

Obergericht des Kantons Zürich

I. Strafkammer



Geschäfts-Nr.: SB230481-O/U/cwo

Mitwirkend: Oberrichter lic. iur. M. Langmeier, Präsident, die Ersatzoberrichterinnen lic. iur. C. Laufer und MLaw N. Menghini-Griessen sowie der Gerichtsschreiber MLaw S. Zuber

Urteil vom 23. Oktober 2024

in Sachen

A. _____,

Beschuldigter und Berufungskläger

amtlich verteidigt durch Rechtsanwalt Dr. iur. X. _____

gegen

Staatsanwaltschaft Limmattal / Albis,

Anklägerin und Berufungsbeklagte

betreffend **Pornografie etc.**

**Berufung gegen ein Urteil des Bezirksgerichts Horgen, Einzelgericht,
vom 17. Juli 2023 (GG230012)**

Anklage:

Die Anklageschrift der Staatsanwaltschaft Limmattal / Albis vom 1. März 2023 (Urk. 18) ist diesem Urteil beigeheftet.

Urteil der Vorinstanz:

(Urk. 36 S. 45 ff.)

" Es wird erkannt:

1. Der Beschuldigte ist schuldig
 - der harten Pornografie im Sinne von Art. 197 Abs. 4 Satz 1 in Verbindung mit Satz 2 StGB sowie
 - des mehrfachen Konsums von harter Pornografie im Sinne von Art. 197 Abs. 5 Satz 1 und 2 StGB.
2. Der Beschuldigte wird mit einer Geldstrafe von 180 Tagessätzen zu je Fr. 40.00 bestraft.
3. Der Vollzug der Geldstrafe wird aufgeschoben und die Probezeit auf 2 Jahre festgesetzt.
4. Dem Beschuldigten wird lebenslang verboten, eine berufliche oder organisierte ausserberufliche Tätigkeit auszuüben, die einen regelmässigen Kontakt zu Minderjährigen umfasst (Tätigkeitsverbot im Sinne von Art. 67 Abs. 3 lit. d Ziff. 2 StGB).
5. Dem Beschuldigten wird im Sinne von Art. 44 Abs. 2 in Verbindung mit Art. 94 StGB die Weisung erteilt, sich für die Dauer der Probezeit einer ambulanten deliktsbezogenen psychologischen Behandlung nach den Vorgaben des Amts für Justizvollzug und Wiedereingliederung des Kantons Zürich zu unterziehen.
6. Die folgenden, mit Verfügung der Staatsanwaltschaft Limmattal / Albis vom 1. März 2023 beschlagnahmten Gegenstände werden eingezogen vernichtet:
 - Mobiltelefon der Marke "Huawei" (Asservat-Nr. A016'109'776)
 - SIM-Karte (Asservat-Nr. A016'163'589)
 - Micro SD Card (Asservat-Nr. A016'163'603)
 - Computer der Marke "Asus" (Asservat-Nr. A016'109'903)
 - Festplatte der Marke "Toshiba" (Asservat-Nr. A016'163'647)
 - Festplatte der Marke "Kingston" (Asservat-Nr. A016'163'669).

Die Lagerbehörde wird angewiesen, diese Anordnung nach Eintritt der Rechtskraft zu vollziehen.

7. Rechtsanwalt Dr. iur. X._____ wird für seine Bemühungen und Auslagen als amtlicher Verteidiger mit Fr. 10'620.45 (Betrag enthält MwSt. und Auslagen) aus der Gerichtskasse entschädigt.

8. Die Entscheidgebühr wird festgesetzt auf:

Fr. 2'400.00 ; die weiteren Kosten betragen:

Fr. 1'500.00 Gebühr des Vorverfahrens

Fr. 10'620.45 Entschädigung für die amtliche Verteidigung
(RA Dr. iur. X._____)

Allfällige weitere Kosten bleiben vorbehalten.

