ZH_OBERGERICHT SB230481 vom 23. Oktober 2024

ZH Obergericht, 2024-10-23, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/zh_obergericht_SB230481

FR: ZH_OBERGERICHT SB230481 du 23 octobre 2024

IT: ZH_OBERGERICHT SB230481 del 23 ottobre 2024

Erwägungen

E. 1

Verfahrensgang

E. 1.1

Dem Beschuldigten wird im ersten Anklagepunkt vorgeworfen, im Zeitraum vom 15. März 2020 bis 26. April 2022 66 Bilder, auf welchen minderjährige Mädchen in sexuell aufreizenden Posen und/oder bei sexuellen Handlungen zu sehen sind, und 200 Bilder mit nicht tatsächlichen sexuellen Handlungen mit Minderjährigen über das Internet heruntergeladen und auf seinem Mobiltelefon und zwei Festplatten abgespeichert zu haben. Der Beschuldige habe gewusst, dass es sich bei den genannten Bildern um verbotene Pornografie handle. Trotzdem habe er die Bilder auf seine Datenträger heruntergeladen, sie gespeichert gelassen und

- 15 - angesehen, bzw. habe zumindest billigend in Kauf genommen, dass es sich bei den grossen (teilweise in Paketen) heruntergeladenen und gespeicherten Mengen pornografischer Bilddateien auch um verbotene Pornografie gehandelt habe, zumal er keinerlei Anstrengungen unternommen habe, um lediglich legale Pornografie herunterzuladen und abzuspeichern (Urk. 18 S. 2 f.). Gestützt auf die Meldung des NCMEC und die polizeilichen Ermittlungen wurde am 26. April 2022 am Wohnort des Beschuldigten eine Hausdurchsuchung durchge- führt, wobei ein Mobiltelefon, ein Notebook und ein Computer sichergestellt wurden (Urk. 3 S. 1 f.; Urk. 4 S. 2 f.; Urk. 11/2). Die Geräte wurden polizeilich ausgewertet, wobei auf zwei Festplatten Dateien festzustellen waren, die als verbotenes porno- grafisches Material eingestuft wurden (Urk. 4 S. 3; Urk. 11/3 S. 2; Urk. 12, ins- besondere S. 32 und S. 33). Der Beschuldigte bestritt vor Vorinstanz nicht, die im Auswertungsbericht aufgelisteten Bilddateien bei mehreren Vorgängen über das Internet heruntergeladen und auf Datenträger abgespeichert zu haben (Urk. 7 S. 4 ff. und 11; Prot. I S. 9 ff.). Anlässlich der Berufungsverhandlung präzisierte er jedoch seinen Standpunkt, indem er zusammengefasst zu Protokoll gab, dass er die illegalen pornografischen Bilder wissentlich nicht heruntergeladen habe und auch nicht wisse, wie diese auf seinen PC gelangt seien. Er vermute jedoch, dass ihm, als er bei Google etwa mit dem Begriff "nackte Frau" nach legalen pornografi- schen Bildern gesucht habe, ein Virus auf seinen Computer geschwemmt worden sei. Er könne nicht sagen, was alles an den legalen pornografischen Bildern drangehangen sei, er vermute jedoch, dass er "etwas Bösartiges" mitgenommen habe. Des Weiteren habe er die legalen Bilder mit "einem Tool", wo man einen Suchbegriff eingeben könne, heruntergeladen. Die illegalen Bilder seien beim Download von legaler Pornografie mitgeschwemmt worden. Sein Computer habe damals mehrere Abstürze gehabt und er habe danach jeweils das Betriebssystem neu installieren müssen. Nach den Neuinstallationen seien ihm die heruntergela- denen Bilder nicht mehr angezeigt worden, somit habe er diese dann auch nicht mehr überprüfen und

allfällige illegale Bilder löschen können (Urk. 51; mehr dazu nachfolgend Ziff. III.3.).

- 16 -

E. 1.2

Wie die Vorinstanz zutreffend erwog, handelt es sich dabei um 66 Bild- dateien mit realen minderjährigen Personen (Urk. 36 S. 20). Soweit die Vertei- digung in ihrem Plädoyer vor Vorinstanz von 660 Bilddateien spricht (Urk. 24 S. 4), muss es sich um einen Irrtum handeln. Mit dem Vorbringen der Verteidigung, wonach viele der Bilder mehrfach, einzelne Bilder über 30 Mal, aufgeführt seien (Urk. 24 S. 4), hat sich bereits die Vorinstanz auseinandergesetzt. Sie hielt fest, dass es sich bei den mehrfach aufgeführten Bildern um eine sog. GIF-Datei handle, in der eine Abfolge von Einzelbildern zusammen abgespeichert sei. Diese Bilder könnten zeitverzögert abgespielt werden, sodass sie einen filmähnlichen Eindruck erweckten. Diese Animationsmöglichkeit ändere jedoch nichts an dem Umstand, dass es sich bei den in der GIF-Datei abgespeicherten Bildern um einzelne Bilder handle, die folglich auch einzeln abgespeichert, versendet und konsumiert werden könnten (Urk. 36 S. 20). Auf diese zutreffenden Erwägungen kann ohne Weiteres verwiesen werden. Zusätzlich zu den bereits erwähnten 66 Bilddateien mit realen Darstellungen wurden auf Datenträgern des Beschuldigten 200 Bilddateien mit virtuellen Darstellungen sichergestellt. Mit der Vorinstanz erweist sich daher in tatsächlicher Hinsicht als erstellt, dass der Beschuldigte die in der Anklage aufge- führten 266 Bilddateien über das Internet heruntergeladen und auf ihm gehörenden Datenträgern abgespeichert hat.

E. 1.3

Der Beschuldigte macht in subjektiver Hinsicht geltend, beim Herunterladen und Abspeichern der Bilddateien nicht erkannt zu haben, dass es sich dabei um verbotenes pornografisches Material gehandelt habe, bzw. habe er legale Porno- grafische Bilder herunterladen wollen und nicht gewusst, dass bei den Downloads auch illegale pornografische Bilder mitenthalten gewesen seien. Was der Täter wusste und wollte, betrifft sog. innere Tatsachen und ist damit Tatfrage. Rechts- frage ist hingegen, ob gestützt auf die festgestellten Tatsachen bewusste Fahr- lässigkeit, Eventualvorsatz oder direkter Vorsatz gegeben ist (BGE 149 IV 57 E. 2.2; 147 IV 439 E. 7.3.1; 141 IV 369 E. 6.3; 137 IV 1 E. 4.2.3; je mit Hinweisen). Für den Nachweis des Vorsatzes kann sich das Gericht – soweit der Täter nicht geständig ist – regelmässig nur auf äusserlich feststellbare Indizien und auf Erfah- rungsregeln stützen, die ihm Rückschlüsse von den äusseren Umständen auf die innere Einstellung der Täterschaft erlauben (BGE 134 IV 26 E. 3.2.2 mit Hinwei-

- 17 - sen). Da Tat- und Rechtsfragen diesbezüglich eng miteinander verknüpft sind und sich insoweit teilweise überschneiden, wird im Rahmen der rechtlichen Würdigung auf den subjektiven Sachverhalt einzugehen sein. 2. Anklagesachverhalt 2: Bildersuche über Microsoft Bing

E. 2

Umfang der Berufung Die Berufung hat im Umfang der Anfechtung aufschiebende Wirkung (Art. 402 StPO). Die Berufung des Beschuldigten richtet sich gegen die Dispositivziffern 1

- 6 - bis 5 und 9 des vorinstanzlichen Urteils. Im Übrigen blieb das vorinstanzliche Urteil unangefochten (Urk. 40 S. 2). Die Staatsanwaltschaft hat weder Berufung noch Anschlussberufung erhoben. Das Urteil des Bezirksgerichts Horgen, Einzelgericht, vom 17.

