Wissenschaftliche Schriften der
Hochschule für Wirtschaft und Recht Berlin

69

Fährmann | Görlitz | Matzdorf | Vollmar [Hrsg.]

# Private Positionsdaten und polizeiliche Aufklärung von Diebstählen

## Rechtliche, kriminalistische und technische Perspektiven

Nomos

edition sigma

HWR Berlin Forschung

herausgegeben von

Prof. Dr. Christoph Dörrenbächer
Prof. Dr. Marianne Egger de Campo
Prof. Dr. Olaf Resch
Prof. Dr. Peter Ries
Prof. Dr. Birgitta Sticher

Band 69

Die Reihe HWR Berlin Forschung schließt an die Reihe fhw forschung der vormaligen Fachhochschule für Wirtschaft Berlin (fhw) an. Aus der Fusion der fhw mit der FHVR (Fachhochschule für Verwaltung und Rechtspflege) ist 2009 die Hochschule für Wirtschaft und Recht Berlin hervorgegangen.

Jan Fährmann | Gudrun Görlitz
Christian Matzdorf | Alexander Vollmar [Hrsg.]

# Private Positionsdaten und polizeiliche Aufklärung von Diebstählen

**Rechtliche, kriminalistische und technische Perspektiven**

Nomos

edition sigma

BERLIN IFAF Institut für angewandte Forschung Berlin

Gefördert durch das Institut für Angewandte Forschung Berlin e.V.

**Die Deutsche Nationalbibliothek** verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2023



Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-5905-7
ISBN (ePDF): 978-3-7489-0032-0

DOI: https://doi.org/10.5771/9783748900320

Onlineversion
Nomos eLibrary

edition sigma in der Nomos Verlagsgesellschaft

# Inhalt

*Hartmut Aden[1]/Jan Fährmann[2]/Gudrun Görlitz[3]/Christian Matzdorf[4]*

# Datenschutzgerechte Lokalisierung gestohlener Gegenstände – eine Einleitung

## 1. Aufklärung von Diebstählen als Forschungsthema

Diebstähle gehören in vielen Ländern zu den am häufigsten registrierten Straftaten. Teilweise wollen Dieb*innen das Diebesgut selbst nutzen, meistens dürfte es aber um die finanziellen Erträge aus einem Weiterverkauf gehen. Für alle Güter, die sich auf illegalen Märkten weiterverkaufen lassen, sind Diebstähle attraktiv, auch wenn die Anzahl der polizeilich erfassten Diebstähle zuletzt gesunken ist.[5] Besonders bei mobilen Gegenständen, für die es einen Nachfragemarkt gibt, besteht ein erhöhtes Diebstahlrisiko.

Indes sind die Aufklärungsquoten bei Diebstahldelikten vergleichsweise gering.[6] Hierfür kommen verschiedene Erklärungshypothesen in Betracht, die in den kriminalistisch-kriminologischen Beiträgen dieses Bandes näher erörtert werden. Sie reichen von fehlenden Anhaltspunkten für die polizeiliche Ermittlungsarbeit über die schwere Identifizierbarkeit gestohlener Gegenstände – etwa wenn Fahrzeuge vor dem Weiterverkauf auf Schwarzmärkten demontiert werden – bis zur Überlastung der zuständigen Polizeidienststellen, die eine Priorisierung der Ermittlungen erfordert. Schwerwiegendere Delikte oder solche, die in der Öffentlichkeit als besonders dringlich wahrgenommen werden, genießen in der polizeilichen Ermittlungsarbeit daher oft eine höhere Priorität als die Aufklärung von Diebstählen und der Verbleib gestohlener Gegenstände. So ist etwa seit einiger Zeit eine höhere polizeiliche Priorisierung der Aufklärung von Wohnungseinbrüchen zu beobachten. Diese höhere Priorität ist gut nachvollziehbar, denn für die Betroffenen können Wohnungseinbrüche

1 Prof. Dr. Hartmut Aden hat das Projekt FindMyBike für den Bereich Rechtswissenschaft geleitet.
2 Dr. Jan Fährmann war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die rechtlichen und kriminologischen Forschungsfragen.
3 Prof. Dr. Gudrun Görlitz hat das Projekt FindMyBike für den Bereich Informatik geleitet.
4 Prof. Christian Matzdorf hat in dem Projekt FindMyBike kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.
5 Statista 2020.
6 Zur Übersicht über die PKS 1987-2019 Statista 2020a.

aufgrund des Eindringens in die Privatsphäre traumatisierend wirken.[7] Indes können auch andere Diebstähle für die Betroffenen schwere Folgen haben, etwa wenn Gegenstände mit einem hohen ideellen Wert gestohlen werden.

In dem Projekt FindMyBike – Rechtliche und technische Konzepte für die Übertragung von zeitbasierten Geodaten zur Aufklärung von Fahrraddiebstählen, aus dessen Kontext die Beiträge dieses Bandes stammen, wurde exemplarisch der Fahrraddiebstahl als häufig vorkommendes Alltagsdelikt untersucht. In diesem Buch wird aber bewusst ein breiterer Ansatz gewählt, da viele der Erkenntnisse sich – teils mit Abweichungen – auch auf andere gestohlene Gegenstände übertragen lassen.

Fahrräder haben in Großstädten als Teil des Mobilitätskonzepts erheblich an Bedeutung gewonnen. Ein Nachteil der Fahrradmobilität besteht allerdings darin, dass Fahrräder zumeist schlecht gegen Diebstahl gesichert sind und daher häufig gestohlen werden. Dabei hinterlassen die Täter*innen in der Regel kaum Spuren, sodass polizeiliche Ermittlungsansätze für die Aufklärung fehlen.[8] Hohe Fallzahlen stehen daher einer sehr niedrigen Aufklärungsquote gegenüber.[9]

## 2. Ortungstechnik in diebstahlgefährdeten Gegenständen

Zunehmend wird Ortungstechnik, typischerweise GPS-Sender, in Fahrzeugen oder anderen Gegenständen, die gestohlen werden könnten, verbaut. In einigen Fällen werden solche Gegenstände bereits bei der Herstellung mit Ortungstechnik ausgestattet. Oft ist der Diebstahlschutz allerdings nicht der Hauptgrund für den Einbau, sondern die Ermittlung der aktuellen Position erfüllt andere Funktionen, etwa bei der Einsatzsteuerung für Lastwagen, Baustellenfahrzeugen, Containern, Mietwagen oder Taxen sowie zur Navigation im Straßenverkehr. Fahrradverleihfirmen nutzen eingebaute Ortungstechnik, um ihrer Kundschaft per Smartphone ausleihbare Fahrräder in der Nähe anzuzeigen und Ausleih- und Rückgabeort sowie Ausleihzeit für die Bezahlung zu erfassen. Auch das Tracken von Leihfahrrädern, d. h. die kontinuierliche Erfassung der Positionsdaten, ist bei Fahrradverleiher*innen durchaus üblich. Durch das Tracken ist eine gefahrene Route darstellbar, nicht nur die aktuelle Position. Dies ermöglicht den Anbietenden eine Anpassung und Verbesserung ihrer Angebote. Für die Aufklärung von Bandenkriminalität bieten diese Routenerfassungen wiederum Ermittlungsansätze, da diese Rückschlüsse auf Abläufe der Diebstähle und dahinterstehende Strukturen ermöglichen.

7 Wollinger, MSchKrim 2015, S. 365-383.
8 Vollmar/Görlitz/Fährmann/Aden 2019, S. 87.
9 Für Berlin etwa Polizeipräsident Berlin 2018.

Einige Anbietende entwickeln Produkte gezielt für den Diebstahlschutz.[10] Wird der Gegenstand gestohlen, so können diejenigen, die Zugriff auf die Positionsdaten haben, erkennen, wo sich der Gegenstand gerade befindet, solange die Sendeleistung ausreicht. Die Trackingdaten werden im IT-System der Eigentümer*innen gespeichert. So können sie die Trackingdaten einsehen und sind dadurch in der Lage, den gestohlenen Gegenstand zu lokalisieren. Die Polizei, die Positionsdaten in die Fahndung einbeziehen sollte, hat dagegen keinen Zugriff auf diese Daten.

## 3. Praktische Herausforderungen

### *3.1 Medienbrüche im Prozess der polizeiinternen Ermittlung zu Diebstählen*

Die polizeilichen Prozesse bei der Diebstahlermittlung sind in den IT-Systemen der Polizei aktuell so implementiert, dass es keine Möglichkeit gibt vorhandene Ortungsdaten gestohlener Gegenstände in die Ermittlung einzubeziehen. Um die zweifelfrei sehr hohen Sicherheitsanforderungen an die polizeilichen Daten zu erfüllen, wurden und werden die IT-Systeme als geschlossene Systeme von ausgewählten IT-Dienstleister*innen programmiert. Damit ist es grundsätzlich nicht möglich, Daten wie beispielsweise Ortungsdaten digital an das IT-System zu übergeben. Dazu müsste ein Programmierprozess aufwändig und zeitintensiv genehmigt und beauftragt werden. Aktuell setzen private Firmen Software ein, mit der bestimmte Kraftfahrzeuge[11] geortet werden können. Die Polizei in Berlin fragt bei diesen Firmen kostenpflichtig die Position des Fahrzeugs ab.

Bei der Ermittlung von Diebstählen ortbarer Gegenstände wird ein Medienbruch bei der Diebstahlanzeige und der Übernahme in das polizeiinterne IT-System deutlich. Auf einer Dienststelle wird der Vorgang oftmals in Papierform aufgenommen. Selbst wenn die Diebstahlanzeige online erfolgt, was heute eine Standardvariante der Anzeigenerstattung ist, sehen die Webformulare nicht vor, Ortungsdaten des gestohlenen Gegenstands zum Zugriff durch die Polizei freizugeben, sodass diese Daten für die Fahndung nicht unmittelbar genutzt werden können. Das Hochladen eines Bildes des gestohlenen Gegenstandes ist ebenfalls nicht möglich.

Bei der bundes- und der länderübergreifenden Fahndung nach gestohlenen Gegenständen arbeiten verschiedene Polizeidienststellen zusammen. Jedoch hat jedes Bundesland ein eigenes polizeiliches IT-System entwickeln lassen. Ein

10 https://velocate.com/ (letzter Aufruf: 25.02.2023).
11 https://www.ubinam.de/ (letzter Aufruf: 25.02.2023).

effizienter Datenaustausch, beispielsweise von Trackingdaten, ist nicht implementiert.

Diese Medienbrüche verhindern eine schnelle und effektive Fahndung nach gestohlenen Gegenständen mit Ortungstechnik. Obwohl die rechtmäßigen Eigentümer*innen den Standort des Gegenstands kennen, kann die Polizei diese Information nicht eigenständig nutzen. Eine effektive Restitution des Eigentums sowie die Strafverfolgung werden daher stark erschwert.

### *3.2 Zielkonflikte zwischen Geschädigten und der Polizei bei der Wiederbeschaffung gestohlener Gegenstände*

Divergierende Interessenlagen bzw. Aufgaben prägen das Verhältnis zwischen Polizei und Anzeigenden, die über privat generierte Positionsdaten zu einem gestohlenen Gegenstand verfügen. Geschädigte sind aus der Perspektive der Polizei zuvörderst potentielle Zeug*innen, die Informationen für die Erfüllung der staatlichen Strafverfolgungsaufgabe liefern können. Die Polizei hat nach dem Strafprozessrecht Straftaten im Interesse des Staates bzw. der Allgemeinheit zu verfolgen, nicht vorrangig aus der Perspektive der Opfer. Ob das Opfer eines Diebstahls den gestohlenen Gegenstand, der möglicherweise einen hohen ideellen oder finanziellen Wert hat, zurückbekommt, wird daher aus polizeilicher Sicht als nachrangig betrachtet. Aus polizeilicher Perspektive kann es sogar sinnvoll sein, das Risiko einzugehen, dass der gestohlene Gegenstand nicht auffindbar ist, um Informationen über hinter dem Diebstahl stehende kriminelle Strukturen zu erhalten. Im Rahmen des rechtlich Zulässigen kann es daher sinnvoll sein, zunächst zu beobachten, wohin der Gegenstand transportiert wird, statt sofort einzugreifen. Erfolgreiche Polizeiarbeit führt zur Ermittlung und Überführung der Täter*innen, weniger zur Zufriedenheit von Opfern mit der Berücksichtigung ihrer spezifischen Interessen – die bei Diebstahlsdelikten in der Wiedererlangung genau des gestohlenen Gegenstandes oder in der Erfüllung der Voraussetzungen für die Auszahlung einer Versicherungsleistung bestehen können.

Auch wenn technische Lösungen wie sie im FindMyBike-Projekt entwickelt wurden, zukünftig dazu führen sollten, dass die Polizei privat generierte Positionsdaten für die Diebstahlsaufklärung unmittelbar verwenden kann, dürfte dies den Interessenunterschied zwischen Polizei und Geschädigten allenfalls abmildern, aber nicht beseitigen. Die Polizei wird weiterhin vorrangig an den Täter*innen interessiert sein, die Geschädigten an der Wiedererlangung gestohlener Gegenstände oder einer Versicherungskompensation. Gleichwohl steigt die Wahrscheinlichkeit, dass Betroffene den gestohlenen Gegenstand zurückerhalten, wenn dieser sichergestellt werden kann und nicht mehr länger als Beweismittel benötigt wird. Trotzdem wird die Polizei allein aufgrund neuer

technischer Möglichkeiten nicht in erster Linie als eine Art „Rückbeschaffungsbehörde“ gestohlener Gegenstände fungieren können.

## 4. Interdisziplinäre Forschungsansätze

Die Beiträge dieses Buches betrachten die Nutzung von privat generierten Positionsdaten für die polizeiliche Aufklärung von Diebstählen aus verschiedenen disziplinären Blickwinkeln, wobei informationstechnische, rechtliche, verwaltungswissenschaftliche, kriminologische und kriminalistische Aspekte im Mittelpunkt stehen. Diese wurden im FindMyBike-Projekt und den Beiträgen dieses Bandes in Form einer rechtlich abgesicherten informationstechnischen Lösung für die Übertragung von Positionsdaten an die Polizei zusammengeführt.

### *4.1 Empirisch-kriminologische und kriminalistische Grundlagen des Diebstahls beweglicher Gegenstände*

Den Ausgangspunkt bilden empirische Erkenntnisse über Diebstähle. Hier basieren die Beiträge dieses Bandes auf Erkenntnissen der Kriminologie und der Kriminalistik sowie auf Erfahrungen der beteiligten Praktizierenden. Dazu wurde die Vorgangsbearbeitung bei Fahrraddiebstählen genauer betrachtet und analysiert. Hinsichtlich des Fahrraddiebstahls sind nur wenige aktuelle kriminalistische und kriminologischen Erkenntnisse verfügbar.[12] Die Polizeiliche Kriminalstatistik gibt nur ein beschränktes Bild der Kriminalität wieder, da diese in erster Linie einen Nachweis über das Anzeige- und Arbeitsverhalten der Polizei darstellt.[13] Insofern sind hier eigene Daten im Rahmen von Expert*innen-Interviews erhoben worden, insbesondere in einem Fall von organisiertem, grenzüberschreitendem Fahrraddiebstahl.[14]

### *4.2 Technische Schnittstelle zur Übertragung von Trackingdaten gestohlener Gegenstände an die Polizei*

Da eine Nutzung von Ortungsdaten innerhalb der polizeilichen IT-Systeme aktuell nicht möglich ist, können die Ortungsdaten der Polizei durch einen Trackingservice-Anbietenden zur Verfügung gestellt werden. Der Trackingservice-Anbietende ist eine private Firma, die unter Einhaltung der datenschutz-

12 Ältere Publikationen z.B. Jitschin 2002; Schwind 1989, S. 252 ff.
13 z.B. Bock 2019, S. 318.
14 Fährmann/Höffner/Matzdorf in diesem Band, S. 79ff.

rechtlichen Bestimmungen der DSGVO (z. B. Datensparsamkeit, privacy by design etc.) die Tracking-Daten nach Freigabe der bestohlenen Eigentümer*in speichert. Auf Anfrage der Polizei stellt der Trackingservice-Anbietende ein Portal zur Verfügung, auf dem die Positionen der gestohlenen Gegenstände auf einer Karte abgebildet sind. Ein solcher Trackingservice-Anbietender ist technisch auch in der Lage, durch geeignete Verschlüsselungsverfahren die Trackingdaten fälschungssicher zu speichern, sodass diese in späteren Gerichtsverhandlungen hinzugezogen werden können. Im Rahmen des FindMyBike-Projekts wurde ein solches System prototypisch implementiert[15] und mit der Polizei in mehreren Feldtests[16] erfolgreich evaluiert.

### *4.3 Recht und Datenschutz*

Die rechtliche Perspektive auf die Übertragung von Positionsdaten an die Polizei erfüllt in Relation zur informationstechnischen Perspektive eine zentrale, komplementäre Funktion. Denn die Polizei darf in einem Rechtsstaat nur so agieren, wie die einschlägigen gesetzlichen Vorschriften es vorgeben. Aus der Forschungsperspektive müssen technische Lösungen für die Übertragung von Positionsdaten an die Polizei von vornherein so konzipiert werden, dass sie gesetzliche Mindeststandards einhalten und darüber hinaus Wege aufzeigen, wie die rechtlichen Anforderungen optimal umgesetzt werden können.

Da es aus polizeilicher Sicht vorrangig um die Aufklärung von Diebstahls-Straftaten geht, sind die strafprozessrechtlichen Eingriffsbefugnisse für das Ermittlungsverfahren anzuwenden. Im Einklang mit rechtsstaatlichen Grundsätzen geht das Strafprozessrecht davon aus, dass der Staat weiterreichende Eingriffsbefugnisse haben soll, wenn es um die Aufklärung schwerer Straftaten geht. Dagegen sind die Befugnisse stark begrenzt, wenn weniger gravierende oder gar Bagatellstraftaten aufgeklärt werden sollen. Für die Diebstahlsaufklärung folgt hieraus die Besonderheit, dass sich die polizeilichen Ermittlungsbefugnisse nach dem Diebstahl einer nicht besonders wertvollen Sache in Grenzen halten. Hinzu kommt noch die Problematik, dass die strafprozessualen Vorschriften kaum der schnellen technischen Entwicklung gefolgt sind, sodass für die Nutzung von Positionsdaten für die Straftatenaufklärung keine speziellen Befugnisse existieren.[17] Weiterreichende Befugnisse kommen erst in Betracht, wenn der Diebstahl als gravierender einzustufen ist, etwa weil er von einer Bande oder organisiert begangen wurde.

15 Vollmar/Görlitz/Kober in diesem Band, S. 227ff.

16 Brandt/Vollmar/Görlitz in diesem Band, S. 245ff.

17 Näher hierzu Aden/Fährmann, Vorgänge 2019, S. 95-106 und Fährmann in diesem Band, S. 141ff.

Das Datenschutzrecht ist neben dem Strafprozessrecht das zweite große Rechtsgebiet, das für die Übertragung von Positionsdaten zentral ist. Aus den Positionsdaten gestohlener Gegenstände lassen sich vielfach personenbezogene Daten ableiten. Zwar geben die Positionsdaten zunächst nur die Position des Gegenstandes wieder, jedoch erlaubt diese Position vielfach Rückschlüsse auf eine Person bzw. Personen; etwa wo sich eine Person üblicherweise aufhält und wie sie sich bewegt. Vor dem Diebstahl sind in der Regel Rückschlüsse über die Mobilität der rechtmäßigen Eigentümer*innen möglich. Ab dem Diebstahl können entsprechende Rückschlüsse über die Dieb*innen, Hehler*innen oder auch mehr oder minder gutgläubige Käufer*innen des Diebesguts generiert werden. Somit greift die Verarbeitung privater Positionsdaten als personenbezogene Daten durch die Polizei in das Grundrecht auf informationelle Selbstbestimmung ein, welches das Bundesverfassungsgericht 1983 aus dem Allgemeinen Persönlichkeitsrecht und der Menschenwürde abgeleitet hat.[18]

Diese rechtlichen Anforderungen einschließlich ihrer grundrechtlichen Implikationen, einfachgesetzlichen Ausgestaltung und rechtspolitischen Handlungsbedarfe sind im Rahmen interdisziplinärer Forschung zur Generierung privater Positionsdaten und ihrer Übertragung an die Polizei nach einem Diebstahl zu berücksichtigen.[19] Datenverarbeitungsprozesse müssen für alle Beteiligten zum Schutz ihrer Grundrechte fair und transparent ausgestaltet werden, was bei der Einführung neuer Technologien im Rahmen einer Technik- und Datenschutzfolgenabschätzung bewertet und optimiert werden muss.[20]

### *4.4 Verwaltungswissenschaftliche Perspektiven auf die polizeiliche Diebstahlsaufklärung*

Schließlich ist auch der Umgang von Polizeibehörden mit technischen Innovationen ein wichtiges Element interdisziplinärer Forschung zur Übertragung privater Positionsdaten an die Polizei im Rahmen der Diebstahlsaufklärung. Polizeibehörden sind besondere Verwaltungen, die durch Spezifika ihrer Aufgaben geprägt sind, etwa durch die Aufklärung von Straftaten im Auftrag der Staatsanwaltschaft. Für den Umgang mit personenbezogenen Daten ist die Polizeiarbeit im Vergleich zu anderen Verwaltungen durch zwei Besonderheiten geprägt: Erstens benötigt sie – stärker noch als andere Verwaltungen – Informationen als Kernressource für ihre Arbeit, etwa als Beweise für das Strafverfahren und als Lageinformationen für die Gefahrenabwehr. Insofern ist

18 Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, BVerfGE 65, 1 (Volkszählungsentscheidung).

