DIE ZEITDIMENSION IN DER COMPUTERFORENSIK

Thomas Hrdinka

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

Schlagworte: ***Zeit, Cyberspuren, Beweismittel, IT-Forensik***

Abstract: *Eine häufig gestellte Frage an Sachverständige ist, ob sich ein Verdacht beweisen lässt, und vielfach wird dabei ein bestimmter, zu untersuchender Tatzeitraum angegeben. In anderen Fällen wird dieser Zeitraum zwar nicht näher spezifiziert, aber doch implizit vorausgesetzt. In jedem Fall ist eine nähere Determinierung des Zeitraums geboten, da die forensischen Hauptfragen, wie die Tat selbst (was ist geschehen), dem Tatort (wo ist es passiert), dem Tathergang (wie wurde vorgegangen), den Spuren (womit wurde gearbeitet) und schließlich der Tatzeit (wann ist es passiert) umfassen. Die Frage nach Zeit stellt sich jedoch nicht nur im Strafrecht sondern vor allem noch granularer im Zivilrecht, insb. dann, wenn technische „hard-core" Sachverhalte bewertet werden müssen.*

1. Einleitung

Im Gegensatz zu physischen Spuren weisen digitale Spuren oftmals, aber nicht immer, Zeitstempel auf, was die Zuordnung zu einer Tatzeit oder einem technischen Sachverhalt vereinfachen kann. Abgesehen davon, was Zeit im physischen Sinne eigentlich sein soll, und folglich im juristischen, ist solch eine Zuordnung nicht wie vielfach angenommen trivial, da die Zeitfrage multilaterale Fallstricke beinhaltet. Das kann im schlimmsten Fall zu einer Fehlinterpretation der Spuren mit Folgen w.z.B. einer Verurteilung eines objektiv unschuldigen Angeklagten aufgrund eines falschen Gutachtens führen – aber auch umgekehrt wie im Falle eines „in dubio pro reo" Freispruchs eines technisch-objektiv Schuldigen. Ein Vernachlässigen des fallrelevanten Zeitraums muss daher folglich den anerkannten Regeln der Technik, jedenfalls dem Stand der Technik, widersprechen, und muss daher als absolut unzulässig anzusehen sein. Die unterschiedlichsten Interpretationen einer Referenzzeit bei Softwareprodukten und technischen Standards erschweren darüber hinaus einen Vergleich der zu untersuchenden Zeitstempel erheblich. Eine automatisierte Auswertung von Datenträgern mit Hilfe von forensischen Werkzeugen ist deswegen immer zu hinterfragen, und solche vielfach als „richtig" anerkannten Reports dieser Softwareprodukte sind keinesfalls unreflektiert zu übernehmen. Darüber hinaus ist die oftmals in Medien publizierte These, dass das Internet angeblich nicht vergisst, nur tlw. richtig: Vielmehr sind länger in der Vergangenheit zurückliegende Daten bereits vernichtet, bestenfalls sind nur Spurenfragmente darüber zu finden.

Abgesehen davon ist ein Computersystem, das mit einem Zeitserver synchronisiert war oder nicht, oder in einer be- oder unbestimmten Zeitzone betrieben wurde, oder auch vollkommen asynchron mit der Normalzeit gelaufen ist, oder sich sogar byzantinisch, also absolut unvorhersehbar, verhalten hat, jedenfalls näher zu prüfen und entsprechend zu bewerten. Die Normalzeit wird in Österreich, zumal das Eichwesen nicht von den Unionsverträgen umfasst ist und daher eine hoheitliche Aufgabe darstellt, gesetzlich unter Berücksichtigung der Standards internationaler Normungsgremien und unionsrechtlicher Vorgaben, wie zur sich in Diskussion befindlichen Sommerzeit, geregelt. Aufgrund der durch die oben beschriebenen Rahmenbedingungen ist es auch nicht auszuschließen, dass erhobene Daten mit der Normalzeit, und folglich einer Tatzeit, sogar erheblich abweichen können.

2. Definition der Zeit

Die gem. der internationalen Meterkonvention[1] für Maßeinheiten zuständige Generalkonferenz CGPM[2] definierte in der 26. Konferenz 2018 die „*Sekunde, Einheitenzeichen s, als die SI3-Einheit der Zeit. Sie ist definiert, indem für die Cäsiumfrequenz ΔvCs, der Frequenz des ungestörten Hyperfeinübergangs des Grundzustands des Cäsiumatoms 133, der Zahlenwert 9 192 631 770 festgelegt wird, ausgedrückt in der Einheit Hz, die gleich s^{-1} ist*“. Da die Festlegung von Maßeinheiten in Österreich eine hoheitliche Aufgabe darstellt, ist in § 2 Abs. 1 Z. 3 MEG[4] normiert, dass „*die Sekunde das 9 192 631 770fache der Periodendauer der dem Übergang zwischen den beiden Hyperfeinstrukturniveaus des Grundzustandes von Atomen des Nuklids Cäsium-133 entsprechenden Strahlung*“ ist. Diese Legaldefinition der Sekunde und jene gleichlautende aus der Richtlinie 80/181/EWG[5] lehnt sich an die veraltete Definition der 13. CGPM aus dem Jahr 1967 an, und sollte tunlichst überarbeitet werden.

Das Zeitzählungsgesetz[6] normiert schließlich in § 1 Abs. 1 die Normalzeit der Republik Österreich als die Mitteleuropäische Zeit (MEZ), welche gem. Abs. 2 die Zonenzeit, für die die Zeit des 15. Längengrades östlich von Greenwich maßgebend ist.

