

BGE 152 IV 107

Bundesgericht (BGE), 2026-01-01, DE

Quelle: [https://mcp.opencaselaw.ch/entscheid/bge_152 IV 107](https://mcp.opencaselaw.ch/entscheid/bge_152_IV_107)

FR: ATF 152 IV 107

IT: DTF 152 IV 107

Regeste

Regeste Art. 248 Abs. 1 StPO; Siegelung und Entsiegelung sichergestellter elektronischer Datenträger; Zulässigkeit der Anordnung einer Datenspiegelung durch die Strafverfolgungsbehörden. Zuständigkeiten und Befugnisse der Strafverfolgungsbehörden und der Zwangsmassnahmengerrichte im Entsiegelungsverfahren (E. 5.2). Nach bisheriger Rechtsprechung (BGE 148 IV 221) ist es den Strafverfolgungsbehörden untersagt, im Zusammenhang mit der Sicherstellung von elektronischen Datenträgern selber die Erstellung einer Datenkopie (sog. Spiegelung) durch eine sachverständige Person anzuordnen (E. 5.3). Insbesondere der aufgrund des technischen Fortschritts zunehmend fragiler werdende Zustand von elektronisch gespeicherten Daten hat in der Lehre zu Kritik an dieser Rechtsprechung geführt, da eine zeitnahe Datenextraktion für die Beweissicherung von zentraler Bedeutung ist (E. 5.6). Eine Analyse der per 1. Januar 2024 in Kraft getretenen revidierten Bestimmungen des Siegelungsverfahrens, der kritischen Lehrmeinungen, des technischen Prozesses des Datenspiegelungsvorgangs sowie des technischen Fortschritts bei der Datensicherung führt zum Ergebnis, dass es den Strafverfolgungsbehörden möglich sein muss, in Fällen eines unmittelbar drohenden Beweisverlusts selber eine Datenspiegelung durch eine sachverständige Person anzuordnen (Änderung der Rechtsprechung; E. 5.7). Die für die Datenspiegelung eingesetzte sachverständige Person darf jedoch nicht auch in die eigentliche Ermittlungstätigkeit eingebunden werden (E. 5.7.8).

Erwägungen

E. 5.1

Der Beschwerdeführer stellt sich weiter auf den Standpunkt, gemäss Art. 248 Abs. 1 StPO könne die beschuldigte Person innert drei Tagen seit der Sicherstellung von Aufzeichnungen und Gegenständen durch die Strafverfolgungsbehörde die Siegelung verlangen. Während dieser Frist und nach einer allfällig bereits erfolgten Siegelungserklärung dürften die Strafverfolgungsbehörden die sichergestellten Asservate weder einsehen noch verwenden. Vorliegend habe die Jugendanwaltschaft unmittelbar nach der Sicherstellung der beiden Mobiltelefone eine vorsorgliche Datensicherung angeordnet. Dies verletze die Vorgaben von Art. 248 Abs. 1 StPO, da durch das gewählte Vorgehen der vorsorglichen Datensicherung nicht gewährleistet sei, dass die Strafverfolgungsbehörden vor Abschluss des Entsiegelungsverfahrens keine Einsicht in geheimnisgeschützte Daten erhalte. Gemäss BGE 148 IV 221 (E. 4) sei im Vorgehen der Jugendanwaltschaft ein schwerer Verfahrensfehler zu sehen, der zur Abweisung des Entsiegelungsgesuchs führen müsse. Namentlich könne die erfolgte vorsorgliche Datensicherung nicht durch eine BGE 152 IV 107 S. 110 nachträgliche Genehmigung durch das Zwangsmassnahmengerricht gerechtfertigt werden, zumal im vorliegenden Fall eine rechtzeitige Anrufung des

Zwangsmassnahmengerichts möglich gewesen wäre.

