SORGFALTSMASSSTÄBE BEI DER ERHEBUNG UND BEWERTUNG ELEKTRONISCHER BEWEISMITTEL

Thomas Hrdinka

Zivilingenieur, Universität Wien, Arbeitsgruppe Rechtsinformatik
Ocwirkgasse 22, 1210 Wien, AT
thrdinka@zth.at; http://www.zth.at

Schlagworte: ***Elektronische Beweismittel, Spuren, IT-Forensik, StPO***

Abstract: *Vielfach wird in Strafverfahren ein bereits von den Ermittlungsbehörden und Staatsanwaltschaft erhobener Sachverhalt nicht mehr hinterfragt, da die Beweislage einerseits von zur Objektivität verpflichteten Organen erhoben wurde, und wenn andererseits die Beweise und Beweisketten als schlüssig erscheinen. Sehr strenge Bestimmungen sollen einen hohen Qualitätsmaßstab bei der Aufklärung von Straftaten, über die Verfolgung verdächtiger Personen und damit zusammenhängenden Entscheidungen gewährleisten. Trotzdem entstehen manchmal Pannen bei der Ermittlung, welche sich dann im Laufe des Verfahrens manifestieren, und schließlich zu einer fehlerhaften Beweiswürdigung führen können. Diese Publikation zeigt exemplarische Fälle, wo elektronische Beweismittel eine wesentliche Rolle zur Aufklärung der Tat spielten.*

1. Einleitung

Gem. § 3 StPO[1] haben Kriminalpolizei, Staatsanwaltschaft und Gericht die Wahrheit zu erforschen und alle Tatsachen aufzuklären, die für die Beurteilung der Tat und des Beschuldigten von Bedeutung sind. Alle Richter, Staatsanwälte und kriminalpolizeilichen Organe haben ihr Amt unparteilich und unvoreingenommen auszuüben und jeden Anschein der Befangenheit zu vermeiden. Sie haben die zur Belastung und die zur Verteidigung des Beschuldigten dienenden Umstände mit der gleichen Sorgfalt zu ermitteln. Diese zentrale Bestimmung regelt die Unparteilichkeit, Unvoreingenommenheit und die Sorgfaltspflichten für die involvierten Organe. Gem. § 126 Abs. 1 StPO sind Sachverständige zu bestellen, wenn für Ermittlungen oder für Beweisaufnahmen besonderes Fachwissen erforderlich ist, über welches die Strafverfolgungsbehörden durch ihre Organe, besondere Einrichtungen oder bei ihnen dauernd angestellte Personen nicht verfügen.

Sachverständiger ist gem. § 125 Z. 1 leg.cit. eine Person, die auf Grund besonderen Fachwissens in der Lage ist, beweiserhebliche Tatsachen festzustellen oder aus diesen rechtsrelevante Schlüsse zu ziehen und sie zu begründen. Die erhöhten Sorgfaltspflichten von Sachverständigen, und das gilt nicht nur für Gerichtssachverständige, sind im § 1300 ABGB[2] geregelt, indem ein Sachverständiger auch dann verantwortlich ist, wenn er gegen Belohnung in Angelegenheiten seiner Kunst oder Wissenschaft aus Versehen einen nachteiligen Rat erteilt. Gem. Punkt 1.1 der Standesregeln[3] des Hauptverbandes der Allgemein beeideten und zertifizierten Sachverständigen Österreichs, welche für Gerichtsgutachter als bindend[4] gelten, sind gerichtliche Sachverständige ein unabhängiges, zur Objektivität und Unparteilichkeit verpflichtetes Hilfsorgan des Gerichtes und der

1 Strafprozessordnung, BGBl. 631/1975, i.d.g.F.
2 Allgemeines bürgerliches Gesetzbuch, JGS. 946/1811, i.d.g.F.
3 https://www.gerichts-sv.at/download/Standesregeln_2014.pdf, gelesen am 06.10.2021.
4 Mitteilung des Bundesministerium für Justiz vom 6. September 2013, BMJZ11.856/005-I 6/2013: „*Die Einhaltung der in den Standesregeln enthaltenen Verhaltensregeln kann aufgrund der ihnen zugestandenen allgemeinen Gültigkeit von allen bei Gericht oder der Staatsanwaltschaft tätig werdenden Sachverständigen verlangt werden.*“

Staatsanwaltschaft und als solches Teil der Rechtspflege. Lt. Punkt 1.2 haben sie daher sowohl im Verfahren vor den Gerichten, Staatsanwaltschaften und Verwaltungsbehörden, aber auch als Privatgutachter die Gegenstände eines Augenscheins sorgfältig zu untersuchen, die gemachten Wahrnehmungen aus Augenschein und Aktenlage treu und vollständig anzugeben und den Befund und das Gutachten nach bestem Wissen und Gewissen und nach den Regeln der Wissenschaft, der Kunst, der Technik, des Gewerbes oder ihres Fachgebiets abzugeben. In den Standesregeln werden damit die erhöhten Sorgfaltspflichten als auch die Objektivität und Unparteilichkeit in Analogie zu den gleichlautenden Verpflichtungen der Organe gem. StPO bestimmt.