2.1. Weltzeit

Durch die hohe Qualität der Zeitmessung mit Hilfe von Atomuhren konnte einerseits 1967 die Definition der Einheit Sekunde präzisiert werden, und weiters seit 1971 eine einheitlich stabile Zeitskala, die TAI,[7] gebildet werden. Die astronomisch berechnete UT1[8] weicht aber von der technisch realisierten Zeitskala TAI geringfügig ab. Die aus diesem Grund seit 1972 neu eingeführte Weltzeit UTC[9] wird mit der TAI synchronisiert, und zumal die Erdrotation nicht periodisch ist, muss bei Bedarf ca. alle 1,5 Jahre eine sogenannte „Schaltsekunde“ eingeführt werden. Das bedeutet, dass der Tag dann nicht, wie in § 2 Abs. 5 Z. 4 MEG bestimmt 86400, sondern 86401 Sekunden dauert. Wenn sich die Zeitverschiebung zwischen UTC und UT1 an 0,9 Sekunden annähert, so wird vom IERS[10] diese Schaltsekunde empfohlen, welche das BIPM beschließen kann. Insgesamt differiert die TAI seit 1972 und der letzten Schaltsekunde am 31.12.2016 um 37 Sekunden von der UTC. Seit 2016 ist auf Schaltsekunden verzichtet worden, da wegen auftretenden Problemen in hoch präzisen Echtzeitsystemen überlegt wird, die gültige Weltzeit zu reformieren und die Schaltsekunden abzuschaffen. Somit ist es fraglich ob die nächste mögliche Schaltsekunde am 30.06.2021 stattfinden wird.

Die UTC, also die mit den Atomuhren synchronisierte Weltzeit, ist in technischen Systemen, inbs. in Computersystem von zentraler Bedeutung. Die bei uns geltende UTC+1 wich jedoch von der ursprünglich astronomisch berechneten MEZ geringfügig ab. Obwohl im alltäglichen Leben dieser Unterschied nicht auffallen würde, sehr wohl aber in technischen Anwendungen, wo Zeitstempel in Sekundenbruchteilen benötigt werden, ist aus diesem Grund die MEZ in eine Zeitzone der UTC umdefiniert worden. Die in Österreich

---

1 Am 20. Mai 1875 geschlossener internationaler Vertrag, in dem die 17 Unterzeichnerstaaten „vom Wunsche geleitet, die internationale Einigung und die Vervollkommnung des metrischen Systems zu sichern“.

2 Conférence Générale des Poids et Mesures: Treffen von Delegierten aller Unterzeichnerstaaten im Abstand von vier bis sechs Jahren.

3 Système international d’unités: definiert von CGPM und BIPM.

4 Maß- und Eichgesetz: BGBl. 152/1950 i.d.g.F.

5 Richtlinie 80/181/EWG des Rates vom 20. Dezember 1979 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Einheiten im Meßwesen und zur Aufhebung der Richtlinie 71/354/EWG.

6 Bundesgesetz vom 27. Jänner 1976 über die Zeitzählung, BGBl. 78/1976 i.d.g.F.

7 Temps Atomique International: Die Internationale Atomzeit wird mit Hilfe von mehr als 600 weltweiten Atomuh ren gewonnen.

8 Universal Time No.1: wird durch astronomische Beobachtungen gewonnen.

9 Universal Time Coordinated: Die koordinierte Weltzeit wurde 1972 vom BIPM eingeführt.

10 International Earth Rotation and Reference Systems Service.

gültige UTC(BEV) wird per Verordnung[11] des zuständigen BEV[12] festgelegt, wo gem. § 1 Abs. 3 leg. cit. die Impulsfolge gem. der vom BIPM festgelegten UTC und der MEZ zu entsprechen hat. Abs. 4 regelt, dass die Ankündigung des Minutenbeginns in der Impulsfolge um eine Sekunde zu verschieben ist, wenn dies vom BIPM beschlossen wurde. Der Zeitpunkt einer solchen Maßnahme ist im „Amtsblatt für das Eichwesen" und im „Amtsblatt für das Vermessungswesen" zu verlautbaren.

2.2. Sommerzeit

Eine weitere Herausforderung stellt die in der Richtlinie 2000/84/EG[13] verbindlich umzusetzende Sommerzeit dar: Gem. § 1 Abs. 3 Zeitzählungsgesetz gilt als Sommerzeit die gegenüber der Normalzeit um eine Stunde vorverlegte Stundenzählung und laut Abs. 3 kann die Sommerzeit innerhalb des Zeitraumes zwischen dem 1. März und dem 31. Oktober eingeführt werden. Das jeweilige Datum und die Uhrzeit des Beginns und des Endes der Sommerzeit ist zuletzt durch Verordnung[14] geregelt worden: Demnach beginnt die nächste Sommerzeit am 28. März 2021 um 2.00 Uhr MEZ und endet am 31. Oktober 2021 um 3.00 Uhr MESZ[15]. Die in Art. 4 der Richtlinie 2000/84/EG alle 5 Jahre zu veröffentlichende Mitteilung des Beginns und Endes der Sommerzeit für die folgenden 5 Jahre ist bis dato nicht erfolgt, da die KOM beschlossen hat das Funktionieren der derzeitigen Sommerzeitregelung zu überprüfen, ob diese geändert oder beibehalten werden soll. I.d.Z. holte die KOM im Rahmen einer öffentlichen Konsultation die Meinung der europäischen Bürger, Interessenträger und MS zur derzeitigen Sommerzeitregelung und zu möglichen Änderungen dieser Regelung ein: Diese ergab einen mehrheitlich zu 80% den Wunsch auf Abschaffung der Zeitumstellung und Beibehaltung einer ganzjährigen Zeitzone, wobei es auch zahlreiche Stimmen zur Abschaffung aufgrund Problemen in Computersystemen gab. Das EP stimmte daher mit einer großen Mehrheit für eine Abschaffung der Zeitumstellung ab dem Jahr 2021. Die MS versuchten in Folge eine diesbezügliche Festlegung von Zeitzonen zu erreichen, welche untereinander abgestimmt werden sollten, was jedoch bis dato nicht gelungen ist. Ob die Abschaffung der Zeitumstellung wie ursprünglich geplant im Jahr 2021 wirksam wird ist daher fraglich.

