SO_GERICHTE STBER.2024.63 vom 16. April 2025

SO Obergericht, 2025-04-16, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/so_gerichte_STBER.2024.63

FR: SO_GERICHTE STBER.2024.63 du 16 avril 2025

IT: SO_GERICHTE STBER.2024.63 del 16 aprile 2025

Regeste

Mehrfache harte Pornografie (sexuelle Handlungen mit Tieren [Besitz] sowie tatsächliche sexuelle Handlungen mit Minderjährigen [Herstellen sowie Anbieten, Überlassen und Zugänglichmachen sowie Besitz]) (Art. 197 Abs. 4 Satz 2 StGB sowie Art. 197 Abs. 5 Satz 1 und 2 StGB); Gewaltdarstellungen (Besitz

Erwägungen

E. 1

Mit Verfügung vom 17. Mai 2023 eröffnete die Staatsanwaltschaft des Kantons Solothurn (nachfolgend: Staatsanwaltschaft) eine Untersuchung gegen A.___ (nachfolgend: Beschuldigter) wegen der Verbreitung harter Pornografie (Art. 197 Abs. 4 Satz 1 StGB) (Aktenseite [AS] 111). Ausgelöst wurde das Verfahren durch eine Meldung der Kantonspolizei Bern vom 23. Februar 2023, die mit einem Child Protection System (CPS) festgestellt habe, dass von einer dem Beschuldigten gehörenden IP-Adresse im Peer-to-Peer-Netzwerk Dateien mit kinderpornografischem Inhalt heruntergeladen und geteilt worden seien (AS 006 ff.).

E. 1.1

Der Beschuldigte obsiegt mit seiner Berufung komplett und wird von sämtlichen Vorwürfen freigesprochen. Sämtliche Kosten (erstinstanzliches Verfahren CHF 3’000.00 und Berufungsverfahren CHF 4'000.00) gehen daher zulasten des Staates Solothurn.

E. 1.2

Auch die Kosten des privaten Gutachtens durch die B.___ AG, von CHF 3'026.80 (inkl. MwSt.) gehen zu Lasten des Staates Solothurn. Es handelt sich zwar um ein Privatgutachten, jedoch ist dessen Einholung den notwendigen Verteidigungskosten zuzuordnen. 2. Entschädigung

E. 2

Am 24. Mai 2023 wurden die Wohnung des Beschuldigten, ein von ihm gemieteter externer Raum sowie eine angemietete Garage durchsucht und mehrere elektronische Geräte und Datenträger sichergestellt (AS 019 ff.).

E. 2.1

Bei diesem Verfahrensausgang ist dem Vertreter des Beschuldigten, Rechtsanwalt Marc Schmid, eine Parteientschädigung zuzusprechen. Der für das erstinstanzliche Verfahren geltend gemacht Aufwand von 23,42 Stunden erweist sich gerade noch als angemessen. Jedoch kann der geforderte Stundenansatz von CHF 390.00 nicht zugesprochen werden. Gemäss Praxis der Strafkammer des Obergerichts des Kantons Solothurn ist dieser auf

maximal CHF 280.00 festzusetzen, es sei denn, es liege ein komplexer Fall vor. Auch vorliegend ist auf diesen Ansatz abzustellen, da nur sehr zurückhaltend ein höherer Tarif zugesprochen wird. Der Fall erwies sich zwar nicht als sehr einfach, doch der Verteidiger holte sich die benötigte technische Unterstützung durch eine externe Firma, weshalb sich kein höherer Stundenansatz rechtfertigt und dieser auch nicht begründet wurde. Im Weiteren sind die Aufwände bis zum 31. Dezember 2023 mit dem alten Mehrwertsteuersatz von 7,7 % und die Aufwendungen ab 1. Januar 2024 mit 8,1 % zu vergüten. Prozentuale Büropauschalen sind gemäss Praxis der Strafkammer des Obergerichts nicht vorgesehen, da die effektiven Auslagen zu vergüten sind. Ein Betrag von CHF 270.00 erscheint aber angemessen. Damit ergibt sich eine Entschädigung von CHF 7'374.25 (Honorar für 23,42 Stunden zu CHF 280.00 pro Stunde von CHF 6’557.60, Auslagen von CHF 270.00, MwSt. zu 7,7 % auf CHF 1'610.00 von CHF 124.00, MwSt. zu 8,1 % auf CHF 5'217.60 von CHF 422.65).

E. 2.1.1

Dem Bericht der Kantonspolizei (KAPO) Bern vom 23. Februar 2023 (AS 006 ff.) kann entnommen werden, dass durch das CPS (Child Protection System) habe festgestellt werden können, dass im Zeitraum zwischen dem 29. Dezember 2021 und dem 30. Januar 2023 mehrere Dateien mit kinderpornografischem Inhalt im Peer-to-Peer-Netzwerk eDonkey heruntergeladen und geteilt worden seien. Beim Nutzer der dabei verwendeten IP-Adresse handle es sich gemäss IRC-Abklärungen um den Beschuldigten. CPS sei ein System zur Überwachung offener Peer-to-Peer Netzwerke. CPS sei von einer NGO in Florida (USA) entwickelt worden. Die gesammelten öffentlichen Daten erlaubten eine Auflistung von IP-Adressen und/oder den User-Flashwerten (auch GUID genannt) von Schweizer Nutzern, die unter Verdacht stünden, Dateien mit kinderpornografischem Inhalt zu teilen. CPS ermögliche es mit der Applikation ShareazaLE, die Dateien einer verdächtigen Person, die den Inhalt ihrer Dateien weiteren Nutzern zur Verfügung stelle, herunterzuladen. Die Applikation ShareazaLE sei eine Version von Shareaza, die speziell für die Strafverfolgungsbehörde entwickelt worden sei. Sie ermögliche die Verbindung zur Download-Quelle (dem Computer der verdächtigen Person) und veranschauliche auf diese Weise die Zuwiderhandlung. Der Fachbereich Spezialeinsätze nutze ShareazaLE, um eine Verbindung zu Peer-to-Peer-Netzwerken herzustellen und von einer Download-Quelle Dateien herunterzuladen, die von Ermittlern weltweit gemäss ihrer Gesetzgebung als «Child notable» (Dateien mit kinderpornografischem Inhalt) kategorisiert würden. Nachdem eine Fileübersicht (Excel CSV) des betroffenen GUID und/oder IP-Adresse heruntergeladen worden sei, kontrolliere der Fachbereich Spezialeinsätze, ob sich darunter mindestens eine Datei mit kinderpornografischem Inhalt gemäss Art. 197 Abs. 4 StGB befinde. Der Bericht liste alle mit dem Fall verbundenen Informationen auf: Wann sei die verdächtige Person zum ersten und letzten Mal im CPS auffällig geworden; die Anzahl der einzelnen Dateien, die von CPS festgestellt worden seien (nach Kategorien klassiert, siehe Excel CSV); die rot markierten Bereiche seien bei der KAPO Bern nach NDHS 1 klassifizierte Erzeugnisse (siehe Excel CSV processed); die verschiedenen IP-Adressen des Benutzers; habe ein «Browse» erfolgreich stattgefunden oder nicht (ein «Browse» sei eine Anfrage eines Benutzers mit dem Ziel, Inhalte zu teilen; hierbei gehe es darum, eine Liste der geteilten Dateien eines P2P-Nutzers in Erfahrung zu bringen; wenn der «Browse-Modus» eines Nutzers aktiviert sei, stelle dessen Computer unter anderem die Liste der in Echtzeit geteilten Dateien sowie des genutzten Clients, die IP-Adresse und GUID zur Verfügung; wenn besagter Modus deaktiviert sei oder der Computer des Verdächtigen andere

Prioritäten setze, gebe es keinen «Browse»; manche P2P-Clients aktivierten diese Option standardmässig); die Liste der heruntergeladenen Dateien mit dem Datum des Downloads, Hashwerten, Dateigrösse und -name sowie Information darüber, ob die Dateien teilweise heruntergeladen worden seien. Die durchgeführten Ermittlungen und Abklärungen im P2P-Netzwerk hätten ergeben, dass zum Zeitpunkt des Anbietens der kinderpornografischen Dateien, die IP-Adresse gemäss IRC-Report an A.___, geb. […], [Ort 1], [Adresse 1], vergeben gewesen sei. Diese IP-Adresse gehöre zum Provider der […] AG. Der dem Bericht beiliegenden Liste (AS 009.1 ff.) ist zu entnehmen, dass an der IP-Adresse […] diverse Dateien mit als Kinderpornografie qualifiziertem Inhalt (rot markiert, 20 Dateien [ohne Duplikate]) sowie mit Präferenzindikatoren (gelb markiert, 3 Dateien) im Netzwerk nachgewiesen werden konnten.