E. 5.2.1

Ersucht die Strafverfolgungsbehörde nach erfolgter Siegelung um Entsiegelung der betreffenden Aufzeichnungen und Gegenstände, hat sie dem Zwangsmassnahmengericht die versiegelten Aufzeichnungen und Gegenstände zur Verfügung zu stellen (Urteil 7B_127/ 2022 vom 5. April 2024 E. 3.3 mit Hinweisen). Im Entsiegelungsverfahren hat nicht die Untersuchungsbehörde, sondern, allenfalls unter Beizug einer sachverständigen Person, das Zwangsmassnahmengericht zu prüfen, ob schutzwürdige Geheimnisinteressen oder andere gesetzliche Entsiegelungshindernisse einer Durchsuchung entgegenstehen (BGE 148 IV 221 E. 2.3 mit Hinweisen; Urteil 7B_805/ 2023 vom 28. Juni 2024 E. 2.1). Ausnahmen bzw. Erledigungen schon im Siegelungsverfahren durch die Strafverfolgungsbehörde können nur in liquiden Fällen in Frage kommen, etwa wenn das Siegelungsbegehren offensichtlich unbegründet bzw. rechtsmissbräuchlich erhoben erscheint und ein förmliches Entsiegelungsverfahren mit materieller Prüfung aller substantiierten Durchsuchungshindernisse geradezu einem Prozessleerlauf gleichkäme (Urteile 7B_1154/ 2024 vom 2. Oktober 2025 E. 2.4.1; 7B_515/2024 vom 3. April 2025 E. 2.2.3, nicht publ. in: BGE 151 IV 322 ; 7B_998/2023 vom 30. September 2024 E. 3; 7B_313/2024 vom 24. September 2024 E. 3.2; je mit Hinweisen).

E. 5.2.2

Das Zwangsmassnahmengericht hat im Entsiegelungsverfahren auch zu prüfen, ob die Strafbehörden die Vorschriften über die Siegelung eingehalten haben. Bei rechtswidrigem Vorgehen im Zusammenhang mit der Siegelung von Aufzeichnungen und Gegenständen ist zwischen der Fortsetzung des Entsiegelungsverfahrens einerseits und der Verwertbarkeit von Beweismitteln andererseits zu unterscheiden. Bei schweren Verfahrensmängeln ist nach der Rechtsprechung eine Fortsetzung des Entsiegelungsverfahrens ausgeschlossen und das Entsiegelungsbegehren abzuweisen (Urteile 7B_515/2024 vom 3. April 2025 E. 2.2.3, nicht publ. in: BGE 151 IV 322 ; 7B_127/ 2022 vom 5. April 2024 E. 3.3; 7B_54/2023 vom 12. Oktober 2023 E. 4.1 f.; je mit Hinweis auf BGE 148 IV 221 E. 4).

E. 5.3

In BGE 148 IV 221 hatte das Bundesgericht über die Entsiegelung von elektronischen Geräten in einem Verwaltungsstrafverfahren wegen Widerhandlungen gegen das Zollgesetz und das BGE 152 IV 107 S. 111 Mehrwertsteuergesetz zu entscheiden. Die Geräte waren von der Zollverwaltung sichergestellt und anschliessend dem Bundesamt für Polizei (fedpol) zwecks Entsperrung und Datenspiegelung übermittelt worden. Im Anschluss stellte die Zollverwaltung bei der Beschwerdekammer des Bundesstrafgerichts ein Entsiegelungsgesuch betreffend die zwischenzeitlich versiegelten Datenträger. Dieses wurde gutgeheissen. Das Bundesgericht hiess die Beschwerde des Beschuldigten gegen die bewilligte Entsiegelung gut. Es hielt im Wesentlichen fest, Zweck der Siegelung sei, jegliche Gelegenheit für die Untersuchungsbehörde zur Kenntnisnahme der sichergestellten Daten auszuschliessen, bevor ein Gericht über die Zulässigkeit des Zugangs zu diesen Daten entscheide. Nehme die Untersuchungsbehörde selber eine Spiegelung vor oder gebe sie diese in Auftrag, lasse sich die Möglichkeit einer verfrühten Kenntnisnahme der Daten nicht ausschliessen. Eine entsprechende Praxis vermöge den Zweck der Siegelung somit nicht zu gewährleisten (BGE 148 IV 221 E. 2.5). Erweise sich eine Kopie der Daten als angebracht, habe die Untersuchungsbehörde nach der sofortigen Siegelung der Datenträger

