

# **BGE 148 IV 221**

Bundesgericht (BGE), 2022-02-28, DE

Quelle: [https://mcp.opencaselaw.ch/entscheid/bge\\_148 IV 221](https://mcp.opencaselaw.ch/entscheid/bge_148_IV_221)

FR: ATF 148 IV 221

IT: DTF 148 IV 221

## **Regeste**

Regeste Art. 14 Abs. 3 lit. g UNO-Pakt II; Art. 3, 25 Abs. 1 sowie Art. 50 VStrR; Art. 264 Abs. 1 und 2 StPO; Siegelung und Entsigelung sichergestellter elektronischer Geräte im Verwaltungsstrafverfahren. Zweck der Siegelung ist, jegliche Gelegenheit für die Untersuchungsbehörde zur Kenntnisnahme der sichergestellten Daten auszuschliessen, bevor ein Gericht über die Zulässigkeit des Zugangs zu diesen Daten entscheidet. Im Entsigelungsverfahren hat daher nicht die Untersuchungsbehörde, sondern, allenfalls unter Beizug einer sachverständigen Person, das Zwangsmassnahmengericht zu prüfen, ob Entsigelungshindernisse einer Durchsuchung entgegenstehen. Erweist sich eine Kopie der Daten zum Schutz vor Verlust oder aus einem anderen Grund als angebracht, darf mit der Siegelung nicht zugewartet werden, sondern ist dies nach sofortiger Siegelung der Geräte ebenfalls vom Zwangsmassnahmengericht, allenfalls auf Antrag der Untersuchungsbehörde hin, anzuordnen. Die Untersuchungsbehörde darf in keiner Weise in die Entsperrung der Geräte und Spiegelung der Daten als Realakte einbezogen werden (E. 2 und 3). Die Vornahme der Entsperrung der Geräte und der Datenspiegelung vor der Siegelung durch eine von der Untersuchungsbehörde beauftragte Behörde stellt einen erheblichen Verfahrensmangel dar, der zur Unverwertbarkeit der Daten und deren Vernichtung sowie zur Rückgabe der Geräte an die daran berechnigte Person führt (E. 4).

## **Erwägungen**

### **E. 2.1**

Gemäss Art. 50 VStrR (SR 313.0) sind im Verwaltungsstrafverfahren Papiere mit grösster Schonung der Privatheimnisse zu durchsuchen (Abs. 1), wobei Amts- und Berufsheimnisse zu wahren sind (Abs. 2). Erhebt der Inhaber der Papiere Einsprache gegen die Durchsuchung, so werden die Papiere versiegelt und verwahrt, und es entscheidet die Beschwerdekammer des Bundesstrafgerichts über die Zulässigkeit der Durchsuchung (Abs. 3 i.V.m. Art. 25 Abs. 1 VStrR ). Die Bestimmung wird heute auch auf elektronische Datenträger angewandt (vgl. die Urteile des Bundesgerichts 1B\_210/2017 vom 23. Oktober 2017 E. 3.3 und 1B\_487/2018 vom 6. Februar 2019 E. 2.2). Nach der bundesgerichtlichen Rechtsprechung sind in Analogie zum ordentlichen Strafprozess auch im Verwaltungsstrafverfahren Aufzeichnungen und Gegenstände, die nach Angaben der BGE 148 IV 221 S. 225 Inhaberin oder des Inhabers wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen nicht durchsucht oder beschlagnahmt werden dürfen, zu versiegeln und dürfen von den Strafbehörden weder eingesehen noch verwendet werden (vgl. Art. 50 VStrR i.V.m. Art. 248 Abs. 1 sowie Art. 264 Abs. 1 und 2 StPO ). Macht eine berechnigte Person geltend, eine Beschlagnahme (oder Edition) von Gegenständen und Vermögenswerten sei wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen nicht zulässig, so gehen die

Strafbehörden nach den Vorschriften über die Siegelung vor (Art. 264 Abs. 3 und Art. 265 Abs. 2 lit. a-b StPO ; vgl. etwa die Urteile des Bundesgerichts 1B\_210/2017 vom 23. Oktober 2017 E. 3.3 und 1B\_487/2018 vom 6. Februar 2019 E. 2.2).