19 Näher dazu Fährmann/Vollmar/Görlitz in diesem Band, S. 177 ff.; Fährmann/Vollmar/Görlitz in diesem Band, S. 211ff.

20 Näher hierzu Aden/Fährmann, TATuP 2020, S. 24-29.

das polizeiliche Interesse, auch an digitalen Daten, sehr groß.[21] Zum anderen sind diese Informationen zumeist mindestens bis zum Beginn des Strafverfahrens nicht öffentlich, sondern unterliegen einer verschärften Geheimhaltung, etwa um Stigmatisierungen zu vermeiden oder weil Tatverdächtige aus ermittlungstaktischen Gründen nicht erfahren sollen, was die Polizei bereits weiß.[22] Diese Aspekte sind bei allen technischen Innovationen zu berücksichtigen, die externe Datenquellen in die polizeilichen IT-Systeme einbinden. Zentral sind damit auch hohe Anforderungen an die IT-Sicherheit, da sensible Daten zu Straftäter*innen und Verursacher*innen von Gefahren keinesfalls für eine breitere Öffentlichkeit bestimmt sind und insbesondere nicht durch Sicherheitslücken für Unbefugte einsehbar sein dürfen.

Schließlich kommt ein weiterer verwaltungswissenschaftlicher Aspekt hinzu, der für technische Innovationen bei der Polizei generell relevant ist: Wie offen sind Polizeibehörden für technische Innovationen? Polizeiarbeit ist heute in hohem Maße technikbasiert, stößt dabei aber neben den grundrechtlichen Schranken der Verwendung personenbezogener Daten auf zwei weitere strukturelle Grenzen: finanzielle Ressourcen und die Bereitschaft der Mitarbeitenden, technische Innovationen tatsächlich für ihre Arbeit zu nutzen.[23] Beide Aspekte sind wichtige Rahmenbedingungen, die bereits beim Design technischer Innovationen für die Polizeiarbeit berücksichtigt werden sollten. Kosten und Nutzen müssen in einem ausgewogenen Verhältnis stehen, wenn es gelingen soll, die erforderlichen Haushaltsmittel zu mobilisieren. Und die genutzte Technik muss so anwendungsfreundlich sein, dass sie nach ihrer Anschaffung auch genutzt wird. Die Testphase des FindMyBike-Projekts hat gezeigt, dass Innovationen gute Aussichten haben, in der Praxis tatsächlich genutzt zu werden, wenn sie sich ohne größeren Schulungsaufwand intuitiv bedienen lassen und Menüführungen und Oberflächen anbieten, wie sie den Polizeibeamt*innen auch von privaten Geräten vertraut sind.

## 5. Struktur und Beiträge dieses Bandes

Das Buch spiegelt das Vorgehen im Forschungsprojekt wider. Die Beiträge des ersten Teils befassen sich mit dem Entwicklungsstand der Ortungstechnologie und ihrer bisherigen Nutzung für polizeiliche Zwecke. Auf dieser Basis werden der bisherige Anwendungsrahmen dieser Technologie und ihre (zukünftigen)

21 Fährmann, MMR 2020, S. 228.

22 Näher Aden, WEP 2018; Aden, Recht und Politik 2019.

23 Dazu näher Matzdorf in diesem Band, S. 257 ff; Fährmann in diesem Band, S. 267ff.

Nutzungsmöglichkeiten im polizeilichen Alltag und die rechtlichen Rahmenbedingungen der polizeilichen Nutzung analysiert und bewertet.

Der zweite Teil präsentiert Beiträge, die sich speziell mit Fahrrädern als diebstahlgefährdete Gegenstände und der Praxis der polizeilichen Fallbearbeitung beim Fahrraddiebstahl befassen. Dieser Teil trägt dazu bei, eine Forschungslücke zu schließen, da zu diesem Massendelikt kaum wissenschaftliche Erkenntnisse vorliegen. Dabei liegt der kriminalistische Schwerpunkt auf den Fragen, wie die Aufklärungsquote verbessert werden kann und welche Rolle dabei die polizeilichen Ermittlungsstrukturen spielen. Der Status quo wird kriminologisch und kriminalistisch untersucht, um anschließend prüfen zu können, wie sich technische Neuerungen auswirken.

Im dritten Teil werden interdisziplinäre Perspektiven auf die Übertragung von Positionsdaten an die Polizei miteinander verknüpft. Basierend auf den bisherigen Erkenntnissen werden aufgrund des rechtlichen Rahmens informationstechnische Lösungsansätze präsentiert. Im vierten Teil wird schließlich im Rahmen eines experimentellen Designs die technische Lösung evaluiert; erste Überlegungen zur praktischen Umsetzung und dabei möglicherweise auftretenden Problemen in der polizeilichen Arbeit werden angestellt. Der Schlussbeitrag befasst sich mit der Zusammenarbeit zwischen Forschung und Polizei im Rahmen von technischen Innovationsprojekten.

## 6. Dank und Ausblick

Die Herausgebenden danken dem Institut für Angewandte Forschung Berlin e.V. (IFAF), der das FindMyBike-Projekt und damit die Forschung an den in diesem Buch versammelten Aspekten der Ortungstechnik gestohlener Gegenstände sowie die Publikation dieses Buches ermöglicht hat. Dank gilt auch den Fachleuten aus verschiedenen Organisationen und Verwaltungen, die das Projekt als Mitglieder des Beirats mit ihren Ideen und Anregungen unterstützt haben. Wertvolle Unterstützung erhielt das Projekt auch von den studentischen Hilfskräften und den weiteren Bachelorabsolvent*innen, die ihre Abschlussarbeiten zu Projektthemen geschrieben haben. Einige von ihnen sind auch als Autor*innen in diesem Band vertreten. Besonders genannt seien Katharina Noeske und Kevin Kober, die das Projektteam in der Schlussphase ihres Studiums während der gesamten Projektlaufzeit engagiert unterstützt haben.

Ein besonderer Dank gilt schließlich den Forschungspartnern Polizei Berlin und noa Technologies GmbH, die das Projekt auf vielfältige Weise unterstützt und sich auch unmittelbar am Forschungsprozess beteiligt haben. Besonders hervorgehoben sei das Engagement von Denny Noack (Landeskriminalamt Berlin) und Sophie von Stockhausen (noa Technologies GmbH), die mit ihrem

unermüdlichen Engagement von der Konzeptions- bis zur Testphase zum Erfolg des Projekts beigetragen haben. Durch die Nutzung der GPS-basierten Flottenfahrräder sowie die intensive Zusammenarbeit mit dem Polizeiabschnitt 15 und der Polizeiakademie konnte die entwickelte technische Lösung praxisnah getestet werden. Besonderer Dank gilt auch Oliver von Dobrowolski (Polizei Berlin) und Benjamin Schmidt (seinerzeit FÖPS Berlin, jetzt Senatsverwaltung für Inneres), die maßgeblich zur Entwicklung der Forschungsidee und des darauf basierenden Projekts beigetragen haben.

Ausblickend ist diese Buchpublikation eng mit der Frage verknüpft, welche praktischen Auswirkungen die Forschungsergebnisse haben könnten. Für die kooperierenden Unternehmen, die meist nicht über eigene Forschungskapazitäten verfügen, bieten Projekte der anwendungsorientierten Forschung die Möglichkeit praktische Fragestellungen wissenschaftlich breit aufzuarbeiten. Durch Evaluationen der wissenschaftlichen Erkenntnisse können zahlreiche Mitarbeitende mit ihrem Know-how einbezogen werden. Das Ziel von Forschungsprojekten sind üblicherweise praxisnahe Prototypen, die nicht den Reifegrad für den unmittelbaren Einsatz in der Praxis besitzen. Weiterentwicklungen sind erforderlich, um das Produkt im Unternehmen zu nutzen.

Bei der Anbindung von Ortungstechnik an polizeiliche Informationssysteme kommt noch hinzu, dass die Einbindung externer Geodaten in die polizeiliche IT-Infrastruktur mit ihren speziellen, besonders hohen Sicherheitsanforderungen eine große Herausforderung darstellt. Wie so oft bei Forschungsprojekten bleiben die Schritte von der Entwicklung eines Demonstrators bis zum Praxistransfer, etwa in Gestalt eines Geschäftsfeldes für ein neues oder ein bereits auf dem Gebiet tätiges Unternehmen, unklar. Möglicherweise kann diese Buchpublikation hierfür Impulse liefern.

## Literatur

Aden, Hartmut (2018) Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union, in: West European Politics (WEP), 41 Jg., Nr. 4, S. 981-1002.

Aden, Hartmut (2019) Polizei und Technik zwischen Praxisanforderungen, in: Recht und Politik, in: Vorgänge, Nr. 227, 58. Jg., Nr. 3, S. 7-19.

Aden, Hartmut/Fährmann, Jan, (2019) Lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen? Ein Ausblick am Beispiel der GPS-Ortung gestohlener Gegenstände, in: Vorgänge Nr. 227, 58. Jg., Nr. 3, S. 95-106.

Aden, Hartmut/Fährmann, Jan (2019a) Defizite der Polizeirechtsentwicklung und Techniknutzung, in: Zeitschrift für Rechtspolitik, 52. Jg., Nr. 6, S. 175-178.

Aden, Hartmut/Fährmann, Jan, (2020) Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, in: TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, 29. Jg., Nr. 3, S. 24-29.

Aden, Hartmut/Fährmann, Jan/Brandt, Hanno (2019) FindMyBike – Rechtliche und technische Konzepte für die Übertragung von zeitbasierten Geodaten zur Aufklärung von Fahrraddiebstählen, in: Sabrina Schönrock und Wim Nettelnstroth (Hrsg.), Urbane Resilienz – Schutz des öffentlichen Raumes. 2. Fachsymposium zum Terroranschlag auf dem Berliner Breitscheidplatz, Stuttgart u.a.: Boorberg Verlag, S. 50-59.

Bock, Michael (2019) Kriminologie, 5. Aufl. München: Franz Vahlen.

Fährmann, Jan (2020) Digitale Beweismittel und Datenmengen im Strafprozess, in: MMR, 23. Jg., Nr. 4, S. 228-233.

Jitschin, Oliver (2002) Der Fahrraddiebstahl: ein Beitrag zur kriminologischen, kriminalpolitischen und strafprozessualen Problematik eines Deliktes der Massenkriminalität, Göttingen.

Polizeipräsident Berlin (2018) Polizeiliche Kriminalstatistik Berlin 2017 – Kurzüberblick, Berlin.

Statista (2020) Anzahl der polizeilich erfassten Fälle von Diebstahldelikten insgesamt in Deutschland von 2008 bis 2019.

Statista (2020a) Anzahl der polizeilich erfassten Fälle ausgewählter Straftaten/-gruppen in Deutschland im Jahr 2019.

Schwind, Hans-Dieter (1989) Dunkelfeldforschung in Bochum 1986/87. Wiesbaden: Bundeskriminalamt.

Vollmar, Alexander/Görlitz, Gudrun/Fährmann, Jan/Aden, Hartmut (2019) Rechtliche Anforderungen an die Übertragung von GPS-Daten gestohlener Fahrräder und ihre informationstechnische Umsetzung, in: Beuth Hochschule (Hrsg.): Research Day 2018. Stadt der Zukunft, Berlin: Berliner Wissenschafts-Verlag, S. 86-95.

Wollinger, Gina Rosa (2015) Wohnungseinbruch als traumatisches Ereignis, in: MSchKrim 98 Jg., Nr. 4, S. 365-383.

*Alexander Vollmar[1]/Kevin Kober[2]/Gudrun Görlitz[3]*

# Positionsbestimmung mit GNSS – Stand der Technik und Grenzen

## 1. Einleitung

Die Positionsbestimmung mit Hilfe eines Globalen Navigationssatellitensystems (GNSS) ist eine der technischen Grundlagen für die Suche nach gestohlenen Fahrrädern im Projekt FindMyBike. Die hierbei eingesetzten Fahrrad-Tracker nutzen im Allgemeinen das Global Positioning System (GPS) zur Positionsbestimmung. Nachfolgend werden in diesem Sammelband zuerst häufig verwendete Begriffe erläutert und anschließend GNSS sowie insbesondere GPS ausführlich beschrieben.

## 2. Begriffsbestimmungen

**GNSS** (Globales Navigationssatellitensystem, engl. *global navigation satellite system*) ist der Oberbegriff für satellitengestützte Systeme mit denen Positionsbestimmung und Navigation betrieben werden kann. Jedes dieser Systeme nutzt mehrere mit Atomuhren bestückte Satelliten, die auf feststehenden Bahnen die Erde umkreisen und die jeweilige eigene Position und die Uhrzeit aussenden. Die Empfänger dieser Signale können mittels der Kenntnis der Signallaufzeiten, Zeitvergleiche und trigonometrischen Berechnungen die eigene Position ermitteln.[4] Neben dem seit den 70er Jahren eingesetzten und bis heute sehr häufig verwendeten US-amerikanischen GPS sind als weitere GNSS auch das russische GLONASS[5], das chinesische Beidou sowie das europäische GALILEO verfügbar.

---

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

2 Kevin Kober war in dem Projekt FindMyBike studentische Hilfskraft im Bereich Informatik.

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

4 Klußmann/Malik (2018), S. 282.

5 **Гло**бальная **на**вигационная **с**путниковая **с**истема; russisch für "Globales Navigationssatellitensystem“.

Das seit den 70er Jahren vom US-Militär entwickelte **NAVSTAR GPS** (*Navigational Satellite Timing and Ranging - Global Positioning System*) und seit einiger Zeit nur noch als GPS bezeichnete System[6], ist das US-amerikanische GNSS. Die Abkürzung *GPS* wird teilweise als Synonym für Navigationssatellitensysteme benutzt.

**Positionsbestimmung** bezeichnet die Ermittlung der Position eines Objekts innerhalb eines Koordinatensystems (meist als geographische Länge und Breite, zum Teil noch um die jeweilige Höhe ergänzt). Hierbei wird keine Aussage getroffen, ob es sich bei dem bestimmten Ort um die eigene oder eine entfernte Position handelt. In der Fachliteratur werden in diesem Zusammenhang verschiedene Begriffe verwendet, für die jedoch keine einheitlichen und allgemeingültigen Definitionen bestehen. In diesem Sammelband werden die Begriffe *Positionsbestimmung*, *Ortbestimmung* und *Lokalisierung* synonym verwendet. Unter *Ortung* wird die Bestimmung der Position eines *entfernten* Objekts verstanden. Der in englischsprachigen Texten häufig genutzte Begriff *Geolocation* bezeichnet ebenso meist die Positionsbestimmung. Hingegen wird im Deutschen unter *Geolokation* in der Regel das Schließen auf die Position einer Person bzw. eines mit dem Internet verbundenen Gerätes mit Hilfe von Zusatzinformationen, die zu der entsprechenden IP-Adresse verfügbar sind, verstanden.

**(GPS-)Tracker** sind Ortungsgeräte, die an bewegliche Objekte zur Überwachung ihrer jeweiligen Positionen angebracht werden. Diese Geräte ermitteln kontinuierlich die jeweils eigene, aktuelle Position mittels GPS und leiten sie an das ortende System weiter. Der Prozess des Erfassens von Positionsdaten über die Zeit wird als *Tracking* bezeichnet.

## 3. Globale Navigationssatellitensysteme – GNSS

Alle globalen Navigationssatellitensysteme funktionieren nach den Grundprinzipien, welche erstmalig bei GPS angewandt wurden: Die Nutzer*innen empfangen mittels eines Empfangsgerätes Signale der GNSS-Satelliten, aus denen sich die jeweilige Position und gegebenenfalls auch die Geschwindigkeit berechnen lassen. Die Ortsbestimmung wird durch Berechnung der Distanz anhand der Signallaufzeit zwischen Satelliten und Empfangsgerät realisiert, wobei die Satellitenpositionen in den übertragenen Signalen enthalten sind. In Kombination mit mehreren Satelliten lässt sich mittels Triangulation die Position auf der Erdoberfläche bestimmen. Prinzipiell werden zur Positionsbestimmung drei Satelliten benötigt. Da allerdings eine Ungenauigkeit der Uhrzeit im Emp-

6 Bauer 2018, S. 297.

fangsgerät gegenüber der Atomuhrzeit des Satelliten besteht, wird ein vierter Satellit zur Zeitsynchronisation hinzugezogen, wodurch eine Ortsbestimmung im Meterbereich erzielt werden kann.[7]

Die heute genutzten GNSS bestehen aus drei verschiedenen Subsystemen: Die auf festgelegten Bahnen kreisenden zugehörigen Satelliten bilden das sogenannte (*Welt-*)*Raumsegment*. Das *Bodensegment* (auch *Kontrollsegment* genannt) setzt sich aus den Steuer- und Kontrolleinrichtungen auf der Erde, die für den Betrieb des Gesamtsystems notwendig sind, zusammen. Die zivilen und militärischen Anwender*innen des GNSS mit ihren verschiedenen Empfangsgeräten (an Bord von Fahr- oder Flugzeugen, auf Schiffen bzw. als mobile Handgeräte) bilden das *Benutzersegment*.[8]

Bezogen auf die Satellitenkonstellationen eines GNSS müssen, um eine Live-Ortung ständig und überall zu ermöglichen, die folgenden Aspekte beachtet werden: Große Bahnhöhen haben den Vorteil, dass die Zahl der benötigten Satelliten vergleichsweise gering ist. Geneigte Bahnen sind vorteilhaft gegenüber Polbahnen, da hierdurch sowohl die Polgebiete abgedeckt werden können, als auch keine Satellitenhäufungen an den Polen entstehen. Die Gleichverteilung der Satelliten erlaubt die vollständige Abdeckung der Erde bei relativ wenigen Satellitenkontakten.[9]

Die Bestimmung der Position mittels GNSS ist ein passives Verfahren, bei dem keine zentrale Datenbankabfrage notwendig ist, um die jeweiligen Geokoordinaten des Empfängers zu bestimmen. Dies hat den Vorteil, dass nur der Empfänger weiß, wo er sich befindet und dass keine Daten zur Positionsbestimmung kommuniziert werden müssen.[10] GNSS benötigen eine freie Sichtverbindung zu mehreren Satelliten, um zuverlässig zu funktionieren. Im Außenbereich kann diese beispielsweise durch Wolken, Bäume, Tunnel oder Hochhäuser unterbrochen sein. In Gebäuden ist die Möglichkeit eines zuverlässigen GNSS-Empfangs sehr gering.

## 4. Global Positioning System – GPS

Das Global Positioning System ist das GNSS, welches heute von den meisten Navigationssystemen und Trackern genutzt wird. Es wurde seit den 1970er-Jah-

7 Bauer 2018, S. 67–68.
8 Klußmann/Malik 2018, S. 12; Zogg 2014, S. 45.
9 Bauer 2018, S. 201.
10 Schelewsky 2014, S. 9.

ren vom US-Verteidigungsministerium zu militärischen Zwecken entwickelt und am 17. Juli 1995 vollständig ausgebaut in Betrieb genommen.[11]

Für das Global Positioning System werden insgesamt 31 Satelliten eingesetzt, welche die Erde in einer Höhe von 20.180 km auf sechs verschiedenen Bahnen umkreisen. Die Neigung der Satellitenbahnen beträgt 55° zum Äquator, wodurch abhängig von der Position und den Empfangsbedingungen bei nicht beschränkten Sichtverhältnissen von jedem Punkt der Erde GPS-Signale meist gleichzeitig von sechs bis zehn, mindestens aber von vier Satelliten empfangen werden können. Die einzelnen Satelliten haben jeweils vier Atomuhren an Bord und umkreisen die Erde in ca. zwölf Stunden. Als Referenzsystem für GPS dienen die geozentrischen Koordinaten der weltweit verteilten Bodenstationen sowie die GPS-Systemzeit, welche ausschließlich von den Atomuhren des Bodensegments erzeugt wird.[12]

### *4.1 Selective Availability*

GPS befindet sich im Besitz der Regierung der USA und wird von den Luftstreitkräften der USA (United States Air Force) betrieben.[13] Dies bedeutet, dass die Regierung der USA alleine entscheidet, ob und in welchem Umfang es der Allgemeinheit zur Verfügung gestellt wird. Das System wurde von Beginn an als *Dual-Use-System* entwickelt, d.h. es kann sowohl militärisch als auch zivil genutzt werden. Der Dienst für militärische Zwecke, der *„Precise Positioning Service"* (PPS), darf nur von autorisierten Stellen verwendet werden, während der zivile Dienst, der *„Standard Positioning Service"* (SPS), von der Allgemeinheit frei nutzbar ist.[14]

Aus politischen Gründen wurde ein Jahr vor dem Erreichen der vollständigen Betriebsbereitschaft der Zugang zum zivilen Standard Positioning Service eingeschränkt. Im Betriebszustand der *Selective Availability*, der „ausgewählten Verfügbarkeit", bestimmt der Systembetreiber welches GPS-Genauigkeitspotential für die nicht-militärische Nutzung verfügbar ist. Durch verfälschte Satellitenbahndaten und künstliches Verrauschen der Trägersignale wurde die potenzielle Genauigkeit der Ortsbestimmung in Echtzeit verschlechtert.[15]

Bei der Positionsbestimmung mit GPS muss wie bei jeder Messung mit Fehlern gerechnet werden. Diese Fehler lagen bis zum Abschalten der künstlichen Signalverschlechterung mittels Selective Availability bei ca. 50 bis 100

11 Bauer 2018, S. 297.
12 Bauer 2018, S. 298ff; Zogg 2014, S. 9.
13 Department of Defense & NAVSTAR GPS 2008) S. 1.
14 Zogg 2014, S. 9; Bauer 2018, S. 297ff.
15 Bauer 2018, S. 314–315.