2. Elektronische Beweismittel: Definition und Eigenheiten

Nach dem Unmittelbarkeitsprinzip lt. § 13 StPO „*sind alle Beweise aufzunehmen, auf Grund deren das Urteil zu fällen ist. Im Ermittlungsverfahren sind die Beweise aufzunehmen, die für die Entscheidung über die Erhebung der Anklage unerlässlich sind oder deren Aufnahme in der Hauptverhandlung aus tatsächlichen oder rechtlichen Gründen voraussichtlich nicht möglich sein wird.*“ Die StPO sieht folgende Beweismittel vor: Vernehmung der Angeklagten, Vernehmung von Zeugen und Sachverständigen, die Kontradiktorische Vernehmung, die Verwertung von **Urkunden** und den Augenschein. Dabei wird nicht zw. Elektronischen bzw. digitalen und sonstigen Beweismitteln unterschieden. Eine für elektronische Beweismittel relevante Legaldefinition findet sich in § 149 Abs. 1 Z. 1, dem Augenscheinbeweis für Bild- und Tonaufnahmen „*jede unmittelbare sinnliche Wahrnehmung und deren Dokumentation durch Ton- oder Bildaufnahme, soweit es sich nicht um eine Vernehmung handelt*“. Zumal elektronische Beweismittel einen Datenträger benötigen, müssen erst diese aus Beweisgründen sicher gestellt (§ 109 Z. 1 StPO), oder in Folge, wenn sie im weiteren Verfahren erforderlich sein werden, beschlagnahmt (Z. 2) werden.

Lt. Nimmervoll[5] sind elektronische Daten „*keine Gegenstände, sondern* ***immaterielle Objekte, die materiell verkörpert werden*** *müssen. Der Sicherstellung unterliegt folglich nur der Datenträger, auf welchem sich die elektronischen Daten befinden*“ und „*auch die Inhalte von E-Mail-Accounts unterliegen der Sicherstellung, da die Nachrichtenübermittlung bereits abgeschlossen ist und dadurch nicht mehr die Regelungen über die Nachrichtenübermittlung anzuwenden sind.*“ Die Rechtsgrundlage dafür bildet § 111 Abs. 2 StPO: „*Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.*“ Wir können in so einem Fall daher nicht von einer Sicherstellung des Datenträgers sprechen, sondern viel mehr von einer „**Sicherungskopie**“, was optimalerweise technisch einer **forensischen Kopie**, also der garantierten 1:1 Kopie der originalen Daten, gleichkommt.

Eine Legaldefinition für Urkunden lautet in § 74 Abs. 1 Z. 7 StGB[6]: „***eine Schrift****, die errichtet worden ist, um ein Recht oder ein Rechtsverhältnis zu begründen, abzuändern oder aufzuheben oder eine Tatsache von rechtlicher Bedeutung zu beweisen*“. Da ein Bezug auf das Medium fehlt, müssen darunter auch elektronische Urkunden subsumiert werden. Daten können somit nur dann eine elektronische Urkunde darstellen, wenn sie die Schriftlichkeit erfüllen. Was elektronische Urkunden verkörpert, kann auch rechtsvergleichend dem Dritten Teil der ZPO[7] entnommen werden, wo der Urkundsbeweis näher spezifiziert wird. Demnach sind gem. § 292 Abs. 1 **Öffentliche Urkunden** „*Urkunden, welche im Geltungsgebiete dieses Gesetzes von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form* ***auf Papier***

[5] Nimmervoll, Das Strafverfahren, Rz 106; Tipold/Zerbes,WK-StPO § 111 Rz 12.
[6] Strafgesetzbuch: BGBl. 60/1974, i.d.g.F.
[7] Zivilprozessordnung, RGBl. 113/1895 i.d.g.F.

oder elektronisch errichtet** sind (öffentliche Urkunden), begründen vollen Beweis dessen, was darin von der Behörde amtlich verfügt oder erklärt, oder von der Behörde oder der Urkundsperson bezeugt wird*", und lt. § 294: „Auf Papier oder elektronisch errichtete Privaturkunden** begründen, sofern sie von den Ausstellern unterschrieben oder mit ihrem gerichtlich oder notariell beglaubigten Handzeichen versehen sind, vollen Beweis dafür, dass die in denselben enthaltenen Erklärungen von den Ausstellern herrühren.*".