### **E. 2.2**

Gemäss dem in Art. 14 Abs. 3 lit. g UNO-Pakt II (SR 0.103.2) verankerten und aus Art. 32 BV sowie Art. 6 Ziff. 1 EMRK abgeleiteten Grundsatz "nemo tenetur se ipsum accusare" ist im Strafverfahren niemand gehalten, zu seiner Belastung beizutragen, und ist der Beschuldigte aufgrund seines Aussageverweigerungsrechts berechtigt zu schweigen, ohne dass ihm daraus Nachteile erwachsen dürfen (vgl. Art. 113 Abs. 1 und Art. 158 Abs. 1 lit. b StPO ; BGE 142 IV 207 E. 8.3 mit Hinweisen). Gestützt darauf kann er auch nicht verpflichtet werden, Gerätesperrcodes offenzulegen (Urteil des Bundesgerichts 1B\_376/2019 vom 12. September 2019 E. 2.3).

### **E. 2.3**

Nach der gefestigten Rechtsprechung des Bundesgerichts hat im Entsiegelungsverfahren nicht die Untersuchungsbehörde, sondern, allenfalls unter Beizug einer sachverständigen Person, das Zwangsmassnahmengericht zu prüfen, ob schutzwürdige Geheimnisinteressen oder andere gesetzliche Entsiegelungshindernisse einer Durchsuchung entgegenstehen ( Art. 248 Abs. 2-4 StPO ; vgl. BGE 144 IV 74 E. 2.2; BGE 142 IV 372 E. 3; BGE 141 IV 77 E. 4.1). Dies dient namentlich der Verhinderung von Zufallsfunden sowie der Wahrung der unter verfassungsrechtlichem Schutz stehenden Privat- und Geheimsphäre gemäss Art. 13 BV (vgl. die Urteile des Bundesgerichts 1B\_274/2019 vom 12. August 2019 E. 3.3 und 1B\_376/2019 vom 12. September 2019 E. 2.4).

### **E. 2.4**

In teilweiser Abweichung von der bundesgerichtlichen Rechtsprechung verfolgt das Bundesstrafgericht eine eigene Praxis, die es offenbar ursprünglich im Zusammenhang mit Amts- und Rechtshilfeverfahren in Anwendung von Art. 50 Abs. 3 VStrR in Verbindung mit Art. 12 des Bundesgesetzes vom 20. März 1981 über BGE 148 IV 221 S. 226 internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, IRSG; SR 351.1) entwickelt und anscheinend auch verschiedentlich mit der Zollverwaltung abgesprochen hat. Danach tritt es auf Entsiegelungsgesuche bei nicht gespiegelten Datenträgern grundsätzlich nicht ein, lässt dafür die Möglichkeit offen, ein neues Entsiegelungsgesuch zusammen mit der Übermittlung einer Datenkopie einzureichen. Dabei greift im Wesentlichen folgender Ablauf: Nach Sicherstellung der elektronischen Geräte wird eine forensische Sicherungskopie der sich darauf befindenden Daten durch die Rechtshilfebehörde bzw. durch eine beauftragte Fachstelle erstellt, woraufhin die Geräte an den Gesuchsgegner zurückgegeben und die gesiegelte forensische Datenkopie dem Bundesstrafgericht übermittelt wird (vgl. TPF 2020 96 und Urteil des Bundesstrafgerichts RR.2019.220 vom 25. Mai 2020). Diese Praxis wendet das Bundesstrafgericht inzwischen wie hier auch in anderen als Amts- oder Rechtshilfefällen an, wobei anstelle der Rechtshilfe- die Untersuchungsbehörde tritt. Es hielt daran selbst dann noch fest, nachdem das Bundesgericht in den Urteilen 1B\_274/2019 vom 12. August 2019 und 1B\_376/2019 vom 12. September 2019 seine bereits publizierte Praxis (vgl. BGE 144 IV 74 E. 2.2; BGE 142 IV 372 E. 3; BGE 141 IV 77 E. 4.1; dazu vorne E. 2.3) bestätigt und konkretisiert hatte, dass in Fällen, in denen der Beschuldigte den Zugangscode gegenüber der Untersuchungsbehörde nicht freigibt, die Entsperrung im Entsiegelungsverfahren vor dem

