LEGALER SCHWINDEL DER JUSTIZ

DIGITALE DATEIN ALS BEWEISMITTEL

Legaler Schwindel der Justiz -
Digitale Beweismittel

Der AKP Faschismus bestraft Oppositionelle, Revolutionäre und Antifaschisten, die er mit Polizeikomplotten festnehmen lässt und diese mit Hilfe seiner Staatsanwälte und Richter „verurteilt."

Digitale Beweismittel und der Geheimzeugen-Schwindel ist die effektivste Waffe des AKP Faschismus im Kampf gegen die Bevölkerung und Revolutionäre. Gefälschte digitale Beweismittel, sogenannte Geheimzeugen, deren Identität nicht veröffentlicht wird, sowie verfälschte Aussagen bilden die Grundlage der Justizkomplotte.

Bei den Schauprozessen werden Revolutionäre, Antifaschisten und Oppositionelle zu hohen Haftstrafen verurteilt.

1. Was sind digitale/elektronische Beweismittel?

Elektronische (digitale) Beweismittel sind alle möglichen Formen von Daten, die auf einem elektronischen Gerät gespeichert, oder mithilfe solcher Geräte transferiert werden können und für Strafprozesse von Bedeutung sind. Alle elektronischen Daten, die in einem digitalen Umfeld, z.B. auf einer Festplatte, einem USB-Stick, einem Handyspeicher oder sonstigem Massenspeichergerät vorhanden sind (z.B. Texte, Bilder, Videos, Sprachaufzeichnungen etc.). Solche Daten sind, sofern sie vertrauenswürdig sind, als digitale Beweismittel in Betracht zu ziehen.

Da digitale Beweismittel eine empfindliche Struktur aufweisen und jegliche Art der Intervention in Form von inhaltlicher Abänderung möglich ist, sind diese Beweismittel auch in Bezug auf die juristische Glaubwürdigkeit höchst sensibel. Deswegen unterliegt ihre Erlangung, ihre Sicherstellung, die Auswertung und ihre Einführung in Strafprozessen gewissen Regeln, die beachtet werden müssen.

Sollten diese Regeln nicht befolgt werden:
-Können diese Beweismittel verschwinden
-Sie können ihre Beweiskraft verwirken,
-oder ihre Einführung in Strafprozesse wird diskutierbar.

2. Die Nutzung digitaler/elektronischer Daten als Beweismittel

Beispiele für digitale Beweismittel sind: Ordner, Chatverläufe, Webseiten, gelöschte und wiedererlangte Ordner, digitale Bilder und Videos, Emails, Browserverläufe, Abonnements.

Damit eine digitale Datei als Beweismittel eingesetzt werden kann, muss diese Datei zwangsläufig von ihrer Sicherstellung bis hin zur Einführung in den Strafprozess sowohl technisch als auch juristisch kontrolliert werden können. Nur so kann sichergestellt werden, dass diese Datei ihren Beweischarakter nicht verwirkt.

Der Prozess von der Erlangung, Sicherstellung, Analysierung und der Einführung in den Strafprozess unter juristischen und wissenschaftlichen Gesichtspunkten wird Forensik genannt.

Im forensischen Prozess wird die Untersuchung von Geräten, auf denen digitale Beweismittel vermutet werden, wie z.B. Festplatten, USB-Sticks, SD-Karten oder anderen Massenspeichergeräten, in einem gesicherten Umfeld durchgeführt. Die Beweisaufnahme wird auf authentischen (1 zu 1) Kopien der Originaldateien durchgeführt. Diese Kopien nennt man Speicherabbild.

Das Kopieren der Originaldateien wird mit der Zuweisung eines Hashwertes (digitaler Fingerabdruck einer Datei) abgeschlossen und es ist verpflichtend, dass dieser Vorgang lückenlos protokolliert wird. Aber auch dieser Vorgang ist nicht ausreichend. Um die Beweisauthentizität zu wahren und sowohl die technische, als auch die juristische Kontrolle darüber zu gewährleisten:

-Muss das Kopieren, sowie das Erstellen des Hashwertes im Beisein des Beschuldigten bzw. seiner Verteidigung geschehen,
-eine Kopie der Datei, also ein Speicherabbild, muss nach Erstellung dem Beschuldigten oder seinem Verteidiger zur Verfügung gestellt werden und
-es ist verpflichtend, dass die Analyse der sichergestellten Datei auf dem Speicherabbild und nicht auf dem Original durchgeführt wird.

Der § 134 Abs. 3 des türkischen Strafgesetzbuches besagt folgendes in Bezug auf digitale Beweismittel: Die Erstellung von Speicherabbildungen von Dateien auf Massenspeichergeräten wie Festplatten, USB-Sticks oder SD Karten muss während der Sicherstellung des Gerätes durchgeführt werden.

Bei der Sicherstellung, z.B. eines Laptops, müsste also ein Speicherabbild angefertigt werden und die Originaldatei dem Beschuldigten oder seiner Verteidigung unverzüglich ausgehändigt werden. Wird das Kopieren der Originaldatei, also die Erstellung des Speicherabbildes, erst im Nachhinein durchgeführt, könnten die Dateien in der Zwischenzeit abgeändert worden sein. Aufgrund dieser Möglichkeit verwirken sie ihren Beweismittelcharakter.

In der Computer-Forensik besteht keine andere Möglichkeit, digitale Beweismittel zu schützen, als die Erstellung des Speicherabbilds unmittelbar nach Sicherstellung des Datenträgers durchzuführen und einen Hashwert zu erstellen, der dem Beschuldigten oder seiner Verteidigung unverzüglich ausgehändigt wird.

