# BGE 151 IV 322

Bundesgericht (BGE), 2021-11-10, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/bge_151 IV 322

FR: ATF 151 IV 322

IT: DTF 151 IV 322

## Regeste

Regeste Art. 46 Abs. 1 lit. a, Art. 47 Abs. 1 und Art. 50 VStrR; Art. 248 Abs. 1 StPO; Edition und Siegelung elektronisch übermittelter Unterlagen. Werden Unterlagen gestützt auf ein Editionsbegehren elektronisch übermittelt, gehören sowohl die Übermittlung als auch das Herunterladen sowie das Abspeichern der Unterlagen durch die Untersuchungsbehörde zum Vorgang der Sicherstellung. Liegt bereits ein Siegelungsbegehren einer siegelungsberechtigten Person vor, sind die übermittelten Daten unverzüglich zu siegeln. Es ist zulässig, die Daten zu diesem Zweck auf einem externen Datenträger abzuspeichern und diesen zu versiegeln. Diese Vorgehensweise stellt keine unzulässige Spiegelung durch die Untersuchungsbehörde im Sinne von BGE 148 IV 221 E. 2-4 dar (E. 3).

## Erwägungen

### E. 3.1

Die Vorinstanz stützt sich im angefochtenen Beschluss hauptsächlich auf die bundesgerichtliche Rechtsprechung, wonach die Sicherung bzw. Spiegelung von Daten im Entsiegelungsverfahren nicht durch die Untersuchungsbehörde veranlasst werden darf ( BGE 148 IV 221 E. 2.5 f.). Sie führt dazu aus, mangels entsprechender Angaben der Beschwerdeführerin lasse sich nicht überprüfen, wie und wann sie auf die von der Bank elektronisch übermittelten Dokumente zugegriffen und ob sie dabei von deren Inhalt Kenntnis genommen habe. In der Editionsverfügung vom 10. November 2021 werde lediglich die E-Mail-Adresse des zuständigen Untersuchungsbeamten erwähnt. Dies lege den Schluss nahe, dass die entsprechenden Bankunterlagen per E-Mail zugestellt worden sein könnten. In diesem Fall seien sie nach Erhalt vom Untersuchungsbeamten grundsätzlich einsehbar gewesen. Die Angaben der Beschwerdeführerin, wonach sie die erhaltenen Daten nicht eingesehen, sondern auf einen Datenstick kopiert und diesen versiegelt habe, ändere nichts daran, dass sie diese grundsätzlich habe einsehen können und, soweit bekannt, nach wie vor einsehen könne. Es bestehe die Möglichkeit eines verfrühten und damit unberechtigten Zugriffs. Das Erstellen von Kopien elektronisch übermittelter Unterlagen durch die Untersuchungsbehörde vermöge den mit der Siegelung verfolgten Zweck mit Blick auf die Grund- und Verfahrensrechte der BGE 151 IV 322 S. 325 beschuldigten Person nicht zu erfüllen. Es stelle nach der bundesgerichtlichen Rechtsprechung einen schweren, nicht korrigierbaren Verfahrensmangel dar, weshalb das Entsiegelungsgesuch abzuweisen sei.

### E. 3.2

In BGE 148 IV 221 hatte das Bundesgericht über die Entsiegelung von elektronischen Geräten in einem Verwaltungsstrafverfahren wegen Widerhandlungen gegen das Zollgesetz und das 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 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 berechtigte Person ( BGE 148 IV 221 E. 4).

**E. 3.3**

Dieser Entscheid stiess in der Lehre auf (grundsätzliche) Zustimmung (MARTIN REIMANN, Die Entsperrung und Spiegelung von BGE 151 IV 322 S. 326 passwortgeschützten Datenträgern im Siegelungsverfahren, sui generis 2022 S. 217 ff.; TAORMINA/WANTZ [als Seite Strafverteidigung], Spiegeln oder Siegeln? - Ein Dialog, forumpoenale 6/2022 S. 441 ff.), aber auch auf Kritik. Die kritischen Stimmen brachten namentlich vor, das Bundesgericht vermische in BGE 148 IV 221 Beweissicherung und Beweisverwertung und unterscheide nicht zwischen Sicherstellung von Daten und deren Durchsuchung. Eine Datenspiegelung stelle keine Durchsuchung dar, da sie sich ausschliesslich auf einer maschinellen Ebene abspiele. Bei diesem technischen Vorgang könnten die Übereinstimmung der Originaldaten mit deren forensischen Kopie im Nachhinein zudem problemlos überprüft und allfällige Einwirkungen und Manipulationen festgestellt werden (vgl. YASMINE DELLAGANA-SABRY, Récolte et sauvegarde de données électroniques au regard de la procédure pénale administrative, in: Tempus fugit, 2024, S. 487 f.; HUNKELER/MOSIMANN [als Seite Strafverfolgung], Spiegeln oder Siegeln? - Ein Dialog, forumpoenale 6/2022 S. 442). Die Datenspiegelung gehe nicht mit einer Kenntnisnahme der Daten auf inhaltlicher Ebene einher (DAMIAN K. GRAF, Praxishandbuch zur Siegelung, 2022, S. 83 Rz. 236). Vor allem Mobiltelefone würden zudem flüchtige, temporäre und fragile Daten enthalten, die sich teilweise automatisch nach einer gewissen Zeit selbst löschen oder auch per Fernzugriff gelöscht werden könnten, weshalb ein überwiegendes öffentliches Interesse an deren sofortigen Sicherung bestehe (DELLAGANA-SABRY, a.a.O., S. 485 f.; GRAF, a.a.O., S. 86 f. Rz. 244; HUNKELER/MOSIMANN, a.a.O., S. 442 und 446 f.). In diesem Zusammenhang ignoriere das Bundesgericht auch die staatsvertraglichen Verpflichtungen der Schweiz. So bestimme Art. 16 Abs. 2 der Cybercrime Convention, dass jede Vertragspartei die erforderlichen

