Schreckensszenario oder doch gerechtfertigt?

Maßvoller Zwang bei Sicherstellungen in Österreich – Überlegungen zur datenschutzrechtlichen Einordnung und Darstellungen de lege lata

Theresa Kuk

Abstract

Mit Voranschreiten der technischen Entwicklung ergeben sich neue Möglichkeiten, die auch neue Problemfelder aufzeigen können. Wie ist zu verfahren, wenn ein Endgerät nur mit Face-ID oder Fingerprint entsperrt werden kann? Die KrimPol wendet in solchen Fällen maßvollen Zwang an. Darunter ist zu verstehen, dass der Kopf festgehalten und das Gerät vor das Gesicht gehalten wird oder die Hand des Betroffenen wird genommen, um mit dem Finger das Endgerät zu entsperren. Auf die Daten kann anschließend zugegriffen werden.

Für all jene, die sich mit Datenschutz auseinandersetzen, drängt sich die Frage auf: Liegt eine Verletzung des Datenschutzes vor? Der folgende Beitrag bespricht diesen Sachverhalt aus der Sicht der Strafprozessordnung, der Grundrechtedogmatik und stellt dar, ob die DSGVO den Datenschutz einmahnen kann.

Normenverzeichnis

Art 2 DSGVO, Art 4 DSGVO, ErwGr 19 der DSGVO; RL 2016/680: Art 1, Art 2, Art 3, Art 4, Art 8; ErwGr 26 der RL; § 1 StPO, § 4 StPO, § 5 StPO, § 7 StPO, § 9 StPO, § 48 StPO, § 93 StPO, § 106 StPO, § 110 StPO, § 111 StPO, § 120 StPO, § 154 StPO, § 164 StPO, § 1 DSG, § 36 DSG, § 37 DSG, § 38 DSG, Art 18 B-VG, Art 90 B-VG, Art 6 MRK, Art 8 MRK, Art 47, 48 GRC

Abkürzungsverzeichnis

Abs Absatz
aM andere Meinung
bspw beispielsweise
BPK Bezirkspolizeikommanden
ErwGr Erwägungsgrund
gem gemäß
gg gegen
ggü gegenüber
idR in der Regel
idZ in diesem Zusammenhang
iE im Ergebnis
KrimPol Kriminalpolizei
Lit Literatur
LPD Landespolizeidirektionen
maW mit anderen Worten
MRK Europäische Menschenrechtskonvention
od oder
PI Polizeiinspektionen
PStSG Polizeiliches Staatsschutzgesetz
Rz Randziffer
SPG Sicherheitspolizeigesetz
SPK Stadtpolizeikommanden
Sta Staatsanwaltschaft
StVG Strafvollzugsgesetz
SV Sachverhalt
ua unter anderem
VfGH Verfassungsgerichtshof

25.06.2021

Inhalt

I. Einleitung

In einer modernen, smarten Welt ist auch die Sicherstellung von elektronischen Daten im kriminalpolizeilichen Ermittlungsverfahren geneigt, sich sukzessive zu verändern. Dass die Sicherstellung von Dokumenten in Papierform in den Hintergrund tritt ggü der Sicherstellung von elektronischen Daten, bedarf keiner eigenen Erwähnung. Die Sicherstellung von elektronischem Datenmaterial ist längst in die gängige Praxis eingezogen. Bemerkenswert ist das *wie*; wie ändern sich Zugangsschlüssel, deren rechtlich-dogmatische Einordnung und wie verändern sich dadurch die Zugangsschranken, die von den strafrechtlichen Ermittlern überwunden werden müssen, damit das Datenmaterial ausgewertet werden kann?

II. Strafprozessrechtlicher Rahmen

Die Voraussetzungen für die Sicherstellung

Die Voraussetzungen für die Sicherstellung ergeben sich aus der zentralen Norm § 110 StPO. Der Abs 1 besagt, dass die Sicherstellung zulässig ist, wenn sie aus Beweisgründen erfolgt, der Sicherung privatrechtlicher Ansprüche dient oder zur Sicherung der Konfiskation (§ 19a StGB), des Verfalles (§ 20 StGB), des erweiterten Verfalles (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung.

Vermutet die Sta beweiswertes Material auf dem Datenträger, wird anzunehmen sein, dass sie die Sicherstellung anordnet und die elektronischen Daten anschließend sichergestellt werden. Das leitet über zum Abs 2, welcher besagt, eine Anordnung zur Sicherstellung von (biometrischen) Daten nur von der Staatsanwaltschaft erfolgen darf und diese dann von Beamten der KrimPol durchzuführen ist[1]. Es ist Aufgabe der Staatsanwaltschaft Daten auszuwerten, belastendes oder entlastendes Material zu finden, Entscheidungen zu treffen und das möglichst zeitnah.[2] Vorstellbar ist durchaus, dass sich auf einem Mobiltelefon Material sicherstellen lässt, welches zur Aufklärung von strafrechtlich relevantem

[1] §110 Abs 2 StPO
[2] § 9 Abs 1 Satz 2 StPO

Handeln beiträgt. Diese Beweise sollen in die Verfügungsmacht der Strafverfolgungsbehörden überstellt werden.