Metern.[16] Nach dem Abschalten der Selective Availability am 2. Mai 2000 kann bei der zivilen Nutzung von GPS von einer erreichbaren Genauigkeit von vier Metern im quadratischen Mittel (*root mean square*) bzw. von 7,8 Metern in 95% aller Messungen ausgegangen werden.[17] Weiterhin könnte im Bedarfsfall die künstliche Verschlechterung der GPS-Signale global oder auch nur regional (z.B. in einem Krisengebiet) wieder eingeschaltet werden.[18]

### *4.2 Genauigkeit und Fehleranfälligkeit von GPS*

Die Positionsbestimmung mit GPS ist aus den unterschiedlichen Gründen häufig ungenau und fehleranfällig. Bei schlechten Bedingungen können Fehler von bis zu 100 Metern gegenüber der tatsächlichen Position auftreten, wogegen die Genauigkeit im besten Fall zwischen drei und zehn Metern liegt.[19] Nachfolgend werden Fehlerquellen, die einen besonders starken Einfluss auf das Messergebnis haben, kurz beschrieben.

#### *4.2.1 Satellitenbahnen*

Die Bahnen der GPS-Satelliten werden von fünf Monitorstationen auf der Erde ständig überwacht und vorherberechnet. Bei der Vorausberechnung der Bahnen treten jedoch Abweichungen zu den realen Satellitenbahnen auf. Der Hauptgrund für diese Abweichungen besteht darin, dass das Schwerefeld der Erde nicht vollständig homogen ist. Hierdurch stellen die Satellitenbahnen keine vollkommen gleichmäßigen Ellipsen dar, sondern weichen von dieser Idealform ab.[20] Die Position eines GPS-Satelliten ist zum Zeitpunkt der Signalausstrahlung damit in der Regel nur auf ca. einen bis fünf Meter genau bekannt.[21]

#### *4.2.2 Atmosphärische Fehler*

Bei der Positionsbestimmung wird die Geschwindigkeit der Satellitensignale als konstant angesehen. Auf dem Weg vom Satelliten zum Empfänger durchläuft das Signal jedoch verschiedene Schichten der Atmosphäre und wird dabei mehrfach gebrochen. Die Verzerrungen sind hierbei umso stärker je näher der Satellit über dem Horizont steht.[22]

16 Schüttler 2014, S. 82.
17 Department of Defense & NAVSTAR GPS 2008, S. B-17.
18 Zogg 2014, S. 52–53.
19 Schelewsky 2014, S. 9.
20 Schüttler 2014, S. 81–82.
21 Zogg 2014, S. 91.
22 Schelewsky 2014, S. 9.

Satellitensignale breiten sich mit Lichtgeschwindigkeit aus. In der Troposphäre (0 bis ca. 15 km Höhe) werden diese durch die Erhöhung der Dichte und der Luftfeuchte herabgesetzt. Es wird versucht diesen Einfluss mittels eines einfachen Modells basierend auf Standardatmosphäre und Standardtemperatur zu korrigieren. In der Ionosphäre (60 bis 1000 km Höhe) sind die Gasmoleküle durch die Sonneneinstrahlung tagsüber stark ionisiert (d.h. durch die einfallende Strahlung werden die Elektronen aus den Gasmolekülen gelöst; es entstehen positiv geladene Ionen sowie freie Elektronen). Durch die Ionisierung, die zeitaber auch ortsabhängig und inhomogen ist, wird in diesem Teil der Atmosphäre ebenso die Ausbreitungsgeschwindigkeit verringert. Der Einfluss dieses Effekts kann zumindest teilweise mit geophysikalischen Korrekturmodellen behoben werden.[23]

### *4.2.3 Einfluss der Satellitengeometrie*

Die Stellung der Satelliten (die sogenannte *Satellitengeometrie*) beeinflusst darüber hinaus die Genauigkeit der Positionsbestimmung. Wenn die Satelliten aus Sicht des Empfängers zu dicht beieinanderstehen oder der Höhenwinkel nur sehr gering ist (kleiner als 15 Grad), lässt sich die Position nur noch ungenau bestimmen.[24]

Der Einfluss der Satellitengeometrie ist von der entsprechenden Situation abhängig. So kann es sein, dass sich durch Abschattung im Gebirge nur wenige Satelliten im Empfangsbereich befinden und so die jeweilige Satellitengeometrie vom Empfänger als ungünstig angesehen werden muss. In solchen Situationen sollten die Positionsangaben von GPS-Empfängern durch die Nutzenden immer kritisch eingeschätzt werden.[25]

Langzeitmessungen haben ergeben, dass der horizontale Fehler (d.h. die Abweichung in der Ebene) infolge von unterschiedlichen Satellitengeometrien (in 95% aller Messungen) bei weniger als 7,4 m liegt.[26]

### *4.2.4 Mehrwegeffekte*

Die von den GPS-Satelliten ausgesendeten Signale gelangen nicht nur auf direktem Weg zur Antenne des Empfangsgerätes, sondern auch indirekt durch Reflexionen an Objekten in der Umgebung der Empfangsantenne. Hierbei überlagern sich die direkt einfallenden und die reflektierenden Signale.[27]

23 Zogg 2014, S. 103–104.
24 Schelewsky 2014, S. 10.
25 Schüttler 2014, S. 86.
26 Zogg 2014, S. 96.
27 Bauer 2018, S. 132.

Die Stärke dieses Effekts ist dabei abhängig von der Beschaffenheit der reflektierenden Oberflächen (z.B. Glas und Beton im Gegensatz zu Rasen oder Fels), der Weglängendifferenz zwischen dem direkten und dem indirekten Weg zum Empfänger sowie der jeweils eingesetzten Technik des Empfängers. Durch Abschätzung der verschiedenen Einflussgrößen kann der Fehler durch Mehrwegeffekte normalerweise auf maximal fünf Meter reduziert werden.[28] So kann durch Auswahl einer Mess-Position, die frei von Reflexionen ist, einer guten Antenne und des Messzeitpunktes der jeweilige Einfluss des Mehrwegempfangs zum Teil kompensiert werden.[29]

### *4.2.5 Uhrenfehler*

Die Ermittlung der Entfernung zu den GPS-Satelliten erfolgt durch das jeweilige GPS-Empfangsgerät. Hierbei wird die Zeitspanne bestimmt, die das GPS-Signal vom Satelliten bis zum Empfänger benötigt. Wenn diese Zeit mit der Signalausbreitungsgeschwindigkeit multipliziert wird, kann die Entfernung daraus errechnet werden. Obwohl die Satelliten Atomuhren mit sich führen, besteht eine Abweichung zwischen der Satelliten-Zeit und der des Bodensegments. Ein Zeitfehler von nur zehn Nanosekunden führt hierbei zu einem Fehler von ca. drei Metern.[30]

## *4.3 GPS-Ergänzungen*

Zur Verminderung der unterschiedlichen Defizite von GPS wurden verschiedene Ergänzungen entwickelt. Nachfolgend werden zwei dieser Verfahren, eines zur Erhöhung der Genauigkeit der Ortsbestimmung (DGPS) und ein weiteres zur Reduzierung der Zeit bis zur ersten Positionsbestimmung durch einen GPS-Empfänger (A-GPS) erläutert.

### *4.3.1 Differential GPS – DGPS*

*Differential GPS* ist ein Verfahren, das zur Erhöhung der Genauigkeit der Positionsbestimmung mit GPS unter Zuhilfenahme von Korrekturdaten dient.

Um die oben beschriebenen Fehler, die bei der Positionsbestimmung mit GPS auftreten, beheben oder zumindest verringern zu können, wird an einer Referenzstation, deren Koordinaten geodätisch festgelegt wurden und die damit als *richtig* angesehen werden können, eine Ortsbestimmung mit GPS durchgeführt. Die so ermittelte Position ist hingegen als *fehlerbehaftet* einzustufen. Der

28 Schüttler 2014, S. 86.
29 Zogg 2014, S. 104.
30 Zogg 2014, S. 103.

dabei beobachtete Fehler wird bestimmt und den Nutzer*innen in der Umgebung dieser Referenzstation mitgeteilt. Die Nutzer*innen gleichen dann mittels geeigneter Algorithmen den bei ihnen zu erwartenden Fehler entsprechend aus. Dieses Verfahren ist umso genauer, je näher sich der*die Nutzer*in an der jeweiligen Referenzstation befindet. Mittels DGPS können nahezu alle oben aufgeführten Fehler ausgeschaltet werden. So ist es möglich bei entsprechender Nähe zu einer Referenzstation alle Satelliten und ihre Bahnen betreffenden Fehler sowie die atmosphärischen Störungen herauszurechnen.[31]

Die Genauigkeit einer horizontalen Positionsbestimmung kann mit Hilfe von DGPS von ca. zwölf Metern[32] auf einen Bereich von 0,3 bis 2,5 Meter verbessert werden. Für das Gebiet der Geodäsie kann dieser Wert durch ein weiteres Verfahren (Vermessung der Trägerwelle) noch bis auf einige Millimeter verringert werden.[33]

Zur Verbreitung der Korrektursignale werden verschiedene Systeme eingesetzt. In den USA wird hierbei das Wide Area Augmentation System (WAAS) eingesetzt. Ein entsprechender Dienst existiert in Europa, der *European Geostationary Navigation Overlay Service* (europäischer geostationärer Überlagerungsservice, EGNOS). Die Zusatzinformationen, die von EGNOS bereitgestellt werden, können von den meisten modernen GPS-Empfängern verarbeitet werden.[34]

### *4.3.2 Assisted GPS – A-GPS*

*Assisted GPS* ist ein Verfahren mit dessen Hilfe sich die Zeit für die erste Positionsbestimmung nach dem Start eines GPS-Geräts deutlich reduzieren lässt. Um eine Position genau bestimmen zu können, müssen einem Empfangsgerät die exakten Bahndaten (*Ephemeriden*) der jeweilig genutzten Satelliten bekannt sein. Die Zeit bis zur Bestimmung der ersten Position (*Time To First Fix*, TTFF) dauert um ein Vielfaches länger je nachdem wie lange der GPS-Empfänger abgeschaltet war. Denn durch eine Abschaltung verfügt das Gerät über keine aktuellen Daten. Ist das Gerät weniger als vier Stunden ausgeschaltet, sind die Ephemeriden-Daten, die es zuvor gespeichert hat, noch gültig[35]. Wenn also die Bahndaten, die das Empfangsgerät gespeichert hat, veraltet sind und vom Satelliten neu bezogen werden müssen, dauert die Positionsbestimmung deutlich länger. Zur Beschleunigung dieses Prozesses werden beim A-GPS Hilfs-

31 Mansfeld 2014, S. 215f; Schüttler 2014, S. 90–91.
32 Zogg 2014, S. 103.
33 Schüttler 2014, S. 90–91.
34 Schüttler 2014, S. 97.
35 Eine typische TTFF-Zeit wäre bei einem Kaltstart 44 Sekunden. Siehe Zogg 2010, S. 19.

daten über zusätzliche Datenübertragungswege (z.B. GSM, Internet) genutzt. Die Hilfsdaten umfassen insbesondere die Ephemeriden der GPS-Satelliten, die Satellitenkonstellationen (der sogenannte Almanach) sowie Zeitinformationen. Mit Hilfe dieser Daten kann die TTFF auf bis zu eine Sekunde reduziert werden.[36]

## Literatur

*Bauer, Manfred* (2018) Vermessung und Ortung mit Satelliten - Globale Navigationssatellitensysteme (GNSS) und andere satellitengestützte Navigationssysteme. Berlin, Offenbach: Wichmann.

*Department of Defense & NAVSTAR GPS* (2008) Global Positioning System - Standard Positioning Service - Performance Standard. Washington DC.: https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf (letzter Aufruf: 28.03.2019).

*Klußmann, Niels; Malik, Armin* (2018) Lexikon der Luftfahrt. Berlin, Heidelberg: Springer Verlag.

*Schelewsky, Mark* (2014) Tracking mit Smartphones: Einführung in die Technik und Stand der Forschung. In: Schelewsky, Marc; Jonuschat, Helga; Bock, Benno; Stephan, Korinna (Hrsg.) (2014): Smartphones unterstützen die Mobilitätsforschung. Neue Einblicke in das Mobilitätsverhalten durch Wege-Tracking. Wiesbaden: Springer Vieweg. S. 5-23.

*Schüttler, Tobias* (2014) Satellitennavigation – Wie sie funktioniert und wie sie unseren Alltag beeinflusst. Wiesbaden: Springer Vieweg.

*Mansfeld, Werner* (2004) Satellitenortung und Navigation - Grundlagen und Anwendung globaler Satellitennavigationssysteme. Wiesbaden: Friedr. Vieweg & Sohn Verlag.

*Zogg, Jean-Marie* (2010) Satelliten, wo seid ihr? – Assisted-GPS zur schnellen und genauen Satellitennavigation. In: Elektronik wireless, 10/2010, S. 18-21.

*Zogg, Jean-Marie* (2014):GPS und GNSS: Grundlagen der Ortung und Navigation mit Satelliten. http://www.zogg-jm.ch/Dateien/Update_Zogg_Deutsche_Version_Jan_09_Version_Z4x.pdf; Revision vom 20. Mai 2014, zuletzt Aufruf: 28.03.2019.

36 Zogg 2010, S. 18ff.

*Jan Fährmann[1]/Annika Höfner[2]/Christian Matzdorf[3]*

# Nutzung von Positionsdaten durch die Polizei in Deutschland – Nutzen und (verfassungs-)rechtliche Probleme

## 1. Einleitung

Positionsdaten werden in der polizeilichen strafprozessualen Ermittlungsarbeit bereits vielfach verwendet. Verschiedene Ermächtigungsgrundlagen ermöglichen es der Polizei, derartige Daten auf unterschiedlichen Wegen zu erheben. Der Beitrag betrachtet die Einsatzmöglichkeiten aus unterschiedlichen Perspektiven. Zunächst werden aus kriminalistischer Sicht heraus die Maßnahmen beschrieben und beurteilt, inwieweit sie das strafprozessuale Ermittlungsverfahren fördern können. Dabei wird berücksichtigt, dass zwar in vielen Fällen die betreffenden Maßnahmen rechtlich und auch technisch möglich sind, aber faktisch aus verschiedenen Gründen (insbesondere der limitierten personellen und technischen Ressourcen) nur in einem begrenzten Umfang von den Ermittlungsbehörden auch umgesetzt werden können.

Anschließend werden die einschlägigen Normen aus einer grundrechtlichen und rechtsstaatlichen Perspektive heraus untersucht. Darauf aufbauend wird begutachtet, wann und inwiefern der Einsatz dieser Maßnahmen rechtswidrig ist. Ein besonderer Fokus wird auf die Kumulierung unterschiedlicher Maßnahmen gelegt. Dabei wird in einem interdisziplinären kriminalistischen und juristischen Ansatz insbesondere berücksichtigt, inwieweit diese Maßnahmen geeignet sind und ob mildere polizeiliche Mittel zur Verfügung stehen. Ziel ist es, ein angemessenes Verhältnis zu bestimmen, in dem Positionsdaten durch die Polizei verwendet werden, damit sie ihren rechtsstaatlich und gesetzlich vorgegebenen (Ermittlungs-)Auftrag erfüllen kann, ohne die Grundrechte der Betroffenen unverhältnismäßig stark zu beeinträchtigen.

---

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

2 Annika Höffner war zum Zeitpunkt des Projektes FindMyBike im LKA Brandenburg beschäftigt und stand im Austausch mit dem Projektteam.

3 Prof. Christian Matzdorf hat in dem Projekt FindMyBike kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

## 2. Polizeiliche Maßnahmen zur Erhebung von Positionsdaten

Die Verkehrsdaten, zu denen auch die Positionsdaten gehören, erlangen immer mehr an Bedeutung für die polizeiliche Ermittlungsarbeit. Durch die rege Nutzung von Mobiltelefonen entstehen immer mehr Datensätze, die Rückschlüsse auf das Verhalten von Personen zulassen.[4] So lassen sich z. B. entsprechende Geräte orten, darauf aufbauend Bewegungsbilder erstellen, und es kann die Identität von Personen festgestellt werden, die sich mit dem Gerät zu einem bestimmten Zeitpunkt an einem bestimmten Ort aufgehalten haben.[5]

### *2.1 Einzelne Maßnahmen zur Erhebung von Positionsdaten in der StPO*

Entsprechende Positionsdaten werden sowohl bei der Funkzellenabfrage, bei der stillen SMS, der Verwendung eines sogenannten IMSI-Catchers wie auch bei der Vorratsdatenspeicherung erhoben.[6]

#### *2.1.1 Umsetzung und kriminalistischer Nutzen der Maßnahmen mit Blick auf die Positionsdaten*

Die Erhebung, Speicherung und Auswertung von Positionsdaten sowie ihre Verknüpfung mit Informationen aus anderen Datenquellen sind bewährte und zukunftsträchtige Formen kriminalistischen Vorgehens. Dies kann einerseits zum Zwecke der Informationsgewinnung für das Ermittlungsverfahren im Rahmen der Beweisführung und andererseits zur Unterstützung konkreter taktischer polizeilicher Maßnahmen geschehen; häufig ist von einer Mischform auszugehen.

Eine mobile Observationsmaßnahme, die durch Telekommunikationsüberwachung (TKÜ) unterstützt wird, stellt einen praktischen Anwendungsfall dar: Hier werden Einsatzkräfte nach Maßgabe der Erkenntnisse aus der TKÜ (ggf. inklusive der damit verbundenen Positionsdaten) verdeckt an die betreffenden Zielpersonen herangeführt. Die dabei genutzten Positionsdaten können zu einem Bewegungsbild zusammengeführt werden und so in Verbindung mit weiteren Daten darüber Aufschluss geben, wo und ggf. mit wem sich eine Zielperson an bestimmten Orten aufhält bzw. aufgehalten hat (respektive, wo sich die betreffenden technischen Geräte, welche die Positionsdaten aussendeten bzw. geortet wurden, zum in Rede stehenden Zeitpunkt befinden bzw. befanden).

4 Fährmann, MMR 2020, S. 228.

5 Singelnstein, NStZ 2012, S. 600-601; vgl. zur Standortdaten aus Verbindungsdaten Münch, Die Polizei 2020, S. 45 ff.

6 Z. B. Bär, NZWiSt 2017, S. 83; Decker 2021, S. 156 f.

Ob sich die jeweiligen technischen Geräte tatsächlich in der Verfügungsgewalt einer konkreten Person befinden, erfordert regelmäßig (von TKÜ-Maßnahmen mit eindeutig identifizierten Sprecher*innen abgesehen) weitere Ermittlungsmaßnahmen, die eine beweissichere Zuordnung ermöglichen. Daraus resultiert auch der Umstand, dass häufig ein erheblicher Ermittlungsaufwand für die sichere Zuordnung der Geräte zu einzelnen Personen betrieben werden muss. Im Zusammenhang mit Positionsdaten, die aus den technischen Einrichtungen von Kraftfahrzeugen heraus genutzt werden, eröffnet sich diesbezüglich ein anspruchsvolles Aufgabenfeld für die Kriminaltechnik und damit auch für die Kriminalistik.

Die seitens der Ermittlungsbehörden technisch aufwandsärmste Maßnahme zur Aufenthaltsbestimmung stellt die sogenannte „Stille SMS" dar.[7] Die Live-Ortung erfolgt hierbei durch die Mobilfunkeinrichtungen der Netzbetreiber und bezieht sich auf eine sog. Funkzelle. Da die Größe der Funkzellen (bzw. der Abstand zwischen den zellenbildenden Funkmasten) stark variiert, lässt diese Methode keine exakte Positionsangabe zu; im städtischen Bereich kann die Live-Ortung auf 50 m genau erfolgen, im ländlichen Raum jedoch im Kilometerbereich liegen.[8] Daraus resultierende Informationen können zu einem Bewegungsbild von Zielpersonen zusammengeführt und damit auch eine Zugriffsmaßnahme, beispielsweise zum Zwecke der Strafverfolgung oder zur Vollstreckung eines Haftbefehls (aber auch im Rahmen der Gefahrenabwehr), vorbereitet werden. „Stille SMS" haben für die Ermittlungsbehörden den Vorteil, dass sie ressourcensparend sind, weil keine Beamt*innen vor Ort sein müssen, um Bewegungen der Personen nachvollziehen zu können. Allerdings ist der Erkenntnisgewinn auf einen ungefähren Aufenthaltsbereich von Zielpersonen beschränkt. Daher dient die stille SMS häufig der Vorbereitung weiterer Ermittlungen sowie als unterstützende Begleitmaßnahme.[9]

Die Kennung eines Mobiltelefons lässt sich u.a. durch Einsatz eines IMSI-Catchers ermitteln. Sie ist eine notwendige Voraussetzung für die Erhebung von Telekommunikationsdaten und muss im Vorfeld entsprechender Maßnahmen ermittelt werden.[10] Die dafür notwendigen Erkenntnisse sind nur durch vorhergehende Ermittlungen zu erlangen und häufig nicht oder nur mit (unverhältnismäßig) großem Aufwand verfügbar.

---

7 Eine für die Nutzer*innen nicht wahrnehmbare Übersendung einer „stummen" Nachricht an das Gerät einer Zielperson, für deren Zustellung eine aktive Positionsbestimmung des Gerätes stattfindet und die Positionsdaten an eine dafür vorgesehene technische Einrichtung bei der Polizei zurückgemeldet werden.