Juli 2023 ist daher bezüglich der Dispositivziffern 6 (Entscheid über beschlagnahmte Gegenstände) sowie 7 und 8 (Kostenfestsetzung) in Rechtskraft erwachsen.

E. 2.1

Die Vorinstanz hat die beim Beschuldigten sichergestellten Bilddateien als Minderjährigenpornografie im Sinne von Art. 197 Abs. 4 und 5 aStGB eingestuft. Der Anklage entsprechend wurden 66 Bilder als Darstellungen mit tatsächlichen sexuellen Handlungen mit Minderjährigen und 200 Bilddateien als solche mit nicht tatsächlichen Handlungen mit Minderjährigen qualifiziert. Die von der Vorinstanz vorgenommene Beurteilung ist korrekt und wurde von der Verteidigung nicht in Frage gestellt. Auf die zutreffenden vorinstanzlichen Erwägungen kann vorab verwiesen werden (Urk. 36 S. 28 f.). Die beim Beschuldigten sichergestellten 66 Bilddateien zeigen reale Personen. Auf der Mehrheit der Bilder ist ein Mädchen zu sehen, das in einer objektiv aufreizenden Stellung posiert, wobei der nackte Genitalbereich aufdringlich in den Vordergrund gerückt und betont wird. Das Mädchen erscheint als reines Sexualobjekt, weshalb die Bilder ohne Weiteres als (kinder-) pornografisch zu qualifizieren sind. Bei den weiteren 200 Bilddateien handelt sich um Bilder, die sexuelle Handlungen mit kindlichen Comicfiguren und computergenerierte Darstellungen von nackten Mädchen zeigen. Nachdem auf den Erzeugnissen keine realen minderjährigen Personen abgebildet sind, wurden sie

- 24 - von der Vorinstanz zutreffend als virtuelle Pornografie und damit als Darstellungen mit nicht tatsächlichen sexuellen Handlungen mit Minderjährigen eingestuft.

E. 2.2

Gemäss erstelltem Sachverhalt hat der Beschuldigte mit den erwähnten Bildern mehrfach Bilddateien mit (tatsächlichen und virtuellen) sexuellen Hand- lungen mit Minderjährigen aus dem Internet heruntergeladen und auf Datenträger abgespeichert. Dieses Verhalten wurde von der Vorinstanz zu Recht als mehrfache Pornografie zum eigenen Konsum im Sinne von Art. 197 Abs. 5 Satz 1 und 2 aStGB eingestuft (Urk. 36 S. 29 f.). Auch diesbezüglich kann auf die zutreffenden vorinstanzlichen Erwägungen verwiesen werden, zumal sie von der Verteidigung nicht in Frage gestellt wurden (Urk. 52, S. 3 Rz 5, S. 8 Rz 27 ff.). 3. Subjektiver Tatbestand

E. 2.3

Die Vorinstanz hielt den Anklagesachverhalt auch in diesem Punkt für erstellt. Zur Begründung erwog sie zusammengefasst, soweit der Sachverhalt vom Beschuldigten nicht eingestanden sei, lasse er sich einzig basierend auf den vorhandenen Indizien und dem Aussageverhalten des Beschuldigten erstellen. Aufgrund seiner Stellung im Verfahren habe der Beschuldigte eine reduzierte Glaubwürdigkeit. Was die Glaubhaftigkeit seiner Aussagen anbelange, falle in erster Linie auf, dass er in objektiver Hinsicht komplett in Abrede stelle, jemals eine Bing-Image-Suche getätigt zu haben, sich aus dem CyberTipline Report und dem Bericht des Bundesamts für Polizei jedoch ergebe, dass ein Internetnutzer über die am Wohnort des Beschuldigten zu verortende IP-Adresse am 23. August 2021 eine Bildersuche über Microsoft Bing vorgenommen habe. Aufgrund der objektiven Beweise stehe fest, dass die inkriminierende Bing-Image-Suche nicht von einer externen Adresse, sondern von der Wohnadresse des Beschuldigten aus getätigt

- 18 - worden sei, weshalb sein Vorbringen, wonach er seine elektronischen Geräte teil- weise auch in die Schule mitgenommen und daher theoretisch jeder darauf Zugriff gehabt

habe, unbeachtlich sei. Des Weiteren falle auf, dass die Suche über Bing just mit einem der inkriminierenden Bilder getätigt worden sei, die der Beschuldigte zuvor aus dem Internet heruntergeladen und auf seinen Datenträgern abgespei- chert habe. Die Aussagen des Beschuldigten seien daher als unglaubhafte Schutz- behauptungen zu werten. Angesichts der Funktionsweise der Suchmaschine – die Bildersuche erfolge durch Heraufladen einer Datei vom eigenen Computer – sei im Ergebnis davon auszugehen, dass nur der Beschuldigte selbst die fragliche Suche über Bing habe tätigen können (Urk. 36 S. 24 f.).

E. 2.4

Die von der Vorinstanz vorgenommene Beweiswürdigung vermag nicht zu überzeugen. Zunächst kann ihr nicht gefolgt werden, wenn sie dem Beschuldigten allein aufgrund seiner Stellung im Verfahren eine reduzierte Glaubwürdigkeit zurechnet (Urk. 36 S. 19 und 24). Dass eine Person beschuldigt bzw. von der Staatsanwaltschaft angeklagt wird und ein Interesse hat, sich in einem günstigen Licht darzustellen, ist ausnahmslos in jedem Strafprozess der Fall. Insofern ist die prozessuale Stellung und Interessenlage einer beschuldigten Person immer gleich und taugt nie für die Unterscheidung, ob eine Person glaubwürdig ist oder nicht. Eine unschuldige Person hat dasselbe Interesse, sich in einem günstigen Licht darzustellen. Damit soll nicht gesagt werden, dass die Glaubwürdigkeit einer Person im Rahmen der Beweiswürdigung nicht relevant sein kann. Sie kann durch- aus Gewicht erlangen. So etwa wenn bekannt ist, dass eine Person schon mehrere Verurteilungen wegen falscher Anschuldigung aufweist und eine Tat mit ähnlicher Vorgehensweise zu beurteilen ist. Die Glaubwürdigkeit kann auch relevant sein, wenn die aussagende Person in einem Verfahren nachweislich verschiedentlich die Unwahrheit gesagt hat. Dies ist vorliegend aber nicht der Fall. Weiter vermag es nicht zu überzeugen, wenn die Vorinstanz die Behauptung des Beschuldigten, noch nie eine Suche über Microsoft Bing vorgenommen zu haben, mit dem CyberTipline Report und dem Bericht des Bundesamts für Polizei widerlegt (Urk. 36 S. 24). Zuerst ist festzuhalten, dass das Bundesamt für Polizei im Strafverfahren gegen den Beschuldigten lediglich die Zuordnung der IP-Adresse vorgenommen hat. In Bezug auf die Frage, von welcher Adresse die Bilddatei hochgeladen wurde,

- 19 - wurden von dieser Behörde keine eigenen Ermittlungshandlungen vorgenommen (Urk. 1; Urk. 3 S. 1 f.). Diesbezüglich liegt als Beweismittel ausschliesslich die Verdachtsmeldung von Microsoft vor. Wenn die Vorinstanz die Behauptung des Beschuldigten, noch nie eine Suche über Microsoft Bing vorgenommen zu haben, mit dem Argument widerlegt, dass am 23. August 2021 über die an seinem Wohnort zu verortende IP-Adresse ein Bild hochgeladen wurde, erweist sich dies als Zirkel- schluss. Die Vorinstanz stützt sich zur Widerlegung der Behauptung des Beschul- digten auf Umstände, die sie eigentlich erst erstellen möchte, womit sie das Resul- tat der Würdigung an den Anfang stellt und als gegeben voraussetzt. Der Vorinstanz kann daher nicht gefolgt werden, wenn sie die Aussagen des Beschul- digten aus diesem Grund als unglaubhafte Schutzbehauptungen wertet (Urk. 36 S. 25).