9. Die Kosten der Untersuchung und des gerichtlichen Verfahrens, ausser diejenigen der amtlichen Verteidigung, werden dem Beschuldigten auferlegt. Die Kosten der amtlichen Verteidigung werden auf die Gerichtskasse genommen; vorbehalten bleibt eine Nachforderung gemäss Art. 135 Abs. 4 StPO.

10. [Mitteilungen]

11. [Rechtsmittel] "

Berufungsanträge:
(Prot. II S. 4 f.)

a) Der Verteidigung des Beschuldigten (Urk. 52):

- " 1. Es seien Dispositiv Ziffern 1. - 5. und 9. des Urteils des Bezirksgerichts Horgen vom 17. Juli 2023, Gesch.-Nr. GG230012, aufzuheben.
2. Es sei der Beschuldigte und Berufungskläger von sämtlichen Vorhalten gemäss Anklage der Staatsanwaltschaft Limmattal/ Albis vom 1. März 2023 von Schuld und Strafe frei zu sprechen und von Massnahmen oder Weisungen abzusehen.
3. Es seien die Verfahrenskosten samt Kosten der amtlichen Verteidigung der Voruntersuchung, des Verfahrens vor dem Bezirksgericht Horgen und des Berufungsverfahrens auf die Staatskasse zu nehmen.

4. Eventualiter sei durch die Berufungsinstanz, subeventualiter durch die Vorinstanz

zu prüfen und mittels (nötigenfalls rechtshilfeweise) beizuziehender Akten zu dokumentieren, wie die im CyberTipline Report 1 vom 24. August 2021 (act. 2) zitierte, von Microsoft - Online Operations ausgehende Meldung, wonach am 23. August 2021 von der IP-Adresse Nr. 2 eine Bilddatei kinderpornografischen Inhalts via Bing Image ins Internet hochgeladen worden sein soll, zustande kam.

5. Eventualiter sei durch die Berufungsinstanz, subeventualiter – nach entsprechender Rückweisung – durch die Vorinstanz oder die Staatsanwaltschaft der Inhalt der auf den sichergestellten Datenträger enthaltenen Bilder legalen pornografischen Inhalts transparent zu machen.
6. Eventualiler sei durch die Berufungsinstanz, subeventualiter durch die Vorinstanz oder Staatsanwaltschaft mittels Beizugs eines Experten prüfen zu lassen, ob der inkriminierte Bildupload via Bing gemäss CyberTipLine Report 1 vom 24. August 2021 auch durch Schadsoftware ausgelöst worden sein könnte bzw. ausgelöst wurde.
7. Eventualiler sei durch die Berufungsinstanz, subeventualiter durch die Vorinstanz oder die Staatsanwaltschaft prüfen zu lassen, wieviele der sichergestellten Dateien legalen pornografischen Inhalts waren.
8. Unter Kosten- und Entschädigungsfolgen inkl. MWSt zu Lasten der Staatskasse. "

b) Der Staatsanwaltschaft (Urk. 46):

Bestätigung des vorinstanzlichen Urteils.

Erwägungen:

I. Verfahrensgang und Prozessuales

1. Verfahrensgang

1.1. Mit Urteil des Bezirksgerichts Horgen, Einzelgericht, vom 17. Juli 2023 wurde der Beschuldigte wegen harter Pornografie sowie mehrfachen Konsums von harter Pornografie mit einer bedingten Geldstrafe von 180 Tagessätzen zu Fr. 40.– bestraft. Die Vorinstanz ordnete ein lebenslängliches Tätigkeitsverbot an und erteilte dem Beschuldigten die Weisung, sich für die Dauer der Probezeit einer ambulanten deliktsbezogenen psychologischen Behandlung nach den Vorgaben des Amts für Justizvollzug und Wiedereingliederung des Kantons Zürich zu unterziehen. Im Weiteren befand sie über die von der Staatsanwaltschaft beschlagnahmten Gegenstände und regelte die Kosten des Vorverfahrens und erstinstanzlichen Gerichtsverfahrens (Urk. 36 S. 45 ff.).

