Bundesstrafgericht
Tribunal pénal fédéral
Tribunale penale federale
Tribunal penal federal

Geschäftsnummer: BE.2022.10

Beschluss vom 24. Januar 2023
Beschwerdekammer

Besetzung	Bundesstrafrichter Roy Garré, Vorsitz, Daniel Kipfer Fasciati und Patrick Robert-Nicoud, Gerichtsschreiberin Santina Pizzonia
Parteien	**BUNDESAMT FÜR ZOLL UND GRENZSICHERHEIT, Direktionsbereich Strafverfolgung,** Gesuchsteller **gegen** **A.,** vertreten durch Rechtsanwalt Friedrich Frank, Gesuchsgegner
Gegenstand	Rückweisungsurteil des Bundesgerichts; Kosten- und Entschädigungsfolgen

Sachverhalt:

A. Infolge einer spontanen Amtshilfemeldung der portugiesischen Zollbehörden führte das Grenzwachtkorps am Flughafen Zürich am 10. September 2020 eine Zollkontrolle und körperliche Durchsuchung von A. durch. Sie konnte dabei 12 Armbanduhren der Marke Rolex im Wert von Fr. 136'334.-- und verschiedene Kaufbelege/Rechnungen sowie zu den Uhren zugehörige Gegenstände feststellen, welche A. bei seiner Einreise nicht zur Einfuhr in die Schweiz anmeldete. Zehn der zwölf Armbanduhren samt Kaufbelegen/Rechnungen trug A. bei der Einreise um seinen Bauch in einem Schmuggelgurt versteckt auf sich (ZFA OST 71-2020.3989 01.01.01/001 ff.).

B. Noch am gleichen Tag eröffnete die damalige Eidgenössische Zollverwaltung (nachfolgend «EZV»), Hauptabteilung Zollfahndung Untersuchung Ost (ZFA), bzw. das heutige Bundesamt für Zoll und Grenzwachtsicherheit (nachfolgend «BAZG») gegen A. ein Strafverfahren wegen Verdachts auf Widerhandlungen gegen das Zollgesetz vom 18. März 2005 (ZG; SR 631.0) sowie gegen das Bundesgesetz vom 12. Juni 2009 über die Mehrwertsteuer (Mehrwertsteuergesetz, MWSTG; SR 641.20).

C. Ebenfalls am 10. September 2020 stellte die EZV unter anderem die beiden Mobiltelefone und das Tablet von A. vorläufig sicher (ZFA OST 71-2020.3989 01.05.01/001 ff.). Gemäss dem von A. am 10. September 2020 unterschriebenen Protokoll über die vorläufige Sicherstellung der IT-Geräte sowie der elektronischen Daten auf den IT-Geräten wurde A. namentlich über das Siegelungsrecht informiert (ZFA OST 71-2020.3989 01.05.01/001). Das Feld «Gründe für die Versiegelung» auf dem Protokoll blieb leer und A. verlangte keine Siegelung seiner Geräte (ZFA OST 71-2020.3989 01.05.01/001 und 01.08.01/008). Anlässlich seiner Einvernahme vom 10. September 2020 erklärte er lediglich, er möchte die Codes nicht bekannt geben (ZFA OST 71-2020.3989 01.08.01/008).

D. Mit E-Mail vom 14. September 2020 erklärte Rechtanwalt Friedrich Frank (nachfolgend «Rechtsanwalt Frank») gegenüber der EZV (d.h. dem zuständigen Inspektor der EZV), A. zu vertreten, und verlangte ohne Angabe von Gründen die umgehende Siegelung der sichergestellten IT-Geräte von A.

Mit E-Mail vom Folgetag (06:42 Uhr) ersuchte die EZV Rechtanwalt Frank, die Vollmacht und das Ersuchen um Siegelung schriftlich nachzureichen (ZFA OST 71-2020.3989 01.03.01/001 f.).

Am 15. September 2020 reichte Rechtsanwalt Frank der EZV vorab per E-Mail (17:56 Uhr) die vom gleichen Tag datierte Vollmacht nach, und kündigte an, die EZV nach Erhalt der Akten kurz telefonisch zu kontaktieren. Mit E-Mail vom 16. September 2020 teilte die EZV Rechtsanwalt Frank mit, ihm die Akten mit seinem Einverständnis am Folgetag elektronisch zur Verfügung zu stellen und anschliessend die «Angelegenheit» telefonisch zu besprechen, womit sich Rechtsanwalt Frank mit E-Mail vom 17. September 2020 einverstanden erklärte (ZFA OST 71-2020.3989 01.03.03/001 ff.). Die Vollmacht und das Ersuchen um Siegelung gingen bei der EZV am 17. September 2020 schriftlich ein (ZFA OST 71-2020.3989 01.03.02/001 ff.). Mit der Anleitung zum Herunterladen der Akten bat die EZV in ihrer E-Mail vom 17. September 2020 Rechtsanwalt Frank, sie betreffend die Siegelung der IT-Geräte kurz anzurufen (ZFA OST 71-2020.3989 01.03.01/001).