E. 2.5

Die Vorinstanz hat zutreffend ausgeführt, dass die von Microsoft als kinder- pornografisch eingestufte Bilddatei auf Datenträgern des Beschuldigten abgespei- chert war (Urk. 36 S. 25). Dies ergab eine Auswertung der anlässlich der Haus- durchsuchung an seinem Wohnort sichergestellten elektronischen Geräte und wird von ihm nicht bestritten (Urk. 7 S.

5; Prot. I S. 13; Urk. 51 S. 5 ff.). Das Herunter- laden und Abspeichern dieser Bilddatei bildet Bestandteil des ersten Anklagesach- verhalts. In Bezug auf die im zweiten Anklagesachverhalt relevante Frage, ob der Beschuldigte die inkriminierte Bilddatei durch Hochladen über die Suchmaschine Microsoft Bing anderen Nutzern zur Verfügung gestellt hat, liegen als Beweismittel lediglich die von Microsoft erstellte und von NCMEC an die Strafverfolgungsbehör- den weitergeleitete Verdachtsmeldung vor. Analog einer durch eine Privatperson erstellten Strafanzeige handelt es sich bei der in der Verdachtsmeldung enthalte- nen Angaben nicht um gesicherte Tatsachen, sondern lediglich um erste Hinweise auf ein potentiell strafbares Verhalten. Dies gilt vorliegend umso mehr, als die an NCMEC gemeldeten Daten in aller Regel auf automatisierten Erkennungsprogram- men der Provider basieren. Eine Kontrolle durch eine natürliche Person findet grundsätzlich nicht statt. NCMEC fungiert als Schnittstelle zwischen den Internet- plattformen und den Strafverfolgungsbehörden und nimmt wie bereits erwähnt ebenfalls keine Ermittlungshandlungen vor. Die Mitarbeitenden des NCMEC erhal- ten wie auch diejenigen von Microsoft keinen Einblick in die gemeldete Bilddatei.

- 20 - Dem CyberTipline Report vom 24. August 2021 lassen sich denn auch keine Anhaltspunkte dafür entnehmen, dass Microsoft oder NCMEC eine inhaltliche Überprüfung der automatisch generierten Daten vorgenommen hätte (vgl. dazu Ziff. I.3.3.2 f.). Es ist daher davon auszugehen, dass das dem Beschuldigten ange- lastete Verhalten, eine Bilddatei mit strafbarem Inhalt hochgeladen zu haben, einzig auf dem von Microsoft angewandten automatisierten Erkennungsprogramm beruht. Mangels entsprechender Abklärungen der Strafverfolgungsbehörden ist unklar, wie fehlerfällig diese Kontrollsysteme sind und auf welche Weise die Authentizität des Absenders und die Verlässlichkeit der gemeldeten Inhalte gewährleistet werden. Weiter muss offen bleiben, wie einfach es für einen Nutzer ist, eine fremde IP- Adresse zu verwenden, um die eigene Identität zu verbergen. Nachdem die mit CyberTipline Report vom 24. August 2021 gemeldete Bilddatei auf Datenträgern des Beschuldigten sichergestellt werden konnte, erscheint es unwahrscheinlich, dass die im Bericht aufgeführte IP-Adresse falsch ist oder in der Folge fälschlicher- weise dem Wohnort des Beschuldigten zugeordnet wurde. Gänzlich ausschliess- lich lässt sich dies allerdings nicht. Setzt man die von Microsoft gemeldete IP-Adresse als richtig voraus, erscheint es im Übrigen auch wenig wahrscheinlich, dass eine Drittperson die Bilddatei über einen Datenträger des Beschuldigten hochgeladen hat, nachdem die Suchanfrage vom Wohnort des Beschuldigten aus getätigt wurde (vgl. dazu die Vorinstanz, Urk. 36 S. 24 f.). Dies ändert letztlich aber nichts daran, dass der dem Beschuldigten in der Anklage zur Last gelegte Vorgang – das Hochladen einer Bilddatei mit tatsächlichen sexuellen Handlungen mit Minderjährigen – einzig auf der von Microsoft vorgenommenen Meldung basiert, wonach durch den Nutzer der IP-Adresse 2 über Microsoft Bing eine Bilddatei mit kinderpornografischem Inhalt verbreitet worden sei.

E. 2.6

Wie erwähnt, wurden die von Microsoft gemeldeten Informationen von den Strafverfolgungsbehörden nicht überprüft. Es wurde auch nicht abgeklärt, ob der Beschuldigte über ein Konto bei Microsoft verfügt oder über Bing jemals Suchan- fragen getätigt hat. Den Akten lässt sich weiter nicht entnehmen, wie die von den Providern angewandten Kontrollsysteme funktionieren und wie das Verhalten der Nutzer konkret erfasst wird, was seitens der Verteidigung zu Recht beanstandet wurde (Urk. 24 S. 7 f.; Urk. 40 S. 4 ff.). Damit ist nicht nachvollziehbar, wie der Vor-

- 21 - gang des Hochladens der Bilddatei vom automatisierten Erkennungsprogramm von Microsoft technisch festgestellt werden konnte und wie zuverlässig dieses Programm agiert. Gemäss CyberTipline Report vom 24. August 2021 ist Bing Image eine Suchfunktion, die dem Nutzer ermöglicht, mithilfe eines Bildes ähnliche Bilder im Web zu finden. Das Bild kann entweder von einem Datenträger hoch- geladen werden oder unter Verwendung der Webadresse (URL) zur Verfügung gestellt werden (S. 2: BingImage is a service that provides similar images to an image provided by the user. This image can be provided either via upload or as a URL). Dass sodann Bilder, die für eine Bildersuche in die Suchfunktion eingegeben werden, automatisch öffentlich zugänglich gemacht und mit anderen Nutzern geteilt werden, wie das die Anklage behauptet, ist nicht anzunehmen. Den Akten lässt sich auch diesbezüglich nichts entnehmen. Im CyberTipline Report wird vielmehr aus- drücklich offen gelassen, ob die vorliegend hochgeladene Datei überhaupt von anderen Nutzern eingesehen werden konnte (S. 2: Were entire contents of uploaded file publicly available? Information Not Provided by Company). Vor diesem Hintergrund kann vorliegend allein gestützt auf die NCMEC-Meldung nicht mit rechtsgenügender Sicherheit als erstellt betrachtet werden, dass von der am Wohnort des Beschuldigten zu verortenden IP-Adresse anderen Internetnutzern eine Bilddatei mit tatsächlichen sexuellen Handlungen mit Minderjährigen zugäng- lich gemacht wurde. Weitere Anhaltspunkte für ein solches Verhalten bestehen nicht. Wie erwähnt, wird dem Beschuldigten das Hochladen einer einzigen Bilddatei angelastet. Der daraufhin erstellte CyberTipline Report vom 24. August 2021 ging gleichentags bei den Schweizer Behörden ein (Urk. 1 f.). Bis zur Hausdurch- suchung am Wohnort des Beschuldigten, die am 26. April 2022 stattfand, vergingen rund acht Monate. Gemäss dem erstellten Sachverhalt wurden vom Beschuldigten in dieser Zeit weiterhin pornografische Bilddateien über das Internet herunterge- laden und abgespeichert (erster Anklagepunkt). Er hat sich damit weiterhin mit dem Thema Pornografie befasst und im Internet nach entsprechenden Dateien gesucht. Aus den Akten geben sich indes keine Hinweise darauf, dass er vor oder nach dem 21. August 2021 Bilddateien mit verbotenem pornografischen Inhalt anderen Nut- zern über Microsoft Bing oder andere Provider zugänglich gemacht hätte. Nachdem die bei NCMEC eingehenden Meldungen jeweils innert Kürze den Strafverfolgungs-