1.2. Gegen dieses Urteil liess der Beschuldigte mit Eingabe vom 24. Juli 2023 fristgerecht Berufung anmelden (Urk. 31). Das begründete Urteil wurde der Verteidigung am 14. September 2023 zugestellt (Urk. 35/2). Mit Eingabe vom 4. Oktober 2023 reichte diese innert der zwanzigtägigen Frist von Art. 399 Abs. 3 StPO die Berufungserklärung ein (Urk. 40). Die Staatsanwaltschaft beantragte mit Eingabe vom 13. Oktober 2023 (Datum Eingang) die Bestätigung des vorinstanzlichen Urteils (Urk. 46). Am 1. Juli 2024 wurde zur Berufungsverhandlung auf den 23. Oktober 2024 vorgeladen (Urk. 47).

1.3. Zur Berufungsverhandlung erschien der Beschuldigte persönlich in Begleitung seines amtlichen Verteidigers, Rechtsanwalt Dr. iur. X._____. Vorfragen waren keine zu entscheiden. Das Urteil wurde dem Beschuldigten mündlich eröffnet und im Dispositiv übergeben (Prot. II S. 4 und S. 9).

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

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.

3. Verwertbarkeit der Beweismittel

3.1. Ausgangslage

Dem Beschuldigten wird in der Anklageschrift vom 1. März 2023 vorgeworfen, über das Internet Bilddateien mit strafbarem pornografischen Inhalt heruntergeladen und auf seinem Mobiltelefon sowie zwei Festplatten gespeichert zu haben. Weiter wird ihm zur Last gelegt, ein Bild mit tatsächlichen sexuellen Handlungen mit Minderjährigen via Microsoft Bing Upload anderen Internetnutzern zugänglich gemacht zu haben (Urk. 18 S. 2 f.). Die Vorinstanz hat zutreffend dargelegt, wie es zur Einleitung des Strafverfahrens gegen den Beschuldigten kam. Auf ihre Erwägungen kann vorab verwiesen werden (Urk. 36 S. 4 ff.). Kurz zusammengefasst wurde der US-amerikanischen Organisation National Center for Missing and Exploited Children (nachfolgend: NCMEC) am 24. August 2021 vom Technologieunternehmen Microsoft gemeldet, dass der Nutzer der IP-Adresse 2 in Verdacht stehe, kinderpornografisches Material via BingImage verbreitet zu haben. Das NCMEC leitete den CyberTipline Report gleichentags an das Bundesamt für Polizei weiter. Die Ermittlungen dieser Behörde ergaben in der Folge, dass es sich bei der Anschlussinhaberin der gemeldeten IP-Adresse um die Mutter des Beschuldigten handelt. Gestützt auf die Meldung des NCMEC und die polizeilichen Ermittlungen wurde am 26. April 2022 am Wohnort des Beschuldigten eine Hausdurchsuchung durchgeführt, wobei ein Mobiltelefon, ein Notebook und ein Computer sichergestellt wurden. Auf drei Datenträgern (Mobiltelefon und zwei Festplatten) wurde potentiell deliktsrelevantes Material festgestellt (Urk. 1 ff.; Urk. 11/1 ff.).