2.3. Kalender

Eine weniger problematische Regelung der Zeit findet sich in § 2 Abs. 5 Z. 4 MEG, wonach die Woche, der Monat und das Jahr des Gregorianischen Kalenders nach der Tageslänge zu bestimmen sind. Aufgrund der Ungenauigkeit des Julianischen Kalenders, welcher um 10 Sonnentage nachhinkte, ist dieser 1582 von Papst Gregor XIII reformiert worden. Aus diesem Grund wurden 10 Tage gestrichen, wobei die Abfolge der Wochentage aber beibehalten wurde: Dem Donnerstag, 4. Oktober folgte demnach der Freitag, 15. Oktober 1582. Für eine korrekte Kalenderrechnung ist es auch wichtig die Schaltjahre korrekt zu berücksichtigen: das sind bei den Jahrhundertsprüngen nur alle durch 400 teilbaren, bei allen anderen durch 4 teilbare Jahreszahlen. Das Gregorianische Jahr dauert somit exakt 365,2425 Tage. Zu berücksichtigen ist weiters, dass diese Kalenderreform nicht in allen Ländern der Welt gleichzeitig eingeführt wurde, was bei manchen Softwareprogrammen, die Zeitrechnungen mit lange zurückliegenden Zeitstempeln durchführen, zu falschen Ergebnissen führt. Darüber hinaus gelten in manchen Ländern nach wie vor andere Kalendersysteme, was bei der Übernahme von Zeitstempeln und deren Umrechnung in UTC entsprechend zu berücksichtigen ist.

[11] Verordnung des Bundesamtes für Eich- und Vermessungswesen über die Darstellungsverfahren der gesetzlichen Maßeinheiten für die Zeit und Frequenz, veröffentlicht im Amtsblatt für das Eichwesen Doppel-Nr. 3- 4/2008.

[12] Bundesamt für Eich- und Vermessungswesen.

[13] Richtlinie 2000/84/EG des Europäischen Parlaments und des Rates vom 19. Januar 2001 zur Regelung der Sommerzeit.

[14] Verordnung der Bundesregierung über die Sommerzeit in den Kalenderjahren 2017 bis 2021, BGBl. II 22/2017.

[15] Mitteleuropäische Sommerzeit.

Aufgrund der hohen Genauigkeit des Gregorianischen Kalenders sind Änderungen in naher Zukunft nicht zu erwarten.

Andere Unsicherheiten sind jedoch, wie eine mögliche Abschaffung der Schaltsekunde und der Winter- Sommerzeitumstellung für eine vorausschauende Planung – ich erinnere an dieser Stelle an die Jahr 2000 Problematik – für Zeitstempel in Computersystemen wenig förderlich, zumal solcherart Umstellung erst programmiert, getestet und die Software dann verteilt werden müsste.

2.4. Zeitformate

Die Darstellung von Zeitstempeln ist äußerst vielfältig, und kulturell bedingt. Eine korrekte Interpretation dieser Schreibweisen ist für eine Umrechnung in UTC daher essenziell. In Österreich und in unionsrechtlichen Materialien wird daher vielfach ein Datumsformat gem. der ISO 8601[16] gefordert. In dieser Norm wurde versucht, die unterschiedlichen nationalen Datumsformate zu vereinheitlichen. Z.B. wird dieses in den Detailspezifikationen zur RKSV[17] gefordert: Demzufolge wird das Feld Beleg-Datum-Uhrzeit, das dem in § 9 Abs. 2 Z. 3 angegebenen Wert entspricht, nach ISO 8601 ohne Angabe der Zeitzone (es wird von MEZ b.z.w MESZ ausgegangen) nach folgendem Muster kodiert: „JJJJ-MM-TT'T'hh:mm:ss". Bsp.: 2015-07-21T14:23:34. Eine Datenbank über die unterschiedlichsten sonstigen in Verwendung befindlichen Zeitformate bildet das CLDR[18] einem Unicode Konsortium[19].

2.5. Granularität der Zeit

Welche Granularität die verwendete Zeit zu haben hat, ist im Wertpapierhandel von entscheidender Bedeutung. Bspw. „*setzt § 16 BörseG[20] den Art 50 MiFID II[21] um, der die MS verpflichtet, allen Handelsplätzen und ihren Mitgliedern oder Teilnehmern vorzuschreiben, die im Geschäftsverkehr verwendeten Uhren zu synchronisieren, die sie benutzen, um das Datum und die Uhrzeit von Ereignissen aufzuzeichnen, die gemeldet werden müssen.*"[22] Die Leitlinien[23] der ESMA[24] geben darüber genauer Auskunft: Wenn in Handelsplätzen die Gateway-to-Gateway-Latenzzeit größer als eine ms ist, so hat die Granularität des Zeitstempels eine ms oder feiner zu sein. Ist die Gateway-to-Gateway-Latenzzeit kleiner gleich einer ms, so hat die Granularität des Zeitstempels eine µs oder feiner zu sein. Für Mitglieder und Teilnehmer von Handelsplätzen gilt bei hochfrequenter algorithmischer Handelstätigkeit eine Granularität des Zeitstempels eine µs oder feiner, bei sonstiger Handelstätigkeit eine ms oder feiner.

Diese hier beispielhaft angeführte gesetzlich normierte Granularität der Zeitstempel ist eine der wenigen solcherart Bestimmungen, zumal in anderen technischen Disziplinen dafür technische Normen geschaffen wurden, welche in diesen Bereichen den Stand der Technik abbilden. Eine Besonderheit in diesem Zusammenhang bildet das europäische zivile Satellitennavigationssystem Galileo[25] zur weltweiten Positionsbestimmung, dessen hoch präzise Atomuhren in Verbindung mit DGPS[26] eine zivile Navigationsgenauigkeit im cm-Bereich zulassen.

---

16 ISO 8601: Data elements and interchange formats – Information interchange – Representation of dates and times.

17 Registrierkassensicherheitsverordnung: Verordnung des Bundesministers für Finanzen über die technischen Einzelheiten für Sicherheitseinrichtungen in den Registrierkassen und andere, der Datensicherheit dienenden Maßnahmen, BGBl. II 410/2015.

