Martin Reimann

Die Entsperrung und Spiegelung von passwortgeschützten Datenträgern im Siegelungsverfahren

Mit seinem Urteil BGE 148 IV 221 hat das Bundesgericht die Praxis der Beschwerdekammer des Bundesstrafgerichts, wonach die Entsperrung und Spiegelung passwortgeschützter Datenträger im Rahmen eines Siegelungsverfahrens durch die Untersuchungsbehörde vorgenommen bzw. an die Forensikabteilung des Bundesamtes für Polizei (fedpol) delegiert werden kann, für bundesrechtswidrig erklärt. Auch wenn der Entscheid des Bundesgerichts im Ergebnis nicht zu beanstanden ist, wirft er mit Bezug auf künftige Siegelungsverfahren verschiedene Fragen auf, die im vorliegenden Beitrag im Anschluss an eine Zusammenfassung der bundesgerichtlichen Erwägungen erörtert werden.

Zitiervorschlag:
MARTIN REIMANN, Die Entsperrung und Spiegelung von passwortgeschützten Datenträgern im Siegelungsverfahren, sui generis 2022, S. 217

Dr. iur. **Martin Reimann,** wissenschaftlicher Assistent und Postdoktorand an den Universitäten Bern und Basel.

URL: sui-generis.ch/222
DOI: https://doi.org/10.21257/sg.222

I. Einleitung

1 Bei Sicherstellungen im Straf- und Verwaltungsstrafverfahren steht es der betroffenen Person zu, hinsichtlich der sichergestellten Gegenstände und Unterlagen die Siegelung zu verlangen und damit deren Durchsuchung und Verwertung je nach Ausgang des Entsiegelungsverfahrens zu verhindern. Nicht selten handelt es sich bei den sichergestellten Gegenständen um elektronische Datenträger, wie beispielsweise Smartphones oder Tablets, wobei sich ein entsprechendes Siegelungsgesuch auf die darauf befindlichen Daten richtet. Besondere Probleme ergeben sich, wenn der Datenträger im Zeitpunkt seiner Sicherstellung durch ein Passwort geschützt ist und die betroffene Person die Herausgabe des Passworts verweigert sowie zugleich die Siegelung verlangt. In einem jüngst ergangenen Urteil hat sich das Bundesgericht mit der Praxis der Beschwerdekammer des Bundesstrafgerichts betreffend solche Konstellationen befasst, wobei der dem Entscheid zugrundeliegende Sachverhalt nachfolgend dargestellt und die Argumentation des Bundesgerichts einer kritischen Würdigung unterzogen wird.

II. Prozessgeschichte

2 Anlässlich einer Durchsuchung von A. am Flughafen Zürich stellte das damalige Grenzwachtkorps (heute: Bundesamt für Zoll und Grenzsicherheit [BAZG]) neben zwölf nicht zur Einfuhr in die Schweiz angemeldeten Armbanduhren der Marke Rolex unter anderem auch zwei Mobiltelefone und ein Tablet sicher, worauf die Eidgenössische Zollverwaltung (heute ebenfalls: Bundesamt für Zoll und Grenzsicherheit [BAZG] und nachfolgend «Zollverwaltung») ein Strafverfahren gegen A. wegen des Verdachts auf Widerhandlungen gegen das Zollgesetz sowie das Mehrwertsteuergesetz eröffnete.

3 Nachdem der Beschuldigte bezüglich der sichergestellten Datenträger vorerst auf einen Siegelungsantrag verzichtete, zugleich aber die Herausgabe der Zugangscodes verweigerte, beantragte er deren Siegelung einige Tage später über seinen inzwischen beigezogenen Anwalt. Konkret machte der Beschuldigte geltend, dass sich auf den Datenträgern Anwaltskorrespondenz, höchstpersönliche Informationen sowie Geschäftsgeheimnisse befinden würden.

4 Gestützt auf die Praxis der in Zollverfahren als Entsiegelungsgericht fungierenden Beschwerdekammer des Bundesstrafgerichts übermittelte die Zollverwaltung die von dem Siegelungsantrag betroffenen Datenträger zunächst der Forensikabteilung des Bundesamtes für Polizei (fedpol) und beauftragte diese mit deren Entsperrung und anschliessenden Datenspiegelung.[1] In einem nächsten Schritt stellte die Zollverwaltung bei der Beschwerdekammer des Bundesstrafgerichts bezüglich der vom fedpol zu entsperrenden und zu spiegelnden Datenträgern ein Entsiegelungsgesuch. Nachdem die zuständige Forensikabteilung des fedpol die Datenträger erfolgreich entsperrt und gespiegelt hatte, wurden diese von derselben Behörde versiegelt und der Beschwerdekammer des Bundesstrafgerichts übermittelt. Das Entsiegelungsgesuch der Zollverwaltung wurde im Anschluss von der Beschwerdekammer des Bundesstrafgerichts gutgeheissen, wobei die Zollverwaltung zur Durchsuchung der gespiegelten Daten ermächtigt wurde.

5 Gegen diesen Entscheid gelangte der Beschuldigte mit Beschwerde in Strafsachen an das Bundesgericht, welches die Beschwerde guthiess. Das Bundesgericht kam zum Ergebnis, dass die Praxis der Beschwerdekammer des Bundesstrafgerichts zumindest ausserhalb des Amts- und Rechtshilfeverfahrens unzulässig und damit das Vorgehen der Zollverwaltung bundesrechtswidrig sei. Zumal es eine Verwertbarkeit der gespiegelten Daten unter diesen Umständen für ausgeschlossen erachtete, ordnete das Bundesgericht ferner die Vernichtung der gespiegelten Daten sowie die Rückgabe der sichergestellten Datenträger an den Beschuldigten an.