3.2. Vorbringen der Verteidigung

Die Verteidigung machte vor Vorinstanz geltend, dass sämtliche Beweise, die der Anklage zugrunde lägen, nicht verwertbar seien. Zur Begründung brachte sie vor, dass gemäss US-amerikanischem Recht für alle Provider eine Pflicht bestehe, verdächtige Internetinhalte beim NCMEC zu melden. Da die Anlass des vorliegenden Strafverfahrens bildende Bilddatei nicht autonom, sondern im Auftrag des Staates gesammelt worden sei, müssten die Regeln gelten, die zur Anwendung kämen, wenn die Strafbehörden selbst handeln würden. Bei der vom Provider vorgenommenen Auswertung handle es sich um eine geheime Überwachungs- bzw. zumindest eine Durchsuchungsmassnahme. In jedem Fall stelle spätestens die Erhebung von Verbindungsnachweis, Zeit, Art des Downloads sowie IP-Adresse des Absenders oder Empfängers eine Zwangsmassnahme dar, die einem hinreichenden Tatverdacht voraussetze und verhältnismässig sein müsse. Da gemäss US-amerikanischem Recht sämtliche Inhalte von Nutzern nach kinderpornografischem Material gefiltert und verglichen würden, stehe auch fest, dass diese Echtzeit-Vergleiche ohne Anfangsverdacht erfolgten. Nach Schweizerischem Recht bestehe keine gesetzliche Grundlage für die systematische Überwachung sämtlicher Bildversendungen. Im Gegenteil liege ein Verstoss gegen das Datenschutzgesetz vor. Schliesslich sei der Eingriff in die Grundrechte auch nicht verhältnismässig, da es sich um eine systematische Überwachung handle. Bei den Voraussetzungen nach Art. 197 Abs. 1 StPO handle es sich um Gültigkeitsvorschriften. Damit seien die Ergebnisse des Berichts des Bundesamts für Polizeij, die auf der Meldung des NCMEC beruhten, nicht verwertbar, zumal keine schwere Straftat im Sinne von Art. 141 Abs. 2 StPO vorliege. Der Beschuldigte sei daher schon aus formellen Gründen freizusprechen (Urk. 24 S. 7 ff.). Daran hielt die Verteidigung mit ausführlicher Begründung im Berufungsverfahren fest (Urk. 40 S. 3 ff.).

3.3. Würdigung

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

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 entsprechende Beweise zu offerieren (Urteil des Bundesgerichts 6B_301/2022 vom 26. August 2022 E. 2.2.2 mit Hinweisen). Die Strafprozessordnung enthält Bestimmungen zu den verbotenen Beweiserhebungen (Art. 140 StPO) und zur Verwertbarkeit rechtswidrig erlangter Beweise (Art. 141 StPO). Wieweit die Beweisverbote auch greifen, wenn nicht staatliche Behörden, sondern Privatpersonen Beweismittel 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 Beweisen 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 qualifizieren ist.

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 festgehalten, 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-

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 Missbrauchskontrolle 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-Kombination 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 Microsoft das NCMEC – ohne Einblick in die Datei – mit den obligatorischen Informationen 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 (Urteil 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 8. März 2024 E. 4.2.1). Die von den Plattformanbietern übermittelten Daten werden vom NCMEC an die Strafverfolgungsbehörden weitergeleitet, wobei weder Unter-

suchungen durchgeführt noch die übermittelten Informationen überprüft werden (vgl. dazu Cyber Tipline Report unter Urk. 2: Incident Type: Auto-referred International. 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 Provider 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 Verdachtsmeldung 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 geographically resolve the IP address via a publicly available online query [...] Geolocation data is approximate and may not display a user's exact location). Die Tätigkeit von NCMEC beschränkt sich daher im Wesentlichen auf die Weiterleitung von Verdachtsmeldungen an die Behörden. Dessen Mitarbeitende nehmen – wie auch diejenigen von Microsoft – keinen Einblick in die fragliche Datei. Entgegen den Vorbringen der Verteidigung (Urk. 24 S. 8 f.; Urk. 40 S. 7 f.) kann unter diesen Umständen nicht von einer flächendeckenden inhaltlichen Kontrolle sämtlicher elektronischen Kommunikation gesprochen werden.