- 22 - behörden weitergeleitet werden, wäre zu erwarten, dass die Schweizer Behörden in diesem Fall informiert worden wären. Vor diesem Hintergrund kann nicht ausge- schlossen werden, dass das Hochladen der fraglichen Bilddatei irrtümlicherweise erfolgte oder bei der Auswertung des automatisierten Erkennungsprogramms ein Fehler passierte, zumal dessen Funktionsweise wie erwähnt nicht nachvollziehbar ist. Die im Rapport von NCMEC enthaltenen Angaben vermögen unter diesen Umständen keine strafbare Handlung zu beweisen. Der Beschuldigte ist daher in diesem Anklagepunkt vom Vorwurf der Pornografie (Zugänglichmachen einer Darstellung mit tatsächlichen sexuellen Handlungen mit Minderjährigen) freizu- sprechen. Damit erübrigen sich Weiterungen in Bezug auf das Zustandekommen der Meldung von Microsoft an das NCMEC, wie sie von der Verteidigung eventua- liter beantragt wurden (Urk. 40 S. 2; Urk. 52). III. Rechtliche Würdigung 1. Grundlagen Per 1. Juli 2024 ist das revidierte Sexualstrafrecht in Kraft getreten. In Bezug auf die dem Beschuldigten in der Anklage vorgeworfenen Tathandlungen brachte das neue Recht keine Änderungen mit sich, weshalb die bisherige Fassung von Art. 197 StGB anwendbar bleibt (Art. 2 StGB). Die Vorinstanz stufte das Verhalten des Beschuldigten im ersten Anklagsachverhalt – wie bereits die Staatsanwaltschaft – als mehrfacher Konsum von harter Pornografie im Sinne von Art. 197

Abs. 5 Satz 1 und 2 aStGB ein (Urk. 18 S. 3; Urk. 36 S. 45). Nach dieser Bestimmung macht sich strafbar, wer Gegenstände oder Vorführungen im Sinne von Absatz 1, die sexuelle Handlungen mit Minderjährigen zum Inhalt haben, konsumiert oder zum eigenen Konsum herstellt, einführt, lagert, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt. Art. 197 Abs. 5 aStGB erfasst den Eigen- konsum sowie Tathandlungen, die ausschliesslich dem Eigenkonsum dienen (BSK StGB-ISENRING/KESSLER, 4. Aufl. 2019, N 49 zu Art. 197; TRECHSEL/BERTOSSA, in: Trechsel/Pieth [Hrsg.], Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. Auflage 2021, N 16 zu Art. 197). Die Vorinstanz hat den Tatbestand von Art. 197 Abs. 5 aStGB ausführlich und zutreffend dargelegt, worauf zur Vermeidung un-

- 23 - nötiger Wiederholungen vollumfänglich verwiesen werden kann (Urk. 36 S. 26 ff.). Ergänzend ist auszuführen, dass für die Erfüllung des subjektiven Tatbestands nicht erforderlich ist, dass den Tathandlungen sexuelle Motive zugrunde liegen. Der Begriff der Pornografie setzt zwar voraus, dass die Darstellungen oder Darbietun- gen objektiv betrachtet darauf ausgelegt sind, den Konsumenten sexuell aufzurei- zen. Das Foto eines Kindes, welches die Kriterien für pornografische Darstellungen nicht erfüllt, wird aber nicht zur Kinderpornografie, weil es von einer Person zur Erregung sexueller Lust verwendet wird (vgl. dazu WEISSENBERGER, in ZBJV 138/2002, S. 356 f.). Umgekehrt fällt die Qualifikation als Kinderpornografie nicht allein deshalb dahin, weil die betreffende Person bei ihren Handlungen keine sexuelle Erregung verspürt bzw. ihr eine solche nicht nachgewiesen werden kann (vgl. dazu BGE 133 IV 31 E. 6.1.2 mit Hinweisen; BSK StGB-ISENRING/KESSLER, a.a.O., N 22d zu Art. 197). 2. Objektiver Tatbestand

E. 3

Verwertbarkeit der Beweismittel

E. 3.1

Der Beschuldigten macht indessen – wie bereits erwähnt – geltend, dass er die inkriminierten Dateien nicht bewusst heruntergeladen und abgespeichert habe. Zur Begründung führt die Verteidigung in Übereinstimmung mit dessen eigenen Aussagen aus, dass der Beschuldigte nicht pädophil sei. Er fühle sich zu Minder- jährigen in keiner Weise sexuell hingezogen. Bilder von Minderjährigen mit sexuel- lem Bezug würden ihn nicht interessieren oder erregen. Der Beschuldigte habe lediglich nach legaler Pornografie gesucht, wobei er mit Suchbegriffen wie etwa "nackte Frau" gesucht habe. Die Bilddateien seien in Datenpaketen herunter- geladen und abgespeichert worden, wobei in der Vorschau keine unerlaubte Pornografie ersichtlich gewesen sei. Bei ein bis zwei Vorschaubildern sei es unwahrscheinlich, dass gerade diejenigen Bilder in der Vorschau erschienen, die sich im Nachhinein als illegal entpuppt hätten. Das Filtern der Dateien sei mit grossem Aufwand verbunden, weshalb es einfacher sei, die Daten erst einmal zu behalten. Die Auswertung habe auch ergeben, dass es sich bei den illegalen Bild- dateien um einen Bruchteil aller beim Beschuldigten vorhandenen Dateien gehan- delt habe. Allein aufgrund der Tatsache, dass jemand heruntergeladene Dateien nicht aktiv durchforste, ob diese auch illegale Inhalte enthalten könnten, lasse sich kein Eventualvorsatz konstruieren (Urk. 24 S. 2 ff.; Urk. 40 S. 10 f.; Urk. 52 S. 8 Rz 27).