Der Abs 3 sieht alternative Tatbestände vor, welche die KrimPol berechtigen, Gegenstände (§ 109 Z lit. a) von sich aus sicherzustellen.[3] Das sind jene Fälle, die weniger grundrechtseingriffsintensiv sind und daher keine Anordnung vorausgehen muss.
Bei schwersten Grundrechtseingriffen ist zusätzlich zur staatsanwaltlichen Anordnung eine gerichtliche Bewilligung erforderlich, wie bei Hausdurchsuchungen oder der Besichtigung des unbekleideten Körpers.[4] Eine Ausnahme hiervon ist, wenn Gefahr im Verzug besteht.[5] Bei Gefahr im Verzug darf die KrimPol ohne eine Anordnung der Sta und ohne vorausgehende gerichtliche Bewilligung eine Durchsuchung vornehmen, die eine Örtlichkeit umfasst, die dem Hausrecht unterliegt, und eine Besichtigung eines unbekleideten Körpers vornehmen. Gefahr im Verzug ist gegeben, wenn durch die Verzögerung der Einholung einer staatsanwaltlichen Anordnung der Gegenstand mutmaßlich zerstört oder weggebracht werden würde[6] oder die Person flüchten könnte[7].

Die Eigenkompetenz der KrimPol ist gem Abs 3 auch dann gegeben, wenn der Gegenstand in niemandes Verfügungsmacht steht, der Gegenstand dem Opfer durch die Straftat entzogen wurde, der Gegenstand am Tatort aufgefunden wurde und dieser zur Begehung der strafbaren Handlung verwendet wurde oder im Versuchsfall, verwendet werden hätte sollen. Die Lit sagt, dass darunter Tatwerkzeuge zu verstehen sind[8], mit welchen die strafbare Handlung gesetzt wurde oder gesetzt hätte werden sollen, im Falle des Versuches.

Die KrimPol darf auch von sich aus sicherstellen, wenn der Gegenstand geringwertig oder vorübergehend leicht ersetzbar ist, der Besitz des Gegenstandes allgemein verboten ist (§ 445a Abs. 1). Der Abs 3 sieht weiter vor, dass die KrimPol von der ihr eingeräumten Eigenkompetenz Gebrauch machen darf, wenn der Gegenstand im Rahmen einer Durchsuchung nach § 120 Abs 2 aufgefunden wurde oder mit denen eine Person festgenommen wird.

Der Abs 4 normiert wann eine Sicherstellung als unzulässig zu sehen ist. Wenn die Bedeutung des sichergestellten Gegenstandes (Mobiltelefon) für die konkrete Untersuchung nicht nachvollziehbar ist,[9] ist sie ein unzulässiger Akt. Bei einem Mobiltelefon, auf welchem sich Chatverläufe etc finden lassen,

[3] *Tipold*/*Zerbes* in *Fuchs*/*Ratz*, WK StPO § 110 (Stand 1.3.2021, rdb.at), Rz 60
[4] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 120 (Stand 1.4.2010, rdb.at), Rz 1
[5] Ebenda Rz 22
[6] Ebenda VfSlg 1.890/1949, 1.811/1949; *S. Mayer*, Commentar §§ 140, 141 und 142 Rz9
[7] Ebenda VfSlg 1.266/1929: Gefahr im Verzug aufgrund einer am gleichen Tag anstehenden Delogierung
[8] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 110 (Stand 1.3.2021, rdb.at), Rz 63
[9] Ebenda Rz 5

ist das aber nicht anzunehmen, da aufgrund des Datenmaterials mögliche Schlüsse gezogen werden könnten, die erheblich für das Ermittlungsverfahren sind.

Worauf stützt sich der maßvolle Zwang durch die KrimPol?

Die Normen §§ 5 iVm 93 Abs 2 iVm Abs 1 iVm 111 Abs 2 iVm Abs 4 StPO sind eindeutig. Sie erlauben in Verbindung gedacht das Vorgehen der KrimPol. Zum § 111 StPO folgt sodann eine nähere Betrachtung, zuvor wird auf die §§ 5, 93 StPO näher eingegangen. Beide Paragraphen sind in der Zusammenschau zu lesen. § 5 StPO normiert, die Gesetz- und Verhältnismäßigkeit. Im Abs 1 sowie im Abs 2 ist ein allgemeines Gebot der Gesetzmäßigkeit und Verhältnismäßigkeit enthalten; es hat einen fundamentalen Charakter.[10] § 5 Abs 1 StPO sieht vor, dass der Eingriff in Rechte von Personen davon abhängig gemacht wird, dass er unter anderem zur Aufgabenerfüllung erforderlich ist. Die Aufgaben bestehen darin, Straftaten aufzuklären und verdächtige Personen zu verfolgen. Das ist auch im § 1 Abs 1 StPO normiert. § 5 Abs 2 StPO knüpft an § 5 Abs 1 StPO an; er verlangt ein angemessenes Verhältnis zwischen den durch den Eingriff beeinträchtigen privaten Interessen und den Strafverfolgungsinteressen.[11]

Wiederin formuliert treffend, dass § 5 StPO fundamentale rechtsstaatliche Erfordernisse an prominenter Stelle in Erinnerung ruft und diese somit gleich am Anfang der StPO wahrt. Diese sind im Abs 1 der Grundsatz der Gesetzmäßigkeit, im Abs 2 der Grundsatz der Verhältnismäßigkeit und im Abs 3 die Tabuisierung des Lockspitzeleinsatzes. Diese drei Rechtspositionen sind bei jeder Eingriffsnorm mitzudenken.[12]