3.3.3. Wie bereits aufgezeigt, sind sowohl Microsoft als auch das NCMEC privatrechtlich 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 verfassungsrechtlichen 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-

MEC mit der Weiterleitung der Verdachtsmeldungen im öffentlichen Interesse liegende Aufgaben erfüllt. Die freiwilligen Kontrollsysteme der Provider erscheinen sodann auch als Folge eines gewissen politischen bzw. staatlichen Drucks. Massgebend 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 vermeiden, die bei einem Missbrauch ihrer Angebote drohen. Derartige Reputationsschäden können sich etwa in der abnehmenden Anzahl von Nutzern, in der Zusammenarbeit 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 Informationserfassung um eine den Strafverfolgungsbehörden vorbehaltene Zwangsmassnahme 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 Verwertbarkeit im Strafprozess sich nach anderen Grundsätzen richtet (Urteil des Bundesgerichts 6B_219/2022 vom 15. Mai 2024 E. 1.5.).

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 rechtmässig 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 Zivilgesetzbuch, 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 Ausführungen der Vorinstanz verwiesen werden (Urk. 36 S. 14 f.). Die vorinstanzlichen Erwägungen zu den Nutzungsbedingungen von Microsoft wurden von der Verteidigung im Berufungsverfahren nicht beanstandet. Vorgebracht wurde indes, dass Microsoft eine monopolähnliche Marktstellung habe. Im Übrigen seien sämtliche Provider 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 angemessener Information noch ausdrücklich erfolgt (Urk. 40 S. 9). Wie bereits von der Vorinstanz dargelegt, macht Microsoft jedem Nutzer in seinen Nutzungsbedingungen transparent, dass die Verwendung seiner Dienste mit einer Überprüfung der Einhaltung der geltenden strafrechtlichen Normen einhergeht und er sich diesbezüglich einer Kontrolle des Providers aussetzt. Dabei wird auch auf verwendeten

Tools zur Erkennung von strafbaren Inhalten hingewiesen (Hash-Abgleichtechnologien). In den Nutzungsbedingungen wird sodann ausdrücklich darauf hingewiesen, 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 Allgemeinen 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 Missbrauchskontrolle 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-

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.

3.4. Fazit

Zusammenfassend kann festgehalten werden, dass die Beweiserhebung durch Microsoft rechtmässig erfolgte, weshalb die Verdachtsmeldung an das NCMEC verwertbar ist. Das NCMEC diente lediglich als Koordinationsstelle und erhob selbst keine Beweise, weshalb es auch nicht als Organ der Strafrechtspflege fungierte. Die gestützt auf die Verdachtsmeldung durchgeführten Zwangsmassnahmen und weiteren Ermittlungshandlungen verblieben im Zuständigkeitsbereich der Schweizer Strafverfolgungsbehörden. Deren Rechtmässigkeit wurde von der Verteidigung zu Recht nicht in Frage gestellt. Ihre Einwände beschlagen lediglich die Erhebung des Erstbeweises. Mit der Vorinstanz liegt daher keine Unverwertbarkeit von Beweismitteln vor. Damit ist noch nichts über die Zuverlässigkeit bzw. den Erkenntniswert der Verdachtsmeldung von Microsoft gesagt. Auf die entsprechenden Argumente der Verteidigung (Urk. 24 S. 7 f.; Urk. 40 S. 4 ff.) ist im Rahmen der Sachverhaltserstellung näher einzugehen.

II. Sachverhalt

1. Anklagesachverhalt 1: Herunterladen und Speichern von Bilddateien

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

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 durchgeführt, 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 pornografisches Material eingestuft wurden (Urk. 4 S. 3; Urk. 11/3 S. 2; Urk. 12, insbesondere 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 pornografischen 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 Böses" 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 heruntergeladenen 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.).

1.2. Wie die Vorinstanz zutreffend erwog, handelt es sich dabei um 66 Bilddateien mit realen minderjährigen Personen (Urk. 36 S. 20). Soweit die Verteidigung 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 aufgeführten 266 Bilddateien über das Internet heruntergeladen und auf ihm gehörenden Datenträgern abgespeichert hat.