Zwangsmassnahmengericht zu erfolgen habe (Beschluss des Bundesstrafgerichts BE.2020.3 vom 27. Juli 2020). Das Bundesstrafgericht begründet dies im vorliegenden Fall im Wesentlichen damit, nach Art. 20 Abs. 1 in Verbindung mit Art. 37 Abs. 1 VStrR sei es Sache der Verwaltungs- als Untersuchungsbehörde, die Daten zwecks Beweissicherung zu spiegeln. Dieser Vorgang bewahre die Untersuchungsbehörde vor dem Vorwurf der Datenmanipulation, diene der Sicherung der Daten und schütze vor einem Datenverlust. Weder die Entsperrung der elektronischen Geräte noch die Datenspiegelung brächten eine Durchsuchung der Datenträger mit sich. Entgegen der Befürchtungen des Beschwerdeführers lasse sich kontrollieren, ob der Inhalt der forensischen Datenkopie demjenigen des gespiegelten Datenträgers entspreche. Schliesslich wäre eine unerlaubte Sichtung des Inhalts durch die Untersuchungsbehörde vor der Entsigelung strafbar.

### **E. 2.5**

Der Beschwerdeführer und die Zollverwaltung erachten übereinstimmend eine Überprüfung des Vorgehens gemäss der Praxis BGE 148 IV 221 S. 227 des Bundesstrafgerichts auf Vereinbarkeit mit der Rechtsprechung des Bundesgerichts als geboten. Zu prüfen ist hier freilich nur, ob der auf der Praxis der Vorinstanz beruhende angefochtene Entscheid mit der bundesgerichtlichen Rechtsprechung zum Entsigelungsverfahren bei Strafprozessen ausserhalb der Amts- und Rechtshilfe im Einklang steht. Zwar mag es zutreffen, dass sich unter Umständen eine Sicherung der Daten aufdrängen kann und dass sich die Deckungsgleichheit des Inhalts von Kopie und Original technisch überprüfen lässt. Dass eine Datenspiegelung ganz ohne Einsicht in die Daten abläuft und dass die Mitarbeitenden der Untersuchungsbehörde unter Strafandrohung stünden, falls sie vom Inhalt verfrüht Kenntnis nähmen, ist aber nicht zwingend. Es erscheint nicht unmöglich, dass es ohne Erfüllung eines Straftatbestands zu einer solchen Kenntnisnahme kommen könnte, die für den Beschuldigten und die Strafgerichte auch gar nicht zwangsläufig zu erkennen sein muss, der Untersuchungsbehörde aber doch einen unerlaubten Vorteil bei der Strafverfolgung verschaffen könnte. Zumindest lässt sich die Möglichkeit einer solchen verfrühten Offenlegung der Daten, bevor eine allenfalls erforderliche Triage vorgenommen wird, nicht von vorneherein ausschliessen. Zweck der Siegelung ist es aber mit Blick auf die entsprechenden Grund- und Verfahrensrechte des Beschuldigten, jegliche Gelegenheit für die Untersuchungsbehörde zur Kenntnisnahme der sichergestellten Daten auszuschliessen, bevor ein Gericht über die Zulässigkeit des Zugangs zu diesen Daten entscheidet. Die Praxis des Bundesstrafgerichts vermag das nicht zu gewährleisten.