III. Die Erwägungen des Bundesgerichts

6 Das Bundesgericht hält zunächst fest, dass die beschuldigte Person aufgrund des in Art. 14 Ziff. 3 lit. g UNO-Pakt II[2] verankerten und aus Art. 32 BV[3] sowie Art. 6 Ziff. 1 EMRK[4] ableitbaren nemo-tenetur-Grundsatzes nicht zur Herausgabe von Gerätesperrcodes verpflichtet werden kann. In der Folge weist es auf seine gefestigte Rechtsprechung hin, wonach im Entsiegelungsverfahren nicht die Untersuchungsbehörde, sondern das Entsiegelungsgericht mit der Prüfung von allfälligen einer Durchsuchung entgegenstehenden schutzwürdigen Geheimnisinteressen oder anderen gesetzlichen Entsiegelungshindernissen betraut sei.[5]

7 Im Anschluss setzt sich das Bundesgericht mit der von der Beschwerdekammer des Bundesstrafgerichts entwickel-

1 Zum Begriff der Datenspiegelung vgl. ANDREAS J. KELLER, in: Donatsch/Lieber/Summers/Wohlers (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020, Art. 247 StPO N 3a.

2 Internationaler Pakt über bürgerliche und politische Rechte, abgeschlossen in New York am 16. Dezember 1966 (UNO-Pakt II; SR 0.103.2).

3 Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

4 Konvention zum Schutze der Menschenrechte und Grundfreiheiten, abgeschlossen in Rom am 4. November 1950 (EMRK; SR 0.101).

5 BGE 148 IV 221 E. 2.2 f.

ten Praxis betreffend die Entsperrung und Spiegelung von elektronischen Datenträgern im Siegelungsverfahren in allgemeiner Weise auseinander, wobei es sich insbesondere wie folgt verlauten lässt:

8 E. 2.4: *«[…] 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; 142 IV 372 E. 3; 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.»*

9 E. 2.5: *«[…] 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.»*

In Anbetracht des vom Bundesgericht festgestellten Widerspruchs der Praxis der Beschwerdekammer des Bundesstrafgerichts mit der bundesgerichtlichen Rechtsprechung erläutert es darauf das aus seiner Sicht korrekte Vorgehen bei einer Datenspiegelung: 10

E. 2.6: *«[…] 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 Weisungsbefugnisse gegenüber der beauftragten Organisation oder Person verfügt.»* 11

In einem nächsten Schritt wendet sich das Bundesgericht der Anwendung der bundesstrafgerichtlichen Praxis durch die Zollverwaltung im konkreten Fall zu, wobei es namentlich Folgendes ausführt (E. 3.2): *«Aus diesem Ablauf ergibt sich, dass sich die fraglichen drei IT-Geräte nach Eingang des Siegelungsgesuchs […] ungesiegelt in der Hand der Zollverwaltung bzw. des von dieser mit der Entsperrung, Spiegelung und Siegelung beauftragten und dementsprechend weisungsgebundenen fedpol befanden. […] Auch wenn es glaubhaft sein mag, dass die Untersuchungsbehörde vor der Siegelung […] 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 Bundesstrafnoch 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* 12

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.»

13 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. […].*»

14 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 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.*»

15 In einem letzten Schritt zieht das Bundesgericht schliesslich die Konsequenzen aus den obigen Feststellungen, wobei es sich mit Bezug auf die Verwertbarkeit der auf den elektronischen Geräten gespeicherten Daten unter anderem wie folgt äussert:

16 E. 4.1: «*[…] 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 […].*»

17 E. 4.2: «*[…] Im vorliegenden Fall geht es […] 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.*»

IV. Würdigung

1. Einleitende Bemerkungen

18 Vorab sei festgehalten, dass das Urteil des Bundesgerichts im Ergebnis überzeugt. Ausgehend von den Feststellungen des Bundesgerichts zum Siegelungszweck und zur Rechtswidrigkeit der Praxis der Beschwerdekammer des Bundesstrafgerichts wird nachfolgend der Frage nachgegangen, ob bzw. inwieweit sich die Feststellungen des Bundesgerichts im Hinblick auf zukünftige Sicherstellungen von Endgeräten wie Smartphones, Tablets, Laptops etc. verallgemeinern lassen. Darüber hinaus wird untersucht, welche Auswirkungen der vorliegende Entscheid auf die bisherige Praxis zur Delegation von Entsperrungen und Datenspiegelungen seitens des Entsiegelungsgerichts an polizeiliche IT-Forensiker im Rahmen von Strafverfahren hat. Ein letzter Abschnitt befasst sich schliesslich mit den Ausführungen des Bundesgerichts zur Verwertbarkeit der auf den sichergestellten Endgeräten befindlichen Daten.

