Arbeitsergebnisse der Dissertation
„Klassifikation elektronischer Beweismittel für strafprozessuale Zwecke“[*]

vorgelegt von Claudia Warken

Berichterstatter: Prof. Dr. Gerhard Dannecker
Prof. Dr. Kai Cornelius

Lehrstuhl für Strafrecht und Strafprozessrecht unter besonderer Berücksichtigung europäischer und internationaler Bezüge, Prof. Dr. Gerhard Dannecker

I. Kernthesen der Arbeit

1. Die bereits heute große Bedeutung elektronischer Daten als Beweismittel im strafrechtlichen Ermittlungsverfahren nimmt weiter zu. Dennoch gibt es sowohl auf europäischer als auch auf nationaler Ebene nur vereinzelte, fragmentierte gesetzliche Vorschriften zu ihrer strafprozessualen Erlangung, Handhabung und Verwertung. Aufgrund der Bedeutung und der spezifischen Besonderheiten dieses Beweismittels, die allesamt auf der Unkörperlichkeit elektronischer Daten beruhen, kommt ein Rückgriff auf die Vorschriften, die sich auf analoge Beweismittel beziehen, nicht in Betracht. Vielmehr bedarf es spezieller Regelungen.

2. Die gesetzlich vorgesehenen Voraussetzungen jeder strafprozessualen Ermittlungsmaßnahme hängen von deren Eingriffsintensität ab, die wiederum auf der konkreten Schutzwürdigkeit des betroffenen Rechtsgutes basiert. Die Schutzwürdigkeit bei Eingriffen im Zusammenhang mit elektronischen Daten kann erheblich variieren, weil ihre Sensibilität ganz unterschiedlich ausfallen kann. Die unterschiedliche Sensibilität oder Schutzwürdigkeit ist wegen des verfassungsrechtlich verankerten Gleichbehandlungsgrundsatzes zwingend für jegliche Gesetzgebung in diesem Bereich zu beachten, so dass wesentlich Gleiches nicht ohne sachlichen Grund ungleich und wesentlich Ungleiches nicht ohne sachlichen Grund gleich behandelt wird.

---

[*] Die zugrundeliegende vollständige Promotionsarbeit wurde von der Autorin als Inauguraldissertation bei der Juristischen Fakultät der Universität Heidelberg eingereicht und im Juli 2019 zur Veröffentlichung freigegeben. Sie wird ab dem Sommer 2019 als open access Publikation auf dem Dokumentenserver der Universität Heidelberg HeiDOK unter http://archiv.ub.uni-heidelberg.de/volltextserver/ öffentlich zugänglich sein. Auf die dortige umfängliche Quellenzitierung wird verwiesen.

3. Die erforderliche gesetzliche Neukonzeptionierung zum Umgang mit elektronischen Beweismitteln im Strafermittlungsverfahren muss durch angemessene Kategorisierungen die unterschiedliche Schutzwürdigkeit verschiedener Typen elektronischer Daten widerspiegeln. Die allgemein angewandte Differenzierung von Kommunikationsdaten in Inhalts- und Metadaten beziehungsweise Inhalts-, Verkehrs- und Bestandsdaten, auf die sich auch die einschlägigen Regelungen in der StPO beziehen,[1] genügt den Anforderungen der modernen Gesetzgebungslehre nicht.

4. Zur Vornahme einer neuen Klassifizierung bedarf es der Bestimmung eines geeigneten Unterscheidungskriteriums. Kriterien, die derzeit in der Literatur diskutiert werden, wie beispielsweise der abstrakte Dateninhalt, das Datenvolumen oder das Dateiformat, sind ungeeignet.

5. Da eine angemessene Datenklassifikation nur auf den einschlägigen Grundrechten des Datensubjekts beruhen kann, ist das maßgebliche Unterscheidungskriterium, aus dem sich die Schutzwürdigkeit eines einzelnen Datensatzes unmittelbar ableiten lässt, allein **die berechtigte Erwartungshaltung der Vertraulichkeitswahrung des Datensubjekts**.