E. 2.1.2

Der Bericht zur forensischen Datensicherung und Auswertung vom 25. Juli 2023 (AS 043 ff.) hält fest, welche Datenträger ausgewertet wurden. Gemäss der Auswertung hätten die von der KAPO Bern gemeldeten Dateien und die drei GUIDs (Globally Unique Identifier; zur eindeutigen Identifizierung der Softwarekomponente) der eMule-Installationen auf keinem der Datenträger gefunden werden können. Auf dem Laptop Asus (1-23-049.02 und 1-23-049.03) seien zwei vom Benutzer nutzbare Partitionen (Partition 4 und 6) eingerichtet. Auf der Partition 4 seien zwei Benutzer («C.___» und «D.___») eingerichtet. Im Papierkorb der Windows-Installation auf Partition 4 sei eine Videodatei mit verbotenem kinderpornografischem Material gefunden worden. Der Original-Dateiname laute «(PHANT) - Mom latina en casa pobre mama y besa sensualmente a su hijo.mp4». Die Datei sei am 28. Dezember 2021 gespeichert bzw. vermutlich heruntergeladen worden. Durch die Löschung bzw. das Verschieben in den Papierkorb sei ein neuer Zeitstempel mit Datum 13. November 2022 generiert worden. An diesem Tag sei die Datei scheinbar gelöscht worden. Wenn eine Datei in Windows in den Papierkorb verschoben werde, erhalte sie von Windows intern automatisch einen neuen Namen (hier «$R172B6Y.mp4»). Zusätzlich seien auf beiden Partitionen (4 und 6) Fragmente von Ausdrücken der Kinderpornografie gefunden worden, wie «pthc», «preteen», «pedomom», «incest», «12yo» oder «14yo». Die Dateiendungen dieser Dateifragmente (.mpg, .wmv, .avi, .mp4) liessen auf Videodateien schliessen. Die Dateien selbst seien jedoch nicht mehr vorhanden bzw. deren Inhalt habe nicht eingesehen werden können. Auch könne angenommen werden, dass eine eMule-Installation auf der Partition 4 unter dem Benutzer «C.___» in der Vergangenheit vorhanden gewesen sei. Es seien Fragmente von Pfadangaben gefunden worden; C:\Users\C.___\Downloads\eMule\Incoming und D:\eMule0.50a. Der Ordner «Incoming» bezeichne dabei das Verzeichnis, wo fertig heruntergeladene Dateien hin geschoben würden. Dieser Ordner bzw. dessen Inhalt werde zusätzlich geteilt und zum Hochladen bzw. Weiterverbreiten verwendet. Auf dem Computer Eigenbau (I-23-049.20) auf einer eingebauten, aber nicht angeschlossenen Festplatte (I-23-049.20B) sei am 4. Oktober 2015 eine Sicherung eines iPhone 5 erstellt bzw. abgespeichert worden. Das iPhone trage den Namen «E.___ iPhone» und habe die Nummer +41 […]. Im Ordner «iPhone Foto» auf dem Desktop des Benutzerverzeichnisses (C:\Users\H.___\Desktop\iPhone Foto) seien je zwei Videos mit tierpornografischem Inhalt und verbotener Gewalt am 9. Dezember 2013 abgespeichert worden. Dieselben Videos seien auch im Papierkorb/Recycle Bin des Benutzers mit der SID «[…]» gefunden worden. Die Abkürzung SID stehe für Security Identifier, eine einzigartige Zeichenfolge, die Windows automatisch jedem Computer, jedem Benutzer und jeder Gruppe zuweise, um das

jeweilige Objekt eindeutig zu identifizieren. Die SID sei unveränderlich und bleibe auch gleich, wenn das Objekt selbst (also zum Beispiel der Benutzer) umbenannt werde. Die oben genannte SID sei dem Benutzer «H.___» (der einzige eingerichtete Windows-Benutzer) zugeordnet. Der Name «E.___» sei abseits vom oben genannten iPhone auch an weiteren Orten aufgetaucht. So sei die E-Mailadresse «E.___@hotmail.com» als Apple Account, und der Skype-Benutzername «E.___» auf dem System hinterlegt. Die E-Mailadresse «[...]@hotmail.com» sei überdies in der Windows Mail-Applikation konfiguriert. Es seien an diese Adresse empfangene Nachrichten mit dem Betreffs-Inhalt «E.___» gefunden worden. Daraus lasse sich ableiten, dass besagte E-Mailadresse «E.___» gehöre. Auch sei im Google Chrome-Browser die vermeintliche Wohnadresse von E.___ ([Adresse 1], [Ort 2]) in der Auto-Vervollständigung hinterlegt. Es sei davon auszugehen, dass E.___ früher als Haupt-Benutzerin mit dieser Windows-Installation gearbeitet habe. Weitere aktive Windows-Benutzer seien nicht eingerichtet. Ansonsten seien keine Daten vom Beschuldigten oder anderweitig verdächtiges Material gefunden worden. Die beiden Festplatten I-23-049.20C und I-23-049.20D seien als sogenannte «Dynamische Datenträger» konfiguriert und zu einer einzigen Partition bzw. als ein einziges Laufwerk zusammengefasst worden. In Windows würden beide Festplatten also nicht separat, sondern als eine Einheit betrachtet und angezeigt. Dieses Laufwerk werde aktuell als Datenablage mit unverdächtigen Dateien genutzt. Es hätte jedoch eine grosse Anzahl verdächtiger Datei- und Ordnerfragmente gefunden werden können, die darauf hindeuten würden, dass einer dieser beiden Datenträger früher von Windows-Installationen genutzt worden sei. Diese Fragmente seien in Speicherbereichen vorhanden, die im bestehenden Dateisystem als frei geführt seien. Das heisse, die Ordner/Dateien seien nicht mehr vorhanden und der Inhalt könne nicht eingesehen werden. In einer der früheren Windows-Installationen seien die beiden Benutzerprofile «F.___» und «G.___» eingerichtet gewesen. Im Downloads Ordner des Benutzers «G.___» seien Spuren einer Installations-Datei für eMule (C:\Users\G.___\Downloads\emule048a.exe) und ein zugehöriges Help-File (C:\Users\G.___\Downloads\emule. 1031.chm) gefunden worden. Im Windows-Startmenü seien die Dateien «emule.Ink» und «emule.com.url» ersichtlich. Die *.Ink-Datei stelle eine Datei-Verknüpfung dar und der Speicherort im Windows-Startmenü (C:\ProgramData\Microsoft\Windows\Start Menu\Programs) weise darauf hin, dass eMule installiert gewesen sei. Zusätzlich seien Fragmente von Ausdrücken der Kinderpornografie gefunden worden, wie «pthc», «preteen», «lolita», «underage» oder «pedo». Es hätten auch Anzeichen von Cookies entdeckt werden können. Cookies seien kleine Textdateien, die über eine besuchte Webseite auf dem lokalen Computer erstellt werden könnten. Die besagten Cookies hätten die Namen «G.___@tgp.my-preteens.com», «G.___@elite-preteens.com» und «G.___@ preteen-portal.com» getragen. Es könne davon ausgegangen werden, dass mittels des Windows-Benutzers «G.___» auf diese Websites zugegriffen worden sei. Zum Namen «G.___» seien keine Informationen zur Person gefunden worden, sondern nur die oben aufgeführten Fragmente. Weiter sei eine Yahoo-Suchmaschinenanfrage mit den Begriffen «preteen+lolita+pics» durchgeführt und eine Torrent-Web-
site «http://www.nowtorrents.com/torrents/pedo-pics-real-pthc-lolita-underage-pr
eteen-babyshvid.htmr» aufgerufen worden. Torrents würden zum Filesharing genutzt, also zum Austausch grosser Datenmengen über das Web. Ob hier die eigentliche Datei heruntergeladen worden sei, sei nicht ersichtlich.

Im Ordner «C:\Backup\WORK\Brennen(Old)\Util» der externen Festplatte I-23-049.4A seien zwei ehemals existierende bzw. gelöschte Videos mit tierpornografischem Inhalt gefunden worden (Wäää.mpg und Nicht Möglich aber Wahr.mpg). Diese beiden Dateien seien nicht durch anderen Inhalt überschrieben worden und hätten somit vollständig wiederhergestellt bzw. abgespielt werden können. Die beiden Videodateien stammten aus dem August 2005. Weiter seien Verweise auf ehemals existierende Videodateien mit Namen wie «Animal Sex» und «Beastiality» gefunden worden. Hier seien die eigentlichen Dateien jedoch durch anderen Inhalt auf der Festplatte bereits überschrieben worden und seien nicht mehr abspielbar.