Im öffentlichen Recht wird zusätzlich noch der Begriff der „Originalfiktion"[8] verwendet, wo der in **elektronischen Urkundenarchiven** (Beglaubigungsarchiv der Justiz, Urkundensammlungen des Grundbuchs und des Firmenbuchs, Urkundenarchive von Körperschaften öffentlichen Rechts) eingespeicherte Dateninhalt bis zum Nachweis des Gegenteils als Original der gespeicherten Urkunde gilt.

Letztlich geht es bei der Bewertung von elektronischen Beweismitteln, und wenn diese die Schriftlichkeit erfüllen von elektronischen Urkunden darum, dass diese unverfälscht der ursprünglichen Datenquelle entsprechen müssen. Medienbrüche führen dazu, dass für die Forensik wichtige Metadaten vernichtet werden können, aber auch kann bei wiederholten Druck- und Scanvorgängen die Qualität bis zur Unkenntlichkeit leiden. Aus diesem Grund ist es essenziell, dass gewährleistet ist, dass die sichergestellten Daten technisch unverfälscht als Asservat den Sachverständigen zur Verfügung stehen.

2.1. Integrität elektronischer Beweismittel

Aufgrund der Tatsache, dass sich Daten leicht manipulieren lassen, ist eine Bewertung aufgrund des festgestellten Manipulationsschutzes, wie bspw., dass elektronische Urkunden, oder zumindest deren Fingerprint,[9] mittels einer digitalen Signatur zu signieren sind, eine sehr brauchbare Lösung, um diese Spuren **qualitativ** zu bewerten. Dies kann auch aus §§ 292 u. 294 ZPO geschlossen werden, wo die Beweiskraft elektronischer Urkunden durch Unterschrift gefordert wird, wobei diese lt. eIDAS-VO[10] i.V.m. dem SVG[11] auch elektronisch erfolgen kann.

Oftmals sind elektronische Spuren jedoch nicht elektronisch signiert, und somit muss in Betracht gezogen werden, dass diese manipuliert sein können. In diesem Fall kommt ein weiterer **quantitativer** Ansatz nach Casey[12] ins Spiel, wo unter der Berücksichtigung der Existenz weiterer, gleichartiger Spuren mit Hilfe einer sechsteiligen Skala von, die Spuren widersprechen Fakten oder stimmen nicht überein, bis hin zu, die Spuren waren vor Manipulationen geschützt oder haben eine hohe statistische Konfidenz, eine brauchbare Bewertung ermöglicht wird.

Weiters sind, wie schon oben angesprochen, **Metadaten** eine wichtige Quelle für die Erkennung einer Manipulation. Metadaten sind in den Dateien eingebaute, für den Nutzer oder Betrachter nicht sichtbare Daten, welche jedoch für die Datenverabeitung essenziell sind. Dies wären Zeitstempel, Koordinaten, Farbräume, Zeichensätze u.v.m., je nach Datenart. Eine Manipulation der Daten kann folglich zu einer Inkonsistenz mit den Metadaten führen.

Weine weitere Methode zur Erkennung von Manipulationen ist, wenn **inhaltliche Inkonsistenzen** erkennbar sind. Dies ist gleichsam auf Texte, Medien- und Binärdaten anwendbar.

Schließlich ist auch die schon erwähnte **Originalfiktion** eine sehr gute Möglichkeit, um eine Echtheit von elektronischen Urkunden zu gewährleisten. Dieses Modell ist nicht nur im öffentlichen Bereich anwendbar, sondern wäre als Idee auch bei privaten Urkunden- oder Datenarchiven, w.z.B. bei Cloudspeichern sinnvoll nutzbar.