beim Zwangsmassnahmengericht ein "Spiegelungsgesuch" zu stellen. Sie dürfe in keiner Weise in die Entsperrung der Geräte und Spiegelung der Daten als Realakte einbezogen werden (BGE 148 IV 221 E. 2.6). Die Entsperrung der Geräte und die Datenspiegelung durch eine von der Untersuchungsbehörde beauftragte Behörde vor der Siegelung stelle einen erheblichen Verfahrensmangel dar, der sich nicht mehr korrigieren lasse. Die Rechtswidrigkeit des behördlichen Vorgehens wiege derart schwer, dass nicht ersichtlich sei, wie die Daten noch verwertbar sein könnten. Dies führe zur Vernichtung der erstellten Datenkopien sowie zur Rückgabe der sichergestellten Geräte an die berechnigte Person (BGE 148 IV 221 E. 4).

E. 5.4

Nach den für das Bundesgericht gemäss Art. 105 Abs. 1 BGG verbindlichen Feststellungen der Vorinstanz wurde der Beschwerdeführer am 3. März 2024 (Sonntag) um ca. 15:30 Uhr verhaftet. Bereits zu diesem Zeitpunkt wurden die Daten auf den sichergestellten zwei Mobiltelefonen vorsorglich durch den kriminaltechnischen Dienst der Kantonspolizei Zürich mittels Datenspiegelung gesichert, um einen Datenverlust zu verhindern. Die auf diesem Weg gespiegelten Daten wurden unmittelbar auf zwei Datenträger abgespeichert und in ein Lagerbehältnis verpackt, an welchem aufgrund des Siegelungsantrags des Beschwerdeführers vom 4. März 2024 ein BGE 152 IV 107 S. 112 amtliches Siegel angebracht wurde. Am 6. März 2025 (Dienstag) stellte die Jugendanwaltschaft bei der Vorinstanz nachträglich ein Gesuch um unverzügliche Spiegelung der sichergestellten Mobiltelefone. Mit korrigiertem Gesuch vom 8. März 2025 legte die Jugendanwaltschaft gegenüber der Vorinstanz offen, dass bereits am Tag der Festnahme des Beschwerdeführers vorab eine Datensicherung bzw. Datenspiegelung durch die Kantonspolizei erfolgt sei. Die Vorinstanz bewilligte die vorsorgliche Datenspiegelung mit Verfügung vom 8. März 2024.

E. 5.5

Mit Blick auf BGE 148 IV 221 ist dem Beschwerdeführer zuzustimmen, dass vergleichbar mit der dem Leitentscheid zugrunde liegenden Sachverhaltskonstellation auch im vorliegenden Fall die Strafverfolgungsbehörden ohne vorgängige Genehmigung durch das Zwangsmassnahmengericht eine Datenspiegelung durch die Dienstabteilung Forensik der Kantonspolizei Zürich anordneten. Es stellt sich deshalb die Frage, ob die Rechtsprechung, die noch unter dem bis zum 31. Dezember 2023 geltenden Siegelungsrecht ergangen ist, auch nach dem per 1. Januar 2024 in Kraft getretenen neuen Siegelungsrecht uneingeschränkt auf das neue Recht übertragen werden kann. Dabei ist namentlich auch der technische Fortschritt bei der elektronischen Datenverarbeitung und Datensicherung zu berücksichtigen.