E. Die EZV informierte am 18. September 2020 Rechtsanwalt Frank telefonisch, dass A. bis dato die Codes der IT-Geräte nicht bekannt gegeben habe, was dazu führe, dass die Geräte kostenpflichtig beim Fedpol entsperrt werden müssen. Gemäss der betreffenden Telefonnotiz der EZV habe Rechtsanwalt Frank zu verstehen gegeben, dass ihm dies nicht bekannt gewesen sei. Der Telefonnotiz zufolge habe Rechtsanwalt Frank erklärt, er hätte noch nicht im Detail mit dem Mandanten sprechen können. Die Siegelung werde dennoch bis auf Weiteres aufrechterhalten. In der Telefonnotiz wurde sodann festgehalten, dass mit Rechtsanwalt Frank vereinbart worden sei, zusammen mit A., den Fall und insbesondere die Siegelung, die Nichtbekanntgabe der Codes und die Folgen daraus persönlich zu besprechen. Der erste Terminvorschlag der EZV (21. September 2020) habe Rechtsanwalt Frank wegen eines anderweitigen Termins nicht bestätigen können. Es sei deshalb ein Gespräch auf den nächstmöglichen Termin am 29. September 2020, 14:00 Uhr, vereinbart worden (ZFA OST 71-2020.3989 01.03.04/001). Abschliessend hielt die EZV in der Telefonnotiz Folgendes fest: «Seitens RA Frank wurde zusätzlich noch mitgeteilt, dass beim Filetransfer der Akten, das Einvernahmeprotokoll fehle. Dies wurde RA Frank im Anschluss umgehend zugestellt.»

F. Am 29. September 2020 erläuterte die EZV A. in Anwesenheit von dessen Rechtsvertreter die weiteren Schritte. Der betreffenden Aktennotiz der EZV ist dazu Folgendes zu entnehmen (ZFA OST 71-2020.3989 01.06.01/001 f.):

> «Seitens ZFA wurden die weiteren Schritte erläutert, wenn der Zugangscode für die IKT-Geräte nicht bekannt ist:
>
> - Übergabe an das Fedpol
> - Dauer 2-6 Monate
> - Kosten pro Gerät mind. CHF 1'200.-- (in der Summe 3'600.--)
> - wenn Gerät entsperrt, Erstellung eines Images durch Fedpol
> - Übergabe eines Speichermediums an ZFA
> - Rückgabe der IT-Geräte an Beschuldigten
> - Sichtung/Ausscheidung der Daten durch Inspektoren
> - Beschlagnahmung der relevanten Daten für die Untersuchung
> - Siegelung kann verlangt werden und der Prozess kann vom Beschuldigten oder RA begleitet werden
>
> Seitens ZFA wurden die weiteren Schritte erläutert betreffend die verlangte Siegelung der IKT-Geräte durch RA Frank:
>
> - wir müssen das Entsiegelungsgesuch zeitnah stellen, dies auch wenn die Geräte noch nicht entsperrt sind
> - Daten, die nicht schützenswert sind, werden mit Sicherheit freigegeben, da der objektive Tatbestand erfüllt ist
> - auch hier entstehen Kosten, die von der unterlegenen Partei getragen werden müssen
>
> Seitens ZFA wurde darauf hingewiesen, dass ein kooperatives Verhalten auch Einfluss auf die Bussenhöhe haben kann.
>
> Es der Auftrag der ZFA ist eine Untersuchung zu führen und zu klären, ob es sich beim Aufgriff vom 10.09.2020 um einen Einzelfall handelte oder nicht. Insbesondere auch da Herr A. im Handel mit Uhren tätig ist und er damit seinen Lebensunterhalt verdient.
>
> Herr A. und RA Frank halten bis auf weiteres an der Siegelung fest und Herr A. wird auch die Codes nicht bekannt geben.
>
> RA Frank wird sich jedoch noch mit Herr A. besprechen, wie in dieser Angelegenheit (Siegelung/Codes) weiter vorgegangen werden soll. RA Frank wird sich bei Inspektor B., bis nächste Woche melden.»

G. Mit E-Mail vom 30. September 2020 (16:31 Uhr) teilte Rechtsanwalt Frank der EZV mit, dass an der Einsprache festgehalten werde und dass eine entsprechende Begründung auf erste Anfrage gegeben werden könne, er aber um Kenntnisnahme bitte, dass er ab dem kommenden Freitag für 14 Tage in den Ferien sei (ZFA OST 71-2020.3989 01.03.06/001).

H. Am 1. Oktober 2020 übermittelte die EZV die Geräte von A. dem Bundesamt für Polizei, Bundeskriminalpolizei (Fedpol), Abteilung IT Forensik und Cybercrime IFC, je mit einem «Unlock mit Bruteforce und Extraction Auftrag» (ZFA OST 71-2020.3989 01.05.14/001).

I. Mit E-Mail vom 2. Oktober 2020 (18:21 Uhr) erklärte Rechtsanwalt Frank gegenüber der EZV, dass er sich den Hinweis erlaube, dass die gesiegelten Datenträger zum einen vertrauliche Anwaltskorrespondenz, zum anderen höchstpersönliche Informationen und Geschäftsgeheimnisse enthalten würden. Falls dies überhaupt erforderlich sein sollte, könne dies weiter begründet werden. Weiter erlaube er sich den Hinweis, dass sein Mandant mit der Nichtbekanntgabe der Codes der Mobiltelefone und des Tablets klar seinen Siegelungswunsch zum Ausdruck gebracht habe. Er habe in seiner Eingabe vom 15. September 2020 diesen lediglich noch einmal bestätigt (ZFA OST 71-2020.3989 01.03.06/001).
.