18 Common Locale Data Repository.

19 Unicode Inc.: Gemeinnützige Organisation, die den Unicode-Standard weiterentwickelt und heraus gibt.

20 Börsegesetz 2018, BGBl. I 107/2017 i.d.g.F.

21 Richtlinie 2014/65/EU vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU.

22 Wurzer in Kalss/Oppitz/U. Torggler/Winner, BörseG/MAR (2019), § 16, V. Einhaltung der Bestimmungen und Sanktionen, Rz 40 – 47.

23 ESMA: Leitlinien Meldung von Geschäften, Aufzeichnung von Auftragsdaten und Synchronisierung der Uhren nach MiFID II.

24 European Securities and Markets Authority.

25 Verodnung (EG) 683/2008 vom 9. Juli 2008 über die weitere Durchführung der europäischen Satellitenprogramme (EGNOS und Galileo).

26 Differential Global Positioning System.

2.6. Zeitsynchronisation

Das NTP[27] ist der verbreitetste Standard zur Synchronisation von Uhren in Computersystemen, die mit dem Internet vernetzt sind, und baut auf UDP[28] mit Port 123 auf. Für den Synchronisierungsprozess setzt NTP auf die UTC, die von den einzelnen Clients und Servern in einem hierarchischen System bezogen wird. Laut dem NTP Projekt existieren weltweit 4000 NTP Server, wobei der Österreichische NTP-Pool unter den Internet Adressen 0.at.pool.ntp.org, 1.at.pool.ntp.org, 2.at.pool.ntp.org und 3.at.pool.ntp.org nutzbar ist. Auch das BEV betreibt drei solcher NTP-Server, die direkt mit den Atomuhren des BEV verbunden sind. Die Zeitinformation dieser Zeitserver ist daher direkt an die Österreichische Normalzeit angeschlossen. Die Internet Adressen lauten bevtime1.metrologie.at, bevtime2.metrologie.at und time.metrologie.at.

3. Zeitforensik

Die Forensik bildet wissenschaftliche Methoden und Techniken zur Untersuchung von Verbrechen ab. In der Kriminaltechnik wird darunter auch die Spurensicherung verstanden. Da physische Spuren i.d.R. von sich aus keine Zeitstempel beinhalten oder auf solche referenzieren, müssen Forensiker mit Hilfe verschiedenster Techniken einen Zusammenhang mit einer Tatzeit rekonstruieren. Gem. der Definition nach Casey[29] sind „Digitale Spuren" keine physischen Spuren, sondern Daten, die in Computersystemen gespeichert werden. Des Weiteren weisen Daten vielfach auch Zeitstempel auf. Die wichtigsten zu nennen wären die Entstehungs-, Änderungs- und Lesezeit einer Datei, oder die Zeitstempel in verschiedensten Protokolldateien (Log-Dateien) wie in Betriebssystemen, Anwendungen oder Datenbanken. Mit Hilfe all dieser Zeitstempel lassen sich – so ferne die Uhr des Computersystems korrekt synchronisiert war, und diese Daten nicht vernichtet wurden – im wahrsten Sinne minutiös Abläufe zu Sachverhalten der Vergangenheit rekonstruieren.

3.1. Tatzeit und Erfolg

Der zeitliche und räumliche Geltungsbereich des Strafrechts wird in den §§ 61 ff. StGB[30] normiert, und damit wird lt. Triffterer auch „*festgelegt, auf welche Straftaten das Strafrecht welchen Staates anwendbar ist*."[31] Die Möglichkeiten der Bestimmung der Tatzeit und des Tatorts wird maßgeblich durch die Handlungstheorie in § 67 Abs. 1 StGB bestimmt: „*Die Tat wurde zu der Zeit begangen, da der Täter gehandelt hat oder hätte handeln sollen; wann der Erfolg eintritt, ist nicht entscheidend. Es kommt somit nur auf den Zeitpunkt des Handelns (bzw. bei Unterlassungsdelikten auf den Zeitpunkt, zu dem der Täter hätte handeln sollen) an. Der Zeitpunkt des Erfolgseintritts spielt bei der Bestimmung der Tatzeit keine Rolle.*"[32] Letzterer Satz ist insb. für Computerdelikte kritisch, da zu beachten ist, dass sich i.d.R. Tatzeit und Erfolg nicht wie in der realen Welt oftmals decken, sondern sich von wenigen ms bis hin zu wesentlich größeren Zeiträumen wie bspw. Tagen, Wochen und Monaten, wenn nicht im Falle von mit Malware befallenen Computern, die als Zombie-Rechner[33] in einem Botnet[34] agieren, sogar Jahren erstrecken können.

---

27 Network Time Protocol Version 4: RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5906: Network Time Protocol Version 4: Autokey Specification, RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4), RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6.

28 User Datagram Protocol: Verbindungsloses Internet Transport-Protokoll.

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

30 Strafgesetzbuch, BGBl. 60/1974 i.d.g.F.

31 Triffterer, Strafrecht Allgemeiner Teil I (1994) 21.

32 Tipold in Leukauf/Steininger, StGB Online, § 67, I. Möglichkeiten der Bestimmung der Tatzeit und des Tatorts, Rz 1.

33 Ein Computer im Internet, der durch Würmer, Viren oder Trojanischen Pferden kontrolliert und ferngesteuert wird, ohne dass der Benutzer es merkt.

34 Netzwerk verbundener Schadprogramme (Bots), abgeleitet von Roboter.

Daher ist es gerade bei Computerdelikten essenziell, dass ausgehend vom i.d.R. bekannten Erfolgszeitpunkt und mit Hilfe weiterer elektronischen Beweise, wie Log-Dateien oder Zeitstempel von Dateien, so ferne noch vorhanden, und sonstiger fallrelevanter Beweise ein noch unbekannter Tatzeitpunkt rekonstruiert werden kann, damit ein Tatverdächtiger, so ferne dieser noch nicht bekannt ist, ermittelt wird, er mit der Tat in Verbindung gebracht und seine Schuld bewiesen werden kann.