E. 5.6

Die in BGE 148 IV 221 entwickelte Rechtsprechung ist von Lehre und Praxis unterschiedlich aufgenommen worden. Es erging Zustimmung wie auch Kritik. Insoweit kann auf die Erwägungen im BGE 151 IV 322 (E. 3.3) verwiesen werden. Ein ernst zu nehmender Kritikpunkt betraf namentlich den gestützt auf den fortlaufenden technischen Fortschritt zunehmend fragiler werdenden Zustand von Daten. Die heutzutage auf Mobiltelefonen gespeicherten Daten werden immer flüchtiger, da sie wegen den in den Betriebssystemen enthaltenen Datenschutzprogrammen oder den darauf gespeicherten Applikationen (sog. "Apps") nach einer immer kürzer werdenden Zeitspanne automatisch, das heisst ohne weiteres Zutun, gelöscht werden. Eine Datenlöschung kann zudem vermehrt

auch mittels Fernzugriff erfolgen (vgl. BGE 151 IV 322 E. 3.3; GRAF/RÜTSCHE, Datensicherung von Mobiltelefonen und Tablets - technische und [siegelungs-]rechtliche Herausforderungen im Strafverfahren, SJZ 121/2025 S. 607 ff.; vgl. auch GETH/WOHLERS, Das Strafverfahren in den Zeiten der Digitalisierung, ZStrR 142/2024 S. 166). Namentlich bei Mobiltelefonen des Typs "iPhone" und dem sich darauf BGE 152 IV 107 S. 113 befindenden Betriebssystem iOS ist es vom Hersteller als Sicherheitsmassnahme verbreitet, dass sich das Betriebssystem nach einer immer kürzeren Zeitspanne aufgrund von Inaktivität automatisch herunterfährt und sich das System danach neu startet. Dies ist für die forensische Datensicherung mit weitreichenden Nachteilen verbunden, weil sich das Mobiltelefon danach im sogenannten "Before First Unlock-Modus" befindet, der eine Datenextraktion nahezu unmöglich macht (vgl. GRAF/RÜTSCHE, a.a.O., S. 607 f. mit detaillierten technischen Ausführungen zur Datenextraktion bei Mobiltelefonen und Tablets). Hinzu kommen zusätzliche Schwierigkeiten in Bezug auf Daten, die sich auf einer sogenannten "Cloud", also nicht direkt auf dem eigentlichen Mobiltelefon, befinden. Der Zugriff auf Daten einer "Cloud" kann jederzeit aus der Ferne unterbunden werden (vgl. GRAF/RÜTSCHE, a.a.O., S. 615). Eine zeitnahe Datenextraktion ist daher von zentraler Bedeutung, weil eine Datensicherung aufgrund der genannten technischen Fortschritte nach Ablauf einer immer kürzer werdenden Zeitspanne nahezu unmöglich wird.

E. 5.7

Die per 1. Januar 2024 in Kraft getretenen neuen Bestimmungen des Siegelungsrechts wie auch die Rechtsprechung gemäss BGE 148 IV 221 sind im Lichte dieser sich fortlaufend verändernden technischen Entwicklungen zu würdigen.

E. 5.7.1

Wie der Beschwerdeführer zu Recht vorbringt, wurde mit Inkrafttreten des neuen Siegelungsrechts für den Inhaber von im Rahmen eines Strafverfahrens sichergestellten Aufzeichnungen und Gegenständen in Art. 248 Abs. 1 StPO eine Bedenkfrist von drei Tagen seit der Sicherstellung eingeführt, um gegenüber den Strafverfolgungsbehörden die Siegelung zu beantragen. Der Beschwerdeführer vertritt insoweit die Auffassung, ausgehend von der Rechtsprechung gemäss BGE 148 IV 221 sei es den Strafverfolgungsbehörden untersagt, vor Ablauf dieser Frist von drei Tagen ohne vorgängige Genehmigung durch das Zwangsmassnahmengericht eine Datensicherung mittels Datenspiegelung anzuordnen. Er begründet dies damit, dass das Bundesgericht im genannten Leitentscheid ausdrücklich festgehalten habe, bei einer eigenmächtigen Datenspiegelung durch die Polizei oder die Staatsanwaltschaft könne nicht hinreichend sichergestellt werden, dass die Strafverfolgungsbehörden vor Abschluss des Entsiegelungsverfahrens keine Kenntnis vom Inhalt der Datenträger erhielten. Eine wie im vorliegenden Fall erfolgte nachträgliche Genehmigung der vorsorglichen Datenspiegelung durch das Zwangsmassnahmengericht vermöge daran nichts zu ändern. BGE 152 IV 107 S. 114 Vielmehr liege ein schwerer Verfahrensmangel vor, der zwingend zur Unverwertbarkeit und Vernichtung der sichergestellten Datenträger führen müsse.