- 25 -

E. 3.2

Anlässlich der Berufungsverhandlung führte der Beschuldigte dazu weiter aus, dass er mittels eines online Programmes (mittels eines "Tools") legale Porno- grafie in Datenpaketen heruntergeladen habe. Das von ihm verwendetet Programm finde er nicht mehr. Der Beschuldigte verwies stattessen auf das seinen Aussagen gemäss ähnliche Programm "Google-Image-Downloader", welches er dem Gericht online demonstrierte (Urk. 51 S. 12 ff.). Der Beschuldigte gab dazu an, dass er im Programm jeweils einen Suchbegriff ein- gegeben sowie die Anzahl Bilder definiert habe, die dazu heruntergeladen werden sollten. Er sei damals im Stress gewesen und habe eine Art "Pornosucht" gehabt. Er habe sich Bilder heruntergeladen, damit er jederzeit seine Sucht befriedigen könne. Man könne mit dem Programm 1'000 oder gar 5'000 Bilder als ZIP-Datei herunterladen. Er selber habe jeweils 100, 200 oder 1'000 Bilder für einen Down- load angegeben. Der Beschuldigte erklärte weiter, dass die inkriminierten Bilder ohne sein Wissen zusammen mit legalen pornografischen Bildern mitheruntergela- den worden sein müssten. Die heruntergeladenen Bilder habe er nicht kontrolliert. Sein PC habe sodann mehrere Abstürze gehabt und ihm sei damit der Zugriff auf die Bilder schliesslich nicht mehr möglich gewesen. Wenn er den Computer gestar- tet habe, seien ihm nur Daten angezeigt worden, die er nach der Neuinstallation gespeichert habe. Als die Polizei ihm den Durchsuchungsbefehl wegen dem Ver- dacht auf Kinderpornografie vorgehalten habe, sei seine Vermutung, dass etwas nicht in Ordnung sein könnte, bestätigt worden (Urk. 51).

E. 3.3

Die Vorinstanz erachtete den subjektiven Sachverhalt als erstellt. Dies- bezüglich erwog sie zunächst, zwar sei denkbar, dass bei einem einmaligen Herunterladen eines Datenpakets mit pornografischen Bilddateien unbeabsichtigt verbotene Inhalte mitgeschwemmt würden. Bei mehrmaligem Herunterladen – dem Beschuldigten würden in der Anklage acht Vorgänge vorgeworfen –, erscheine es aber zusehends unglaubhaft, dass jedes Mal kinderpornografisches Material darin enthalten sei (Urk. 36 S. 21). Diese Begründung vermag nicht zu überzeugen. Zunächst ist insbesondere unklar, wie häufig der Beschuldigte kinderpornografi- sche Daten aus dem Internet (mit-) heruntergeladen haben soll. Er selbst konnte diesbezüglich keine Angaben machen. Die in der Anklage erwähnten Daten

- 26 - stammen – soweit ersichtlich – aus der polizeilichen Auswertung vom 30. Mai 2022 (Urk. 12). Im entsprechenden Bericht wird indes darauf hingewiesen, dass es sich bei den im Auswertungsbericht genannten Datum- und Zeitangaben um systembe- dingten Angaben handle, die nicht mit der tatsächlichen Zeit übereinstimmen müss- ten. Sie würden sich auf die eingestellte Systemzeit in jenem System beziehen, mit dem die Daten erstellt oder auf die jeweiligen Datenträger übertragen worden seien (Urk. 11/3 S. 3). Gemäss Auswertungsbericht konnten auf den Datenträgern des Beschuldigten 383'451 Bilddateien und 3'695 Filme sichergestellt werden. Bei den Bildern handle es sich um private Aufnahmen, Spiele und pornografische Aufnahmen. Davon seien insgesamt 266 als verbotene Pornografie einzustufen. Bei den Filmen handle es sich um Systemfilme, Spiele und pornografische Filme. Verbotene Filme seien nicht festgestellt worden (Urk. 11/3 S. 1 f.; Urk. 12 S. 1). Über wie viele legale Pornografie der Beschuldigte verfügte, ergibt sich allerdings weder aus dem Auswertungsbericht noch aus den weiteren Akten. Nachdem die Datenträger ohne deliktsrelevanten Daten dem Beschuldigten wieder ausgehändigt worden sind, kann dies auch nicht mehr erstellt werden. Es muss daher offen bleiben, welchen Anteil die kinderpornografischen Bilddateien am ganzen pornografischen Material ausmachten. Unklar bleibt sodann – wie erwähnt –, ob das kinderpornografische Material in

einem oder mehreren Downloads heruntergeladen wurde. Insofern verfängt der Einwand der Vorinstanz nicht, es sei unglaubhaft, dass sich gleich in mehreren Downloads unbeabsichtigt auch Kinderpornografie befunden habe. Die Vorinstanz hielt zudem fest, dass die Gesamtzahl an verbotener bzw. proble- matischer Bilder "durchaus nicht vernachlässigbar" sei, nachdem neben den 266 Bilddateien mit kinderpornografischem Material 92 Erzeugnisse mit Präferenzindi- katoren gefunden worden seien (Urk. 36 S. 22). Nachdem unklar ist, wie viele Dateien mit legaler Pornografie der Beschuldigte besass, kann indes nicht erstellt werden, ob die Gesamtzahl an verbotenen oder problematischen Bilder vernach- lässigbar ist oder nicht. Der Anzahl Bilddateien mit Kinderpornografie kann zumin- dest unter diesen Umständen keine entscheidende Bedeutung zukommen. Im Verhältnis zu den gesamten 383'451 Bildern würden die 266 kinderpornografischen

- 27 - Bilder denn auch nur gerade 0,07 % ausmachen und so jedenfalls nicht indizieren, dass der Beschuldigte bewusst nach Kinderpornografie gesucht hat. Der Beschuldigte konnte anlässlich der Berufungsverhandlung nachvollziehbar auf- zeigen, wie er mit seinem "Tool" themenbezogen automatisch im Internet gesuchte Bilder als Datenpakete heruntergeladen hat. Dabei stellte er sich – wie erwähnt – auf den Standpunkt, dass er stets nur nach legaler Pornografie gesucht und diese heruntergeladen habe und dass er die heruntergeladenen Bilder hernach zufolge Computerabstürzen und Neuinstallationen zum grossen Teil nicht mehr habe ansehen und kontrollieren können. Diese Vorbringen können dem Beschuldigten nicht widerlegt werden. Hinzuweisen ist namentlich auch darauf, dass er nicht über derart viel verbotene Pornografie verfügte, so dass diese Vorbringen von vorn- herein als unglaubhaft erschienen. Dies gilt insbesondere vor dem Hintergrund, dass er auch animierte Bilddateien (GIF) besass, bei denen es sich um Duplikate von unikalen Bilddateien handelt (Urk. 11/3 S. 2), was für nicht weniger als 56 der 66 als tatsächlich kinderpornografisch eingestuften Bilder gilt und die Gesamtzahl an Dateien nochmals relativiert. Schliesslich erwog die Vorinstanz, es sei "generell nicht unüblich", dass kinderpornografische Inhalte gezielt in grossen Datenpaketen mit mehrheitlich legalen pornografischen Inhalten "versteckt" würden, um deren Entdeckung durch die Strafbehörden zu erschweren (Urk. 36 S. 22). Weshalb dar- aus auf das Wissen des Beschuldigten geschlossen werden könnte, ist indes nicht ersichtlich. Notorisch wäre die vorinstanzliche Erwägung – so sie denn überhaupt zutrifft – jedenfalls nicht.

