kinderschutz organisiert wird. Ebenso ist der Runde Tisch der Medizinischen Hochschule Hannover oder die vom Kinder- und Jugendkrankenhaus Auf der Bult initiierte Kinderschutzgruppe zu nennen. Neben der wichtigen Netzwerkarbeit wird so auch der interdisziplinäre Austausch ermöglicht, der hier sehr in den Vordergrund zu stellen ist.

Auch der regelmäßige Erfahrungsaustausch, den die Staatsanwaltschaft Hannover mit Beratungsstellen vornimmt, die z. B. soziale Trainingskurse für gewalttätige und gewaltbereite Väter und Mütter anbieten, trägt viel zu einer guten interdisziplinären Zusammenarbeit bei.

Die Kehrseite der Medaille ist, dass erfahrungsgemäß auch in vielen Fällen schwerer und schwerster körperlicher - man denke z. B. an das Schütteltrauma eines Säuglings - oder auch seelischer - diese ist bei der Misshandlung Schutzbefohlener strafrechtlich relevant - Gewalt von verschiedenen Institutionen nur mit erheblicher zeitlicher Verzögerung oder gar nicht Strafanzeige erstattet wird.

Die Erfahrung zeigt auch, dass der sehr wichtige Datenaustausch zwischen der Staatsanwaltschaft und anderen Institutionen nicht rund läuft bzw. nur verzögert stattfindet, wenn ein Ermittlungs- oder Strafverfahren läuft. Dadurch gehen nicht nur wichtige Beweismittel verloren, die für eine effiziente Strafverfolgung wichtig sind, sondern letztlich geht das auch zulasten des Opferschutzes.

Ich möchte im Besonderen darauf hinweisen, dass Verfahren zum Nachteil von Säuglingen und Kleinkindern auf Ereignisse zurückgehen, die sich in der großen Mehrzahl im häuslichen Bereich abspielen. Der Täter oder die Täterin sind erziehungsberechtigt oder aber Personen, die zeitweise mit der Betreuung des Kindes befasst waren, z. B. der Lebensgefährte der Erziehungsberechtigten.

Bei sehr kleinen Kindern muss man im Auge behalten, dass bei ihnen Personen fehlen, die die berechtigten Interessen des Kindes in irgendeiner Form vertreten können. Zu einem solchen Interesse gehört mit Sicherheit auch der Wunsch nach einer Strafverfolgung - auch, wenn dieser Wunsch erst später gefasst werden sollte.

Vor diesem Hintergrund ist es aus Sicht der Staatsanwaltschaft überaus wünschenswert, wenn insbesondere auf der Jugendamtsebene allgemeine Handlungsempfehlungen sowie fachliche Standards entwickelt werden. Das sollte vom Jugendamt ausgehen, weil dieses häufig die erste Anlaufstelle für Fälle von schwerer oder schwerster körperlicher Gewalt ist. Dazu kann ich auf Wunsch auch noch mehr sagen, ich habe es aber auch in der Stellungnahme dargelegt.

Hier ist also das Setzen eines klaren Zeichens erforderlich. Der Opferschutz - das will ich deutlich hervorheben - muss hier eine besondere Berücksichtigung finden. Es geht in erster Linie nicht um eine effiziente Strafverfolgung - um die geht es *auch*, denn durch sie werden weitere Straftaten verhindert -, sondern der Opferschutz muss ganz klar im Vordergrund stehen.

Handlungsempfehlungen könnten dazu beitragen, dass die Strafverfolgungsbehörden rechtzeitig eingeschaltet werden, und dass die richtigen Daten in einem Ermittlungs- oder Strafverfahren schnell ausgetauscht werden.

Daniela Hermann: Heute spreche ich in meiner Funktion als Leiterin der Zentralstelle im Wesentlichen zu sexualisierter Gewalt gegen Kinder im digitalen Raum. Letztes Mal habe ich schon ein wenig dazu ausgeführt, wie dramatisch die Fallzahlen sexualisierter Gewalt im digitalen Raum in den letzten Jahren angestiegen sind.

Für Niedersachsen - in meinen Augen ist das aber ein bundesweiter Trend - ist die Zahl der Verfahren gegen bekannte Täter um ca. 500 % angestiegen. Die Zahl der Verfahren gegen unbekannte Täter - danach haben Sie in Ihrem Einsetzungsbeschluss auch gefragt - ist in den letzten drei Jahren um 40 % gestiegen.

40 % klingt im Vergleich zu den 500 % erst einmal nach relativ wenig. Man muss aber bedenken, dass wir zeitgleich dazu übergegangen sind, bei Taten aus einem bestimmten Anlass - z. B. bei einer großen WhatsApp-Gruppe oder einer riesigen Tauschbörsen etc. - nicht mehr jede einzelne Tat als Einzelverfahren zu erfassen, sondern dass wir nur noch ein Mantelverfahren führen, das hunderte oder tausende Beschuldigte umfasst. Insofern beziehen sich die 40 % gegen unbekannte Täter auf eine sehr große Anzahl an Einzelfällen.

Warum steigen die Zahlen an? - Ich meine, es gibt zwei wesentliche Faktoren:

Erstens. Die viel einfacher gewordene Verbreitbarkeit in den digitalen Medien. Vor 20 Jahren haben wir Hefte an Tankstellen beschlagnahmt, dann haben wir irgendwann E-Mail-Verteiler mit vielleicht 20 Mails aufgenommen. Heute haben wir WhatsApp-Gruppen mit 1 500 Teilnehmenden. Das geht auch von Kindern und Jugendlichen aus, die relativ unreflektiert mit derartigem Material umgehen, wenn sie z. B. entsprechende Sticker versticken, weil sie das ganz lustig finden.

Zweitens. Es gibt eine exponentielle Zunahme von Ermittlungshinweisen aus dem Ausland, insbesondere aus den USA. Dort sind Provider verpflichtet, entsprechende Vorgängen an die Behörden bzw. eine verantwortliche halbstaatliche Institution zu melden. Inzwischen gibt es ca. 70 000 Meldungen. Ich nehme an, dass die Angehörigen der Generalstaatsanwaltschaft Frankfurt am Main gleich auch noch etwas dazu sagen können werden, da sie einen besseren Überblick darüber haben.

Zur kommerziellen Verbreitung kinderpornografischen Materials kann ich nur für Niedersachsen etwas sagen. Hierzu stehen wir weitestgehend noch am Anfang. Bislang haben wir keine Verfahren gegen Händler geführt, die solches Material für Geld verkaufen. Wir haben nur ab und an Verfahren gegen Ankäufer geführt.

Nach meiner Auffassung ist der Tauschhandel kinderpornografischen Materials quid pro quo häufiger als der Kauf mit Geld. Das findet vielfach in sehr konspirativ angelegten Foren im Darknet statt, die sehr auf Abschottung angelegt sind und neue Mitglieder in der Regel nur dann aufnehmen, wenn diese selber kinderpornografisches Material posten. Das hatte für die Täter den Vorteil, dass sie sicher sein konnten, keiner Polizeibeamtin oder keinem Polizeibeamten aufzusitzen, weil diesen das Posten entsprechenden Materials bis vor Kurzem verboten gewesen ist.

Im Darknet wird aber nicht nur Bild- und Videomaterial ausgetauscht, sondern es werden auch real

existierende Kinder jeglichen Alters zum sexuellen Missbrauch angeboten und vermittelt bzw. verkauft. Verabredungen werden getroffen, um diese Kinder anderen zum sexuellen Missbrauch zu überlassen, am Missbrauch fremder Kinder teilzunehmen oder diesem per Stream beizuwohnen. Manchmal gibt es Videos von Misshandlungen und Missbräuchen geradezu nach Wunschliste, für die das Kind sogar mit Edding oder Creme für den jeweiligen Täter - z. B. „Das ist für Karl“ - beschriftet wird.

Die Täter werden zu den Missbräuchen motiviert und angestachelt. Viele intensivieren ihren Missbrauch durch den Kontakt mit Gleichgesinnten in den einschlägigen Foren. Sie tauschen sich darüber aus, auf welche Art und Weise man am besten an ein Kind herankommen kann, z. B. ob man es besser entführt oder im sozialen Nahraum manipuliert oder wie man es am besten ruhigstellt.

Ich zitiere aus deinem Chat, den ich neulich vorliegen hatte, damit Sie wissen, wovon ich rede: Schlafmittel xy funktioniert gut, aber nur innerhalb der ersten halben Stunde nach der Verabreichung. Ansonsten wacht das Kind durch die Penetration auf.

Sie tauschen sich darüber aus, wie man sich das Schweigen nach durchgeführtem Missbrauch sichert usw. Das sind nicht in allen Fällen Fantastereien, sondern das ermöglicht schwere Missbrauchstaten. Verfahren der ZIT gegen Darknetforen wie „Elysium“ oder „Zauberwald“ zeigen das. Die Verfahren in Münster, Lügde, Staufen oder Bergisch Gladbach belegen sehr deutlich, dass es sich nicht um Einzelfälle handelt, sondern um eine Vielzahl gut organisierter, hochkriminalisierter Täterstrukturen.

Diese Strukturen muss man ermitteln und zerstören. Dazu bedarf es umfassender, ganzheitlicher Ermittlungen, um die Betreiber, Administratoren, Moderatoren und Hauptnutzer zu ermitteln und dann Zugriffsmaßnahmen zu koordinieren. Diese müssen schlagkräftig sein, weil die Täter in technischer Hinsicht relativ gut organisiert sind.

Die Strafverfolgung reagiert, aber sie reagiert verhältnismäßig langsam. Es gab bis 2019 mit der Zentralstelle Cybercrime Bayern in Bamberg und der heute anwesenden ZIT im gesamten Bundesgebiet lediglich zwei Strafverfolgungsbehörden, die derartige Verfahren überhaupt regelmäßig in Angriff genommen haben.

Nach den umfassenden Missbrauchsfällen in Bergisch Gladbach führt auch die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) in Köln entsprechende Ermittlungen. Wenn man sich die Vielzahl der über die Bühne gehenden Straftaten ansieht, ist das aber entschieden zu wenig. Niedersachsen ist eines der flächengrößten und bevölkerungsreichsten Bundesländer und bei diesen Straftaten meines Erachtens in der Pflicht, für eine effektive Bekämpfung der Kriminalität Sorge zu tragen. Das ist aktuell nicht im ausreichendem Maße der Fall.

Die Vorfälle in Lügde, Bergisch Gladbach und Münster machen mehr als deutlich, dass wir uns da bewegen müssen. Das hat auch der Bundesgesetzgeber erkannt. Er hat uns die Möglichkeit der sogenannten Keuschheitsprobe geschaffen, um in genau solchen abgeschotteten Zirkeln ermitteln zu können.

Das ist keine Kriminalität, die auf dem Silbertablett serviert wird, sondern es handelt sich um Holkriminalität, für die man Initiativermittlungen betreiben und das gesamte Instrumentarium der Strafprozessordnung nutzen muss. Das sind riesige, zeitintensive Verfahren mit einer Vielzahl von Beschuldigten. Das sind viele, sehr, sehr schwierige, umfangreiche, oft verdeckte Ermittlungsmaßnahmen - und das nicht nur in Deutschland, sondern weltweit.

Das erfordert vielfältige, schnelle internationale Zusammenarbeit und eine Vernetzung der Strafverfolger, weil es eben nur wenige und vor allen Dingen nur wahnsinnig kurzlebige Spuren gibt. Deswegen ist der Faktor Zeit für einen Ermittlungserfolg essenziell. Um zu verhindern, dass das Darknet zukünftig ein rechtsfreier Raum ist, in dem solche Straftaten zum Nachteil von Kindern begangen werden können, brauchen wir meines Erachtens auch in Niedersachsen eine Einheit, die derart strukturierte Ermittlungen führen und solche Verfahrenskomplexe mit der gebotenen Intensität bearbeiten kann.

Wir haben eine Zentralstelle, aber deren Dezernentinnen und Dezernenten können diese zusätzliche Arbeit wegen der massiven vorhandenen Arbeitslast, die ich ja schon dargestellt habe, einfach nicht leisten. Wir werden keine Verfahren verschieben, sondern eher neue Kriminalität ins Licht bringen. Wir werden bei der bisherigen Zentralstelle also keine Arbeit einsparen. Das ist keine Arbeit, die neben der vorhandenen Belastung gestemmt werden kann.

Hinzu kommt, dass sich die Lage in der Zentralstelle und auch bei der Bearbeitung von Sexualdelikten durch das Gesetz zur Bekämpfung von sexualisierter Gewalt gegen Kinder noch erheblich verschärfen wird.

Einerseits werden vermutlich acht neue Staatsanwaltsstellen für die Zentralstelle geschaffen werden. Wir alle wissen, wie die Haushaltslage im Moment aussieht, und vor diesem Hintergrund sind wir natürlich außerordentlich dankbar dafür. Andererseits fängt das aber nur die bisherige Überlastung auf. Es wird eigentlich keine Spielräume geben, um neue initiative Ermittlungen in diese Richtung führen zu können. Das werden wir aber müssen.

Mir ist bekannt, dass das LKA diese Notwendigkeiten erkannt hat zum November 2021 eine entsprechende Ermittlungseinheit einrichten will. Wenn diese die Arbeit aufnimmt, werden wir mit entsprechenden Verfahren konfrontiert werden. Dann brauchen wir bei der Staatsanwaltschaft eine Einheit, die sich das mit der gleichen Energie und Schlagkraft betreiben kann. Ansonsten sind diese Verfahren zum Scheitern verurteilt.