J. Während des Entsperrungs- und Spiegelungsvorgangs beim Fedpol gelangte die EZV mit Gesuch vom 8. Oktober 2020 an die Beschwerdekammer des Bundesstrafgerichts und beantragte, das Entsiegelungsgesuch sei gutzuheissen (BE.2020.17, act. 1).

Darin führte die EZV ausdrücklich aus, dass die sichergestellten Mobiltelefone sowie das Tablet zwecks Entsperrung und Erstellung einer Sicherungskopie mittels Spiegelung an die Abteilung IT Forensik und Cybercrime IFC des Fedpol weitergeleitet worden seien, da A. die Entsperrcodes für die sichergestellten Geräte nicht habe bekannt geben wollen. Die EZV erklärte weiter, dass nach erfolgter Erstellung der Sicherungskopien diese in Anwesenheit von A. bzw. dessen Rechtsvertreter sicherzustellen und zu siegeln seien. Sodann würden diese gesiegelten Sicherungskopien dem Bundesstrafgericht in der vorliegenden Sache übermittelt werden (BB.2020.17, act. 1 S. 3).

Mit Schreiben vom 12. Oktober 2020 wurde Rechtsanwalt Frank zur Gesuchsantwort eingeladen (BE.2020.17, act. 2).

K. Nach Entsperrung der Geräte sowie Erstellung der Sicherungskopien durch das Fedpol nahm die EZV (bzw. ein IT-Forensiker der EZV) vom Fedpol am 13. Oktober 2020, 15:40 Uhr, die Datenträger von A. sowie die Festplatte mit den Sicherungskopien entgegen und verwahrte sie umgehend im Safe der Forensik-Abteilung (BE.2020.17, act. 5.2, 5.1, 10 S. 3 f.). Zur Übergabe der entsperrten Geräte samt forensischer Festplatte durch den Mitarbeiter des Fedpol an den IT-Forensiker der EZV und deren Verwahrung erstellte der betreffende Inspektor Digitale Forensik der EZV am 13. Oktober 2020, 16:30 Uhr, eine Aktennotiz mit folgendem Inhalt (BE.2020.17, act. 5.2):

> «Die sichergestellten Geräte Samsung Galaxy A40, Samsung Galaxy S10+, Samsung Tab S6 sowie die forensische Festplatte mit Datenextraktionen von den genannten Geräten wurden mir am 13. Oktober 2020 um 15:40 vom Mitarbeiter des Kommissariats IFC 2 Forensik (fedpol), Herrn C., zurückgegeben. Die forensischen Daten wurden nicht gesichtet und auf keine Weise manipuliert, die forensische Festplatte ist verschlüsselt und seit der Übergabe im Tresor des DB Digitalforensik sicher aufbewahrt.»

Die EZV informierte umgehend Rechtsanwalt Frank mit E-Mail vom 13. Oktober 2020, 17:10 Uhr, dass sich die Festplatte bereits bei der EZV in Bern, Abteilung Forensik, befinde. Sie hielt fest, dass die Festplatte vorgängig durch das Fedpol verschlüsselt worden sei. Sie bat Rechtsanwalt Frank, bis spätestens am 20. Oktober 2020 mitzuteilen, ob er an der Versiegelung beiwohnen möchte, damit sie die Festplatte so rasch als möglich auch physisch versiegeln und an das Bundesstrafgericht übermitteln könne (BE.2020.17, act. 7.1).

L. Mit E-Mail vom 20. Oktober 2020, 14:14 Uhr, teilte Rechtsanwalt Frank der EZV Folgendes mit (BE.2020.17, act. 7.2):

> «Das offenbar gewählte Vorgehen, die drei Datenträger zunächst an das fedpol zu übersenden resp. der damit einhergehende (mutmassliche) «Unlock mit Bruteforce und Extraction Auftrag» sowie dessen (mutmassliche Durchführung durch das fedpol – ohne Anwesenheit meines Mandanten – verstossen gegen die bundesgerichtliche Rechtsprechung mit Urteil 1B_376/2019 vom 12. September 2019 (und weiteren Entscheide). Nach meiner Rechtsauffassung sind deswegen sowohl die drei Datenträger als auch die (von Ihnen erwähnte) Festplatte umgehend an meinen Mandanten herauszugeben. Die bisherigen Siegel

hätten erst gar nicht gebrochen werden dürfen, was aber offenbar geschehen ist, womit der Schutzzweck der gesamten Siegelung entfallen ist.»

M. Mit Schreiben vom 22. Oktober 2020 ersuchte die EZV Rechtsanwalt Frank erneut, nun innert fünf Arbeitstagen unter Angabe möglicher zeitnaher Termine, mitzuteilen, ob er und/oder sein Mandant der Siegelung teilnehmen möchten. Ohne eine entsprechende Mitteilung würde die EZV davon ausgehen, dass er auf dieses Recht verzichte und die EZV die Datenträger mit den gespiegelten Daten selbständig siegeln und dem Bundesstrafgericht zustellen werde. Die EZV hielt in ihrem Schreiben weiter Folgendes fest (BE.2020.17, act. 5.1):

«Da sich sowohl die IT-Geräte Ihres Mandanten wie auch die Datenträger mit den gespiegelten Daten aufgrund eines Fehlers bereits bei der Forensik der EZV befinden und in Bern verwahrt werden, werden die Siegel vor Ort an der Taubenstrasse 16 anzubringen sein. Bei dieser Gelegenheit können die IT-Geräte Ihrem Mandanten zurück gegeben werden.

