Jan Fährmann[1]/Alexander Vollmar[2]/Gudrun Görlitz[3]

Rechtliche Anforderungen an die Übertragung von Positionsdaten an die Polizei als Beweismittel für Strafverfahren

1. Einführung

Für die Beweisführung in Strafverfahren gegen Dieb*innen bzw. Hehler*innen können Positionsdaten von besonderer Bedeutung sein,[4] da sie sowohl Rückschlüsse auf die Position und Bewegungen von Beschuldigten, Zeug*innen als auch auf Tatgegenstände erlauben. Werden Positionsdaten in zeitlicher Abfolge verknüpft, können Bewegungen sowie die Bewegungsgeschwindigkeit von Gegenständen nachvollzogen werden, was auch Rückschlüsse auf das Verhalten sowie die Beziehung von Personen zueinander und damit auf das Vorliegen von objektiven und ggf. auch von subjektiven Tatbestandsmerkmalen und weiteren für das Strafverfahren relevanten Tatsachen erlaubt.[5]

Positionsdaten werden im Allgemeinen digital erhoben. Digitale Beweismittel sind von erheblicher Bedeutung für die gerichtliche und polizeiliche Beweisführung, und es ist damit zu rechnen, dass diese Bedeutung noch weiter ansteigt.[6] Dies ist u. a. darauf zurückzuführen, dass digitale Daten von Behörden, Firmen und Privatleute mittlerweile in nahezu jedem gesellschaftlichen Kontext über Smartphones, Computer, Kameras, Haushaltsgeräte, Fitnesstracker und andere digitale Anwendungen erhoben werden, die Geräte untereinander Informationen austauschen und damit stetig neue Daten kreieren.[7] So kann über die Auswertung eines Smartphones etwa festgestellt werden, wo eine Person sich aufgehalten und ggf. was sie dort gemacht hat, wenn sie das Smartphone etwa zur Bezahlung eingesetzt hat. Auch verlagern sich zahlreiche Verhaltensweisen

---

1 Dr. Jan Fährmann war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die rechtlichen und kriminologischen Forschungsfragen.

2 Alexander Vollmar war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die Forschungsfragen aus dem Bereich Informatik.

3 Prof. Dr. Gudrun Görlitz hat das Projekt FindMyBike für den Bereich Informatik geleitet.

4 Vgl. Warken NZWiSt 2017, S. 291 m. w. N.

5 Momsen 2020, S. 77.

6 Fährmann, MMR 2020, S. 228 ; Schuba 2016, S. 241 ff.; Momsen 2015, S. 71; Sieber 2012, S. 67.

7 Momsen 2020, S. 77.

- etwa die soziale Interaktion (z. B. in sozialen Netzwerken) - vermehrt in den digitalen Raum.[8] Bereits heute sind daher digitale Daten in kaum bearbeitbaren Mengen vorhanden.[9] Dies stellt die Justiz vor zahlreiche Herausforderungen und Schwierigkeiten. Einerseits sind bei der Aufbewahrung und Verwendung digitaler Daten besondere Anforderungen zu beachten und einzuhalten. Andererseits müssen Konzepte und technische Lösungen entwickelt werden, wie Polizei, Justiz und Verteidiger*innen sowie sonstige Beteiligte eines Strafverfahrens mit den Datenmengen umgehen können und wie ein hoher Beweiswert der Daten sichergestellt wird.[10] Dabei stellt sich nicht nur die Frage nach einer elektronischen Aktenführung sondern auch das Problem, wie Daten im Strafverfahren elektronisch ausgewertet und übertragen werden können.[11] Dieser Beitrag legt exemplarisch dar, welche Anforderungen zur Sicherung der Integrität und Authentizität an digitale Positionsdaten zu stellen sind. Dabei beziehen sich die Ausführungen auf den Beweis von Diebstahls- und Hehlerei-Delikten. Zudem wird beschrieben, wie mittels der im *FindMyBike*-Projekt entwickelten Anwendung – *FindMyBike-System* –[12] Positionsdaten von privaten Trackingservice-Anbieter*innen so an die Polizei übertragen werden können, dass im IT-System und bei der Übertragung eine hohe Beweisqualität gesichert wird.

2. Gerichtliche Verwertbarkeit von Positionsdaten

Die Einhaltung strafverfahrensrechtlicher Regelungen in Ermittlungsverfahren ist eine Kernanforderung an die Strafverfolgungsbehörden in Rechtsstaaten. Die Verwertbarkeit und die Beweisqualität von Positionsdaten gestohlener Gegenstände hängen maßgeblich davon ab, ob die einschlägigen rechtlichen Anforderungen im Ermittlungsverfahren eingehalten wurden. Im Folgenden wird zunächst erläutert, wie digitale Daten in die gerichtliche Verhandlung eingeführt werden und welche Rückschlüsse aus ihnen gezogen werden können. Aufbauend auf diesen Erkenntnissen ergeben sich spezifische Anforderungen, die die Beweisqualität der Positionsdaten bestimmen. Abschließend werden Voraussetzung für eine hohe Beweisqualität digitaler Daten hergeleitet und beschrieben, wie diese im *FindMyBike-System* umgesetzt wurden.

8 Müller, NZWiSt 2020, S. 96.
9 Vgl. Müller, NZWiSt 2020, S. 96; Momsen 2015, S. 75; Freiling/Sack DuD 2014, S. 112 f.
10 Ausführlich dazu Fährmann, MMR 2020, S. 228 ff.
11 Vgl. dazu etwa Freiling/Sack DuD 2014.
12 Umfassend zum *FindMyBike-System* Vollmar/Görlitz/Kober in diesem Band, S. 227ff.

2.1 Positionsdaten als Beweismittel

Beweismittel müssen geeignet sein, den Beweis der Schuld oder der Unschuld der Angeklagten zu erbringen oder zur Erbringung beizutragen. Diese Anforderung gilt auch für Positionsdaten, die als Beweismittel in einem Strafverfahren dienen sollen.