8 Farthofer 2020, S. 190.

9 Vgl. Graulich 2021, E. Rn. 8166.

10 Keller/Braun/Hoppe 2015, S. 63.

Auch bei Kenntnis der Kennung der betreffenden Mobiltelefongeräte geht neben der Prüfung der rechtlichen Grundlagen eine Betrachtung der Aufwand-Nutzen-Relation voraus. Die Nutzung der kriminalistischen Möglichkeiten zur Erhebung von Telekommunikationsdaten scheitert häufig auch an dem Volumen der auszuwertenden Daten, die zwar bereitgestellt und technisch aufbereitet sind, aber im (gerichtsverwertbaren) Ergebnis durch fachkundige Ermittlungspersonen bewertet werden müssen. Dieser Vorgang ist aufwändig und setzt besonderes Wissen bei den Ermittelnden voraus, da ansonsten die Ergebnisse nicht beweiskräftig in das Ermittlungsverfahren eingebracht werden können.[11] Aus Einsatzführungssicht müssen daher vorab immer die verfügbaren technischen und personellen Ressourcen in Einklang mit dem Ermittlungsgegenstand (verletztes Rechtsgut, erwarteter Erkenntnisgewinn u.a.) gebracht werden. Daraufhin erfolgt eine Priorisierung, die andere laufende und geplante Ermittlungsmaßnahmen (ggf. ebenfalls unter Einsatz der hier in Rede stehenden technischen Mittel) mit einbeziehen muss.

Der kriminalistische Nutzen von Funkzellenabfragen kann über die bisher dargestellten Erkenntnisgewinne hinaus auch darin liegen, dass durch die Vergleiche mehrerer Abfrageergebnisse einzelne Mobilfunkgeräte identifiziert werden können, die mehrfach in den betroffenen Bereichen eingeloggt waren. Selbst wenn diese noch nicht konkreten Nutzer*innen zugeordnet werden können, besteht beispielsweise auf Basis dieser Erkenntnisse die Möglichkeit, Tatserienzusammenhänge zu erkennen. Oftmals begründen diese Erkenntnisse die Möglichkeit, weitere rechtliche Mittel auszuschöpfen; beispielsweise können im Zusammenhang mit schwerem Bandendiebstahl in Verbindung mit weiteren Informationen entsprechende richterliche Beschlüsse beantragt werden. Bei einer späteren Zuordnung der Daten zu bestimmten Geräten und deren Nutzer*innen ergibt sich ein hoher Beweiswert, der unverzichtbar für die kriminalistische Beweisführung sein kann.

Eine pauschale, vorherige Aussage zum kriminalistischen Nutzen von Positionsdaten ist nicht möglich. So kann ein ganzes Bündel von Eingriffsmaßnahmen unter Umständen lediglich zu geringen Erkenntnisgewinnen führen, sodass regelmäßig bereits begonnene Maßnahmen nach entsprechender Abwägung abgebrochen werden. Dies könnte beispielsweise bei einem großen Kreis von Mobilfunknutzer*innen mit wechselnden Nutzungsgewohnheiten und hoher Fluktuation der Fall sein. Andererseits ist es möglich, mit geringem Aufwand zu einer entscheidenden, für das Ermittlungsverfahren grundlegenden Erkenntnis zu gelangen. Dies wäre beispielsweise bei der Ermittlung eines Aufenthaltsortes einer Zielperson zu einer bestimmten Zeit an einem bestimmten Ort in einem entsprechenden Zusammenhang mit einer Straftat der Fall.

11 Vgl. dazu umfassend Fährmann/Vollmar/Görlitz in diesem Band, S. 211ff.

Diese Umstände erschweren eine Prognose im Rahmen der den Maßnahmen vorgeschalteten Abwägungen und Priorisierungen. Generell kann zumindest festgestellt werden, dass die Nutzung von Positionsdaten von Zielpersonen eine wichtige und in bestimmten Fällen unverzichtbare kriminalistisch-kriminaltechnische Informationsquelle darstellt. Die Positionsdaten müssen immer eingebettet in weitere Ermittlungshandlungen und in deren Kontext betrachtet werden. Die personelle und technische Ausstattung sowie die ebenfalls zu berücksichtigenden weiteren Ermittlungsaufgaben limitieren den Einsatz der technischen Mittel zur Positionsdatenermittlung. Dadurch wird die Anwendungshäufigkeit der entsprechenden Maßnahmen faktisch determiniert.

### *2.1.2 Rechtliche Betrachtung*

Gerade mit Blick auf das Recht auf informationelle Selbstbestimmung führen die Maßnahmen zu verschiedenen Problemen, für die Lösungsansätze zu erarbeiten sind. Die Maßnahmen können in diesem Beitrag allerdings nicht vollständig betrachtet werden, daher konzentriert sich die Beurteilung auf die Positionsdaten.

Jede staatliche Erhebung und Verarbeitung personenbezogener Daten natürlicher Personen stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, welcher einer bereichsspezifischen, hinreichend bestimmten und verhältnismäßigen gesetzlichen Grundlage bedarf.[12] Dies gilt vor allem für polizeiliche Datenerhebung, da der Polizei weitgehende Befugnisse wie beispielsweise verdeckte Maßnahmen zur Informationserhebung und -verarbeitung zustehen.[13]

Das allgemeine Persönlichkeitsrecht gem. Art. 2 I GG i. V. m. Art. 1 I GG gewährleistet den Schutz privater Lebensgestaltung und trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen der Einzelnen Rechnung.[14] Ein zentraler Baustein ist dabei das Recht auf Abschirmung und Rückzug, insbesondere der Schutz der Vertraulichkeit persönlicher Sachverhalte. Am umfassendsten ist die Intimsphäre bzw. der Kernbereich der Persönlichkeit geschützt, d.h. der unantastbare Bereich privater Lebensgestaltung. Staatliche Eingriffe in diesen Bereich sind gänzlich ausgeschlossen.[15] Die Privatsphäre umfasst den engeren persönlichen Lebensbereich, in den nur aufgrund überwiegender Allgemeinwohlinteressen eingegriffen werden kann. Die Sozialsphäre bezeichnet schließlich die gesamte

12 Z.B. BVerfG NJW 2008, 1505 (1507).
13 Arzt 2019, ATDG, § 1 Rn. 10.
14 BVerfG NJW 2009, 3293 (3294).
15 Z.B. BVerfGE 6, 32 (41); BVerfGE 27, 344 (350); BVerfGE 119, 1 (29 f.).

Teilhabe der Grundrechtsträger*innen am öffentlichen Leben. Das Gewicht des Persönlichkeitsschutzes wiegt hier regelmäßig weniger schwer als bei Eingriffen in die Privatsphäre.[16]

Durch das allgemeine Persönlichkeitsrecht soll insbesondere die individuelle Selbstbestimmung geschützt werden. Diese setzt aber – gerade unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass die Einzelnen Entscheidungsfreiheiten über vorzunehmende oder zu unterlassende Handlungen haben. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt oder dem Staat bekannt sind, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.[17] Durch die elektronische Datenverarbeitung sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit in Sekundenschnelle abrufbar. Auch eine Verknüpfung mit anderen Datensammlungen ist möglich, wodurch vielfältige Nutzungsmöglichkeiten entstehen und immer umfassendere Persönlichkeitsprofile erstellt werden können.[18]

Neben dem allgemeinen Persönlichkeitsrecht ist bei der Abwägung auch das staatliche Interesse an einer wirksamen Strafverfolgung zu berücksichtigen. Die Sicherung des Rechtsfriedens durch behördliche Intervention ist eine zentrale Aufgabe staatlicher Gewalt. Die Aufklärung von Straftaten, die Ermittlung der Beschuldigten, die Feststellung ihrer Schuld und ihre Bestrafung bzw. der Freispruch Unschuldiger sind wesentliche Aufgaben der Strafrechtspflege, die zum Schutz der Bürger*innen den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen sollen.[19] Dies folgt aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG).[20]

#### *2.1.2.1 Funkzellenabfrage und Vorratsdatenspeicherung*

Bei der Vorratsdatenspeicherung (§§ 100g StPO, 113 TKG ff.) ist es erforderlich, dass sämtliche Verkehrs- und Positionsdaten ausnahmslos aller am Telekommunikationsverkehr Teilnehmenden durch die Dienstanbieter verpflichtend gespeichert werden. Für jedes elektronische Kommunikationsmittel wird dabei erfasst, wer, wann, von wo, in welcher Weise und wie lange mit wem kom-

16 Vgl. z.B. Martini, JA 2009, S. 840-843. m. w. N.
17 BVerfG NJW 1984, 419 (422).
18 BVerfG NJW 2008, 1505 (1507).
19 BVerfG NJW 2018, 2385 (2387); BVerfGE 107, 104 (118 f.); BVerfGE 113, 29 (54).
20 BVerfGE 46, 214 (222); BVerfGE 80, 367 (375); BVerfG, Beschl. v. 15.1.2009, 2 BvR 2044/07, Rn. 72.

muniziert, damit die Strafverfolgungsbehörden gegebenenfalls später darauf zugreifen können. Im Gegensatz dazu wird bei der Funkzellenabfrage (§ 100g Abs. 3 StPO) ermittelt, welche Endgeräte (Personen) sich zu einem bestimmten Zeitpunkt innerhalb eines abgegrenzten Bereichs des Mobilfunknetzes befanden.

Bei der Vorratsdatenspeicherung und der Funkzellenabfrage besteht die Problematik, dass in großem Umfang Daten von Personen betroffen sind, die an der verfolgten Straftat in keiner Weise beteiligt waren. Grundrechtseingriffe, die sich sowohl durch Verdachtslosigkeit als auch durch eine große Streubreite auszeichnen, weisen grundsätzlich eine hohe Eingriffsintensität auf, auch, wenn sie nur kurzfristig erfolgen.[21] Dabei werden nämlich zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und keine Veranlassung zu dem Eingriff gegeben haben.[22]

Aus der Gesamtheit der bei der Vorratsdatenspeicherung erhobenen Daten könnten sehr genaue Schlüsse auf das Privatleben der betroffenen Personen gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, regelmäßig erfolgende Ortsveränderungen, ausgeübte Tätigkeiten oder auf ihr soziales Umfeld, in dem sie verkehren.[23]

Daher stellt sich gerade bei der Vorratsdatenspeicherung die Frage,[24] ob sie überhaupt mit den europäischen Vorgaben und dem Grundgesetz vereinbar ist.[25] Der EuGH führte aus, dass die schwerwiegenden Eingriffe in die Art. 7 und 8 der Grundrechtecharta erfolgen würden, ohne dass die Nutzer*innen der Kommunikationsdienste darüber informiert würden. Dies sei geeignet, bei den Betroffenen ein Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung sei. Auch könnte die Speicherung der Verkehrs- und Positionsdaten Auswirkungen auf die Nutzung der elektronischen Kommunikationsmittel und infolgedessen auf die Ausübung der in Art. 11 der Charta gewährleisteten Freiheit der Meinungsäußerung durch die Betroffenen haben. Daher vermöge die Bekämpfung schwerer Kriminalität allein diese unterschiedslosen Eingriffe nicht zu rechtfertigen, sondern muss sich auf die absolut notwendige Datenerhebung bei der Bekämpfung schwerer Kriminalität und zur Verhütung ernsthafter Bedrohungen der öffentlichen Sicherheit beschränken.[26] Da die Regelung der Vorratsdatenspeicherung in Deutschland

21 EuGH ZD 2021, 517, 518-519.
22 BVerfG NJW 2006, 1939 1944 m.w.N.; Aden/Fährmann 2018, S. 17-19.
23 EuGH ZUM 2017, 414, 426; EuGH ZD 2021, 517, 518.
24 EuGH ZUM 2017, 414, 414 ff.
25 Z.B. Oehmichen/Mickler, NZWiSt 2017, S. 307; Roßnagel, NJW 2017, S. 697-698.
26 EuGH ZUM 2017, 414, 426 f.; EuGH ZD 2021, 517,

sich in den Grundvoraussetzungen nicht von den Regelungen in Großbritannien und Schweden unterscheidet, ist dementsprechend davon auszugehen, dass sie verfassungs- und europarechtswidrig ist.[27]

Auch die Funkzellenabfrage betrifft fast ausschließlich unverdächtige Personen.[28] Bei ihr werden – aus technischer Sicht unvermeidbar – die Verkehrsdaten aller Personen erhoben, die in der abgefragten Funkzelle mit ihrem Mobiltelefon anwesend waren. Auch bemerken die Betroffenen die Eingriffe im Regelfall nicht, wodurch die Rechtsschutzmöglichkeiten erheblich eingeschränkt sind.[29] Der Eingriff wiegt also schwer. Gleichwohl ist aber zu beachten, dass die Eingriffstiefe gegenüber der Vorratsdatenspeicherung deutlich geringer ist, da der Eingriff räumlich (auf die Funkzelle) und zeitlich begrenzt ist. Auch wenn die Polizei bei einer entsprechenden Abfrage nur die Nummern von Endgeräten erhält, die sich in einer bestimmten Funkzelle befunden haben, handelt es sich dabei jedoch um personenbezogene Daten. Diese Nummern können unproblematisch (allerdings nur innerhalb der gesetzlich vorgesehenen und aus kriminalistischer Ermittlungsperspektive zu knappen Fristen) im Rahmen einer Bestandsdatenabfrage beim Telekommunikationsanbieter einzelnen Personen direkt zugeordnet werden. Durch die Fristen wird das Maß der Drittbetroffenheit auch wieder reduziert, da die Polizei allein aus Kapazitätsgründen nicht alle Daten abgleichen kann bzw. zum Zeitpunkt der Abfrage aus Gründen der Speicherfristen nicht mehr alle relevanten Daten zur Verfügung stehen.

Weiterhin kommt es in der Ermittlungspraxis gelegentlich zu Konstellationen, in denen eine Funkzellenabfrage wesentlich für die Aufklärung von schweren Straftaten ist; besonders in Situationen, in denen ansonsten keine oder nur unzureichende alternative Ermittlungsansätze bestehen. Insofern kann die Abfrage gewichtigen Interessen dienen, sodass eine verfassungskonforme Regelung denkbar ist.

Aufgrund der trotzdem bestehenden Schwere des Eingriffs gebietet der verfassungsrechtliche Bestimmtheitsgrundsatz, dass hohe Anforderungen an die Normenklarheit zu stellen sind.[30] Diese erfordert, dass Grundrechtseingriffe für Bürger*innen vorhersehbar sein müssen, d.h. dass sie abschätzen können, wann und unter welchen Umständen sie damit rechnen müssen. Die Normenklarheit dient auch der wirksamen Begrenzung staatlicher Eingriffe und soll deren effektive gerichtliche Kontrolle sicherstellen.[31] Fraglich ist aber, ob die

27 So auch OVG Münster NVwZ-RR 2018, 43 (47 f.); Petri, ZD 2021, S. 495.

28 Singelnstein, NStZ 2012, S. 602; Eisenberg 2017, Rn. 2478; Fährmann/Aden/Bosch, KrimJ 2020, S. 142; Bär, NZWiSt 2017, S. 85.

29 BVerfG NJW 2016, 1781 (1781); BVerfG 110, 33 (55); BVerfG 113, 348 (376).

30 BVerfG NJW 2016, 1781 (1781) m.w.N.

31 BVerfG NJW 2016, 1781 (1781); BVerfGE 113, 348 (375 ff.)

geltenden Regelungen zur Funkzellenabfrage in § 100g Abs. 1 und 3 StPO diesen Anforderungen genügen.

Eine Funkzellenabfrage ist nach den geltenden Bestimmungen der Strafprozessordnung nur dann zulässig, wenn Straftaten von erheblicher Bedeutung vorliegen, die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert ist. Vor diesem Hintergrund kann man geteilter Ansicht darüber sein, ob die Anforderungen dem Bestimmtheitsgrundsatz genügen und ob die Maßnahme dem Verhältnismäßigkeitsgrundsatz entsprechend ausreichend beschränkt wird. Bär ist der Ansicht, dass der Rahmen im ausreichenden Maße vorgegeben wird, insbesondere um die Rechte von Dritten zu schützen und der Erstellung von Bewegungsprofilen entgegenzuwirken.[32] Dagegen spricht allerdings, dass die Rechte von Dritten nur berücksichtigt werden können, wenn an die Verhältnismäßigkeit oder an die Bedeutung der Sache angeknüpft wird. Diese Tatbestandsmerkmale erscheinen aufgrund ihrer Weite und unterschiedlichen Interpretationsmöglichkeiten aber für den polizeilichen Alltag kaum praktikabel. Gesetzesnormen sollten generell die Beschränkung der Maßnahme nicht im Wesentlichen auf eine Verhältnismäßigkeitsprüfung stützen, vielmehr sollte die Legislative ihrer Verantwortung nachkommen und die Grenzen des Handelns der Exekutive festlegen. Dies ist gerade dann notwendig, wenn komplexe Einsatzlagen vorliegen, die eine schnelle Reaktion erfordern.

Ob die gesetzlichen Vorgaben den Einsatz der Norm ausreichend begrenzen und die Einsatzmöglichkeiten nachvollziehbar verdeutlichen, kann allein schon aufgrund der Anzahl durchgeführter Funkzellenabfragen bezweifelt werden. So wurden allein in Niedersachsen im Jahr 2016 über 19.000 Funkzellenabfragen durchgeführt,[33] wodurch Millionen von Datensätzen entstanden. Im gleichen Zeitraum führten Schleswig-Holstein und Berlin „nur" 866 bzw. 491 Abfragen durch,[34] was die unterschiedlichen Interpretationsmöglichkeiten der Norm verdeutlicht. Allerdings liegen nicht aus allen Bundesländern Zahlen vor. Die Anzahl der Abfragen lässt sich also nur schätzen und ist in anderen Polizeieinheiten möglicherweise deutlich geringer oder höher.

---

32 Bär, NZWiSt 2017, S. 84-85.

33 Niedersächsischer Landtag Drs. 17/7262, S. 2.

34 https://netzpolitik.org/2017/fast-20-000-funkzellenabfragen-pro-jahr-alleine-in-niedersachsen (letzter Aufruf: 20.07.2023).
https://netzpolitik.org/2020/berlin-12-funkzellenabfragen-pro-woche/ (letzter Aufruf: 20.07.2023).

Oft ist der Einsatz der Maßnahme durch technische und personelle Ressourcen faktisch beschränkt. Es ist davon auszugehen, dass zahlreiche Ermittlungsbehörden die Abfrage mit Bedacht und Blick auf den Grundrechtsschutz auslegen und einsetzen. Jedoch deuten gerade die Zahlen in Niedersachsen darauf hin, dass zumindest in einigen Bereichen der Polizei dies nicht erfolgt,[35] wodurch eine eindeutigere Beschränkung der Norm notwendig ist, um den ausufernden Einsatz der Funkzellenabfrage zu unterbinden. Ferner laufen immer mehr Vorgänge automatisiert ab und die Polizei erhält immer mehr technische Hilfsmittel, sodass der personelle und technische Aufwand künftig sinkt und die begrenzten Ressourcen keine „natürliche" Beschränkung für massenhafte Abfragen mehr darstellen.[36] So besteht die Gefahr, dass die Funkzellenabfrage (wie andere Maßnahmen auch) immer umfassender eingesetzt wird. Dem sollte durch klare Tatbestandsvoraussetzungen entgegengewirkt werden.

Derzeit kann allenfalls eine restriktive Interpretation der Norm dazu führen, dass sie als verfassungskonform einzustufen ist. Aufgrund des Verhältnismäßigkeitsgrundsatzes müssen hinreichend konkrete tatsächliche Anhaltspunkte für die Geeignetheit und Erforderlichkeit der Abfrage vorliegen. Die Maßnahme ist als subsidiär gegenüber weniger eingriffsintensiven oder auf einzelne Beschuldigte gerichtete Maßnahmen zu verstehen. *Nicht erlaubt* ist die Abfrage, um potenzielle Tatzeug*innen ausfindig zu machen.[37] Die Erhebung über mehrere Stunden oder gar Tage ist weitgehend ausgeschlossen.[38] Vielmehr muss der Einsatz kurz und präzise erfolgen, auch weil nicht damit zu rechnen ist, dass sich potenziell Beschuldigte nach einer Tat üblicherweise länger im Radius einer Funkzelle aufhalten.

#### *2.1.2.2 Stille SMS und IMSI-Catcher*

Die stille SMS richtet sich dezidiert gegen eine bestimmte Person. Dadurch ist ihre Eingriffsintensität vergleichsweise geringer. Die Ermittlung der Position ist an sich kein so schwerwiegender Eingriff, dass dieser nicht verhältnismäßig sein kann. Mit dem Verhältnismäßigkeitsgrundsatz wäre jedoch unvereinbar, wenn die Maßnahme sehr häufig (d.h. in kurzen Abständen) und über einen längeren Zeitraum angewandt würde, sodass daraus umfassende und aussage-

35 Anzumerken ist, dass die Anzahl der Abfragen von zahlreichen Determinanten wie beispielsweise der Anzahl ermittlungsintensiver (Groß-)Verfahren, die auf technische Auswertung basieren, abhängig ist. Insofern sind die in Rede stehenden Zahlen als allgemeiner Beleg für das breite Spektrum zu interpretieren.