Im Übrigen teilen wir Ihnen mit, dass das Vorgehen der EZV bei der Sicherstellung und Siegelung der Daten u.E. der aktuellen Rechtsprechung des Bundesstrafgerichts betreffend Entsperrung, Spiegelung und Siegelung von passwortgeschützten Daten und Datenträgern entspricht (vgl. die Entscheide der Beschwerdekammer des Bundesstrafgerichts RR.2019.219 und RR.2019.220 beide vom 25. Mai 2020, jeweils E. 5, sowie deren Bestätigung im Rahmen der Beschlüsse der Beschwerdekammer des Bundesstrafgerichts BE.2020.3 und BE.2020.5, beide vom 27. Juli 2020, jeweils E. 1.4.3). Über das Vorgehen *in casu* wurden Sie und Ihr Mandant zudem anlässlich der Besprechung mit der Zollfahndung Ost am 29. September 2020 sowie durch die entsprechenden Ausführungen im Entsiegelungsgesuch vom 8. Oktober 2020, welches Ihnen vom Bundesstrafgericht zugestellt wurde, in Kenntnis gesetzt.»

In der Beilage stellte die EZV Rechtsanwalt Frank die Aktennotiz des Inspektors Digitale Forensik vom 13. Oktober 2020 zu (BE.2020.17, act. 5.2; s. supra lit. K).

N. Mit Schreiben vom 22. Oktober 2020 übermittelte die EZV der Beschwerdekammer ihr Schreiben vom 22. Oktober 2020 an Rechtsanwalt Frank samt Beilage zur Kenntnis (BE.2020.17, act. 5, 5.1, 5.2; s. supra lit. K und M).

O. Mit Schreiben vom 29. Oktober 2020 (vorab per E-Mail) teilte Rechtsanwalt Frank der EZV mit, er nehme zur Kenntnis, dass sowohl die «– zu Unrecht und ohne jegliche Rechtsgrundlage entsiegelten und entsperrten –» Datenträger seines Mandanten als auch die «– zu Unrecht und ohne jegliche Rechtsgrundlage erstellte – Festplatte aufgrund eines Fehlers bereits bei der Forensik der EZV in Bern befinden und in Bern verwahrt werden». Er hielt fest, dass er dieses Vorgehen der EZV nicht akzeptiere. Das von der EZV erwähnte weitere Vorgehen, einer Siegelung der Festplatte beizuwohnen, sei nicht akzeptabel und solle offenbar lediglich den Anschein der Rechtskonformität wahren. Dass sich die Datenträger nunmehr darüber hinaus bei der EZV in Bern befinden, befremde umso mehr (BE.2020.17, act. 7.4).

P. Mit Schreiben vom 6. November 2020 übermittelte die EZV der Beschwerdekammer die versiegelten Datenträger, welche die zwischenzeitlich gespiegelten Daten der Mobiltelefone und des Tablets von A. enthielten. Die EZV hielt fest, dass die Datenträger am 5. November 2020 in den Räumlichkeiten der EZV in Bern sichergestellt und versiegelt worden seien und dass Rechtsanwalt Frank auf telefonische Nachfrage hin auf eine Teilnahme an der Siegelung verzichtet habe (BE.202017, act. 8). In der Beilage stellte es zusätzlich das Sicherstellungsprotokoll der EZV vom 5. November 2020 zu (BE.2020.17, act. 8.1).

Q. Mit Gesuchsantwort vom 6. November 2020 liess A. durch seinen Rechtsvertreter zur Hauptsache beantragen, das Gesuch sei abzuweisen, die Siegelungen seien aufrechtzuerhalten, die versiegelten Daten bzw. Datenträger seien dem Gesuchsgegner zurückzugeben und die vom Fedpol angefertigte Festplatte resp. die darauf befindliche Sicherungskopie der vorerwähnten Geräte seien umgehend zu löschen. Eventualiter seien im Rahmen einer geeigneten durch das Bundesstrafgericht durchzuführenden Triage diejenigen Aufzeichnungen auszusondern und dem Gesuchsgegner herauszugeben, welche vom Anwalts-, Arzt- und Geschäftsgeheimnis geschützt seien, unter Kosten und Entschädigungsfolgen zu Lasten der Staatskasse (BE.2020.17, act. 7).

Rechtsanwalt Frank argumentierte im Wesentlichen, es sei nicht belegt, dass eine Datenkopie schnellstmöglich angefertigt werden müsse. Sodann müsse der IT-Forensiker im Auftrage des «Zwangsmassnahmengerichts» tätig werden, nicht im Auftrag der Untersuchungsbehörde. Dies gelte um so mehr, als die entsperrten und nicht gesiegelten Geräte wie vorliegend einfach wieder der Untersuchungsbehörde vorgelegt würden, wo sie dann

durchsehbar seien (BE.2020.17, act. 7 S. 5 f.). Was dort mit den Geräten geschehen sei, sei unbekannt (BE.2020.17, act. 7 S. 4). Rechtsanwalt Frank machte unter anderem geltend, auf den sichergestellten Datenträgern würden sich u.a. Informationen und Unterlagen aus dem Verkehr von A. mit ihm befinden, welche unzweifelhaft vom Anwaltsgeheimnis betroffen seien und über die E-Mail-Adresse versendet worden seien (BE.2020.17, act. 7 S. 7).