2.1.1 Was kann durch Positionsdaten bewiesen werden?

Nach § 261 StPO muss das Gericht nach seiner freien, aus der Gesamtbetrachtung der Verhandlung geschöpften Überzeugung entscheiden, wobei alle Beweise zu würdigen sind. Die richterliche Überzeugung ist die subjektive, persönliche Gewissheit der Richter*innen.[13] Eine Verurteilung kann demnach nur erfolgen, wenn das Gericht aufgrund der Hauptverhandlung von der Schuld der Angeklagten voll überzeugt ist.[14] Der Schuldspruch muss dazu auf einer tragfähigen Beweisgrundlage beruhen, die die objektive hohe Wahrscheinlichkeit der Richtigkeit des Beweisergebnisses ergibt.[15] Eine Verurteilung kann nur auf bewiesene (Indiz-)Tatsachen gestützt werden; bloße Vermutungen genügen nicht.[16] Das Gericht muss sich mit allen wesentlich für und gegen die Angeklagten sprechenden Umständen auseinandersetzen.[17] Dazu müssen die Beweise unmittelbar in die Verhandlung eingeführt und gewürdigt werden (§§ 250 StPO ff.). Die richterliche Überzeugung erfordert ein nach der Lebenserfahrung ausreichendes Maß an Sicherheit bzgl. der Schuld, dem vernünftige Zweifel nicht mehr entgegenstehen.[18] Bloße theoretische Zweifel an der Schuld bleiben unberücksichtigt, da die Anforderungen an eine Verurteilung nicht überspannt werden dürfen.[19]

Den Umstand, ob sich die Schuld der Beschuldigten beweisen lässt, muss auch die Polizei und vor allem die verfahrensleitende Staatsanwaltschaft bei der Entscheidung berücksichtigten, ob weitere Ermittlungen erforderlich sind und ob Anklage zu erheben ist. Insofern kann das Verfahren bereits einzustellen sein, wenn deutlich wird, dass vor Gericht eine Beweisführung nicht gelingen wird, § 170 Abs. 2 StPO.

Unter welchen Umständen ist aber eine Beweisführung mittels digitaler Positionsdaten gestohlener Gegenstände vor Gericht zur Aufklärung von Dieb-

13 Z. B. BGHSt 10, 208 (209).
14 Meyer-Goßner/Schmitt Meyer-Goßner 2022, § 261, Rn. 1.
15 BVerfG NJW 2003, 2444 (2445).
16 Meyer-Goßner/Schmitt-Meyer-Goßner 2022, § 261, Rn. 2 m. w. N.
17 BGH NJW 1988, 3273 (3273 f.), BGH NStZ 1990, 404 (404 f.).
18 St. Rspr. z. B. BGH NStZ 2010 293 (293).
19 Meyer-Goßner/Schmitt-Meyer-Goßner 2022, § 261, Rn. 2 m. w. N.

stählen und Hehlerei vorstellbar? Dabei muss beachtet werden, dass die Position des Gegenstandes allein oftmals noch keine konkreten Rückschlüsse auf das Tatgeschehen zulässt, da lediglich belegt wird, dass sich dieser an einem bestimmten Ort befunden hat. Speziell beim Diebstahl von mobilen Gegenständen wie Fahrzeugen ist nur zu erkennen, dass dieses an einen bestimmten Ort bewegt wurde. Liegen Positionsdaten in einer zeitlichen Abfolge vor, dann ist erkennbar, welche Routen mit dem Gegenstand zurückgelegt wurden. Welche Person das Diebesgut gestohlen hat und zu welchem Zeitpunkt eine bestimmte Person dieses im Gewahrsam hatte, lässt sich anhand von Positionsdaten allein nicht bestimmen. Dies gilt insbesondere bei Gegenständen, die leicht weitergegeben werden können. Anhand der Daten kann ggf. nur erkannt werden, ob ein entsprechender Wechsel möglich war. Das ist dann der Fall, wenn beispielsweise ein Fahrzeug zum Stillstand gekommen ist. Auch wird vielfach nicht ersichtlich, ob und ggf. wie Sicherungsmaßnahmen überwunden wurden – etwa ein Schloss bei einem Fahrraddiebstahl;[20] was für die Beurteilung der Frage entscheidend ist, ob ein einfacher Diebstahl nach § 242 StGB vorliegt oder ob ein Fall der §§ 243 oder 244 StGB in Betracht kommt. Die Bestimmung des dem Tatverdacht zugrundeliegenden Deliktes hat nicht nur Einfluss auf die zu erwartende Strafe, sondern auch darauf, welche Ermittlungsmaßnamen die Strafverfolgungsbehörden einsetzen dürfen; tendenziell gehen bei schweren Delikten die Ermittlungskompetenzen weiter. Insofern wird deutlich, dass Positionsdaten im Regelfall nur Indizienbeweise sind und, dass weitere (Indizien-)Beweise zum Beweis der Schuld notwendig sind.

Aber auch Indizienbeweise können für den Beweis der Schuld von wesentlicher Bedeutung sein. Bei vielen Diebstahlsdelikten sind weitere Ermittlungsansätze erforderlich, etwa beim Fahrraddiebstahl, bei dem der Polizei oft Ermittlungsansätze fehlen.[21] Insofern können auch Positionsdaten als Indizienbeweise dazu führen, dass die Aufklärungsquote gesteigert wird. Von großer Bedeutung für das Ermittlungsverfahren ist, ob der Standort des Fahrrades überhaupt ermittelt werden kann. Dies führt dazu, dass die Polizei nicht nur das Diebesgut beschlagnahmen kann, sondern, dass ausgehend von dem Standort weitere Ermittlungsansätze bestehen können, sodass auch weitere Ermittlungsmaßnahmen, wie Beschuldigten- oder Zeug*innenvernehmung und ggf. Durchsuchungsmaßnahmen, in die Wege geleitet werden können.