Die Kombination von Zeit und Ort der Vornahme der Tathandlung oder der Unterlassung wird durch die Einheits- oder Ubiquitätstheorie[35] bestimmt. Demzufolge hat der OGH in seiner Entscheidung vom 10.11.2006 erkannt, dass es für die Reichweite der österreichischen Strafgerichtsbarkeit entscheidend darauf ankommt *„ob es sich um eine Inlandstat oder um eine Auslandstat handelt. Für Inlandstaten gilt § 62 StGB, der die uneingeschränkte Geltung des Territorialitätspinzips normiert und demzufolge die österreichischen Strafgesetze für alle Straftaten gelten, die im Inland von wem immer an wem immer begangen worden sind. Ob der Täter Inländer oder Ausländer ist, spielt ebenso wenig eine Rolle wie die Nationalität des Opfers; maßgebend ist allein der inländische Tatort. Ein solcher liegt gemäß § 67 Abs 2 StGB im Sinne der geltenden Einheitstheorie vor, wenn der Ort, an dem der Täter gehandelt hat oder hätte handeln sollen oder ein dem Tatbild entsprechender Erfolg ganz oder zum Teil eingetreten ist oder nach der Vorstellung des Täters hätte eintreten sollen, im Inland liegt.*“[36]

Dem gegenüber steht im Strafrecht ein seltener Fall, jedoch im im Falle Cybercrime besonders häufiger, das Distanzdelikt: Hier wird durch das räumliche Auseinanderfallen von Handlung und Erfolg, w.z.B. wenn der Erfolg im Inland eingetreten ist, oder eintreten sollte, jedoch im Ausland gehandelt wurde. „*Das gilt auch in Bezug auf mehraktige Delikte oder Dauerdelikte. Es genügt, wenn im Inland bloß ein Zwischenerfolg eingetreten ist oder wenn der Erfolg zwar nicht im Inland eingetreten ist, aber nach den Vorstellungen des Täters hier hätte eintreten sollen.*“[37] Lt. Salimi gibt es keine Probleme, wenn der Erfolg an dem Ort eintritt, an dem auch gehandelt wurde. Allerdings spielt bei Distanzdelikten, „*bei denen Handlungs- und Erfolgsort auseinanderfallen, § 67 Abs 2 eine wichtige Rolle, indem er die Inlandstat auch auf Verhaltensweisen im Ausland ausdehnt, deren Erfolg aber im Inland eingetreten ist oder eintreten hätte sollen.*“[38]

I.d.Z. haben lt. Tipold sog. Transitverbrechen *„keinen inländischen Tatort. Ein solches Verbrechen liegt vor, wenn der Täter im Ausland handelt und auch der Erfolg im Ausland eintreten soll, gewisse Zwischenwirkungen aber auch in Österreich liegen, wenn also etwa eine Bombe mit der Post von München nach Belgrad gesandt wird, wobei der Postweg über Österreich führt. Nach der Ubiquitätstheorie wäre die Tat auch in Österreich strafbar.“*[37] Somit können auch Computerdelikte, die im Ausland begangen wurden, in Österreich verfolgt werden, wenn österreichische Computer oder Netze dafür als Mittel genutzt wurden.

Eine weitere und weniger granulare Bestimmung über die Zeit findet sich in § 68 Abs. 1 StGB: Demnach wird normiert, dass „*Jahre und Monate nach dem Kalender zu berechnen sind, Zeiträume werden so berechnet, daß der Tag, auf den das Ereignis fällt, mit dem der Zeitraum beginnt, nicht mitgezählt wird. Sie enden mit dem Ablauf des letzten Tages.*“ Diese Vorschriften über die Zeitberechnung gelten jedoch nur für Fristen des materiellen Strafrechts, wie die Rückfallsfristen und Probezeiten[39] sowie die Verjährungsfristen.

Obwohl die Definition der Zeit selbst durchaus präzise ist, kann es aufgrund verschiedener technischer Unzulänglichkeiten zu einer Fehlinterpretation oder im schlimmsten Fall sogar zu Datenverlusten kommen, was eine Strafverfolgung erschwert oder unmöglich machen kann. Daher folgt aus den o.a. Überlegungen, dass eine präzise Bestimmung der Tatzeit, samt Zeitzone – inbs. bei Begehung von Computerdelikten – wesentlich ist, wobei gerade die Zeitzone bei Delikten, die im Ausland begangen wurden vielfach entscheidend ist.

---

35 Kienapfel, Höpfel, Kert, AT15 E 12 Rz. 6; Oehler, Internationales Strafrecht Rz 246; Ambos, Internationales Strafrecht § 1 Rz 17.
36 OGH 12 Os 111/06z.
37 Tipold in Leukauf/Steininger, StGB Online, § 67, III. Einheitstheorie, Rz. 4 – 8.
38 Salimi in Höpfel, Ratz, Wiener Kommentar zum StGB, § 67.
39 Vgl. Rainer, SbgK § 68 Rz. 6 ff.

3.2. Technische Fallstricke

Aufgrund der Vielfältigkeit der Betriebssysteme, Dateisysteme, Anwendungen, Datenbanken u.v.m. werden Zeitstempel unterschiedlichst erzeugt, gespeichert und interpretiert. Obwohl die UTC heutzutage eine zentrale Rolle in der Datenverarbeitung spielt, existieren dennoch zahllose Legacy-Systeme mit unterschiedlichen Zeitformaten.