Der § 93 StPO normiert die Zwangsgewalt und Beugemittel. Kraft Gesetz ist die KrimPol ermächtigt, verhältnismäßigen Zwang anzuwenden, um die ihr eingeräumten Befugnisse (idF Durchführung einer staatsanwaltlichen Anordnung) durchzusetzen. Das darf die KrimPol tun, soweit das für ihre Aufgabenerfüllung erforderlich ist. Dem Begriff „Zwang“ kommt ein weites Verständnis zu. Es gibt keine Legaldefinition; gemeint sind jedenfalls Zwangsmaßnahmen, die geeignet sind, die eingeräumte Befugnis auch gg den Willen des Betroffenen durchzusetzen.[13] Jedoch ist unter physischem Zwang keine körperliche Gewaltanwendung zu verstehen.[14] Der Abs 2 ist ggü dem Abs 1 vorranging zu lesen;
Abs 2 normiert, wenn sich eine Person weigert eine Handlung zu setzen, zu welcher sie gesetzlich verpflichtet ist, kann dieses Verhalten durch Zwang nach Abs 1 (…) ersetzt werden. Mit Zwangsgewalt werden Handlungs- und Mitwirkungspflichten durchgesetzt.[15]

§ 93 Abs 1 weist ausdrücklich auf den Grundsatz der Verhältnismäßigkeit hin; es darf nur verhältnismäßiger Zwang angewandt werden. Dieser Grundsatz ist in vielen Bestimmungen der StPO verankert;

[10] *Wiederin* in *Fuchs/Ratz*, WK StPO § 5 (Stand 1.10.2013, rdb.at), Rz 1
[11] Ebenda Rz 7
[12] Ebenda Rz 10
[13] *Vogl* in *Fuchs/Ratz*, WK StPO § 93 (Stand 1.11.2019, rdb.at), Rz 2
[14] Ebenda Rz 4
[15] Ebenda Rz 7

durch die doppelte Verankerung der Verhältnismäßigkeit kann abgeleitet werden, dass bei der Ausübung von Zwang eine besonders sorgfältige Abwägung der Verhältnismäßigkeit vorgenommen wird.[16] Bei Vorliegen einer Rechtsgutbeeinträchtigung ist das angemessene Verhältnis zum angestrebten Erfolg zu wahren.

§ 111 Abs 2 erster Halbsatz StPO (dazu sogleich näher) normiert, dass wenn auf Informationen zugegriffen wird, die auf Datenträgern gespeichert sind, die Person den Zugang zu diesen Informationen zu gewähren hat. Das leitet zu der Frage über, welche Personen Zugang zu gewähren haben.

Bei *wem* kann maßvoller Zwang angewandt werden?

Zu besprechen ist nun weiters, bei wem maßvoller Zwang angewandt werden kann. In dieser Fallkonstellation sind zumindest zwei Personen denkbar: der Beschuldigte und der Betroffene.

DER BESCHULDIGTE[17]

Grundsätzlich sieht § 111 Abs 2 StPO vor, wenn auf Datenträgern gespeicherte Informationen sichergestellt werden sollen, so ist der Zugang zu diesen Informationen zu gewähren. Von der Mitwirkungspflicht bestehen allerdings Ausnahmen.[18] Tritt ein Beschuldigter auf, so ist der Grundsatz *nemo tenetur se ipsum accusare* einschlägig. Das Verbot eines Zwanges zur Selbstbelastung stellt einen fundamentalen Verfahrensgrundsatz dar.[19] Die Aussage eines Beschuldigten ist nicht erzwingbar; er ist nicht verpflichtet an seiner eigenen Tatüberführung mitzuwirken.[20]
Das ergibt sich aus § 7 Abs 2 StPO; der Beschuldigte darf nicht gezwungen werden, sich selbst zu belasten.[21] Den Grundsatz *nemo tenetur se ipsum accusare* leitet der VfGH direkt ab aus Art 90 Abs 2 B-VG.[22]

In der Lit gibt es diesbezüglich einen Streitstand, auf welchen ich verweisen möchte, damit das gedankliche Bild vollständig ist.[23]

[16] *Vogl* in *Fuchs/Ratz*, WK StPO § 93 (Stand 1.11.2019, rdb.at), Rz 16
[17] § 48 Abs 1 Z 2 StPO
[18] Die StPO sieht folgende Ausnahmen vor: § 155 StPO: Vernehmungsverbot, § 156 StPO: Aussagebefreiung, §§ 157, 158 StPO: Aussageverweigerungssrecht
[19] *Seiler*, Strafprozessrecht, 18. Auflage, Rz 373, 374; Die Möglichkeit zur Aussageverweigerung besteht auch dann, wenn durch die Aussage ein Angehöriger der Gefahr einer strafrechtlichen Verfolgung ausgesetzt sein würde.
[20] Ebenda Rz 397
[21] Das Verbot zur Pflicht der Selbstbelastung ergibt sich weiters aus §164 Abs 4 StPO: Vernehmungsgrundsätze; Art 6 MRK: Recht auf ein faires Verfahren; Art 47, 48 GRC; § 5 Abs 3 StPO;
[22] *Seiler*, Strafprozessrecht, 18. Auflage, Rz 397; VfSlg 5295, 9950, 12.454; 18164 ua;
[23] *Wiederin* in *Fuchs/Ratz*, WK StPO § 4 (Stand 1.2.2012, rdb.at), Rz 15-17

Wiederin vertritt nicht, dass aus Art 90 Abs 2 B-VG der besagte Grundsatz abgeleitet werden kann; Art 90 Abs 2 B-VG gewährleistet dem Beschuldigten nicht das Recht, nicht gg sich selbst aussagen zu müssen oder seinen Körper als Beweismittel zur Verfügung zu stellen.
Das Selbstbezichtigungsverbot hat allgemeinen rechtsstaatlichen Gehalt. Daher kann es lt Wiederin nicht im Wege eines Größenschlusses, wie ihn der VfGH bei der Ableitung anwandte, auf Verfahrensordnungen erstreckt werden, die keinen Anklagegrundsatz (§ 4 StPO) kennen. Art 90 Abs 2 B-VG bezieht sich gem dem Wortlaut und seiner Systematik ausschließlich auf das gerichtliche Strafverfahren. Durch die Ableitung gesteht der VfGH ein, dass die rechtsstaatliche Garantie des Selbstbezichtigungsverbotes mit dem Anklageprozess wenig zu tun hat. Art 6 MRK verbürgt sich, anders als Art 90 Abs 2 B-VG, ohnehin für alle strafrechtlichen Systeme.