E. 3.3.1

Die Strafprozessordnung regelt nur die Erhebung von Beweisen durch die staatlichen Strafbehörden. Diese klären von Amtes wegen alle für die Beurteilung der Tat und der beschuldigten Person bedeutsamen Tatsachen ab (Art. 6 Abs. 1 StPO) und setzen zur Wahrheitsfindung alle nach dem Stand von Wissenschaft

- 8 - und Erfahrung geeigneten Beweismittel ein, die rechtlich zulässig sind (Art. 139 Abs. 1 StPO). Der Untersuchungsgrundsatz gemäss Art. 6 StPO begründet kein staatliches Monopol für Beweiserhebungen im Strafverfahren. Eigene Ermittlungen der Parteien und der anderen Verfahrensbeteiligten sind zulässig, soweit sie sich darauf beschränken, Be- oder Entlastungsmaterial beizubringen und entspre- chende Beweise zu offerieren (Urteil des Bundesgerichts 6B_301/2022 vom 26. August 2022 E. 2.2.2 mit Hinweisen). Die Strafprozessordnung enthält Bestim- mungen zu den verbotenen Beweiserhebungen (Art. 140 StPO) und zur Verwert- barkeit rechtswidrig erlangter Beweise (Art. 141 StPO). Wieweit die Beweisverbote auch greifen, wenn nicht staatliche Behörden, sondern Privatpersonen Beweis- mittel sammeln, wird in der Strafprozessordnung nicht explizit

geregelt. Nach der Rechtsprechung sind von Privaten rechtmässig erlangte Beweismittel ohne Einschränkungen im Strafprozess verwertbar. Von Privaten rechtswidrig erlangte Beweise sind dagegen nur verwertbar, wenn sie von den Strafverfolgungsbehörden rechtmässig hätten erhältlich gemacht werden können und kumulativ dazu eine Interessenabwägung für deren Verwertung spricht. Bei der Interessenabwägung ist derselbe Massstab wie bei von den Strafbehörden rechtswidrig erhobenen Bewei- sen anzuwenden. Die Verwertung ist damit nur zulässig, wenn sie im Sinne von Art. 141 Abs. 2 StPO zur Aufklärung einer schweren Straftat unerlässlich ist (Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.3.1 mit Hinweisen). Nachfolgend ist daher zunächst zu klären, ob die von Microsoft vorgenommene Verdachtsmeldung, die über die Organisation NCMEC an das Bundesamt für Polizei weitergeleitet wurde, als staatliche oder private Beweiserhebung zu qualifi- zieren ist.

E. 3.3.2

Wie die Vorinstanz zutreffend erwog, sind Provider nach der amerikanischen Gesetzgebung verpflichtet, dem NCMEC verdächtige kinderpornografische Darstellungen zu melden. Rechtsgrundlage hierfür bildet der 18 U.S. Code § 2258A (Urk. 36 S. 11). Eine Pflicht zur systematischen Kontrolle der übermittelten Daten wird im entsprechenden Erlass indes nicht statuiert. Vielmehr wird explizit fest- halten, dass die Provider nicht verpflichtet sind, Nutzer oder den Inhalt der Kommunikation zu überwachen (§ 2258A [f]). Bei Microsoft handelt es sich um ein US-amerikanisches Technologieunternehmen, das unter anderem die Such-

- 9 - maschine BingImage anbietet. Als Provider hat es die vom amerikanischen Gesetzgeber aufgestellten Vorgaben zu erfüllen. Als privates Unternehmen kann es zudem weitergehende eigene Regeln aufstellen und Massnahmen ergreifen, um diese Regeln wirksam durchzusetzen. Aufgrund der grossen Datenmengen, die täglich über die sozialen Medien verbreitet werden, wäre eine manuelle Miss- brauchskontrolle kaum zu bewältigen. Um eine missbräuchliche Verwendung der von ihnen zur Verfügung gestellten sozialen Plattformen (insbesondere durch die Verbreitung von kinderpornografischen Erzeugnissen) zu verhindern, haben die Provider daher technische Lösungen entwickelt, die eine automatisierte Kontrolle ermöglichen. Konkret und stark vereinfacht dargestellt bringen amerikanische Provider Technologien zum Einsatz, die mittels Suchalgorithmen (Listen mit Hashwerten) in der Lage sind, geteilte bzw. verschickte Bilder mit bereits bekannten kinderpornografischen Bildern abzugleichen und die Übereinstimmungen zeitnah zu erkennen. Die Hashwerte, welche in Form einer Buchstaben-Zahlen-Kombina- tion das Extrakt der Datei bilden, werden auch als elektronische Fingerabdrücke bezeichnet (Urteil des Obergerichts Solothurn STBER.2022.64 vom 8. März 2024 E. 4.2.1). Eine Übereinstimmung der Hashwerte begründet den Verdacht, dass die geprüfte Datei einen illegalen Inhalt aufweist. Gemäss den Akten nahm Microsoft am 24. August 2021 die Meldung an das NCMEC vor, nachdem festgestellt worden war, dass über seine Internetsuchmaschine BingImage eine Datei mit vermeintlich illegalem Inhalt hochgeladen wurde. Wie sich aus dem CyberTipline Report vom 24. August 2021 ergibt, erfolgte die Meldung an das NCMEC automatisiert, ohne dass eine inhaltliche Kontrolle der fraglichen Bilddatei erfolgt wäre. Vielmehr ergab ein Vergleich der Hashwerte ein Verdacht auf einen strafbaren Inhalt, weshalb Mi- crosoft das NCMEC – ohne Einblick in die Datei – mit den obligatorischen Informa- tionen bediente (CyberTipline Report unter Urk. 2 S. 2). Beim NCMEC handelt es sich um eine private gemeinnützige Organisation, die eine

Schnittstellenfunktion zwischen den Internetplattformen und den Strafverfolgungsbehörden einnimmt (Ur- teil des Obergerichts Zürich SB220372 vom 18. Januar 2023 E. II.3.1, publiziert in ZR 122/2023 S. 167 ff.; Urteil des Obergerichts Solothurn STBER.2022.64 vom

E. 3.3.3

Wie bereits aufgezeigt, sind sowohl Microsoft als auch das NCMEC privat- rechtlich organisiert, was für eine private Beweiserhebung spricht. Bei der Frage der Zurechnung des erhobenen Beweises darf indes nicht unberücksichtigt bleiben, dass der Staat den Privaten nicht Aufgaben delegieren darf, um sich auf diese Weise der Bindung an die Grundrechte zu entziehen. Dementsprechend wird eine Zurechnung des privaten Verhaltens zum Staat in der strafprozessualen und ver- fassungsrechtlichen Zurechnungsdogmatik insbesondere dann befürwortet, wenn die Privatperson im staatlichen Auftrag oder nach Weisung staatlicher Behörden tätig oder als staatliches Werkzeug eingesetzt wird (BSK StPO-GLESS, 3. Aufl. 2023, N 40b zu Art. 141; GODENZI, Private Beweisbeschaffung im Strafprozess, Zürich/Basel/Genf 2008, S. 175 f.). Es ist nicht von der Hand zu weisen, dass NC-