### **E. 2.6**

Das bedeutet allerdings nicht, dass eine Spiegelung der Daten an sich unzulässig wäre. Sie darf jedoch nicht durch die Untersuchungsbehörde veranlasst bzw. einer von ihr beauftragten und damit auch weisungsgebundenen Person oder Behörde übertragen werden. Geht ein Siegelungsgesuch ein, sind vielmehr die betreffenden Unterlagen bzw. wie hier elektronischen Geräte unverzüglich zu siegeln. Erweist sich eine Kopie der Daten zum Schutz vor Verlust oder aus einem sonstigen Grund für das weitere Verfahren als angebracht, hat die Untersuchungsbehörde nach der Siegelung der Datenträger beim Zwangsmassnahmengericht bzw. hier dem Bundesstrafgericht ein entsprechendes Spiegelungsgesuch zu stellen. Dieses kann auch zusammen mit dem Entsigelungsantrag ergehen. Das Gericht könnte eine Kopierung der Dateien auch von Amtes wegen anordnen, wenn es dies als notwendig oder zur Vermeidung des möglichen Vorwurfs BGE 148 IV 221 S. 228 der Datenmanipulation als erforderlich beurteilt. Es kann damit eine spezialisierte

Behörde oder private Fachpersonen beauftragen, wobei gewährleistet bleiben muss, dass die Untersuchungsbehörde in keiner Weise in die Entsperrung und Spiegelung als Realakte einbezogen wird und bis zum Entsiegelungsentscheid keine Möglichkeit des Zugangs zu den auf den sichergestellten Geräten liegenden Dateien erhält und auch über keine Weisungsbefugnisse gegenüber der beauftragten Organisation oder Person verfügt. Dieser Auftrag könnte dann auch dem fedpol übertragen werden, wenn dieses nicht selbst Untersuchungsbehörde ist. Nur so lassen sich die Rechte des Beschuldigten vollumfänglich gewährleisten.

### **E. 2.7**

Wie es sich im Amts- und Rechtshilfeverfahren unter Abwägung der entsprechenden speziellen Umstände verhält, braucht hier nicht abschliessend entschieden zu werden. Es dürfte sich allerdings ein zumindest analoges Verfahren rechtfertigen, sollte das genau gleiche Vorgehen nicht möglich sein.

### **E. 3.1**

Im vorliegenden Fall wurden die drei elektronischen Geräte des Beschwerdeführers bei der Zollkontrolle vom 10. September 2020 durch die Zollverwaltung sichergestellt. Daraus, dass er sich weigerte, die Zugangscodes offenzulegen, darf ihm kein Nachteil erwachsen. Am 14. September 2020 stellte er über seinen Rechtsanwalt zunächst per Mail und in der Folge per schriftliche Eingabe, die am 17. September 2020 bei der Zollverwaltung einging, das Siegelungsgesuch. Am 29. September 2020 fand eine Besprechung über das weitere Vorgehen statt, an welcher der Beschwerdeführer seine Einwände gegen die Durchsichtung seiner Dateien bekräftigte. Es kann hier offenbleiben, ob der Beschwerdeführer vorgängig hinreichend über den Gegenstand der Besprechung informiert worden war, was er bestreitet, wogegen die Zollverwaltung jedoch einwendet, das werde durch eine aktenkundige Telefonnotiz vom 23. September 2020 ausreichend belegt. Jedenfalls übermittelte die Zollverwaltung in der Folge am 1. Oktober 2020 die Datenträger dem fedpol zwecks Entsperrung, Spiegelung und Siegelung. Am 8. Oktober 2020 stellte die Zollverwaltung das Entsiegelungsgesuch beim Bundesstrafgericht. Die Siegelung durch das fedpol fand am 5. November 2020 statt und tags darauf stellte dieses dem Bundesstrafgericht die gesiegelten Datenkopien zu.