2. Die Ausführungen des Bundesgerichts zum Siegelungszweck

19 Umstritten war im vorliegenden Fall insbesondere, ob sich die Praxis der Beschwerdekammer des Bundesstrafgerichts mit dem von der Siegelung ausgehenden Schutzzweck vereinbaren lässt. Eine entsprechende Klärung bedingt zunächst die Beantwortung der Frage, was die Siegelung denn überhaupt schützt. Ausgehend von dieser Frage lässt sich festhalten, dass die Siegelung die betroffene Person davor bewahren soll, dass Untersuchungsbehörden Kenntnis von Informationen erlangen, welche von diesen weder durchsucht, beschlagnahmt noch verwertet werden dürfen. Dabei wird regelmässig vorgebracht, dass die Siegelung dem Schutz der Geheim- und Privatsphäre der betroffenen Person diene.[6] Dies ist freilich nicht falsch, greift aber zu kurz. Zwar lässt sich festhalten, dass der Siegelung vorgelagerte Zwangsmassnahmen, wie namentlich Haus- bzw. Personendurchsuchungen

6 Siehe statt vieler OLIVIER THORMANN / BEAT BRECHBÜHL, in: Niggli/Heer/Wiprächtiger (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung/Jugendstrafprozessordnung (StPO/JStPO), 2. Aufl., Basel 2014, Art. 248 StPO N 2 (zit. BSK StPO-BEARBEITER:IN).

oder Editionsbegehren mit einem Eingriff in entsprechende grundrechtliche Positionen verbunden sind.[7] Das Hauptinteresse der siegelungsantragsstellenden Person ist aber regelmässig nicht auf die Verhinderung der Kenntnisnahme von geheimnisgeschützten Daten selbst, sondern vielmehr darauf gerichtet, dass entsprechende Informationen nicht zu Ermittlungs- bzw. zu Beweiszwecken in einem (Verwaltungs-)Strafverfahren verwendet oder verwertet werden können.[8] Im Kern bezieht sich der Schutzzweck der Siegelung damit nicht auf den Schutz der Geheim- und Privatsphäre, sondern vielmehr auf die Verfahrensfairness: Informationen, die aufgrund entsprechender Geheimnisschutzinteressen oder aus anderen Gründen nicht beschlagnahmt oder verwertet werden können, sollen gar nicht erst in die Ermittlungen einfliessen dürfen, zumal dies mit einem ungebührenden Vorteil für die Untersuchungsbehörde verbunden wäre.[9]

20 Wenngleich im vorliegenden Fall keine Anhaltspunkte für eine unzulässige verfrühte Auswertung der Daten im Rahmen der Entsperrung bzw. Datenspiegelung bestanden, erachtete das Bundesgericht aufgrund des von der Beschwerdekammer des Bundesstrafgerichts vorgeschriebenen Vorgehens die Möglichkeit einer unbefugten Einsichtnahme in die infrage stehenden Daten und damit die Erlangung eines entsprechenden ungebührenden Vorteils durch die Zollverwaltung zumindest nicht für ausgeschlossen.[10] Zwar weist die Beschwerdekammer des Bundesstrafgerichts darauf hin, dass die Datenspiegelung nicht mit einer Durchsuchung der auf dem Gerät befindlichen Daten gleichzusetzen sei, da ein allfälliger unbefugter Zugriff durch die Untersuchungsbehörde auf den sichergestellten Datenträger im Zeitraum zwischen Sicherstellung, Entsperrung bzw. Datenspiegelung und Versiegelung der gespiegelten Daten unweigerlich Spuren hinterlassen würde.[11] Zumal aber auch aus den Ausführungen der Beschwerdekammer des Bundesstrafgerichts (zumindest implizit) hervorgeht, dass sich die Löschung bzw. die Manipulation entsprechender Spuren und oder das vorsätzliche Unterlassen der Dokumentation eines unbefugten Zugriffs nicht ausschliessen liesse,[12] ist die vom Bundesgericht getroffene Annahme einer hypothetischen Befangenheit der Zollverwaltung grundsätzlich nicht zu beanstanden. Ausgehend von dieser Annahme konkretisiert das Bundesgericht den Zweck der Siegelung dahingehend, dass damit bereits «jegliche Gelegenheit für die Untersuchungsbehörde zur Kenntnisnahme der sichergestellten Daten» ausgeschlossen werden soll.[13] Da im vorliegenden Fall weder der Beschwerdeführer noch das Bundesstraf- bzw. das Bundesgericht zu kontrollieren vermochten, «wer, wann genau wie Zugang zu den Datenträgern hatte»,[14] kam das Bundesgericht zum Ergebnis, dass sich eine solche Unsicherheit mit einem rechtsstaatlichen Verfahren nicht vertrage, wobei es das an die Praxis der Beschwerdekammer des Bundesstrafgerichts angelehnte behördliche Vorgehen insgesamt für bundesrechtswidrig erachtete.[15] In Anbetracht der Tatsache, dass der im Rahmen einer verfrühten Kenntnisnahme unter Umständen erlangte Vorteil sich nicht zwingend in einem durch das Sachgericht auf seine Verwertbarkeit überprüfbaren Beweis niederschlagen muss, sondern vielmehr auch auf informeller Ebene in Form von Ermittlungs- oder Spurenansätzen bestehen kann,[16] vermögen die Schlussfolgerungen des Bundesgerichts auch in dieser Hinsicht zu überzeugen. Dass sich diese Überlegungen ohne weiteres auch auf strafprozessuale Siegelungskonstellationen übertragen lassen, wird vom Bundesgericht zwar nicht explizit erwähnt, seht aber ausser Frage.[17]

Der Auffassung des Bundesgerichts zufolge lässt sich die 21
Rechtswidrigkeit der Praxis der Beschwerdekammer des Bundesstrafgerichts schliesslich auch dadurch verdeutlichen, dass die in Art. 248 Abs. 2 StPO[18] verankerte Frist zur Stellung des Entsiegelungsgesuchs von der Zollverwaltung offensichtlich nicht eingehalten würde.[19] Dies vermag insofern zu erstaunen, als dass das Bundesgericht trotz der in der Lehre dagegen vorgebrachten Kritik[20]

7 Eingehend dazu MICHAEL AEPLI, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Diss., Zürich et al. 2004, S. 27 ff.

8 Vgl. DAMIAN K. GRAF, Die strafprozessuale Siegelung: Eine Privilegierung von Komödien, Jusletter vom 9. November 2020, Rz. 21.