Abg. **Sebastian Zinke** (SPD) sagte, die Empfehlungen seien dahingehend nicht überraschend, da das hohe Arbeitsaufkommen bekannt sei. Aus diesem Grund sehe der Haushaltsentwurf der Landesregierung die von Frau Ballnus erwähnten zusätzlichen Stellen vor.

Er fragte nach zusätzlichen Änderungswünschen, z. B. nach technischen Hilfsmitteln oder das Prozessrecht betreffend.

Daniela Hermann antwortete, die Einführung der Vorratsdatenspeicherung durch die Bundesgesetzgebung, durch welche ein Verfolgen der flüchtigen Spuren erleichtert würde, sei ein bekannter Wunsch der Strafverfolgungsbehörden.

Überdies werde eine deutlich bessere Ausstattung benötigt. Im Zuge der Bedarfsanmeldung der zusätzlichen Stellen sei auch der Bedarf nach entsprechendem Equipment auf der Grundlage von Erfahrungsberichten bestehender Zentralstellen angemeldet worden. Die genauen technischen Details hierzu könne sie, aber nicht spontan nennen.

Dr. Bianca Vieregge ergänzte den Wunsch nach einer befruchtenden Zusammenarbeit mit IT-Fachkräften, wie sie in anderen Zentralstellen der Fall sei. Das ermögliche es, schnell auf technische Problemstellung zu reagieren.

Abg. **Annette Schütze** (SPD) wollte wissen, ob Hinweise auf den Missbrauch sehr junger Kinder primär von behandelnden Ärztinnen und Ärzten eingingen oder ob es auch weitere Quellen wie Kinderkrippen - die von vielen Kindern aber gar nicht besucht würden - in nennenswertem Ausmaß gebe.

Ihre Befürchtung sei, dass Missbräuche besonders jungen Kinder zu großen Teilen unentdeckt blieben, weil entsprechende Spuren lediglich im Zuge von Arztbesuchen entdeckt werden könnten.

Dr. Bianca Vieregge bezeichnete den angesprochenen Sachverhalt als großes Problem. In der Tat, erläuterte sie, gingen Strafanzeigen häufig erst nach dem Besuch eines Kinderkrankenhauses infolge schwerwiegender Missbrauchsanzeichen wie Schütteltraumata ein. Es sei notwendig, dass sämtliche Institutionen stärker für das Thema sensibilisiert würden, damit im Falle von Verdachtsfällen die notwendige Anzeigebereitschaft vorliege.

In der Vergangenheit habe es wiederholt enge Kooperationen zwischen der Staatsanwaltschaft und der Kinderschutzambulanz von Professorin Debertin gegeben.

Die Rechtsmedizin werde bei solchen Fällen zumeist nur in konsiliarischer Funktion zum Kinderarzt oder ins Kinderkrankenhaus gerufen, um vorliegende Verletzungen feststellen und z. B. zu begutachten, ob diese auf Fremdeinwirkung zurückzuführen seien. In den letzten Jahren hätten sich Mitarbeitende der Rechtsmedizin - obwohl dies nicht deren Aufgabe sei - aber wiederkehrend bereiterklärt, Strafanzeige gegen Unbekannt zu erstatten, um der Generalstaatsanwaltschaft das Einleiten der Ermittlungen zu ermöglichen.

Insbesondere bei sehr jungen Kindern sei die Beweislage sehr kritisch. In der Regel beschränke sich der Täterkreis auf deren Familie, und häufig fehlten aussagebereite Zeugen. Wenn z. B. beide Elternteile tatverdächtigt seien, würden diese sich in der Regel nicht dazu äußern. Ein dezidiertes und umfangreiches rechtsmedizinisches Gutachten müsse daher frühzeitig in Auftrag gegeben werden. Oftmals werde danach noch ein neuroradiologisches und ein neuropädiatrisches Gutachten benötigt.

Die Staatsanwaltschaft sei also auf Anzeigen aus externen Bereichen angewiesen. Die Arbeit an diesen Schnittstellen sei wegen mangelnder Bereitschaft häufig schwierig.

Der § 4 KKG berechtige Berufsgeheimnisträger, das Jugendamt für eine anonyme und auch für eine weitergehende Beratung zu konsultieren. Dadurch erführen die Jugendämter von Missbrauchsfällen. Zwar erstatteten bereits viele engagierte Mitarbeitende in Jugendämtern zeitnah Anzeige, in anderen Fällen dauere es aber auch Wochen, bis die Staatsanwaltschaft Kenntnis von einer Tat erhalte. Ohne eine zwischenzeitliche rechtsmedizinische Untersuchung seien die wichtigsten Beweise größtenteils verloren, was eine Handhabe unterbinde.

Abg. **Editha Westmann** (CDU) fragte, welche Veränderungen vonseiten der Politik die Situation verbessern könnten.

Dr. Bianca Vieregge wünschte sich auf kommunaler Ebene eine konkrete Handlungsempfehlung für Jugendämter, um die zuvor geschilderte Problematik zu entschärfen.

Gegenwärtig sei nicht konkret vorgeschrieben, unter welchen Umständen Daten auszutauschen - den rechtlichen Rahmen hierfür gebe es bereits - oder Anzeigen zu erstatten seien. Ein Handout für die Jugendämter oder entsprechende Schulungen könnten die Sensibilisierung und die Handlungssicherheit in den Jugendämtern bereits erhöhen.

Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT)
Bereich Kinderpornographiebekämpfung
Generalstaatsanwaltschaft Frankfurt am Main

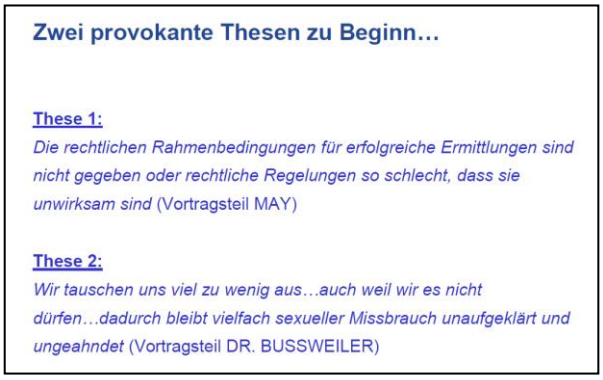
Schriftliche Stellungnahme: Vorlage 47
Präsentationsgrafiken: 1. Nachtrag zu Vorlage 47

***Per Videokonferenztechnik zugeschaltet**:*

- ***Andreas May,** Oberstaatsanwalt, Leiter der Zentralstelle*
- ***Julia Bussweiler**, Staatsanwältin*

Andreas May: Ich leite seit etwa elf Jahren die Zentralstelle zur Bekämpfung der Internetkriminalität. Wir beschäftigen uns von Anfang an mit dem wichtigen Teilbereich der Verbreitung von Kinderpornografie und, damit einhergehend, natürlich auch mit dem sexuellen Missbrauch von Kindern.

Frau Hermann hat unser erstes Verfahren gegen die Plattform „Zauberwald“ schon genannt. Dort gab es auch im Jahre 2010 schon eine bandenmäßige, organisierte Verbreitung von Kinderpornografie. Damals fand das noch im „normalen Internet“ und nicht im Darknet statt. Später hat sich das stark geändert.



Wir möchten mit zwei provokanten Thesen beginnen. Die erste These schließt quasi direkt an die letzte Frage von Frau Westmann - welche Wünsche für die Verbesserung des Ermittlungserfolgs es gibt - an. - Dazu kann ich nur sagen: Wir wünschen uns ganz viel. Zwei Kernpunkte möchte ich heute ansprechen.

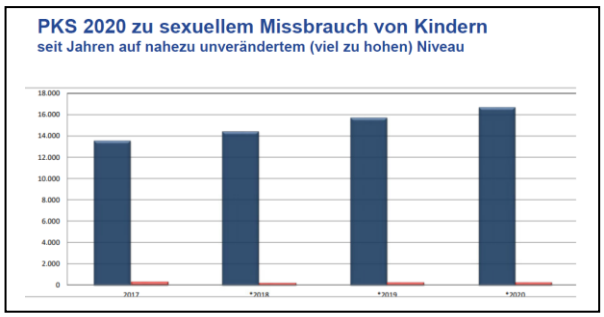
Ich trage zu These 1 vor. Sie lautet: Die rechtlichen Rahmenbedingungen für erfolgreiche Ermittlungen sind entweder überhaupt nicht gegeben, oder die Regelungen sind so schlecht - ich spreche hier insbesondere über das Prozessrecht -, dass sie schlicht und ergreifend unwirksam sind.

Ich werde das gleich an ein paar Beispielen illustrieren. Um das Problem in Kürze zusammenzufassen: Der Gesetzgeber hat das materielle Recht in meinen Augen wahnsinnig intensiv novelliert. Ich glaube, keine gesetzliche Regelung wurde so oft geändert wurde wie §§ 174 ff. StGB. Das Ganze ist unglaublich detailreich. Missbrauchsanleitungen, der Besitz von kindlichen Sexpuppen und viele andere Dinge sind strafbar geworden. Das alles nutzt aus meiner Sicht gar nichts, wenn die Werkzeuge, um Täter namhaft zu machen, nicht vorhanden sind. Der Zustand ist stark defizitär.

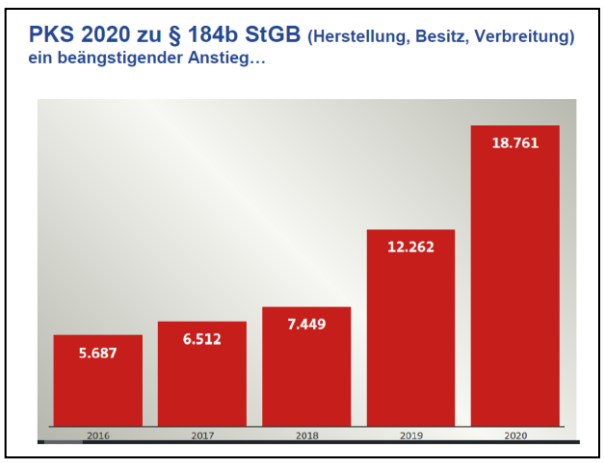
Ich schließe an vieles an, was gerade eben schon von den Kolleginnen gesagt worden ist. Wir sind der festen Überzeugung, dass wir uns trotz all der Runden Tische und der bestehenden Kommuni-

kationsstrukturen immer noch viel zu wenig austauschen. Das liegt daran, dass vielfach höchst unklar ist, was überhaupt übermittelt werden darf und was nicht. Davon wird der Vortragsteil von Frau Bussweiler handeln.

Wir haben heute schon einige Zahlen gehört. Die aktuelle Situation ist natürlich sehr beunruhigend. Die Zahlen für sexuellen Missbrauch steigen bundesweit stark an. Ich bin froh, dass die Kolleginnen aus Niedersachsen Sie über die niedersächsischen Zahlen informiert haben. Ich habe die bundesweiten Zahlen aus der PKS 2020 dabei.

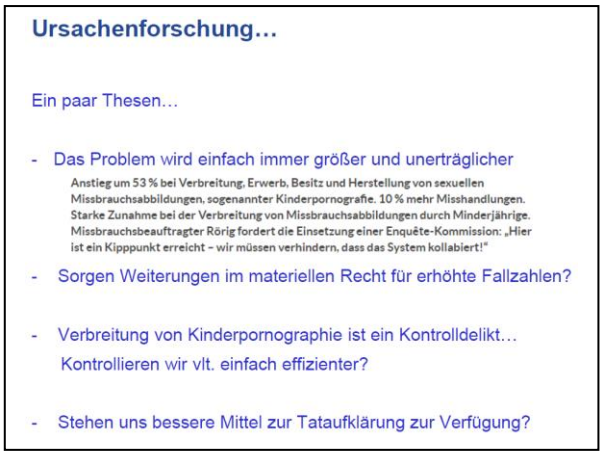


Man erkennt einen relativ moderaten, aber auch sehr kontinuierlichen Anstieg im Jahren 2020 gegenüber den Vorjahren. Es sind ca. 10 % mehr Missbrauchsfälle zu verzeichnen.



Ganz anders sieht es dagegen aus, wenn man sich die Zahlen zur Verbreitung von Kinderpornografie anschaut. Hier gibt es seit 2016 einen stetigen, sehr massiven Anstieg. Von 2019 auf 2020 hat es einen erheblichen Anstieg um über 50 % gegeben.

Was sind die Ursachen für diese massiv ansteigenden Zahlen, insbesondere bei der Verbreitung von Kinderpornografie? - Hierzu möchte ich ein paar sehr unterschiedliche Thesen in den Raum stellen.



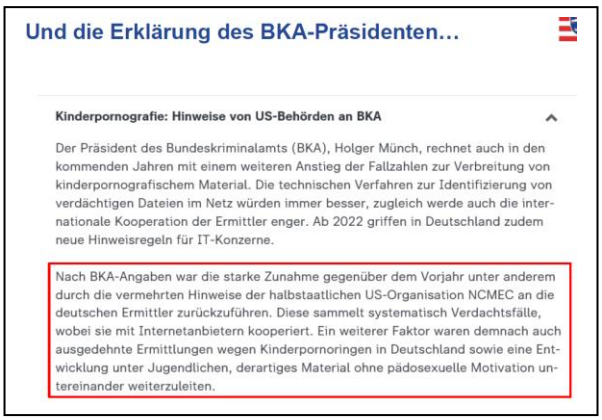
These 1: Das Problem wird einfach immer größer und unerträglicher. Die Verbreitung wird immer einfacher und kann immer anonymer stattfinden. Deshalb steigen die Fallzahlen stark an. Das ist im Sinne des Missbrauchsbeauftragten Herrn Johannes-Wilhelm Rörig, der die Statistik in dieser Art kommentiert hat.