### **E. 3.2**

Aus diesem Ablauf ergibt sich, dass sich die fraglichen drei IT-Geräte nach Eingang des Siegelungsgesuchs am 14. bzw. BGE 148 IV 221 S. 229 17. September bis zum 5. November 2020 ungesiegelt in der Hand der Zollverwaltung bzw. des von dieser mit der Entsperrung, Spiegelung und Siegelung beauftragten und dementsprechend weisungsgebundenen fedpol befanden. Dass möglicherweise noch eine Besprechung der Modalitäten des weiteren Vorgehens anberaumt war, erlaubte der Untersuchungsbehörde nicht, mit der Siegelung zuzuwarten. Unabhängig davon fand diese auch nicht unmittelbar nach dem auf den 29. September 2020 anberaumten Besprechungstermin statt. Auch wenn es glaubhaft sein mag, dass die Untersuchungsbehörde vor der Siegelung am 5. November 2020 nicht auf die Dateien zugegriffen hat, so lässt sich das nicht eindeutig überprüfen. Bei entsprechenden technischen Fertigkeiten erscheint die Möglichkeit eines Zugangs bei der Zollverwaltung genauso wenig ausgeschlossen wie ein solcher nach Entsperrung, aber vor Siegelung beim fedpol. Aufgrund des Auftragsverhältnisses bestand zwangsläufig eine enge Zusammenarbeit zwischen den beiden Bundesbehörden. Es ist weder dem Bundesstraf-

noch dem Bundesgericht möglich, zu kontrollieren, wer wann genau wie Zugang zu den Datenträgern hatte, und erst recht trifft das auf den Beschwerdeführer zu. Eine solche Unsicherheit verträgt ein rechtsstaatliches Verfahren nicht. Der Beschwerdeführer vermag zwar nicht zu belegen, dass die Untersuchungsbehörde tatsächlich vorzeitig Kenntnis von den Daten seiner IT-Geräte erhalten hat. Ein solcher Beweis von Tatsachen auf Seiten der Behörden wäre aber auch kaum zu erbringen, weshalb ihm die entsprechende Beweislast nicht auferlegt werden darf. Es muss daher genügen, dass ab dem Zeitpunkt des Siegelungsgesuchs die Möglichkeit eines verfrühten Zugangs der Zollverwaltung als Untersuchungsbehörde zu den Dateien bestanden hat, was aufgrund der aktenkundigen Umstände des behördlichen Vorgehens im vorliegenden Fall ausreichend erhärtet ist.

### **E. 3.3**

Der sachgerechte Ablauf würde überdies nahelegen, dass die Frist für das gemäss Art. 248 Abs. 2 StPO innert 20 Tagen zu stellende Entsiegelungsgesuch ab dem Zeitpunkt der Siegelung zu laufen beginnt und dieses nicht wie hier bereits vorher eingereicht wird. Würde für den Beginn der Frist allenfalls alternativ auf den Zeitpunkt des Antrags des Beschwerdeführers um Siegelung abgestellt, wäre die Frist im Übrigen bereits abgelaufen, bevor das Entsiegelungsgesuch gestellt wurde. Würde sie ab dem Maileingang vom 14. September 2020 berechnet, hätte sie am 5. Oktober 2020 geendet; würde vom Eingang des schriftlichen Siegelungsgesuchs bei der BGE 148 IV 221 S. 230 Zollverwaltung am 17. September 2020 ausgegangen, wäre der Endtermin der 7. Oktober 2020 gewesen. Die Zollverwaltung stellte das Entsiegelungsgesuch jedoch erst am 8. Oktober 2020.