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 Pornografische 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. Rechtsfrage ist hingegen, ob gestützt auf die festgestellten Tatsachen bewusste Fahrlässigkeit, 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 Erfahrungsregeln 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-

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

2.1. Dem Beschuldigten wird im zweiten Anklagepunkt vorgeworfen, am 23. August 2021 über die auf seine Mutter vergebene IP-Adresse von seinem Wohnort aus ein Bild mit tatsächlichen sexuellen Handlungen mit Minderjährigen anderen Internetnutzern via Microsoft Bing Upload zugänglich gemacht zu haben, indem er die Datei über die Bilder-Suchmaschine hochgeladen habe (Urk. 18 S. 3).

2.2. Der Beschuldigte bestritt schon im Vorverfahren und vor Vorinstanz, ein Bild mit tatsächlichen sexuellen Handlungen mit Minderjährigen über Microsoft Bing hochgeladen zu haben. Zusammengefasst brachte er vor, dass er diese Suchmaschine nicht verwende. Für Suchanfragen benutze er jeweils Google. Er könne sich nicht erklären, wie die Bildersuche zustande gekommen sei. Er habe nie wissentlich Bilder zur Verfügung stellen wollen (Urk. 7 S. 6 f. und 11; Prot. I S. 13 f.). Daran hielt er im Berufungsverfahren fest. Er könne sich den Upload schlicht nicht erklären, gab er zu Protokoll (Urk. 51).

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

worden sei, weshalb sein Vorbringen, wonach er seine elektronischen Geräte teilweise 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 abgespeichert habe. Die Aussagen des Beschuldigten seien daher als unglaubliche Schutzbehauptungen 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.).

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 durchaus 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,

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 Zirkelschluss. Die Vorinstanz stützt sich zur Widerlegung der Behauptung des Beschuldigten auf Umstände, die sie eigentlich erst erstellen möchte, womit sie das Resultat der Würdigung an den Anfang stellt und als gegeben voraussetzt. Der Vorinstanz kann daher nicht gefolgt werden, wenn sie die Aussagen des Beschuldigten aus diesem Grund als ungläubhafte Schutzbehauptungen wertet (Urk. 36 S. 25).

2.5. Die Vorinstanz hat zutreffend ausgeführt, dass die von Microsoft als kinderpornografisch eingestufte Bilddatei auf Datenträgern des Beschuldigten abgespeichert war (Urk. 36 S. 25). Dies ergab eine Auswertung der anlässlich der Hausdurchsuchung 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 Herunterladen und Abspeichern dieser Bilddatei bildet Bestandteil des ersten Anklagesachverhalts. 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 Strafverfolgungsbehörden weitergeleitete Verdachtsmeldung vor. Analog einer durch eine Privatperson erstellten Strafanzeige handelt es sich bei der in der Verdachtsmeldung enthaltenen 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 Erkennungsprogrammen der Provider basieren. Eine Kontrolle durch eine natürliche Person findet grundsätzlich nicht statt. NCMEC fungiert als Schnittstelle zwischen den Internetplattformen und den Strafverfolgungsbehörden und nimmt wie bereits erwähnt ebenfalls keine Ermittlungshandlungen vor. Die Mitarbeitenden des NCMEC erhalten wie auch diejenigen von Microsoft keinen Einblick in die gemeldete Bilddatei.

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 angelastete 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 fälschlicherweise dem Wohnort des Beschuldigten zugeordnet wurde. Gänzlich ausschliesslich 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.