In der Konstellation, dass das Diebesgut in zeitlicher und räumlicher Nähe zusammen mit den Täter*innen aufgespürt wird, dürfte zwar vielfach die Einführung der Positionsdaten in das Hauptverfahren nicht entscheidend für den

20 Bei einigen Fahrradflottenbetreibern werden die Daten mittlerweile jedoch direkt vom Schloss erhoben.

21 Ausführlich dazu Matzdorf in diesem Band, S. 69ff.

Verfahrenseingang sein. In dieser Situation ist es vielfach wahrscheinlich, dass der gestohlene Gegenstand noch nicht weitergegeben wurde, sodass damit zu rechnen ist, dass gleichzeitig mit ihm auch die Dieb*in aufgespürt wurde. Jedoch sind die Tatumstände und die Beweissituation im Einzelnen zu würdigen, sodass es auch in einer solchen Konstellation auf die Beweisführung mit Positionsdaten ankommen kann. So können mittels der Positionsdaten Einlassungen der Beschuldigten wider- oder belegt werden. Etwa könnten die Beschuldigten vorbringen, dass sie den Gegenstand erst vor zwei Tagen erworben hätten. Dem würde beispielsweise der Umstand entgegenstehen, dass dieser bereits Tage zuvor vor dem Haus des oder der Beschuldigten gestanden hat oder in das Haus verbracht wurde. Auch können andere Orte wie der Arbeitsplatz oder übliche Aufenthaltsorte von Freunden und Familie sowie Orte, an denen die Beschuldigten regelmäßig ihre Freizeit verbringen, im Abgleich mit den Positionsdaten des Diebesgutes Rückschlüsse auf die Tatumstände möglich machen.

Denkbar sind zudem viele Situationen, in denen Positionsdaten für das Verfahren entscheidend sind, etwa bei der Überprüfung der Angaben von Angeklagten oder Zeug*innen.[22] So können Beschuldigte etwa eine Veräußerungssituation schildern. Diese kann durch die Positionsdaten belegt oder widerlegt werden. Beispielsweise kann sich der gestohlene Gegenstand einige Zeit auf einem Flohmarktgelände befunden haben, was für die Schilderung spräche, dass dieser dort erworben wurde. Dies kann allerdings neben einem Diebstahlsverdacht auch einen Tatverdacht der Hehlerei begründen.

Positionsdaten können überdies dazu beitragen, einen Gegenstand, welcher ohne die Beschuldigten aufgefunden wurde, einer bestimmten Person zuzuordnen, was wiederum Rückschlüsse auf die Diebstahlshandlung zulassen und weitere Ermittlungsansätze eröffnen kann. Auch kann der Fall eintreten, dass das Diebesgut nicht aufgefunden werden kann. In diesem Fall können meist lediglich die Bewegungsdaten Rückschlüsse auf die Täter*innen oder weitere Ermittlungsansätze ermöglichen. In solchen Situationen kann die Beweislage so schwierig sein, dass es auf jeden Indizienbeweis ankommt.

Ferner können Positionsdaten eine besondere Bedeutung haben, wenn es darum geht, bandenmäßige Diebstähle und organisierte Strukturen des Diebstahls nachzuweisen. Insbesondere im Falle des Fahrzeugdiebstahls ist es nicht unwahrscheinlich, dass diese schnell ins Ausland verbracht werden und so als Beweismittel nicht mehr zur Verfügung stehen, wodurch die Ermittlungsbehörden für die Beweisführung auf Positionsdaten angewiesen sind. Auch kann es gerade zum Nachweis krimineller Strukturen notwendig sein, die Bewegungen gestohlener Gegenstände über einen längeren Zeitraum zu beobachten, um

22 Vgl. dazu etwa: LG Köln, Urteil v. 23.5.2016 - 113 KLs 34/15; LG Braunschweig, Urteil v. 21.6.2011 – 4a KLs 7/11.

Muster zu erkennen, die Rückschlüsse auf sämtliche bzw. die meisten Tatbeteiligte zulassen. Im Falle einer durchstrukturierten Arbeitsteilung ist oftmals nicht viel gewonnen, wenn nur einzelne Täter*innen aufgespürt werden, da die anderen Beteiligten weiter aktiv bleiben können. Ferner sind Rückschlüsse auf Hehler*innen nur dann möglich, wenn ein Verkauf von Diebesgut beobachtet wird. Insgesamt können bei Anhaltspunkten auf eine bandenmäßige ggf. internationale Kriminalität ein Zuwarten und Beobachten der Bewegungen des Diebesgutes erforderlich sein, um entsprechende Delikte aufzuklären. Mit dem längeren Zuwarten geht aber das Risiko einher, dass die Fahrräder gerade nicht mehr aufgefunden werden können. Insofern ist es wahrscheinlich, dass bei einem polizeilichen Zugriff nicht sämtliche gestohlene Fahrräder aufgefunden werden und es daher notwendig ist, die Positionsdaten heranzuziehen, um weitere Diebstähle und die kriminellen Strukturen nachzuweisen.

2.1.2 Wie kommen die Positionsdaten in die Hauptverhandlung?

Die Beweisführung erfolgt mit den Beweismitteln der StPO. Früher wurden Beweise ausschließlich durch Zeug*innen, Sachverständige, Augenschein, Urkunden sowie durch Beschuldigtenaussagen überwiegend in einer körperlichen Form in die gerichtliche Verhandlung eingeführt.[23] Dies ist bei digitalen Daten nicht möglich, da diesen gerade die Körperlichkeit fehlt.[24] Die Originaldatensätze verbleiben meist bei den Inhaber*innen der Daten und die Strafverfolgungsbehörden erlangen lediglich eine Kopie, sofern sie die Daten nicht selbst erheben. Die Kopie ist aber – anders bei den anderen Beweismitteln, insbesondere bei Urkunden[25] – regelmäßig identisch mit dem originalen Datensatz.[26]