### **E. 3.4**

Diese Zusammenhänge unterstreichen, dass der vom Bundesstrafgericht vorgegebene und im vorliegenden Fall von der Zollverwaltung verfolgte Ablauf nicht der gesetzlichen Regelung entspricht. Die Datenträger hätten vielmehr unmittelbar gesiegelt und dem Bundesstrafgericht übergeben werden müssen, das in der Folge die Entsperrung und bei Bedarf Spiegelung und Neusiegelung bis zur Entscheid über die Entsiegelung durch eine unabhängige Fachperson, Organisation oder Behörde hätte anordnen können. Das hätte durchaus auch das fedpol sein können, da dieses im vorliegenden Fall nicht Untersuchungsbehörde ist und bei einer Beauftragung durch das Bundesstrafgericht im Unterschied zur hier zu beurteilenden Konstellation einzig mit diesem zusammengearbeitet und dessen Weisungen unterstanden hätte und von der Zollverwaltung völlig unabhängig geblieben wäre. Schliesslich war die Zollverwaltung zwar bemüht, sich an die prozessualen Vorgaben des Bundesstrafgerichts zur Behandlung eines Siegelungsgesuchs bei elektronischen Datenträgern zu halten. Da sich dessen Praxis aber als unzulässig erweist, ist das behördliche Vorgehen insgesamt bundesrechtswidrig.

### **E. 4.1**

Damit stellt sich die Frage, welche Auswirkungen die Rechtswidrigkeit des Vorgehens der Vorinstanzen im Zusammenhang mit der Siegelung der Datenträger des Beschwerdeführers auf das weitere Verfahren zeitigt. Dabei ist grundsätzlich zwischen der Fortsetzung des Entsiegelungsverfahrens und der Verwertbarkeit von Beweismitteln zu unterscheiden. Im Strafprozess ist die Frage der Verwertbarkeit von Beweismitteln grundsätzlich dem Sachgericht bzw. der den Endentscheid fällenden Strafbehörde zu unterbreiten. Lediglich ausnahmsweise kann bereits im Untersuchungsverfahren ein abschliessender Entscheid über die Frage erreicht werden. Insbesondere darf das Zwangsmassnahmengericht im

Entsiegelungsprozess im Vorverfahren ( Art. 248 Abs. 3 lit. a StPO ) nur dann abschliessend über Verwertungsverbote gemäss Art. 140 und 141 StPO entscheiden, wenn die Unverwertbarkeit offensichtlich ist; andernfalls können solche Verbote in diesem Prozess nicht durchgesetzt werden ( BGE 143 IV 387 E. 4.4 mit Hinweisen; Urteil des Bundesgerichts 1B\_355/2021 vom 26. August 2021 E. 2.4). BGE 148 IV 221 S. 231

#### **E. 4.2**

Wie dargelegt (vgl. vorne E. 3.4), hat sich die Zollverwaltung an die Praxis des Bundesstrafgerichts bzw. an dessen Vorgaben zum Vorgehen bei Vorliegen eines Siegelungsgesuchs bei elektronischen Datenträgern gehalten. Im vorliegenden Fall geht es jedoch um einen erheblichen Verfahrensfehler. Eine Rückweisung an die Vorinstanzen zur Wiederholung des Siegelungsverfahrens gemäss den rechtsstaatlichen Anforderungen ist ausgeschlossen, da sich der Verfahrensmangel nicht mehr korrigieren lässt. Im Ergebnis wiegt die Rechtswidrigkeit des behördlichen Vorgehens im vorliegenden Verfahren derart schwer, dass nicht ersichtlich ist, wie die Daten auf den elektronischen Geräten des Beschwerdeführers noch verwertbar sein könnten.

#### **E. 4.3**

Damit kann dem Entsiegelungsgesuch der früheren Zollverwaltung bzw. des heutigen Bundesamts für Zoll und Grenzsicherheit nicht stattgegeben werden. Der angefochtene Entscheid ist entsprechend zu korrigieren. Dem Beschwerdeführer sind seine sichergestellten drei elektronischen Geräte zurückzugeben und die durch Spiegelung erstellten Datenkopien sind zu vernichten. Das Verwaltungsstrafverfahren wird ohne diese Dateien fortzuführen sein.

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