IE bedeutet das nun für einen Beschuldigten in dieser Fallkonstellation, dass er nicht verpflichtet werden kann, an dem maßvollen Zwang mitzuwirken. Es wäre ein unzulässiger Akt, würde man seinen Kopf festhalten oder seine Hand nehmen um das Endgerät zu entsperren. Sollte sich nämlich beweiswertes Material auf seinem Endgerät auffinden und ist dieses geneigt ihn zu belasten, was im Vorfeld von den Ermittlern allerdings nicht gewusst werden kann, dann hätte er an seiner eigenen Überführung mitgewirkt und das wäre contra legem zu § 7 Abs 2 StPO.[24]

Cracking-Software

Gänzlich unbeholfen sind die Strafverfolgungsbehörden allerdings nicht. Zum Einsatz kommen Cracking- oder Spionage-Software, um den Datenbestand eines Datenträgers auslesen zu können. Das wird als zulässig erachtet, da in der analogen Realität bei einer verschlossenen Schatulle ohne zugehörigen Schlüssel, auch versucht wird, diese Schatulle zu öffnen, etwa mit einem nachgemachten Schlüssel. Der Einsatz der Cracking-Software wird als nachgemachter Schlüssel gesehen und somit als zulässig betrachtet. Die Teleologie der Sicherstellung ist nämlich, das sichergestellte Beweismittel nutzbar zu machen.[25] Das Bearbeiten des sichergestellten Gerätes mit Cracking-Software ist allerdings nur zulässig, wenn die KrimPol mit der Aufforderung der Herausgabe des Zugangsschlüssels keinen Erfolg hat. Erst dann dürfen sie das Gerät cracken.[26]

Für diesen SV bedeutet das, dass ein Beschuldigter nicht verpflichtet werden kann an dem maßvollen Zwang mitzuwirken, jedoch sein Endgerät mittels Cracking-Software bearbeitet werden könnte, weil

[24] Angemerkt soll noch sein, ob einem Beschuldigten ggü überhaupt eine staatsanwaltliche Anordnung vorausgehen würde, wenn von der Beschuldigtenstellung der Person gewusst wird. Die Anordnung könnte in weiterer Folge aufgrund des Verbotes zur Pflicht der Selbstbezichtigung ins Leere laufen.
[25] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 (Stand 1.3.2021, rdb.at), Rz 13/2
[26] Ebenda Rz 13/3

der Zugangsschlüssel (Face-ID, Fingerprint) nicht herausgegeben werden darf, da das § 7 Abs 2 StPO zuwiderliefe.

DER BETROFFENE[27]

Es kann angenommen werden, dass sich beweiswertes Material auch bei von Beschuldigten verschiedenen Personen finden lassen könnte und das sichergestellte Material den Kenntnisstand des Ermittlungsverfahrens voranbringt. Bei einem Betroffenen könnte es sich jedenfalls um einen Zeugen handeln. § 154 StPO normiert den Zeugen und die Wahrheitspflicht. Gem Abs 2 fällt dem Zeugen die Pflicht zu, *richtig und vollständig auszusagen*.

Ruft man § 111 Abs 2 StPO in Erinnerung, ist fraglich, *was* zu gewähren ist, auch im Hinblick auf eine richtige und vollständige Aussage gem § 154 Abs 2 StPO. Muss ein Passwort herausgegeben werden? Und wie wäre das mit anderen elektronischen Zugangsschlüsseln, wie der Face-ID und dem Fingerabdruck?

Gegenstand einer Zeugenbefragung kann jedenfalls sein, dass die Ermittler nach einem Passwort fragen und auch dann ist der Zeuge verpflichtet, *richtig und vollständig auszusagen* und iE das Passwort herauszugeben hat. Die KrimPol muss die virtuellen Zugangsschranken beseitigen, damit ein behördlicher Zugriff auf die Daten erfolgen kann.[28] Eine Person hat demnach grundsätzlich alle Passwörter und sonstigen Zugangsdaten preiszugeben. Ein Passwort ist kein biometrisches Datum iSd Art 4 Z 14 DSGVO oder des Art 3 Z 13 der RL 2016/680 und es ist auch keine Face-ID noch ein Fingerabdruck. Ein Passwort ist jedoch nur sehr wenigen Personen bekannt, wenn überhaupt weiß dieses nur die betreffende Person selbst dh es ist ein Zugangsschlüssel, der versteckbar ist. Das Zwischenergebnis ist, wenn ein versteckbarer elektronischer Zugangsschlüssel verpflichtend herauszugeben ist, dann sind pragmatisch gedacht per analogiam (argumentum a maiori ad minus) „umso eher" auch weitere elektronische Zugangsschlüssel (Gesicht, Fingerabdruck) „herauszugeben", sollten diese auf dem Endgerät bestehen.