E. 2.1.3

Der Nachtragsrapport vom 20. Dezember 2023 (AS 110.1 ff.) hält zu den vom Verteidiger gestellten Fragen vom 6. November 2023 (AS 129.9 ff.) Folgendes fest: Vom Anschluss des Beschuldigten seien via P2P-Netzwerk kinderpornografische Darstellungen verbreitet worden. Es stelle sich die Frage, warum der Beschuldigte wahllos Inhalte fremder USB-Sticks auf seine Festplatte kopieren sollte, ohne diese zeitnah zu prüfen. Die technische Aussage, dass grössere Videodateien nicht direkt von qualitativ minderwertigen, sprich langsamen, USB-Sticks abgespielt werden könnten, könnten sie nicht bestätigen. Das besagte Video weise nur eine Dateigrösse von

E. 2.1.4

Der Nachtragsrapport vom 4. November 2024 (ASB 28 ff.) hält zu den vom Verteidiger mit Eingabe vom 22. August 2024 gestellten Fragen fest, der im Schreiben des Verteidigers genannte PC mit dem User «CCB» (PC Eigenbau) habe eine aktive Windows-Installation auf der Festplatte 20A. Der einzige User sei «CCB». Die Festplatte 20B sei nicht eingesteckt gewesen und auf dem Festplattenverbund 20C/20D kein Windows installiert, sondern nur eine Datenablage vorhanden. Es reiche nicht, dass der Computer eingeschaltet und mit dem Internet verbunden sei. U.a. müsse der Fernzugriff in den Einstellungen explizit erlaubt werden. Auf dem PC sei der RDP Zugriff gemäss Registry (Windows-Datenbank für Einstellungen) deaktiviert. Infolgedessen sei eine Fern-Anmeldung am einzigen Benutzerkonto «CCB» nicht möglich. Die RDP Verbindung sei auch beim Windows auf der ausgesteckten Festplatte 20B deaktiviert. Die letzten Änderungen stammten dort überdies vom 22. September 2022, also vor Ende des Tatzeitraums. Auf Festplatte 20C seien zwei gelöschte Windows-Ordner vorhanden, die aber schon in den Jahren 2007 und 2012 gelöscht worden seien. Eine Anmeldung – ob lokal oder aus der Ferne – wäre nur beim aktuell gestarteten Windows möglich, was hier nicht möglich sei, da diese Windows-Installationen gelöscht seien. Stattdessen sei beim PC das installierte Fernwartungsprogramm TeamViewer gefunden worden. Auf der Festplatte 20A seien diverse Verbindungen von TeamViewer festgestellt worden. Die Verbindungslog seien in «TeamViewer 1» und «TeamViewer 2» zusammengestellt worden. Bei den ersten beiden Einträgen in «TeamViewer 2» sei zudem ersichtlich, dass der Computername des Gegenübers DESKT0P-[…] laute. Dabei handelt es sich offensichtlich um einen automatisch bei der Installation von Windows vergebenen Namen, nicht einen selbst gewählten. Bei allen anderen Einträgen laute der Computername […]. […] sei aber (auch) der Computername der Windows-Installation auf Festplatte 20A. Zudem laute der Computername der Windows-Installation auf Festplatte 06B (PC Eigenbau «[…]») DESKTOP-[…]. Zusätzlich sei auf Festplatte 02A (Laptop Asus) ein Verbindungslog der Spieleplattform Steam gefunden. Durch eine solche Verbindung könnten auf dem einen PC

installierte Spiele auf einem anderen PC im lokalen Netzwerk gespielt werden. Im Log sei ersichtlich, dass am 31. Januar 2021 ebenfalls zum PC mit dem Computernamen DESKT0P-[…] eine Verbindung bestanden habe. Dahinter sei sogar dessen IP-Adresse sichtbar: […]. Dabei handle es sich um eine sog. Private IP-Adresse. Private IP-Adressen könnten ausschliesslich im lokalen Netzwerk verwendet werden. Das beweise, dass sich der Computer DESKT0P-[…] im gleichen lokalen Netzwerk befunden habe wie der Laptop Asus. Zusammengefasst lasse sich sagen, dass die TeamViewer-Verbindungen nicht von fremden Personen benutzt worden sein dürften. Sowieso hätte der lokale User TeamViewer installieren müssen. Ohne zusätzliche Tools sei das aus der Ferne nicht möglich. Notabene sei TeamViewer kein Tool, welches vorzugsweise von Hackern verwendet werde. Im aktuellen Fall erscheine es doch eher naheliegend, dass eben gerade der Beschuldigte den PC in der Garage von zuhause aus habe steuern wollen. Es sei keine weitere Software für Remote-Verbindungen gefunden worden. Am 31. Oktober 2024 sei ein kompletter Viren-Scan des PC-lmages 20A durchgeführt worden. Dabei seien keinerlei Viren, Hacker-Tools (Backdoors) etc. gefunden worden. Da der Scan offline durchgeführt worden sei, habe eine im Windows installierte Malware nicht die Möglichkeit, sich vor dem Virenscanner zu verstecken. Überdies sei der PC vor rund 1 1/2 Jahren sichergestellt worden, sodass durchaus davon auszugehen sei, dass eine damals noch nicht bekannte Malware am heutigen Tag erkannt werden müsste.

E. 2.2

Für das Berufungsverfahren macht der Verteidiger einen Aufwand von 30.67 Stunden geltend. Dies erweist sich als überhöht. Die Verhandlung dauerte lediglich rund 1,75 Stunden und es wurde auf eine mündliche Eröffnung verzichtet. Daher sind zwei Stunden zu streichen. Am 26. Februar 2025 macht Rechtsanwalt Schmid 15 Minuten geltend für das Zurücksenden von USB-Sticks, dies ist als Kanzleiaufwand zu werten und zu streichen. Dasselbe gilt für die 15 Minuten für das Rücksenden von Akten am 13. März 2025. Im Weiteren wurden insgesamt 16,25 Stunden für die Ausarbeitung des Plädoyers geltend gemacht. Im Anbetracht des Umfangs des Plädoyers und im Vergleich mit dem Parteivortrag vor der Vorinstanz ist dies deutlich überhöht, weshalb sich eine Kürzung um vier Stunden rechtfertigt. Die vorherigen Ausführungen zur Büropauschale gelten auch hier, weshalb ein ermessensweiser Betrag von CHF 280.00 für die Auslagen zu vergüten ist. Ebenfalls ist der Stundenansatz – wie zuvor erwähnt – auf CHF 280.00 zu kürzen. Damit resultiert eine Entschädigung von CHF 7'618.50 (Honorar für 24,17 Stunden zu CHF 280.00 pro Stunde von CHF 6'767.60, Auslagen von CHF 280.00, MwSt. zu 8,1 % auf CHF 7'047.60 von CHF 570.90). Demnach wird in Anwendung von Art. 197 Abs. 6 i.V.m Art. 69 StGB; Art. 398 ff., Art. 428 Abs. 1 und 3, Art. 429 StPO erkannt : 1. A.___ wird von folgenden Vorhalten freigesprochen: a) mehrfache harte Pornografie (tatsächliche sexuelle Handlungen mit Minderjährigen [Herstellen sowie Anbieten, Überlassen und Zugänglichmachen]), begangen in der Zeit vom 29. Dezember 2021 bis am 30. Januar 2023, b) mehrfache harte Pornografie (sexuelle Handlungen mit Tieren [Besitz]; tatsächliche sexuelle Handlungen mit Minderjährigen [Besitz]), begangen in der Zeit vom 28. Dezember 2021 bis am bis am 24. Mai 2023, c) Gewaltdarstellungen (Besitz), begangen in der Zeit vom 9. Dezember 2013 bis am 24. Mai 2023. 2. Folgende im Verfahren gegen A.___ beschlagnahmten Gegenstände (alle aufbewahrt bei der Polizei Kanton Solothurn, FB Asservate) werden eingezogen und sind nach Rechtskraft des Urteils durch die Polizei zu vernichten: a) 1 Festplatte Hitachi, HDD, 5K750-500 (Objekt-Nr. I-23-049.20B); b) 1 Festplatte Seagate, Barracuda, ST3320820A (Objekt-Nr. I-23-049.04A); c) 1 Festplatte