9 Siehe dazu MARTIN REIMANN, Die strafprozessuale Siegelung, Basel 2022, Rz. 15 ff. und insbesondere Rz. 26.

10 BGE 148 IV 221 E. 2.5.

11 TPF 2020 96 E. 5.1.5, auf welche die Beschwerdekammer in BE.2020.17 E. 2.4.2 verweist.

12 TPF 2020 96 E. 5.1.5.

13 BGE 148 IV 221 E. 2.5.

14 Zwar beteuert die Beschwerdekammer, dass eine unbefugte Datensichtung «eine gegen jede Vernunft sprechende kriminelle Energie auf Seiten des betreffenden IT-Forensikers des fedpols und des untersuchenden Beamten» voraussetzen und sowohl den Grundsätzen der IT-Forensik bzw. dem Grundsatz von Treu und Glauben widersprechen als auch den Tatbestand von Art. 317 StGB (Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 [StGB; SR 311.0]) erfüllen würde (BE.2020.17 E. 2.4.2 unter Hinweis auf die Ausführungen in TPF 2020 96 E. 5.1.). So glaubhaft diese Beteuerungen auch erscheinen mögen, kann von der siegelungsantragsstellenden Person kaum verlangt werden, dass sie der Untersuchungsbehörde in dieser Hinsicht bedingungslos vertraut. Vgl. kritisch dazu auch DENISE WÜST, Nr. 40 Bundesstrafgericht, Beschwerdekammer, Urteil vom 25. Mai 2020 i.S. Eidgenössische Zollverwaltung, Oberzolldirektion gegen A. SA – RR.2019.220, forumpoenale 2021, S. 449.

15 BGE 148 IV 221 E. 2.5, 3.2 und 3.4.

16 REIMANN (Fn. 9), Rz. 26 und Rz. 252.

17 Offen lässt das Bundesgericht hingegen, wie es sich im Amts- und Rechtshilfeverfahren verhält, BGE 148 IV 221 E. 2.7.

18 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO; SR 312.0).

19 BGE 148 IV 221 E. 3.3.

20 LUCIUS RICHARD BLATTNER / NICOLAS LEU / FRIEDRICH FRANK, Länderbericht Schweiz: Aktuelles Wirtschaftsstrafrecht, WiJ 2013, S. 171 ff.

bis anhin davon ausgegangen ist, dass die besagte Frist im verwaltungsstrafrechtlichen Entsiegelungsverfahren keine analoge Geltung erlangt.[21] Ob das Bundesgericht mit seiner Argumentation den Weg für eine entsprechende Analogie geebnet hat, bleibt – mangels eines expliziten Hinweises auf eine entsprechende Praxisänderung – abzuwarten.

3. Ausschliessliche Spiegelungskompetenz des Entsiegelungsgerichts für passwortgeschützte Datenträger?

22 Sofern nun das Bundesgericht aus der Feststellung der Rechtswidrigkeit der Praxis der Beschwerdekammer des Bundesstrafgerichts die Schlussfolgerung zieht, dass im Falle eines Siegelungsantrags die Entsperrung des Endgeräts bzw. die Datenspiegelung zwingend durch das Entsiegelungsgericht vorgenommen werden müsse,[22] stellt sich aber die Frage, ob das Bundesgericht damit den Bogen nicht überspannt:

23 Zwar trifft es zu, dass der beschuldigten Person aufgrund der Verweigerung der Herausgabe des Passworts zu einem sichergestellten Endgerät im Lichte des nemo-tenetur-Grundsatzes keine Nachteile entstehen dürfen.[23] Demgegenüber hat die beschuldigte Person im Rahmen des von der Rechtsordnung vorgegebenen Rahmens behördlichen Zwang, wie etwa die Entsperrung eines passwortgeschützten Mobiltelefons über sich ergehen zu lassen.[24] Dies gilt grundsätzlich auch für nichtbeschuldigte Drittpersonen, die ebenfalls von einer Sicherstellung betroffen sein können.[25] Zumindest wenn die Entsperrung des Endgeräts in Anwesenheit der betroffenen Person vorgenommen werden kann und im Anschluss die Datenspiegelung erfolgt, ist nicht ersichtlich, weshalb dies nicht von der Untersuchungsbehörde vorgenommen werden sollte.[26] Verlangt die betroffene Person die Siegelung, würde sich diese auf die gespiegelten Daten beziehen, die sich auf einem von der Untersuchungsbehörde gestellten Datenträger befänden.[27] Diese Konstellation lässt sich vergleichen mit einem während einer Hausdurchsuchung vorgefundenen Safe, wobei die Herausgabe des Schlüssels vom Inhaber verweigert wird und der Schlüssel anlässlich der Hausdurchsuchung nicht zu Tage gefördert werden kann. Auch in diesem Fall muss sich der Inhaber des Safes gefallen lassen, dass dieser von der Untersuchungsbehörde gewaltsam geöffnet wird, wobei ihm mit Bezug auf allfällige sich im Safe befindlichen Unterlagen ein Siegelungsrecht zukäme. Aufgrund dieser Feststellungen wird deutlich, dass der vom Bundesgericht etablierte kategorische Vorbehalt betreffend die Entsperrung und/oder die Datenspiegelung zugunsten des Entsiegelungsgerichts zu weit geht.