36 Fährmann/Aden/Bosch, KrimJ 2020, S. 141-142; Fährmann, MMR 2021, S. 777-778.

37 Eisenberg 2017, Rn. 2478.

38 Bär, NZWiSt 2017, S. 85.

kräftige Bewegungsprofile der betroffenen Personen erstellt werden können.[39] Umstritten ist immer noch, auf welche gesetzliche Ermächtigungsgrundlage die stille SMS gestützt werden kann.[40] Der BGH hat zwar jüngst bestätigt, dass § 100i Abs. 1 Nr. 2 StPO einschlägig sei, und damit Stellung in einem seit längerem bestehenden Meinungsstreit bezogen.[41] Allerdings kommt auch keine andere Norm innerhalb der StPO in Betracht;[42] pragmatisch betrachtet stellt § 100i Abs. 1 Nr. 2 StPO die einzige mögliche Ermächtigungsgrundlage dar. Jedoch ist fraglich, ob diese Norm ausreichend bestimmt ist und ob ihr Anwendungsbereich dem Grundsatz der Verhältnismäßigkeit genügt. Insbesondere darf kein Automatismus entstehen, die Maßnahme generell oder sogar aus Bequemlichkeitsgründen einzusetzen.

Nach § 100i Abs. 1 Nr. 2 StPO muss eine Straftat von im Einzelfall erheblicher Bedeutung vorliegen, d.h. es bedarf zumindest einer Straftat mittlerer Schwere.[43] Außerdem muss die Maßnahme erforderlich sein.

Durch das Versenden von „stillen SMS" in regelmäßigen Abständen kann mit geringem Aufwand exakter verfolgt werden, wo und wie sich eine Zielperson bewegt. Insofern können mittels der stillen SMS heimlich sehr genaue Bewegungsprofile erstellt werden,[44] da der Polizei oftmals (jedoch nicht zwingend) bekannt sein wird, wer das Mobiltelefon nutzt. So kann aus den Live-Positionsdaten beispielsweise geschlossen werden, wo die betroffene Person arbeitet (etwa an dem Ort, den sie regelmäßig aufsucht), welche Interessen sie hat und wie sie ihren Tag strukturiert; was je nach Ermittlungsfall wertvolle Hinweise für die weitere Einsatztaktik liefert. Gerade das Mobiltelefon ist mittlerweile ein häufig genutzter Gegenstand, den viele Menschen sogar immer mit sich führen, sodass eine längeren Beobachtung sehr genaue Rückschlüsse auf seine Besitzer*innen erlaubt.

Das Versenden der stillen SMS hat eine hohe Bedeutung im polizeilichen Alltag;[45] insbesondere bei der Observation wird die Variationsbreite erheblich und effektiv erweitert (s.o.). Insofern sprechen gewichtige Gründe dafür, den Einsatz dieses Instruments zu ermöglichen.

Die stille SMS wird sehr oft verwendet. So verschickten jeweils im ersten Halbjahr 2018 das Bundesamt für Verfassungsschutz 103.224, das Bundeskri-

39 BGH NJW 2013, 2530 (2537): OLG Lüneburg NJW 2008, 3508 (3509); OVG Hamburg NJW 2008, 96 (97); OLG Koblenz NJW 2007, 2863 (2863); vgl. Damm 2017, S. 77.
40 Singelnstein, NStZ 2012, S. 601; Singelnstein, NStZ 2014, S. 308; Tölpe 2008, S. 257.
41 BGH NStZ 2018, 611, 612 f; kritisch dazu Farthofer, ZIS 2020, S. 192 ff.
42 Vgl. dazu umfassend Tölpe 2008.
43 Eisenberg 2017, Rn. 2508.
44 Rückert, NStZ 2018, S. 613.
45 Rückert, NStZ 2018, S. 613 m. w. N.

minalamt 30.988 und die Bundespolizei 38.990 stille SMS.[46] Unklar ist dabei, auf wie viele Personen sich diese Maßnahmen bezogen. Es ist vorstellbar, dass aufgrund dieser Zahlen für einzelne Personen sehr genaue Bewegungsprofile erstellt werden konnten, abhängig von der Frequenz, mit der die stillen SMS verschickt wurden. Vor diesem Hintergrund ist damit zu rechnen, dass die Landespolizeien und Landesverfassungsschutzbehörden ebenfalls große Mengen an stillen SMS versenden,[47] sodass mit einem Einsatz im Millionenbereich zu rechnen ist. Vor diesem Hintergrund ist fraglich, ob allein das Merkmal „Straftat von erheblicher Bedeutung" und der Hinweis auf die Erforderlichkeit der Maßnahme ausreichend sind, um den Einsatz stiller SMS wirksam zu beschränken. Die Erstellung von Bewegungsprofilen, vor allem aber deren Umfang wird nicht in ausreichendem Maße beschränkt, sodass Zweifel an der Bestimmtheit der Norm gerechtfertigt erscheinen. Im Interesse eines geregelten Einsatzes wäre es sinnvoll, einen klaren Rahmen vorzugeben, etwa hinsichtlich der Länge, da ein länger dauernder Einsatz von stillen SMS mit einer längerfristigen Observation vergleichbar wird, die aber an deutlich strengere Tatbestandsvoraussetzungen geknüpft ist. Klarere Vorgaben sind aus einer rechtsstaatlichen Perspektive heraus wünschenswert, damit die im Einzelfall effektive Maßnahme ausreichend legitimiert ist. Hinsichtlich der Häufigkeit des Einsatzes wird überdies auf die Ausführungen zur Funkzellenabfrage verwiesen (s.o.).

Der Einsatz des IMSI-Catchers richtet sich ebenfalls nach den Voraussetzungen von § 100i Abs. 1 StPO. Dementsprechend stellt sich auch hier wieder die Frage, ob die Tatbestandsvoraussetzungen für die Bestimmtheit ausreichend sind. Ähnlich wie bei der stillen SMS ist auch der Einsatz eines IMSI-Catchers dezidiert auf eine Person bzw. ein konkretes technisches Gerät gerichtet, sodass die Streubreite der Maßnahme nicht hoch ist. Jedoch lässt sich – anders als bei der stillen SMS – nicht ausschließen, dass durch ihn auch die Daten unverdächtiger Personen erhoben werden,[48] wobei der Radius des IMSI-Catchers deutlich kleiner ist als bei einer Funkzelle.[49] Allerdings muss auch beachtet werden, dass sich mittels des Einsatzes von IMSI-Catchern kaum Bewegungsprofile erstellen lassen, da dieser voraussetzt, dass die ungefähre Position des Mobiltelefons bekannt ist. Auch wird die Eingriffstiefe dadurch beschränkt, dass die Daten Dritter sofort nach der Maßnahme zu löschen sind (§ 100i Abs. 2 Satz 2 StPO). Ferner kommt der IMSI-Catcher deutlich weniger zum Einsatz

46 BT-Drs. 19/3678, 9 b.

47 So wurden allein in Berlin 2015 137.905 stille SMS versendet, AGH-Drs. 17/ 17721; in Bayern 2013 654.386, Farthofer, ZIS 2020, S. 191.

48 Lisken/Denninger 2018, Petri G. Rn. 760.

49 Puschke 2006, S. 44.

als die stille SMS,[50] was darauf hindeuten könnte, dass von einer ausreichenden Beschränkung der Maßnahme hinsichtlich der Position auszugehen ist. Dies kann allerdings auch darauf hindeuten, dass es nicht ausreichend Geräte gibt (in Berlin war über Jahre kein derartiges Gerät verfügbar), oder dass die Maßnahme keinen großen polizeilichen Anwendungsbereich hat. Insgesamt lässt sich festhalten, dass die Maßnahme zumindest die Bestimmung der Position betreffend, den verfassungsrechtlichen Anforderungen entspricht.[51]

Insgesamt ist also zu konstatieren, dass aus einer verfassungsrechtlichen Perspektive vor allem eine hohe Streubreite bei der Erhebung von Positionsdaten problematisch ist, da in hohem Umfang Unbeteiligte betroffen werden. Auch sind klarere Tatbestandsvoraussetzungen dort nötig, wo die Gefahr besteht, dass Positionsdaten in einem unverhältnismäßigen Umfang erhoben werden. Da die Daten einen hohen Nutzen für die polizeiliche Arbeit haben können, sind klare gesetzliche Vorgaben notwendig, um sowohl einen Schutz der Grundrechte als auch eine effektive Ermittlungsarbeit zu ermöglichen.

### *2.2 Kumulation von anderen Maßnahmen mit den Positionsdaten von Beschuldigten am Beispiel der Observation*

Ein weiterer Aspekt, den es hinsichtlich der Positionsdaten zu beachten gilt, ergibt sich aus dem Umstand, dass während polizeilicher Ermittlungsmaßnahmen nicht nur einzelne Eingriffsmaßnahmen unabhängig voneinander, sondern in bestimmten Situationen auch gemeinsam (also kumulativ) eingesetzt werden. Dies führt dazu, dass neben dem allgemeinen Persönlichkeitsrecht weitere Grundrechte wie beispielsweise Art. 10 oder 13 GG betroffen sein können.[52] Gleichzeitig besteht die Gefahr, dass durch die verschiedenen Maßnahmen umfassende Profile und damit „gläserne Beschuldigte“ geschaffen werden, was einem schwerwiegenden Eingriff in das allgemeine Persönlichkeitsrecht gleichkommt. Auf der anderen Seite kann es für die Aufklärung von Straftaten erforderlich sein, ein möglichst umfassendes Verhaltensprofil von den Beschuldigten zu erstellen, um Rückschlüsse auf das Tatverhalten ziehen zu können. Eine genaue und umfängliche Beobachtung der Beschuldigten kann daher aus einer

50 2018 wurde die Maßnahme von den Bundespolizeibehörden 52 Mal eingesetzt, siehe https://netzpolitik.org/2018/halbjahreswerte-fuer-stille-sms-imsi-catcher-und-funkzellenabfragen/ (letzter Aufruf: 20.07.2023).

51 Wobei bei den Erwägungen an dieser Stelle nicht die Umstände einbezogen werden können, dass dies im Regelfall der Vorbereitung von weiteren eingriffsintensiven Datenerhebungen dient (der stillen SMS oder der TKÜ) sowie eine Störung von Notrufen möglich macht, was durchaus eine andere verfassungsrechtliche Wertung rechtfertigen kann.

52 Puschke 2006, S. 61-77.

ermittlungstaktischen Perspektive geboten sein. Dementsprechend gilt es zu bewerten, in welchem Umfang sich aus dem Zusammenführen von unterschiedlichen Ermittlungsmaßnahmen ein Mehrwert für die Ermittlungsarbeit ergibt und wie die Kumulation von Informationseingriffen insoweit beschränkt werden kann, dass keine unverhältnismäßigen Profile einzelner Personen kreiert werden. Dazu wird exemplarisch die Observation untersucht.

### *2.2.1 Umsetzung der Maßnahme und kriminalistischer Nutzen*

Die kriminalistische Ermittlungsarbeit basiert auf den Grundlagen des kriminalistischen Denkens und Vorgehens. Dies beinhaltet das Aufstellen von (Tathergangs-)Hypothesen und deren Überprüfung im Rahmen des Verifizierens bzw. Falsifizierens der entsprechenden Annahmen.

Einfach gelagerte Sachverhalte mit kausalen Handlungssträngen und nachvollziehbaren Handlungsanteilen der jeweiligen Personen können regelmäßig durch kriminalistische Arbeit (Inaugenscheinnahme von Örtlichkeiten, eigene Beobachtungen und Feststellungen, Befragungen, Vernehmungen u.v.m.) im Sinne der Ermittlung der materiellen „Wahrheit“[53] (soweit dies überhaupt möglich ist) rekonstruiert werden. Sobald Sachverhalte in Bezug auf einzelne Handlungsabschnitte oder -ebenen bzw. (Tat-)Beteiligungen der handelnden Personen komplexer werden, kann der Einsatz kriminaltechnischer Mittel notwendig werden. Dies ist regelmäßig der Fall, wenn mehrere Personen handeln, eine Fluktuation der beteiligten Personen stattfindet oder Handlungsabläufe sich überschneiden bzw. parallel laufen. Um gerichtsfeste Ermittlungsergebnisse im Sinne einer zweifelsfreien Be- oder Entlastung einzelner Akteur*innen zu erlangen, muss je nach Lebenssachverhalt auch der Einsatz verschiedener technischer Mittel (ggf. kombiniert) angedacht werden.

Konkret auf Observationsmaßnahmen bezogen können dabei – neben anderen technischen Daten – auch Positionsdaten aus verschiedenen technischen Quellen eine Rolle spielen. So wäre es denkbar, dass Positionsdaten eines Kraftfahrzeuges durch Einsatz entsprechender Technik (Anbringen von Sendern, aber auch aktuelles oder retrogrades Auswerten von fahrzeugeigenen Datenspeichern von Navigationssystem, zentraler Steuerungseinheit, Schließtechnik u.a.) ausgewertet werden.

Da der Betrieb eines Fahrzeuges nicht an eine bestimmte Person gebunden ist und aus verschiedenen Gründen eine Observationsmaßnahme „auf Sicht“[54]

53 Matzdorf, Richter ohne Robe 2014, S. 137-139.

54 D.h. ohne direkten oder nur mit eingeschränktem Blickkontakt zur Zielperson (beispielsweise im Rahmen einer durch TKÜ unterstützten mobilen Observationsmaßnahme), vgl. Martini 2009.

nicht möglich sein könnte, kann die Erfassung weiterer (Positions-)Daten notwendig sein. Hier wären die o.g. technischen Möglichkeiten der Live-Ortung mobiler Geräte (einschließlich Mobilfunkgeräte) bzw. die Auswertung der Positions- und Verbindungsdaten zu prüfen. Sollte eine Entscheidung zur „Handyortung" getroffen werden, könnten die fahrzeugbezogenen Daten und die letztgenannten miteinander verbunden werden. Aus der Verbindung von Fahrzeug- und Mobilfunk-Positionsdaten ergäbe sich ein weitaus höherer Informationsgehalt. Jedoch wären auch diese Daten, unbewertet miteinander verbunden, nicht unbedingt beweiskräftig genug, da die Nutzung bzw. konkrete Verfügung über das Mobiltelefon zu einem konkreten Zeitpunkt nicht unbedingt zweifelsfrei einer Person zuzuordnen ist – Handys können leicht weitergegeben werden.

Vor dem Hintergrund des beschriebenen Beispielfalls wäre weiterhin die rechtliche und technische Möglichkeit einer TKÜ zu prüfen, die zum einen Hinweise auf den bzw. die Nutzer*in des Mobiltelefons (Identifikation der sprechenden Person) und weiterhin aus den Gesprächsinhalten entsprechende Informationen erbringen dürfte. Alternativ oder kumulativ könnte von „stillen SMS" Gebrauch gemacht werden, was bei Observationen regelmäßig der Fall ist.[55]

Im Rahmen der Beschreibung des beispielhaften Falls wurden verschiedene kriminalistische und kriminaltechnische Möglichkeiten angeführt. Sofern die rechtlichen Grundlagen geklärt sind, können diese dem jeweiligen Lebenssachverhalt angepasst und in verschiedenen Varianten miteinander kombiniert werden. Die Annahme, dass ein möglichst breiter Einsatz technischer Mittel beispielsweise zur Positionsermittlung den größten ermittlungstechnischen Nutzen erbringt, entspricht jedoch nicht der Realität. Vielmehr ist es notwendig, den Einsatz der technischen und sonstigen Mittel so zu kombinieren, dass das Anforderungsprofil des Einzelfalls optimal erfüllt wird.

Dies setzt vorab und fortlaufend eine Lagebewertung der einsatzführenden Dienstkräfte voraus, die dynamische Lagebilder berücksichtigt und ggf. getroffene Entscheidungen kritisch hinterfragt, was auch aus rechtlichen Gründen geboten ist. So führt der Wegfall von Voraussetzungen für StPO-basierte Maßnahmen zu deren Einstellung. Es kann zudem ermittlungstaktische Gründe geben, die zur vorläufigen oder endgültigen Einstellung einzelner Maßnahmen führen (beispielsweise Bekanntwerden der Maßnahmen oder deren einzelner Komponenten durch Enttarnung, Auffinden von technischem Überwachungsgerät o.a.). Seltener handelt es sich um Entscheidungen aus ermittlungsstrategischer Sicht, die sich dann auf der Basis von Abstimmungen mit der Staatsanwaltschaft hinsichtlich der perspektivischen Vorgehensweise (beispielsweise im Zusammenhang mit Groß- oder Sammelverfahren) ergeben. Dies kann der Fall sein,

55 Eisenberg 2017, Rn. 2479; Singelnstein 2012, S. 601; BGH NStZ 2018, 10/2018, 611, 613.

wenn sich im Rahmen von Ermittlungen (auch anderer Stellen) Erkenntnisse ergeben, die eine neue Bewertung des Gesamtsachverhaltes hinsichtlich von Zuständigkeiten (Polizei und Staatsanwaltschaft), abgestufter Vorgehensweise gegen einzelne Tatbeteiligte, priorisierter Ermittlungsziele und antizipierter Anklagestrategien notwendig machen.

Die wesentlichsten Determinanten für den Einsatz und Umfang von Ermittlungsmaßnahmen liegen jedoch in der Organisation der Ermittlungsbehörden selbst. Sie sind indirekt das Ergebnis von politischen Entscheidungen bzgl. der finanziellen und personellen Ausstattung sowie der Umsetzung dieser Vorgaben in den jeweiligen Behörden. Die hier beschriebenen technischen Maßnahmen erfordern – trotz oder vielmehr wegen der eingesetzten Technik – einen erheblichen Personaleinsatz. So bedarf die TKÜ der Einrichtung, des Betriebes und insbesondere der gerichtsfesten Auswertung durch mit dem Ermittlungssachverhalt betraute Personen, häufig rund um die Uhr an allen Wochentagen. Hier kommt in Zukunft der an technische, aber insbesondere an personelle Grenzen stoßende Anfall von Massendaten hinzu, der oftmals nur noch eine selektive, punktuelle Auswertung erlaubt oder durch eine technische Unterstützung bei der Auswertung (z.B. durch den Einsatz von selbstlernender, künstlicher Intelligenz[56]) bewältigt werden kann.[57] Die Ergebnisse sind in einem Ermittlungsvorgang nicht nur zusammenzufassen, sondern in einen sinnvollen, mögliche Zweifel ausschließenden Bezug zu bringen. Allein die schriftliche Auswertung erfordert einen erheblichen Kräfteeinsatz.

Die Durchführung einer mobilen Observation bedingt ebenfalls einen erheblichen Kräfteeinsatz, ebenfalls regelmäßig rund um die Uhr. Je nach Sachverhalt sind Mitarbeiterzahlen im niedrigen bis mittleren zweistelligen Bereich die Voraussetzung für die Durchführung derartiger Maßnahmen. Zudem muss die Mobilität durch eine Vielzahl von wechselnden Fahrzeugen gewährleistet sein. Selbst das verdeckte Anbringen von technischem Gerät (Peilsendern o.a.), wie auch die vorher notwendigen Ermittlungsschritte, sind personalintensive Aufgaben.

Auch wenn die limitierende Variable der Verfügbarkeit von ausreichendem Personal nicht bestehen würde, müssen die technischen Voraussetzungen für den Einsatz der o.g. Mittel vorhanden sein. Die notwendigen Geräte zur Durchführung von TKÜ-Maßnahmen (z.B. IMSI-Catcher, Peilsender, sonstige Ausrüstung), aber auch Raumkapazitäten sind nicht frei verfügbar, sondern in

56 Wie am Beispiel der Besonderen Aufbauorganisation (BAO) und des Einsatzes neuartiger technischer Lösungen zur Auswertung der (in einem bisher unbekannten Umfang) angefallenen Datenmengen im Zusammenhang mit der Auswertung der sog. „Panama-Papers“ und „Paradiese-Papers“ beim Deutschen Bundeskriminalamt (BKA) ersichtlich.

57 Vgl. dazu Fährmann, MMR 2020, S. 231-232.

den Ermittlungsbehörden (je nach ihrer Ausrichtung auf bestimmte Kriminalitätsformen und ihrer Anbindung an nachgeordnete oder Haupt-Verwaltungen) nur in begrenztem Maße vorhanden. Vor diesem Hintergrund ist jede Maßnahme, wie eingangs beschrieben, einem Priorisierungsverfahren zu unterziehen und muss nicht nur an der rechtlichen Grundlage, der Verfügbarkeit von personellen, technischen und räumlichen Ressourcen, sondern auch noch an der konkreten Belastung der jeweiligen Dienststelle ausgerichtet werden. Triviale Einflussvariablen wie Ferienzeiten, Krankenstände, Baumaßnahmen, Ausfall und lange Reparaturdauer von technischem Gerät beeinflussen regelmäßig den Entscheidungsfindungsprozess und zwingen teilweise auch zur Änderung der Ausrichtung oder zum Abbruch der Maßnahmen.

Vor diesem Hintergrund ist die häufig unterschwellig bestehende Befürchtung, Ermittlungsbehörden würden die rechtlichen Möglichkeiten exzessiv nutzen, um eine möglichst große Anzahl an Daten zu sammeln und somit einen Beitrag zur Entwicklung des „gläsernen Bürgers" leisten, allein aus faktischen Gründen kein realistisches Szenario.