Samsung, SSD, 840 EVO (Objekt-Nr. I-23-049.02A). 3. Die Polizei Kanton Solothurn wird angewiesen, die forensisch gesicherten Daten der Mobile-Forensik, Fallnummer M-23-163-01, sowie der IT-Forensik, IT-Fallnummer I-23-049, nach Rechtskraft dieses Urteils zu löschen. 4. Für das erstinstanzliche Verfahren wird dem privaten Vertreter von A.___, Rechtsanwalt Marc Schmid, zulasten des Staates Solothurn eine Entschädigung von CHF 7'374.25 (inkl. Auslagen und MwSt.) zugesprochen (auszahlbar durch die Zentrale Gerichtskasse Solothurn nach Rechtskraft des Urteils). 5. Für das Berufungsverfahren wird dem privaten Vertreter von A.___, Rechtsanwalt Marc Schmid, zulasten des Staates Solothurn eine Entschädigung von CHF 7'618.50 (inkl. Auslagen und MwSt.) zugesprochen (auszahlbar durch die Zentrale Gerichtskasse Solothurn nach Rechtskraft des Urteils). 6. Die Kosten des privaten Gutachtens durch die B.___ AG, von CHF 3'026.80 (inkl. MwSt.) gehen zu Lasten des Staates Solothurn. 7. Sämtliche Kosten (erstinstanzliches Verfahren CHF 3’000.00 und Berufungsverfahren CHF 4'000.00) gehen zulasten des Staates Solothurn. Rechtsmittel : Gegen diesen Entscheid kann innert 30 Tagen seit Erhalt des begründeten Urteils beim Bundesgericht Beschwerde in Strafsachen eingereicht werden (Adresse: 1000 Lausanne 14). Die Frist beginnt am Tag nach dem Empfang des begründeten Urteils zu laufen und wird durch rechtzeitige Aufgabe bei der Post gewahrt. Die Frist ist nicht erstreckbar. Die Beschwerdeschrift hat die Begehren, deren Begründung mit Angabe der Beweismittel und die Unterschrift des Beschwerdeführers oder seines Vertreters zu enthalten. Für die weiteren Voraussetzungen sind die Art. 78 ff. und 90 ff. des Bundesgerichtsgesetzes massgeblich. Im Namen der Strafkammer des Obergerichts Der Präsident Die Gerichtsschreiberin
Werner Schmid

E. 2.2.1

Anlässlich der Einvernahme vom 2. Juni 2023 (AS 082 ff.) gab der Beschuldigte zu Protokoll, er sei über die Vorwürfe gegen ihn schockiert. Er habe mittels Peer-to-Peer(P2P)-Netzwerk eine Windows 95 Kopie heruntergeladen. Der Name sei etwas wie eDonkey. Das sei schon länger her. Er habe das Netzwerk auf dem Computer in der Halle genutzt. Die Nutzung sei nur durch ihn vorgesehen gewesen, in der Theorie habe ihn aber jeder nutzen können, der in die Halle gekommen sei. Der Computer sei passwortgeschützt. Er wisse nicht, ob er ihn immer gesperrt habe. Das Passwort habe niemand sonst gekannt. Das P2P-Netzwerk habe er nicht auf anderen Geräten verwendet. Der Beschuldigte verneinte Videos und/oder Bilder mit kinderpornografischem Inhalt aus dem P2P-Netzwerk heruntergeladen, angeboten oder gespeichert zu haben. An der [Strasse] nutze er WLan und Festnetz. Der Anschluss sei passwortgeschützt. Er selbst habe das Passwort nie herausgegeben, aber sein Kollege. Es sei dort bekannt gewesen, aber er könne es nicht bestätigen. Er habe nur alte Windows-Versionen über das Netzwerk heruntergeladen, sonst nichts. Er verneinte, die ihm als Standbilder gezeigten Videos zu kennen, besessen, heruntergeladen oder verbreitet zu haben. Er habe nie nach verbotener Pornografie gesucht. Er habe auf dem Computer an der [Strasse] legale Pornografie konsumiert, aber nicht via P2P-Netzwerk. Er konsumiere keine Kinderpornografie. Normalerweise sperre er den Computer schon. Aber er könne es auch einmal vergessen haben. Diverse Personen hätten einen Schlüssel. Niemand ausser ihm kenne das Passwort des Computers. Es könne nicht sein, dass auf den sichergestellten Geräten verbotene Pornografie gespeichert sei.

E. 2.2.2

An der Einvernahme vom 23. August 2023 (AS 098 ff.) gab der Beschuldigte an, er habe so in den Jahren 1999 bis 2000 ein eMule-Profil besessen, um alte Software herunterzuladen. Er habe vielleicht auch einmal einen Kinofilm heruntergeladen. Er habe auch schon unbestellte Dateien erhalten, aber alles harmlos. Der Laptop Asus gehöre ihm. Er habe ihn vom [Zentrum], wo er gearbeitet habe, übernehmen können. Beide Laptops seien ursprünglich von dort, sie wären sonst entsorgt, verschenkt oder verkauft worden. Den Asus-Laptop besitze er seit 2021. Damals habe er gekündigt und einige Computer mitnehmen dürfen. Er benutze den Laptop zum Spielen und um Filme zu schauen. Vor Oktober 2021, als er den Laptop nach Hause genommen habe, habe er den Kunden des [Zentrums] zur Verfügung gestanden. An den drei genannten Adressen habe niemand Zugriff gehabt. Er habe an diesem Laptop eine neue Festplatte eingebaut. Das Profil «C.___» benutze er, «D.___» habe er für seine Partnerin eingerichtet. Mit diesem Laptop habe er nie eMule benutzt. Er habe das Windows zurückgesetzt, als er den Laptop nach Hause genommen habe. Davon, dass aufgrund von gefundenen Fragmenten kinderpornografische Filme gespeichert gewesen sein müssen, wisse er nichts. Den darauf gefundenen Film mit kinderpornografischem Inhalt kenne er nicht, er habe ihn nicht heruntergeladen oder anderen zur Verfügung gestellt. Zu den auf einer seiner externen Festplatten gefundenen Filmen mit tierpornografischem Inhalt sagte er lediglich «keine Ahnung» und bestritt ebenfalls jede Handlung damit. Den selbst zusammengebauten Computer besitze er seit etwa 2010. Er habe manchmal etwas ein- und ausgebaut. Er nutze ihn als Minecraft-Server. Der sei ständig im Internet. Wenn er in der Halle gewesen sei, habe er damit Bauteile bestellt oder im Internet recherchiert. An der [Strasse] hätten viele Leute Zugriff auf den PC. Dieser sei permanent gelaufen und am Internet angeschlossen gewesen. Er habe das so eingerichtet, dass er von extern auf diesem Computer Minecraft spielen könne. Er habe aus Spass vier Festplatten eingebaut. Diese seien nicht neu gekauft, sondern sie wären weggegeben oder -geworfen worden. E.___ habe ihm einen kaputten Laptop gegeben. Es sei möglich, dass er von diesem Laptop eine Windows-Version auf die Festplatte kopiert habe. Von den Videos in einem entsprechenden Ordner wisse er nichts. «G.___» sei ein Kollege, der früher Material in seiner Halle gelagert habe. Er (der Beschuldigte) habe dieses brauchen können. Er wisse nicht, ob er Festplatten von ihm verbaut habe. Zu den Fragmenten von Ausdrücken von Kinderpornografie wisse er nichts. Er sei nicht pädophil. Er stehe nicht auf Filme mit Tieren. Gewaltdarstellungen interessierten ihn nicht.