Spannend ist idZ, dass wir von geschützten Daten sprechen, jedoch der Zugangsschlüssel (das Gesicht) nicht vernünftig zu verstecken ist und der Fingerabdruck nur begrenzt versteckbar ist (etwa mit einem Handschuh); das Gesicht kann nicht verweigert werden, wie die Herausgabe eines Passwortes. Der Finger kann nur begrenzt verweigert werden; er tritt zutage, wenn bspw der Handschuh ausgezogen wird.[29] [30]

[27] § 48 Abs 1 Z 4 StPO

[28] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 111 (Stand 1.3.2021, rdb.at), Rz 13/1

[29] Notabene, beim Beschuldigten ist der Analogieschluss unzulässig, da diesem das Nemo-Tenetur-Prinzip entgegensteht.

[30] Freilich kann berechtigterweise auch gedacht werden, dass ein Gesicht, ein Finger eo ipso einen erhöhten Schutzbedarf benötigt, gerade weil sie nicht versteckbar, begrenzt versteckbar sind. IE würde das aber in dieser Fallkonstellation der Verhältnismäßigkeitsprüfung zuwiderlaufen, auf welche im Punkt III. eingegangen wird.

IE bedeutet das für einen Zeugen in dieser Fallkonstellation, dass er per analogiam[31] verpflichtet werden kann, an dem maßvollen Zwang mitzuwirken. Es wäre ein zulässiger Akt, würde man seinen Kopf festhalten oder seine Hand nehmen, um das Endgerät zu entsperren.[32] Die Analogieschlüsse sind gestützt auf §§ 111 Abs 2 iVm 154 Abs 2 StPO und bedeuten rechtsdogmatisch, dass die Maßnahme datenschutzrechtlich unproblematisch ist.

Von der Sicherstellung betroffene Person

Gem § 111 Abs 4 StPO ist eine Person, die an der Sicherstellung von elektronischen Daten beteiligt ist, eine Person die von der Sicherstellung betroffen ist, um es mit den Worten des Gesetzgebers zu sagen. Gegenüber dieser betroffenen Person ist die Sicherstellung transparent vorzunehmen. Dem Betroffenen ist eine Bestätigung über die Sicherstellung auszufolgen oder längstens binnen 24 Stunden zuzustellen. Diese Bestätigung hat schriftlich zu erfolgen und ist eine öffentliche Urkunde; zuständig ist die Behörde, welche die Sicherstellung veranlasst hat.
Wurde gem § 110 Abs 2 StPO die Sicherstellung von der Staatsanwaltschaft angeordnet, ist sie die zuständige Behörde. Ansonsten die Sicherheitsbehörde, welcher das Verhalten des Organs zuzurechnen ist.[33] [34]

Die Bestätigung hat auch eine Rechtsbelehrung zu enthalten; sie hat über das Einspruchsrecht zu informieren gem § 106 StPO, sowie über das Recht des Betroffenen, eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung einer Sicherstellung zu beantragen.[35]
Die von der Sicherstellung betroffene Person wird vom Gesetzgeber also nicht alleingelassen und könnte sich notfalls mit Rechtsbehelfen zur Wehr setzen.

[31] *Bydlinski* Grundzüge der juristischen Methodenlehre, 3. Auflage, S 85-86; Es ist eine wirklichkeitsferne Vorstellung anzunehmen, dass eine Gesetzesordnung ohne Lücken entsteht. Der Gesetzgeber lässt aufgrund geringerer praktischer Bedeutung Sachverhalte bewusst ungeregelt, weil diese die Lehre und Rsp per analogiam schließt.
[32] Um einer potenziellen Eskalation vorzubeugen, könnte in der Praxis der maßvolle Zwang durch die KrimPol angekündigt werden oder nachgefragt werden, ob die Person einverstanden ist, wenn die KrimPol von sich aus maßvollen Zwang anwendet. Denkbar ist auch, dass die KrimPol die Person ihr Endgerät selbst entsperren lässt.
[33] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO §111 (Stand 1.3.2021, rdb.at), Rz 22
[34] Art 78a B-VG Sicherheitsbehörden des Bundes
[35] *Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO §111 (Stand 1.3.2021, rdb.at), Rz 24

III. Die grundrechtliche Falllösung

Wendet man auf diesen Sachverhalt nun die Prüfungsformel der allgemeinen Grundrechtedogmatik an, sowie die grundrechtliche Falllösung der unionsrechtlichen Grundrechtecharta, so gelangt man beim Grundrecht auf Datenschutz zu folgendem Ergebnis.

Art 8 MRK normiert die Achtung des Privat- und Familienlebens. Im Abs 2 ist normiert, dass der Eingriff einer öffentlichen Behörde (PI, BPK, SPK, LPD) nur statthaft ist, wenn dieser Eingriff eine Maßnahme darstellt, die (…) *zum Schutz der Rechte und Freiheiten* anderer notwendig ist. Das Festhalten des Kopfes oder dass das Mobiltelefon vor das Gesicht gehalten wird, damit das Endgerät entsperrt wird, ist ein Eingriff, der aufgrund einer Zwangsmaßnahme im Ermittlungsverfahren erfolgt, um Freiheits- und Vermögensrechte Dritter zu schützen, wenn das Datenmaterial im Ermittlungsverfahren zur Aufklärung beiträgt.