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 Suchanfragen 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-

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 hochgeladen 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 ausdrücklich 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 zugänglich 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 Hausdurchsuchung 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 heruntergeladen 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 verbotenen pornografischen Inhalt anderen Nutzern über Microsoft Bing oder andere Provider zugänglich gemacht hätte. Nachdem die bei NCMEC eingehenden Meldungen jeweils innert Kürze den Strafverfolgungs-

behörden weitergeleitet werden, wäre zu erwarten, dass die Schweizer Behörden in diesem Fall informiert worden wären. Vor diesem Hintergrund kann nicht ausgeschlossen 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) freizusprechen. 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 Eigenkonsum 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-

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 Darbietungen objektiv betrachtet darauf ausgelegt sind, den Konsumenten sexuell aufzureizen. 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 WEISSENBARGER, 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

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

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

2.2. Gemäss erstelltem Sachverhalt hat der Beschuldigte mit den erwähnten Bildern mehrfach Bilddateien mit (tatsächlichen und virtuellen) sexuellen Handlungen 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

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 Minderjährigen in keiner Weise sexuell hingezogen. Bilder von Minderjährigen mit sexuellem 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 heruntergeladen 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 Bilddateien um einen Bruchteil aller beim Beschuldigten vorhandenen Dateien gehandelt 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).

3.2. Anlässlich der Berufungsverhandlung führte der Beschuldigte dazu weiter aus, dass er mittels eines online Programmes (mittels eines "Tools") legale Pornografie in Datenpaketen heruntergeladen habe. Das von ihm verwendete Programm finde er nicht mehr. Der Beschuldigte verwies stattdessen 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 eingegeben 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 Download angegeben. Der Beschuldigte erklärte weiter, dass die inkriminierten Bilder ohne sein Wissen zusammen mit legalen pornografischen Bildern mitheruntergeladen 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 gestartet habe, seien ihm nur Daten angezeigt worden, die er nach der Neuinstallation gespeichert habe. Als die Polizei ihm den Durchsuchungsbefehl wegen dem Verdacht auf Kinderpornografie vorgehalten habe, sei seine Vermutung, dass etwas nicht in Ordnung sein könnte, bestätigt worden (Urk. 51).

3.3. Die Vorinstanz erachtete den subjektiven Sachverhalt als erstellt. Diesbezüglich 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 kinderpornografische Daten aus dem Internet (mit-) heruntergeladen haben soll. Er selbst konnte diesbezüglich keine Angaben machen. Die in der Anklage erwähnten Daten

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 systembedingten Angaben handle, die nicht mit der tatsächlichen Zeit übereinstimmen müssten. 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 unglaublich, dass sich gleich in mehreren Downloads unbeabsichtigt auch Kinderpornografie befunden habe.

Die Vorinstanz hielt zudem fest, dass die Gesamtzahl an verbotener bzw. problematischer Bilder "durchaus nicht vernachlässigbar" sei, nachdem neben den 266 Bilddateien mit kinderpornografischem Material 92 Erzeugnisse mit Präferenzindikatoren 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 vernachlässigbar ist oder nicht. Der Anzahl Bilddateien mit Kinderpornografie kann zumindest unter diesen Umständen keine entscheidende Bedeutung zukommen. Im Verhältnis zu den gesamten 383'451 Bildern würden die 266 kinderpornografischen

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 aufzeigen, 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 vornherein 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 daraus auf das Wissen des Beschuldigten geschlossen werden könnte, ist indes nicht ersichtlich. Notorisch wäre die vorinstanzliche Erwägung – so sie denn überhaupt zutrifft – jedenfalls nicht.

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 befinden. 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.

3.5. Zusammen mit dem bereits unter E. II.2.6 erwähnten Freispruch vom Vorwurf 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 Berufungsprozess bei Straffällen im – wie vorliegend – Zuständigkeitsbereich eines Einzelgerichts 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 aufgefasst werden, wohingegen der tatsächlich geleistete Zeitaufwand nur sehr bedingt berücksichtigt wird. Entsprechend ist das Gericht bei der rein pauschalen Entschädigungsbemessung 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 Ausbildung 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-

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).

Es wird beschlossen:

1. Es wird festgestellt, dass das Urteil des Bezirksgerichts Horgen, Einzelgericht, vom 17. Juli 2023 wie folgt in Rechtskraft erwachsen ist:

" Es wird erkannt:

1.-5. [...]