24 Unter Hinweis auf die Gefahr eines Datenverlustes im Falle des Zuwartens mit der Entsperrung bzw. Datenspiegelung bis zum Entsiegelungsverfahren bringt die Beschwerdekammer des Bundesstrafgerichts denn auch zum Ausdruck, dass durchaus triftige Gründe für eine unmittelbare Entsperrungs- bzw. Datenspiegelungskompetenz der Untersuchungsbehörde bestehen.[28] Zum einen verfügen Endgeräte wie Smartphones oder Tablets nämlich regelmässig über eine standardisierte Einrichtung, durch welche vom Benutzer als gelöscht markierte Objekte nach Ablauf einer gewissen Zeitspanne vom Gerät entfernt werden. Ähnliche Löschfunktionen können häufig auch bei der Nutzung von Chat-Diensten eingerichtet werden.[29] Zum anderen ist zu bedenken, dass sich auf einem sichergestellten Endgerät abrufbare Daten – zumindest sofern sie auf externen Servern oder Clouds abgespeichert sind – vom Täter über ein anderes Endgerät gelöscht werden können.[30] Die Wahrscheinlichkeit einer Wiederherstellungsmöglichkeit solcher Daten wird in der Literatur unterschiedlich beurteilt.[31] Vor diesem Hintergrund kann der Zeitpunkt der Datenspiegelung somit von entscheidender Bedeutung sein, weshalb eine frühzeitige Sicherung der Daten im Lichte des Strafverfolgungsinteresses von grosser Wichtigkeit ist.[32] Mit Bezug auf den vom Bundesgericht zu beurteilenden Fall bleibt jedoch anzumerken, dass die Zollverwaltung die Entsperrung der betroffenen Endgeräte erst 20 Tage nach deren

21 BGE 139 IV 246 E. 3.2.

22 BGE 148 IV 221 E. 2.6; befürwortend ANDREW GARBARSKI / DYLAN FROSSARD, Mise sous scellés et copie forensique de données informatiques: la pratique du TPF désavouée par le TF, Verwaltungsstrafrecht.ch vom 21. März 2022.

23 Dies wäre bspw. der Fall, wenn die Verweigerung der Herausgabe eines entsprechenden Codes die Gutheissung des Entsiegelungsgesuchs zur Folge hätte.

24 BGE 142 IV 207 E. 9.4.

25 In solchen Fällen bestehen nach Massgabe von Art. 197 Abs. 2 StPO mit Bezug auf die Verhältnismässigkeit besonders strenge Anforderungen. Auch wenn im VStrR eine entsprechende Bestimmung fehlt, ist doch von einer analogen Geltung auszugehen.

26 Dasselbe muss selbstverständlich gelten, wenn sich die betroffene Person im Vornherein mit der Datenspiegelung einverstanden erklärt. Siehe dazu DAMIAN K. GRAF, Praxishandbuch zur Siegelung, Bern 2022, Rz. 240, der gestützt auf Art. 247 Abs. 3 StPO für die betroffene Person ein Recht auf die Vornahme einer Datenspiegelung ableitet.

27 Vgl. etwa die Konstellation im Urteil des Bundesgerichts 1B_314/2021 vom 27. Juli 2021.

28 TPF 2020 96 E. 5.2.4.

29 GRAF (Fn. 26), Rz. 244.

30 Vorbehalten bleiben freilich technische Mittel der Untersuchungsbehörden, mittels welchen eine externe Löschung verhindert werden kann, siehe dazu sogleich Rz. 26.

31 Siehe dazu WÜST (Fn. 14), S. 449, die davon ausgeht, dass eine Datenwiederherstellung «ohne Weiteres» möglich wäre; a.A. hingegen FABIAN TEICHMANN, Strafprozessrecht und Digitalisierung – Die Siegelung im Sinne von Art. 248 StPO in Zeiten von Signal, Telegram und Threema, forumpoenale 2021, S. 463 f.

32 Vgl. hierzu GRAF (Fn. 26), Rz. 244; In diesem Sinne wohl auch ALEXANDRE GUISAN, Procédure de scellés, copie-miroir des données et inexploitabilité des preuves, crimen.ch vom 7. April 2022, Rz. 21.

Sicherstellung in Auftrag gegeben hatte[33]. Inwiefern unter diesen Umständen angenommen werden kann, dass die Untersuchungsbehörde mit einem drohenden Beweisverlust gerechnet hätte, ist freilich nicht ersichtlich.

25 So wichtig im Allgemeinen aber eine frühzeitige Datensicherung auch sein mag, sind die durch den Siegelungszweck geschützten Interessen der betroffenen Person nicht aus den Augen zu verlieren. Problematisch ist in diesem Zusammenhang, dass die Entsperrung eines passwortgeschützten Endgeräts unter Umständen mehrere Tage bis sogar Wochen in Anspruch nimmt.[34] Vor diesem Hintergrund stellt sich allerdings zunächst die Frage, welche Rolle es im Hinblick auf einen drohenden Beweisverlust denn überhaupt spielt, ob die Entsperrung und anschliessende Datenspiegelung nun unmittelbar von der Untersuchungsbehörde oder erst durch das Entsiegelungsgericht vorgenommen wird.