Einer der wesentlichsten Definitionen ist die Unix-Zeit, die für das Betriebssystem Unix entwickelt und im POSIX[40] Standard festgelegt wurde. Die Unixzeit zählt die vergangenen Sekunden seit Donnerstag, 1. Jänner 1970, 00:00 Uhr UTC. Das Startdatum wird auch als „The Epoch" bezeichnet. Die Umschaltung von einer Sekunde zur nächsten ist synchron zur UTC. Schaltsekunden werden jedoch ignoriert,[41] eine Synchronisation erfolgt allenfalls später über NTP. Zumal Android und die verschiedensten Unix Derivate wie Linux auf diesem Standard aufbauen, sind auch die Zeitstempel entsprechend (manchmal mit Unterschieden) vergleichbar. Auch Apple baut mit seinen Betriebssystemen iOS und macOS auf Unix auf, verwendet jedoch andere Zeitstempel: Der Kalender beginnt hier mit dem 1. Jänner 2001 mit ±10.000 Jahren. Bei der Synchronisierung von Dateisystemen kommt es bei Windows zu Problemen, da NTFS[42] und FAT[43] die Zeit mit verschiedener Genauigkeit auflösen. Verwendet FAT (nicht hingegen das auf USB-Sticks oder SD-Karten genutzte exFAT) die Lokalzeit ohne Zeitzonen, so baut NTFS auf UTC mit Zeitzonen auf. Obwohl NTFS grds. zu POSIX konform ist, beginnt die Zeitrechnung mit dem 1. Jänner 1601.

In Datenbanken, welche von verschiedensten Anwendungen genutzt werden, kommen je nach Produkt und verwendetem Datentyp andere Zeitformate zur Anwendung. Z.B. ist die Unix-Zeit unter SQLite und MySQL nutzbar. Den Julianischen Kalender, beginnend mit dem 1. Jänner 4712 A.D. kombiniert mit dem Gregorianischen, beginnend mit dem 15. Oktober 1582, unterstützen sowohl Oracle als auch SQLite. SAS[44] beginnt den Kalender mit den 1. Jänner 1960, und setzt dieses Datum als „Default" falls kein Datum eingetragen wird, anstatt korrekterweise „Null", also nichts. Dies führt u.U. zu eigenartig anmutenden Ergebnissen bei Datumsberechnungen.

Auch Anwendungen wie das weit verbreitete Microsoft Excel oder LibreOffice Calc unterstützen Zeitberechnungen: Hier beginnt der Kalender mit dem 30. Dezember 1899.

Diese verschiedenen Zeitstempel liegen vielfach nicht im Textformat wie nach ISO 8601 codiert, sondern entsprechen einer ganzen Zahl in Sekunden, was eine Umrechnung unter Berücksichtigung des jeweils genutzten Kalenders erforderlich macht. Da sich die Liste der Unterschiede beliebig verlängern ließe, wird an dieser Stelle die Nennung von Beispielen beendet.

Oftmals sind auch Spuren im Internet zu suchen, welche einem bestimmten Zeitpunkt zuzuordnen sind, aber die gesuchten Webseiten wurden längst verändert, oder existieren nicht mehr. Abgesehen von der Google Suchmaschine, welche auch historische Daten kurzfristig im „Cache" speichert, existieren längerfristige Archive, so wie das Internet Archive mit der „Wayback Machine".[45] Dieses Non-Profit Projekt ist das weltweit umfassendste Archiv von Inhalten im Internet, und archiviert aktuell nicht ganz 500 Milliarden Internetseiten, aber auch sonstige multimediale Inhalte der Vergangenheit. In Österreich müssen sämtliche öffentlich zugängliche Internetseiten unter der Domäne „.at" mit Bezug zu Österreich im Webarchiv der Österreichischen Nationalbibliothek höchstens vier mal im Jahr archiviert werden. Die gesetzliche Grundlage dazu bildet § 43b MedienG[46]. Beide Archive können als Quelle für Recherchen in der Vergangenheit dienlich sein.

---

40 POSIX.1-2017 is simultaneously IEEE Std 1003.1™-2017 and The Open Group Technical Standard Base Specifications, Issue 7.
41 https://pubs.opengroup.org/onlinepubs/9699919799/xrat/V4_xbd_chap04.html#tag_21_04_16, gelesen am 31.10.2020.
42 Microsoft: New Technology File System.
43 Microsoft: File Allocation Table.
44 The Essential Guide to SAS® Dates and Times, Art Carpenter & Derek P. Morgan, SAS Institute, June 2006.
45 https://archive.org/
46 Mediengesetz, BGBl. 314/1981 i.d.g.F.

3.3. Bewertung der Zeitstempel

Eine Bewertung der Zeitstempel hat aus den o.g. Gründen immer bezogen auf den Fall zu erfolgen. Eine Fälschung von Zeitstempeln ist zwar grds. technisch – auch spurenlos – möglich, da es sich lediglich um (meistens) ungeschützte Daten handelt. Jedoch erfordert eine Manipulation in Datei- und Betriebssystemen einerseits hohes technisches Fachwissen, andererseits sind Zeitstempel oftmals mehrfach redundant gespeichert, was Fälscher vielfach vergessen.

Der Forensiker hat daher Zeitstempel immer zu hinterfragen, und zu prüfen ob Inkonsistenzen vorhanden sind, auch jene, die nicht durch wie o.a. „Produkteigenheiten" erklärbar sind. Allenfalls hat er seine Suche auf weitere Spuren auszudehnen, und so einen Abgleich verschiedener Datenquellen, welche auf dasselbe Ereignis verweisen, vorzunehmen. Schließlich hat der Sachverständige die mit seinem Eid (§ 5 Abs. 1 SDG[47]) übernommenen Verpflichtungen bei seiner Tätigkeit, in wessen Auftrag diese auch immer erfolgt, sorgfältig und gewissenhaft einzuhalten. Auch lässt sich diese Sorgfaltsverpflichtung aus § 1299 ABGB, bzw. aus den berufsrechtlichen Vorschriften der jeweiligen Befugnisse ableiten.