- 11 - MEC mit der Weiterleitung der Verdachtsmeldungen im öffentlichen Interesse lie- gende Aufgaben erfüllt. Die freiwilligen Kontrollsysteme der Provider erscheinen sodann auch als Folge eines gewissen politischen bzw. staatlichen Drucks. Mass- gebend ist indes, dass wie bereits dargelegt keine gesetzliche Verpflichtung der Provider besteht, den Datenverkehr inhaltlich zu überwachen bzw. nach strafbaren Inhalten zu suchen. Ihre Verpflichtung besteht lediglich darin, bei Verstössen eine Verdachtsmeldung an das NCMEC zu machen. Zudem verfügen die Anbieter auch über ein erhebliches eigenes Interesse daran, eine missbräuchliche Verwendung ihrer Plattformen zu verhindern. Es besteht darin, Reputationsschäden zu vermei- den, die bei einem Missbrauch ihrer Angebote drohen. Derartige Reputationsschä- den können sich etwa in der abnehmenden Anzahl von Nutzern, in der Zusamme- narbeit mit Werbepartnern und in der Schädigung der Marke niederschlagen. Unter diesem Aspekt liegt es im eigenen wirtschaftlichen Interesse der Anbieter, den Erwartungen einer breiten Öffentlichkeit Rechnung zu tragen, dass soziale Medien nicht zum rechtsfreien Raum verkommen. Gleichzeitig dürfte es den Betreibern solcher Plattformen mit der Missbrauchsbekämpfung auch darum gehen, einer staatlichen Regulierung zuvorzukommen, die beispielsweise in einer Ausweitung der Haftung auf die Provider bestehen könnte. Fraglich ist zudem, inwiefern ein Durchsetzungsmechanismus besteht, wenn die freiwillige Kontrolle unterbleibt. Unter diesen Umständen ist die Erhebung der die inkriminierte Datei betreffenden Informationen und Zuordnung derselben an die IP-Adresse in der Schweiz durch Microsoft unter Mitwirkung des NCMEC als private autonome Beweiserhebung zu qualifizieren (vgl. dazu auch Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.4.1). Soweit die Argumentation der Verteidigung auf der unzutreffenden Annahme aufbaut, dass es sich bei der vorliegend vorgenommenen Informations- erfassung um eine den Strafverfolgungsbehörden vorbehaltene Zwangsmass- nahme im Sinne von Art. 196 ff. StPO handelt (Urk. 24 S. 8 ff.; Urk. 40 S. 7 ff.), ist darauf nicht weiter einzugehen. Wie erwähnt, liegt keine staatlich angeordnete Beweismassnahme, sondern eine private Datenerhebung vor, deren Verwertbar- keit im Strafprozess sich nach anderen Grundsätzen richtet (Urteil des Bundesge- richts 6B_219/2022 vom 15. Mai 2024 E. 1.5.).

E. 3.3.4

Wie eingangs dargelegt, sind von Privaten rechtmässig erlangte Beweise ohne Einschränkungen im Strafprozess verwertbar. Rechtswidrig erlangte Beweise sind dagegen nur verwertbar, wenn sie von den Strafverfolgungsbehörden recht- mässig hätten erhältlich gemacht werden können und eine Interessenabwägung für deren Verwertung spricht. Als rechtswidrig erlangt gelten namentlich Beweise, die unter Verletzung des Bundesgesetzes über den Datenschutz erlangt wurden (Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.3.2). Der Verteidigung ist beizupflichten, dass die Provider mit den automatisierten Erkennungsprogrammen in die Privatsphäre ihrer Nutzer eingreifen. Die Erhebung von Nutzerdaten durch einen Provider ist als datenschutzrechtlich relevanter Vorgang einzustufen (vgl. dazu auch Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.4.2). Das Datenschutzrecht ergänzt und konkretisiert den bereits im Zivilge- setzbuch, insbesondere in Art. 28 ZGB, gewährleisteten Persönlichkeitsschutz (BGE 147 IV 16 E. 2.2). Entscheidend ist vorliegend indes, dass Microsoft nicht im Geheimen agiert, sondern jeden Nutzer, der das Angebot von BingImage nutzen möchte, in den Nutzungsbedingungen umfassend über die Bearbeitung seiner Personendaten informiert. Es kann diesbezüglich auf die zutreffenden Ausführ- ungen der Vorinstanz verwiesen werden (Urk. 36 S. 14 f.). Die vorinstanzlichen Erwägungen zu den Nutzungsbedingungen von Microsoft wurden von der Verteidi- gung im Berufungsverfahren nicht beanstandet. Vorgebracht wurde indes, dass Mi- crosoft eine monopolähnliche Marktstellung habe. Im Übrigen seien sämtliche Pro- vider verpflichtet, flächendeckend alle Bildversande zu überprüfen. Wer das Internet nutzen wolle, habe keine andere Wahl, als in die Nutzungsbedingungen und die Datenfreigabe einzuwilligen. Es sei zudem fraglich, ob die entsprechenden Bestimmungen in den Nutzungsbedingungen nicht überraschend seien und ob der Einwilligende den Umfang der Auswertung und die technischen Möglichkeiten richtig habe erfassen können. Im Ergebnis sei die Einwilligung weder nach ange- messener Information noch ausdrücklich erfolgt (Urk. 40 S. 9). Wie bereits von der Vorinstanz dargelegt, macht Microsoft jedem Nutzer in seinen Nutzungsbedingun- gen transparent, dass die Verwendung seiner Dienste mit einer Überprüfung der Einhaltung der geltenden strafrechtlichen Normen einhergeht und er sich diesbe- züglich einer Kontrolle des Providers aussetzt. Dabei wird auch auf verwendeten

 Tools zur Erkennung von strafbaren Inhalten hingewiesen (Hash-Abgleichtechno- logien). In den Nutzungsbedingungen wird sodann ausdrücklich darauf hinge- wiesen, dass Inhalte bei einem Verdacht auf sexuelle Ausbeutung und sexuellen Missbrauch von Kindern an das NCMEC gemeldet werden. Explizit erwähnt wird auch die Weitergabe visueller Medien mit sexuellem Inhalt, die ein Kind betreffen oder sexualisieren. Die Nutzer werden damit über Gegenstand, Zweck und Umfang der beabsichtigten Datenbearbeitung sowie über die daraus resultierenden Risiken aufgeklärt. Damit sollte jedem Nutzer hinreichend klar sein, dass eine Kontrolle der geteilten Inhalte, insbesondere bezüglich Kinderpornografie, stattfindet und seine Daten bei Verdacht auf strafrechtlich relevante Verhaltensweisen weitergegeben werden. Entgegen der Ansicht der Verteidigung ist daher von einer angemessenen Information auszugehen. Die Nutzer erklären sich mit den vom Unternehmen definierten Regeln betreffend Datenerhebung, -verwendung und -weitergabe an Dritte ausdrücklich einverstanden, indem sie ein Microsoft-Konto erstellen und die Dienste von Microsoft nutzen. Entgegen der Ansicht der Verteidigung weisen die Nutzungsbestimmungen keinen ungewöhnlichen oder überraschenden Inhalt auf. Vielmehr entspricht es dem allgemeinen Erfahrungswissen, dass in den Allgemei- nen