### *2.2.2 Rechtliche Probleme*

Der mit der kumulativen Nutzung mehrerer Ermittlungsmethoden verfolgte Zweck der umfänglichen und genauen Sachverhaltsermittlung ist im Interesse des rechtsstaatlichen Gemeinwesens. Die Kumulation der Maßnahmen ist daher als verfassungsrechtlich legitim anzusehen.[58] Die Zusammenführung unterschiedlicher Eingriffsmaßnahmen wirkt sich aber auch auf den Grundrechtsgebrauch aus. Dadurch wird die Punktualität des Eingriffsbegriffs relativiert und die Wirkung mehrerer Maßnahmen zu einer Gesamtbetrachtung zusammengefasst. Das hat Auswirkungen insbesondere auf die Verhältnismäßigkeitsprüfung,[59] da durch die Kumulation mehrerer Eingriffsmaßnahmen von unterschiedlicher oder gleichartiger Qualität in der Regel eine Steigerung der Eingriffsqualität erfolgt.[60] Gerade der Einsatz mehrerer Grundrechtseingriffe durch Maßnahmen der Informationsbeschaffung auf unterschiedlichen Ebenen

58 Z.B. BVerfGE 107, 299 (316); Puschke 2006, S. 122.

59 Winkler, JA 2014, S. 884; Schwabenbauer 2021, G Rn. 342.

60 Zu der Frage, inwieweit diese noch auf die einzelnen Ermächtigungsgrundlagen gestützt werden können; umfassend Puschke 2006, S. 113-117. Sollte die Eingriffsintensität immens ansteigen oder die Kumulation von verschiedenen Maßnahmen dazu führen, dass sich der Charakter der einzelnen Maßnahmen durch die Zusammenführung ändert, ist es denkbar, dass die Maßnahme nicht allein auf die jeweiligen einzelnen Ermächtigungsgrundlagen gestützt werden kann, sondern, dass eine weitere Ermächtigungsgrundlage oder zumindest eine speziell auf die Kumulation von verschiedenartigen qualifizierten Maßnahmen zugeschnittene Auslegung erforderlich wird.

kann dazu führen, ein sehr umfassendes und dementsprechend sehr eingriffsintensives Profil der Beschuldigten zu erstellen, welches in einer unzulässigen „Rundumüberwachung“ oder „Totalüberwachung“ münden kann, die nicht mit dem allgemeinen Persönlichkeitsrecht und anderen Grundrechten zu vereinbaren wäre.[61] Die Bestimmung der Position kann innerhalb dieses Profils ein wesentlicher Baustein sein.

Unter einer solchen „totalen“ Überwachung ist die umfassende Ansammlung von personenbezogenen Daten zu verstehen, deren Verknüpfung zu einem Erkenntnisstand führt, der Verhaltens- und Lebensweisen sehr detailliert oder nahezu lückenlos nachvollziehbar macht.[62] Wann diese Schwelle überschritten ist, hängt von den Umständen des Einzelfalles ab, d.h. von der Länge der Maßnahmen, dem von den Maßnahmen betroffenen Personenkreis und vor allem davon, ob diese Daten der Privatsphäre bzw. dem Kernbereich der Persönlichkeit zuzuordnen sind. Daher ist es möglich, dass verschiedene einzelne, für sich betrachtet geringfügige, nicht schwerwiegende oder gerade noch verhältnismäßige Eingriffe in ihrer Gesamtwirkung zu einer schwerwiegenden Beeinträchtigung führen, die das Maß der rechtsstaatlich hinnehmbaren Eingriffsintensität überschreitet.[63] Nicht zuletzt kann die Kumulierung von mehreren Maßnahmen zur Datenerhebung das Risiko vergrößern, dass die strafprozessualen Eingriffsmaßnahmen in Richtung des absolut geschützten Kernbereichs der Persönlichkeit[64] vordringen,[65] da exaktere Persönlichkeitsprofile erstellt werden können.

Hinzu kommt, dass mittlerweile nahezu alle Lebensbereiche von Informationstechnik durchdrungen sind und immer größere Verhaltens- und Lebensanteile digitale Spuren hinterlassen. Aus technischen Informationseingriffen können heute sehr viele Rückschlüsse auf die Lebensführung der Bürger*innen gezogen werden, die Polizei kann immer weiter in den privaten Bereich der Bürger*innen vordringen.[66]

Allerdings ist aktuell (noch) davon auszugehen, dass eine Totalüberwachung regelmäßig nur dann in Betracht kommt, wenn umfassende Daten aus der Wohnraumüberwachung, Daten über das Onlineverhalten, der TKÜ oder Live-Positionsdaten über einen längeren Zeitraum kombiniert werden. Die Auswertung von digitalen Daten aus dem Smartphone birgt aber zunehmend die Gefahr, schon für sich zu einer faktischen Totalüberwachung zu werden.

---

61 Vgl. BGH NJW 2009, 3448 (3458); BVerfG MMR 2005, 371, (372); Puschke 2006, S. 81-82, 117-118; Schwabenbauer 2021, G Rn. 371.

62 Puschke 2006, S. 81.

63 BVerfG 2009, 2033 (2045 m. w. N.).

64 Z.B. BVerfGE 6, 32 (41); BVerfGE 27, 344 (350); BVerfGE 119, 1 (29 f.).

65 Aden/Fährmann 2018, S. 23; Puschke (2006), S. 117-118.

66 Aden/Fährmann 2018, S. 18; vgl. BVerfG NJW 2008, 12/2008, 822 (833).

Während der Observation werden ggf. zahlreiche Ermächtigungsgrundlagen kombiniert, sodass aus mehreren parallelen Ermittlungsmaßnahmen systematische verdichtete Informationen gebildet werden können. Da in gewissen Situationen gerade bezweckt wird, ein möglichst genaues Profil der Person zu erstellen, ist davon auszugehen, dass die Eingriffsintensität – auch wenn keine Totalüberwachung vorliegt – oft hoch ist.[67] Insbesondere bei längeren Überwachungen werden umfassende Informationen gewonnen, die genauere Rückschlüsse auf den persönlichen Lebensbereich zulassen.[68] Dies ist aufgrund der beschränkten personellen Ressourcen (s.o.) nicht bei jeder Observation der Fall. Zudem zielt keineswegs jede Observation auf ein umfassendes Profil der Beschuldigten; für die Aufklärung der Straftat kann auch ein beschränktes, weniger eingriffsintensives Bewegungsprofil (beispielsweise nur Bewegungen in einem gewissen Bereich des öffentlichen Raums) ausreichend sein. Da aber die Gefahr einer hohen Eingriffsintensität besteht, muss bei der Bewertung des Maßnahmenbündels eine sorgfältige Verhältnismäßigkeitsprüfung durchgeführt werden.

Grundsätzlich ist hinsichtlich der Geeignetheit davon auszugehen, dass die Wahrheitsermittlung durch eine Verknüpfung von mehreren Maßnahmen (möglicherweise) gefördert wird. Dabei ist in jedem Einzelfall kritisch zu prüfen, ob eine Kombination von Ermittlungsmaßnahmen tatsächlich zu dem gewünschten Erfolg führt.[69]

Probleme können bei der Erforderlichkeit der kumulierten Maßnahmen entstehen. Dazu muss im Einzelfall ermittelt werden, inwieweit jede einzelne Maßnahme in der konkreten Situation tatsächlich benötigt wird, um den Erfolg der Ermittlungen zu gewährleisten. Insbesondere ist zu beachten, ob eine umfängliche Überwachung in jeder Situation erforderlich ist – vor allem, wenn andere Personen zugegen sind, gegen die sich die Ermittlungsmaßnahmen nicht direkt richten.[70] Zur Aufklärung von gewissen Straftaten kann es etwa ausreichen, wenn nur bestimmte Verhaltensweisen beobachtet werden, da nur diese für die Aufklärung relevant sind.

Die Polizei muss sich bei der Datenerhebung auf die Daten beschränken, die sie für die Ermittlungen benötigt. Es darf keinen Automatismus geben, bei der Observation sämtliche Maßnahmen zur Informationsgewinnung zusammenzuführen. Dies wird sich oft schon aus der polizeilichen Bewertung der Einsatzlage ergeben, allein schon aufgrund der beschränkten Ressourcen. Das beugt in vielen Fällen faktisch einer nicht erforderlichen Kombination von

67 Vgl. BVerfG ZD 2013, 03/2013, 126 (127); Puschke 2006, S. 129 f.
68 Puschke 2006, S. 130.
69 Puschke 2006, S. 122.
70 Vgl. BVerfG MMR 2005, 371, (372).

Maßnahmen vor. Gleichwohl besteht die Gefahr, dass Beamt*innen „über das Ziel hinaus schießen“. Zudem wird auch die Observation durch den vermehrten Einsatz technischer Mittel – auch vor dem Hintergrund der o.g. Determinanten – leichter und kann in Zukunft möglicherweise deutlich stärker technisch unterstützt ablaufen, was wiederum die Gefahr eines Automatismus, auf mehrere technische Maßnahmen zuzugreifen, erhöht (s.o.).

Die Zusammenführung unterschiedlicher Ermittlungsmaßnahmen kann in bestimmten Fällen nicht angemessen sein. Hier ist insbesondere die Eingriffsintensität, die durch die Kumulierung entsteht, in Relation zum Verfolgungsinteresse zu setzen. Dabei ist zu beachten, dass die Observation (auch durch technisch gestützte Maßnahmen) eine wesentliche Bedeutung in der Polizeiarbeit hat, denn sie ist sehr aufwendig, sodass die technische Unterstützung diese erheblich erleichtert. Die Observation eröffnet deutlich mehr ermittlungstaktische Möglichkeiten (s.o.). Bei besonders schweren Straftaten kann dementsprechend eine umfassende Kumulierung von Maßnahmen angemessen sein. Allerdings muss auch der möglichen Eingriffsintensität durch die ggf. sehr umfassende Überwachung ausreichend Rechnung gezollt werden. Die wesentlichen Kriterien für die Abwägung der gegenläufigen Interessen sind damit die Schwere der verfolgten Tat(en)[71] und das Maß der Eingriffsintensität. Die Intensität drückt sich insbesondere in folgenden Merkmalen aus: dem zeitlichen Umfang der Observation,[72] dem Umfang der eingesetzten technischen Maßnahmen, den dabei erhobenen Daten sowie den daraus möglichen Rückschlüssen.[73]

### *2.3 Nutzung von GSM- und GPS-Ortungssystemen im Rahmen der Kfz-Diebstahlsaufklärung*

Beispielhaft für die Live-Ortung von Kraftfahrzeugen ist das ursprünglich für die Transportlogistik entwickelte Fahrzeug- und Logistik-Trackingsystem UBINAM.[74] Es stellt ein System für die Nachverfolgbarkeit von Fahrtwegen sowie der aktuellen und retrograden Positionsermittlung von Kraftfahrzeugen dar. Das System arbeitet auf der Basis von GSM- und GPS-Daten, um jederzeit (d.h. je nach den technischen Rahmenbedingungen am jeweiligen Ort) eine entsprechende Positionsdatenübertragung zu gewährleisten.

Insbesondere in der Verbindung von verschiedenen Informationen (Fahrtwege, Live-Positionsdaten, Nutzerdaten, vergangene und aktuelle Positionsda-

71 BVerfG NJW 2016, 1781 (1784).
72 BVerFG NJW 2016, 1781 (1792).
73 Vgl. BVerfG NJW 2008, 1505 (1507).
74 UBINAM: lat. Interrogativadverb, verwendet im Sinne von „wo denn“ von der Ubinam track&act GmbH; https://www.ubinam.de (letzter Aufruf: 20.07.2023).

ten) und der Möglichkeit des Zugriffs auf diese Daten innerhalb der Arbeitszeit des Unternehmens, welches das System betreut (in den jeweiligen Unternehmen mit abgestuften Berechtigungen) ist das Gesamtsystem für kriminalistische Ermittlungen und kriminaltechnische Auswertungen in zahlreichen Straftatzusammenhängen interessant. Vor allem bei überörtlich agierenden Straftäter*innen sowie Banden (beispielsweise in Zusammenhang mit dem Diebstahl hochwertiger Kraftfahrzeuge, Baumaschinendiebstahl, Betäubungsmittelschmuggel, Schleuserkriminalität u.a.) bietet die Auswertung der Daten in Verbindung mit weiteren Ermittlungsergebnissen relevante Ansätze für die Fortentwicklung von Ermittlungsverfahren.

GSM-Daten liefern im ländlichen Kontext allerdings nur sehr ungenaue Positionsdaten. Jedenfalls besteht zumindest ein erster Anhaltspunkt für weitere Ermittlungen, der ansonsten oft fehlt. Innerhalb des städtischen Raums ist GSM dagegen deutlich effektiver. Die technische Entwicklung ermöglicht aber wesentlich genauere Daten, beispielsweise über GPS. Entsprechende technische Einrichtungen sind bereits in vielen privat genutzten und einem großen Teil der gewerblich genutzten Kfz vorhanden oder lassen sich nachträglich leicht einbauen. Der alleinige Zugriff auf GSM-Daten ist auch deshalb nicht ausreichend, weil bei dieser Variante die Positionsdaten beim Anbieter abgefragt werden müssen, wodurch den Ermittlungsbehörden Kosten entstehen und die Ermittlungsarbeit von externen Stellen abhängig wird. Dies ist von Nachteil, da so einerseits Zeit vergeht und andererseits in Eilfällen ein Zugriff auf die Daten außerhalb der Arbeitszeiten des Unternehmens nicht möglich ist.

Die Diebstahlsaufklärung mittels Positionsdaten weist eine deutlich geringere Eingriffsintensität im Vergleich zu den vorher beschriebenen Maßnahmen auf. Zwar besteht auch hier die Problematik, dass gesetzgeberische Vorgaben noch zu unkonkret sind;[75] betrachtet man die Situation aber allein unter dem Gesichtspunkt der Eingriffsintensität, wird deutlich, dass an dieser Stelle gerade keine Kumulation von unterschiedlichen Maßnahmen erfolgt. Weitere Eingriffsmittel stehen schließlich zu diesem Zeitpunkt in der Regel nicht zur Verfügung oder sind nicht ohne Weiteres miteinander verknüpfbar. Regelmäßig können erst nach einer erfolgreichen Live-Ortung weitere Ermittlungsmaßnahmen ergriffen werden.

Zudem handelt es sich um gezielte Eingriffe, die einzelne Personen (die jeweiligen Nutzenden des Kfz) betreffen. Keinesfalls sind Personen betroffen, die nicht in Bezug zur gestohlenen Sache stehen. Dadurch wird gewährleistet, dass die Maßnahme keine große Streubreite hat. Zwar besteht die Möglichkeit, Bewegungsprofile zu erstellen, aber die Eingriffsintensität wiegt in diesem Kontext nicht schwer, da die besitzende Person unklar ist und das Kfz leicht

75 Fährmann in diesem Band, S. 141ff.

weitergegeben werden kann. Insofern sind die Bewegungsprofile weniger eindeutig und ermöglichen nur begrenzte Rückschlüsse auf das gesamte Verhalten der Personen. Ferner werden die Verdächtigen das Kfz oder andere gestohlene Gegenstände – es sei denn, es handelt sich um ein Mobiltelefon, welches weiter genutzt wird – nicht dauerhaft bei sich führen, sodass insbesondere bei Fahrzeugen die Aussagekraft der Daten auf die Bewegungen im öffentlichen Raum beschränkt ist.

Zu beachten ist auch, dass der Einsatz entsprechender Maßnahmen eindeutig durch die Zahl der Delikte und die notwendigen GPS-Sender beschränkt wird. Insofern ist ein „Ausufern" wie bei der stillen SMS aktuell nicht zu befürchten.

Aus einer verfassungsrechtlichen Perspektive wird deutlich, dass der Einsatz neuer Technologien durchaus mit unterschiedlicher Eingriffsintensität einhergehen kann. Die verfassungsrechtlichen Problematiken ergeben sich in erster Linie aus unbestimmten Normen und Eingriffen mit extremer Streubreite, die nicht mehr zwischen unbeteiligten Bürger*innen und beschuldigten Personen unterscheiden. Insgesamt ist ein gezielter Einsatz neuer Technologien, der sich gezielt auf einzelne Personen und/oder Sachen richtet, deutlich weniger eingriffsintensiv und kann gerade bei gestohlenen Gegenständen die Ermittlungsarbeit verbessern bzw. diese erst möglich machen.

### *2.4 Besondere Problematik: „Lockgegenstände"*

Aus Experten*inneninterviews mit Angehörigen unterschiedliche Polizeidienststellen folgte unter anderem die Erkenntnis, dass im Rahmen der Fahrraddiebstahlsaufklärung der Einsatz von sogenannten Lockfahrrädern als eine probate Ermittlungsmaßnahme angesehen wird. Zudem ist der Einsatz von Lockgegenständen auch in anderen Bereichen der polizeilichen Ermittlungsarbeit denkbar.

#### *2.4.1 Einsatz von Lockgegenständen*

Mittlerweile bietet sich Ortungstechnologie für immer mehr Gegenstände an. Mit dem technologischen Fortschritt der letzten Jahre (insbesondere leistungsfähigeren Akkus) und der Entwicklung eines eigenen Marktes für Ortungssysteme (durch Start-Up-Unternehmen) steht nunmehr eine Vielzahl kompakter, leicht verbaubarer und zugleich getarnter Systeme zur Verfügung.

Auch seitens der Polizei wird Ortungstechnik (weiter)entwickelt und in Gegenstände integriert, die potenziell gestohlen werden können. So wurde etwa von der Polizei Brandenburg ein eigenes System für den Einsatz in Fahrrädern entwickelt. Dieses beinhaltete neben einer getarnten Empfangs- und Sendeeinheit, welche über verschiedene Einstellmöglichkeiten zur Taktung verfügt,

einen leistungsfähigen Akku mit einer Laufzeit von mehreren Monaten. Die Signalisierung erfolgte dabei fast ausschließlich aus abgeschirmten Bereichen, etwa umschlossenen Fahrzeugen oder Gebäuden. Die Darstellung der Signalwiedergabe erfolgte über eine separate Anwendersoftware.

Die Nutzung von Ortungstechnik an einem Fahrrad im Rahmen operativer Maßnahmen, in diesem Fall als sog. Lockvogel oder „object provocateur", sollte sich daran ausrichten, welche Ermittlungsziele verfolgt werden. Erst nachdem das Ermittlungsziel bestimmt wurde, kann die entsprechende Ortungstechnik (hier GPS-Tracker) ausgewählt werden. Das Lockvogel-Fahrrad kann einerseits als Einstieg in ein Ermittlungsverfahren dienen, um eine bzw. einen Fahrraddieb*in als Täter*in zu stellen. Damit können aber auch weiterreichende Ziele verfolgt werden, etwa die Identifizierung von Lagerstätten entwendeter Fahrräder, die Ermittlung weiterer Beteiligter (z.B. Zwischenhändler*innen im Rahmen von Hehlereiverfahren oder zum Nachweis der gewerbsmäßigen Begehung von Fahrraddiebstählen), oder die Nachvollziehbarkeit der Vertriebswege des Diebesgutes bis hin zu den Endabnehmer*innen.

Für die weiterreichenden Ziele muss zunächst ermittelt werden, was mit dem entwendeten Fahrrad oder anderen Gegenständen nach dem Diebstahl passiert. Verbleibt dieses nicht für einen gewissen Zeitraum in seinem Originalzustand, sondern wird zeitnah umgebaut oder gar zerlegt und dem Ersatzteilemarkt zugeführt, ist die Präparierung eines Lockfahrrades nur bedingt hilfreich, wenn nicht sogar kontraproduktiv. Das kann über den – noch zu verkrafteten – Verlust der Technik bis hin zur Entdeckung durch die Täter*innen und entsprechenden Verdunkelungshandlungen führen.

Ist dagegen eine „einfache" Stellung der Täter*innen vorgesehen oder besteht die Gefahr des Auseinanderbauens des Fahrrades, so genügt ein kleines kompakteres System ohne externe Stromanbindung an einen separaten Akku, E-Bike-Akku oder als Ladealternative an einen Dynamo den technischen Anforderungen.

Systeme mit integriertem Akku senden nur einen relativ kurzen Zeitraum. Ihre Sendeleistung ist aufgrund der geringeren Spannungskapazität nur beschränkt. So könnte bereits das Befördern des Fahrrades in einem geschlossenen System (z.B. in einem Fahrzeug) oder das Abstellen des Fahrrades in einem Gebäude den Sender abschirmen und das Ortungssignal unterbrechen.

Das bedeutet für die Polizei, dass ein alleiniges Verlassen auf einen GPS-Tracker und dessen Signal keinen Erfolg garantiert. Mit Beginn des Trackings ist daher zeitnah eine visuelle Aufnahme des Fahrrades notwendig, um bei Signalverlust schnell die Ursache erkennen und entsprechend reagieren zu können. Auch spielt die Visualisierung der Täter*innen auf dem präparierten Fahrrad im unmittelbaren zeitlichen und örtlichen Zusammenhang zur Tat eine wesentliche Rolle für den Tatnachweis. Bei einer Feststellung mit wesentlichem

Zeitverzug ist ohne weitere Ermittlungshandlungen möglicherweise nur noch Hehlerei tatsächlich nachweisbar, nicht jedoch der Diebstahl im besonders schweren Fall. Letzterer erweitert jedoch die Bandbreite an möglichen strafprozessualen Maßnahmen erheblich.

Grundsätzlich ist die direkte Tatbeobachtung für ein Ermittlungsverfahren der bestmögliche Fall. Lässt sich diese aber auf Grund der baulichen Gestaltung am Tatort nicht realisieren oder wird aus personellen bzw. taktischen Gründen darauf verzichtet, können anstelle einer konkreten Tatbeobachtung die Täter*innen unmittelbar visuell aufgenommen und ihnen die Taten durch weitere Maßnahmen (wie Beweismittelsicherung oder Spurenauswertung) eindeutig zugeordnet werden.