E. 5.7.2

Im vorliegenden Fall gilt es zunächst festzuhalten, dass der Beschwerdeführer anlässlich seiner Festnahme und der Sicherstellung seiner beiden Mobiltelefone am 3. März 2024 keinen Siegelungsantrag stellte. Dieser erfolgte erst am nachfolgenden Tag im Rahmen

seiner polizeilichen Einvernahme. Zu diesem Zeitpunkt war der Auftrag zur Datensicherung mittels Spiegelung der Mobiltelefonaten bereits erfolgt und der entsprechende Extraktionsprozess im Gang. Es stellt sich damit die Frage, ob die in Art. 248 Abs. 1 StPO normierte Frist für einen Siegelungsantrag dahingehend zu verstehen ist, dass die Strafverfolgungsbehörden in jedem Fall den Fristablauf abwarten müssen, bevor sie eine Datenspiegelung anordnen, oder ob sie zur Verhinderung eines unwiderruflichen Datenverlusts bereits zum Zeitpunkt der Sicherstellung eine sachverständige Person mit der vorsorglichen Datensicherung beauftragen dürfen.

E. 5.7.3

Gemäss Art. 248 Abs. 1 erster Satz StPO hat die Strafverfolgungsbehörde sichergestellte Gegenstände und Aufzeichnungen zu siegeln, sofern die Inhaberin oder der Inhaber geltend machen, diese dürften aufgrund von Art. 264 Abs. 1 StPO nicht beschlagnahmt werden. Art. 248 Abs. 1 zweiter Satz StPO sieht weiter vor, dass die Inhaberin oder der Inhaber das Siegelungsbegehren innert drei Tagen seit der Sicherstellung vorzubringen hat. Während dieser Frist und nach einer allfälligen Siegelung darf die Strafbehörde die Aufzeichnungen und Gegenstände weder einsehen noch verwenden (Art. 248 Abs. 1 dritter Satz StPO).

E. 5.7.4

Diesem Gesetzeswortlaut folgend ist es den Strafverfolgungsbehörden ab dem Moment der Sicherstellung untersagt, während der gesetzlich normierten Siegelungsfrist von drei Tagen die auf sichergestellten elektronischen Datenträgern enthaltenen Aufzeichnungen einzusehen oder zu verwenden. Es stellt sich insoweit die Frage, ob der Vorgang der Sicherstellung der Daten mittels Spiegelung des Datenträgers ein Einsehen oder eine Verwendung darstellt beziehungsweise ob ein Einsehen in den Datenträger in diesem Zeitpunkt überhaupt möglich ist.

E. 5.7.5

Um einen Fernzugriff auf die Mobiltelefone zu verunmöglichen, werden diese nach der Sicherstellung in faradayschen Behältnissen verschlossen und zugleich an den Strom angeschlossen, um BGE 152 IV 107 S. 115 eine automatische Rückversetzung des Geräts zufolge Inaktivität in den "Before First Unlock-Modus" und einen damit einhergehenden endgültigen Datenverlust zu vermeiden (vgl. E. 5.6 hiervor). Durch die faradayschen Behältnisse ist eine Bedienung des Bildschirms des Geräts und damit ein Einsehen in die darauf gespeicherten Daten unmöglich (vgl. GRAF/RÜTSCHKE, a.a.O., S. 614). Sofern der Entsperrungscode des Geräts nicht bekannt ist, wäre eine haptische Manipulation des Bildschirms ohnehin nicht zielführend, weil sich die Geräte aus Sicherheitsgründen oftmals nach mehrfacher Eingabe eines falschen Codes automatisch sperren, was eine Datenextraktion erheblich erschwert oder gar unmöglich macht (vgl. GRAF/RÜTSCHKE, a.a.O., S. 608). Die eigentliche Datenspiegelung ist ihrerseits kein Prozess, bei welchem das Mobiltelefon bedient wird und erfolgt ohne bildgebende Technik. Es handelt sich vielmehr um einen technischen Prozess, bei welchem mittels forensischen Programmen über Sicherheitslücken versucht wird, im Betriebssystem des Mobiltelefons auf das verschlüsselte Gerät zuzugreifen und die darauf befindlichen Daten abzuspeichern (vgl. GRAF/RÜTSCHKE, a.a.O., S. 606 und S. 616). Und selbst danach erfordert die Aufbereitung der gespiegelten und auf elektronischen Datenträgern gespeicherten Daten spezielle forensische Programme, die ein grosses Fachwissen verlangen, damit das Datenmaterial für die Strafverfolgung überhaupt in einem tauglichen und einsehbaren Datenformat erhältlich