Digitale Daten können auf verschiedene Weise in die Hauptverhandlung eingeführt werden.[27] Wenn die digitalen Daten optisch visualisiert von einer Person wahrgenommen wurden, kommt auch der Zeug*innenbeweis in Betracht.[28] Positionsdaten können auch in Ermittlungsberichten von der Polizei ausgewertet werden. Zu diesen Ermittlungsergebnissen können die jeweiligen Beamt*innen dann als Zeug*innen vernommen werden. Allerdings kann auch der Datensatz für die Beweisführung erforderlich sein, da ggf. überprüft werden muss, ob die von der Polizei gezogenen Schlüsse stimmen. Dies kann insbesondere der Fall sein, wenn die Beschuldigten bestreiten, an diesen Orten

23 Marberth-Kubicki 2010, S. 286; Obenhaus, NJW 2010, S. 651; vgl. Bär, MMR 1998, S. 579.
24 BVerfG NJW 33/2009, 2431 (2434); Sieber 2012, S. 153; Warken, NZWiSt 2017, S. 291; Obenhaus, NJW 2010, S. 61; Bär 1998, S. 579.
25 Vgl. Freiling/Sack DuD 2014, S. 112.
26 Warken, NZWiSt 2017, S. 294 f.; Wicker, MMR 2013, S. 766; Schuba 2016, S. 233.
27 Warken, NZWiSt 2017, S. 294.
28 Marberth-Kubicki 2010, S. 291; Geschonneck 2008, S. 74; Sieber 2012, S. 67 f.

gewesen zu sein oder es andere Beweismittel gibt, die an der Richtigkeit der Schlüsse im Ermittlungsbericht zweifeln lassen. In solchen Fällen muss der Positionsdatensatz allen Verfahrensbeteiligten zugänglich gemacht werden.

Damit die digitalen Positionsdaten in die Hauptverhandlung eingebracht werden können, müssen sie zunächst der sinnlichen Wahrnehmung zugänglich gemacht, d. h., dass sie gewissermaßen zu einem Beweismittel transformiert werden.[29] Überwiegend werden elektronische Beweismittel mithilfe von Visualisierungen (auf Papier oder auf dem Bildschirm) durch Inaugenscheinnahme oder durch zu verlesende Schriftstücke in den Strafprozess eingeführt, da sie so verkörpert werden.[30]

Im Falle der Positionsdaten erfolgt die Visualisierung durch die Standortdarstellung als Punkt (bzw. Kreis mit gewisser Aufenthaltswahrscheinlichkeit) auf einer digitalen Karte, die bei Bedarf auch ausgedruckt werden kann. Mithin handelt es sich um einen Augenscheinbeweis.

2.2 Beweisqualität der Positionsdaten

Digitale Daten allein reichen regelmäßig nicht aus, um den alleinigen Beweis der Schuld zu erbringen, da ein spezifischer Unsicherheitsfaktor besteht, dass Daten verfälscht wurden.[31] D. h. es besteht die Möglichkeit, dass sie aufgrund von be- und unbewussten Veränderungen nicht mit den Ursprungsdaten übereinstimmen.[32] Der Inhalt digitaler Daten kann in vielerlei Hinsicht verändert werden. So ist z. B. oft ohne größere Schwierigkeiten möglich, mit einem Computer erstellte Texte zu verändern oder Bilder und Videos zu bearbeiten, ggf. sogar mit kostenfreien Programmen. Zwar können auch andere Beweismittel verfälscht werden. Eine Veränderung ist aber bei einem handschriftlich erstellten Dokument oder einem von einem Negativ entwickelten Foto unter ganz anderen Bedingungen möglich. Digitale Datensätze können zudem grundsätzlich jederzeit manuell verändert werden, was bei entsprechenden technischen Zugangsmöglichkeiten (etwa über das Internet) grundsätzlich von überall aus erfolgen kann.[33] Aber auch ungewollte Veränderungen sind nicht unwahrscheinlich. Selbst einfache Programmierfehler können Veränderungen der Datensätze nach sich ziehen. Auch sonstige Veränderungen der Daten können auf den verschiedenen Stufen der Datenverarbeitung auftreten, d. h., während der Speicherung, der Verwahrung, der Übertragung, der Auswertung oder der

29 Momsen 2015, S. 70.
30 Marberth-Kubicki 2010, S. 291; Heinson 2015, S. 118 ff.; Warken, NZWiSt 2017, S. 421.
31 Momsen 2020, S. 78.
32 Momsen 2015, S. 73.
33 Warken, NZWiSt 2017, S. 332.

Umwandlung in eine wahrnehmbare Form.[34] Darin liegt der wesentliche Unterschied zu den herkömmlichen Beweismitteln. Zwar können auch sie verfälscht werden, aber den herkömmlichen Beweismitteln ist diese Gefahr regelmäßig nicht im gleichen Ausmaß immanent – hinsichtlich des Zeugenbeweises gelten Besonderheiten[35] – da sie während ihres Transportes oder ihrer Auswertung oftmals keinem stetigem Verarbeitungsprozess unterliegen und weil Veränderungen von körperlichen Gegenständen vielfach einfacher zu erkennen sind;[36] hinsichtlich der Erkennbarkeit kommt es aber darauf an, wer die Fälschung vornimmt und wer versucht, diese zu erkennen.

Beweismittel, die ihrer Natur nach fehleranfällig sind, haben zunächst einen geringen Beweiswert.[37] Sie erlangen aber einen höheren Beweiswert, wenn parallele Beweisstränge vorhanden sind, die Fehler ausschließen. Dementsprechend müssen Zusatztatsachen vorliegen, die belegen, dass digitale Daten authentisch sind, d. h., dass sie ordnungsgemäß erhoben und verarbeitet wurden.[38] Diese Stränge müssen im Einklang mit den Daten und zueinander in einem logischen und nachvollziehbarem Verhältnis stehen.[39] Insgesamt ist es daher erforderlich, sowohl den Prozess der Datenerhebung als auch den Prozess der Verarbeitung und Analyse der Daten strategisch vorzubereiten, um auszuschließen, dass die Daten verfälscht werden.[40] Dementsprechend sind Vorkehrungen für die Gewährleistung von Integrität und Authentizität der Datensätze zu treffen.[41] Ein hoher Beweiswert lässt sich durch eine Kombination technischer und organisatorischer Maßnahmen bei der Beweisgewinnung und Verarbeitung sichern.[42] Zur näheren Erläuterung der Gewinnung und Verarbeitung der Daten und bzgl. des Dateninhaltes können dann vor Gericht Sachverständige oder Zeug*innen gehört werden, oder das Gericht kann an Hand der Dokumentation des Datenerhebungsprozesses prüfen, ob die Daten authentisch sind.[43]