Der Begriff *notwendig* muss gelesen werden als Rechtfertigung, warum überhaupt eingegriffen wird. Der Abs 2 des Art 8 MRK sieht einen Katalog an legitimen Zielen vor, die einen Eingriff als verhältnismäßig ausweisen. Diese legitimen Ziele sind zum Beispiel die öffentliche Ruhe und Ordnung oder der Schutz der Rechte und Freiheiten anderer.
Die MRK ist im Denken Fortschrittlicher als unser StGG 1867. Die legitimen Ziele der MRK sind inhaltlich determiniert, das bedeutet, dass ausdrücklich normiert ist, aus welchen Zwecken in das Grundrecht eingegriffen werden kann.
Schreitet man in der grundrechtlichen Fallprüfung weiter voran, so ist Art 8 MRK in Verbindung zu denken mit § 1 DSG. §1 DSG ist die Norm, die das Grundrecht auf Datenschutz gewährleistet.[36]
§ 1 Abs 2 DSG verweist auf die in Art 8 Abs 2 MRK genannten Gründe. Der Gesetzgeber erachtet es demzufolge als legitim, dass das Grundrecht auf Datenschutz zugunsten dieser in Art 8 Abs 2 MRK genannten Gründe zurücktritt.[37]

Der Grundsatz der Verhältnismäßigkeit

Der maßvolle Zwang bei der Sicherstellung von elektronischen Daten durch die KrimPol ist kein Schreckensszenario. Es ist vielmehr von einer verhältnismäßigen Zweck-Mittel-Relation auszugehen. Der legitime Zweck, der verfolgt wird, darf nicht unverhältnismäßig sein zu dem Eingriff in die Freiheitssphäre der betroffenen Grundrechteträger. Der Grundsatz der Verhältnismäßigkeit ist dann gewahrt, wenn seine Bedingungen erfüllt sind. Diese sind, dass der Staat nur aus legitimen Zielen in ein Grundrecht eingreifen darf; das von ihm eingesetzte Mittel muss geeignet sein, dieses Ziel zu

[36] Die DSGVO überlagert seit 25.5.2018 das DSG 2000.
[37] *Gärner*, *Oswald*; Strukturen für die grundrechtliche Falllösung, 2. Auflage, S 29 Datenschutz

erreichen; das eingesetzte Mittel muss zudem notwendig sein und insgesamt muss ein adäquates Verhältnis zwischen dem eingesetzten Mittel und dem Grundrechtseingriff gewahrt bleiben.[38]
Die Sicherstellung ist eine Ermittlungsmaßnahme; ihre Durchführung als auch ihr Umfang müssen dem Grundsatz der Verhältnismäßigkeit genügen.

IV. DSGVO oder RL 2016/680?

Ist die DSGVO anwendbar?

Zu klären ist, ob der sachliche Anwendungsbereich der DSGVO überhaupt eröffnet ist. Art 2 DSGVO normiert diesen und schließt im Abs 2 aus, wann die DSGVO nicht zur Anwendung gelangt. Die Verordnung findet gem Art 2 Abs 2 lit d iVm ErwGr 19 keine Anwendung auf die Verarbeitung personenbezogener Daten, wenn diese von der zuständigen Behörde, die zum Zwecke der Verhütung, der Ermittlung, der Aufdeckung oder Verfolgung von Straftaten (…) diese Daten verarbeitet. Ob überhaupt personenbezogene Daten verarbeitet werden, wird sogleich dargestellt. Personenbezogene Daten, die von Behörden nach dieser Verordnung verarbeitet werden, sollten einem spezifischerem Unionsrechtsakt unterliegen; das ist die RL 2016/680, folgend als RL bezeichnet. [39] Die RL war von den Mitgliedstaaten bis 6. Mai 2018 umzusetzen; Österreich ist dem mit dem Datenschutz-Anpassungsgesetz 2018 nachgekommen.[40]

RL 2016/680

Erfolgt die Datenverarbeitung iSd Art 2 Abs 2 lit d nach der StPO, dem SPG, dem PStSG und dem StVG, ist als Rechtsquelle die Richtlinie 2016/680 heranzuziehen.[41] Die DSGVO kann den Datenschutz nicht einmahnen, da sie nicht zur Anwendung gelangt. Schafft es womöglich diese RL?
Die Richtlinie *zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr* hat gem Art 1 Abs 2 lit a zum Gegenstand, die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen. Der Art 2 Abs 2 der RL 2016/680 normiert den Anwendungsbereich und sieht vor, dass die Richtlinie für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten gilt, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Im nächsten Schritt

[38] *Berka*, Verfassungsrecht, 8. Auflage 2021, Rz 1300
[39] ErwGr 19 der DSGVO
[40] *Bergauer*, Überblick über die österreichische Umsetzung der Richtlinie (EU) 2016/680 für den Bereich der Strafverfolgung, Jahrbuch Datenschutzrecht 2017, 281
[41] *Feiler, Forgó;* EU-DSGVO Kurzkommentar, 2017; S 55, Art 2 Rz 8

ist nun zu klären, ob eine Verarbeitung personenbezogener Daten vorliegt, zuvor pressiert es, auf die Umsetzung der Richtlinie in das österreichische Datenschutzgesetz zu blicken.

Die österreichische Umsetzung der RL 2016/680

Im Datenschutz- Anpassungsgesetz 2018 findet sich im 3. Hauptstück mit dem Titel *Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei einschließlich des polizeilichen Staatsschutzes, des militärischen Eigenschutzes, der Aufklärung und Verfolgung von Straftaten, der Strafvollstreckung und des Maßnahmenvollzugs*
die Umsetzung der Richtlinie.[42] Die Normen stehen seit dem 25.5.2018 im 3. Hauptstück des österreichischen Datenschutzgesetzes (DSG) in Geltung und tragen dem Geist der Richtlinie Rechnung.

Liegt durch die Entsperrung eine Verarbeitung personenbezogener Daten vor iSd RL 2016/680?