gemacht werden kann (vgl. Urteil 7B_610/2023 vom 15. Januar 2025 E. 3.2 f.).

E. 5.7.6

Zusammengefasst stellt die Extraktion von Mobiltelefon-, Tablet- und Computerdaten auf externe Datenträger einen komplexen technischen Vorgang dar, der ohne bildgebende technische Mittel abläuft und darüber hinaus nur von hierzu speziell befähigten sachverständigen Personen vorgenommen werden kann. Und selbst wenn bei diesem Vorgang auf Umwegen dennoch ein Einblick in die gespeicherten Dateien stattfinden sollte, könnte bei einem entsprechenden Verdacht ein unzulässiger Zugriff auf das Mobiltelefon mittels Auswertung der System- und Logdaten des Geräts nachverfolgt werden (vgl. GRAF/RÜTSCHKE, a.a.O., S. 614). Die Anordnung einer Spiegelung beziehungsweise der Spiegelungsvorgang stellt damit kein eigentliches Auslesen und auch keine Datenverwendung dar. Vielmehr handelt es sich um einen rein technischen Vorgang zur Datensicherstellung, bei dem keine Einsicht in die Daten erfolgt, sondern diese auf einen Datenträger extrahiert werden, der im BGE 152 IV 107 S. 116 Anschluss versiegelt wird. Durch diesen Prozess der Datenextraktion, der nicht durch die Strafverfolgungsbehörde, sondern durch einen forensischen Sachverständigen zu erfolgen hat, ist hinreichend garantiert, dass die Strafverfolgungsbehörde vor Abschluss des Entsiegelungsverfahrens keine Kenntnis vom Dateninhalt erhält. Mit anderen Worten ausgedrückt stellt die im Rahmen einer Spiegelung erfolgende Datenextraktion kein eigentliches Sichten und auch keine Datenverwendung durch die Strafverfolgungsbehörde im Sinne von Art. 248 Abs. 1 StPO dar, weil bei diesem Prozess noch gar keine inhaltliche Durchsuchung oder Auswertung der Daten vorgenommen wird (vgl. BGE 151 IV 322 E. 3.4.2).