6. Aus dem genannten Kriterium ergibt sich eine mögliche Unterscheidung wie folgt (Auflistung nach abnehmender Schutzwürdigkeit):

- **Daten, die den Kernbereich der privaten Lebensgestaltung betreffen,**
- **geheime Daten,**
- **vertrauliche Daten,**
- **beschränkt zugängliche Daten und**
- **unbeschränkt zugängliche Daten.**

7. Die vorgeschlagene Klassifikation ist systemkohärent mit den Kategorisierungsmodellen der analogen Beweismittel. Sie kann stimmig in das Strafprozessrecht übernommen werden und erlaubt, wie anhand eines konkreten gesetzlichen Musterentwurfes gezeigt wird, eine umfassende, technikunabhängige und damit beständige gesetzliche Neuregelung, die den Anforderungen der modernen Gesetzgebungslehre entspricht.

1 Vgl. §§ 100g, 100j und (indirekt) § 100d StPO.

II. Erläuterungen

1. Zur Bedeutung und den spezifischen Besonderheiten elektronischer Beweismittel

Der Begriff elektronische Beweismittel bezieht sich, grob gesprochen, auf alle Daten oder Informationen, die in einer Form vorliegen, die unmittelbar eine Verarbeitung in einem Computersystem erlaubt. Mit der Digitalisierung des Alltags, der weiten Verbreitung mobilfunk- beziehungsweise internetbasierter Kommunikation und der wachsenden Bedeutung des Internets der Dinge (Stichworte: „smart homes“, autonomes Fahren etc) treten elektronische Beweismittel im Strafermittlungsverfahren zunehmend in den Vordergrund.
Zudem beziehen sie sich nicht nur auf klassische Internetdelikte wie das Abfangen und Ausspähen von Daten, Computersabotage, Ransomware- oder DDoS-Angriffe, sondern können mittlerweile potentiell für jegliche Straftaten eine entscheidende Rolle spielen. In diesem Zusammenhang sei beispielsweise an die computerbasierte Manipulation eines Herzschrittmachers erinnert, die in den Bereich der klassischen Körperverletzungsdelikte fällt, oder an die Begehung eines Betruges mittels Phishing.

Aus technischer Sicht stellen elektronische Beweismittel zunächst nichts weiter als eine Notation mit zwei Variablen, 0 und 1, dar. Sie sind – anders als mögliche Datenträger - unkörperlich und unterscheiden sich dadurch maßgeblich von allen anderen, körperlichen Beweismitteln. Daraus ergeben sich verschiedene Konsequenzen:

Zum einen bewirkt ihre „Übergabe“ keinen automatischen Gewahrsamswechsel; der Originaldatensatz verbleibt für gewöhnlich beim Dateninhaber, während der Empfänger durch elektronische Übertragung, Übergabe eines Speichermediums oder einer Visualisierung beispielsweise durch einen Ausdruck in Papierform häufig nur eine Datenkopie erlangt.

In tatsächlicher Hinsicht kann ein Zugriff auf einen bestimmten Datensatz zudem grundsätzlich von überall aus erfolgen, solange die beteiligten Datenverarbeitungsgeräte mit dem Internet verbunden sind.

Gerade im Ermittlungsverfahren spielt der Zeitfaktor eine erhebliche Rolle, weil elektronische Daten im Wortsinne „mit einem Klick“ in nahezu Lichtgeschwindigkeit und ungeachtet territorialer Grenzen von einem Ort der Welt zu einem anderen verschoben oder ganz gelöscht werden können.

Schließlich erlaubt die Anonymität im Netz eine deutlich effektivere Verschleierung der Datenherkunft und -veränderung, als dies bei analogen Beweismitteln möglich wäre, so dass auch von einer erhöhten Manipulationsanfälligkeit auszugehen ist.

2. Die derzeitige Rechtslage

Die derzeitigen strafprozessualen Regelungen auf nationaler wie auf supranationaler Ebene werden den genannten Besonderheiten weder quantitativ noch qualitativ gerecht.