26 Unerheblich ist dies zweifelsohne bezüglich der Gefahr einer durch die betroffene Person vorgenommene externe Datenlöschung. Unabhängig davon, ob die Untersuchungsbehörde oder das Entsiegelungsgericht die Entsperrung vornimmt, ist in diesem Zusammenhang vielmehr entscheidend, dass unmittelbar nach der Sicherstellung und Versiegelung Massnahmen eingeleitet werden, mit welchen eine externe Löschung verhindert werden kann. Gemäss GRAF lässt sich dies bei Mobiltelefonen durch den Einsatz von faradayschen Käfigen bzw. durch das Versetzen des Mobiltelefons in den Flugmodus erreichen.[35] Letzteres wiederum ist aber nur möglich, wenn das Mobiltelefon im Zeitpunkt der Sicherstellung auch eingeschaltet ist. Sofern sich die Sicherstellung gegen die beschuldigte Person richtet, liesse sich unter der Voraussetzung des Vorliegens eines dringenden Tatverdachts das Risiko einer Datenmanipulation gestützt auf den Haftgrund der Kollusionsgefahr nach Massgabe von Art. 52 Abs. 1 lit. b VStrR[36] bzw. von Art. 221 Abs. 1 lit. b StPO unter Umständen auch durch die Anordnung von Untersuchungshaft abwenden.[37] Neben der Schwere der infrage stehenden Straftat[38] dürfte die Verhältnismässigkeit eines entsprechenden Vorgehens aber namentlich von der Dauer des Entsperrungs- bzw. Datenspiegelungsvorgangs abhängen.

27 Anders verhält es sich hingegen hinsichtlich des Risikos eines Beweisverlustes, das von standardisierten Löschfunktionen ausgeht. In diesen Konstellationen ist entscheidend, dass der Entsperrungsvorgang möglichst rasch vonstattengeht, wobei ein Beweisverlust unter Umständen auch noch abgewendet werden kann, wenn die Entsperrung erst nach einigen Tagen oder Wochen gelingt. Erstreckt sich der Entsperrungsvorgang aber auf eine solche Zeitspanne, so fällt die Möglichkeit der Anwesenheit der betroffenen Person ausser Betracht. Die Vornahme der Entsperrung bzw. der Spiegelung durch die Untersuchungsbehörde erscheint in diesem Fall ausgeschlossen, zumal – wie bereits dargelegt – die Gefahr besteht, dass der von der Siegelung ausgehende Schutzzweck unterlaufen wird, was im Lichte der Verfahrensfairness nicht hinnehmbar wäre.[39] Solange seitens der Untersuchungsbehörde die theoretische Möglichkeit einer unbefugten Einsichtnahme in die gespiegelten Daten besteht, vermag daran auch eine digitale Protokollierung des Entsperrungs- und Spiegelungsvorgangs nichts zu ändern.[40]

28 In solchen Fällen kann dem Rechtsschutz der betroffenen Person nur Rechnung getragen werden, wenn das Entsiegelungsgericht die Entsperrung und Datenspiegelung vornimmt. Um einen drohenden Beweisverlust abzuwenden, müsste es der Untersuchungsbehörde aber immerhin möglich sein, das Entsiegleungsgericht unmittelbar nach der Sicherstellung und Versiegelung des Endgeräts mit dessen Entsperrung und Spiegelung zu befassen. Für ein solches dem Entsiegelungsverfahren vorgelagertes Spiegelungsverfahren fehlt es jedoch sowohl im Straf- als auch im Verwaltungsstrafverfahren an einer gesetzlichen Grundlage.[41] Gerade in Anbetracht der Tatsache, dass die Praxisrelevanz der Sicherstellung von passwortgeschützten Endgeräten in Zukunft kaum abnehmen wird, würde sich die Schaffung einer entsprechenden Grundlage durch eine zusätzliche Anpassung der jüngst revidierten Siegelungsbestimmung in der StPO durchaus anbieten. Als rechtsstaatlich vertretbare Alternative bliebe die Hoffnung auf den technischen Fortschritt, welcher in Zukunft zügige, in Anwesenheit der betroffenen Person vornehmbare Entsperrungs- und Spiegelungsvorgänge garantieren könnte.

33 Vgl. dazu die Sachverhaltsdarstellung des Bundesgerichts zu BGE 148 IV 221.

34 GRAF (Fn. 26), Rz. 253.

35 GRAF (Fn. 26), Rz. 244 Fn. 252.

36 Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (VStrR; SR 313.0).

37 So im Urteil des Bundesgerichts 1B_146/2017 vom 2. Mai 2017 E. 2.2.2.

38 Während Art. 52 Abs. 2 VStrR explizit festhält, dass ein allfälliger Haftbefehl nicht in einem Missverhältnis «zu der Bedeutung der Sache» stehen dürfe, lässt sich dem Wortlaut von Art. 221 Abs. 1 StPO lediglich eine Beschränkung der Untersuchungshaft auf Verbrechen und Vergehen entnehmen. Allerdings lässt sich aus Art. 212 Abs. 3 StPO ableiten, dass die Anordnung der Untersuchungshaft nur bei jenen Straftaten in Frage kommen kann, die wenigstens alternativ mit einer Freiheitsstrafe bedroht sind, siehe auch BSK StPO-FORSTER, Art. 221 N 2.

