Urteilskopf

148 IV 221

21. Auszug aus dem Urteil der I. öffentlich-rechtlichen Abteilung i.S. A. gegen Bundesamt für Zoll und Grenzsicherheit (BAZG) (Beschwerde in Strafsachen) 1B_432/2021 vom 28. Februar 2022

Regeste (de):
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 Entsiegelung 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 Entsiegelungsverfahren hat daher nicht die Untersuchungsbehörde, sondern, allenfalls unter Beizug einer sachverständigen Person, das Zwangsmassnahmengericht zu prüfen, ob Entsiegelungshindernisse 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 berechtigte Person führt (E. 4).

Regeste (fr):
Art. 14 par. 3 let. g Pacte ONU II; art. 3, 25 al. 1 et art. 50 DPA; art. 264 al. 1 et 2 CPP; mise sous scellés d'appareils électroniques saisis et levée de cette mesure en procédure pénale administrative.

Le but des scellés est de soustraire les données saisies de la connaissance des autorités d'enquête tant qu'un tribunal ne s'est pas prononcé sur la licéité de l'accès à ces données. Dans le cadre de la procédure de levée des scellés, il n'appartient ainsi pas aux autorités d'enquête, mais au Tribunal des mesures de contrainte, tout au plus avec l'assistance d'un expert, de vérifier s'il existe des motifs s'opposant à la levée des scellés et à la perquisition. Si une copie des données s'avère nécessaire afin de se protéger contre un risque de perte ou pour une autre raison, la mise sous scellés des objets saisis ne saurait cependant attendre; après l'apposition des scelés - qui doit intervenir immédiatement -, la copie des données doit également être ordonnée par le Tribunal des mesures de contrainte, le cas échéant sur demande des autorités d'enquête. Ces dernières ne doivent en aucun cas être impliquées dans les actes matériels permettant de déverrouiller les objets saisis et d'obtenir une copie-miroir des données (consid. 2 et 3).

La participation d'une autorité mandatée par les autorités d'enquête à la procédure de déverrouillage des appareils et de copie des données avant la mise sous scellés constitue un vice de procédure important, lequel conduit à l'inexploitabilité des données et à leur destruction, ainsi qu'à la restitution des appareils à l'ayant droit (consid. 4).

Regesto (it):
Art. 14 n. 3 lett. g Patto ONU II; art. 3, 25 cpv. 1 nonché art. 50 DPA; art. 264 cpv. 1 e 2 CPP; apposizione di sigilli e dissigillamento di apparecchi elettronici sequestrati nell'ambito di una procedura penale amministrativa.

Scopo del sigillamento è di escludere qualsiasi possibilità per l'autorità inquirente di prendere conoscenza dei dati sequestrati prima che un tribunale decida sull'ammissibilità dell'accesso agli stessi. Nella procedura di dissigillamento non spetta quindi all'autorità inquirente, ma semmai con l'ausilio di una persona esperta, al Giudice dei provvedimenti coercitivi esaminare se sussistano impedimenti al dissigillamento, che si oppongano alla perquisizione. Qualora appaia opportuno allestire una copia dei dati per tutelarne la perdita o per un altro motivo, non si può ritardare l'apposizione dei sigilli sugli apparecchi; la copia dei dati dev'essere ordinata immediatamente, pure da parte dal Giudice dei provvedimenti coercitivi, dopo l'apposizione dei sigilli, semmai a richiesta dell'autorità inquirente. Quest'ultima non può essere coinvolta in alcun modo negli atti reali dello sblocco degli apparecchi e del mirroring dei dati (consid. 2 e 3).

L'esecuzione dello sblocco degli apparecchi e del mirroring prima dell'apposizione dei sigilli da parte di un'autorità incaricata da quella inquirente costituisce un vizio procedurale considerevole, che comporta l'inutilizzabilità dei dati e la loro distruzione, come pure la restituzione degli apparecchi all'avente diritto (consid. 4).

Sachverhalt ab Seite 222

A. Im Anschluss an eine Amtshilfemeldung der portugiesischen Zollbehörden führte das (damalige) Grenzwachtkorps (heute: Bundesamt für Zoll und Grenzsicherheit [BAZG]) am 10. September 2020 am Flughafen Zürich eine Zollkontrolle mit körperlicher Durchsuchung von A. durch. Dabei wurden zwölf Armbanduhren der Marke Rolex mit Zugehör sowie verschiedene Kaufbelege und Rechnungen sichergestellt, die A. bei seiner Einreise nicht zur Einfuhr in die Schweiz angemeldet hatte. Zehn der zwölf Armbanduhren mit den entsprechenden Kaufbelegen und Rechnungen trug A. bei der Einreise versteckt in einem um den Bauch gebundenen Schmuggelgurt auf sich.