gesetzgeberischen und anderen Massnahmen treffe, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten anordnen oder in ähnlicher Weise bewirken könnten, insbesondere wenn Gründe zu der Annahme bestünden, dass bei diesen Daten eine besondere Gefahr des Verlusts oder der Veränderung bestehe (GRAF, a.a.O., S. 87 Rz. 246). Manche Autoren weisen schliesslich darauf hin, dass das vom Bundesgericht beschriebene Vorgehen die bereits heute schon sehr lange dauernden Entsiegelungsverfahren erheblich verzögere, womit dem Beschleunigungsgebot kaum mehr Rechnung getragen werden könne (HUNKELER/MOSIMANN, a.a.O., S. 444). BGE 151 IV 322 S. 327

**E. 3.4**

Die Beschwerdeführerin ist der Auffassung, indem die Vorinstanz BGE 148 IV 221 in dieser Absolutheit auf den vorliegenden Fall übertrage, verletze sie Bundesrecht. Sie weist dabei mit Recht darauf hin, dass sich der vorliegende Sachverhalt in wesentlichen Punkten vom besagten Urteil unterscheidet.

**E. 3.4.1**

Die Beschwerdeführerin hat die Bank E. als Inhaberin der streitigen Bankunterlagen gestützt auf Art. 46 Abs. 1 lit. a und Art. 47 Abs. 1 VStrR (SR 313.0) zur freiwilligen Herausgabe aufgefordert. Die Übermittlung dieser Daten - sei es per gewöhnlicher E-Mail, wie die Vorinstanz mutmasst, oder sei es über die Plattform PrivaSphere, wie die Beschwerdeführerin behauptet - stellt dabei den Sicherstellungsvorgang dar. Zu diesem Sicherstellungsvorgang gehört auch, die fraglichen Daten im Anschluss an die Übermittlung herunterzuladen und abzuspeichern. Es verhält sich somit ähnlich, wie wenn bei einer Hausdurchsuchung elektronische Geräte vorläufig sichergestellt und somit physisch behändigt und in die Räumlichkeiten der Strafverfolgungsbehörden verbracht werden. Dabei hindert ein bereits bestehender Siegelungsantrag den (physischen) Übergang des Gewahrsams an den versiegelten Aufzeichnungen und Gegenständen an die Untersuchungsbehörde nicht (GRAF, a.a.O., S. 77 Rz. 209). Weiter leuchtet ein, dass die Beschwerdeführerin die Speicherung auf einem externen Datenträger vorgenommen hat, um diesen, und damit die Daten, anschliessend versiegeln zu können (zur Siegelung von Kopien vgl. THORMANN/BRECHBÜHL, in: Basler Kommentar, Schweizerische Strafprozessordnung, 3. Aufl. 2023, N. 32 zu Art. 248 StPO ). In der Tat scheint fraglich, wie Daten, die anderweitig, beispielsweise auf einem lokalen Server oder in einer Cloud gespeichert wurden, gesiegelt und anschliessend dem Zwangsmassnahmengericht zwecks Entsiegelung übermittelt werden könnten. Zwar wäre als Alternative auch denkbar, die edierten Unterlagen auszudrucken und anschliessend den Ausdruck in Papierform zu versiegeln (OTHMAR STRASSER, Elektronische Aktendedition von Banken an Strafuntersuchungsbehörden, in: Recht im digitalen Zeitalter, Gschwend und andere [Hrsg.], 2015, S. 681). Dieses Vorgehen bietet im Hinblick auf den Zweck der Siegelung jedoch keinen höheren Schutz als das von der Beschwerdeführerin gewählte Vorgehen. Ebenfalls wenig zielführend ist die von STRASSER vorgeschlagene Möglichkeit, die elektronisch überlieferten Akten bei einer Revisionsgesellschaft bis BGE 151 IV 322 S. 328 zur rechtsgültigen Aufhebung der Siegelung unter Verschluss zu halten (STRASSER, a.a.O., S. 681 f.). Denn das Anbringen des Siegels bleibt gemäss Art. 248 Abs. 1 StPO grundsätzlich Sache der Untersuchungsbehörde und setzt voraus, dass sich die betroffenen Daten in siegelungsfähiger Form befinden. Die Zwischenschaltung einer Revisionsstelle verlangt somit ebenfalls, dass die Untersuchungsbehörde die Daten zunächst von der