In der StPO spiegeln sich Verfahren zur Gewährleistung der Authentizität von Daten bisher nur an einigen Stellen wider.[44] Generelle Vorgaben fehlen, um die Authentizität und Integrität digitaler Daten verfahrensrechtlich bestmöglich

34 Vgl. Momsen 2015, S. 70; Marberth-Kubicki 2010, S. 221 f.; Heinson 2015, S. 147.
35 Auch Erinnerungen unterliegen einem Veränderungsprozess.
36 Vgl. Warken, NZWiSt 2017, S. 331; Bär 2007, S. 282.
37 Sieber 2012, S. 67 f.
38 Vgl. Heinson 2015, S. 121; Momsen 2015, S. 78.
39 Vgl. Momsen 2015, S. 83.
40 Bundesamt für Sicherheit und Informationstechnik 2011, 8.
41 Heinson 2015, S. 147; vgl. Geschonneck 2008, S. 80 ff.; Marberth-Kubicki 2010, S. 221 f.
42 Heinson 2015, S. 141.
43 Warken, NZWiSt 2017, S. 421; vgl. LG Köln, Urteil vom 23.05.2016 - 113 KLs 34/15.
44 Vgl. Marberth-Kubicki 2010, S. 286; Warken, NZWiSt 2017, S. 291; Sieber 2012, S. 68.

abzusichern. Bisher wurde die Bedeutung der Beweissicherung digitaler Daten lediglich für ganz spezielle Datengruppen mit den §§ 41a und 483 ff. StPO zum Ausdruck gebracht. Auch ist in § 100a ist in Abs. 5 Satz 2 StPO festgelegt, dass „kopierte Daten [...] nach dem Stand der Technik gegen Veränderungen, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen" sind.[45] Ähnliche Vorgaben gibt es in den §§ 488 Abs. 1 Satz 2 und 32 Abs. 2 StPO.

Es stellt sich allerdings die Frage, ob entsprechende Standards über Vorschriften außerhalb der StPO sichergestellt werden. In Betracht kommt dabei das BDSG und zwar die §§ 45 BDSG ff., die den Datenschutz bzgl. der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung regeln. Das speziellere Gesetz ist in diesem Rahmen zwar die StPO, allerdings lassen sich Hinweise auf Mindeststandards auch anderen Normen entnehmen. So folgt aus § 64 Abs. 1 S. 2 BDSG, dass die einschlägigen Technischen Richtlinien und Empfehlungen des BSI (BSI-TR) zu berücksichtigen sind. Dementsprechend sind die Standards des BSI zu Grunde zu legen. Das BSI hat unter anderem einen Leitfaden „IT-Forensik" herausgegeben, um die Integrität und die Authentizität von digitalen Beweismitteln zu sichern. Wenn der Gesetzgeber an dieser Stelle schon verdeutlicht hat, dass die BSI-TR eine Vorgabe für die Anwendung darstellen, so sind auch im Bereich der StPO die Vorgaben wenigstens zur Orientierung heranzuziehen.

Auch wenn damit Regelungen zur Orientierung vorliegen, sollte die Gesetzgebung die Verwertung digitaler Beweise eindeutiger und verbindlicher regeln.[46] Eine Möglichkeit wäre, sich dabei an den bereits vorhandenen Maßstäben des BSI zu orientieren. Wie bereits verdeutlicht, unterscheidet sich die Beweisführung mittels digitaler Daten grundlegend von den übrigen Beweismitteln, sodass ein anderer Umgang mit diesen Beweismitteln erforderlich ist. Insbesondere können die Daten regelmäßig leichter geändert oder unbewusst verfälscht werden als eine Urkunde oder ein Augenscheinobjekt. Technische Laien können diese Veränderungen oft nicht ohne Weiteres erkennen. Daher sind gesetzliche Maßstäbe zur Sicherung der Daten festzulegen, um die Fehlerquote so gering wie möglich zu halten. Ferner sollte dringend vermieden werden, dass sich unterschiedliche Standards in verschiedenen Bereichen der Strafjustiz entwickeln. Es ist daher eine klare und verbindliche gesetzliche Leitlinie erforderlich.

45 Warken, NZWiSt 2017, S. 421.

46 Vgl. Momsen 2015, S. 79.

2.3 Beweisqualität der Positionsdaten im FindMyBike-System

Insgesamt ergeben sich unter Zugrundelegung der Erkenntnisse des BSI und der IT-Forensik verschiedene Anforderungen an Informationsverarbeitungssysteme, um eine hohe Beweisqualität der Daten sicherzustellen. Diese Anforderungen wurden in dem *FindMyBike-System* zur Übertragung von Positionsdaten gestohlener Fahrräder an die Polizei umgesetzt.