E. 2.2.3

Vor der Vorinstanz sagte der Beschuldigte betreffend Vorhalt 1 aus, er habe das nicht gemacht. Er habe das P2P-Netzwerk vor etwa 20 Jahren benutzt für den Download von Windows-Versionen. Seither habe er es nicht mehr benutzt. Es sei für ihn schwierig nachzuvollziehen, wer diese Downloads getätigt haben könnte. Er sei nicht oft in der Halle gewesen. Er habe keine Zeit gehabt. Er habe seinen Mitmieter rauswerfen müssen. Er habe auch Mieter drin gehabt. Er sei daran gewesen, die Halle abzustossen. Ihm sei nicht aufgefallen, dass jemand etwas manipuliert habe. Die Leute der [Firma] hätten Zutritt gehabt, wie auch die Untermieter. Von einem Nachbarn wisse er, dass er das WIFI-Passwort gewusst habe. Er wisse nicht, wo das überall herumgegangen sei und wem sein Mitmieter das Passwort gegeben habe. Alle seine Computer seien passwortgeschützt, ausser er habe vergessen den Computer zu sperren. Zum eMule-Profil sagte er aus, das sei damals wie ein Client gewesen. Man habe sich nur verbinden müssen. Er wisse nicht, ob sich das geändert habe. Als er das Windows heruntergeladen habe, hätten andere die Daten

auch laden können. Die eingebaute Festplatte (auf der zwei tierpornografische Videos gefunden worden seien) habe er zur Sicherung des Computers von E.___ verwendet. Sie habe ihn gebeten, die Daten rüberzuladen. Sie habe sie aber nie abgeholt und er habe es dann vergessen. Zum kinderpornografischen Video auf dem Asus Laptop gab er an, er habe einen Laptop gebraucht, um diverse USB-Sticks auszuprobieren. Er habe von den Kongressen Präsentationen gesammelt. Die Sticks seien liegengeblieben oder sonst gefunden worden. Auch von Mitmietern habe er USB-Sticks erhalten und G.___ habe ihm alles hinterlassen. Den genauen Zeitpunkt der Mitnahme des Laptops wisse er nicht mehr, er habe per 1. Dezember 2021 gekündigt und angefangen, Sachen zu sammeln und angefragt, was er mitnehmen könne. Er habe das System zurückgesetzt. Spätestens ab 1. Dezember 2021 sei der Laptop nicht mehr im [Zentrum] genutzt worden. Er vermute, das Video sei beim Überprüfen der Sticks auf den Laptop gelangt. Das Video sei ihm nicht aufgefallen. Ein Jahr später habe er alles gelöscht. Die Gewaltvideos stammten vom selben Datenträger von E.___. Diese Art von Video habe er nicht gesehen. Er habe keine Erklärung für die Feststellung des CPS. Er habe den Verdacht, es komme alles aus der Ecke von «G.___». Dieser habe auch im [Zentrum] gearbeitet. Er habe nie verbotene Pornografie gesucht, heruntergeladen, konsumiert oder weiterverbreitet.

E. 2.2.4

Vor Obergericht (ASB 127 ff.) sagte der Beschuldigte aus, G.___ sei ein guter Freund gewesen, mit dem er zusammengearbeitet habe. Er sei auch sein Mitmieter der Halle gewesen. G.___ habe seine Sachen in seiner Halle lagern dürfen. Er denke, dort sei der Hund begraben. Auch aufgrund der Ergebnisse der Forensik sei sein Fokus stark auf G.___ geschwenkt. Er denke, dort sei etwas passiert. G.___ sei Techniker, er habe das Wissen und könne mit Computern umgehen. G.___ sei ein Stammtechniker im [Zentrum] und als Freelancer immer wieder dort angestellt gewesen. Er habe auf alles Zugriff gehabt. Die Laptops würden von verschiedenen Personen bedient und auf der administrativen Ebene hätten alle das gleiche Passwort gehabt. Das sei G.___ auch bewusst gewesen. Das eingereichte Foto zeige G.___ mit ihm und einem weiteren Freund am [Tagung]. Die dort tätigen Personen hätten grosses Vertrauen genossen und sich frei bewegen können. Die B.___ AG habe auf einem Laptop, den er von ihm und vom [Zentrum] habe, solche Begriffe gefunden. Er habe dann die Ferienfotos von G.___ darauf entdeckt. Also müsse dieser das Ding in den Fingern gehabt haben. Die Begriffe hätten auch alle einen Datumsstempel aus den Jahren 2013 und 2014, der letzte 2022. 2012 oder 2013 habe G.___ bei ihnen angefangen. Er habe ja auch Zugriff auf die Halle gehabt, er habe einen Schlüssel gehabt. Es wäre für ihn ohne weiteres möglich gewesen, dort so etwas auszuführen. Er wolle ihm nicht die Schuld geben, er wisse es ja nicht, aber er tendiere in diese Richtung. Sicher mit dem Handy habe G.___ den Internetzugang genutzt. Auch auf seinen Computer habe jeder, der es gekannt habe, Zugang gehabt. Er habe den Computer aus dem Büro mitgenommen und daran herumgebastelt. Das Windows habe er belassen. Da sei auch der Micro Torrent drauf gewesen. Das Internetpasswort sei nicht restriktiv gehandhabt worden. Oben in der Halle habe es einen CBD-Anbauer gehabt, der habe es ihm auch abgeluchst. Er habe keinen Kontakt mehr zu G.___. Bis Ende 2022 habe dieser sich noch ab und zu gemeldet, wenn er in der Schweiz gewesen sei. Seit dem Vorfall wolle er nichts mehr mit ihm zu tun haben. Er habe ihm noch gesagt, er müsse sein Zeug aus der Halle holen, das sei im Jahr 2023 gewesen. Der Laptop, auf dem das Video mit sexuellen Handlungen mit Minderjährigen gefunden worden sei, habe er aus dem Zentrum. Es sei einer, der aussortiert worden sei. Zuerst sei er in der Halle gewesen. Damit habe er die Sticks geprüft, da ein

Virus oder so darauf nicht tragisch gewesen wäre, es sei nicht sein Hauptcomputer, mit dem er zuhause arbeite. Er habe viele Sticks auch von G.___ gehabt. Er habe kein Interesse mehr gehabt, die Sticks durchzusehen und alles gelöscht. Normalerweise lösche er komplett, nicht über den Papierkorb. Auch das Spanisch sei für ihn ein Hinweis, da G.___ nicht nur Portugiesisch gesprochen habe. Die Dateien auf den Sticks seien zahlreich gewesen. Darum habe er es gesammelt und gedacht, er sehe es durch, wenn er Zeit habe. Auf dem PC sei es einfacher das durchzuschauen. Sicherheitsüberlegungen habe er sich nicht gemacht, dieser Laptop sei ihm nicht wichtig gewesen. Betreffend die verbotenen Videos, die man auf der Festplatte mit dem Backup von Frau E.___ gefunden habe: er kenne Frau E.___. Er habe ihren Laptop reparieren wollen. Sie habe die auf die Festplatte geladenen Daten abholen wollen. Er habe mit der Festplatte dann etwas ausprobieren wollen, er habe ja nicht gewusst was drauf sei. Er habe sie dann eingebaut gelassen, damit er sie nicht aus Versehen wegwerfe. Er habe ihre privaten Fotos nicht durchsehen wollen. Er habe in der Halle auch Untermieter gehabt. G.___ habe den Schlüssel noch gehabt, auch als er nicht mehr in der Schweiz gewesen sei. Ein Onkel habe dann auch seine Sachen geholt. Betreffend die Verwendung von eMule gab er an, er habe früher eDonkey genutzt. eMule sei kein Netzwerk, sondern ein client. Im Tatzeitraum habe er ein P2P-Netzwerk benutzt, aber Micro Torrent und nicht eMule. 3. Beweiswürdigung

E. 2.3

Der Fundort der Dateien im Ordner «iPhone Foto» und ein dazugehöriges iPhone-Backup von E.___ deuten darauf hin, dass die Videos sich in deren Besitz auf ihrem iPhone befanden und – wie der Beschuldigte schlüssig erklärte – durch ein altes Gerät von ihr zum Beschuldigten gelangt sind. Nichtsdestotrotz befanden sich die beiden Dateien auf einem Gerät im Besitz des Beschuldigten. Der Sachverhalt gemäss Anklage ist damit grundsätzlich erstellt. 3. Rechtliche Würdigung

E. 3

Am 2. Juni 2023 wurde der Beschuldigte polizeilich einvernommen (AS 082 ff.). Am 23. August 2023 folgte eine zweite Einvernahme (AS 098 ff.).

E. 3.1

Per 1. Juli 2023 trat eine revidierte Fassung von Art. 135 StGB in Kraft. Es stellt sich deshalb die Frage des anwendbaren Rechts. Nach Art. 135 Abs. 1 bis aStGB wurde der Besitz von Gewaltdarstellungen mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Nach neuem Recht wird gemäss Art. 135 Abs. 2 StGB der Besitz ebenfalls mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Die neue Strafnorm ist folglich nicht milder als die alte. Entsprechend ist gemäss dem Grundsatz von Art. 2 Abs. 2 StGB (lex mitior) Art. 135 Abs. 1 bis aStGB in der früher gültigen Fassung anzuwenden.