39 Siehe dazu Rz. 19 ff.

40 Vgl. dazu aber THOMAS HUNKELER et al., Spiegeln oder Siegeln – Ein Dialog, forumpoenale 2022, S. 446.

41 HUNKELER et al. (Fn. 40), S. 444 f.

4. Überlegungen zur Delegation von Datenspiegelungen

29 Was nun die Durchführung der Entsperrung bzw. Datenspiegelung durch das Entsiegelungsgericht anbelangt, hält das Bundesgericht fest, dass damit auch eine spezialisierte Behörde oder private Fachpersonen beauftragt werden könnte. Sofern diese nicht selbst als Untersuchungsbehörde fungiert, hätte die Beschwerdekammer des Bundesstrafgerichts die Entsperrung bzw. Datenspiegelung gemäss der Auffassung des Bundesgerichts im vorliegenden Fall insbesondere auch an die IT-Forensikabteilung von fedpol übertragen können. Entscheidend sei jedoch, 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».[42] Überträgt man die Feststellungen des Bundesgerichts auf den Strafprozess, könnte man sich auf den Standpunkt stellen, dass eine Delegation der Entsperrung bzw. Datenspiegelung der als Entsiegelungsgerichte wirkenden kantonalen Zwangsmassnahmengerichte an die jeweilige polizeiliche IT-Forensikabteilung grundsätzlich nicht infrage käme, zumal die Staatsanwaltschaft als Untersuchungsbehörde regelmässig über Weisungsbefugnisse gegenüber der ihr untergeordneten kantonalen Polizeibehörde verfügt.

30 Ferner liesse sich argumentieren, dass aufgrund der engen personellen Verflechtung zwischen Polizei und Staatsanwaltschaft einer Delegation an polizeiliche IT-Spezialisten ganz generell immer auch ein Hauch an Befangenheit anhaftet.[43] In einem jüngst ergangenen Entscheid hat das Bundesgericht allerdings festgehalten, dass die Delegation der Datenextraktion – auch in diesem Fall ging es um die Vornahme einer Datenspiegelung – durch das Entsiegelungsgericht an die Polizeibehörde zulässig sei, sofern «der mit dem Fall betraute polizeiliche Sachbearbeiter» die Datenauslese nicht selbst vornehme.[44] In dieselbe Richtung geht nun auch die anlässlich der StPO-Revision überarbeitete Siegelungsbestimmung: Gemäss Art. 248*a* Abs. 6 lit. b N-StPO ist nämlich explizit vorgesehen, dass das Entsiegelungsgericht Angehörige der Polizei bezeichnen kann, «um den Zugang zum Inhalt der Aufzeichnungen und Gegenstände zu erhalten oder deren Integrität zu gewährleisten».[45] Die damit einhergehende potentielle Befangenheitsproblematik liesse sich immerhin dahingehend entschärfen, dass der beschuldigten Person die Möglichkeit gewährt würde, einer gestützt auf Art. 248*a* Abs. 6 lit. b N-StPO von der polizeilichen Forensikabteilung vorgenommenen Datenspiegelung beizuwohnen. In Anbetracht der Tatsache, dass gerade die Entsperrung von passwortgeschützten Endgeräten nicht selten erhebliche Dauer in Anspruch nimmt[46], stellt sich die Frage, ob es nicht sinnvoller wäre, die Entsiegelungsgerichte mit eigenen Forensikexperten auszustatten. Dieser Schritt würde sich insbesondere auch im Hinblick auf die Etablierung eines unmittelbar an die Sicherstellung anknüpfenden Spiegelungsverfahrens[47] empfehlen. Alternativ könnte die Schaffung eines spezialisierten gesamtschweizerischen Entsiegelungsgerichts mit eigener IT-Forensikabteilung in Betracht gezogen werden.[48]

5. Konsequenz der Unverwertbarkeit

31 Mit Bezug auf die Folgen der Rechtswidrigkeit der bundesstrafgerichtlichen Praxis hinsichtlich der Verwertbarkeit der infrage stehenden Daten, verweist das Bundesgericht zunächst auf seine im Strafverfahren etablierte Rechtssprechung,[49] wonach die Beurteilung der Verwertbarkeit gemäss Art. 140 f. StPO – mit Ausnahme von Fällen offensichtlicher Unverwertbarkeit – grundsätzlich dem Sachgericht vorbehalten ist.[50] Ob sich diese Praxis bzw. die Verwertbarkeitsprüfung gemäss Art. 140 f. StPO analog auf Verwaltungsstrafverfahren übertragen lässt, wird vom Bundesgericht offengelassen. Zumindest was die absolute Unverwertbarkeit gemäss Art. 141 Abs. 1 StPO betrifft, wird in der Lehre insbesondere unter Hinweis auf das auch im Verwaltungsstrafverfahren geltende Fairness-Gebot für eine analoge Anwendung plädiert.[51] Obwohl sich mit demselben Argument grundsätzlich auch die Regelung betreffend die relative Unverwertbarkeit gemäss Art. 141 Abs. 2 StPO in das Verwaltungsstrafverfahren übertragen liesse, beschränkt sich das Bundesgericht zur Begründung der Unverwertbarkeit auf die Feststellung, dass es sich bei dem Vorgehen der Zollverwaltung um einen erheblichen, nicht mehr korrigierbaren Verfahrensfehler handle.[52] Auch wenn eine Präzisierung des