These 2: Wenn das materielle Recht und der Begriff der Kinderpornografie immer stärker erweitert werden, steigen die Fallzahlen automatisch, da immer mehr als Kinderpornografie gilt.

These 3: Es handelt sich um ein Kontrolldelikt. Je mehr Kräfte daran arbeiten, je stärker wir unsere Bemühungen intensivieren, desto erfolgreicher sind wir. Vielleicht sind wir in den letzten Jahren einfach viel besser geworden.

These 4: Vielleicht ist unser Werkzeug gar nicht so schlecht, wenn wir so viele Taten aufklären. aufdecken.

Das sind vier völlig unterschiedliche Thesen.



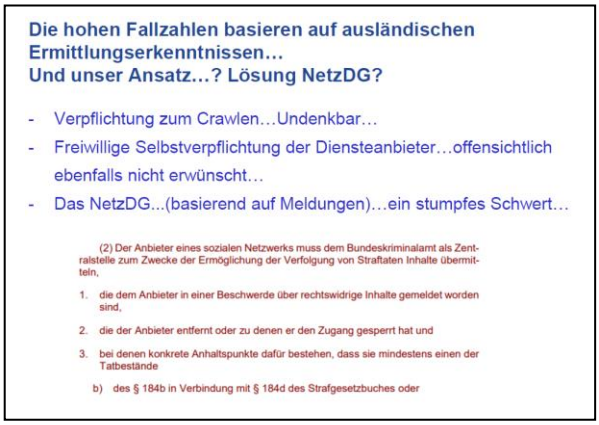
Der BKA-Präsident - auch das hat Frau Hermann schon aufgegriffen - hat interessanterweise eine ganz einfache Erklärung: Er sagt, es liegt an den von der halbstaatlichen US-Organisation „National Center for Missing and Exploited Children“ (NCMEC) gemeldeten Fällen. Diese Organisation nimmt Hinweise von großen amerikanischen sozialen Netzwerken entgegen, die eine freiwillige Selbstverpflichtung eingegangen sind,

Diese Netzwerke durchsuchen ihre gesamten Datenbestände mittels Crawling über sogenannte HashSets nach kinderpornografischem Material, sortieren die Ergebnisse nach Ländern und geben die Daten dann an das NCMEC weiter, das daraus den NCMEC-Report gießt. Dieser Report wird dann zu Strafverfolgungszwecken an die jeweiligen Länder gegeben.

Der BKA-Präsident sagt aber noch mehr: Die technischen Verfahren zur Identifizierung von Kinderpornografie im Netz seien immer besser geworden, und - das ist auch ganz interessant - die internationale Kooperation werde enger. Es sei außerdem zu erwarten, dass die Zahlen ab dem Jahr 2022 wegen einer anstehenden Hinweispflicht für IT-Konzerne noch stärker ansteigen werden.

Eigentlich haben wir es also den Amerikanern zu verdanken, dass unsere Zahlen ansteigen, weil die ihre Arbeit besser machen können als wir.

Auf der Folie ist ein standardisierter CyberTipline Report, wie er bei uns ankam, zu sehen. Dass die Masse unserer Verfahren auf Hinweisen basiert, die uns von Amerika sozusagen über den Zaun geworfen werden, ist eigentlich ein Armutszeugnis für uns.



Was ist unser Ansatz, um das Problem in den Griff zu bekommen? Wer schon so lange wie ich im Geschäft ist, weiß, dass es mal eine Bemühung des BKA gegeben hat, die kläglich gescheitert ist.

Sie erinnern sich vielleicht noch an den Begriff „Zensursula“ - ich glaube, es gab auch T-Shirts mit diesem Aufdruck. Ursula von der Leyen hatte sich für das sogenannte Access Blocking ausgesprochen, um den Zugang zu Seiten mit kinderpornografischen Inhalten einfach zu sperren. Selbst das stieß auf große Skepsis in der Netzgemeinde, wo man sich fragte, ob das die Vorbereitung zu einer allgemeinen Netzzensur sei. Das war nicht durchsetzbar.

Daher erscheint mir eine Verpflichtung der Provider, ihre Datenbestände im Hinblick auf Kinderpornografie zu crawlen, in der jetzigen politischen Lage eigentlich undenkbar zu sein. Auch eine freiwillige Selbstverpflichtung der Diensteanbieter - ähnlich dem amerikanischen Konzept, dem sich immer mehr soziale Netzwerke anschließen - ist offensichtlich ebenfalls nicht erwünscht.

Unsere Lösung ist eine ganz andere gewesen, nämlich das Netzwerkdurchsetzungsgesetz (NetzDG), das von Facebook und Google gerade vor dem Verwaltungsgericht Köln beklagt wird. Das NetzDG verpflichtet soziale Netzwerke, eingehende Hinweise auf kinderpornografische In-

halte zu überprüfen und - falls die Hinweise zutreffen sollten - diese an die Strafverfolgungsbehörden zu melden.

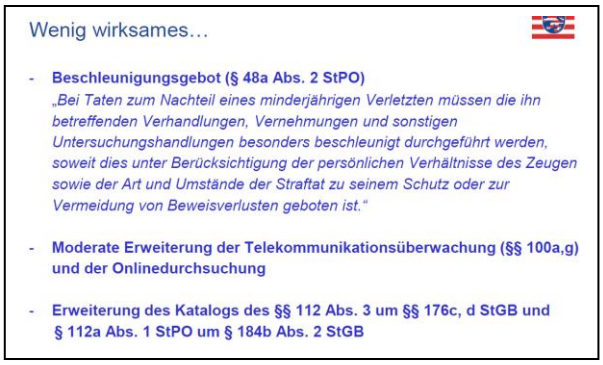
Allerdings muss das immer nur dann geschehen, wenn es Hinweise gibt. Das macht mich, ehrlich gesagt, sehr skeptisch. Die Verbreitung von Kinderpornografie findet in aller Regel nicht in offen zugänglichen Bereichen statt. Meistens sind das moderne, abgeschottete Kommunikationsstrukturen, die durch Keuschheitsproben abgesichert sind. Ich erwarte nicht, dass da wahnsinnig viel passieren wird.

Im Übrigen haben sehr viele Menschen auch Angst, eine derartige Mitteilung zu machen, weil sie befürchten, dann selber in den Fokus der Strafverfolgungsbehörden zu geraten. Das ist aus meiner Sicht also ein relativ schwaches Mittel.

Über das Gesetz zur Bekämpfung von sexualisierter Gewalt gegen Kinder, das am 1. Juli 2021 in Kraft getreten ist, habe ich schon kurz gesprochen. Meine Kollegin Frau Dr. Bussweiler war Sachverständige im Deutschen Bundestag. Dort ist das Gesetz von allen Seiten kritisiert worden. Es war gleich, ob die Sachverständigen aus dem medizinischen oder dem universitären Bereich kamen oder ob sie zur Strafverfolgung gehörten, alle haben es kritisiert. Genutzt hat all das überhaupt nichts.

Am Ende hat man marginale Änderungen vorgenommen, indem man nur sprachlich etwas geändert hat: Man hat aus „sexuellem Missbrauch“ „sexualisierte Gewalt“ gemacht und das Gesetz dann ansonsten völlig unverändert durchgewunken.

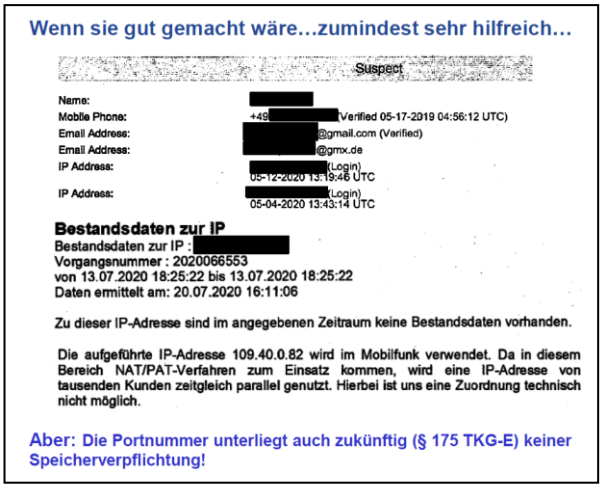
Beim materiellen Recht hat man hingegen ganz erhebliche Änderungen vorgenommen. Alles zählt nun als Verbrechen. Das bereitet uns erhebliche Probleme, da wir nun relativ geringfügige Straftaten mit erheblichem Ermittlungsaufwand verfolgen müssen.



Im Prozessrecht sind nur sehr überschaubare Änderungen vorgenommen worden. Es wurde ein Beschleunigungsgebot aufgenommen. Ehrlich gesagt, es sollte das Selbstverständnis eines jeden Staatsanwalts sein, dass sexueller Missbrauch und die Verbreitung von Kinderpornografie schnell beendet werden müssen. Das ist also eine sehr schwache Regelung.

Es gab außerdem noch eine moderate Erweiterung der Telekommunikationsüberwachung und der Onlinedurchsuchung sowie des Katalogs der Haftgründe in § 112 Abs. 3. Das ist alles, was im Prozessrecht verändert worden ist.

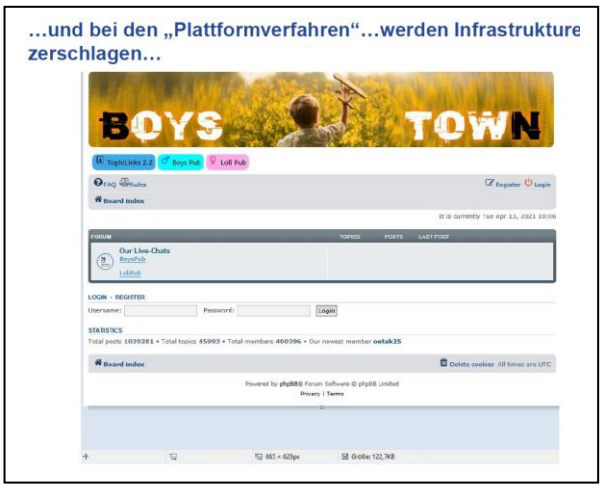
Wir haben es im vorherigen Vortrag schon gehört: Die Vorratsdatenspeicherung wäre super, die wünschen wir uns sehr. - Ich sage aber auch offen und ehrlich: In manchen Fällen ist sie wirksam, in anderen aber völlig unbrauchbar. Wenn Vorratsdatenspeicherung, dann so, dass man auch etwas mit ihr anfangen kann. Das sieht momentan tatsächlich ganz anders aus.



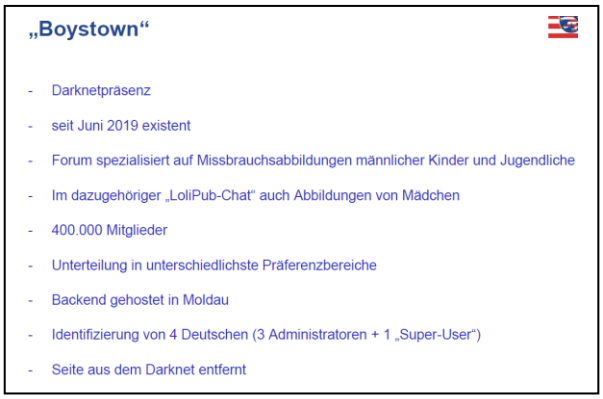
Auf der Folie sehen Sie einen Hinweis von NCMEC. Dort stehen der Name, die Mobilfunknummer, die E-Mail-Adresse und auch die IP-Adresse, die für den Login genutzt wurde. Wenn diese IP-Adresse beim zugehörigen Access-Betreiber abfragen, erhalten Sie in aller Regel genau die Auskunft, die Sie auf der Folie sehen können.

Die IP-Adresse kann keinem einzelnen Anschlussinhaber zugeordnet werden. Das liegt daran, dass eine IP-Adresse gleichzeitig an bis zu 60 000 Kunden vergeben wird. Die Zuordnung erfolgt über einen sogenannte Netzwerk-Port.

Die Portnummer hat niemals der Vorratsdatenspeicherung unterlegen, und nach § 175 TKG-E - das Telekommunikationsmodernisierungsgesetz, das am 1. Dezember 2021 in Kraft tritt - unterliegt sie auch zukünftig keiner Speicherverpflichtung. Das heißt, IP-Adressen können bei der Nutzung mobiler Endgeräte in aller Regel keinem Anschluss zugeordnet werden. In dieser Form ist die Vorratsdatenspeicherung also wirkungslos.



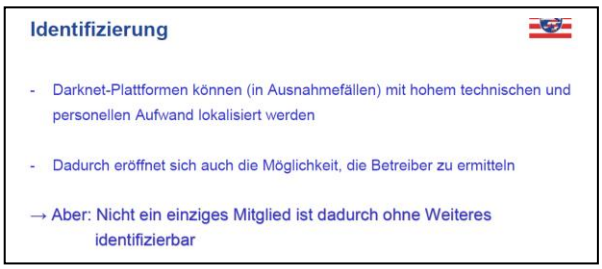
Auch das hat Frau Hermann angesprochen: Wir haben sehr viele Plattformverfahren geführt. Sie hat die älteren erwähnt. Ich habe hier ein Bild der neusten Plattform namens „Boystown". Alle Beschuldigten sitzen derzeit in U-Haft, einer wartet in Paraguay auf die Auslieferung.



Um die Dimension des Problems mit solchen Plattformen zu schildern, ist zu sagen, dass es sich um eine unglaublich schwer zu ermittelnde Darknet-Plattform handelt. Viele dieser Plattformen sind relativ jung, sie kommen schnell, und manchmal verschwinden sie auch wieder schnell, um woanders unter neuem Namen wiederaufzutauchen.