E. 3.1.1

Wer pornografische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen, die sexuelle Handlungen mit Tieren oder mit Gewalttätigkeiten unter Erwachsenen oder nicht tatsächliche sexuelle Handlungen mit Minderjährigen zum Inhalt haben, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt, zugänglich macht, erwirbt, sich über elektronische Mittel oder sonst sie beschafft oder besitzt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft. Haben die Gegenstände oder Vorführungen tatsächliche sexuelle Handlungen mit Minderjährigen zum Inhalt, so ist die Strafe Freiheitsstrafe bis zu

fünf Jahren oder Geldstrafe (Art. 197 Abs. 4 StGB). Wer pornografische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen, die sexuelle Handlungen mit Tieren oder nicht tatsächliche 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, wird mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft. Haben die Gegenstände oder Vorführungen tatsächliche sexuelle Handlungen mit Minderjährigen zum Inhalt, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe (Art. 197 Abs. 5).

E. 3.1.2

Nach der bundesgerichtlichen Rechtsprechung setzt der allgemeine Begriff der Pornografie zum einen voraus, dass die Darstellungen oder Darbietungen objektiv betrachtet darauf angelegt sind, den Konsumenten sexuell aufzureizen. Zum andern ist erforderlich, dass die Sexualität so stark aus ihren menschlichen und emotionalen Bezügen gelöst wird, dass die jeweilige Person als ein blosses Sexualobjekt erscheint, über das nach Belieben verfügt werden kann. Das sexuelle Verhalten wird dadurch vergröbert und aufdringlich in den Vordergrund gerückt (Urteil des Bundesgerichts 6B_148/2019 vom 11. Dezember 2019 E. 1.4.2 mit Hinweis auf BGE 144 II 233 E. 8.2.3 S. 242 und BGE 131 IV 64 E. 10.1.1 S. 66).

E. 3.1.3

Abs. 4 und 5 verbieten die sogenannte harte Pornografie, die gemäss dem vorgenannten Gesetzeswortlaut gegeben ist, wenn zum pornografischen Charakter mindestens eines von vier abschliessend aufgeführten Merkmale hinzukommt, nämlich die Beteiligung von Tieren, der Einsatz von Gewalttätigkeiten sowie der nicht tatsächliche Einbezug von Minderjährigen und der tatsächliche Einbezug von Minderjährigen (Stefan Trechsel/Carlo Bertossa in: Stefan Trechsel/Mark Pieth [Hrsg.], Praxiskommentar Schweizerisches Strafgesetzbuch, 4. Auflage, St. Gallen/Zürich 2021, Art. 197 StGB N 10).

E. 3.1.4

Erfasst werden gemäss Art. 197 Abs. 4 StGB zunächst einmal umfassend alle Verhaltensweisen auf der Anbieterseite («herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt [und] zugänglich macht»). Über die Tathandlungsvarianten «erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt» werden zusätzlich auch Verhaltensweisen erfasst, die theoretisch sowohl von einem reinen Konsumenten als auch vom Anbieter verwirklicht werden können. Bei einem reinen Konsumenten, der also nur seinen eigenen Konsum vorbereitet, kommt Abs. 4 allerdings nicht zur Anwendung, weil hier der privilegierende Tatbestand von Abs. 5 (mit einer herabgesetzten Strafobergrenze) vorgeht (Wolfang Wohlers in: AJP 4/2020: Strafbarkeit des Umgangs mit Kinderpornografie, S. 393; ebenso Bernhard Isenring / Martin A. Kessler in: Marcel Alexander Niggli / Hans Wiprächtiger [Hrsg.], Basler Kommentar, Strafrecht II, 4. Auflage, Basel 2019, Art. 197 StGB N 49; vgl. in Bezug auf diese Abgrenzung auch die kantonale Rechtsprechung: STBER.2020.98 und STBER.2020.66).

E. 3.1.5

In subjektiver Hinsicht wird Vorsatz verlangt, wobei Eventualvorsatz ausreichend ist und im Hinblick auf die Wissenskomponente des Vorsatzes keine exakten juristischen Kenntnisse erforderlich sind. Es reicht aus, dass der Beschuldigte den (kinder-)pornografischen Gehalt der Darstellung laienhaft (sog. Parallelwertung in der

Laiensphäre) nachvollzogen hat (Wolfgang Wohlers in: AJP 4/2020, S. 393 mit Hinweis auf das Urteil des Bundesgerichts 6B_229/2019 vom 27. Mai 2019 E. 3.2).

E. 3.1.6

Bei der Tatbestandsvariante des Besitzes wird auf der subjektiven Seite primär der Wille vorausgesetzt, den pornografischen Inhalt in der eigenen Verfügungsmacht zu behalten und darauf pro futuro wieder zuzugreifen (Isenring / Kessler , a.a.O., Art. 197 N 52l). Gemäss BGE 137 IV 208 manifestiert seinen Besitzeswillen, wer um die automatische Speicherung der strafbaren pornografischen Daten weiss und diese im Nachgang an eine Internetsitzung nicht löscht, selbst wenn er nicht mehr darauf zurückgreift. Allerdings ist bei der Bejahung des subjektiven Tatbestandes des Besitzes von pornografischen Dateien im Cache-Speicher Zurückhaltung geboten. Ein ungeübter Computer-/Internetbenutzer, der von der Existenz des Cache-Speichers und den darin enthaltenen Daten nichts weiss, fällt als Täter nach Art. 197 Ziff. 4 StGB ausser Betracht. Ob er von den Daten Kenntnis hat, ist nach den konkreten Umständen im Einzelfall zu entscheiden. Hinweise darauf können sich beispielsweise aus der Änderung der automatischen Internet-Einstellungen, dem Vorhandensein von Programmen wie Cache-Viewer bzw. Cache-Reader, der manuellen Löschung des Cache-Speichers, dem Nachweis eines Offline-Zugriffs oder aus seinen allgemeinen Fachkenntnissen im Zusammenhang mit Computern und Internet ergeben (BGE 137 IV 208 E. 4.2.2).

E. 3.2

Gemäss Art. 135 aStGB wird, wer Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände oder Vorführungen, die, ohne schutzwürdigen kulturellen oder wissenschaftlichen Wert zu haben, grausame Gewalttätigkeiten gegen Menschen oder Tiere eindringlich darstellen und dabei die elementare Würde des Menschen in schwerer Weise verletzen, herstellt, einführt, lagert, in Verkehr bringt, anpreist, ausstellt, anbietet, zeigt, überlässt oder zugänglich macht, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft (Abs. 1). Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer Gegenstände oder Vorführungen nach Absatz 1, soweit sie Gewalttätigkeiten gegen Menschen oder Tiere darstellen, erwirbt, sich über elektronische Mittel oder sonst wie beschafft oder besitzt (Abs. 1 bis). Die Rechtsprechung und Lehre zum Besitz gemäss Art. 197 StGB ist analog auch in Bezug auf Art. 135 Abs. 1 bis aStGB anwendbar. Es kann auf die diesbezüglichen Ausführungen verwiesen werden.

E. 3.2.1

Der Bericht der KAPO Bern und die daraus hervorgehenden Erkenntnisse sind grundsätzlich unbestritten. Es erfolgten nachweislich von der IP-Adresse, die auf den Beschuldigten registriert war, Downloads verbotener Pornografie in einem P2P-Netzwerk. Dass es sich bei den Videos um tatsächliche sexuelle Handlungen mit Minderjährigen handelt, ist durch die aktenkundigen Videodateien ebenfalls erstellt. Es handelt sich dabei um 18 Videos im entsprechenden Dateiordner. Auf der dem Bericht der KAPO Bern beiliegenden Liste sind zwar 20 Dateien entsprechend markiert (rot), da sich aber nur 18 Dateien überprüfen lassen, ist vorliegend – entgegen der Anklageschrift, die von mindestens 20 Dateien ausgeht – nur von 18 Dateien mit verbotener Pornografie auszugehen.