---

8 Vgl. die Originalfiktion in §§ 91b Abs. 7 i.V.m. 91c Abs. 2 GOG, Gerichtsorganisationsgesetz, RGBl. 217/1896, i.d.g.F.

9 Auch Hashwert: eindeutiger, nicht umkehrbarer kryptographischer Extrakt von Daten.

10 Vgl. „elektronische Signaturen": Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

11 Signatur- und Vertrauensdienstegesetz, BGBl. I 50/2016, i.d.g.F.

12 Casey: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press, 2011.

2.2. Unionsrechtliche Rahmenbedingungen zur Herausgabe, Sicherstellung und Einziehung

Mit der EEA, die Europäische Ermittlungsanordnung,[13] sollten die Verfahren der gegenseitigen Rechtshilfe verkürzt und vereinfacht werden, „*wobei in jedem Fall Behörden im ersuchten Staat den ausländischen Akt anerkennen und Gründe geregelt sind, die zur Nichtanerkennung berechtigen.*“[14] Die KOM hat weiters am 17.04.2018 den Vorschlag einer E-Evidence-VO[15] eingebracht, da lt. ErwGr. 2 des Vorschlags „*für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen in der gesamten Union Maßnahmen zur Einholung und Sicherung elektronischer Beweismittel immer wichtiger werden*“. Mit dieser VO sollten die Regeln festgelegt werden, nach denen eine Behörde eines MS von einem in der Union tätigen Diensteanbieter verlangen kann, **elektronische Beweismittel herauszugeben oder zu sichern**, unabhängig davon, wo sich die Daten befinden. Zu den Datenkategorien, die unter diese VO fallen, gehören gem. ErwGr. 20 Teilnehmerdaten, Zugangsdaten, Transaktionsdaten und Inhaltsdaten. Dieser Vorschlag wurde heftigst diskutiert wie, dass „*ein solches Verfahren und die damit einhergehende „Privatisierung“ der Rechtskontrolle schwerwiegende Folgen für den Grundrechtsschutz hat,*“[16] und wurde deswegen breit abgelehnt. Gegenwärtig befindet sich diese VO im Trilog, d.h. der Rat, das EP und die KOM versuchen eine Einigung in diesem Gesetzgebungsverfahren herbeizuführen.

Die KOM erließ 2018 auch eine neue VO über die **gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen**,[17] und versprach sich dabei die Behebung von strukturellen Problemen bei der grenzüberschreitenden Sicherstellung und Einziehung. Der Anwendungsbereich erstreckt sich auf alle Sicherstellungs- und Einziehungsmaßnahmen, die i.Z.m. Strafverfahren gelten, darunter auch elektronische Beweismittel. Auch diese – geltende – VO ist umstritten, da „d*er Anwendungsbereich der VO damit über jenen der RL 2014/42*[18] *hinausgeht, weil er etwa auch non conviction based confiscation*[19] *erfasst.*“[20] und auch lt. Schumann damit „*noch eingriffsintensiveres punitives Recht eines einzelnen Mitgliedstaates europaweit durchsetzbar sein soll.*“[21]

Die unionsrechtlichen Herausforderungen erscheinen i.d.Z. als wesentlich, da gerade die Zeit bei elektronischen Beweisen ein entscheidender Faktor ist. Diese Daten unterliegen mglw. gesetzlichen Löschungsfristen, und sind dann nicht mehr erhebbar, oder diese Daten wurden nach einer – allenfalls gesetzlichen – Aufbewahrungsfrist automatisch gelöscht. Eine **effiziente und zeitnahe** gesetzliche Möglichkeit zur Erlangung solcher elektronischer Beweismittel wäre daher in der Union anzustreben. Ob dies mit der umstrittenen und sich derzeit im Trilog befindlichen Vorschlags einer E-Evidence-VO gelingt, kann sich – so ferne sie in Kraft tritt – erst in Zukunft nach deren Anwendung erweisen.

---

13 Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen.

14 Niekrenz: Die Cloud, Territorialität und Souveränität, recht & gesellschaft, juridikum 2020, S. 160, Heft 2 v. 15.6.2020.

15 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, COM/2018/225 final – 2018/0108 (COD).

16 Vgl. Stellungnahme der ÖRAK 21/18/142 vom 25.9.2018, S. 3.

17 Verordnung (EU) 2018/1805 des Europäischen Parlaments und des Rates vom 14. November 2018 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen.

18 Richtlinie 2014/42/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Sicherstellung und Einziehung von Tatwerkzeugen und Erträgen aus Straftaten in der Europäischen Union.

19 Nicht auf Verurteilung beruhende Sicherstellung oder Einziehung bedeutet die Einziehung von Vermögenswerten ohne die Verurteilung des Täters. Kann als synonym zum erweiterten Verfall gem. § 20b StGB verstanden werden. Findet Anwendung im Bereich der organisierten Kriminalität und Korruption.

20 Staffler: Konfiskation ohne Grenzen? Zur VO über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen, Aufsätze Europastrafrecht Aktuell, JSt 2019, 240 Heft 3 v. 1.5.2019.

21 Schumann: „(Non-)conviction based und extended confiscation in Österreich. Überlegungen zur Rechtsnatur, Systematik und Problemen vermögensrechtlicher Anordnungen“, NZWiSt 2018, S. 441.