Bei „Boystown" geht es überwiegend um männliche Kinder und Jugendliche. Die Plattform hatte sage und schreibe 400 000 Mitglieder. In unseren ersten Verfahren gegen „Zauberwald" oder „Sonneninsel" ging es um 500 Mitglieder, und wir dachten damals, das sei viel. Es hat einen kontinuierlichen Anstieg gegeben. „Elysium" hatte, glaube ich, um die 100 000 oder 120 000 Nutzer. Nun sind wir bei 400 000 Nutzern, und die Zahlen steigen munter weiter.

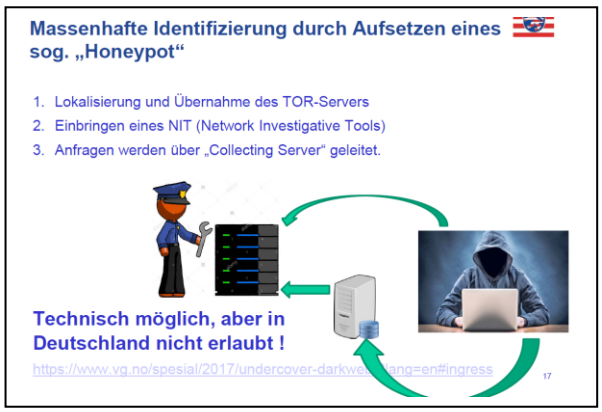
Die Seite wurde auf Servern in der Republik Moldau betrieben, weshalb es ein paar Probleme mit der Serverabschaltung gegeben hat. Wir haben vier Deutsche Mitbetreiber - drei Administratoren und einen Superuser - identifizieren und die Seite aus dem Darknet entfernen können.



Es hört sich immer so toll an, wenn in der Presse von solchen Erfolgen berichtet wird: Infrastruktur zerschlagen! Betreiber festgenommen! - Ich möchte an dieser Stelle aber bei der Wahrheit bleiben: In Ausnahmefällen können wir solche Darknet-Plattformen lokalisieren, und wir können versuchen, die Betreiber zu identifizieren. Wenn wir Glück haben, können wir diese Darknet-Plattformen auch aus dem Internet entfernen.

Aber wir können kein einziges Mitglied ohne Weiteres durch solche Maßnahmen identifizieren. Ganz Im Gegenteil: Wenn die Seite vom Netz genommen wird, haben wir erst einmal keinen Ermittlungsansatz mehr. Das ist ein riesiges Problem. Das heißt, wir haben 400 000 Nutzer - darunter eine Vielzahl von Missbrauchstätern -, die wir nicht identifizieren können.

In der Zeit, in der wir die Betreiber identifizieren, konzentrieren wir uns auf die sogenannten High-Value-Targets - die Verursacher von ganz schwerem Missbrauch -, um diese aus dem Verkehr zu ziehen. Gleichwohl ist es unglaublich frustrierend, wenn Sie am Ende des Tages vielleicht zehn Personen identifizieren konnten und wissen, es gibt noch 399 990, die Ihnen gerade durch die Lappen gegangen sind.



Hätten wir hier eine Möglichkeit zur Identifizierung? - Ich sage: Ja, die hätten wir. Wir könnten eine massenhafte Identifizierung aber nur dann durchführen, wenn wir einen sogenannten Honeypot aufsetzen würden. Dafür müssten wir den TOR-Server, auf dem die Plattform gehostet ist, übernehmen. Das könnten wir problemlos, indem wir Rechtezugriff auf dem Board erlangen, was in aller Regel möglich ist.

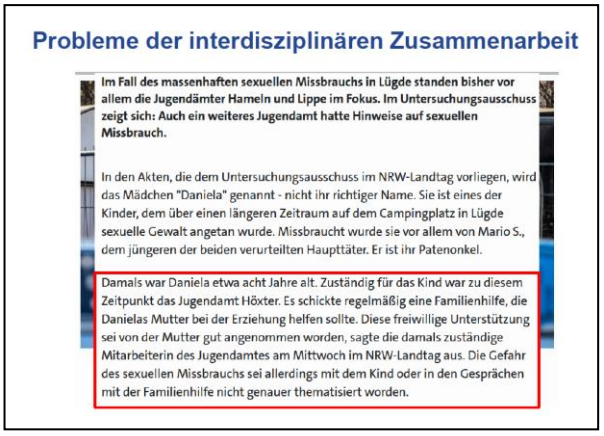
Der böse Bube sitzt an seinem Rechner, greift auf den TOR-Server zu, der vom Polizeibeamten übernommen wurde. Dieser nimmt den großen Schraubenschlüssel und fummelt ein bisschen Technik hinein. Wenn der Server des Users dann mit dem Server kommuniziert, bemerkt dieser nicht, dass er auf einem sogenannten Collecting Server der Strafverfolgungsbehörden läuft.

Das hört sich unglaublich kompliziert an. Bei sexuellem Missbrauch und bei der Verbreitung von Kinderpornografie ist dieses Verfahren strafbar. Wir haben es aber tatsächlich einmal beim Kauf von Daten ausprobiert. Gemeinsam mit dem BKA habe ich vor Jahren ein solches Board ersteigert, um die technischen Möglichkeiten auszuprobieren. Und siehe da: Nach kurzer Zeit hatten wir alle Nutzer identifiziert.

In Deutschland ist der Honeypot ein No-Go, in anderen Ländern - auch Länder wie die Niederlande, Italien oder Australien, die wir ganz sicher nicht als „Unrechtsstaaten“ bezeichnen würden - ist das Mittel gang und gäbe, um Mitglieder dieser Boards zu identifizieren. Man sollte ehrlicherweise mal darüber nachdenken, dass wir in diesem Bereich nicht immer nur die Profiteure von ausländischen Ermittlungen sein können, sondern möglicherweise auch mal selbst tätig werden sollten.

Julia Bussweiler: Ich knüpfe ebenfalls an das an, was unsere Vorrednerinnen aus Niedersachsen schon gesagt haben, indem ich jetzt auf Fragen der interdisziplinären Zusammenarbeit eingehe.

Ich führe hierfür beispielhaft den Fall Lügde an, der uns allen noch sehr präsent sein dürfte. Wenn man sich die öffentlichen Berichte über den Fall anschaut, sieht man die Probleme, die ich ansprechen will, schon relativ gut.



Probleme der interdisziplinären Zusammenarbeit

Im Fall des massenhaften sexuellen Missbrauchs in Lügde standen bisher vor allem die Jugendämter Hameln und Lippe im Fokus. Im Untersuchungsausschuss zeigt sich: Auch ein weiteres Jugendamt hatte Hinweise auf sexuellen Missbrauch.

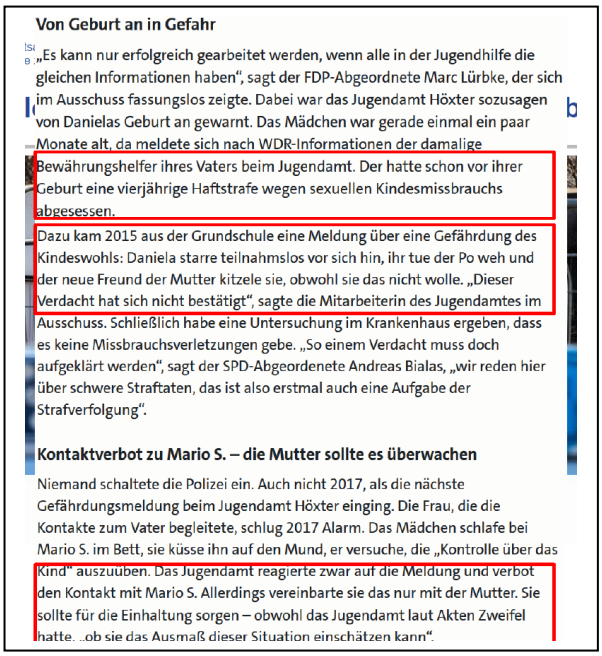
In den Akten, die dem Untersuchungsausschuss im NRW-Landtag vorliegen, wird das Mädchen "Daniela" genannt - nicht ihr richtiger Name. Sie ist eines der Kinder, dem über einen längeren Zeitraum auf dem Campingplatz in Lügde sexuelle Gewalt angetan wurde. Missbraucht wurde sie vor allem von Mario S., dem jüngeren der beiden verurteilten Haupttäter. Er ist ihr Patenonkel.

Damals war Daniela etwa acht Jahre alt. Zuständig für das Kind war zu diesem Zeitpunkt das Jugendamt Höxter. Es schickte regelmäßig eine Familienhilfe, die Danielas Mutter bei der Erziehung helfen sollte. Diese freiwillige Unterstützung sei von der Mutter gut angenommen worden, sagte die damals zuständige Mitarbeiterin des Jugendamtes am Mittwoch im NRW-Landtag aus. Die Gefahr des sexuellen Missbrauchs sei allerdings mit dem Kind oder in den Gesprächen mit der Familienhilfe nicht genauer thematisiert worden.

In diesem Artikel wird der Fall eines der Opfer - ein achtjähriges Mädchen - aufgearbeitet.

> „Damals war Daniela etwa acht Jahre alt. Zuständig für das Kind war zu diesem Zeitpunkt das Jugendamt Höxter. Es schickte regelmäßig eine Familienhilfe, die Danielas Mutter bei der Erziehung helfen sollte. Diese freiwillige Unterstützung sei von der Mutter gut angenommen worden, sagte die damals zuständige Mitarbeiterin des Jugendamtes am Mittwoch im NRW-Landtag aus."

Man sei sich sicher gewesen, das Problem gut in den Griff zu bekommen. Später sind noch andere Stellen hinzugezogen worden, da es Hinweise darauf gab, dass eine Gefährdung des Kinds bestehen könnte.



Von Geburt an in Gefahr

„Es kann nur erfolgreich gearbeitet werden, wenn alle in der Jugendhilfe die gleichen Informationen haben", sagt der FDP-Abgeordnete Marc Lürbke, der sich im Ausschuss fassungslos zeigte. Dabei war das Jugendamt Höxter sozusagen von Danielas Geburt an gewarnt. Das Mädchen war gerade einmal ein paar Monate alt, da meldete sich nach WDR-Informationen der damalige Bewährungshelfer ihres Vaters beim Jugendamt. Der hatte schon vor ihrer Geburt eine vierjährige Haftstrafe wegen sexuellen Kindesmissbrauchs abgesessen.

Dazu kam 2015 aus der Grundschule eine Meldung über eine Gefährdung des Kindeswohls: Daniela starre teilnahmslos vor sich hin, ihr tue der Po weh und der neue Freund der Mutter kitzele sie, obwohl sie das nicht wolle. „Dieser Verdacht hat sich nicht bestätigt", sagte die Mitarbeiterin des Jugendamtes im Ausschuss. Schließlich habe eine Untersuchung im Krankenhaus ergeben, dass es keine Missbrauchsverletzungen gebe. „So einem Verdacht muss doch aufgeklärt werden", sagt der SPD-Abgeordenete Andreas Bialas, „wir reden hier über schwere Straftaten, das ist also erstmal auch eine Aufgabe der Strafverfolgung".

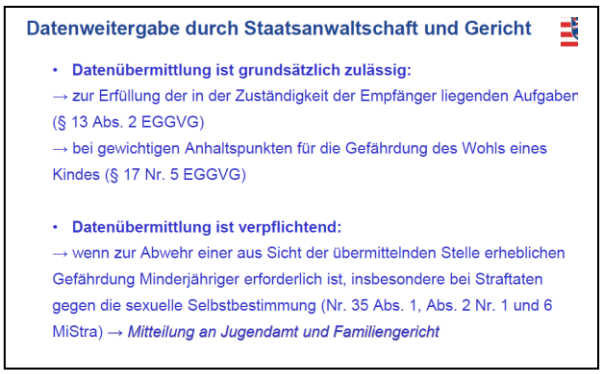
Kontaktverbot zu Mario S. – die Mutter sollte es überwachen

Niemand schaltete die Polizei ein. Auch nicht 2017, als die nächste Gefährdungsmeldung beim Jugendamt Höxter einging. Die Frau, die die Kontakte zum Vater begleitete, schlug 2017 Alarm. Das Mädchen schlafe bei Mario S. im Bett, sie küsse ihn auf den Mund, er versuche, die „Kontrolle über das Kind" auszuüben. Das Jugendamt reagierte zwar auf die Meldung und verbot den Kontakt mit Mario S. Allerdings vereinbarte sie das nur mit der Mutter. Sie sollte für die Einhaltung sorgen – obwohl das Jugendamt laut Akten Zweifel hatte, „ob sie das Ausmaß dieser Situation einschätzen kann".

Ein Bewährungshelfer des Vaters ist beim Jugendamt vorstellig geworden. Später wurde von der Grundschule eine Mail wegen des auffälligen Kinds geschickt, in der stand, Daniela sei teilnahmslos und würde darüber berichten, dass ihr Po wehtue und der neue Freund der Mutter sie kitzeln würde, obwohl sie das nicht wolle.

Später wurde versucht, den Kontakt zum Täter zu unterbinden. Man hat wohl größtenteils darauf gesetzt, dass die Mutter überwacht, ob es tatsächlich auch zur Umsetzung des Kontaktverbots kommt. Die Polizei wurde darüber allerdings nicht informiert.

Ich glaube, dieser kurze Abriss zeigt das Problem auf, dass vorhin schon von meinen Vorrednerinnen geschildert wurde: Die Informationen, die wir benötigen, um solche Missbrauchsfälle zeitnah und zuverlässig aufzuklären, bekommen wir häufig nicht frühzeitig genug und manchmal auch gar nicht.