Unter *personenbezogenen Daten* sind gem Art 3 Z 1 der RL (§ 36 Abs 2 Z 1 DSG) Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine natürliche Person, wenn ihr Merkmale zuordbar sind, die ihre physische, physiologische, genetische (…) Identität ausdrücken. Das kann bei einer Face-ID, einem Fingerabdruck angenommen werden.

Die RL definiert zudem den Begriff *biometrisches Datum* im Art 3 Z 13 (§ 36 Abs 2 Z 13 DSG). Demnach kann ein biometrisches Datum, wie Gesichtsbilder oder daktyloskopische Daten (Fingerabdruck), mit speziellen technischen Verfahren gewonnen werden und ermöglicht eine eindeutige Identifizierung der natürlichen Person. Auch das ist bei einer Face-ID und einem Fingerabdruck anzunehmen.

Im Art 3 Z 2 der RL (§ 36 Abs 2 Z 2 DSG) ist der Term *Verarbeitung* normiert. Darunter ist ein Vorgang zu verstehen, der mit oder ohne automatisierter Verfahren personenbezogene Daten verarbeitet. Diese Vorgänge sind: das Erheben, das Erfassen, die Organisation, das Ordnen, das Speichern, das Anpassen oder verändern, das Auslesen, das Abfragen, das Verwenden, das Offenlegen durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, das Abgleichen oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten. Jedenfalls einer dieser Vorgänge ist bei biometrischen Entsperrmethoden einschlägig, wie sie bei Mobiltelefonen zum Einsatz kommen.

Wird ein Endgerät mittels Face-ID oder Fingerprint entsperrt, wird ein personenbezogenes Datum verarbeitet; Gesicht und Fingerabdruck sind körperliche Merkmale, die eine Zuordnung zu einer Person

[42] BGBl. I Nr. 120/2017
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig

erlauben. In weiterer Folge wird ein Vorgang angewandt, mit welchem dieses personenbezogene Datum verarbeitet wird, um das Endgerät zu entsperren.

Die Voraussetzungen für die Verarbeitung personenbezogener Daten ergeben sich zumindest aus der Zusammenschau des ErwGr 26 der RL, dem Art 4 der RL (§ 37 DSG) *Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten* und dem Art 8 der RL (§ 38 DSG) *Die Rechtmäßigkeit der Verarbeitung.*
Der Erwägungsgrund 26 besagt, dass jede Verarbeitung personenbezogener Daten auf rechtmäßige Weise erfolgt, auf dem Grundsatz von Treu und Glauben basiert und in einer nachvollziehbaren Weise für die betroffene natürliche Person geschieht.
Der Telos des ErwGr 26 findet sich wieder in den Artikeln 4 (§ 37 DSG) und 8 (§ 38 DSG) der RL.

Art 4 der RL (§ 37 Abs 1 DSG) normiert die Grundsätze, auf welchen eine Datenverarbeitung basiert. Diese entsprechen weitestgehend den Grundsätzen der DSGVO[43] und sind iZm der Verarbeitung personenbezogener Daten zu beachten. In der Richtlinie ist das der Grundsatz der Rechtmäßigkeit und die Verarbeitung nach Treu und Glauben, Zweckbindung, Datenminimierung, Datenrichtigkeit und Speicherbegrenzung.[44]

Wann eine Datenverarbeitung rechtmäßig ist, normiert der Art 8 der RL; er besagt, dass wenn die Verarbeitung zur Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde wahrgenommen wird, dann ist die Verarbeitung personenbezogener Daten zulässig. Art 8 verweist auf Art 1 Abs 1 der RL (§ 36 Abs 1 DSG), der diese Aufgaben normiert; damit geht gleichzeitig auch der Grundsatz der Zweckmäßigkeit einher. Denn Art 1 Abs 1 besagt, dass die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (…) zulässig ist. In unserem Fall können diese Zwecke abgeleitet werden aus § 1 Abs 1 StPO (Zweck: Aufklärung von Straftaten) iVm § 110 Abs 2 StPO (Zweck: Anordnung der Sta durchführen).

Treu und Glauben ist ein eherner Rechtssatz, welcher von den Römern stammt und in die kontinentaleuropäische Rechtskultur übernommen wurde. Er entsprang der römischen *bona fides.*[45] Treu und Glauben sind allgemeine Wertvorstellungen. Im Rechtsverkehr ist darunter die Redlichkeit und Billigkeit der handelnden Personen zu verstehen.[46]

[43] Die DSGVO trat am selben Tag in Kraft, wie die transformierten Normen im 3. Hauptstück des DSG: am 25.5.2018
[44] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 37 (Stand 1.1.2020, rdb.at), Rz 6
[45] *Hausmaninger, Selb*; Römisches Privatrecht, 9. Auflage, S 26 Rechtsgeschichte
[46] Ebenda, S 200 Obligationenrecht

Dass die RL 2016/680 und auch die DSGVO diesen Grundsatz ausdrücklich normiert haben, bedeutet, dass bei der Verarbeitung personenbezogenen Daten die römischrechtliche ethische Wertung der *bona fides* in den Normtexten Einzug gefunden hat und mitzudenken ist.[47]

Der Grundsatz der Datenminimierung besagt in diesem Fall etwas anderes als in der DSGVO, welche aber ohnehin keine Anwendung findet. Die Behörden haben bei der Verarbeitung idR mehr Flexibilität und personenbezogene Daten sollen nur dann verarbeitet werden, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.[48]

Datenrichtigkeit bedeutet, dass Daten stets aktuell, richtig sowie vollständig zu sein haben.[49]