E. 3.2.2

Fraglich bleibt, ob diese Downloads dem Beschuldigten nachzuweisen sind. Zwar war die IP-Adresse an der [Strasse] in [Ort 1] auf den Beschuldigten registriert und dieser war unbestritten zum Tatzeitpunkt Mieter eines Lagerraums an der genannten Adresse. Jedoch liefert die IP-Adresse noch keinen Aufschluss über das verwendete Gerät. Keines der 18 Videos, die via P2P-Netzwerk heruntergeladen wurden, konnte auf einem der Geräte des Beschuldigten gefunden werden. Auch die dazugehörigen GUID-Nummern konnten in keinem Datenträger nachgewiesen werden. Der Beschuldigte teilte seinen Internetzugang gemäss seinen Aussagen mit einem Mitmieter, der das Passwort auch weitergegeben haben könnte. Da es sich um einen Lagerraum handelte, den der Beschuldigte mit anderen Personen teilte, ist es nicht abwegig, dass das WLan-Passwort auch anderen Personen bekannt war und diese den Internetzugang des Beschuldigten nutzten. Dies bestätigt auch seine Aussage vor Obergericht, wonach ihm andere Mieter das Passwort abgeschwatzt hätten. Die Vorinstanz tat die Aussagen des Beschuldigten vorschnell pauschal als Schutzbehauptungen ab. Seine Aussagen zu diesem Vorhalt waren grundsätzlich konstant. Dass er ein P2P-Netzwerk nutzte, stritt er nie ab und Spuren des eMule-Client dessen konnten auch auf dem Computer Eigenbau und dem Laptop Asus nachgewiesen werden. Einzig über den Nutzungszeitraum des Netzwerks eDonkey – über welches die Downloads erfolgten – machte er zunächst widersprüchliche Aussagen. In der ersten Einvernahme sagte er aus, der Download der alten Windows-Version sei ein, vielleicht auch zwei Jahre her. In den späteren Einvernahmen (Polizei und Vorinstanz) gab er jeweils an, es sei rund 20 Jahre her. Vor Obergericht erklärte er, die Fragen zuvor missverständlich beantwortet zu haben. Er habe eDonkey zu Schulzeiten genutzt, was lange her sei, im Tatzeitraum habe er ein anderes P2P genutzt, Micro Torrent. Wofür er den Client genutzt habe, gab er dagegen immer gleich an, nämlich zum Download von alten Windows-Versionen. Bei eDonkey handelt es sich sodann um ein weitum bekanntes P2P-Netzwerk. Es wurden Fragmente von Suchen mit einschlägigen Stichwörtern («preteen» etc.) auf dem Asus Laptop wie auch dem Computer Eigenbau gefunden. Diese lassen sich zeitlich jedoch nicht einordnen und der Laptop Asus wurde durch den Beschuldigten nicht neu gekauft, sondern stammte von seinem früheren Arbeitsort im [Zentrum]. Es lässt sich nicht ausschliessen, dass entsprechende Suchen mit dem Laptop zuvor oder auch durch eine andere Person getätigt wurden; zumal der Beschuldigte den Laptop gemäss dem Nutzerprofil «D.___» zusammen mit seiner Partnerin nutzte. Der eMule-Client und die Fragmente mit Präferenzindikatoren auf dem Computer Eigenbau wurden auf einer Festplatte festgestellt, die der Beschuldigte ebenfalls nicht neu gekauft hatte. Darauf fanden sich zahlreiche Hinweise auf einen «G.___» (AS 049), weshalb auch die Möglichkeit besteht, dass dieser «G.___» entsprechende Suchen getätigt hat und nicht der Beschuldigte. «G.___» hatte gemäss Aussage des Beschuldigten denn auch bis ins Jahr 2023, als die Halle aufgelöst wurde, mittels eigenem Schlüssel Zugang zu dieser. Dies fällt in den Tatzeitraum von Dezember 2021 bis Januar 2023. Die Aussagen des Beschuldigten vor Obergericht sind überzeugend. Er bemühte sich, die für ihn unangenehme Situation zu erklären und seine Aussagen werden durch die objektiven Beweismittel unterstrichen. Die Möglichkeit eines Fernzugriffs ist gemäss Nachtragsrapport vom 4. November 2024 ausgeschlossen. Dies ändert jedoch nichts daran, dass nicht nachgewiesen ist, dass die Downloads von einem Gerät des Beschuldigten getätigt wurden, da keinerlei Spuren dieser Videos auf seinen Geräten gefunden werden konnten. Dass er diese, wenn überhaupt, selbst getätigt habe, ist ebenfalls nicht erstellt. Ihm zu unterstellen, er hätte sie nach dem Download endgültig löschen können, geht insbesondere in Anbetracht anderer Dateien, die wiederhergestellt werden konnten, zu weit.

Dasselbe gilt für den Hinweis der Polizei bezüglich des Geschäftslaptops des Beschuldigten. Dieser wurde nicht beschlagnahmt und ausgewertet, weshalb jegliche Spekulationen diesen betreffend gänzlich unbeachtlich sind. Es lässt sich im Ergebnis nicht rechtsgenüglich nachweisen, dass der Beschuldigte selbst die Downloads getätigt hat. Der Sachverhalt gemäss Anklage ist nicht erstellt und der Beschuldigte von diesem Vorhalt freizusprechen. B. Mehrfache harte Pornografie (sexuelle Handlungen mit Tieren [Besitz] und tatsächliche sexuelle Handlungen mit Minderjährigen [Besitz]) (Art. 197 Abs. 5 Satz 1 und 2 StGB) a. Sexuelle Handlungen mit Tieren 1. Vorhalt gemäss Anklageschrift Ziffer 2a Die Staatsanwaltschaft wirft dem Beschuldigten Folgendes vor: «begangen bis am 24. Mai 2023 (Datum der Sicherstellung der elektronischen Geräte), in [Ort 3], [Adresse 2] (Garage des Beschuldigten) und evtl. anderswo, indem der Beschuldigte zwei Videodateien, welche sexuelle Handlungen mit Tieren zum Inhalt haben, auf dem eigens gebauten Computer mit dem Gehäuse «Sharkoon» (Objekt-Nr. I-23-049.20) bzw. auf der darin eingebauten Festplatte «Hitachi, HDD, 5K750-500» (Objekt-Nr. I-23-049.20B) besass. Konkret zeigen die Videos einerseits sexuelle Handlungen einer unbekannten weiblichen Person mit einem Pferd (die Frau befriedigt das Pferd oral) und andererseits sexuelle Handlungen einer unbekannten männlichen Person mit einem Huhn (der Mann übt Geschlechtsverkehr mit einem Huhn aus bzw. penetriert mit seinem Penis ein Huhn).» 2. Beweiswürdigung

E. 3.3

Der Inhalt der beiden Videodateien ist vorliegend nicht strittig. Es stellt sich dieselbe Frage wie in Bezug auf die Videos mit Tierpornografie. Die Dateien mit Gewaltdarstellungen befanden sich am gleichen Speicherort wie die anderen beiden Videodateien. Es hat damit auch für sie zu gelten, dass durch den Sachverhalt kein Vorsatz des Beschuldigten begründet werden kann und es kann auf die Ausführungen zum anderen Vorhalt (III.B.a.) verwiesen werden. Auch von diesem Vorhalt ist der Beschuldigte damit freizusprechen. IV. Einziehung und Löschung der Daten 1. Der Beschuldigte wurde zwar von sämtlichen Vorwürfen freigesprochen, es handelt sich aber bei den gefundenen Dateien unbestritten um verbotene Pornografie, weshalb die entsprechenden Datenträger dennoch einzuziehen und zu vernichten sind (Art. 197 Abs. 6 i.V.m. Art. 69 StGB). Es liegt im Übrigen kein anderslautender Antrag der Verteidigung vor. 2. Zudem sind die forensisch gesicherten Daten der Mobile-Forensik, Fallnummer M-23-163-01, sowie der IT-Forensik, IT-Fallnummer I-23-049, nach Rechtskraft dieses Urteils zu löschen. Die Polizei Kanton Solothurn ist deshalb anzuweisen, dies nach Rechtskraft vorzunehmen. V. Kosten und Entschädigungen 1. Verfahrenskosten

E. 4

Die Anklageschrift an das Richteramt Dorneck-Thierstein datiert vom 12. März 2024 (AS unpaginiert, vor 001).

E. 5

Folgende im Verfahren gegen A.___ beschlagnahmten Gegenstände (alle aufbewahrt bei der Polizei Kanton Solothurn, FB Asservate) werden eingezogen und sind nach Rechtskraft des Urteils durch die Polizei zu vernichten: a) 1 Festplatte Hitachi, HDD, 5K750-500 (Objekt-Nr. I-23-049.20B) b) 1 Festplatte Seagate, Barracuda, ST3320820A (Objekt-Nr. I-23-049.04A) c) 1 Festplatte Samsung, SSD, 840 EVO (Objekt-Nr. I-23-049.02A).