Eine vollkommen andere Vorgehensweise ist dagegen beim Einsatz von GPS-Trackern notwendig, wenn es um die Ermittlung von „Hinterleuten" bzw. Zwischenhändler*innen oder Verbindungswegen geht. Das setzt jedoch wiederum voraus, dass das Fahrrad im Originalzustand verbleibt. Jede bauliche Veränderung kann zur Entdeckung der Ortungstechnik führen.

Eine Tatbeobachtung ist hierbei auch notwendig, jedoch geht es in diesem Fall in erster Linie darum sicherzugehen, dass der Fahrraddiebstahl wirklich von der Zielperson begangen wird, gegen die sich die Maßnahme richtet. Nach der Tathandlung und der Aktivierung des Trackingsignales konzentrieren sich die Ermittlungen darauf, den weiteren Transportweg des Fahrrads zu verfolgen.

### *2.4.2 Rechtliche Auswirkungen des Einsatzes von Lockgegenständen*

Für die grundrechtliche Eingriffsintensität kann bzgl. des Rechts auf informationelle Selbstbestimmung und das Allgemeine Persönlichkeitsrecht im Wesentlichen auf die Ausführungen unter 2.3 verwiesen werden. Die Intensität des Grundrechtseingriffs wird durch die Aktualisierungshäufigkeit des Ortungssignals beeinflusst, da durch häufigere Übertragungen ein genaueres Bewegungsprofil erstellt werden kann. Jedoch ist gerade bei gestohlenen Gegenständen mit einem zeitnahen Zugriff zu rechnen; je länger gewartet wird, desto höher ist auch die Wahrscheinlichkeit, dass der Diebstahl nicht mehr einer bestimmten Person zugeordnet werden kann. Etwaige erstellte Bewegungsprofile werden meist nicht sehr viele Rückschlüsse auf privates Verhalten zulassen.[76] Jedoch kann es sich wieder eingriffsverschärfend auswirken, wenn das Tracking des Lockgegenstandes mit anderen Maßnahmen kumuliert wird, beispielsweise mit einer TKÜ oder einer Observation. In solchen Situationen ist wiederum der Grundsatz der Verhältnismäßigkeit zu beachten (s.o.).

76 Vgl. auch die Beiträge von Fährmann in diesem Band, S. 141ff; Matzdorf in diesem Band, S. 69ff.

Es stellt sich allerdings die Frage, ob sich aus dem Umstand, dass die Polizei selbst die Tatsituation geschaffen hat, ein Verstoß gegen den aus dem Rechtsstaatsprinzip folgenden Grundsatz des fairen Verfahrens ergibt.[77] Dies kommt insbesondere in Fällen der Tatprovokation in Betracht.

In welchen Situationen eine Tatprovokation unzulässig ist und welche Rechtsfolgen daraus entstehen, ist seit Langem umstritten.[78] Auch wenn die Rechtsprechung tatprovozierendes Verhalten als polizeiliche Ermittlungsmaßnahme grundsätzlich billigt, sieht sie Konflikte mit dem Rechtsstaatsprinzip, gerade wenn bisher unbestrafte, rauschgiftabhängige oder gar unverdächtige Personen zur Straftatbegehung verleitet werden oder die Einwirkung auf die Provozierten besonders intensiv war.[79] Nach der Rechtsprechung des BGH ist das Provokationsverhalten bei der Strafzumessung zu berücksichtigen.[80] Für den Europäischen Gerichtshof für Menschenrechte (EGMR) dagegen kann die Tatprovokation zu einer Verletzung des Rechts auf ein faires Verfahren führen (Art. 6 Abs. 1 EMRK), wodurch die auf die Provokation gestützten Beweise unverwertbar werden oder das Verfahren unter bestimmten Umständen sogar einzustellen ist.[81]

Zunächst ist aber die Frage zu beantworten, ob Lockgegenstände oder sogenannte Diebesfallen überhaupt eine Tatprovokation darstellen. Die Rechtsprechung beschäftigt sich in erster Linie mit sog. Lockspitzeln, d.h. mit verdeckten Ermittler*innen, die auf die Täter*innen einwirken, damit sie Straftaten begehen. Die Situation bei einer Diebesfalle weist dazu zwar Parallelen auf,[82] allerdings ist für Lockspitzel auch charakteristisch, dass sie zumindest den objektiven Tatbestand einer Anstiftung gem. § 26 StGB erfüllen, indem sie spätere Beschuldigte durch Ansprechen, Versprechen oder Überreden – d.h. durch ihr kommunikatives Verhalten – zur Tatbegehung bewegen. Daran könnte es jedoch fehlen, wenn lediglich eine Situation geschaffen wird, die eine andere Person zur Begehung einer Straftat verleitet.[83] Allerdings lässt sich die Frage, ob ein Tatentschluss unter Überschreitung rechtsstaatlicher Grenzen durch staatliche Akteure hervorgerufen wurde, nur unter Beachtung der Umstände des Einzelfalles beantworten. Die dafür notwendige Gesamtbetrachtung erfordert eine Berücksichtigung der Schuld, des Grades des gegen die Beschuldigten

77 Vgl. dazu BVerfG NJW 1981, 1719 (1722).
78 Zur Übersicht: Rönnau, JuS 2015, S. 22.
79 BGH NJW 1984, 2300 (2301); Rönnau, JuS 2015, S. 22; vgl. BayObLGSt 1978, 145 (145 ff.); OLG Düsseldorf NStZ 1992, 237 (237).
80 BGH NJW 1984, 2300 (2302).
81 EGMR NJW 2015, 3631 (3633 ff.); EGMR NJW 2021, 3515 (3521)
82 Vgl. Rönnau, JuS 2015, S. 19; Janssen, NStZ 1992, S. 238.
83 Möllers 2018, S. 550-551.

bestehenden Verdachtes, der vorher bestehenden Tatbereitschaft und der nicht fremdbeeinflussten Aktivitäten im Vorfeld sowie während der Tat. Weiterhin sind die Art, die Intensität und der Zweck der Einflussnahme der staatlichen Akteur*innen sowie die Schwere der Tat zu berücksichtigen.[84]

Sofern beispielsweise ein mit einem Sender ausgestattetes Fahrrad oder ein anderer Gegenstand im öffentlichen Raum abgestellt und an- oder abgeschlossen wird, könnte gegen eine Provokation sprechen, dass gerade Fahrzeuge oft im öffentlichen Raum abgestellt werden und es sich nur um ein übliches Verhalten handelt. In Einzelfällen könnten die Gesamtumstände aber für eine Provokation sprechen, wenn bspw. der Gegenstand nicht ausreichend gesichert wird. Auch kann es sein, dass die Polizei Orte auswählt, von denen sie weiß, dass dort ein hohes Diebstahlsrisiko besteht, oder dass dort potenzielle Täter*innen agieren. In solchen Fällen ist denkbar, dass das Tatverhalten beeinflusst wird, indem eine besondere Tatgelegenheit geschaffen wird.

Sofern die Polizei aber bezweckt, organisierte Diebstahlsstrukturen aufzudecken, ist davon auszugehen, dass die Täter*innen den Tatort bereits mit dem im Vorfeld gefällten Entschluss aufsuchen, einen Diebstahl zu begehen. In einer solchen Konstellation erscheint die Annahme einer Provokation fernliegend. Sollte ein wertvoller Gegenstand hingegen gänzlich ungesichert oder nur sehr schlecht gesichert abgestellt werden, besteht dagegen die Gefahr, dass Personen zum Diebstahl angeregt werden, die diesen sonst nie begangen hätten. In einer solchen Konstellation erscheint eine Tatprovokation wieder näher zu liegen. Aufgrund der mit der Strafverfolgung einhergehenden Grundrechtsverletzungen darf es nicht sein, dass der Staat selbst Bürger*innen, die sonst keine Straftaten begangen hätten, dazu veranlasst, solche zu begehen.[85] Locksituationen sollten in erster Linie diejenigen Personen ansprechen, die nach der Kenntnislage der Polizei gewillt sind, Diebstähle zu begehen (dies erfolgt regelmäßig bereits aus ermittlungstaktischen Erwägungen, s.o.). In solchen Situationen wird ein Beweisverwertungsverbot oder eine Strafmilderung meist nicht in Betracht kommen.

### *2.5 Folgemaßnahmen*

Für die polizeiliche Ermittlungsarbeit und die Beurteilung der Eingriffsintensität ist außerdem relevant, zu welchen Folgemaßnahmen die Erhebung der Positionsdaten führen können.[86] Sofern die Polizei eine Person mit dem gestohlenen

84 BGH NJW 1984, 2300 (2301); vgl. OLG Bremen NZWiSt 2012, 465 (466).

85 Vgl. Sommer, NStZ 1999, S. 49.

86 Zur Verwendung von Positionsdaten im gerichtlichen Verfahren vgl. Fährmann/Vollmar/Görlitz in diesem Band, S. 211ff.

Gegenstand im öffentlichen Raum antrifft, kann sie diesen nach §§ 94 ff. StPO beschlagnahmen und eine Beschuldigtenvernehmung durchführen. Allerdings können sich die gestohlenen Gegenstände auch innerhalb eines Gebäudes, in den Taschen von Personen oder in einem Kfz befinden. Dann stellt sich die Frage, ob auch Fahrzeuge, Personen und vor allem Wohnungen nach §§ 102 StPO ff. aufgrund der Erkenntnisse aus den Positionsdaten durchsucht werden dürfen, was im Folgenden vertieft untersucht wird. Dies setzt einen Anfangsverdacht voraus, d.h. die Begehung einer Straftat muss durch tatsächliche Anhaltspunkte oder durch kriminalistische Erfahrungen belegbar sein.[87]

Ferner bedarf es einer Auffindungsvermutung hinsichtlich der Beweismittel, was beispielsweise durch in den gestohlenen Gegenstände verbaute Ortungstechnik gegeben sein kann.[88] Überdies muss der Eingriff in einem angemessenen Verhältnis zu der Schwere der Straftat und dem Grad des Tatverdachts stehen. Zudem ist die Bedeutung des potenziellen Beweismittels für das Strafverfahren sowie die Auffindungswahrscheinlichkeit von Beweismitteln in die Wertung mit einzubeziehen.[89] Je geringer die Wahrscheinlichkeit ist, dass die Durchsuchung zum Erfolg führt, desto eher ist die Verhältnismäßigkeit zu verneinen.[90]

Wie bereits in diesem Band ausführlich beschrieben, weisen die GPS-Daten eine Ungenauigkeit auf, die je nach den äußeren Umständen mehrere Meter betragen kann. Auch wird das GPS-Signal durch Hauswände stark gestört bzw. kann nicht mehr empfangen werden.[91] Daher werden entsprechende Positionsdaten regelmäßig nicht ausreichen, um einen Durchsuchungsbeschluss für eine Wohnung zu begründen. Für einen Durchsuchungsbeschluss ist essentiell, dass die Position auf einen konkreten Bereich begrenzt werden kann. Es reicht keinesfalls aus, sich nur auf einen nicht näher bestimmten Bereich beziehen. Auf Grundlage einer bloßen Möglichkeit, dass sich dort der „grob" lokalisierte Gegenstand befindet, soll keine Durchsuchungsmaßnahme mit entsprechenden Grundrechtseingriffen für die betroffenen Menschen durchgeführt werden.

Gerade in Großstädten ist eine genaue Zuordnung der gestohlenen Sache zu einer Wohnung äußerst schwierig, insbesondere bei Mehrfamilienhäusern. Oft lässt sich aufgrund der Abweichung noch nicht einmal die genaue Adresse feststellen, erst recht nicht die exakte Wohnung. Wird das Diebesgut in einem Mehrfamilienhaus gelagert, führt dies im Regelfall dazu, dass kein Signal mehr zu empfangen ist. Insofern verbleibt nur die letzte übermittelte Position, die

87 BVerfG NStZ-RR 2006, 110 (110); Müller 2003, S. 26-30 m. w. N.; Park 2002, S. 16.
88 Park 2002, S. 19.
89 BVerfG NJW 2007, 1804 (1804 f.).
90 Knauer/Kudlich/Schneider 2014-Hauschild § 102 Rn. 30.
91 Vollmar/Kober/Görltz in diesem Band, S. 19ff.

aber allenfalls Hinweise auf mehrere Wohnungen gibt, sodass nur eine geringe Auffindungswahrscheinlichkeit für eine einzelne Wohnung besteht. Wenige Meter Spielraum können auf diese Weise die eindeutige Zuordnung eines gestohlenen Objektes zu einer Wohnung und damit eine Durchsuchung unmöglich machen.

Auch für die Durchsuchung einer Person oder von Gegenständen (etwa einem Kfz) sind die GPS-Daten im städtischen Raum oftmals zu ungenau, sofern sich im Radius von einigen Metern mehrere Personen oder Fahrzeuge aufhalten. Aufgrund der Ungenauigkeit des GPS-Systems können die Daten meist nicht einer bestimmten Person zugeordnet werden, es sei denn, es befindet sich nur eine Person in dem Radius des Signals. Daher sind in dieser Konstellation neben den Positionsdaten häufig noch weitere Anhaltspunkte erforderlich, um eine ausreichend hohe Auffindungswahrscheinlichkeit zu begründen. Entsprechend muss die Polizei die Bewegungen der entwendeten Sachen und/oder der Personen, die die Sache möglicherweise besitzen, beobachten, um eine eindeutige Zuordnung zwischen ihnen vornehmen zu können.

Befindet sich der Gegenstand in einer ländlichen, weniger stark besiedelten Gegend, so kann oftmals ein Grundstück konkretisiert und somit ein/e von der Maßnahme betroffener Grundstücksinhaber*in bestimmt werden. Bei einem freistehenden Haus oder einer Lagerhalle kann gegebenenfalls eine ausreichend hohe Auffindungswahrscheinlichkeit begründet sein, vor allem, wenn das Gebäude nicht in unterschiedliche Wohnungen unterteilt ist. In solch einem Fall können die Positionsdaten möglicherweise eindeutig einer Wohnung zugeordnet werden.

Es ist also grundsätzlich notwendig, der lokalisierten Position auf seine Genauigkeit hin zu überprüfen. Ein Abgleich zwischen den vom Sender ausgegebenen Positionsdaten mit den vor Ort bestehenden Umständen ist unerlässlich. Bei großen Unklarheiten sollte ggf. eine Referenzmessung erfolgen. Über die Vor-Ort-Aufklärung ist die geografische und bauliche Beschaffenheit der Position zu bestimmen, aus der sich weitere Anhalte zur Bestimmung des Aufenthaltsortes des Gegenstandes ergeben können. Die Positionsdaten können so einen wesentlichen Anhaltspunkt in der Begründung zum Durchsuchungsantrag darstellen. Dieser muss jedoch regelmäßig durch weitere Ermittlungen untermauert werden.

Daher ist von vornherein abzuwägen, ob GPS-Sender oder andere Ortungstechnik durch weitere Technologien ergänzt werden können, etwa durch Bluetooth zur Lokalisierung innerhalb eines Gebäudes oder durch optische bzw. akustische Signale. Ferner könnten Ortungssysteme so konstruiert werden, dass die Polizei ein Signal (Ton/Licht) auslösen kann, wenn sie sich in unmittelbarer Nähe des Gegenstandes befindet.

## 3. Zusammenfassung

Positionsdaten werden heute bereits umfangreich im polizeilichen Alltag eingesetzt. Sie nehmen in der Ermittlungsarbeit eine wichtige Rolle ein, da sie unterschiedliche Ermittlungsmaßnahmen effektiv unterstützen können. Aus verfassungsrechtlicher Perspektive sind diese Maßnahmen als mehr oder weniger eingriffsintensiv zu bewerten. Eingriffe mit einer hohen Streubreite wiegen deutlich schwerer als zielgerichtete Maßnahmen, die sich auf einen beschränkten Personenkreis beziehen. Bei der Kumulation mit anderen Ermittlungsmaßnahmen ist darauf zu achten, dass der Verhältnismäßigkeitsgrundsatz eingehalten wird.

## Literaturverzeichnis

*Aden, Hartmut/Fährmann, Jan* (2018): Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive. https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf (letzter Aufruf: 21.02.2023).

*Arzt*, *Clemens (2019)*: F. Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz-ATDG). In: Schenke, W.-R./Graulich, K./Ruthig, J. (Hg.): Sicherheitsrecht des Bundes. 2. Aufl. München: C.H. Beck, S. 921–976.

*Bär, Wolfgang* (2017): Die Neuregelung zur Erhebung von Verkehrsdaten – Inhalt und Auswirkungen, in: NZWiSt, 6. Jg., Nr. 2, S. 81–86.

*Damm, Matthias* (2017): Der Zugang zu staatlichen Geodaten als Element der Daseinsvorsorge. Berlin: Duncker & Humblot.

*Decker, Davin* (2021): Systematik der Beweisverwertung, Wiesbaden: Springer.

*Eisenberg, Ulrich* (2017): Beweisrecht der StPO. Spezialkommentar. 10. Aufl.

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

*Fährmann, Jan (2021):* Mehr Transparenz durch technische Innovationen?, in: MMR, 24. Jg., Nr. 10, S. 775-779.

*Fährmann, Jan/Aden, Hartmut/Bosch, Alexander (2020):* Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzänderungen, in: KrimJ, 52 Jg., Nr. 2, S. 135-148.

*Farthofer, Hilde* (2020): Der Einsatz neuer Ermittlungsmaßnahmen, in: ZIS 4/2020, S. 190-195

*Graulich, Kurt* (2021): Das Polizeihandeln. In: Lisken, H./Denninger, E. (Hg.): Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz. 7. Aufl. München: C.H. Beck, S. 341–644.

*Knauer, Christoph/Kudlich, Hans/Schneider, Hartmut* (2014): Münchener Kommentar zur StPO, München: Beck.

*Janssen, Bernhard* (1992): Anmerkung zu OLG Düsseldorf, Beschluss vom 29.11.1990 - 130/90 II - 2 Ss 330/90, in: NStZ, 12 Jg., Nr. 5, S. 237–238.

*Keller, Christoph/Braun, Frank/Hoppe, René* (2015): Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen. 2. Aufl. Stuttgart, München, Hannover, Berlin, Weimar, Dresden: Boorberg.

*Matzdorf, Christian* (2014): Der Beitrag der Kriminalistik zur Wahrheitsfindung, in: Richter ohne Robe 4/2014, S. 137–141.

*Martini, Mario* (2009): Das allgemeine Persönlichkeitsrecht im Spiegel der jüngeren Rechtsprechung des Bundesverfassungsgerichts, in: JA, 41 Jg., Nr. 12, S. 839–845.

*Möllers, Martin H. W.* (2018): Wörterbuch der Polizei. 3. Aufl. München: C.H.Beck.

*Müller, Cathrin* (2003): Rechtsgrundlagen und Grenzen zulässiger Maßnahmen bei der Durchsuchung von Wohn- und Geschäftsräumen. Baden-Baden: Nomos-Verl.-Ges.

*Münch, Holger* (2020): Mindestspeicherfristen und ihre Bedeutung für eine erfolgreiche Polizeiarbeit, in: Die Polizei, S. 45-49.

*Oehmichen, Anna/Mickler, Christina* (2017): Die Vorratsdatenspeicherung – Eine never ending story?, in: NZWiSt, 6 Jg., Nr. 8, S. 298–307.

*Park, Tido* (2002): Handbuch Durchsuchung und Beschlagnahme. Mit Sonderteil zur Unternehmensdurchsuchung. München: Beck.

*Petri, Thomas* (2021): Die Vorratsdatenspeicherung, in: ZD, 11 Jg., Nr. 9, S. 493-496.

*Puschke, Jens* (2006): Die kumulative Anordnung von Informationsbeschaffungsmaßnahmen im Rahmen der Strafverfolgung. Eine Untersuchung unter rechtlichen, rechtstatsächlichen und kriminologischen Aspekten. Berlin: Duncker & Humblot.

*Rönnau, Thomas* (2015): Grundwissen – Strafrecht: Agent provocateur, in: JuS, 55 Jg., Nr. 1, S. 19–22.

*Roßnagel, Alexander* (2017): Vorratsdatenspeicherung rechtlich vor dem Aus?, in: NJW, 70 Jg., Nr. 10, S. 696–698.

*Rückert, Christian* (2018): Praxiskommentar, in: NStZ, 38 Jg., Nr. 10, S. 613–614.

*Schwabenbauer, Thomas* (2021): G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht. In: Lisken, H./Denninger, E. (Hg.): Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz. 7. Aufl. München: C.H. Beck, S. 835–1218.

*Singelnstein, Tobias* (2012): Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen. Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: NStZ, 32. Jg., Nr. 11, S. 593–606.

*Singelnstein, Tobias* (2014): Bildaufnahmen, Orten, Abhören – Entwicklungen und Streitfragen beim Einsatz technischer Mittel zur Strafverfolgung, in: NStZ, 34 Jg., Nr. 06, S. 305–311.

*Sommer, Ullrich* (1999): Anmerkung zu EGMR, Urteil vom 09.06.1998 – 44/1997/828/1034, in: NStZ, 19 Jg., Nr. 1, S. 47-50.

*Tölpe, Stephan* (2008): Die strafprozessuale Ermittlungsmaßnahme „stille SMS“, Zugl.: Frankfurt/Oder, Univ., Diss., 2007. Berlin: wvb Wissenschaftlicher Verl.

*Winkler, Roland* (2014): Der „additive Grundrechtseingriff“: Eine adäquate Beschreibung kumulierender Belastungen?, in: JA, 46 Jg., Nr. 12, S. 881–887.