2.3. Der Bias elektronischer Beweismittel

Nach Girod-Frais wird die „*Forensik oder forensische Wissenschaft als die Wissenschaft der Spur defniert. Alle Methoden, Techniken und Prozesse, die zur Suche, Sicherung, Analyse und Auswertung von Spuren verwendet werden können, sind daher Teilbereiche der Forensik.*“[22] 2011 hat erstmals Dewald[23] die „Forensische Informatik“ qualifiziert als „*Die Anwendung wissenschaftlicher Methoden der Informatik auf Fragen des Rechtssystems. Insbesondere stellt die forensische Informatik Methoden zur gerichtsfesten Sicherung und Verwertung digitaler Spuren bereit.*“ Letztlich geht es demnach bei der Forensischen Informatik um die Suche, Sicherstellung Analyse und Auswertung elektronischer Beweismittel, und daher „*unterliegen die Anforderungen an die Glaubwürdigkeit, der Wiederholbarkeit, der Integrität und Dokumentation der Beweissicherung hohen Maßstäben, denn die Gefahr, dass durch die forensische Arbeit digitale Spuren verändert oder vernichtet werden ist latent hoch*“.[24] Bei der Erhebung entstehen leider manchmal Fehler, welche sich dann im Laufe des Verfahrens manifestieren, und schließlich zu einer fehlerhaften Beweiswürdigung führen können.

2.3.1. Ursachen für den Bias

Einer dieser Fehler ist der sog. „Bias“, worunter eigentlich der englische Begriff „cognitive bias“ zu verstehen ist, wie die systematische fehlerhafte Neigungen beim Wahrnehmen, Erinnern, Denken und Urteilen. Sie geschehen oft unbewusst und basieren auf kognitiven Vorurteilen. Quellen solch eines Bias können sein:[25]

- Erwartungen von Ergebnissen vor der Untersuchung,
- Ergebnisse wissensbasierender Technologien w.z.B. Forensic-Toolkits,
- Rückwärtsvergleiche, d.h. Erwartungshaltungen bei Treffern, wobei die Spuren fehlen,
- Kontextbasierende Informationen, wenn irrelevante Daten in die Bewertung einfließen.

Der Einsatz innovativer, wissensbasierender Technologien aber auch der sog. „Künstlichen Intelligenz“ mag als Werkzeug den Aufwand reduzieren, welcher für die Analysen des vielfach massenhaft vorliegenden elektronischen Datenmaterials erforderlich ist. Diese Technologie unterstützt Forensiker dabei, Ergebnisse in kurzer Zeit zu erhalten, welche diese bei manueller Sichtung niemals erhalten hätten. Aufgrund der Unsicherheiten und Unausgereiftheit solcherart KI-Systeme sollten sich Forensiker aber nicht von solchen Ergebnissen hinreißen lassen, und voreilige und womöglich falsche Schlussfolgerungen tätigen. Schließlich sollen sie bei der Bewertung der Ergebnisse nicht nur ihre Erfahrung, Sorgfalt und Objektivitität, sondern auch den „gesunden Hausverstand“ walten lassen.

2.3.2. Fallbeispiele mit Bias

Ein berühmtes Fallbeispiel für einen Bias ist die fehlerhafte Zuordnung einer Fingerspur bei den Bombenanschlägen[26] auf Züge in Madrid im Jahre 2004. Die Interpol Ermittlungen führten auch zu Untersuchungen in den USA: Eine automationsunterstützte Suche in der IAFIS[27] Datenbank beim FBI lieferte eine große Ähnlichkeit mit den Fingerabdrücken von Brandon Mayfield, einem zum Islam konvertierten Anwalt in den USA. Aufgrund dessen, und im Kontext der vor wenigen Jahren erfolgten 9/11 Anschläge, ignorierten die Ermittler dabei die Tatsache, dass nur einige wenige Fingerspur-Charakteristika tatsächlich übereinstimmten,

---

22 Girod-Frais, Kappler: „Rudolf Archibald Reiss und der Stellenwert der Forensik“ in SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1/2021), S. 4–18.

23 Dewald, Freiling: „Forensische Informatik“, Books on Demand, 2011.

24 Hrdinka: „Herausforderungen verantwortungsloser Digitalisierung“, Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020, S 503.

25 Vgl. Czebe, Kovács: „The impact of bias in latent fingerprint identification“, 2015 6th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), 2015, S. 569–574.

26 Stacey: „A Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case“, Journal of Forensic Investigation, S. 706, FBI, 2004.

27 Integrated Automated Fingerprint Identification System des FBI.

und übernahmen unreflektiert das Ergebnis der Datenbank. Weiters wurde das wissenschaftliche ACE-V[28] Prinzip ignoriert, wo zuerst die Analyse, der Vergleich, dann eine Auswertung und letztlich die Verifikation erfolgen muss. Nach der Identifizierung des tatsächlichen Täters, einem Algerier, durch die spanischen Behörden, wurde der Beschuldigte aus der monatelangen Untersuchungshaft entlassen.