Die Beweisführung kann nur zweifelsfrei gelingen, wenn alle Schritte der Datenverarbeitung und der Datenanalyse lückenlos chronologisch dokumentiert werden. Nur so können die einzelnen Schritte von allen Verfahrensbeteiligten nachvollzogen und (Ver-)Fälschungen erkannt werden.[47] Bei der Dokumentation muss erkennbar werden, wer Zugang zu den Daten hatte und dass die Daten seit der Erhebung nicht verändert worden sind, bzw. wie sich eine Veränderung ausgewirkt hat.[48] So wird sichergestellt, dass zu jedem Zeitpunkt der Erfassung und Analyse der digitalen Daten ein möglicher Missbrauch bzw. eine Verfälschung nachgewiesen werden kann.[49]

Für die Bewertung der Beweisqualität ist es entscheidend, dass dem (Ver-)Fälschungsrisiko in einer zum Risiko angemessenen Art und Weise entgegengewirkt wird. Je größer das Risiko ist, desto umfassender müssen die Maßnahmen sein. Vor allem ist entscheidend, dass die Datensätze so gespeichert und geschützt werden, dass sie einen hohen Beweiswert haben.[50] Der Zugang zu Beweismitteln muss so abgesichert sein, dass ein Zugriff durch Unbefugte soweit wie möglich ausgeschlossen ist.[51] Dabei ist allerdings zu beachten, dass eine absolute Sicherheit von technischen Systemen nicht ermöglicht werden kann. Allein der Umstand, dass unbefugte Zugriffe nicht ausgeschlossen werden können, kann daher nicht dazu führen, dass digitale Daten vor Gericht nicht verwendet werden können. Einerseits können weitere Umstände dafür sprechen, dass die Daten authentisch sind und andererseits können Standards bei der Datensicherung eingehalten werden, die eine Veränderung der Daten sehr unwahrscheinlich machen.

Auch ist zu beachten, dass der Original-Datensatz durch Weiternutzung oder Verwendung für Analysen verändert werden kann. Mithin muss dokumen-

47 Bär 2007, Rn. 431; Heinson 2015, S. 144 ff. m. w. N.; Bundesamt für Sicherheit und Informationstechnik 2011, S. 23.

48 European Informatics Data Exchange Framework for Courts and Evidence, S. 15; Schuba 2016, S. 262; Heinson 2015, S. 146 f.; Bundesamt für Sicherheit und Informationstechnik 2011, S. 23.

49 Bundesamt für Sicherheit und Informationstechnik 2011, S. 23.

50 Schuba 2016, S. 262 f.; Heinson 2015, S. 141; Sieber 2012, S. 67 f.

51 Momsen 2015, S. 87.

tiert werden, welchen Inhalt der Original-Datensatz, der für das Verfahren relevant ist, vom Zeitpunkt der Sicherstellung bis zum Abschluss des Ermittlungsverfahrens hat.[52] Die Daten sind also zu sichern bzw. konservieren.[53] Im besten Falle sollten die Daten so gespeichert werden, dass für die Verfahrensbeteiligten jeder Analyseschritt bzw. Verarbeitungsschritt reproduzierbar ist.[54] Hierfür müssen Kopien der Datensätze erstellt werden, damit ein Datensatz ausgewertet werden kann, während ein anderer unverändert erhalten bleibt.[55] Die Originaldaten und die Kopien müssen gegen Veränderungen besonders geschützt werden.[56] Ein Datensatz, der an verschiedenen Orten identisch gespeichert ist, erhöht den Beweiswert erheblich, da es sehr unwahrscheinlich ist, dass alle Speicherorte manipuliert worden sind.[57]

Sofern entsprechende Kopien vorhanden sind, kann mittels eines Hashwertes die Authentizität der Daten überprüft werden.[58] Bei einem Hashwert handelt es sich, um eine längere Zahlen- und Buchstabenreihenfolge, die sich aus der Kombination der Daten und dem Ergebnis einer komplexen mathematischen Aufgabe ergibt.[59] Wenn die Hashfunktion für zwei Datensätze den gleichen Wert (eben den Hashwert) ergibt, sind die beiden Datensätze auch identisch.[60] Stimmt dieser Hashwert mit dem abgespeicherten Hashwert überein, spricht dies mit großer Wahrscheinlichkeit dafür, dass die Daten seither nicht verändert wurden,[61] allenfalls könnten beide Datensätze gleichartig verändert worden sein. Falls die Polizei mit den Datensätzen arbeitet, sollten im polizeilichen System Kopien erstellt werden. So muss also nur ein Hashwert der Ausgangspositionsdaten existieren, mit dem ggf. belegt werden kann, dass die Daten zum Zeitpunkt der Erhebung mit den Daten, die in das Gerichtsverfahren eingeführt werden, übereinstimmen. Etwaige Fehler sollten auch möglichst früh im Verfahren für Polizei und ggf. für die Staatsanwaltschaft erkennbar sein, damit

52 KK-StPO/Greven StPO § 94 Rn. 4.
53 Heinson 2015, S. 27.
54 Heinson 2015, S. 147; vgl. Bär 2007, S. 281 f.; Bundesamt für Sicherheit und Informationstechnik 2011, S. 23 ff.; Momsen 2015, S. 83.
55 Bundesamt für Sicherheit und Informationstechnik 2011, S. 26; Heinson 2015, S. 147; Schuba 2016, S. 265.
56 Heinson 2015, S. 147.
57 Momsen 2015, S. 83.
58 Momsen 2015, S. 85 f.; Heinson 2015, S. 146 ff.
59 Bechtolf/Vogt, ZD 2018, S. 67.
60 BVerwG, Urteil vom 07. Dezember 2016 – 6 C 14/15 –, Rn. 22; Oberverwaltungsgericht für das Land Schleswig-Holstein, Urteil vom 14. März 2016 – 14 LB 8/13 –, Rn. 56; Heinson 2015, S. 149.
61 Heinson 2015, S. 149 f.

geprüft werden kann, ob das Verfahren trotz fehlerhafter Daten noch sinnvoll weitergeführt werden kann.