E. 5.7.7

Selbstredend ist dem Beschwerdeführer zu folgen, wenn er ausführt, bei einer direkt durch die Strafverfolgungsbehörde angeordneten Spiegelung könne nicht mit absoluter Sicherheit garantiert werden, dass keine Kenntnisnahme des Dateninhalts durch die Strafverfolgungsbehörde erfolge. Wie das Bundesgericht in der Vergangenheit bereits wiederholt festgehalten hat, lässt sich eine solche vorzeitige Kenntnisnahme aber auch bei der Sicherstellung physischer Unterlagen nicht vollends vermeiden. Dies schadet allerdings deshalb nicht, weil die Untersuchungsbehörde nach der Rechtsprechung zum Zwecke der vorläufigen Sicherstellung eine thematische Grobsichtung von Aufzeichnungen vornehmen darf, um zu gewährleisten, dass nur Gegenstände sichergestellt werden, die potentiell untersuchungsrelevant erscheinen (BGE 143 IV 270 E. 7.5). Dies gilt auch bei elektronischen Datenträgern (BGE 151 IV 322 E. 3.4.2). Insoweit ist präzisierend festzuhalten, dass die elektronischen Datenträger nicht durch die Untersuchungsbehörden grob gesichtet werden, sondern diese zur Durchführung einer Datenspiegelung eine sachverständige Person beizieht. Diese unterliegt nach Art. 184 Abs. 2 lit. e StPO ihrerseits einer gesetzlichen Geheimhaltungspflicht und sie wird durch die Verfahrensleitung gemäss Art. 184 Abs. 2 lit. f StPO auf die Straffolgen eines falschen Gutachtens nach Art. 307 StGB hingewiesen. Vor dem Hintergrund, dass bei einer Datenspiegelung keine eigentliche Sichtung des Dateninhalts erfolgt und die sachverständige Person in derselben Strafuntersuchung nicht mit weiteren Ermittlungstätigkeiten beauftragt werden darf (vgl. E. 5.7.8 hiernach), besteht beim Vorgang der Datenspiegelung im Vergleich zu einer Grobsichtung von physischen Aufzeichnungen damit gar ein geringeres Risiko einer Kenntnisnahme durch die Strafverfolgungsbehörden. BGE 152 IV 107 S. 117

E. 5.7.8

Angesichts des vorgenannten technischen Fortschritts bei der Datensicherung von Mobiltelefonen ist die Zulässigkeit einer vorsorglichen Datenspiegelung umso mehr angezeigt, als angesichts des immer kürzer werdenden Zeitfensters für eine Datensicherung grundsätzlich nahezu in jedem Fall der Sicherstellung eines Mobiltelefons ein unmittelbarer Datenverlust droht. Wird dieser Gedanke fortgeführt, wäre ein Zuwarten mit der Datenspiegelung bis zum Ablauf der in Art. 248 Abs. 1 StPO normierten Bedenkfrist von drei Tagen zwangsläufig mit einem erheblichen und irreversiblen Datenverlust verbunden, was nicht dem Sinn und Zweck des Siegelungsverfahrens entspricht. Damit liegen ernsthafte und sachliche Gründe vor, die in Situationen mit einem aufgrund des technischen Fortschritts unmittelbar drohenden Datenverlust eine Abkehr von der mit BGE 148 IV 221 eingeführten Rechtsprechung rechtfertigen (vgl. BGE 150 IV 277 E. 2.3.1 mit Hinweisen). Präzisierend gilt es allerdings festzuhalten, dass die mit der Datensicherung betrauten forensischen Sachverständigen später nicht auch in die eigentliche Ermittlungstätigkeit des konkreten Strafverfahrens eingebunden werden dürfen. Durch diese Massnahme ist in Berücksichtigung der mit BGE 148 IV 221 begründeten Praxis weiterhin hinreichend gewährleistet, dass eventuelle grobe Kenntnis von Dateninhalten durch die sachverständige Person nicht auf Umwegen trotzdem Eingang in die Ermittlungshandlungen finden.

E. 5.7.9

Zusammengefasst ist festzuhalten, dass eine durch die Strafverfolgungsbehörden aufgrund eines konkret drohenden Beweisverlusts vorsorglich angeordnete Datenspiegelung keine Verletzung von Bundesrecht darstellt, sofern die Datenspiegelung durch eine sachverständige Person durchgeführt wird und diese später nicht auch in die eigentlichen Strafermittlungen involviert ist. Jedenfalls in Situationen eines unmittelbar drohenden Beweisverlusts gilt die Rechtsprechung gemäss BGE 148 IV 221 somit als überholt. Die Rügen des Beschwerdeführers, wonach die durch die Jugendanwaltschaft angeordnete Datenspiegelung bundesrechtswidrig sei, sind damit unbegründet.

Export aus OpenCaseLaw (CC0). Verbindlich ist allein der vom erlassenden Gericht veröffentlichte Originaltext. Quellen-URL siehe oben.