Cetin Arslan, Staatsanwalt am Obersten Gerichtshof der Türkei, beschreibt dies wie folgt:
„Ein anderer Aspekt von digitalen Beweismitteln ist ihre Glaubwürdigkeit. Die Schwierigkeiten bei der Identifizierung der Zugehörigkeit der Dateien und die Möglichkeit der nachträglichen Abänderung machen digitale Beweismittel zum schwächsten Glied der Beweisführungskette. So sehr digitale Beweismittel auch den Anschein erwecken, dass sie ein Ereignis erklären oder stichhaltige Hinweise liefern, besteht jedoch keine Möglichkeit, diese Dateien für sich genommen als Beweismittel zu benutzen, da es oftmals nicht möglich ist, sicherzustellen, ob und wann diese Dateien hergestellt wurden und ob der Inhalt nach Sicherstellung abgeändert wurde oder nicht. Deswegen ist es zwingend notwendig, diese Beweismittel mit anderen Beweismitteln im Kontext zu benutzen.“

3. Warum sind digitale Beweismittel nicht vertrauenswürdig und warum können sie nicht als Beweismittel benutzt werden?

Dateien, die in einem digitalen Umfeld hergestellt wurden, können sowohl im Inhalt als auch im Bezug auf Metadateien, ohne großen Aufwand und völlig unbemerkt verändert werden. Die Einsicht darüber, ob sichergestellte Dateien im Nachhinein abgeändert wurden oder nicht, ist nur möglich, wenn ein Speicherabbild und ein Hashwert bei der Sicherstellung des Beweismittels erstellt und dem Beschuldigten oder seiner Verteidigung zur Verfügung gestellt wird. Jedes Speicherabbild ist eine exakte Kopie der Datei im Zeitpunkt der Sicherstellung. Sollte dieses Speicherabbild zum Zeitpunkt der Sicherstellung nicht erstellt werden, ist es daher nicht möglich, die sichergestellte Datei mit einer Kopie zu einem späteren Zeitpunkt abzugleichen, da die Datei in der Zwischenzeit abgeändert worden sein kann. So sind Dateien, die abgeändert wurden, um einen Prozess in einer bestimmten Richtung zu beeinflussen und von denen man nicht weiß, wo sie erstellt wurden, beinhalten keine Einsicht über die Abänderung.
Die 16.Strafkammer des Obersten Gerichtshof der Türkei hat im Ergenekon Prozess folgende Kriterien für digitale Beweismittel eingeführt:

-Bei Sicherstellung der Dateien muss ein Speicherabbild und ein Hashwert erstellt werden.

-Eine Kopie des Speicherabbilds muss dem Beschuldigten oder seinem Anwalt zur Verfügung gestellt werden.

-Sollte während der Sicherstellung die Erstellung eines Speicherabbilds nicht möglich sein, müssen die Seriennummern protokolliert werden und die Datenträger müssen in einer Form verschlossen werden, die den Schutz vor Abänderung zweifellos sicherstellt.

-Sollte der Beschuldigte oder der Verteidiger darauf bestehen, so muss sichergestellt werden, dass sie bei der Erstellung des Speicherabbilds anwesend sind.

-Sobald sichergestellt wird, dass der Beschuldigte oder sein Verteidiger anwesend sind, muss der verschlossene Datenträger unverzüglich bereitgestellt und das Speicherabbild erstellt werden.

-Nach der Erstellung des Speicherabbildes muss das Original, sowie das Speicherabbild der Datei, dem Beschuldigten oder seiner Verteidigung zur Einsicht zur Verfügung gestellt werden.

-Sollte die Anwesenheit des Beschuldigten oder seiner Verteidiger zum Zeitpunkt der Erstellung des Speicherabbilds nicht gewährleistet werden können, muss dieser Vorgang in Anwesenheit des Richters durchgeführt werden, der die Sicherstellung des Mediums veranlasst hat.

Die 16.Strafkammer des Obersten Gerichtshofes hat festgestellt, dass die Sicherstellung und Analyse von Dateien nur nach diesen Vorgaben durchgeführt werden darf und dass die Dateien andernfalls nicht als Beweismittel zulässig sind. Es wurde offen darauf hingewiesen, dass solche streitbaren Beweismittel nicht in die Entscheidung des Gerichts einfließen werden.

4. Worauf muss bei digitalen Beweismitteln geachtet werden?

-Wurden die digitalen Beweismittel regelkonform sichergestellt?
-Wie verlief die Sicherstellung der Dateien? Die Protokolle müssen sorgfältig überprüft werden.
-Wurde im Zuge der Sicherstellung ein Speicherabbild erstellt? Wann wurde dies exakt getan?
-Wurde die Erstellung des Speicherabbilds in Anwesehnheit der Beschuldigten bzw. der Verteidigung durchgeführt?
-Wurde eine Kopie des Speicherabbildes dem Beschuldigten oder der Verteidigung zur Verfügung gestellt?
-Wurde die Analyse auf dem Speicherabbild vorgenommen?
-Wieviel Zeit ist zwischen der Sicherstellung, der Erstellung des Speicherabbilds sowie der Analyse der Dateien vergangen?
-Wo befinden sich die Originaldateien?
-Sollte die Sicherstellung nicht regelkonform durchgeführt worden sein, dürfen diese Beweismittel nicht benutzt werden, denn es ist nicht nachvollziehbar, ob diese Dateien im Nachhinein verändert wurden.


FREIHEIT FÜR ALLE
ANTIFASCHISTISCHEN &
REVOLUTIONÄREN GEFANGENEN
WEG MIT DEM PARAGRAFEN 129 A & B
E-MAIL: FREEGRUPYORUM@GMAIL.COM
TWITTER: @NAZIPARAGRAF129
FACEBOOK: UMUT TV DEUTSCH
WEBSITE: ANTIIMPERIALISSTRUGGLE.NOBLOGS.ORG