R. Mit Gesuchsreplik vom 20. November 2020 stellte die EZV klar, dass die Geräte von A. sowie die Festplatte mit den Sicherungskopien am 13. Oktober 2020 nach erfolgter Entsperrung der Geräte sowie Erstellung der Sicherungskopien durch das Fedpol zur EZV verbracht und umgehend im Safe der Forensik-Abteilung verwahrt worden seien. Dies sei der Aktennotiz vom 13. Oktober 2020 des zuständigen IT-Forensikers der EZV zu entnehmen. Die EZV führte aus, aufgrund eines internen Kommunikationsfehlers habe der Mitarbeiter der IT-Forensik der EZV keine Kenntnis davon gehabt, dass die vom Fedpol gespiegelten Daten Gegenstand des Entsiegelungsverfahrens seien und beim Fedpol in Anwesenheit von A. hätten gesiegelt und unmittelbar anschliessend der Beschwerdekammer des Bundesstrafgerichts hätten übermittelt werden müssen. Aus diesem Grund habe der IT-Forensiker der EZV die Geräte von A. sowie die Festplatte mit den Sicherungskopien vom Mitarbeiter des Fedpol entgegengenommen (BE.2020.17, act. 10 S. 3 f.). Die EZV betonte, dass jedoch zu keiner Zeit Einsicht in die Daten der Festplatte oder in diejenigen der Geräte des Gesuchsgegner genommen worden sei. Auch seien die Daten nicht durchsucht oder manipuliert worden. Sämtliche Datenträger seien im Safe des DB Digitalforensik – wie auch sonst bis zur Übergabe an den zuständigen Untersuchungsbeamten bzw. bis zur weiteren Auftragserteilung an den DB Digitalforensik – sicher aufbewahrt worden und anschliessend versiegelt worden. Die EZV merkte an, dass beim Fedpol nichts Anderes geschehen wäre. Die EZV erläuterte, weshalb es sich dabei nicht um einen relevanten Fehler handle, und erklärte, dass die Geräte von A. sowie die Festplatte mit den Sicherungskopien sofort nach Erhalt durch das Fedpol im Safe der Abteilung IT-Forensik der EZV verwahrt worden seien und sich weder der mit der Untersuchung befasste Inspektor noch unbefugte Dritte Zugang dazu hätten verschaffen können. Zudem seien die Festplatten mit den Sicherungskopien vom Fedpol im Rahmen der Rückgabe nach Erfüllung des Unlock mit Brute Force und Extraction Auftrags mit einem Passwort versehen. Sie führte aus, dass die Festplatte vom Mitarbeiter der IT-Forensik aus dem Safe entnommen und durch den zuständigen Inspektor in Anwesenheit des IT-Forensikers der EZV gesiegelt worden sei, nachdem der Rechtsvertreter von A. auch auf telefonische Nachfrage hin mitgeteilt habe, auf das Teilnahmerecht an der Siegelung zu verzichten. Dem

Rechtsvertreter sei dabei nochmals das Vorgehen erläutert und mitgeteilt worden, dass die Geräte von A. diesem nach erfolgter Spiegelung und Erstellung der Sicherungskopien zurückgegeben werden können und hierfür ein Termin mit dem zuständigen Inspektor zu vereinbaren sei (BE.2020.17, act. 10 S. 3 f.). Die Rückgabe sei wie erläutert angeboten worden, A. und sein Rechtsvertreter hätten noch keinen diesbezüglichen Termin bekannt gegeben, weshalb die Geräte nach wie vor im Safe der DB Digitalforensik der EZV verwahrt werden (BE.2020.17, act. 10 S. 6).

Über diese Eingabe sowie die Eingabe der EZV vom 6. November 2020 wurde A. mit Schreiben vom 23. November 2020 in Kenntnis gesetzt (BE.2020.17, act. 11).

S. Mit Schreiben vom 3. Februar 2021 wurden beide Parteien darüber orientiert, dass aufgrund des behaupteten, absolut zu schützenden Arztgeheimnisses die Entsiegelung und Durchsuchung durch die Beschwerdekammer durchzuführen sei (BE.2020.17, act. 12). Am 4. Mai 2021 reichten die mit der Triage der elektronischen Daten beauftragten Sachverständigen ihren forensischen Analysebericht vom 3. Mai 2021 samt den selektierten Daten bei der Beschwerdekammer ein (BE.2020.17, act. 24, 24.1).

Nach einer inhaltlichen Analyse aller durch die Sachverständigen selektierten Daten wurde der Gesuchsgegner mit Schreiben vom 1. Juli 2021 unter Beilage namentlich des forensischen Analyseberichts und der selektierten Daten darüber informiert, dass kein einziges Element habe aufgefunden werden können, welches unter das Arztgeheimnis fallen würde und auszusondern wäre. Es wurde ihm abschliessend Gelegenheit zur freigestellten Stellungnahme gegeben (BE.2020.17, act. 25). Innert Frist liess sich der Gesuchsgegner nicht vernehmen.