Dies gilt trotz der jüngsten Ergänzungen wie beispielsweise der Überarbeitung des § 100a StPO zur Einführung der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und der Einführung der online-Durchsuchung über § 100b StPO im Sommer 2017, des US-amerikanischen CLOUD Acts vom Februar 2018[2] oder des aktuellen „e-evidence"-Vorschlags der Europäischen Kommission vom April 2018[3]. Die vorhandenen Regelungslücken beeinträchtigen nicht nur die allgemeine Rechtssicherheit, sondern auch den Grundrechtsschutz des Einzelnen sowohl auf Täter- als auch auf Opferseite. Daher bedarf es dringend einer umfassenden gesetzlichen Neuregelung zum strafprozessualen Umgang mit elektronischen Beweismitteln.

3. Allgemeine Anforderungen an den Gesetzgeber

Unterschiedliche Ermittlungsmaßnahmen unterliegen unterschiedlichen Voraussetzungen und Umsetzungsanforderungen; die Strafprozessordnung kennt nicht nur verschiedene Stufen des Tatverdachts, sondern differenziert beispielsweise auch hinsichtlich der Anordnungs- und Durchführungsbefugnisse, der Dauer einer Maßnahme, der Mitteilung an den Betroffenen und der gerichtlichen Überprüfbarkeit.

Allgemein lässt sich feststellen, dass die Anforderungen umso strikter sind, je eingriffsintensiver sich eine Maßnahme auf die Grundrechte des Betroffenen auswirkt. Die Eingriffsintensität hängt dabei maßgeblich von der konkreten Schutzwürdigkeit des betroffenen Rechtsgutes ab.

In Bezug auf elektronische Daten ist prinzipiell anerkannt, dass ihre Schutzwürdigkeit stark variieren kann. Es gibt höchst sensible Datensätze, solche mit kaum nennenswerter Schutzwürdigkeit und ein weites Spektrum zwischen diesen beiden Polen.

---

2 Clarifying Lawful Overseas Use of Data Act (CLOUD Act, H.R. 4943, https://www.congress.gov/bill/115th-congress/house-bill/4943), in Kraft seit 23.03.2018.

3 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen vom 17.04.2018 (COM/2018/225 final), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018PC0225&from=DE; sowie Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren vom 17.04.2018 (COM/2018/226 final), https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018PC0226&from=DE.

Aufgrund des in Art. 3 GG verfassungsrechtlich verankerten Gleichbehandlungsgrundsatzes, wonach wesentlich Gleiches nicht ohne sachlichen Grund ungleich und wesentlich Ungleiches nicht ohne sachlichen Grund gleich behandelt werden darf, ist der Gesetzgeber verpflichtet, die unterschiedliche Schutzwürdigkeit einzelner Datensätze zu berücksichtigen und deswegen Datenklassen zu bilden, die in sich homogen, also „gleich“ und im Verhältnis zueinander nach der unterschiedlichen Schutzwürdigkeit differenzierend, also „ungleich“ sind. Nur dann kann im Rahmen der gesetzgeberischen Prärogative sinnvoll geprüft werden, ob es einen sachlichen Grund für die (Un-)Gleichbehandlung zweier oder mehrerer Datenklassen gibt.

4. Die bisherige Differenzierung

Im nationalen wie internationalen Kontext hat sich eine Differenzierung von Kommunikationsdaten in Inhalts- und Metadaten beziehungsweise Inhalts-, Verkehrs- und Bestandsdaten durchgesetzt. Sie beruht auf den praktischen Bedürfnissen der traditionellen Telekommunikationsdienstleister, die diese Einteilung Anfang der 1990-er einführten, als die damals übliche ortsgebundene und grundsätzlich auf zwei Kommunikationspartner beschränkte Fernkommunikation technisch von analoger auf digitale Informationsübermittlung umgestellt wurde. Die Einteilung wurde zunächst im Datenschutzrecht und sodann sukzessive auch im Strafprozessrecht übernommen.

Sie ist insoweit problematisch, als sie sich ausschließlich auf Kommunikationsdaten bezieht und somit sonstige elektronische Daten, wie beispielsweise beim Verdächtigen gespeicherte aber nicht weitergegebene Daten oder solche, die im Internet der Dinge von Maschine zu Maschine ausgetauscht werden, nicht erfasst, obwohl auch diese Daten unterschiedlich schutzwürdig sein können.