Allerdings muss bei der Übertragung auch berücksichtigt werden, dass die Positionsdaten von einem privaten Trackingservice-Anbieter stammen. Gerade digitale Beweismittel werden in einem erheblichen Umfang durch Privatpersonen erhoben und verarbeitet.[62] Die Polizei kann Positionsdaten erst bei einem Tatverdacht hinsichtlich eines Diebstahls selbst erheben, d. h., wenn sie von dem Diebstahl erfährt (meist durch Anzeige). Auch kann die Polizei die Bewegungsdaten nach § 100h Abs. 1 Nr. 2 StPO nur erheben, wenn es sich um Straftaten von erheblicher Bedeutung handelt. Im Falle von Diebstählen mit einem geringeren Wert (z. B. bei Fahrraddiebstählen) muss demnach gewerbsmäßige oder Bandenkriminalität oder eine Diebstahlsserie vorliegen. Daraus ergibt sich, dass regelmäßig Privatpersonen freiwillig die ersten Bewegungsdaten des Diebesgutes an die Polizei übertragen.[63]

Die Datenerhebung und Datenübermittlung durch Private begründet ein erhöhtes Risiko im Hinblick auf Manipulation und Verlust von beweisrelevanten Informationen.[64] Dies ist einerseits darauf zurückzuführen, dass im privaten Sektor wohl kaum berücksichtigt wird, dass der Beweiswert von digitalen Daten nur dann hoch ist, wenn die beschriebenen Anforderungen eingehalten werden. Zudem ist es aufwendig und mit Kosten verbunden, ein entsprechendes Konzept zu entwickeln und umzusetzen, welches die Beweisqualität der Daten in dem nötigen Umfang erhält und das System gegen Zugriffe von außen ausreichend schützt. Auch ist zu beachten, dass mehr Fehler entstehen können, wenn die Daten sich in verschiedenen Verarbeitungssystemen befinden oder zwischen den Systemen übertragen werden (etwa von einem privaten Unternehmen an die Polizei). Da so deutlich mehr Personen Zugriff auf die Daten haben, erhöht sich das Risiko von Verfälschungen.

Insofern kann eine Beweisführung selbst dann nicht gelingen, wenn die Polizei die Daten gerichtsfest speichert und verarbeitet, solange nicht auszuschließen ist, dass die Beweise bei der Verarbeitung durch private Anbieter oder bei der Übermittlung an die Polizei verfälscht wurden. Zwar könnte man sich auf den Standpunkt stellen, dass solange eine Vermutung für die Richtigkeit der Daten gilt, wie es keine Anhaltspunkte auf Verfälschungen gibt.[65] Aus einer rechtsstaatlichen Perspektive heraus ist es aber ein unerträglicher Zustand, wenn Daten zu einer Verurteilung verwendet werden, die möglicherweise manipuliert oder sonst verändert wurden. Insofern kann eine Vermutung für die

62 Momsen 2015, S. 72.
63 Ausführlich dazu Fährmann, in diesem Band, S. 141ff.
64 Momsen 2015, S. 75.
65 Vgl. Momsen 2015, S. 84.

Richtigkeit der Daten nur dann gelten, wenn Verfahrensabläufe eingehalten wurden, um die Authentizität der Daten sicherzustellen.

Es stellt sich damit die Frage, wie effektive Strategien zur Vermeidung von beabsichtigten oder unbeabsichtigten Datenveränderungen entwickelt werden können. Dies lässt sich nur sicherstellen, wenn auch von privater Seite bei der Erhebung der Daten gewisse Standards eingehalten werden und wenn die Einhaltung dieser Standards durch das Gericht und Staatsanwaltschaft kontrolliert werden können. Insofern müssen auch private Unternehmen sicherstellen, dass die Daten authentisch sind. Dazu sind Fehler oder bewusste Veränderungen soweit wie möglich auszuschließen und die Daten müssen gegen Veränderungen von außen geschützt werden.

Eine Möglichkeit wäre die Entwicklung von Zertifikaten, die nur Anbieter erhalten, die die beschriebenen Qualitätsstandards bei der Datenerhebung und der Weitergabe an die Polizei technisch sicherstellen können. Diese könnten einerseits vor Gericht zu einer Erhöhung des Beweiswertes beitragen. Auf der anderen Seite könnten sich auch Verbraucher*innen an diesem Zertifikat bei der Auswahl entsprechender Trackingservice-Anbieter orientieren.

Das im Projekt entwickelte *FindMyBike-System* wurde so konzipiert, dass ein möglichst hoher Beweiswert der Positionsdaten im System und bei der Übertragung an die Polizei umgesetzt wird. So wurde durch eine Verschlüsselung und andere Sicherheitsvorkehrungen der Schutz der Integrität der Daten sichergestellt. Zwar ist im Falle des entwickelten *FindMyBike-Systems* eine bewusste Fälschung von Positionsdaten gestohlener Fahrräder eher unwahrscheinlich. Diese ist aber auch nicht ausgeschlossen, gerade wenn es um Verfahren der banden- oder gewerbsmäßigen Kriminalität geht. Insofern müssen in Verfahren, in denen es um gravierende Strafen geht, die Server der beteiligten Akteure ausreichend gegen Zugriffe gesichert sein. Auch wurde bereits dargestellt, dass Positionsdaten ein Indiz in der Beweiskette sein können, die zu einer Verurteilung führt. Auch hier ist ein Schutz der Daten gerade bei umfangreicheren Diebstählen relevant, da oftmals nur aus den Routen der Fahrräder Rückschlüsse auf einen organsierten und arbeitsteiligen Diebstahl möglich sind. Wird gegen die Beweisführung mittels Positionsdaten vorgebracht, dass diese verfälscht wurden, etwa dass die Koordinaten verändert wurden, kann dies dazu führen, dass der Beweiswert stark sinkt, wenn eine Manipulation nicht ausgeschlossen werden kann. Dies kann also dazu führen, dass es nicht zu einer Verurteilung kommt. Verfälschungen bei den Trackingservice-Anbieter*innen und bei der Polizei müssen von diesen Stellen ausgeschlossen werden.

Auch erfolgt eine lückenlose Dokumentation der Übertragungsvorgänge. Das *FindMyBike-System* berechnet unmittelbar nach der Übertragung mittels einer kryptographischen Hashfunktion aus den Trackingdaten einen Hashwert des Datensatzes.

Insgesamt besteht eine ausreichend große Beweisqualität vor Gericht. Zu berücksichtigen ist, dass bei einer Umsetzung des Systems in der Praxis eine Dokumentation und Sicherheitsstandards auch bei den Trackingservice-Anbieter*innen und der Polizei bestehen müssen, da das *FindMyBike-System* letztlich nur eine Anwendung zur sicheren Übertragung von Daten darstellt.