T. Die Beschwerdekammer des Bundesstrafgerichts hiess mit Beschluss BE.2020.17 das Gesuch um Entsiegelung gut und ermächtigte die Gesuchstellerin, alle sichergestellten Daten zu durchsuchen. Die Gerichtskosten von Fr. 8'000.--, darin inbegriffen die Auslagen in der Höhe von Fr. 4‘604.20 für die durchgeführte Triage der elektronischen Daten, auferlegte sie dem Gesuchsgegner (BE.2020.17, act. 28).

Zum Vorbringen in der Sache, auf den sichergestellten Datenträger würden sich Informationen und Unterlagen aus dem Verkehr des Gesuchsgegners mit seinem Rechtsvertreter, Rechtsanwalt Friedrich Frank, befinden, wurde

erwogen, dass sich die ab dem 14. September 2020 aufgenommene Rechtsbeziehung zwischen Rechtsanwalt Frank und dem Gesuchsgegner bzw. die entsprechende Kommunikation nicht auf den am 10. September 2020 sichergestellten Geräten befinden und auch nicht abgerufen werden könne, wenn die Geräte nach den Vorgaben der IT-Forensik sichergestellt worden seien, wovon auszugehen sei. Die Beschwerdekammer hielt fest, dass sich demnach auch keine Anwaltskorrespondenz auf der forensischen Datenkopie befinden könne, deren Entsiegelung verlangt werde (E. 6.3).

Zum Einwand, das Entsiegelungsgesuch betreffe die Korrespondenz des Gesuchsgegners mit einem in Hong Kong tätigen Rechtsanwalt, erwog die Beschwerdekammer, dass der Gesuchsgegner weder behauptet noch glaubhaft gemacht habe, es sei eine berufsspezifische Tätigkeit des genannten Rechtsanwalts betroffen. Die Beschwerdekammer hielt fest, dass hier wie bei der Geltendmachung von Geschäftsgeheimnissen der Gesuchsgegner seiner Substantiierungsobliegenheit nicht nachgekommen sei. Die Beschwerdekammer kam zum Schluss, dass mit Ausnahme des absolut zu schützenden Arztgeheimnisses der Gesuchsgegner keine schutzwürdigen Geheimhaltungsinteressen glaubhaft gemacht habe, welche einer Entsiegelung und Durchsuchung durch die Gesuchstellerin entgegenstehen würden (E. 6.4 ff.).

Die Beschwerdekammer stellte nach einer inhaltlichen Analyse der triagierten Daten fest, dass kein einziges Element habe aufgefunden werden können, welches unter das Arztgeheimnis fallen würde und auszusondern wäre (E. 7).

Was die vom Gesuchsgegner gerügte Entsperrung und Spiegelung anbelangt, hielt die Beschwerdekammer fest, dass die Gesuchstellerin im Grundsatz der im Einzelnen erläuterten bundesstrafgerichtlichen Rechtsprechung gefolgt sei, indem sie die Entsperrung und Spiegelung der beiden Mobiltelefone und des Tablets vor der Siegelung veranlasste und im Nachgang zu ihrem Entsiegelungsgesuch die gesiegelte forensische Datenkopie einreichte. Dass die Entsperrung und Spiegelung nicht unmittelbar nach der Sicherstellung am 10. September 2020, was es grundsätzlich anzustreben gelte, sondern erst am 1. Oktober 2020 veranlasst worden sei, sei auf das zwischen den Parteien vereinbarte Vorgehen zurückzuführen, zuvor den Fall und insbesondere die Siegelung, die Nichtbekanntgabe der Codes und die Folgen daraus zusammen persönlich zu besprechen (E. 2).

U. Gegen diesen Beschluss erhob der Gesuchsgegner (nachfolgend auch Beschwerdeführer) Beschwerde beim Bundesgericht (BE.2020.17, act. 32.1).

Zur Sache machte er geltend, es bestünden schutzwürdige Geheimhaltungsinteressen, welche er glaubhaft gemacht habe. Die Erkenntnis des Bundesstrafgerichts in Bezug auf die Korrespondenz mit den erwähnten Ärzten sei unverwertbar. Darüber hinaus gebe es auch Anwaltskorrespondenz mit Rechtsanwalt Frank und dem in Hong Kong tätigen Rechtsanwalt. Er machte geltend, das Bundesstrafgericht stelle darauf ab, dass die Gesuchstellerin am 10. September 2020 die Geräte des Beschwerdeführers lege artis, d.h. entsprechend den Vorgaben der IT-Forensik sichergestellt habe. Woraus das Bundesstrafgericht «dieses lege artis-Handeln» der Gesuchstellerin bzw. Beschwerdegegnerin schliesse, sei nicht ersichtlich, zumal diese explizit selbst gefordert habe, dass die Datenträger auf Anwaltskorrespondenz zu durchsuchen seien. Bereits dies hätte das Bundesstrafgericht zu einer solchen Durchsuchung veranlassen müssen, zumal es entsprechende Anwaltskorrespondenz gebe (S. 15).

Sodann brachte der Beschwerdeführer im Wesentlichen vor, dass es keine gesetzliche Grundlage für ein «Entsperr- und Datenspiegelungs- resp. -sicherungsverfahren» gebe. Ein «Entsperr- und Datenspiegelungs- resp. -sicherungsverfahren» müsse, falls erforderlich, nach bundesgerichtlicher Rechtsprechung im Entsiegelungsverfahren durch das Entsiegelungsgericht durchgeführt werden. Der angefochtene Entscheid verletze Art. 50 VStrR, mithin Bundesrecht (S. 8 f.). Der Beschwerdeführer bestritt, dass eine betroffene Person auf einen Datenträger zugreifen könnte, welcher sich gar nicht mehr in ihrem Besitz befinde (S. 10 f.). Er bezweifelte, dass die auf dem sichergestellten Datenträger befindlichen Daten überhaupt unwiderruflich gelöscht werden könnten. Er erklärte, ein IT-Forensiker des Fedpol könne gelöschte Daten wiederherstellen (S. 11).