Zudem entspricht die gängige Unterscheidung nicht mehr dem klassischen Nutzerbild, da Telekommunikation heute zunehmend über Mobilfunkgeräte oder Internet-Anwendungsprogramme wie WhatsApp oder Skype durchgeführt wird und dabei häufig mehr als zwei Beteiligte an einer konkreten Kommunikation teilnehmen; Beiträge in Chaträumen und Postings sind dafür entsprechende Beispiele. Die allgemeine Verfügbarkeit der technischen Möglichkeiten und ihre einfache, kostengünstige Nutzung haben zudem zu einer generellen Trivialisierung der Kommunikationsinhalte geführt. Daneben senden mobile Geräte teilweise ohne Kenntnis des Betroffenen permanent Metadaten wie beispielsweise Geräte- oder Lokalisationsdaten an Datenverarbeitungszentren, die im Einzelfall aus Sicht des Datensubjekts eine besondere Sensibilität aufweisen können, zumal wenn sie zur Erstellung beispielsweise eines Bewegungsprofils verarbeitet werden.

Aufgrund all dieser Entwicklungen kann entgegen der derzeit gängigen

Auffassung nicht mehr allgemein unterstellt werden, dass elektronische Kommunikationsinhaltsdaten per se schutzwürdiger wären als Metadaten, zumal eine rechtliche Begründung für diese Annahme fehlt.

5. Ein neuer Ansatz

Eine verfassungskonforme Datenklassifikation, die die unterschiedliche Schutzwürdigkeit verschiedener Datensätze widerspiegelt, darf nur auf den einschlägigen Grundrechten des Betroffenen beruhen. Diese sind das Fernmeldegeheimnis des Art. 10 Abs. 1 GG, das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Die beiden letztgenannten wurden vom Bundesverfassungsgericht im sogenannten „Volkszählungsurteil“[4] bzw. im Urteil zum „Großen Lauschangriff“[5] aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1, 1 Abs. 1 GG entwickelt.

Die Bezugnahme auf praktische Bedürfnisse der Kommunikationsdienstleister ist ebenso unzulässig wie diejenige auf technische Kriterien (Datenvolumen, Datenherkunft, Datenformat, Datenzustand) oder rechtspolitische Aspekte (Relevanz der konkreten Daten für das Strafverfahren, Schwere des zugrundeliegenden Deliktes, anwendbare Ermittlungsmaßnahmen).

Das maßgebliche Unterscheidungskriterium, mit dem sich die Schutzwürdigkeit eines einzelnen Datensatzes unmittelbar aus den einschlägigen Grundrechten herleiten lässt, liegt allein in der **berechtigten Erwartungshaltung der Vertraulichkeitswahrung des Datensubjekts**.

Die Betonung der berechtigte Erwartungshaltung schließt einerseits unangemessene und überzogene Erwartungen aus und erlaubt andererseits eine Objektivierung des subjektiven Ansatzes. Sie richtet sich maßgeblich danach, ob der Datenberechtigte seine Information überhaupt mit Dritten teilt und, wenn ja, mit wem. Im letzteren Fall ist vorrangig auf die Anzahl der Datenempfänger und auf ihr Verhältnis zum Datenberechtigten abzustellen. So kann zum Beispiel zwischen Personen der höchsten Vertraulichkeit (die nicht zwingend identisch mit den Zeugnisverweigerungsberechtigten im Sinne des § 52 StPO sind), persönlich bekannten, aber nicht besonders Nahestehenden und gänzlich Unbekannten, die beispielsweise über eine Massenkommunikation erreicht werden, unterschieden werden.

Die Bezugnahme auf die Erwartungshaltung verdeutlicht die Maßgeblichkeit der ex-ante Sicht des Betroffenen. Für die strafprozessuale Einteilung ist es daher unerheblich, ob sich im konkreten Fall die Erwartung erfüllt oder, etwa durch

4 BVerfG, Urteil vom 15.02.1983, 1 BvR 209/83, zugleich BVerfGE 65, 1.

5 BVerfG, Urteil vom 03.03.2004, 1 BvR 2378/98, zugleich BVerfGE 109, 279.

einen Vertrauensbruch durch eine unerwartete Weitergabe vertraulicher Informationen durch den informierten Dritten, die Erwartung enttäuscht wird. Vertraulichkeitswahrung meint schlicht die Nichtweitergabe der betreffenden Daten, während das Datensubjekt der originäre Datenberechtigte ist.