E. 5.14

MB auf. Ein Video dieser Grösse stelle kaum Anforderungen an die Leistungsfähigkeit des jeweiligen Computers/USB-Sticks und könne grundsätzlich problemlos von Geräten auch älteren Baujahres verzögerungsfrei abgespielt werden. Beim Begriff «PHANT» im Dateinamen handle es sich um ein Label für Kinderpornografie, aber es sei klar, dass dies nur derjenige wissen könne, der sich damit beschäftige. Das Video sei gar nicht effektiv aus dem Dateisystem gelöscht worden, sondern habe noch im Papierkorb gelegen. Das Video könne also vom User auf Knopfdruck wiederhergestellt werden. Ferner vermöge die Darstellung des Beschuldigten nicht zu erklären, warum an zahlreichen Stellen auf der Festplatte Dateinamen von Videos mit eindeutig kinderpornografischen Begriffen gefunden worden seien. Ausserdem sei festgestellt worden, dass tatsächlich die gesuchte P2P-Software eMule installiert gewesen sei. Die Polizei teile grundsätzlich die Feststellungen des Verteidigers, dass es nicht beweisbar sei, dass diese Videos dem Beschuldigten gehörten. Auch wenn es eher unwahrscheinlich erscheine, dass jemand seinen Ordner \Backup\WORK\ an einer LAN-Party mit anderen geteilt haben solle. Es stehe fest, dass die Videos im einzigen Benutzerprofil namens «H.___» gespeichert seien (auf dem Desktop und im Papierkorb). Weiter sei ersichtlich, dass mindestens E.___ diese Festplatte benutzt zu haben scheine. Es könne forensisch nicht überprüft werden, wer effektiv alles an dem Computer gearbeitet habe. Es seien jedoch keinerlei Hinweise gefunden worden, dass der Beschuldigte irgendetwas damit zu tun gehabt hätte, bis auf die Tatsache, dass die Festplatte in seinem Computer eingebaut sei und die beiden Videos direkt in einem Ordner auf dem Desktop gelegen hätten und damit recht einfach zugänglich seien. Es stimme, dass die beiden Datenträger 20C und 20D zu einem Volume verbunden seien. Zwar sei es möglich, dass die alten Daten von anderen Personen stammen würden, es sei damit jedoch nicht bewiesen. Diese Daten könnten auch von einer früheren Nutzung durch den Beschuldigten stammen. Die Suche nach «preteen+lolita+pics» zeige tatsächlich nicht, ob aufgrund dieser Suche effektiv eine entsprechende Datei heruntergeladen worden sei. Allerdings zeige sie, dass mit dieser Festplatte zumindest versucht worden sei, sich entsprechende Dateien zu beschaffen. Es könne technisch nicht bewiesen werden, dass die «verdächtigen Tätigkeiten» auf diesem PC tatsächlich vom Beschuldigten ausgeübt worden seien. Effektiv seien die enthaltenen Festplatten aber in dessen Besitz und mindestens die beiden Videos auf dem Desktop wären einfach auffindbar gewesen. Die Feststellungen der Polizei seien v.a. im Zusammenhang mit der gemeldeten Verbreitung kinderpornografischer Darstellungen via P2P vom Anschluss des Beschuldigten aus relevant, da mit diesen Festplatten nachweislich sowohl die P2P-Software eMule verwendet als auch nach Kinderpornografie gesucht und entsprechende Websites besucht worden seien. Es seien eindeutig vom Anschluss des Beschuldigten aus kinderpornografische Darstellungen via P2P-Software verbreitet worden. Ungeachtet, ob der Beschuldigte dies getan habe, widerspreche die Tatsache, dass nichts gefunden worden sei, nicht den von der KAPO Bern dokumentierten Tatsachen. Die Durchsuchung sei rund 4 Monate später erfolgt, sodass leicht verständlich sei, dass die zur Tatzeit verwendeten Geräte oder Darstellungen nicht mehr vorgefunden worden seien. Insbesondere auch, da der Beschuldigte gemäss eigenen Angaben gerne an den Computersystemen herumbastle. Weiter habe gerade ein teilweiser Umzug an einen neuen Lagerstandort stattgefunden. Und schliesslich sei dem Beschuldigten auch das Geschäftslaptop, an dessen Passwort er sich nicht mehr habe erinnern können, aus Verhältnismässigkeitsgründen belassen worden. Die Verwendung als Minecraft-Server könne unmöglich als entlastende Erklärung hinzugezogen werden. Alleine dadurch könnten keine verbotenen Darstellungen auf den

Computer gelangt (und dann noch zusätzlich via P2P-Software verbreitet worden sein). Das Minecraft-Serverprogramm stelle übers Internet Minecraft-Spielern Welten zur Verfügung. Die Spieler könnten dadurch keine Dateien irgendwo auf dem Computer speichern.

E. 6
Gegen dieses Urteil meldete der Beschuldigte mit Eingabe vom 18. Juni 2024 die Berufung an. Nach Zustellung des begründeten Urteils am 14. August 2024 erklärte der Beschuldigte gleichentags die Berufung (Aktenseite Berufungsgericht [ASB] 1). Er ficht das Urteil vollumfänglich an und verlangt einen Freispruch sowie die Kostenübernahme durch den Staat. Für den Fall einer Verurteilung sei auf das Berufsverbot zu verzichten und von der Bewährungshilfe abzusehen.

E. 7
Mit Eingabe vom 22. August 2024 verzichtete die Staatsanwaltschaft auf eine Anschlussberufung und die weitere Teilnahme am Berufungsverfahren, in Erwartung des begründeten Urteils des Obergerichts.

E. 8
Der Verteidiger des Beschuldigten stellte am 22. August 2024 den Beweisantrag, es sei ein technisches Gutachten zu erstellen (ASB 15 f.). Der Beweisantrag wurde mit Verfügung vom 22. Oktober 2024 in dem Sinne gutgeheissen, als dass die Kantonspolizei Solothurn aufgefordert wurde, einen Nachtragsrapport betreffend die Eingabe des Verteidigers einzureichen (ASB 20 f.).

E. 9
Mit Schreiben vom 18. September 2024 teilte der Verteidiger mit, der Beschuldigte wünsche eine mündliche Berufungsverhandlung (ASB 19).

E. 10
Am 4. November 2024 erfolgte die Vorladung zur Berufungsverhandlung (ASB 22 ff.).

E. 11
Nach Zustellung des Nachtragsrapports vom 4. November 2024 (ASB 28 ff.) beantragte der Beschuldigte die Zustellung der dem Bericht zugrunde liegenden Daten, damit diese einem externen Gutachter zur Verfügung gestellt werden könnten (ASB 42). Nach Konkretisierung der gewünschten Datenträger wurde die Kantonspolizei Solothurn mit Verfügung vom 27. Januar 2025 aufgefordert, die verlangten Datenträger zu kopieren und der Verteidiger ermächtigt, diese der ausgewählten Firma zwecks forensischer Prüfung bzw. Analyse zu übergeben (ASB 47 f.). Mit Verfügung vom 10. Februar 2025 wurden die Datenträger dem Verteidiger zugestellt (ASB 58).

E. 12
Am 26. März 2025 gingen die schriftlichen Plädoyernotizen des Verteidigers ein (ASB 80 ff.).

E. 13
Mit Verfügung vom 31. März 2025 wurde die Kantonspolizei Solothurn nochmals aufgefordert, die nun zusätzlich verlangten Datenträger zu kopieren und der Verteidiger ermächtigt, diese der ausgewählten Firma zwecks forensischer Prüfung bzw. Analyse zu übergeben (ASB 92 f.). Mit Verfügung vom 7. April 2025 wurden die Datenträger dem

Verteidiger zugestellt (ASB 96).

E. 14

Die Berufungsverhandlung fand am 16. April 2025 statt. Anlässlich der Verhandlung reichte der Verteidiger u.a. einen Kurzbericht der B.___ AG (ASB 104 f.) sowie deren Korrektur seiner Plädoyernotizen (ASB 106 ff.) ein. II. Formelles 1. Anwendbares Recht Per 1. Januar 2024 trat die Revision der Schweizerischen Strafprozessordnung (StPO, SR 312.0) in Kraft. Unter dem Abschnitt der Rechtsmittelverfahren hält Art. 454 Abs. 1 StPO fest, dass für Rechtsmittel gegen erstinstanzliche Entscheide, die nach Inkrafttreten dieses Gesetzes gefällt werden, neues Recht gilt. Da die Vorinstanz das Urteil am 17. Juni 2024 fällte, ist das neue Recht anwendbar. 2. Anklagegrundsatz