V. Auf entsprechende Einladung hin liess die Beschwerdekammer dem Bundesgericht ihre Vernehmlassung zukommen, in welcher sie auf den angefochtenen Beschluss verwies und an dessen Begründung unter Hinweis auf TPF 2020 96 E. 5 festhielt (BE.2020.17, act. 33).

Sie erlaubte sich dabei mit Nachdruck die gesetzliche Zuständigkeit des untersuchenden Beamten zur Beweissicherung sowie die Notwendigkeit zu betonen, die Datenspiegelung inkl. Entsperrung der fraglichen Datenträger zur Beweissicherung schnellstmöglich durchzuführen. Sie hielt fest, es könne nicht genug hervorgehoben werden, dass weder die Datenspiegelung noch

die vorangehende Entsperrung eine «Durchsuchung» der Datenträger beinhalten. Der Schutzzweck des Siegelungs- bzw. Entsiegelungsverfahrens werde damit nicht beeinträchtigt. Sie wies darauf hin, der Beschwerdeführer scheine in seiner Beschwerde die in TPF 2020 96 erläuterten Grundsätze der IT-Forensik und die Beschaffenheit der fraglichen Datenträger nicht zur Kenntnis nehmen zu wollen. Sie führte aus, dass, wie in TPF 2020 96 E. 5 im Einzelnen erläutert, sich eine unbefugte «Sichtung» der forensischen Datenkopie ohne eine kriminelle Herangehensweise der betreffenden Beamten nicht verheimlichen lasse. Solle nach den Worten des Beschwerdeführers «der Verdacht einer Kenntnisnahme von besonders geheimnisgeschützten Daten durch die Untersuchungsbehörde verunmöglicht werden», könne dies im Zusammenhang mit den fraglichen Datenträgern nur bedeuten, dass man im Ernst eine Daten-, Beweis- und Aktenmanipulation durch den untersuchenden Beamten bzw. die untersuchende Behörde zwecks unbefugter Einsicht bzw. deren Verheimlichung in Betracht zieht und auf dieser Grundlage die Sicherungsvorkehrungen begründet. Die Beschwerdekammer gab zu bedenken, dass folgerichtig und unabhängig von einem Antrag auf Siegelung bereits im Grundsatz die Aktenführung und Sicherung aller Beweise einer neutralen Stelle überlassen werden müssten, wenn man von einer solchen gravierenden Verdachtslage ausgehen wollte. Die Beschwerdekammer hielt fest, dass ein solches Misstrauen gegenüber der untersuchenden Behörde dem schweizerischen (Verwaltungs-)Strafverfahren fremd sei und sich in Abwesenheit von konkreten Anhaltspunkten nicht rechtfertigen lasse, ohne – nicht nur die gesetzliche Verfahrensordnung – sondern auch die redliche Tätigkeit aller Strafbehörden im Ergebnis in Frage zu stellen.

W. Mit Schreiben vom 9. September 2021 reichte die EZV die Beschwerdeantwort ein (BE.2020.17, act. 36.1). Mit Schreiben vom 1. Oktober 2021 reichte der Beschwerdeführer seine Stellungnahme zu den Vernehmlassungsantworten ein (BE.2020.17, act. 37.1). Die Beschwerdekammer des Bundesstrafgerichts verzichtete mit Schreiben vom 21. Januar 2022 auf eine weitergehende Stellungnahme (BE.2020.17, act. 38).

Mit Schreiben vom 28. Januar 2022 reichte der Beschwerdeführer eine weitere Stellungnahme ein (BE.2020.17, act. 39.1). Mit Schreiben vom 31. Januar 2022 reichte die EZV bzw. neu BAZG seine Stellungnahme ein (BE.2020.17, act. 39.2).

X. Mit Urteil 1B_432/2021 vom 28. Februar 2022 hiess das Bundesgericht die Beschwerde des Beschwerdeführers gut und hob den Beschluss der Beschwerdekammer auf. Sie wies diese an, dem Beschwerdeführer die drei

sichergestellten elektronischen Geräte mit den darauf vorhandenen Dateien auszuhändigen und die durch die Spiegelung erstellten Datenkopien zu vernichten. Sie hielt weiter fest, dass die Beschwerdekammer über die Verlegung der Kosten und Entschädigungen im vorinstanzlichen Verfahren neu zu entscheiden habe (act. 1).

Y. Die Beschwerdekammer des Bundesstrafgerichts nahm das Verfahren BE.2020.17 unter der Geschäftsnummer BE.2022.10 wieder auf. Mit Schreiben vom 7. April 2022 reichte der Rechtsvertreter des Gesuchsgegners seine Kostennote ein (act. 2). Mit Schreiben vom 29. Dezember 2021 wurde diese Eingabe der Gegenseite zur Kenntnis zugestellt (act. 3).

Z. Auf die Ausführungen der Parteien und die eingereichten Akten wird, soweit erforderlich, in den folgenden rechtlichen Erwägungen Bezug genommen.