Ein Beispiel dafür, dass eine Anklage auch ohne des zwar zwingend vorhandenen, aber nicht vorgelegten elektronischen Beweismaterials möglich ist, ist folgender Fall: Ein 80-jähriger Kunde hebt vom Foyerbankomaten seiner Stammfiliale einen Betrag von 300,– Euro ab. Ein Jahr später wurde er beschuldigt er hätte zu dieser Zeit 3.000,– Euro von einem fremden Konto behoben, und in Folge wg. §§ 127 und 129 Abs. 1 Z. 3 StGB, des Diebstahls und des Diebstahls durch Einbruch angeklagt. Als einziger Beweis dafür wurde eine Standbildsequenz mit Zeitstempeln aus der Überwachungskamera zum inkriminierten Zeitpunkt in Form eines PDF Dokuments vorgelegt, wo der Angeklagte erkennbar war. Für den Anzeiger war diese Person mit Sicherheit der Täter, und daher wurden auch keine Bilder unmittelbar vor oder nach dieser Behebung vorgelegt, auch fehlten das Transaktions- und Stückelungsprotokoll des von der Bank selbst betriebenen Bankomaten, welche angeblich nicht mehr vorhanden waren. Auch seien die weiteren Videosequenzen vor und nach dieser Behebung inzwischen gelöscht. Vorgelegt wurden lediglich die Kontoauszüge über beide Transaktionen. Aufgrund dieser Wunderlichkeiten wurden vom Privat-SV des Angeklagten die vorhandenen Zeitstempel näher untersucht, wo schließlich herauskam, dass die Uhrzeit der Kamera um 4 Minuten vorgehen musste, und der wahre Täter genau 4 Minuten nach der 300,– Euro Behebung des Angeklagten die inkriminierten 3.000,– Euro behob. Als Beweis dafür diente die Zusammensetzung der Einzelbilder in eine Filmsequenz, wo nach Abspielen erkennbar war, dass der Angeklagte nach der Behebung exakt 5 Geldscheine zählte, davon war auf der einen Seite ein 50 Euro und auf der Rückseite des Pakets ein 100 Euro Schein erkennbar. Ein vergleichsweises Geldpaket von 3.000,– Euro ist darüber hinaus wesentlich stärker als am Bild erkennbar. Zumal bei Bankomaten keine höheren Geldscheine als 100 Euro ausgegeben werden und höhere als 500 nicht existieren, musste es sich bei der Aufnahme um die Behebung der 300,– Euro gehandelt haben. Ein weiterer Beweis war die im Hintergrund, jedoch aufgrund der Auflösung nur schlecht erkennbare, analoge Wanduhr. Durch eine forensische Verbesserung des Bildes konnte anhand des Zeigerstandes gezeigt werden, dass die Zeit der Wanduhr mit jener der Behebung der 300,– Euro korrelierte, was durch den entsprechenden Kontoauszug des Angeklagten belegbar war. Die Uhrzeit am Bild des Überwachungssystems musste folglich falsch sein. Das Verfahren ist mittlerweile ohne Urteil beendet, da der Angeklagte vorzeitig an einem Schlaganfall verstarb.

2.4. Straftatbestände i.V.m. elektronischen Beweismitteln

Daten, darunter fallen elektronische Beweismittel, sind vielfältig und werden daher in den verschiedensten gesellschaftlichen Bereichen erzeugt, genutzt und auch manipuliert. Die hier dargestellten Straftatbestände samt Beispiel können daher nur sehr eingeschränkt einen Überblick bieten.

Die Betrugsdelikte insb. § 146 Betrug, § 147 Schwerer Betrug, § 148 Gewerbsmäßiger Betrug und schließlich § 148a Betrügerischer Datenverarbeitungsmissbrauch werden vermehrt mit Hilfe elektronischer Mittel verübt. Demzufolge ergeben sich entsprechend zahlreiche elektronische Beweismittel, welche zur Aufklärung der Tat dienlich sind.

Neben den zahlreichen Fälschungsdelikten im StGB, darunter die Urkundenfälschung (§ 223 ff. StGB), oder die Datenfälschung (§ 225a), ist die Fälschung von (elektronischen) Beweismitteln (§ 293) ebenso im Vormarsch. Grund dafür dürfte sein, dass es den technisch oft wenig versierten Fälschern sehr einfach erscheint, bspw. eine falsche oder manipulierte PDF Urkunde zu erstellen und als Beweis vorzulegen, und verkennen dabei, dass es zahlreiche forensische Methoden gibt, solcherart Manipulationen auf die Spur zu kommen. Auch technisch versierte Fälscher sind nicht vor Aufdeckung gefeilt, da Menschen eben Fehler machen.

[28] Analysis, Comparison, Evaluation and Verification: Wissenschaftliche Methode zur Untersuchung und Dokumentation von latenten Fingerabdrücken.