Datenweitergabe durch Staatsanwaltschaft und Gericht

- **Datenübermittlung ist grundsätzlich zulässig:**

→ zur Erfüllung der in der Zuständigkeit der Empfänger liegenden Aufgaben (§ 13 Abs. 2 EGGVG)

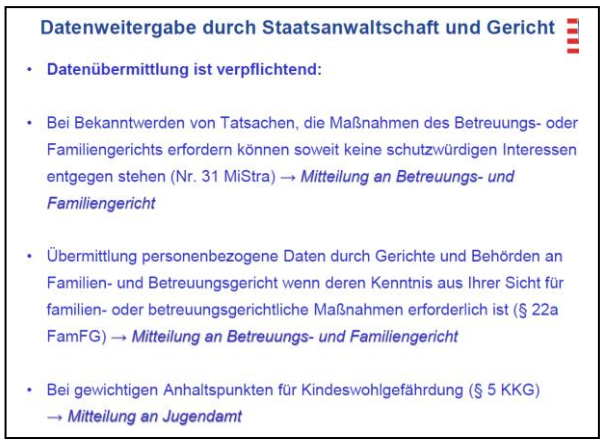
→ bei gewichtigen Anhaltspunkten für die Gefährdung des Wohls eines Kindes (§ 17 Nr. 5 EGGVG)

- **Datenübermittlung ist verpflichtend:**

→ wenn zur Abwehr einer aus Sicht der übermittelnden Stelle erheblichen Gefährdung Minderjähriger erforderlich ist, insbesondere bei Straftaten gegen die sexuelle Selbstbestimmung (Nr. 35 Abs. 1, Abs. 2 Nr. 1 und 6 MiStra) → *Mitteilung an Jugendamt und Familiengericht*

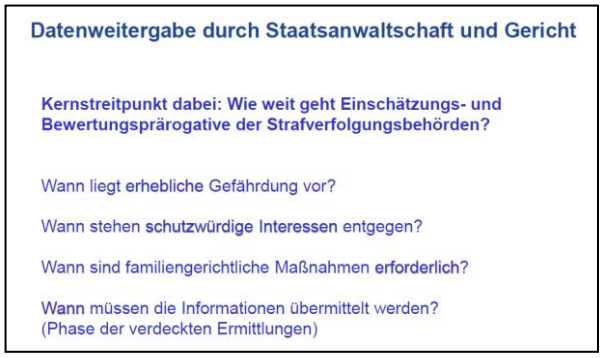
Ich habe die verschiedenen Vorschriften rausgesucht, die die einzelnen Stellen verpflichten, Informationen weiterzugeben.

Für Staatsanwaltschaften und Gerichte sind einige Informationen vorhanden. Grundsätzlich ist die Datenübermittlung zulässig. In bestimmten Fällen ist sie sogar geboten - insbesondere dann, wenn es Hinweise auf eine erhebliche Kindeswohlgefährdung gibt und Straftaten gegen die sexuelle Selbstbestimmung im Raum stehen. Dann muss man das an das Jugendamt und an das Familiengericht weitergeben.



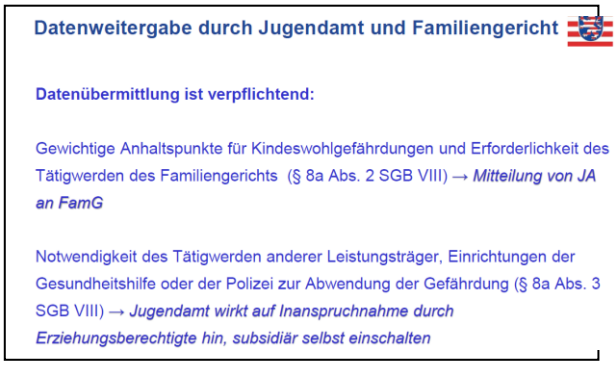
Das ist ebenso der Fall, wenn man Hinweise darauf hat, dass das Betreuungs- oder Familiengericht tätig werden müssen, weil z. B. ein Sorgerecht entzogen werden oder eine Inobhutnahme stattfinden muss. Auch das muss man weitergeben - das ist alles über die Mitteilungspflicht in Straf- und Bußgeldsachen geregelt. Man muss alle Informationen, die für die Umsetzung solcher Maßnahmen erforderlich sind, weiterleiten.

Seit Juni dieses Jahres ist in § 5 KKG noch einmal klargestellt, dass bei gewichtigen Anhaltspunkten für Kindeswohlgefährdung von Staatsanwaltschaft und Gericht eine Mitteilung an das Jugendamt zu machen ist.

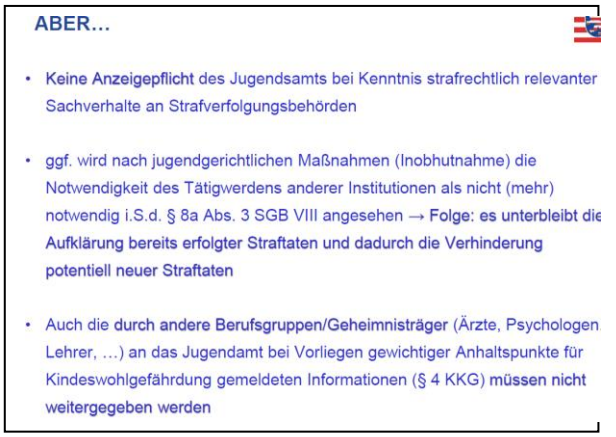


Bestehende Streitpunkte sind: Geht die Einschätzungsprägorative zu weit? Wann liegt eine erhebliche Gefährdung vor? Wann sprechen schutzwürdige Interessen gegen eine Datenweitergabe? Wann sind familiengerichtliche Maßnahmen erforderlich? Zu welchem Zeitpunkt ist eine Mitteilung zu machen? - Letzteres ist manchmal ein Streitpunkt; denn in manchen Fällen werden verdeckte Ermittlungen geführt. In Fällen von andauerndem sexuellem Missbrauch sind das in der Regel aber keine langen Phasen, denn da kann keiner einfach nur zusehen.

Diese Streitpunkte gibt es zwar, aber *dass* entsprechende Mitteilungen gemacht werden müssen, ist unstrittig.



Man kann die Frage auch umdrehen: Wann kriegen wir Mitteilungen von den entsprechenden Institutionen? - Nach § 8 a Abs. 2 SGB VIII gibt es eine Mitteilungspflicht der Jugendämter an die Familiengerichte, wenn das Einschalten des Familiengerichts erforderlich ist. Das ist z. B. der Fall, wenn die elterliche Sorge vernachlässigt wird oder bestimmte Maßnahmen zum Schutz des Kindes zu treffen sind. Es ist auch der Fall, wenn das Tätigwerden anderer Leistungsträger als erforderlich erachtet wird. Dann soll das Jugendamt darauf hinwirken, dass die Erziehungsberechtigten das in Anspruch nehmen. Wenn sie das nicht tun, darf das Jugendamt tätig werden.



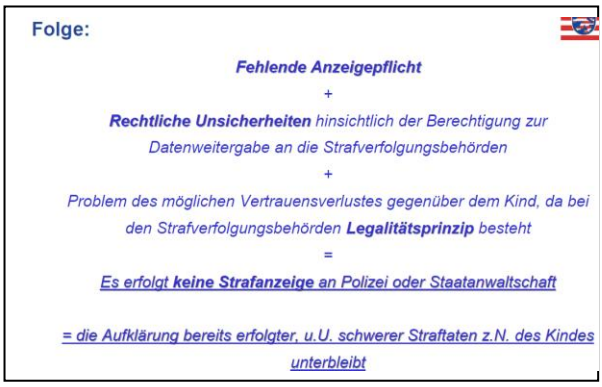
Aus meiner Sicht ist das alles im Gesetz sehr schwammig geregelt. Deswegen wundert es mich nicht, dass ich bei Veranstaltungen, bei denen verschiedene Berufsgruppen zusammenkommen, regelmäßig von Mitarbeitenden aus Jugendämtern angesprochen werde, die zum Teil sehr gerne Informationen weitergeben möchten, aber unglaublich unsicher sind, was sie eigentlich weitergeben dürfen.

Es gibt keine Anzeigepflicht - sei es durch Jugendämter oder durch andere -, die besagt, dass

man den Strafverfolgungsbehörden entsprechende Informationen, über die man Kenntnis hat, weitergeben muss, damit sie ihre Arbeit machen können. Möglicherweise denken Mitarbeitende bei Jugendämtern auch, dass das nicht mehr notwendig ist, wenn sie ihre Maßnahmen aktiviert haben, weil die Gefahr dann gebannt ist. Vielleicht gehen da auch einfach die Einschätzungen der Situation auseinander.

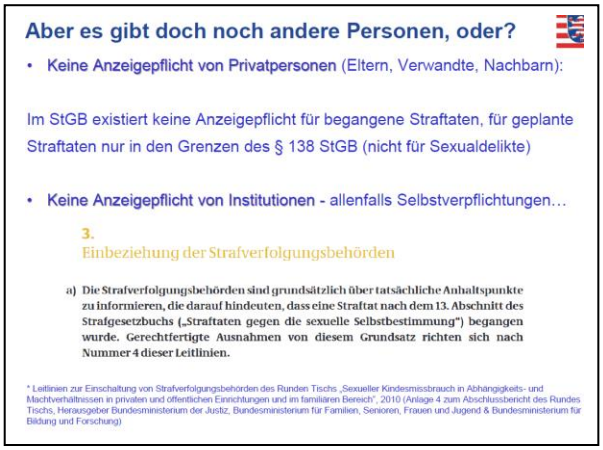
Zwar gibt es eine Meldepflicht für die Geheimnisträger, diese Informationen gelangen in der Regel aber nur bis zu den Jugendämtern und nicht bis zu uns.

Ich sehe hier also eine unglaublich starke Unklarheit. Es gibt keine Anzeigepflicht, und es gibt rechtliche Unsicherheiten vonseiten der Verwaltung des Jugendamts darüber, was überhaupt weitergegeben werden darf.



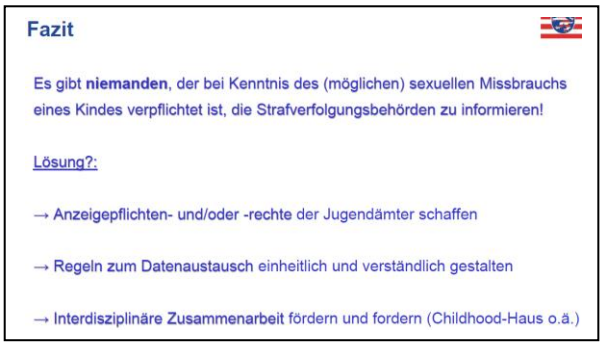
Natürlich unterscheiden sich die Aufgaben der Institutionen. Wir haben die Aufgabe, Straftaten aufzuklären und Straftäter zur Verantwortung zu ziehen, während beim Jugendamt natürlich das Kindeswohl im Mittelpunkt steht. Zum Teil bestehen dort Unsicherheiten darüber, inwiefern es dem Kind womöglich mehr schaden könnte, die entsprechenden Informationen an uns weiterzugeben, weil wir uns bei Straftaten natürlich nicht aussuchen können, ob wir was machen oder nicht.

In der Folge wird häufig keine Anzeige erstattet. Straftaten werden dann zum Nachteil des Kindes nicht aufgeklärt, und mögliche weitere nicht verhindert.



Nun könnte man überlegen, ob uns Informationen von anderen Personen erreichen, wenn uns die Jugendämter nicht informieren. - Das wäre schön, aber auch für Privatpersonen gibt es keine Anzeigepflicht. Eine Anzeigepflicht für bereits begangene Straftaten gibt es gar nicht, und für geplante Strafteten gibt es sie nur im bestimmten Katalog des § 138 StGB, wo Sexualstraftaten nicht vorkommen. Insofern ist es mitnichten so, dass Privatpersonen - seien es Angehörige, Nachbarn oder andere - Strafanzeige erstatten.

Auch Institutionen tun das nicht, denn auch hier gibt es allenfalls eine Selbstverpflichtung. Es existiert eine Leitlinie darüber, wann man eine Strafverfolgungsbehörde einschalten könnte. Wir wissen aus zahlreichen Erkenntnissen und Medienbeiträgen, dass das nicht immer für bare Münze genommen wird, weshalb nicht immer Strafanzeige erstattet wird.



Insofern lautet das sehr traurige Fazit, dass niemand dazu verpflichtet ist, den sexuellen oder möglichen sexuellen Missbrauch eines Kindes anzuzeigen, wenn er Kenntnis von ihm hat.

Ich persönlich denke, dass es ganz klare Regelungen zur Lösung dieses Konflikts geben muss. Es gibt verschiedene Möglichkeiten. Man kann z. B. Handlungsanleitungen geben.

Ich persönlich als Strafverfolgerin würde mir eine Anzeigepflicht wünschen, oder - wenn man davor zurückschreckt - zumindest eine klare Definition, die besagt, dass die Jugendämter berechtigt sind, die Daten weiterzugeben, und dass ein gebundenes Ermessen besteht, sodass sie Anhaltspunkte für sehr schwere Missbrauchshandlungen weitergeben müssen. Diese Regeln müssten ganz klar und verständlich formuliert sein.

Außerdem ist interdisziplinäre Zusammenarbeit zu fördern und zu fordern. Als aktuelles Beispiel hierfür kann ein Childhood-Haus-Projekt in Hessen genannt werden, das wir gerade ins Leben rufen. Mein Wunsch ist es - ich hoffe, das lässt sich umsetzen -, dass solche interdisziplinäre Zusammenarbeit gestärkt wird, sodass man sich vernetzt und Informationen, die notwendig sind, um schwerste Straftaten zum Nachteil von Kindern zu verfolgen und zu ahnden, ausgetauscht werden können.

