Autor: MMag. Dr. Christopher Schrank

Sicherstellung von Smartphones mit Fingerabdruck oder Face-ID

Christopher Schrank
ist Partner der Brandl & Talos Rechtsanwälte GmbH und auf Gesellschafts- und Wirtschaftsstrafrecht sowie Corporate Compliance spezialisiert

In Strafverfahren sind Mobiltelefone vielfach ergiebige Informationsquellen für Ermittlungsbehörden. Smartphones der neuesten Generation können nunmehr über einen Fingerabdrucksensor oder mittels Gesichtserkennung entsperrt werden. Was aus technischer Sicht sicher sinnvoll ist, kann bei Hausdurchsuchungen allerdings ein Nachteil sein: Es ist nämlich davon auszugehen, dass die Ermittler die biometrischen Merkmale des Verfügungsberechtigten nutzen dürfen, um das Gerät zu entsperren.

Keine Herausgabe von Passwörtern

Im Rahmen des Ermittlungsverfahrens ist es für die Strafverfolgungsbehörden wichtig, rasch an die relevanten Unterlagen und Informationen zu gelangen und diese zu sichern. Der Fokus der Ermittler liegt dabei zunehmend auf digitalen Datenträgern wie etwa Smartphones oder Laptops, weil gerade auf diesen Geräten oft Unmengen an (zum Teil sehr persönlichen und damit aussagekräftigen) Daten gespeichert sind. Allerdings sind diese elektronischen Geräte nur dann für die Beamten hilfreich, wenn sie entsperrt werden können. Bei Laptops und Mobiltelefonen erfolgt dies in aller Regel mittels Passwort. Diesbezüglich ist klar, dass Wirtschaftsprüfer, gegen die ermittelt wird, nicht verpflichtet sind, das Passwort herauszugeben. Vielmehr greift das sogenannte nemo-tenetur-Prinzip, wonach kein Beschuldigter gezwungen werden darf, sich selbst zu belasten oder gegen ihn sprechende Beweismittel aktiv herauszugeben (siehe dazu auch iwp journal 1/2020, 30).

Entsperren mittels biometrischer Verfahren

Anders ist die Situation bei Geräten, die mittels biometrischer Verfahren entsperrt werden können. Hier ermöglichen die technischen Gegebenheiten den Ermittlern schon rein faktisch weitere Handlungsspielräume. Denn während die Ausübung von Zwang zur Erlangung der Zugangsdaten des Beschuldigten unzulässig ist, bilden biometrische Verfahren der Zugangskennung einen Sonderfall. Die Ermittler müssen dabei nämlich nicht den Beschuldigten nach dem Zugangscode befragen oder ihn auffordern, diesen einzugeben. Stattdessen nutzen sie schlicht körperliche Merkmale des Beschuldigten, um einen vorab programmierten Entschlüsselungsmechanismus zu aktivieren. So wäre es etwa denkbar, dass die Ermittler den Finger des Beschuldigten auf einen im Gerät selbst integrierten Fingerabdrucksensor drücken oder das Smartphone des Beschuldigten vor dessen Gesicht halten, um eine Gesichtserkennung (Face-ID) zu aktivieren.

Fraglich bleibt, ob eine solche Vorgehensweise zulässig ist. In Österreich gibt es dazu weder Literatur noch Judikatur. Erste Auseinandersetzungen mit diesem Thema gibt es allerdings in Deutschland, wobei dort die Zulässigkeit der Nutzung biometrischer Verfahren grundsätzlich bejaht wird. Dieses Ergebnis wird auch auf die österreichische Rechtslage zutreffen. Grund dafür ist in erster Linie der Umstand, dass biometrische Merkmale kein (neues) selbstbelastendes Material bilden. Vielmehr bestehen diese Merkmale unabhängig vom Willen des Beschuldigten (der Beschuldigte hat einen Fingerabdruck, ob er will oder nicht) und es bedarf auch keiner aktiven Mitwirkung des Beschuldigten zur Erlangung dieser Beweismaterialien. Genauso wie die Kriminalpolizei also den Fingerabdruck eines Beschuldigten abnehmen darf (§ 118 Abs 2 StPO), darf sie diesen auch direkt auf einen Fingerabdrucksensor halten. Gleiches muss sinngemäß auch für Iris- und Gesichtserkennungen (zB Face-ID) gelten. Hier wird nämlich wiederum ein bloßes Dulden des Beschuldigten (und damit kein aktives Handeln) gefordert. Das nemo-tenetur-Prinzip wird dadurch nicht verletzt.

Praxistipp

Für die Praxis bedeutet das: Möchte man den Ermittlern kein leichtes Spiel im Umgang mit verschlüsselten Daten bieten, greift man auf den altbewährten Passwortschutz zurück. Dies gilt im Übrigen nicht nur für die Verschlüsselung des Homescreens. Da selbst Apps mittlerweile Zugang mittels Fingerabdruck oder Face-ID ermöglichen, ist auch hier Vorsicht geboten.

Kontaktadresse:
schrank@btp.at