2.4.1. Beispiel: Anklage wg. Betrug aufgrund gefälschter Beweise

Solch ein Fall betrifft einen wg. § 146 StGB Angeklagten, welcher beschuldigt wurde eine FritzBox auf einem Online-Portal inseriert zu haben, die er nach Bezahlung mittels PayPal nicht lieferte. Es handelte sich um ein Verfahren nach Rechtshilfe für Deutschland. Der Prüfauftrag an den gerichtlich bestellten SV lautete „*Befund und Gutachten darüber zu erstatten, ob der Angeklagte im September 2019 über einen ***-Account verfügte und ob das Inserat und der Chat-Verlauf vom Angeklagten stammen.*“ Dem Angeklagten wurde vorgeworfen, er habe über einen anonymen Account den Käufer betrogen. Zu seiner Verteidigung gab er an, der überwiesene PayPal Betrag entstammt aus einem Verkauf von Spiele-Items, da er das Spiel fertig spielte und diese am fallgegenständlichen Tag an einen für ihn anonymen Unbekannten im Internet verkaufte.

Das in Berlin ansässige Online-Portal zeigte sich wenig kooperativ, da trotz mehrfacher Aufforderung zur Befundaufnahme samt Fristsetzung behauptet wurde, das Inserat sei inzwischen automatisch gelöscht und das Nutzerkonto sei niemanden zuordenbar (Anm.: Backups schienen unbekannt zu sein), was insgesamt als unglaubwürdig erschien. Eine Recherche und Analyse über alle in schlechter Qualität vorliegenden Papier-Beweise, darunter inkriminierte Screenshots der Anzeige, einem Chatverlauf zw. Käufer und Verkäufer, und den PayPal- und Kreditkartenprotokollen ergab, dass die PayPal Transaktion vor dem Erstkontakt zw. Käufer und Verkäufer am selben Tag statt fand, was die Ermittlungsbehörden offenbar übersahen oder ignorierten. Damit wäre der Erfolgszeitpunkt vor dem Tatzeitpunkt, was physisch unmöglich ist. Nach dem darauf folgenden Chat über die FritzBox zw. Käufer und Verkäufer erhielt der Käufer eine E-Mail Warnung vom Online-Portal, dass dieser Account missbräuchlich verwendet werde. Aufgrund dieser verdächtigen Gegebenheiten wurden alle Beweise als elektronische Urkunde angefordert um allfälligen Manipulationen auf die Spur kommen zu können.

Es wurde forensisch festgestellt, dass das PDF-Dokument, welches das Online-Inserat dokumentieren sollte, ein vom Anzeiger selbst erzeugtes PDF-Dokument war, welches er als Beweis vorlegte. Solch ein PDF eines vermeintlichen Inserats ist aus diesem Online-Portal aber graphisch nicht erzeugbar. Ob der Chat-Verlauf vom Angeklagten stammt, musste aus diesem Grund stark angezweifelt werden. Aufgrund der Tatsache, dass die E-Mail des Angeklagten lediglich in einem Chat in einer nicht vor Manipulationen geschützten Datei als Beweis vorlag, und es darüber hinaus keinerlei Screenshot aus dem Online-Portal mit der E-Mail des Angeklagten existierte – diese war lediglich im Chat als Text – musste von einer Fälschung ausgegangen werden.

Der wahre Tathergang samt Motiv konnte somit mittels den elektronischen Beweisen wie folgt rekonstruiert werden: Offensichtlich hat eine PayPal Transaktion mit dem inkriminierten Betrag am Vormittag statt gefunden. Dies korreliert mit den Aussagen des Angeklagten, als Items eines Spiels verkauft wurden. Die PayPal Transaktion zwischen dem Anzeiger und dem Angeklagten ist demzufolge der einzige Zusammenhang zwischen beiden. Erst viel später am selben Tag abends fand ein Verkauf über eine Fritzbox statt, wobei gar nicht belegt war, dass dieser Verkauf tatsächlich abgeschlossen wurde. Ein Zusammenhang dieser Transaktion mit jener am Vormittag konnte technisch ausgeschlossen werden. Nachdem der Anzeiger einen (vermeintlichen) Betrug erkannte, er erhielt keine Ware, versuchte er Beweise zu erstellen um sich beim Angeklagten schadlos halten zu können. Auch ist es denkbar, dass er sich den Betrag der Spiel-Items zurück holen wollte. Zusätzlich zu den erstellten Screenshots wurde nach der Anzeige bei der Polizei der Screenshot über das angebliche Inserat, und ein vorhandener Chatverlauf durch die E-Mail des Angeklagten ergänzt, vorgelegt. Der angebliche Chatverlauf war ein einfacher Text einer Textverarbeitung als PDF gespeichert.

Da erwiesenermaßen der subjektive Tatbestand des § 146 StGB nicht erfüllt war, wurde der Angeklagte aufgrund des ermittelten wahren Tathergangs und den damit aufgedeckten Fälschungen zu Recht freigesprochen. Das Urteil ist inzwischen rechtskräftig.