Landeskriminalamt Niedersachsen

Schriftliche Stellungnahme: Vorlage 46
Präsentationsgrafiken: 1. Nachtrag zu Vorlage 46

***Anwesend**:*

***Francesco Hartmann**, Kriminalrat*

Francesco Hartmann: In meiner Funktion als Leiter der Aufgabenbereiche Cybercrime und Kinderpornografie im LKA Niedersachsen habe ich im letzten Jahr die Aufgabe gehabt, die kriminalpolizeiliche Bearbeitung der Kinderpornografie in der gesamten Polizei Niedersachen einer Revision zu unterziehen, die im Dezember 2020 abgeschlossen werden konnte.

Somit habe ich nunmehr schon zwei Jahre lang tiefgreifende Erfahrungen hinsichtlich der Handlungsnotwendigkeiten in diesem Deliktbereich gesammelt. Aus dieser Erfahrung heraus möchte ich auf die von Ihnen übermittelten Unterthemen eingehen.

Es wird Überschneidungen zu den Ausführungen der Generalstaatsanwaltschaft Frankfurt am Main und der Staatsanwaltschaft Hannover geben.

Der Kindesmissbrauch im digitalen Raum ist in allen sozialen Medien zu finden - in den sehr bekannten wie Facebook, YouTube und Twitter, aber auch in Messengern wie WhatsApp und auf kleineren Plattformen wie Houseparty, Signal usw. Dort finden Straftaten wie Cyber-Grooming - wozu heute schon vorgetragen wurde -, sexuelle Belästigung und die Verbreitung von Kinderpornografie statt.

Vor einigen Jahren hat die Polizei noch selbst anlassunabhängig im Netz nach solchen Inhalten gesucht. Im Jahr 2021 muss die Polizei nicht mehr nach Kinderpornografie suchen, um sie bekämpfen zu können. Das liegt vor allem daran, dass externe Stellen - allen voran die US-amerikanische Organisation NCMEC, über die heute auch schon gesprochen wurde - entsprechende Hinweise über das BKA und die LKAs den niedersächsischen Polizeidienststellen zuleiten.

Im digitalen Raum bieten sich für pädosexuelle Täter alle nur denkbaren Konsummöglichkeiten. Selbst speziell hergestelltes, auf die individuellen Wünsche zugeschnittenes Material ist dort zu bekommen. Stellen Sie sich das aber bitte nicht wie in einem öffentlichen Videoverleih vor, wo das Material angeklickt und runtergeladen werden kann. Wir werden keinen Betreiber ohne Weiteres identifizieren und keine Plattformen aus Gründen der Gefahrenabwehr schließen können.

User registrieren sich für den Konsum nicht. Das Darknet ist technisch darauf ausgelegt, absolute Anonymität zu gewähren. In diesem Raum können die Täter agieren und sich frei bewegen.

Der Anteil kommerzieller Verbreitung ist statistisch nicht erfasst. Strafrechtlich wird bei der Art der Verbreitung nicht differenziert. Insofern wissen wir auch nicht, wie viel von dem Material zum Kauf angeboten wird. Nach polizeilicher Erfahrung ist dieser Anteil aber verhältnismäßig gering. In aller Regel wird das Material zum Tausch angeboten - auch das haben wir schon gehört. Das Einbringen eigenen Materials - eigener Fotos und Videos - dient dazu, überhaupt einen Zugang zu den einschlägigen Plattformen zu bekommen. Das ist die sogenannte Keuschheitsprobe.

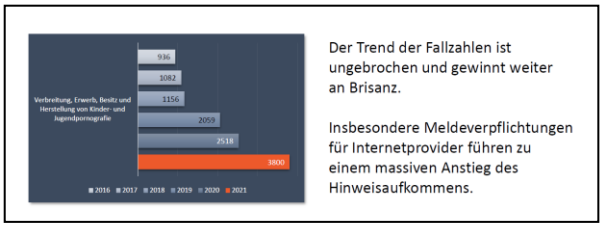
Insofern würde ich die kommerzielle Verbreitung aus polizeilicher Sicht gar nicht besonders problematisieren. Zumindest aus Opfersicht ist es dringlicher, zu verhindern, dass die Täter an das Material gelangen, indem sie dafür mit weiterem Material - das also extra noch herzustellen ist - bezahlen, statt mit Geld.

Cyber-Grooming meint Anbahnungsversuche zum sexuellen Missbrauch. Diese nehmen stetig zu. Nach unseren Erkenntnissen aus der polizeilichen Kriminalstatistik fand ein Anstieg von 300 Taten im Jahr 2015 auf 600 Taten im Jahr 2020 statt. Die Aussagekraft dieser Statistik ist allerdings begrenzt, weil hier immer nur das strafrechtlich höherwertige Delikt gezählt wird. Wenn es also nach einer solchen Anbahnung zu einem sexuellen Missbrauch kam, wird dieser, aber nicht die Anbahnung statistisch erfasst. Insofern müssen wir davon ausgehen, dass die Zahl der tatsächlichen Anbahnungsversuche größer ist als die von uns gezählten 600 Taten aus dem vergangenen Jahr.

Dieses Tätervorgehen findet überall dort statt, wo es eine Kontaktmöglichkeit über Medien gibt. Das sind wieder die etablierten Social-Media-Plattformen, aber eben auch auf den ersten Blick ungefährlich erscheinende Seiten, in den Kommentarbereichen von Onlinespielen oder auf Verkaufsplattformen wie eBay, Vinted usw.

Hier ist die Polizei tatsächlich auf die Anzeigebereitschaft der Opfer angewiesen. Die Anzeige muss zeitnah erfolgen, damit die notwendigen Ermittlungsmaßnahmen ergriffen werden können, um die Täter zu identifizieren. Auch hier ist die Vorratsdatenspeicherung das Stichwort.

Positiv ist zu nennen, dass es durchaus Präventionsansätze gibt. Die Tätermuster sind bekannt. Das Vorgehen ist immer ähnlich: Es beginnt subtil und freundlich mit der Kontaktaufnahme, bei der die Kinder zu ihrem Alter und zu ihrer Person ausgefragt werden. Dann folgen Aufforderungen, den öffentlichen Chatbereich zu verlassen und in einen privaten zu wechseln. Dann werden sie gebeten, die Webcam einzuschalten. Die des Täters bleibt in der Regel aber aus, wofür bestimmte Begründungen vorgetragen werden. Die Eltern sollen nicht von den Kindern darüber informiert werden. Sie sollen von sich selbst gemachte Bilder und Videos übermitteln. All diese Dinge sind bekannt, und insofern lassen sich potenzielle Opfer durchaus sensibilisieren.



Beim letzten Mal - in der 14. Kommissionssitzung - haben Dr. Lars Wistuba und ich bereits die besorgniserregende Entwicklung der Fallzahlen aufgezeigt. Hier können Sie noch einmal den Anstieg von 2019 sehen, der einen deutlichen Ausbruch aus dem vorherigen stetigen Anstieg markiert. Hier sehen Sie die Zahlen von Niedersachsen. Die Zahlen des Bundes - rund 18 000 Fälle im vergangenen Jahr - sind Ihnen heute schon vorgestellt worden.

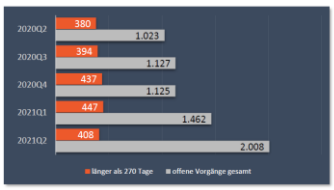
Zur Einordnung der niedersächsischen Zahlen: Niedersachsen rangiert auf Platz 4 der Fallzahlen. Das viel wichtigere Ergebnis ergibt sich für mich aber, wenn man diese Zahl in Relation zur Einwohnerzahl setzt. Bei den Fällen pro 100 000 Einwohnern ist Niedersachsen im negativen Sinne führend, hier gibt es also die meisten Fälle in Relation zur Einwohnerzahl.

Zu 2021 kann ich Ihnen noch keine abschließenden Zahlen liefern, weil viele Fälle derzeit noch ausgewertet werden und demnach noch nicht statistisch erfasst sind. Die Hinweise des NCMEC - die den größten Teil zum Fallaufkommen beisteuern - erlauben eine erste vorsichtige Prognose. Selbst bei zurückhaltender Schätzung gehen

wir davon aus, dass die Fallzahlen 2021 noch einmal um mehr als 50 % gegenüber den Zahlen des vergangenen Jahrs ansteigen werden.

Einem derartigen Anstieg der Fallzahlen - das ist bei der Polizei nicht anders als bei der Justiz - muss mit entsprechend hohen personellen Ressourcen entgegengetreten werden, denn diese Fälle müssen nun bearbeitet werden.

Wir gehen von weiteren Anstiegen über das Jahr 2021 hinaus aus. Auch in Europa wird der Gesetzgeber ab nächstem Jahr Internetprovider nach dem Vorbild des NCMEC mit einer Meldeverpflichtung belegen. Über diesen Weg werden wir weitere Hinweise und auszuwertende Daten erhalten. Wie wir im Juni schon aufgezeigt haben, wird die Trendkurve aktuell immer steiler, was sich in den kommenden Jahren fortsetzen wird.



Schwerpunktbildungen in der Polizei Niedersachsen unter Ausschöpfung der verfügbaren Sach- und Personalmittel geraten an ihre Grenzen.

Mit dieser Grafik möchte ich Ihnen zeigen, dass die Polizei Niedersachsen große Anstrengungen unternimmt, um das Fallaufkommen zu bewältigen. Bei der letzten Anhörung haben wir schon beschrieben, dass die Bearbeitung eines Vorgangs mehrere Monate in Anspruch nimmt. Ungefähr 3 800 solcher Vorgänge haben wir dieses Jahr zu bearbeiten.

Entsprechend der im Rahmen der Revision der Polizei Niedersachsen festgestellten Optimierungsmöglichkeiten setzen wir in diesem Deliktsbereich vermehrt Personal ein. Vor allem tun wir das nun hauptamtlich. In der Vergangenheit ist es eher nebenamtlich gewesen. Wir zentralisieren die Sachbearbeitung in den Polizeiinspektionen und erhoffen uns davon weitere Synergie- und Effizienzeffekte.

Darüber hinaus verweise ich an dieser Stelle auf den Abschlussbericht, der der Kommission vorliegt. Sie dürfen davon ausgehen, dass wir versuchen, sämtliche dort genannten Handlungsempfehlungen umzusetzen. Mit dieser Kraftanstrengung gelingt es uns aktuell noch, die Vorgänge, die bei uns in der Polizei länger als ein dreiviertel Jahr in Bearbeitung sind - sie sind auf der Folie als die orangen Balken dargestellt -, auf einem Level von ca. 400 zu halten.

Die Gesamtzahl der offenen Vorgänge - also alle Akten, die bei den Polizistinnen und Polizisten auf den Schreibtischen liegen - schnellt in die Höhe. Aktuell sind es etwa 2 000 Vorgänge, während wir vor einem Jahr noch etwa 1 000 Vorgänge auf den Schreibtischen liegen hatten. Obwohl wir uns auf die Vorgänge fokussieren, deren Auswertung mehrere Monate in Anspruch nimmt, werden wir die Arbeit mit dem uns möglichen Mitteleinsatz in absehbarer Zeit nicht schaffen, weil die Fallzahlen schneller anwachsen, als wir arbeiten können.

Wie gesagt, 400 Vorgänge sind ein dreiviertel Jahr lang in Bearbeitung. In einzelnen Fällen kommt es vor, dass wir in den Materialien Hinweise auf einen tatsächlich stattgefundenen oder stattfindenden Missbrauch finden. Es ist natürlich einleuchtend, dass mit der Zunahme der Fallzahlen auch die Wahrscheinlichkeit wächst, dass der Polizei solche Hinweise nominell zwar bekannt sind, während sie sie faktisch aber noch nicht in Augenschein nehmen konnte. Insofern muss es das Ziel sein, diese Zahl immer möglichst niedrig zu halten und dafür entsprechende Mittel einzusetzen.

Der digitale Raum darf nicht zu einem rechtsfreien Raum werden.

Ich sagte es schon: Die Strafverfolgungsbehörden müssen im Netz nicht mehr nach Kinderpornografie suchen. Das heißt in meinen Augen aber nicht, dass die Polizei nicht trotzdem im Netz präsent sein muss. Dass diese Ermittlungen noch nicht flächendeckend geführt werden - nicht in Niedersachsen und auch nicht bundesweit -, liegt an dem hohen Aufwand, von dem wir heute gehört haben.

Die Täter sitzen in aller Welt verteilt. Die Server befinden sich in aller Regel nicht in Deutschland. Wir brauchen internationale Zusammenarbeit. Wir brauchen Rechtshilfeverfahren. Um einen Server im Darknet aufspüren und übernehmen zu können, brauchen wir umfangreiche technische Überwachung. Vor allem brauchen die Ermittlerinnen und Ermittler einen herausragenden IT-Fachverstand. Der ist nicht jeder Polizeibeamtin

und jedem Polizeibeamten in Niedersachsen - und auch nicht in den anderen Bundesländern - gegeben. Wir brauchen also spezialisierte Personalbereiche.

Ab November 2021 werden wir ein Cybercrime-Team im LKA einsetzen. Das ist eine Organisationseinheit, die Initiativermittlungen im Darknet durchführen soll, um zu verhindern, dass sich das Darknet für Teile der Bevölkerung weiter zu einem rechtsfreien Raum entwickelt. Der Beginn dieser Entwicklung ist ja eigentlich schon abzusehen.