Unter Speicherbegrenzung ist zu verstehen, dass Daten nicht länger als nötig gespeichert werden.[50]

Art 8 der RL (§ 38 DSG) sieht die Rechtmäßigkeit der Datenverarbeitung vor. Dafür bedarf es ausnahmslos eine gesetzliche Grundlage. Damit die lebenswichtigen Interessen von Personen gewahrt sind, ist eine gesetzliche Regelung geboten. Den Strafverfolgungsbehörden sollten keine zusätzlichen Einschränkungen auferlegt werden. § 38 DSG gewährleistet, dass die Verarbeitung der Daten erforderlich und verhältnismäßig erfolgt.[51]
Einschlägig sind idF folgende gesetzlichen Grundlagen, wie bereits ausgeführt: § 1 Abs 1 StPO iVm § 110 Abs 2 StPO iVm § 111 Abs 2 StPO iVm § 154 Abs 2 StPO.[52]

Das Erfordernis einer gesetzlichen Grundlage ergibt sich innerstaatlich gesehen auch aus dem Legalitätsprinzip des Art 18 B-VG.[53]

IE sind die Voraussetzungen für die Verarbeitung personenbezogener Daten jedenfalls gegeben.

Festzuhalten ist, dass bei der Anwendung des maßvollen Zwanges durch die KrimPol (Vorhalten des Endgerätes, Nehmen des Fingers) durch den ausgelösten biometrischen Entsperrvorgang gem der Richtlinie ein personenbezogenes und ein biometrisches Datum verarbeitet wird und diese auch zur Identifizierung einer natürlichen Person geeignet sind. Jedoch findet die Verarbeitung nicht zum

[47] Ebenda S 28 Rechtsbegriff und Rechtsschichten
[48] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 37 (Stand 1.1.2020, rdb.at), Rz 8
[49] Ebenda Rz 9
[50] Ebenda Rz 10
[51] *Thiele/Wagner*, Praxiskommentar zum Datenschutzgesetz (DSG) § 38 (Stand 1.1.2020, rdb.at), Rz 4
[52] Ebenda Rz 11: Eine nationale Rechtsgrundlage ist dann tauglich, wenn sie den *»Rang eines Gesetzes«* aufweist. Es kommen nur Landes- oder Bundesgesetze (einschließlich der im Verfassungsrang stehenden Normen) in Betracht.
[53] Ebenda Rz 6

Zwecke der Identifizierung einer natürlichen Person statt. Für die polizeilichen Ermittler sind das personenbezogene Datum und das biometrische Datum von geringerer Relevanz als das sicherzustellende Datenmaterial, da dieses beweiswerter sein könnte und so dem Ermittlungsverfahren neue Kenntnisse zuführen kann als die personenbezogenen und die biometrischen Daten als solche.

Abschließend ist die Frage zu beantworten, ob die RL es schafft den Datenschutz einzumahnen? Summa summarum gibt es nichts einzumahnen, wenn diese Fallkonstellation und die RL 2016/680 mit Augenmaß betrachtet wird. Nicht überall, wo Daten verarbeitet werden, liegt auch eine Verletzung des Datenschutzes vor, noch ist das Grundrecht auf Datenschutz gem § 1 DSG verletzt. [54] [55] Wenn die Verhältnismäßigkeit gewahrt ist, ist ein Grundrecht (auf Datenschutz) nicht verletzt.

VII. Schluss

Prima vista kann man sich bei diesem Sachverhalt fragen, wozu es sich überhaupt lohnt darüber nachzudenken? Zurzeit ist das eine theoretische Diskussion.[56] Nimmt der Einsatz und die Anwendung der biometrischen Daten zu, könnten neue Gedanken auftauchen, die juristisch einzuordnen sind. Zweifelsohne birgt die Technologie das Potenzial, gesamtgesellschaftliche Auswirkungen mit ihrem Fortschritt zu prägen.

Schlussendlich ergibt sich ein erwartungsvoller Ausblick in die Zukunft wie sich der Umgang mit biometrischen Daten weiter entwickeln wird und insbesondere welche (und ob neue?) juristische Lösungen bereitgestellt werden.

[54] „Es gibt ähnliche Fälle, in welchen auf die körperliche Integrität eingewirkt wird, um biometrisches Material und in weiterer Folge auch Daten zu gewinnen. Bspw bei erzwungenem Atemalkoholtest oder der Blutabnahme und das wurde datenschutzrechtlich noch nie als überschießend wahrgenommen.“ So Univ.-Prof. Dr. Nikolaus Forgó auf Nachfrage im Seminar „Aktuelle Fragen des IT-Rechts für Diplomand*innen im SS 2021“.
[55] Zustimmend auch Ass.-Prof. Dr. Farsam Salimi, in der Übung aus Strafrecht- und Strafprozessrecht am 31.05.2021 auf Nachfrage: „Alles was die KrimPol tut ist ein Eingriff in den Datenschutz.“

[56] *Salimi* hat auf Nachfrage noch angemerkt, dass die oben beschriebene Situation bislang rein theoretisch überlegt wird; in der Praxis wird das eher nicht angewandt, da es noch als zu heikel empfunden wird. Das impliziert nach meinem Verständnis, dass man sich unsicher fühlt und deshalb im Zweifel lieber davon ablässt. Diese Situation ist lt Salimi sehr unbefriedigend, da es davon abhängt, ob die Person „mitspielt“ oder nicht. Freilich könnte der Gesetzgeber sachgerecht eine Regelung zu einer Verhaltensanordnung schaffen, die sich von den im Kapitel V. genannten Normen unterscheidet und eine eindeutige Interpretation zulässt.