Dieses Beispiel verdeutlicht, dass trotz Medienbrüchen und zeitaufwändigen grenzüberschreitenden Ermittlungen, der Fall gelöst werden konnte.

2.4.2. Ergebnis und rechtliche Beurteilung des Falls

Ob der Anzeiger und allenfalls Beitragstäter den Tatbestand der Beweismittelfälschung (§ 293) erfüllten, hängt maßgeblich davon ab, ob die ausdrückliche Subsidiarität des § 293 Abs. 1 gegeben ist: „*Wer ein falsches Beweismittel herstellt oder ein echtes Beweismittel verfälscht, ist, wenn er mit dem Vorsatz handelt, daß das Beweismittel in einem gerichtlichen oder verwaltungsbehördlichen Verfahren, in einem Ermittlungsverfahren nach der Strafprozessordnung, nach der Verordnung (EU) 2017/1939 oder im Verfahren vor einem Untersuchungsausschuss des Nationalrates gebraucht werde, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen, wenn die Tat nicht nach den* ***§§ 223, 224, 225 oder 230*** *mit Strafe bedroht ist.*“ Wenn eine falsche oder verfälschte Urkunde auch als Beweismittel dienen soll, so tritt die Beweismittelfälschung nach § 293 Kraft ausdrücklicher Subsidiarität gegenüber §§ 223 ff. zurück. In diesem Fall wäre die Urkundenfälschung nach § 223 erfüllt, wonach zwei (elektronische) Urkunden vom Anzeiger im Rechtsverkehr als Beweis hergestellt und gebraucht wurden. Durch deren Gebrauch ist auch die Tätige Reue gem. § 226 ausgeschlossen. Keine Subsidiarität wäre hingegen bei einer Datenfälschung gem. § 225a gegeben; „*Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.*“ Ob der objektive Tatbestand der Datenfälschung erfüllt war, ist auch anzuzweifeln, da wenn „*das Tatobjekt keine Schrift ist, sondern Daten iSd § 74 Abs. 2 StGB.*[29] *Diese kommen mangels Urkundenähnlichkeit nicht als Tatobjekt in Frage.*“[30] Der angebliche Screenshot der Anzeige und der Chat wären somit als Urkunden, die zweifelsfrei die Schriftlichkeit erfüllten, zu werten.

3. Zusammenfassung und Ausblick

Bei der Pönalisierung ist zw. der Fälschung elektronischer Beweismittel und der Fälschung elektronischer Urkunden zu unterscheiden. Den Unterschied macht die Schriftlichkeit der Urkunde, was bei Papierurkunden einfacher zu bewerten ist als bei sonstigen Daten, welche vielfältigere Darstellungsformate wie z.B. kombinierte Texte und Medien aufweisen.

Jedenfalls ist bei der Erhebung und Archivierung elektronischer Beweismittel darauf zu achten, dass keine Medienbrüche entstehen, möglichst elektronische Signaturen als Unterschrift verwendet werden (was technisch nicht immer einfach möglich ist), oder organisatorische Maßnahmen getroffen werden, sodass eine sog. Originalfiktion der elektronischen Urkunden gewährleistet wird.

Bei der Bewertung der elektronischen Beweismittel ist darauf zu achten, dass eine qualitative, quantitative und inhaltliche Untersuchung erfolgt, wobei Letztere darauf abzielt, dass mögliche Inkonsistenzen der Metadaten und Inhaltsdaten aufgedeckt werden.

Ein weitere Herausforderung ist die Zeit, denn Daten sind nicht endlos lange verfügbar, und werden je nach technischen oder rechtlichen Rahmenbedingungen zu gegebener Zeit gelöscht bzw. sogar vernichtet. Im letzten Fall sind diese nicht mehr wiederherstellbar.

Aufgrund des Bias, mit welchem trotz höchster Sorgfaltsmaßstäbe der Organe und der strengen gesetzlichen Rahmenbedingungen, grds. gerechnet werden muss, wäre künftig analog zum ACE-V Prinzip, das bei latenten Fingerabdrücken zum Einsatz kommt, ein Modell für die Forensische Informatik zu entwickeln. Mit bspw. der Rechtsvisualisierung könnte zukünftig den Experten aufgezeigt werden, welche Prüfschritte erforderlich sind, um zu gesicherten Ergebnissen zu gelangen.

---

[29] Sowohl personenbezogene und nicht personenbezogene Daten als auch Programme.

[30] Reindl-Krauskopf, Salimi, Stricker: „IT-Strafrecht: Cyberdelikte und Ermittlungsbefugnisse“. MANZ’sche Verlags-und Universitätsbuchhandlung, 2018.