Ich schließe mich den Worten von Frau Hermann an: Wir müssen die Täterstrukturen aufbrechen, wir müssen Strukturermittlungen führen. Mit der Organisationseinheit im LKA gehen wir im übernächsten Monat einen ersten Schritt in diese Richtung.

Wenn wir im Jahr 2021 von Kinderpornografie sprechen, sprechen wir auch von zwei wesentlichen Herausforderungen für die Strafverfolgungsbehörden.

Die erste Herausforderung ist, den Strafverfolgungsdruck zu erhöhen. Die Täter dürfen sich in ihrem Tun nicht mehr sicher fühlen - nicht im normalen Internet, aber eben auch nicht im Darknet. Das ist eine anspruchsvolle Aufgabe, die einiges an Anstrengung erfordert.

Die zweite Herausforderung ist, dass Polizei und Justiz einen Weg finden müssen, die mit den Delikten einhergehenden Massendaten zu beherrschen. Ein naheliegender Weg hierfür ist eine technische Unterstützung durch - wie Sie es nennen - algorithmenbasierte Verfahren.

Hierfür könnten wir auf die großen Unternehmen wie Facebook gucken, die solche Verfahren natürlich schon seit Längerem Nutzen. Als Strafverfolgungsbehörde können wir uns das aber nicht einfach so zunutze machen. Weder sind diese Verfahren im Detail bekannt, noch werden sie von Facebook transparent gemacht.

Darüber hinaus - das nur am Rande - wissen wir auch nichts über die Zuverlässigkeit und Trefferquote dieser Verfahren. Jedenfalls müssen wir durchaus das ein oder andere vom dem, was durch NCMEC zu uns gelangt und - zumindest nach deutschem Recht - nicht strafrechtlich relevant sind, aussortieren. Wir brauchen also algorithmenbasierte Verfahren, die auch unserem Qualitätsanspruch gerecht werden, damit das, was wir technisch selektieren lassen, auch wirklich Kinderpornografie ist. Das ist die Herausforderung.

Insofern ergeben sich für die Polizei zwei Anwendungszwecke von algorithmenbasierten Verfahren. Das ist einmal die Suche nach entsprechenden Inhalten im Internet. Ich sagte schon, dass ich diese Notwendigkeit für Strafverfolgungsbehörden heute nicht mehr zwingend sehe. Der zweite und wesentliche Zweck ist die Reduzierung und Vorselektion der Daten, die uns schon vorliegen, weil wir sie von Externen übermittelt bekommen oder in überbordender Menge bei Durchsuchungen sicherstellt haben.

Eine solche technische Unterstützung ist für die Polizei unverzichtbar. Das heißt aber nicht, dass wir die manuelle Ermittlungsarbeit durch unser Personal damit ersetzen können werden. Die wird weiterhin stattfinden müssen.

Zusätzlich zur technischen Unterstützung müssen wir einen Weg finden, die Daten zu priorisieren. Unlängst ist hierzu - auch mit niedersächsischer Beteiligung - eine Bund-Länder-Projektgruppe eingerichtet worden, der auch ich beiwohnen werde. Dort werden wir uns mit den kriminalistischen Anforderungen einer solchen Auswertung von kinderpornografischen Daten befassen. Letztendlich wird festzulegen sein, wie die Auswertung begrenzt werden kann. Im Klartext heißt das: Welche der vielen Daten, die wir sichergestellt haben, gucken wir uns unter Umständen nicht an?

Das Bild der Lkw-Schlange soll noch einmal deutlich machen, wie notwendig eine solche Begren-

zung heutzutage - und in Zukunft noch mehr - ist. Beim letzten Mal haben wir Ihnen gesagt, dass wir im vergangenen Jahr 2,3 Petabyte an Daten allein aufgrund der Delikte der Kinderpornografie sichergestellt haben. Gerundet sind das 2,3 Milliarden Bilder. Damit verlangen wir den Polizistinnen und Polizisten ab, dass sie 245 solcher Vierzigtonner, vollbeladenen bis unters Dach, mit Fotokisten sichten, bewerten und kategorisieren. Um es noch ein bisschen plastischer zu machen: Das wäre ein Lkw-Stau von 4 km Länge. Ich glaube nicht, dass irgendjemand in analogen Zeiten eine solche Menge sichergestellt hätte. In der digitalen Zeit geht das sehr leicht. Es stellt sich die Frage, wie wir damit umgehen.

Insofern müssen wir uns für eine erfolgreiche Bekämpfung der Kinderpornografie zukünftig die rechtliche und auch moralische Frage stellen, wie viele Daten der Staat verarbeiten kann. Ich plädiere dafür, dass wir in dieser Frage ehrlich sind. Die Strafverfolgungsbehörden und die Politik sollten gegenüber der Gesellschaft transparent machen, was der Staat leisten kann. Zukünftig werden wir eben nicht mehr alle Bilder manuell auswerten können. Weder wird das im Bereich der Kinderpornografie gehen noch in den anderen Deliktsbereichen.

Jetzt komme ich auf die KI zu sprechen, die wir im LKA Niedersachsen entwickelt haben. Sie ist bereits ziemlich gut darin, pornografisches von nicht-pornografischem Material zu unterscheiden. Im nächsten Schritt muss sie aber auch kinderpornografisches Material von anderem pornografischem Material unterscheiden können. Dort liegt die Schwierigkeit, und wir werden feststellen, wie gut die Technik funktioniert bzw. wie hoch die Fehlerquote der KI ist. Die Fehlerquote des Menschen wird statistisch nicht erfasst. Der Mensch ist aber nicht fehlerfrei - weder bei der Auszählung von Stimmzetteln in Wahllokalen noch bei der Bearbeitung von Kinderpornografie. Ich erlaube mir aber die Bemerkung, dass bei der Bearbeitung von Kinderpornografie leichter Fehler gemacht werden können als bei der Auszählung von Stimmzetteln.

Der sexuellen Gewalt an Kindern im digitalen Raum will die Polizei Niedersachsen mit Initiativermittlungen und einer verantwortungsvollen Begrenzung der Massendaten begegnen.

Die KI ist derzeit die zukunftsgerichtete Alternative für die Begrenzung des Arbeitsaufkommens bei der Auswertung von Massendaten. Ressortübergreifend innerhalb der Polizei, aber auch politisch und mit der Gesellschaft werden wir eine Diskussion darüber führen müssen, welche Fehlerquote wir einer solchen Technologie zugestehen können und wollen. Um diese moralische Frage am Ende überhaupt stellen zu können, ist noch ein Weg zu beschreiten, denn diese KI muss noch finalisiert werden. Die dafür erforderliche Auswerteinfrastruktur muss erst aufgebaut werden, wofür finanzielle Mittel in nicht unerheblicher Menge gebraucht werden.

Die Zeit bis zu diesem Moment muss mit manueller Ausweitung überbrückt werden. Wir müssen also mehr Ermittlerinnen und Ermittler dafür einsetzen. Ich möchte mit dem Ergebnis schließen, zu dem ich in den vergangenen zwei Jahren immer wieder gekommen bin: Wollen wir Kinderpornografie wirklich effektiv im Zeitalter der Digitalisierung bekämpfen, dürfen wir die notwendigen finanziellen Investitionen nicht scheuen.

Microsoft Deutschland GmbH

Präsentationsgrafiken: Vorlage 48

***Per Videokonferenztechnik zugeschaltet**:*

- ***Jörg Bartholomy**, Client Technology Lead - Public Sector NRW*
- ***Mathias Göpel**, Senior Solution Sales - Azure AI, Data, Security - Public Sector*

Jörg Bartholomy: Ich bin für Microsofts Geschäft mit den öffentlichen Auftraggebern in Nordrhein-Westfalen zuständig. Das ist ein relativ großes Feld. Es umfasst Ministerien, Landesbehörden, Bezirksregierungen, die Kommunalebene und angeschlossene Eigenbetriebe. Mein Kollege Mathias Göpel ist Consulting-Spezialist und war federführend bei dem Projekt tätig, das ich Ihnen nun vorstellen darf.

Wir haben in dem vorherigen Vortrag bereits die Fallzahlen von Niedersachsen gesehen. Ich kann das bestätigen. Nach den Gesprächen, die wir mit

unseren Projektpartnern geführt haben, kann ich von ähnlichen Fallzahlen berichten.

Die Quelle dieser Zahlen seit 2018 ist die Polizeiliche Kriminalstatistik für NRW. Der Steigerungstrend, der für Niedersachsen zu sehen war, bildet sich in Nordrhein-Westfalen genauso ab. Genauso trifft das auf die sichergestellten Abbildungen von sexuellem Kindesmissbrauch zu.

Die Auswertung dieser Bilddateien alleine mit menschlichen Ressourcen stell eine große Herausforderung dar. Das ist de facto auch die Motivation für das Projekt gewesen, das wir gemeinsam mit unseren Partnern ins Leben gerufen haben. Wir wollen verifizieren, inwiefern KI in der Lage ist, dieses Problem sinnvoll zu verringern.

Hierbei ist natürlich zu berücksichtigen - Sie sehen es unter „04“ -, dass der Besitz, die Verbreitung und die Verarbeitung solcher Daten durch den Gesetzgeber als illegal eingestuft ist. Dass trifft auch auf die Firma Microsoft zu, die dieser Arbeit mit besten Intentionen nachgeht.

Die ZAC NRW war bei dem Projekt unter der Leitung von Oberstaatsanwalt Markus Hartmann federführend. Neben Microsoft waren insbesondere wissenschaftliche Berater der Rechtswissenschaftlichen Fakultät der Universität des Saarlandes beteiligt. Namentlich sind das Professor Dr. Dominik Brodowski und Professor Dr. Christoph Sorge gewesen. Sie haben uns während des gesamten Zyklus begleitet, um uns Hilfestellungen bei den Fragen zu geben, was im Rahmen unserer Vorhaben rechtlich machbar ist und wie wir sicherstellen können, dass die produzierten Ergebnisse gerichtsverwertbar sind.

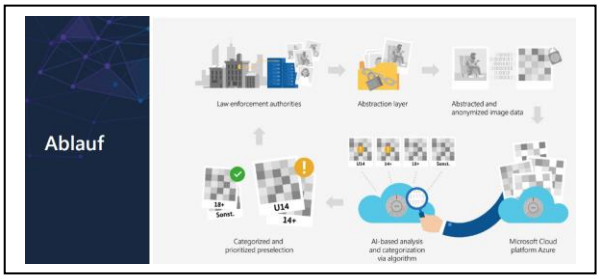
Das Ziel des Projekts war von vornherein, die Beweissicherung des umfangreichen Materials deutlich zu beschleunigen, um die Beamten zu einem großen Teil von dieser belastenden Tätigkeit zu befreien. Die Frage, die wir von Anfang an verfolgt haben, war, inwiefern nicht nur der Einsatz einer KI, sondern auch der skalierbare, flexible Einsatz cloudbasierter Services möglich ist.

All dies hat Microsoft - auch angesichts der entsprechenden Rechtsvorschriften - vor nicht unerhebliche Herausforderungen gestellt, wie ich offen zugebe.

Ich will Ihnen einen kleinen Einblick in den Austausch mit unserer Rechtsabteilung geben: Als wir dort mit der grundsätzlichen Projektidee vorstellig geworden sind, hat man uns erst einmal dazu befragt, woraufhin unsere Rechtsabteilung zu einer Einschätzung kam. Wir haben geprüft, inwiefern das Thema für die Firma Microsoft eine strafrechtliche Relevanz hat, insbesondere aber auch, wie eine datenschutzrechtliche Bewertung eines solchen Projekts aussehen kann.

Als Ergebnis unserer Bewertung der strafrechtlichen Relevanz in Zusammenarbeit mit der Staatsanwaltschaft haben wir das Risiko als akzeptabel eingeschätzt. Die Einschätzung, inwiefern wir damit die DSGVO verletzen, war aber nicht akzeptabel. Wenn wir eine KI trainieren, oder wenn wir mit einer trainierten KI Bilder auswerten, nutzen wir Bilder, auf denen menschliche Opfer zu sehen sind, deren Einwilligung zur Verarbeitung dieser Daten schwerlich einzuholen ist. Insofern war die Aussage unserer Abteilung: Ihr müsst entweder alle abgebildeten Menschen fragen, ob sie damit einverstanden sind, oder aber dafür sorgen, dass sie unkenntlich gemacht werden.

Im ersten Moment sah das wie das Ende dieses Projekts aus, weil uns damit die Arbeitsgrundlage genommen worden ist. De facto war es aber der Startschuss für einen neuen, innovativen Einsatz, den wir auf der nächsten Folie schematisch dargestellt haben.



Die Idee, Daten vollständig zu abstrahieren und sie gleichwohl trotzdem noch nutzbar zu halten, um eine KI damit trainieren zu können, ist der innovative Ansatz, mit dem wir arbeiten. Das neue Verfahren, das wir mit unseren Experten entwickelt haben, ist so aufgebaut, dass wir in der Lage sind, über die Endgeräte der Sicherheitsbehörden eine Abstraktion der Bilder vorzunehmen.

Es handelt sich hierbei nicht um eine Verschlüsselung, und es ist keine Pseudonymisierung im Sinne der datenschutzrechtlichen Gesetzgebung. Tatsächlich ist es eine vollständige Abstraktion, die dadurch ermöglicht wird, dass wir den Prozess des Trainings eines neuronalen Netzes nach ein paar Layern auf der On-Premise-Seite anhalten. Die dabei entstandenen Daten transferieren wir in die Cloud. Diese Transformation resultiert in 512 Bildern mit einer Größe von acht mal acht Pixeln. Das menschliche Auge kann auf ihnen keine relevanten Inhalte mehr erkennen. Trotz allem ist es mit den Daten noch möglich, eine KI vollständig zu trainieren.