6. Die folgenden, mit Verfügung der Staatsanwaltschaft Limmattal / Albis vom 1. März 2023 beschlagnahmten Gegenstände werden eingezogen vernichtet:

- Mobiltelefon der Marke "Huawei" (Asservat-Nr. A016'109'776)
- SIM-Karte (Asservat-Nr. A016'163'589)
- Micro SD Card (Asservat-Nr. A016'163'603)
- Computer der Marke "Asus" (Asservat-Nr. A016'109'903)
- Festplatte der Marke "Toshiba" (Asservat-Nr. A016'163'647)
- Festplatte der Marke "Kingston" (Asservat-Nr. A016'163'669).

Die Lagerbehörde wird angewiesen, diese Anordnung nach Eintritt der Rechtskraft zu vollziehen.

7. Rechtsanwalt Dr. iur. X. _____ wird für seine Bemühungen und Auslagen als amtlicher Verteidiger mit Fr. 10'620.45 (Betrag enthält MwSt. und Auslagen) aus der Gerichtskasse entschädigt.

8. Die Entscheidgebühr wird festgesetzt auf:

Fr. 2'400.00 ; die weiteren Kosten betragen:

Fr. 1'500.00 Gebühr des Vorverfahrens

Fr. 10'620.45 Entschädigung für die amtliche Verteidigung
(RA Dr. iur. X. _____)

Allfällige weitere Kosten bleiben vorbehalten.

9. [...]

10. [Mitteilungen]

11. [Rechtsmittel] "

2. Mündliche Eröffnung und schriftliche Mitteilung mit nachfolgendem Urteil.

Es wird erkannt:

1. Der Beschuldigte **A.**_____ wird freigesprochen.
2. Die zweitinstanzliche Gerichtsgebühr wird festgesetzt auf:
Fr. 3'600.– ; die weiteren Kosten betragen:
Fr. 6'000.– amtliche Verteidigung
3. Die Kosten der Untersuchung und der gerichtlichen Verfahren in beiden Instanzen, einschliesslich derjenigen der amtlichen Verteidigung, werden auf die Gerichtskasse genommen.
4. Mündliche Eröffnung und schriftliche Mitteilung im Dispositiv an
 - die amtliche Verteidigung im Doppel für sich und zuhanden des Beschuldigten (übergeben)
 - die Staatsanwaltschaft Limmattal/Albis (versendet)sowie in vollständiger Ausfertigung an
 - die amtliche Verteidigung im Doppel für sich und zuhanden des Beschuldigten
 - die Staatsanwaltschaft Limmattal/Albis
 - das Bundesamt für Polizei, Bundeskriminalpolizeiund nach unbenütztem Ablauf der Rechtsmittelfrist bzw. Erledigung allfälliger Rechtsmittel an
 - die Vorinstanz
 - die Koordinationsstelle VOSTRA/DNA zur Entfernung der Daten gemäss Art. 32 Abs. 1 StReG mittels Kopie von Urk. 49
 - die Kantonspolizei Zürich, KDM-ZD, mit separatem Schreiben (§ 54a Abs. 1 PolG).
5. Gegen diesen Entscheid kann **bundesrechtliche Beschwerde in Strafsachen** erhoben werden.

Die Beschwerde ist innert **30 Tagen**, von der Zustellung der vollständigen, begründeten Ausfertigung an gerechnet, bei der gemäss Art. 35 und 35a BGerR zuständigen strafrechtlichen Abteilung des Bundesgerichts (1000

Lausanne 14) in der in Art. 42 des Bundesgerichtsgesetzes vorgeschriebenen Weise schriftlich einzureichen.

Die Beschwerdelegitimation und die weiteren Beschwerdevoraussetzungen richten sich nach den massgeblichen Bestimmungen des Bundesgerichtsgesetzes.

Obergericht des Kantons Zürich
I. Strafkammer

Zürich, 23. Oktober 2024

Der Präsident:

Der Gerichtsschreiber:

lic. iur. M. Langmeier

MLaw S. Zuber