Noch am gleichen Tag eröffnete die (damalige) Eidgenössische Zollverwaltung (heute ebenfalls: Bundesamt für Zoll und Grenzsicherheit [BAZG]) gegen A. ein Strafverfahren wegen des Verdachts auf Widerhandlungen gegen das Zollgesetz sowie das Mehrwertsteuergesetz. Ebenfalls am 10. September 2020 stellte die Zollverwaltung unter anderem zwei Mobiltelefone (Samsung Galaxy A40 und Samsung Galaxy S10+) sowie ein Tablet (Samsung Tab S6) von A. vorläufig sicher. Dieser verlangte zunächst keine Siegelung der IT-Geräte, sondern erklärte lediglich, die Codes nicht bekannt zu geben. Am 14. September 2020 beantragte der inzwischen beigezogene Rechtsvertreter von A. die Siegelung der sichergestellten IT-Geräte. Am 29. September 2020 erläuterte die Zollverwaltung A. und seinem Rechtsanwalt ihr Vorgehen, wenn der Zugangscode zu sichergestellten IT-Geräten nicht bekannt ist. A. bekräftigte dabei sein Siegelungsgesuch mit der Begründung, die Datenträger enthielten vertrauliche Anwaltskorrespondenz, höchstpersönliche Informationen sowie Geschäftsgeheimnisse. Am 1. Oktober 2020 übermittelte die Zollverwaltung die IT-Geräte von A. dem Bundesamt für Polizei (fedpol), Bundeskriminalpolizei (Abteilung IT Forensik und Cybercrime IFC), mit dem Auftrag "Unlock mit Bruteforce und Extraction".

B. Mit Gesuch vom 8. Oktober 2020 stellte die Zollverwaltung der Beschwerdekammer des Bundesstrafgerichts den im Wesentlichen folgenden Antrag auf Entsiegelung der drei IT-Geräte von A.: "Die Gesuchstellerin sei zu ermächtigen, die mit Sicherstellungsbeschluss vom 10. September 2020 sichergestellten und durch das

Bundesamt für Polizei (fedpol) ... zu entsperrenden und sodann zu versiegelnden forensischen Kopien der Daten der Mobiltelefonie sowie des Tablet Computers des Gesuchgegners zu entsiegeln und zu durchsuchen." Am 5. November 2020 versiegelte das fedpol die drei Datenträger nach deren Entsperrung und Spiegelung ihres Inhalts. A. und sein Rechtsanwalt hatten auf eine Teilnahme an der Siegelung verzichtet. Tags darauf, am 6. November 2020, stellte das fedpol die versiegelten Datenträger der Beschwerdekammer des Bundesstrafgerichts zu. Mit Beschluss vom 14. Juli 2021 hiess die Beschwerdekammer des Bundesstrafgerichts das Entsiegelungsgesuch gut und ermächtigte die Zollverwaltung, alle sichergestellten Daten zu durchsuchen.

C. A. führt mit Eingabe vom 16. August 2021 Beschwerde in Strafsachen beim Bundesgericht und stellt den Hauptantrag, den Beschluss der Beschwerdekammer des Bundesstrafgerichts aufzuheben und die Sache zu neuer Beurteilung an diese zurückzuweisen. (...) Die Zollverwaltung schliesst in ihrer Stellungnahme vom 9. September 2021 auf Abweisung der Beschwerde, soweit darauf einzutreten sei, und reichte dazu eine Aktennotiz vom 5. November 2020 nach. Das Bundesstrafgericht erläuterte in seiner Vernehmlassung vom 26. August 2021 seine Rechtsprechung zur Siegelung von Datenträgern und hält sinngemäss ohne formelles Rechtsbegehren an seinem Beschluss fest. In seiner Replik vom 1. Oktober 2021 bekräftigt A. im Wesentlichen seinen Standpunkt und konkretisiert sein Rechtsbegehren dahingehend, dass der vom fedpol als Spiegelung angefertigte Datenträger zu vernichten und die sichergestellten IT-Geräte zurückzugeben seien. (...) Das Bundesamt für Zoll und Grenzsicherheit (als Nachfolgebehörde der früheren Zollverwaltung) erklärte in einer zweiten Stellungnahme vom 31. Januar 2022 seine auf der Rechtsprechung des Bundesstrafgerichts beruhende Praxis und ersucht sinngemäss darum, Klarheit über die Rechtmässigkeit dieses Vorgehens zu schaffen. Das Bundesstrafgericht verzichtete auf eine weitere Vernehmlassung. (...) Das Bundesgericht heisst die Beschwerde gut.
(Auszug)

Erwägungen

Aus den Erwägungen:

2.

2.1 Gemäss Art. 50 VStrR (SR 313.0) sind im Verwaltungsstrafverfahren Papiere mit grösster Schonung der Privatgeheimnisse zu durchsuchen (Abs. 1), wobei Amts- und Berufsgeheimnisse 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

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 berechtigte 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).

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).

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).

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

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 Entsiegelung strafbar.

2.5 Der Beschwerdeführer und die Zollverwaltung erachten übereinstimmend eine Überprüfung des Vorgehens gemäss der Praxis

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 Entsiegelungsverfahren 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.

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 Entsiegelungsantrag ergehen. Das Gericht könnte eine Kopierung der Dateien auch von Amtes wegen anordnen, wenn es dies als notwendig oder zur Vermeidung des möglichen Vorwurfs

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 Wei-

sungsbefugnisse 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.

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.

3.

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 Durchsuchung 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.

3.2 Aus diesem Ablauf ergibt sich, dass sich die fraglichen drei IT-Geräte nach Eingang des Siegelungsgesuchs am 14. bzw.

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.

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

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.

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 zum 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.

4.

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).

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 aus-

geschlossen, 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.

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.