3.4. Fallbeispiele

Die folgenden Praxisbeispiele sollen die vorher beschriebenen Effekte und Folgen beispielhaft verdeutlichen:

In einem Verfahren wg. Schadenersatz – es ging um eine Versicherungsleistung eines Turbinenschadens – wurden schließlich fehlende Einträge in den Log-Dateien eines Prozessleitsystems, welche von Klägerin, einer Versicherung, vorgelegt wurden, zur Streitfrage. Die beklagte Partei, der Hersteller der Turbine, jedoch nicht des Prozesssteuerungssystems, machte diesen Umstand geltend, da die Klägerin beweispflichtig ist. Die Überprüfung dieses Umstandes seitens der Klägerin ergab schließlich, dass im gegenständlichen Prozessleitsystem ein VBScript[48] täglich Daten aus einem Microsoft SQL-Server ausliest. Dabei wurde u.a. festgestellt, dass von April bis Oktober Daten ab 23:00 Uhr fehlen. Die Untersuchung ergab, dass das Script täglich um 01:00 lokaler Zeit gestartet wurde, was im Winter 00:00 (UTC) entsprach, und da die Zeitstempel der Datenbank in UTC gespeichert waren, funktionierte das Script korrekt. Nach Umstellung auf Sommerzeit wurde die Zeitdifferenz um eine Stunde vorgestellt, was bedingte, dass das Script um 23:00 (UTC) gestartet wurde, was zur Folge hatte, dass alle Zeitstempel von 23:00 bis Mitternacht fehlten. Dieses Beispiel ist eines von mehreren, wo aufgrund der Winter-/Sommerzeitumstellung es zu scheinbar unerklärlichen Phänomenen kommen kann, welche letztlich entscheidend für den Ausgang des Prozesses sein können.

Ein PC eines Angeklagten, der wg. §§ 207a Abs. 1 Z 2, 207a Abs. 3 erster und zweiter Fall, sowie 207a Abs. 3a StGB angeklagt war, sollte auf relevante Spuren hin untersucht werden. Es wurde u.a. die Beantwortung der Fragen begehrt, wann über die Programme AnyDesk und TeamViewer auf das Computersystem des Angeklagten zugegriffen wurde, und wann die im Strafantrag genannten Dateien, die Kinderpornografie enthalten, auf den Speichermedien gespeichert bzw. erstellt und ob dabei ein Zusammenhang zu den Zugriffen auf das Computersystem über TeamViewer und AnyDesk hergestellt werden kann. Die Untersuchung dieses PCs ergab, dass dieser zwar mit einem NTP-Server synchronisiert war, aber die Uhr auf GMT[49] (UTC+0) eingestellt war. Somit mussten sämtlichen Zeitstempeln eine Stunde hinzu gezählt werden. Da die zu untersuchenden Dateien aus dem gelöschten, aber nicht vernichteten „Recycler" stammen, konnte eine Reihenfolge der Entstehung der inkriminierten Dateien rekonstruiert werden: „Created" ist jener Zeitstempel, wann die Datei auf eine Festplatte kopiert wurde. Da alle „Modified" Zeitstempel älter als „Created" waren, mussten die Dateien von einer Festplatte auf die andere des PCs kopiert worden sein. Das klingt unlogisch, ist aber bei NTFS und FAT so gegeben, nicht jedoch bei Unix-Dateisystemen. Der neue „Created" Zeitstempel entspricht

[47] Sachverständigen- und Dolmetschergesetz: BGBl. 137/1975 i.d.g.F.
[48] Microsoft: Visual Basic Script.
[49] Greenwich Median Time.

somit dem Zeitpunkt des Kopierens auf den PC. Alle „Accessed“ Zeitstempel waren jünger als „Created“ , was bedeutet, dass diese Dateien zu diesem Zeitpunkten geöffnet wurden. Somit konnte die zeitliche Abfolge der Tat genau rekonstruiert werden: Dabei konnte durch Protokolle und mit Hilfe zahlreicher Zeitstempel nachgewiesen werden, dass die inkriminierten Daten dem Angeklagten zu exakt bestimmbaren Zeitpunkten von Dritten untergeschoben wurden, welche einen Adminstrator-Zugang zum inkriminierten PC besaßen, den sie als Tauschplattform für kinderpornographisches Material nutzten. Es konnte weiters bewiesen werden, dass der Angeklagte zu genau diesen Zeitpunkten seinen PC nicht nutzte. Es mussten daher aus o.g. Gründen eine neuerliche Ermittlung über andere Täter aufgenommen werden, deren Pseudonyme wie IP-Adressen aber auch natürliche Namen im Beweismaterial enthalten waren.

Ein wg. §§ 146, 147 Abs. 3, 148 2. Fall StGB und §28 Abs. 1 1. Satz 2. Fall SMG[50] Angeklagter soll über einen mehr als 10-jährigen Zeitraum zu Unrecht Honorare über nicht erbrachte Leistungen verrechnet haben. Eine Analyse aller Abrechnungsdatensätze aus diesem Zeitraum verbunden mit jenen aus der zentralen Datenbank des Leistungsträgers, einer Gebietskrankenkasse, ergab zahlreiche Differenzen: Eine dieser Unstimmigkeiten war, dass manchmal das Leistungsdatum mit 01.01.1960 bestimmt war. Die Untersuchung ergab, dass das Datenbanksystem SAS dieses Datum einträgt, wenn keines angegeben wurde – somit konnte dieser Differenz erklärt werden. Auch wurde festgestellt, dass in diesem Zeitraum das zentrale Abrechnungssystem drei mal geändert wurde, was unterschiedlichste Datenarten in diversen Darstellungsformaten erklärte, was bei der Auswertung ebenso zu Differenzen führte. Jedenfalls konnte durch umfangreiche Untersuchungen, wobei die (manchmal) jährlich geänderten Gesamtverträge mit geänderten Abrechnungsregeln ebenso zu berücksichtigen waren, festgestellt werden, dass die vorgelegten Beweise des Geschädigten authentisch und nicht manipuliert waren, was zu einer rechtskräftigen Verurteilung des Angeklagten – übrigens der Einzigen in drei analog gelagerten Fällen – führte. Dieser Fall verdeutlicht, dass das zu untersuchende Beweismaterial entsprechend seines einstigen, längst vergangenen Kontextes zu interpretieren ist.