3. Zusammenfassung

Digitale Positionsdaten können im strafprozessualen Verfahren von großer Bedeutung sein, und es ist damit zu rechnen, dass zukünftig immer mehr solcher Datensätze verfügbar sein werden. Zwar ist hinsichtlich gestohlener Gegenstände davon auszugehen, dass die Positionsdaten im Rahmen der Diebstahlsaufklärung überwiegend Teil eines Indizienbeweises sein werden. Diese können aber Konstellationen, in denen die Ermittlungsansätze fehlen, einen wertvollen Beitrag zum Beweis der Schuld oder Unschuld der Beschuldigten leisten. Um jedoch einen hohen Beweiswert digitaler Daten im Gerichtsverfahren sicherzustellen, müssen Verfahrensweisen implementiert werden, die diese Daten vor be- oder unbeabsichtigten Verfälschungen schützen, welche aufgrund der fehlenden Körperlichkeit von digitalen Daten vielfach leichter erfolgen können als bei Urkunden oder Augenscheinobjekten. Diese Verfahren müssen also die Integrität und die Authentizität der Daten soweit wie möglich sicherstellen, insbesondere beim Übertragungsvorgang. Eine besondere Problematik besteht hinsichtlich Daten, die von privaten Personen erhoben werden und dann an die Polizei weitergeleitet werden. Besonders bei diesen Daten müssen Verfahrensweisen und entsprechende IT-Systeme entwickeln, die eine Verfälschung soweit wie möglich ausschließen. Die bisherige Rechtslage wird den beschriebenen Problemen nicht ausreichend gerecht und sollte daher angepasst werden.

Literatur

Bär, Wolfgang (1998) Strafprozessuale Fragen der EDV-Beweissicherung, in: MMR 21 Jg., Nr. 11, S. 577–584.

Bär, Wolfgang (2007) Handbuch zur EDV-Beweissicherung, Stuttgart.

Bär, Wolfgang (2022) 27. Kapitel. EDV-Beweissicherung, in: Wabnitz, Heinz-Bernd/Janovsky, Thomas/Schmitt, Lothar (Hg.): Handbuch des Wirtschafts- und Steuerstrafrechts. 5. Aufl., München, S. 1711–1789.

Bechtolf, Hans/Vogt, Niklas (2018) Datenschutz in der Blockchain – Eine Frage der Technik. Technologische Hürden und konzeptionelle Chancen, in: ZD 9 Jg., Nr. 02, S. 66–70.

Bundesamt für Sicherheit und Informationstechnik (2011) Leitfaden „IT-Forensik“. Version 1.0.1 (März 2011). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf;jsessionid=4D553B311BB6952EFEB51FBB1E0CD561.1_cid341?__blob=publicationFile&v=2, zuletzt besucht am 21.02.2023.

European Informatics Data Exchange Framework for Courts and Evidence: D9.2 Roadmap. Deliverable prepared by Partner 2 – RUG. http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426.pdf, zuletzt besucht am 21.02.2023.

Fährmann, Jan (2020) Digitale Beweismittel und Datenmengen im Strafprozess, in: MMR 23 Jg., Nr. 04, S. 228–233.

Freiling, Felix/Sack, Konstantin (2014) Selektive Datensicherungen in der IT-Forensik. Der Mittelweg zwischen Übermaß und Untermaßverbot in: DuD Nr. 38, S. 112–117.

Geschonneck, Alexander (2008) Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 3. Aufl., Heidelberg.

Heinson, Dennis (2015) IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen, Tübingen.

Marberth-Kubicki, Annette (2010) Computer- und Internetstrafrecht. 2. Auflage, München.

Meyer-Goßner, Lutz/Schmitt, Bertram (2022) Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen. 65. Auflage.

Momsen, Carsten (2015) Digitale Beweismittel aus der Sicht der Strafverteidigung, Beck, Susanne/Meier, Bernd-Dieter/Momsen, Carsten (Hg.): Cybercrime und Cyberinvestigations. Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, Baden-Baden, S. 67–91.

Momsen, Carsten (2020) Strafrechtliche Relevanz von Datensicherheit und Datenschutz im Unternehmen, in: Frenz, Walter (Hg.): Handbuch Industrie 4.0: Recht, Technik, Gesellschaft, Berlin, Heidelberg, S. 61–85.

Müller, Sebastian (2020) Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts-)Strafverfahren, in: NZWiSt 9 Jg., Nr. 3, S. 96–101.

Obenhaus, Nils (2010) Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, in: NJW 63 Jg., Nr. 10, S. 651-655.

Schuba, Marko (2016) 7. IT-Forensik, in: Galley, Birgit/Minoggio, Ingo/Schuba, Marko (Hg.): Unternehmenseigene Ermittlungen. Recht - Kriminalistik - IT, S. 227–307.

Sieber, Ulrich (2012) Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag, München.

Warken, Claudia (2017) Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1. Beweissicherung im Zeitalter der digitalen Cloud, in: NZWiSt 6 Jg., Nr. 08, S. 289–298.

Warken, Claudia (2017) Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2. Beweisverwertung im Zeitalter der digitalen Cloud und datenspezifische Regelungen in der StPO, in: NZWiSt 6 Jg., Nr. 09, S. 329–338.

Warken, Claudia (2017) Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 3. Jenseits der StPO: Analogie, supra- und internationale Regelungen, praktische Lösungsansätze, in: NZWiSt 6 Jg., Nr. 11,S. 417–425.

Warken, Claudia (2017) Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 4. Quo vadis, StPO? Warum es expliziter gesetzlicher Regelungen für den Umgang mit elektronischen Beweismitteln im Strafprozess bedarf und welche Rolle die Europäische Union dabei spielt, in: NZWiSt 6 Jg., Nr. 12, S. 449–456.

Wicker, Magda (2013) Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, in: MMR 16 Jg., Nr. 12, S. 765–769.