Die Beschwerdekammer zieht in Erwägung:

1. Mit Rückweisungsurteil des Bundesgerichts 1B_43/2021 vom 28. Februar 2022 wurde die Beschwerdekammer angewiesen, dem Beschwerdeführer bzw. Gesuchsgegner die drei sichergestellten elektronischen Geräte auszuhändigen und die durch Spiegelung erstellten Datenkopien zu vernichten. Da sich die drei sichergestellten elektronischen Geräte beim Beschwerdegegner bzw. Gesuchsteller befinden, ist er anzuweisen, die Geräte dem Gesuchsgegner auf erste Aufforderung hin auszuhändigen. Nach Eintritt der Rechtskraft sind die durch Spiegelung erstellten Datenkopien zu vernichten. Vollständigkeitshalber sind auch die Datenträger mit den triagierten Daten zu vernichten.

2.

2.1 Bei diesem Ausgang des Verfahrens ist von der Erhebung einer Gerichtsgebühr abzusehen (Art. 66 Abs. 4 BGG analog; TPF 2011 25 E. 3).

2.2 Dem Gesuchsgegner ist in analoger Anwendung von Art. 68 Abs. 1 und 2 BGG eine Parteientschädigungen zuzusprechen. Grundlage für die Bemessung der Entschädigung bilden Art. 10 und 12 des Reglements des

Bundesstrafgerichts vom 31. August 2010 über die Kosten, Gebühren und Entschädigungen im Bundesstrafverfahren (BStKR; SR 173.713.162). Der Vertreter des Gesuchsgegners hat eine Kostennote im Gesamtbetrage von Fr. 4‘026.80 eingereicht, welche sich aus einem Aufwand von 12.1 Stunden à Fr. 300.--/h (d.h. Fr. 3‘630.--), eine Kleinspesenpauschale von 3 % (Fr. 208.90) und MWST 7,7 % (Fr. 287.90) zusammensetze (act. 2). Der entschädigungsberechtigte Stundenansatz ist auf die vor Bundesstrafgericht üblichen Fr. 230.-- pro Stunde festzusetzen (vgl. hierzu Beschluss des Bundesstrafgerichts BB.2012.8 vom 2. März 2012 E. 4.2; s. zuletzt auch Beschluss des Bundesstrafgericht BB.2022.96 vom 5. Dezember 2022 E. 4.2). Besondere Schwierigkeiten oder erhöhte Komplexität, welche einen höheren Ansatz für die Entschädigung rechtfertigen würden, liegen nicht vor. Das Honorar beträgt somit Fr. 2‘783.-- samt Barauslagen in der Höhe von pauschal von Fr. 50.--, zuzüglich 7,7 % MWST. Der Gesuchsteller hat dem Gesuchsgegner für dessen Aufwendungen im vorliegenden Verfahren eine Parteientschädigung in der Höhe von Fr. 3‘051.15 (inkl. Auslagen und MWST) zu entrichten (Art. 68 Abs. 1 und 2 BGG analog; Art. 10 und 12 Abs. 1 BStKR).

Demnach erkennt die Beschwerdekammer:

1. Der Gesuchsteller wird angewiesen, dem Gesuchsgegner die drei sichergestellten elektronischen Geräte auf erste Aufforderung hin auszuhändigen.

2. Nach Eintritt der Rechtskraft dieses Beschlusses werden die entfernten Siegel, die durch Spiegelung erstellten Datenkopien sowie die Datenträger mit den triagierten Daten vernichtet.

3. Es wird keine Gerichtsgebühr erhoben.

4. Der Gesuchsteller hat den Gesuchsgegner für das Entsiegelungsverfahren mit Fr. 3'051.15 (inkl. Auslagen und MWST) zu entschädigen.

Bellinzona, 25. Januar 2023

Im Namen der Beschwerdekammer
des Bundesstrafgerichts

Der Präsident: Die Gerichtsschreiberin:

Zustellung an

- Bundesamt für Zoll und Grenzsicherheit, Direktionsbereich Strafverfolgung
- Rechtsanwalt Friedrich Frank

Rechtsmittelbelehrung

Gegen Entscheide der Beschwerdekammer über Zwangsmassnahmen kann innert 30 Tagen nach der Eröffnung der vollständigen Ausfertigung beim Bundesgericht Beschwerde geführt werden (Art. 79 und 100 Abs. 1 des Bundesgesetzes über das Bundesgericht vom 17. Juni 2005; BGG). Eingaben müssen spätestens am letzten Tag der Frist beim Bundesgericht eingereicht oder zu dessen Handen der Schweizerischen Post oder einer schweizerischen diplomatischen oder konsularischen Vertretung übergeben werden (Art. 48 Abs. 1 BGG). Im Falle der elektronischen Einreichung ist für die Wahrung einer Frist der Zeitpunkt massgebend, in dem die Quittung ausgestellt wird, die bestätigt, dass alle Schritte abgeschlossen sind, die auf der Seite der Partei für die Übermittlung notwendig sind (Art. 48 Abs. 2 BGG). Das Verfahren richtet sich nach den Artikeln 90 ff. BGG.

Eine Beschwerde hemmt den Vollzug des angefochtenen Entscheides nur, wenn der Instruktionsrichter oder die Instruktionsrichterin es anordnet (Art. 103 BGG).