Geschäftsbedingungen von Internetplattformen insbesondere auch Fragen der Privatsphäre geregelt werden. Die Datenerhebung, -verwendung und -weitergabe (insbesondere auch zu Marketingzwecken) ist regelmässig Bestandteil des Geschäftsmodells dieser Anbieter, was sich auch dem gewöhnlichen Nutzer nicht verschliessen kann. Ebenso wenig überrascht, dass solche Unternehmen aus eigenem Interesse strafbare und gesellschaftlich stark geächtete Inhalte wie Kinderpornografie auf ihren Plattformen aktiv bekämpfen und zu diesem Zweck auch mit Dritten zusammenarbeiten. Der Kunde hat demzufolge auch mit solchen Regeln zu rechnen. Dass auf Internetplattformen eine gewisse Missbrauchs- kontrolle stattfindet, muss daher ebenfalls als notorisch bezeichnet werden. Auch wenn dem Beschuldigten im Detail allenfalls nicht bewusst gewesen sein dürfte, welche Daten in welcher Form kontrolliert und weitergegeben werden, kann die Regelung von Microsoft nicht als derart aussergewöhnlich oder geschäftsfremd bezeichnet werden, dass man mit ihr nicht rechnen müsste. Nachdem Microsoft bekanntermassen in den USA ansässig ist und von dort aus seiner Unter-

- 14 - nehmenstätigkeit nachgeht, muss einem Nutzer auch klar sein, dass Informationen betreffend seine Inhalte in die USA gelangen könnten, zumal die Organisation NC- MEC in den Nutzungsbedingungen von Microsoft wie erwähnt explizit genannt wird (vgl. dazu Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.6.3). Im Ergebnis ist die Einwilligung mit der Vorinstanz als rechtsgültig zu bezeichnen.

E. 3.4

Insgesamt verbleiben somit zu viele Zweifel daran, ob der Beschuldigte in Kauf genommen hat, kinderpornografisches Material herunterzuladen. Diese Zweifel sind für das Gericht nicht überwindbar. Es kann ihm nicht rechtsgenügend widerlegt werden, dass die tatbestandsmässigen Bilder ohne sein Wissen auf seine Datenträger gelangt sind und dass er auch keine Anhaltspunkte dafür haben musste, es könnte sich verbotene Kinderpornografie unter seinen Dateien befin- den. Der Beschuldigte ist entsprechend nach dem Grundsatz in dubio pro reo vom Vorwurf des mehrfachen Konsums von harter Pornografie im Sinne von Art. 197 Abs. 5 Satz 1 und 2 aStGB freizusprechen.

- 28 -

E. 3.5

Zusammen mit dem bereits unter E. II.2.6 erwähnten Freispruch vom Vor- wurf der harten Pornografie im Sinne von Art. 197 Abs. 4 Satz 1 in Verbindung mit Satz 2 StGB hat demnach ein vollumfänglicher Freispruch zu ergehen. V. Kosten- und Entschädigungsfolgen 1. Die Gerichtsgebühr für das Berufungsverfahren ist praxisgemäss auf Fr. 3'600.– festzusetzen (Art. 424 StPO i.V.m. § 16 Abs. 1 und § 14 GebV OG). 2. Für die Verteidigung des Beschuldigten im Berufungsverfahren werden vom amtlichen Verteidiger Fr. 9'928.45 (inkl. MwSt und Barauslagen; Urk. 54) geltend gemacht. Gemäss § 18 Abs. 1 AnwGebV OG in Verbindung mit § 17 Abs. 1 lit. b AnwGebV OG reicht der anwendbare Tarifrahmen für das Verteidigerhonorar im Berufungs- prozess bei Straffällen im – wie vorliegend – Zuständigkeitsbereich eines Einzelge- richts in der Regel von Fr. 600.– bis Fr. 8'000.–. Konkret erfolgt die Festsetzung der Entschädigungssumme bei einer Honorarbemessung nach Pauschalgebühr so, dass alle prozessualen Bemühungen zusammen als einheitliches Ganzes aufge- fasst werden, wohingegen der tatsächlich geleistete Zeitaufwand nur sehr bedingt berücksichtigt wird. Entsprechend ist das Gericht bei der rein pauschalen Entschä- digungsbemessung auch nicht gehalten, sich mit den in der

Honorarnote der Verteidigung enthaltenen Aufwandspositionen im Einzelnen auseinanderzusetzen (BGE 143 IV 453 E. 2.5). Nach Massgabe von § 2 Abs. 1 AnwGebV OG bemisst sich die Gebühr vielmehr vor allem nach der Bedeutung der Strafsache, der Verantwortung der Verteidigung und der Schwierigkeit des Falls. Vorliegend ist zu berücksichtigen, dass für den Beschuldigten, der sich in Aus- bildung zum Sekundarschullehrer befindet, das Verfahren zwar von erheblicher Bedeutung war, weil ein lebenslanges Tätigkeitsverbot zur Beurteilung stand. Hingegen weist der Fall keine komplexen rechtlichen Fragen auf. Ungeachtet der Bedeutung des Verfahrens für den Beschuldigten persönlich ist auch die Tragweite des Falles innerhalb der Bandbreite der möglichen Delikte als durchschnittlich zu bezeichnen. In Anbetracht der dargelegten Umstände erweist sich der geltend ge-

- 29 - machte, bereits ausserhalb der Regelbandbreite für die Grundgebühr in einzelgerichtlichen Verfahren liegende Aufwand von rund Fr. 9'928.45 als deutlich zu hoch. Als angemessen erscheint ein Pauschalbetrag von Fr. 6'000.– (inkl. MwSt und Barauslagen). Der amtliche Verteidiger, Rechtsanwalt Dr. iur. X._____, ist daher mit Fr. 6'000.– (inkl. MwSt und Barauslagen) aus der Gerichtskasse zu entschädigen. 3. Bei diesem Ausgang des Verfahrens sind die Kosten der Untersuchung und der gerichtlichen Verfahren in beiden Instanzen, einschliesslich derjenigen der amtlichen Verteidigung, auf die Gerichtskasse zu nehmen (Art. 426 Abs. 1 Satz 1 StPO und Art. 428 Abs. 1 und 3 StPO).

- 30 - Es wird beschlossen:

E. 8

März 2024 E. 4.2.1). Die von den Plattformanbietern übermittelten Daten werden vom NCMEC an die Strafverfolgungsbehörden weitergeleitet, wobei weder Unter-

- 10 - suchungen durchgeführt noch die übermittelten Informationen überprüft werden (vgl. dazu Cyber Tipline Report unter Urk. 2: Incident Type: Auto-referred Internati- onal. Files Not Reviewed by NCMEC, NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties). Alle wesentlichen Informationen werden vom Pro- vider beigesteuert. Soweit der NCMEC-Meldung weitere Informationen beigefügt werden, stammen diese aus öffentlich zugänglichen Quellen. Zu verweisen ist hier etwa auf die örtliche Zuordnung der IP-Adresse. NCMEC verknüpft die Verdachts- meldung des Providers mit Hilfe der anhand der IP-Adresse ermittelten ungefähren Geolokalisierungsdaten, die den Standort des Nutzers abschätzen lassen (vgl. dazu CyberTipLine Report unter Urk. 2 S. 4: Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "Suspect", NCMEC Systems will geogra- phically resolve the IP address via a publicly available online query […] Geolocation date is approximate and may not display a user's exact location). Die Tätigkeit von NCMEC beschränkt sich daher im Wesentlichen auf die Weiterleitung von Ver- dachtsmeldungen an die Behörden. Dessen Mitarbeitende nehmen – wie auch diejenigen von Microsoft – keinen Einblick in die fragliche Datei. Entgegen den Vor- bringen der Verteidigung (Urk. 24 S. 8 f.; Urk. 40 S. 7 f.) kann unter diesen Umstän- den nicht von einer flächendeckenden inhaltlichen Kontrolle sämtlicher elektroni- schen Kommunikation gesprochen werden.