Ein wg. § 125 2. Fall StGB, § 297 Abs. 1 2. Fall und § 288 Abs. 4 StGB Angeklagter legte Beweise eines Screenshots eines Handy SMS-Chats als JPEG[51] Bilder vor, wonach er angeblich mit Mord bedroht sein sollte. Des Weiteren behauptete er, dass die Uhrzeiten des belastenden Materials nicht stimmen können. Eine der zentralen Fragen war, ob es nachvollziehbar ist, wann dieser Screenshot angefertigt wurde, und wenn ja wie und ob dies manipuliert werden kann. Abgesehen von den gefundenen, offensichtlichen technischen Manipulationsspuren dieser Bilder, welche eine Fotomontage darstellten, war auf dem Screenshot eine Uhrzeit erkennbar: Der Angeklagte vergaß offenbar beim Editieren, dass die Uhrzeit 17:06 des Chats österreichischer Lokalzeit entsprach (UTC+1), an einer weiteren Stelle des Chats 12:06 (und am Handy 12:59) erkennbar waren. Der Angeklagte befand sich folglich zu dieser Zeit in der Zeitzone ATC[52] (UTC-4), und dieser Zeitunterschied von exakt 5 Stunden entsprach genau der Zeitdifferenzen im Chat, was schließlich einem beim Opfer gefundenen, als angeblich gefälscht angesehenen Chat entsprach, welcher mit unterschiedlichem, da getauschtem Text als Beweis vorgelegt wurde. Auch dieser Fall ist – abgesehen von der Fotomontage – ein Fall, wo Zeitstempel i.V.m. ihrem korrekten Kontext, der Zeitzone, zu interpretieren sind.

Ein wg. §§ 15 und 148a StGB Angeklagter buchte über Internet mit Hilfe fremder Kreditkartendaten Tickets, und führte Einkäufe online durch. Die Kreditkarte selbst wurde dabei nicht entwendet und befand sich zum Tatzeitpunkt im Besitz des Opfers. Aufgrund der Aufmerksamkeit des Opfers – dieses erhielt unmittelbar nach den Buchungen von der Bank eine SMS über diese Transaktionen – führten die Daten zu Tatverdächtigen: Mit Hilfe der Daten der Ticketbuchung wurden sie am nächsten Tag am Bahnhof von der Polizei erwartet. Obwohl keine Endgeräte sichergestellt wurden, konnte in Folge mit Hilfe von Protokollen, welche die Online Shops und der Zahlungsdienstleister zur Verfügung stellten, die Tathandlung rekonstruiert werden.

[50] Suchtmittelgesetz, BGBl. I 112/1997 i.d.g.F.
[51] Joint Photographic Experts Group (ISO/IEC 10918-1).
[52] Atlantic Standard Time.

Mit Hilfe der Zeitstempel konnte auch ein Bewegungsprofil des angeklagten Täters vom Tatort bis zu einem Ticketautomaten erstellt werden. Auch der Einkauf im Onlineshop konnte zeitlich exakt rekonstruiert werden, wie auch, dass abgelehnte Transaktionen wegen Überschreitung des Limits jedes Mal halbiert wurden, also in logarithmischer Zeit, was statistisch gesehen die wenigsten Versuche umfasst, und verdeutlicht, dass die Buchungen nicht willkürlich sondern vielmehr professionell erfolgten. Auch konnte beim zeitlichen Aufrollen des Beweismaterials der Verdacht erhärtet werden, dass dieser Angeklagte auch eine andere Identität führte. Dieser Fall ist ein Beispiel dafür, dass rasches und zeitnahes Handeln ein Mittel zum Erfolg sind. Ein Zuwarten oder eine Verzögerungen, wie bei Rechtshilfeverfahren bedingt, sind gerade bei Computerkriminalität hinderlich, da entscheidende Beweise unwiederbringlich vernichtet sind, je länger zugewartet wird.

Ein letzter beispielhafter Fall ist das e-card System des Gesundheitswesens: hier wurde vor Abnahme ein byzantinisch anmutendes (d.h. vollkommen nicht nachvollziehbares) Antwortzeitverhalten festgestellt, wo sich folglich Betreiber und Nutzer nicht über eine Abnahme einigen konnten. Die Lösung wurde mit Hilfe einer multidimensionalen Analyse – einem Datenwürfel über Nutzerort, Provider und Anwendungs-Requests samt den zugehörigen Responses, nur um einige wichtige Attribute zu nennen – erreicht, die wöchentlich ergänzt wurde. Die monatelangen Analysen führten schließlich zu einer defekten Hardware, einem Core-Router eines bestimmten Providers. Nach Hardwaretausch war das byzantinische Verhalten behoben, und es konnte eine erfolgreiche Abnahme stattfinden. Dieses Beispiel verdeutlicht, dass beständiges, über einen längeren Zeitraum beobachtendes Analysieren der verschiedensten Zeitstempel schließlich zur Lösung führen.

4. Bewertung und Ausblick

Diese beispielhaft beschriebenen Fälle geben den Sachverhalt natürlich nur stark gekürzt wieder. Tatsächlich erfordern die beschriebenen Analysen tlw. enorm viel Zeit und Sorgfalt des Sachverständigen. Die sorgfältige Berücksichtigung der Zeit samt den in dieser Publikation beschriebenen Fallstricken erscheint zwar selbstverständlich, ist jedoch keineswegs eine triviale Aufgabe. Nicht zu vergessen ist, dass so manche Analysten genau diese Faktoren vernachlässigen, was schließlich zu fehlerhaften Gutachten führt. Weiters zu beachten sind gesetzliche Normen, welche entsprechend anzuwenden sind. Eine Vernachlässigung dieser Rahmenbedingungen kann schließlich zu falsch bewerteten Tatzeiten, oder zivilrechtlich zu falsch bewerten Sachverhalten führen. Darüber hinaus wäre der Gesetzgeber aufgerufen, bzgl. der Abschaffung von Sommerzeit und Schaltsekunden, die nicht unerhebliche Probleme in Computersystemen schaffen können, endlich Klarheit zu schaffen.