Übermittlungsplattform herunterlädt bzw. die als Anhang einer gewöhnlichen E-Mail übermittelten Daten (was in der Praxis selten vorkommen dürfte) auf einem Datenträger speichert (bzw. ausdruckt). Diese Variante gewährt deshalb ebenfalls keinen verbesserten Schutz im Vergleich zu jener, bei der die Daten nach dem Download auf einem externen Datenträger gespeichert, dieser umgehend versiegelt und dem Zwangsmassnahmengericht übermittelt wird. Grundsätzlich stünde es der Staatsanwaltschaft jedoch frei, eine Revisionsstelle beizuziehen. Es ist im Ergebnis somit nicht zu beanstanden, dass die Beschwerdeführerin die ihr übermittelten Daten auf einem Datenstick abgespeichert hat, um dem Siegelungsantrag, von dem sie in diesem Zeitpunkt bereits Kenntnis hatte, zu entsprechen. Letztlich geht es vorliegend, wie eingangs erwähnt, nicht um ein Kopieren bereits sichergestellter Daten, sondern das Kopieren bzw. Abspeichern war Teil der Sicherstellung.

**E. 3.4.2**

Die theoretische Möglichkeit einer vorzeitigen Kenntnisnahme gewisser Daten lässt sich dabei genauso wenig vermeiden, wie dies bei der Sicherstellung physischer Unterlagen wie Ordnern, Notizbüchern etc. anlässlich einer Hausdurchsuchung der Fall ist. Dies schadet aber insbesondere 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; Urteil 1B_656/2021 vom 4. August 2022 E. 6.2). Die Befugnis zur Grobtriage gilt auch für elektronische Datenträger (THORMANN/BRECHBÜHL, a.a.O., N. 13a zu Art. 247 StPO ; ANDREAS J. KELLER, in: Kommentar zur Schweizerischen Strafprozessordnung StPO, 3. Aufl. 2020, N. 3a zu Art. 247 StPO ). In vergleichbarem Sinne weist die Beschwerdeführerin zutreffend darauf hin, dass sie überprüfen können muss, ob die Adressatin der Editionsverfügung ihren Editionspflichten vollständig nachgekommen BGE 151 IV 322 S. 329 ist. Dies scheint in analoger Anwendung der zitierten Rechtsprechung grundsätzlich zulässig, sofern keine verfrühte inhaltliche Durchsuchung und Auswertung vorgenommen wird. Insoweit ist die vorliegende Konstellation gleich zu beurteilen, wie wenn die edierten Unterlagen von der Bank physisch per Post übermittelt worden wären. Auch in diesem Fall wird die edierende Behörde die Unterlagen kurz auf ihre Vollständigkeit hin überprüfen, bevor sie die betreffenden Umschläge oder Behältnisse versiegelt. Indem die Vorinstanz der Beschwerdeführerin einen schweren Verfahrensmangel unterstellt, der zur Abweisung des Entsiegelungsgesuchs führt, verletzt sie nach dem Gesagten Bundesrecht.

**E. 3.4.3**

Problematisch ist vorliegend einzig, dass die Beschwerdeführerin nach dem Download und Abspeichern weiterhin auf die ursprünglichen Daten zugreifen konnte - dies so oder anders mindestens während den 30 Tagen, in denen nach ihren Angaben der Link für den Zugriff auf die Daten bei PrivaSphere gültig war. Sie wird deshalb aufgefordert, bei Vorliegen eines Siegelungsbegehrens die edierten Originaldaten nach erfolgter Sicherung und Siegelung umgehend zu löschen, damit ein unbefugter Zugriff verhindert werden kann. Dies hat sie, sofern nicht bereits geschehen, auch im vorliegenden Verfahren unverzüglich zu tun.

**E. 3.5**

Es liegt nicht in der Kompetenz des Bundesgerichts, als erste Instanz über das Vorliegen schutzwürdiger Geheimnisinteressen auf Seiten der Beschwerdegegnerin oder sonstige materielle Entsiegelungshindernisse zu entscheiden (vgl. Art. 80 Abs. 1 BGG ). Entsprechend ist die Sache zur nochmaligen Beurteilung an die Vorinstanz zurückzuweisen.