Wir haben zwei strafrechtlich relevante Klassen gebildet: Die Abbildungen von Menschen, die jünger als 14 Jahre sind, und von denen, die zwischen 14 und 18 Jahre alt sind. Dann haben wir noch zwei Klassen, die wir als strafrechtlich nicht relevant einordnen: Erwachsenenpornografie und alles, was in keine der drei vorherigen Kategorien passt.

Mit diesem trainierten Algorithmus können wir große Datenmengen skalieren und auswerten. Wir können die entsprechenden Funde dann an die jeweiligen Sicherheitsbehörden zurückgeben.

Ausschnittvergrößerung der Reihe links oben:

Hier sehen Sie ein Beispiel für unser Abstraktionsverfahren. Oben ist das originale Eingabebild, das wir in den Algorithmus gegeben haben. Darunter sehen Sie einen Teil der 512 acht mal acht Pixel großen Abstraktionslayer, die wir in die Cloud transferieren. Sie sind sicher einer Meinung mit mir, dass wir die Abbildungen auf diesen Bildern auf keinerlei Inhalte zurückführen können.

Dieser Ansatz ist - auch nach der Einschätzung unserer wissenschaftlichen Begleiter - dazu geeignet, die Daten aus den direkten Strafrechts- und Datenschutzbereichen zu lösen, sodass wir in die Lage versetzt werden, die KI mit entsprechend sensiblen Daten zu trainieren.

Das Projekt teilt sich in drei Phasen. Zunächst haben wir mit Bildern gearbeitet, die keinerlei strafrechtlichen Inhalte hatten - z. B. Bilder von Hunden und Katzen -, um herauszufinden, ob wir in der Lage sind, KI-Algorithmen über ein solches Abstraktions-Layer zu trainieren. Diese Phase konnten wir erfolgreich abschließen.

In der zweiten Phase haben wir mit einer entsprechenden Anzahl strafrechtlich relevanter Bilder trainiert, um zu verifizieren, dass das Ergebnis für uns und für unsere Projektpartner am Ende gut genug ist, um diesen Ansatz weiterzuverfolgen. Die Trefferquote in dieser Phase lag bei über 85 % bis 90 %.

In der dritten Phase haben wir uns darüber Gedanken gemacht, in welchen Anwendungsfällen wir diese Technologie konkret einsetzen könnten.

Der erste Anwendungsfall zielt auf die reine Bildklassifizierung. Es dient also dem Erkennen von Darstellungen sexuellen Missbrauchs von Minderjährigen und der Unterscheidung von strafrechtlich nicht relevantem Material. Hierfür nehmen wir die Unterteilung in drei bzw. vier Kategorien vor.

Die vier Kategorien habe ich Ihnen eben schon vorgestellt. Zugunsten der Modellgenauigkeit haben wir die Unterscheidung von „unter 14" und „14 bis 18" in der Kategorie Kinder- und Jugendpornografie zusammengefasst, die Ergebnisse verglichen und daraufhin entschieden, welches Kategorienmodell die bessere Trefferquote erzielt. Um es vorwegzunehmen: Es war das Drei-Kategorien-Modell.

In einem weiteren Anwendungsfall soll eine Textanalyse auf den entsprechenden Bildern vorgenommen und die Suche nach vorher festgelegten Schlagworten ermöglicht werden. Das liegt insbesondere darin begründet, dass uns die Ermittelnden mitgegeben haben, dass es Wasserzeichen oder ähnliche Tags auf Bildern geben kann, die Rückschlüsse auf die Quellen oder die Verbreiter des Materials zulassen.

Im dritten Anwendungsfall sollen Rückschlüsse auf die Kontexte der relevanten Bilder bzw. ihre Ursprünge ermöglicht werden. In unseren Anwendungsfällen haben wir bei Durchsuchungen beschlagnahmtes Material wie Handys untersucht. In solchen Fällen haben wir vollständige Chatprotokolle mit ein- und ausgehenden Bildern. Warum ist das relevant? - Eingehende Bilder sind die Bilder, die man aus anderen Quellen empfängt. Ausgehende Bilder erfüllen den Straftatbestand der Verbreitung. Sie geben direkte Möglichkeiten, zu Hinweisen darüber zu kommen, ob ein aktiver Missbrauch vorliegt.

Ich will Sie nicht lange mit Details zu dieser Darstellung langweilen oder überfordern. Es kommt auf einen wichtigen Punkt an dieser Stelle an: Wir haben unsere Architektur in ihrer Gesamtheit so aufgebaut, dass ein großer Bestandteil der Arbeit vor Ort im Rechenzentrum der jeweiligen Strafverfolgungsbehörde stattfinden kann.

Wir haben sogenannte Azure-Stack-Edge-Devices eingesetzt. Das ist eine von Microsoft entwickelte Hardware, die sich über ein Mietmodell beziehen lässt. Sie ist eine Höheneinheit groß und hat als Basis ein gehärtetes Linux-System. Über die Cloud ist eine vollständige Verwaltung dieser Edge-Devices möglich. Relevante Schritte im Gesamtprozess können dadurch on premise durchgeführt werden.

Die Anwendungsschicht befindet sich in einem Software-Container, wo sich die Web-Anwendung mit dem KI- und dem OCR-Modul für die Ermittler befindet. Das ist quasi ein Modell von der Stange aus dem Microsoft-Universum.

Die reine Verwaltung und die Skalierung werden nach entsprechender Abstraktion mit den Ressourcen der Cloud vorgenommen.

Als wir in der dritten Phase begonnen haben, unser Prinzip und die Gesamtarchitektur umzusetzen, waren uns von vornherein ein paar Grundprinzipien wichtig:

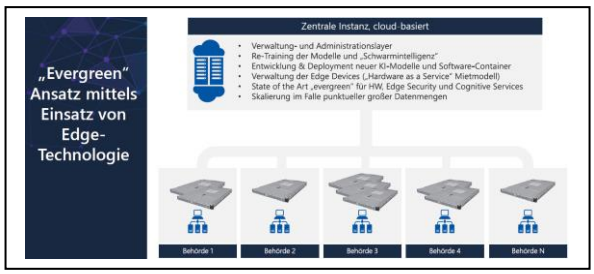
Erstens war es uns wichtig, eine offene Plattform zu entwickeln, die allen Ermittlern, die sich beteiligen wollen, einen möglichst barrierefreien Zugang ermöglicht. Wir wollen keine Installation von Software-Derivaten auf den Arbeitsgeräten der jeweiligen Ermittler, sondern eine webbasierte Schnittstelle, die über den Browser bedient werden kann.

Zweitens ging es uns auch darum, diese offene Plattform so zu gestalten, dass dort nicht nur der von uns entwickelte Algorithmus Platz findet, sondern auch weitere sinnvolle Technologien, die in der Zukunft möglicherweise von weiteren Anbietern bzw. Entwicklern kommen werden. Wir sagen: Die von uns entwickelte Plattform bzw. Lösung wird niemals ganz fertig sein. Sie ist immer bereit, weitere Innovationen aufzunehmen.

Als Nächstes mussten wir die Frage klären, an welcher Stelle des Gesamtverfahrens wir die Lösung platzieren wollten. Für uns war es wichtig, dass die Lösung die Ermittler in die Lage versetzt, eine sehr schnelle Erstanamnese beschlagnahmter Asservate vorzunehmen.

Die effiziente und schnelle Erstanalyse soll nach dem Motto erfolgen: Bitte werte diese Festplatte bzw. dieses Handy für mich aus, zeige mir von den 100 000 Dateien, die sich insgesamt darauf befinden, die 20 oder 30 für uns relevanten an und gib uns einen Hinweis darauf, ob das Material strafrechtlich relevant ist.

Das nächste Grundprinzip korrespondiert mit dem ersten. Wir wollen in Zukunft viele Sicherheitsbehörden mit dieser Lösung ausstatten. Je mehr Ermittler daran arbeiten und die Ergebnisse der KI bewerten, desto besser, da wir deren Expertise für die Weiterentwicklung einfangen können.



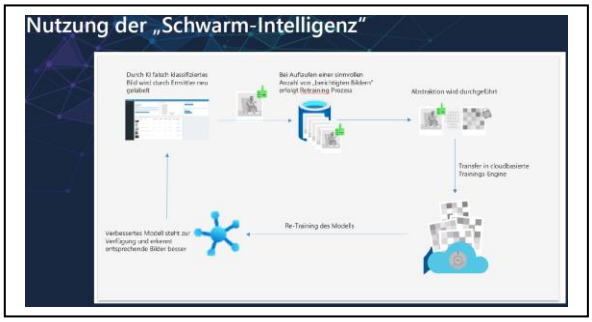
KI ist niemals perfekt. Sie ist dazu gedacht, auf Basis von Retrainings verbessert zu werden. Und wer könnte eine KI besser nachtrainieren als die Experten, die sich mit diesem Thema konkret auseinandersetzen? Dafür nutzen wir den vielleicht etwas saloppen Begriff „Schwarmintelligenz". Das heißt, wie haben eine Funktion eingebaut, die es den Ermittlern ermöglicht, potenziell falsch klassifizierte Bilder neu zu labeln und in das System zurückzuführen. So entstehet eine neue Datenbank für das weitere Training der KI.

Das letzte Grundprinzip der Cloud ist eine zentrale Verwaltung, um möglichst ohne großen Aufwand im Sinne eines Evergreen-Ansatzes regelmäßige Updates und weitere Devices zur Verfügung zu stellen.

Die Gesamtarchitektur ist so aufgebaut, dass ein oder mehrere der Azure-Stack-Edge-Devices in einer Behörde platziert werden können, in Abhängigkeit davon, wie groß die Notwendigkeit einer Skalierung ist. Ein Azure-Stack-Edge-Device ist mit zwei GPUs ausgestattet, die es uns erlauben, sekündlich ungefähr 20 bis 25 Bilder pro Device auszuwerten. Eine OCR-Analyse ist sehr langwierig. Die reine Analyse der Bilder würde deutlich schneller funktionieren. Bei großen Datenmengen können die Devices entsprechend skaliert werden, um größere Durchsatzraten zu erzielen.

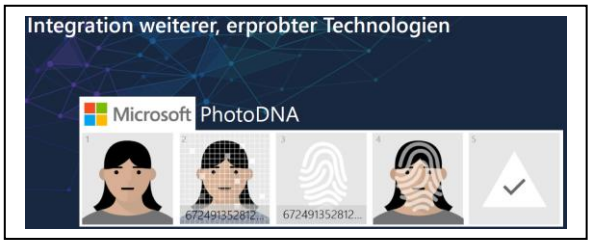
Unser Prinzip - ich habe es eben schon dargestellt - ist ein Hardware-Miet-Modell. Das heißt, Sie können sich monatlich jederzeit weitere Devices anschaffen und diese, wenn die Auswertung des Falls abgeschlossen ist, auch wieder zurückgeben. Das ist natürlich ganz im Sinne der Kostenfrage in Peak-Zeiten. Die Elastizität einer Cloud wird direkt auf die Hardware transferiert, und der Umgang mit ihr wird für die Behörden entsprechend einfach gestaltet.

Die Verteilung der Geräte erfolgt zentralisiert. Man kann sich eine solche Hardware - das nackte Modul - in die Behörde liefern lassen. Ein zentraler Administrator ist dann in der Lage, diese Behörde von jedem Ort aus mit den relevantesten, neuesten Modellen auszustatten, damit die Lösung vor Ort auf dem aktuellsten Stand installiert werden kann.



Die Nutzung der Schwarmintelligenz habe ich schon kurz dargestellt. In unserer Anwendung gibt es die Möglichkeit, ein Bild neu zu labeln. Angenommen, ein Bild wird als kinderpornografisch einsortiert, der Ermittler ist aber der Meinung, dass dem nicht so ist, dann kann er das Bild per Auswahl in einem Drop-Down-Menü einfach neu labeln.

Es wird dann in eine Datenbank zurückgeführt und bei einem neuen Anschub des Prozesses, der entweder zeitbasiert oder quantitativ sein wird, erneut in das Modell gespeist. Die Abstraktion bzw. das neue Training werden durchgeführt, und das neue Modell steht dann allen Ermittlern sofort wieder zur Verfügung.



Microsoft PhotoDNA ist eine Technologie, die potenziell auf einer solchen Plattform eingesetzt werden könnte. Sie basiert darauf, dass hashbasierte, digitale Fingerabdrücke von Bildern gezogen werden, um auf dieser Basis eine Datenbank mit bereits bekannten, als kinderpornografisch und strafrechtlich relevant eingestuften Bildern zur Verfügung zu stellen.

Ein solches Verfahren mit in diese Lösung zu integrieren, würde die Genauigkeit und Schnelligkeit insofern erhöhen, dass wir alles, was über den hashbasierten Fingerabdruck identifiziert wird, von vornherein ein Stück weit aus der Analyse ausklammern könnten. Dann würde das Kinderpornografie-Modul nur die neuen, hinsichtlich

von Missbrauchsfällen wahrscheinlich relevanten Bilder anzeigen.

Das war ein Überflug über die Lösungen, die wir gemeinsam mit der ZAC NRW entwickelt haben. Das Forschungsprojekt ist abgeschlossen. Ein Prototyp ist über ZAC NRW einsehbar und nutzbar. Er kann über den Kollegen Herrn Hartmann angefragt werden.

Zur Möglichkeit, diese Technologie in der Breite anzuwenden: Derzeit bereitet das Justizministerium eine Ausschreibung vor, um die entsprechenden Handlungsschritte sauber durchführen zu können.

***