42 BGE 148 IV 221 E. 2.6.

43 Vgl. dazu auch die Ausführungen des Bundesgerichts in BGE 142 IV 372 E. 3.2.1 f.

44 Urteil des Bundesgerichts 1B_136/2021 vom 9. August 2021 E. 3.4.

45 Siehe Art. 248 Abs. 6 N-StPO gemäss Schlussabstimmung vom 17. Juni 2022.

46 Siehe Rz. 25.

47 Siehe Rz. 28.

48 Vgl. dazu bereits MARTIN REIMANN, Nr. 16 Bundesgericht, I. öffentlichrechtliche Abteilung, Urteil vom 9. August 2021 i.S. A. gegen Staatsanwaltschaft des Kantons Basel-Landschaft – 1B_136/2021, forumpoenale 2022, S. 106

49 Vgl. etwa BGE 142 IV 207 E. 9.8.; BGE 143 IV 387 E. 4.4; Urteil des Bundesgerichts 1B_412/2021 vom 29. November 2021 E. 3.1; Urteil des Bundesgerichts 1B_535/2021 vom 19. Mai 2022 E. 2.2.

50 BGE 148 IV 221 E. 4.1.

51 ANDREA SCHÜTZ / INES MEIER, in: Frank/Eicker/Markwalder/Achermann (Hrsg.), Basler Kommentar, Verwaltungsstrafrecht, Basel 2020, Art. 39 N 56 f.

52 BGE 148 IV 221 E. 4.2.

Bundesgerichts an dieser Stelle sicher wünschenswert gewesen wäre, ist davon auszugehen, dass man bei der Verwertbarkeitsprüfung gemäss Art. 140 f. StPO zu keinem anderen Ergebnis gelangt wäre. Da es sich bei den dem Beschwerdeführer vorgeworfenen Delikten offensichtlich nicht um schwere Straftaten handeln dürfte, würde eine Verwertbarkeit nach Massgabe von Art. 141 Abs. 2 StPO nämlich kaum in Betracht fallen.[53]

V. Fazit

32 Wie eingangs erwähnt, ist der Entscheid des Bundesgerichts mit Bezug auf die Beurteilung der Praxis der Beschwerdekammer des Bundesstrafgerichts nicht zu beanstanden. Während insbesondere die Ausführungen zum Siegelungszweck und der daraus gezogenen Schlussfolgerung der Rechtswidrigkeit der Praxis der Beschwerdekammer des Bundesstrafgerichts überzeugen, erscheint der vom Bundesgericht etablierte kategorische Vorbehalt der Entsperrung bzw. Datenspiegelung zugunsten des Entsiegelungsgerichts nicht zwingend. Sofern die der Untersuchungsbehörde zur Verfügung stehenden technischen Möglichkeiten ein transparentes Vorgehen erlauben, ist nicht ersichtlich, weshalb die Entsperrung bzw. Datenspiegelung nicht durch diese vorgenommen werden soll. Lässt sich die Entsperrung bzw. Datenspiegelung hingegen nicht in Anwesenheit der betroffenen Person vornehmen, ist die Einschaltung des Entsiegelungsgerichts zur Wahrung des Schutzzwecks der Siegelung unumgänglich. Im Interesse einer wirksamen Strafverfolgung würde sich dabei die gesetzliche Verankerung eines dem Entsiegelungsverfahren vorgelagerten, unmittelbar an die Sicherstellung anknüpfenden Spiegelungsverfahrens anbieten. Überzeugend erscheinen demgegenüber wiederum die bundesgerichtlichen Feststellungen betreffend die Delegation der Datenspiegelung, wonach insbesondere auszuschliessen ist, dass die mit der Entsperrung betraute Person von der Untersuchungsbehörde weisungsabhängig ist. Zumal de lege ferenda in Art. 248*a* Abs. 6 lit. b N-StPO explizit verankert, wird sich damit die rechtsstaatlich bedenkliche Delegation der Datenspiegelung an polizeiliche IT-Forensiker im Strafverfahren jedoch nicht verhindern lassen. Aus diesen Gründen wäre es naheliegend, die Entsiegelungsgerichte personell und organisatorisch so auszurüsten, dass diese inskünftig Entsperrungen und Datenspiegelungen von passwortgeschützten Datenträgern selbst vornehmen könnten. Konsequent und begrüssenswert ist schliesslich die vom Bundesgericht getroffene Feststellung betreffend die Unverwertbarkeit der auf den sichergestellten Datenträgern befindlichen Informationen, wobei sich allerdings eine analoge Anwendung von Art. 141 StPO im Verwaltungsstrafverfahren angeboten hätte.

53 Daran vermag auch die neue Praxis des Bundesgerichts nichts zu ändern, wonach die Frage des Vorliegens einer schweren Straftat unter Berücksichtigung der «gesamten Umstände des konkreten Falls» zu beantworten sei (BGE 147 IV 9 E. 1.4.2).

Résumé

Dans son arrêt ATF 148 IV 221, le Tribunal fédéral a déclaré contraire au droit fédéral la pratique de la Cour des plaintes du Tribunal pénal fédéral selon laquelle l'autorité d'instruction peut, dans le cadre d'une procédure d'apposition de scellés, procéder à la copie-miroir de supports de données protégés par un mot de passe ou déléguer ces tâches à la division forensique de l'Office fédéral de la police (fedpol). Bien que le résultat de cette décision ne soit pas critiquable, elle soulève plusieurs questions en ce qui concerne les futures procédures de scellés. Ces questions sont abordées dans cet article, après un résumé des considérants de l'arrêt.