Das neu vorgestellte Kriterium erlaubt folgende Klassifizierung:

Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, sind absolut geschützt und damit unantastbar. Diese vom Bundesverfassungsgericht für sämtliche, also analoge wie elektronische Daten entwickelte Kategorie ergibt sich letztlich aus dem Schutz der Menschenwürde, wie er in Art. 1 Abs. 1 GG festgehalten ist. Sie greift nur im Ausnahmefall und kann ausschließlich auf Grundlage der konkreten Umstände des Einzelfalles festgestellt werden.

Geheime Daten genießen einen erhöhten, wenngleich nicht absoluten Schutz, weil sie nach dem Willen des Grundrechtsträgers nicht für Dritte zugänglich sein sollen und er daher davon ausgehen darf, dass die entsprechenden Informationen geheim bleiben. Sie umfassen beispielsweise Daten, die der Betroffene lediglich auf seinem Rechner oder in der Cloud speichert, ohne dass sonstigen Personen Zugang zu diesen Daten eingeräumt wird.

Eine etwas abgestufte Schutzwürdigkeit erfahren **vertrauliche Daten**, die im Unterschied zu geheimen Daten zwar weitergegeben werden, allerdings ausschließlich an solche Personen, in deren Motivation und Identität der Betroffene ein besonders schutzwürdiges Vertrauen setzen darf. Gedacht sei hier beispielsweise an besonders Nahestehende oder Berufsgeheimnisträger wie Rechtsanwälte oder Priester.

Eine deutlich verminderte Schutzwürdigkeit betrifft **beschränkt zugängliche Daten**, die sich von den vertraulichen Daten durch das Fehlen der besonderen persönlichen Beziehung der Kommunikationsbeteiligten unterscheiden, wobei die einzelnen Empfänger aus Sicht des Grundrechtsträgers immer noch individualisierbar sind.

Kein besonderer datenspezifischer Grundrechtsschutz kommt schließlich **unbeschränkt zugänglichen Daten** zu. Ihnen unterfallen neben nicht-personenbezogenen Daten wie beispielsweise reiner Maschine-zu-Maschine Kommunikation auch öffentlich zugängliche personenbezogene Daten, die etwa über öffentliche Chaträume einer unbekannten Vielzahl von Personen zugänglich gemacht werden, und schließlich solche, die entweder das Datensubjekt oder ein informierter Dritter rechtmäßig an die Strafverfolgungsbehörde weitergibt.

6. Fazit und Ausblick

Die vorgeschlagene Neuklassifikation elektronischer Beweismittel beseitigt die rechtlichen und tatsächlichen Unzulänglichkeiten des derzeit gängigen Klassifikationsmodells.

Sie entspricht den Wertungen der StPO im Hinblick auf die analogen Beweismittel, ist also systemkohärent und kann stimmig in das Strafprozessrecht übernommen werden.

Der in der Promotionsarbeit vorgestellte und erläuterte ausführliche Gesetzesentwurf belegt, dass auf der Grundlage des neuen Modells eine umfassende, technikunabhängige und damit beständige gesetzliche Neuregelung möglich ist, die den Anforderungen der modernen Gesetzgebungslehre entspricht.

Die Arbeit schließt mit der nicht abschließenden Auflistung von – nach Ansicht der Autorin durchaus lösbaren - Fragen, die das neue Klassifikationsmodell dadurch aufwirft, dass es auf unbestimmten Rechtsbegriffen basiert.

Diesbezüglich ist insbesondere klärungsbedürftig, welcher Grad an Vertraulichkeitserwartung im „Cyberspace“ überhaupt berechtigt sein kann, welche Bedeutung der bewussten Datenverschlüsselung zukommt, wie das Auseinanderfallen von Vertraulichkeitserwartung und tatsächlicher Entwicklung zu berücksichtigen ist und wie die Bestimmung des Datensubjekts beispielsweise bei Personengruppen, juristischen Personen oder Datengenerierungen im Internet der Dinge vorgenommen werden kann.