*Jessica Kraus[1]/Jan Fährmann[2]*

# Nutzung von Live-Positionsdaten im Rahmen von längerfristigen Observationen und bei der Fahndung nach Diebesgut im Vergleich

Wie bereits dargelegt, nutzt die Polizei bereits Positionsdaten im Ermittlungsverfahren, insbesondere bei der Observation.[3] Mithin verfügt die Polizei über Erfahrungswissen hinsichtlich des Einsatzes von Ortungstechnologie. Daher stellen sich die Fragen, welche Rückschlüsse aus diesen Erkenntnissen hinsichtlich der Live-Ortung von Diebesgut gezogen werden können und inwieweit das Erfahrungswissen aus der Observation auf das Auffinden von Diebesgut übertragen werden kann? Zur Beantwortung dieser Fragen sind die beiden Maßnahmen aus einer kriminalistischen und polizeitaktischen Perspektive heraus miteinander zu vergleichen. Auf den Gemeinsamkeiten sowie den Unterschieden aufbauend werden Anforderungen an die Ortungstechnik zur Diebstahlsaufklärung formuliert. Dabei werden auch der Einbau und die Einsatzbereitschaft der Ortungstechnologie, Qualitätsmerkmale der GPS-Module sowie die Akkulaufzeiten betrachtet.

Untersucht wird primär die Positionsermittlung mittels GPS-Technologie, da die Live-Ortung in der Polizeipraxis überwiegend über GPS erfolgt,[4] sodass diesbezüglich die meisten Erkenntnisse bestehen.

## 1. Einbau des GPS-Senders und polizeiliche Ressourcen

### *1.1 Parallelen zwischen der längerfristigen Observation und der Diebesgutfahndung*

Die Live-Ortung setzt voraus, dass ein GPS-Trackingmodul an oder in dem zu ortenden Gegenstand verbaut wurde, und zwar so, dass der Gegenstand von den Nutzer*innen nur schwer entdeckt werden kann. Andernfalls besteht

1 Jessica Kraus hat ihre Bachelorarbeit begleitend zum Projekt FindMyBike geschrieben.
2 Dr. Jan Fährmann war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die rechtlichen und kriminologischen Forschungsfragen.
3 Siehe Vollmar/Kober/Görlitz Beitrag in diesem Band, S. 19ff.
4 Vgl. BVerfG NJW 2005, 1338 (1338 ff.); Singelnstein NStZ 2012, S. 559; Glitza 2014, S. 178.

die Gefahr, dass dieser Sender entfernt oder unbrauchbar gemacht wird. Beim Einbau des Moduls wird zudem auf die Optimierung der Signalstärke geachtet. Dazu muss die optimale Platzierung gefunden und der Sender muss stabil befestigt werden. Die Signalstärke ist von mehreren Faktoren abhängig, die ausführlich unter 19 ff. beschrieben werden. Um eine möglichst hohe Signalstärke zu ermöglichen, muss sichergestellt werden, dass Faktoren, die das GPS-Signal stören, soweit wie möglich minimiert werden. So verringern etwa metallische Gegenstände – auch Kunststoffverkleidungen mit metallischen Anteilen – zwischen Empfänger und Satelliten die Signalstärke. Für eine versteckte Positionierung kann es aber notwendig sein, auf eine optimale Signalstärke zu verzichten, da der Einsatz des Ortungsmittels sinnlos wäre, wenn der Sender von den Betroffenen entdeckt und entfernt wird. Vor dem Einbau müssen daher die gegenläufigen Faktoren sorgfältig gewichtet und gegeneinander abgewogen werden. Darauf aufbauend wird der Anbringungsort sowie das Befestigungsmaterial festgelegt.[5]

### *1.2 Einbau des GPS-Senders bei der Observation*

Bei der Observation wird das Modul üblicherweise an oder in einen viel genutzten Gegenstand verbaut,[6] der Rückschlüsse auf die Observierten erlaubt, etwa einem Kraftfahrzeug (Kfz). Der Polizei ist zu diesem Zeitpunkt regelmäßig bekannt, wo sich die zu observierende Person, bzw. der von ihr genutzte Gegenstand befindet. Der Einbau muss häufig schnell, unauffällig und reibungslos verlaufen, damit er nicht bemerkt wird. Ein Festeinbau kommt daher im Regelfall nicht in Betracht. Zunächst ist der Festeinbau rechtlich problematisch, da es sich häufig um Gegenstände handelt, die nicht im Eigentum der Polizei stehen.[7] Außerdem wird die Ortungstechnik meist nicht nur für einen Einsatz angeschafft, sondern sie wird auch für andere Einsätze benötigt. Die Polizei kann darüber hinaus ein Interesse daran haben, den Sendern selbst unproblematisch entfernen zu können, um das Risiko zu minimieren, dass dieser entdeckt wird. Zur Befestigung kommen daher Industriemagnete, elastische Haftmasse, Klebstoffe, Spezialstoffe zur Abdichtung der Karosserie oder Klebebänder in Verbindung mit Kabelbindern in Betracht. Die Wahl des Befestigungsstoffes ist von den vorliegenden Gegebenheiten und der gewählten Positionierung abhängig.[8] Mit dem passenden Befestigungsstoff kann gewährleistet werden, dass die

5 Umfassend dazu Glitza 2014, S. 179.
6 Vgl. Vahle NVwZ 2003, S. 515; Glitza 2014, S. 178.
7 Vgl. Glitza 2014, S. 191; Gola ZD 2012, S. 310.
8 Glitza 2014, S. 187.

Sender leicht und schnell von den Beamt*innen angebracht, aber auch entfernt werden können.

Beim Kfz sollte eine Anbringung in unmittelbarer Nähe zu beheizbaren Front- oder Heckscheiben vermieden werden, da diese die Sendeleistung negativ beeinflussen können. Daher sollte die Montage beim Kfz möglichst nahe an den Außenrändern des Unterbodens erfolgen, im Idealfall in Richtung des Hecks. So ist der Empfänger in der optimalen Position zum Signalabtausch mit den Satelliten. Gleichzeitig sollte das Modul aber so angebracht werden, dass es bei einer Inspektion des Kfz nicht ohne weiteres entdeckt wird, was der vorherigen Positionierungsempfehlung in Teilen widerspricht. Demnach bieten sich als Montagepunkte die hinteren seitlichen Bereiche der Schürze, die Innenseite bzw. Befestigungselemente der Stoßfänger, Kunststoffkotflügel sowie der Radlauf an.[9]

Allein aus dem Aufwand des Einbaus wird bereits deutlich, dass für eine Observation nicht unbeträchtliche polizeiliche Ressourcen erforderlich sind. Zudem werden bei der Observation auch Personen für die Beobachtung der Observierten und weitere Aufgaben notwendig, sodass im Regelfall mehr als 15 Personen für die Durchführung einer Observation benötigt werden.[10]

### *1.3 Einbau des GPS-Senders zur Ortung von Diebesgut*

Zur Ortung von Diebesgut wird das GPS-Modul durch oder im Auftrag der Eigentümer*innen des potenziell gestohlenen Gegenstandes eingebaut.[11] Ein nachträgliches Anbringen nach dem Diebstahl ist nicht möglich. Für die Live-Ortung potentiellen Diebesguts ist hingegen ein Festeinbau denkbar, wenn kein Interesse daran besteht, den Sender später zu entfernen, beispielsweise, um ihn in einen anderen Gegenstand zu verbauen.[12] Also kann ggf. auch eine dauerhafte Befestigungsmöglichkeit verwendet werden. Diese hat den Vorteil, dass der Sender so verbaut werden kann, dass er nicht ohne Beschädigung des potenziellen Diebesgutes entfernt werden kann, wodurch der Gegenstand als Diebesgut unattraktiver wird.[13] Beim Festeinbau in Fahrzeugen besteht zudem die Möglichkeit, die Sender langfristig mit Strom zu versorgen und so seine Leistungsdauer, ggf. auch seine Leistungsfähigkeit zu erhöhen. Beim Fahrrad

9 Glitza 2014, S. 186-187.

10 Siehe dazu Fährmann/Matzdofr/Höffner in diesem Band, S. 29ff.

11 Zur rechtlichen Berechtigung dazu vgl. Glitza 2014, S. 270; Gola ZD 2012, S. 310; Weisser/Färber MMR 2015, S. 509.

12 Dies wird im Wesentlichen von der Qualität und des Preises des GPS-Senders abhängen.

13 Darauf könnte aus Präventionszwecken hingewiesen werden.

ist z.B. eine Verbindung zum Nabendynamo denkbar.[14] Auch bei anderen mit GPS ausgestatteten Gegenständen gibt es Möglichkeiten einer langfristigen Stromversorgung, etwa mittels Solarelementen.

Der Einbau erfolgt – anders als bei der Observation – bei der Live-Ortung von Diebesgut ohne Zeitdruck, sodass deutlich mehr Möglichkeiten bestehen, beispielsweise hinsichtlich der unauffälligen Verbauung oder in Bezug auf die Steigerung der Leistungsfähigkeit.

Ist ein GPS-Modul in einem gestohlenen Gegenstand fest verbaut, so wird die Detektion bzw. das Aufspüren des GPS-Moduls unwahrscheinlicher. Zumindest solange kein Fernabruf der Daten erfolgt und das Modul nicht sendet, ist ein Aufspüren auch nicht mit einem sogenannten Mobifinder möglich. Zu beachten ist auch, dass die Täter*innen eines einfachen Diebstahls grundsätzlich weniger in Bezug auf Ortungstechnik sensibilisiert sind als Tatverdächtige der schweren Kriminalität, die potentiell regelmäßig observiert werden. So ist damit zu rechnen, dass die Sender zumindest bei einfachen Diebstählen oder bei unprofessionellen Ausführungen im Regelfall nicht entdeckt werden. Auch ist bei einer Festverbauung ein Entfernen oft mit mehr Aufwand verbunden, insbesondere, wenn der Gegenstand dabei beschädigt werden muss, wodurch er an Wert verlieren könnte.[15]

Zur Bearbeitung eines Diebstahls eines getrackten Gegenstands ist von einem deutlich geringeren Personalansatz als bei der Observation auszugehen. Die Ermittlung des Standortes kann durch einen einzelnen Funkwagen mit zwei Polizeikräften erfolgen. Im Optimalfall hat die Besatzung des Funkwagens ein internetfähiges Gerät bei sich, um die Diebstahlsverfolgung selbstständig durchführen zu können, wodurch die Leitstelle entlastet würde. Wenn das Diebesgut aufgefunden wurde, kann es jedoch im Einzelfall notwendig sein, Unterstützung anzufordern, um Tatverdächtige zu stellen.

## 2. Einsatzbereitschaft der GPS-Sender

Bei GPS-Modulen wird bei der Einsatzbereitschaft zwischen dem Kalt-, dem Warm- und dem Heißstart unterschieden. Eine längere Nicht-Nutzung oder -Bewegung des Gegenstandes führt zu einem Kaltstart des GPS-Moduls. Dieser kann bis zu 12,5 Minuten in Anspruch nehmen. Bei einer Standzeit von mehr

14 Ähnlich der Vorteile des Festeinbaus beim Kfz, Glitza 2014, S. 191-193.

15 Insofern könnte ein Aufspüren des Senders an einer nicht zugänglichen Stelle sogar sinnvoll sein, da so einige Diebe sich von dem Diebstahl sogar abhalten lassen. Insofern kann auch ein Hinweis auf eine festverbaute Trackingvorrichtung aus generalpräventiven Gründen sinnvoll zu sein.

als vier Stunden, erfolgt der Warmstart, der lediglich bis zu 45 Sekunden dauert. Der Heißstart erfolgt hingegen in unter 30 Sekunden, dieser ist aber nur bei einer Standzeit von unter vier Stunden möglich. Während der Startzeit werden die Positionsdaten weder gesendet, noch dokumentiert. Belastende als auch entlastende Handlungen der Tatverdächtigen können nur teilweise und bei kürzeren Strecken möglicherweise gar nicht erfasst werden, so dass im Ermittlungsverfahren mit unvollständigen Bildern gearbeitet werden muss.

Um das GPS-Modul sofort nach den ersten Bewegungen des Gegenstandes nutzen zu können, muss vor dem ersten Senden eine Positionsbestimmung erfolgen. Hierdurch wird die Dauer bis zur ersten verwertbaren Positionsberechnung durch das Modul verringert.[16] Dazu müsste ein regelmäßiges Senden stattfinden, was aber gegenläufig zur Akkulaufzeit sein kann, da dies Strom verbraucht. Um Strom zu sparen, bietet sich daher ein Standby-Modus an, in dem kein Signal gesendet wird. Sowohl Warm- als auch Heißstart setzen eine vorherige Positionsbestimmung voraus.[17]

### *2.1 Einsatzbereitschaft der GPS-Sender bei der Observation*

Die Standzeit des observierten Gegenstandes kann nur bedingt beeinflusst werden, etwa wenn der Polizei bekannt ist, dass die observierte Person in diesem Zeitraum den Gegenstand nutzt oder transportiert. Der Kaltstart ist aber oft nicht vermeidbar, da eine längere Standzeit oft nicht verhindert werden kann.

### *2.2 Einsatzbereitschaft der GPS-Sender bei einem Diebstahl*

Beim gestohlenen Gegenstand besteht hingegen keine Möglichkeit der Einflussnahme auf den Diebstahlszeitpunkt, sodass eine Lücke in den Positionsdaten aufgrund eines Kaltstarts wahrscheinlich ist.

Ist die Akkulaufzeit aufgrund einer Energiezufuhr – etwa beim Festeinbau – kein zu berücksichtigender Punkt, kann das GPS-Modul dauerhaft senden und muss nicht in den Standby-Modus übergehen. So könnte auch im Rahmen der Diebstahlsbearbeitung, eine geringe Standzeit vorausgesetzt, häufig ein Warm- oder Heißstart erfolgen. Dies wäre etwa denkbar, wenn die Eigentümer*innen ein Interesse an einer dauerhaften Speicherung ihrer Live-Positionsdaten haben, etwa zur Aufzeichnung von sportlichen Leistungen, oder falls ein besonders wertvoller Gegenstand mit Ortungstechnologie ausgestattet werden soll.

16 Vgl. Glitza 2014, S. 181.
17 Ausführlich dazu Glitza 2014, S. 181-182.

### *2.3 Parallelen bei der Einsatzbereitschaft*

Zur Überbrückung der Lücken bei der Übertragung kann in beiden Konstellationen auf GSM-Positionsdaten zurückgegriffen werden; diese sind zwar ungenauer, dafür aber schneller verfügbar.

Bei der Observation wird das Modul häufig mittels eines Bewegungssensors aktiviert, um eine möglichst lückenlose Überwachung zu ermöglichen und gleichzeitig Strom zu sparen. Beim Diebstahl wäre ein solcher Bewegungssensor auch effizient, allerdings nur dann, wenn sichergestellt ist, dass nur unberechtigte Bewegungen des Gegenstandes den Bewegungssensor aktivieren.

## 3. Qualität der GPS-Tracking-Module

Gemein haben die verwendeten Module sowohl im Rahmen der Observation als auch bei der Suche nach Diebesgut die Grundbestandteile. Die Firmware sowie die Antennen und der Akku müssen in allen GPS-Sendern enthalten sein. Allerdings wird sich die erforderliche Qualität nach dem jeweiligen Gegenstand bemessen oder nach der Art der Observation.

Es gibt verschiedene Ausführungsvarianten der GPS-Module. Die Leistungsparameter der Tracking-Module sind grds. sehr ähnlich. Hochwertige Module verfügen aber über mehr individuelle Konfigurationsmöglichkeiten. Qualitätskriterien für GPS-Module sind zudem die Langzeitstabilität des Gerätesystems, eine lange Akkulaufzeit, flexible Einsatzparameter sowie das Preis-Leistungs-Verhältnis.[18]

Zweck der Positionsdatennutzung bei der Observation ist oft die Erstellung eines möglichst genauen Bewegungsprofils.[19] Soll ein Tatnachweis gelingen, müssen die Daten schließlich möglichst genau sein, da nur so sichere Rückschlüsse auf ein Tatverhalten möglich sind. Bei der Diebstahlsaufklärung besteht an der Beobachtung der betroffenen Person aber meist nur ein untergeordnetes Interesse. Die Überwachung von Diebesgut sollte daher oft kürzer als bei der Observation sein, da sie vielfach dem Auffinden des Gegenstandes dient. Es ist jedoch denkbar, dass z. B. Serien von Diebstählen durch eine Positionsermittlung aufgeklärt werden oder eine Live-Ortung zum Auffinden eines entwendeten Gegenstandes zu einer Observation oder weiteren polizeilichen Maßnahmen führt. Dafür wären möglichst exakte Positionsdaten wünschenswert. Dennoch muss die Sendequalität zum Auffinden von Diebesgut regelmäßig nicht so genau wie bei der Observation sein, da es seltener auf ex-

18 Glitza 2014, S. 196-197.
19 Imping 2018, 70.12 Rn 17.

akte Bewegungsmuster ankommen wird.[20] Es ist ausreichend, dass die Polizei erkennen kann, wo sich der Gegenstand befindet. Dabei wirken sich leichte Abweichungen nicht so gravierend aus, insbesondere, da die Möglichkeit einer Unterstützung durch andere Technologien besteht, z. B. durch Bluetooth.

Sehr leistungsstarke Module - speziell für Observationszwecke - sind sehr kostspielig. Gerade der Wunsch nach einer geringen Gehäuseabmessung bei gleichzeitig hoher Akkulaufzeit führt zu technischen Schwierigkeiten, die sich im Preis niederschlagen.[21] Im besten Falle wäre der GPS-Empfänger, welcher zum Auffinden von möglichem Diebesgut genutzt werden soll, von einer vergleichbaren Qualität, da so die Wahrscheinlichkeit eines Auffindens erhöht wird. Ungenauigkeiten können die Polizeiarbeit erschweren. Allerdings sind die Eigentümer*innen eines Gegenstandes wahrscheinlich nicht gewillt, einen hohen Geldbetrag für einen GPS-Empfänger auszugeben, der außer Verhältnis zum Wert des zu ortenden Gegenstandes steht. Besonders, da zudem monatliche oder einmalige Kosten für den Betrieb des Moduls anfallen können, die ebenfalls bei der Kalkulation zu berücksichtigen sind. Allerdings können Gegenstände auch mit hohen ideellen oder sentimentalen Werten verknüpft sein. Insofern wird an dieser Stelle das Preis-Leistungs-Verhältnis entscheidend sein, wobei die Leistung in Relation zum Preis sich sowohl darauf beziehen kann, wie viel der Gegenstand bei wirtschaftlicher Betrachtungsweise wert, als auch wie hoch das ggf. ideelle Interesse an der Wiedererlangung ist. Daher sind Lösungen und Angebote für Einzelfälle erforderlich.

## 4. Akkulaufzeit von GPS-Sendern

Zur Bestimmung der notwendigen Akkulaufzeit ist entscheidend, was mit der polizeilichen Maßnahme bezweckt wird.

### *4.1 Akkulaufzeit von GPS-Sendern bei der Observation*

Bei der Observation steht die zu observierende Person im Mittelpunkt des polizeilichen Interesses. Der getrackte Gegenstand liefert lediglich Rückschlüsse auf die Person. Der Einsatz von GPS-Trackern hat damit eher eine unterstützende Funktion, etwa, wenn die Polizei nicht nahe an die Observierten herangehen will, damit sie nicht bemerkt wird. Trotzdem müssen die Daten möglichst

20 Diese lassen sich ohnehin effektiver erstellen, wenn weitere Maßnahmen, etwa eine Observation oder eine TKÜ, erfolgen, da die GPS-Daten ohnehin gewisse Ungenauigkeiten aufweisen, siehe dazu Vollmar/Kober/Görlitz S. 19ff. in diesem Band.

21 Glitza 2014, S. 195-196.

genau sein, sodass eine hohe Sendefrequenz erforderlich ist. Sonst können kaum Rückschlüsse auf das Verhalten der observierten Person gezogen werden. Der dabei anfallende Stromverbrauch muss bei der Akkuleistung berücksichtigt werden.

Während des Akkuwechsels besteht bei der Observation ein großes Entdeckungsrisiko, das mit dem Risiko beim Ein- und Ausbau des Senders vergleichbar ist (s.o.). Da dadurch die Ermittlungen gefährdet werden können, sollte ein Akkuwechsel auf wenige Fälle beschränkt werden. Wenn jedoch besonders genaue Daten erforderlich sind, ist dies nur mit einer höheren Sendefrequenz und einem damit zwingend verbundenen höheren Stromverbrauch zu erreichen. Dies bleibt dank der Möglichkeit des Akkuwechsels eine Option.

### *4.2 Akkulaufzeit von GPS-Sendern bei einem Diebstahl*

Bei der Suche nach Diebesgut hat auch das Auffinden des Gegenstandes eine zentrale Bedeutung, insbesondere für die geschädigte Person. Gleichwohl besteht für die Polizei im Rahmen der Strafverfolgung auch ein Interesse an der Person, die im Besitz des Diebesguts ist. Durch die Positionsdatennutzung kann der Diebstahl einer Person, dem*der Täter*in, zugeordnet werden. Zudem können Hehler*innen oder hinter den Dieb*innen stehende Strukturen aufgespürt werden. Daher kann eine hohe Sendefrequenz sinnvoll sein, damit entsprechende Rückschlüsse auf die Besitzer*innen des Gegenstandes möglich sind. Die nachzuweisende Tathandlung ist bei einem gestohlenen Gegenstand bereits erfolgt, weswegen primär der Position des entwendeten Gegenstandes von Interesse ist, um weitere Anhaltspunkte zur Strafverfolgung zu erhalten bzw. den Gegenstand zurückzuholen. Dafür muss die Sendeleistung nicht besonders hoch sein. Die GPS-Positionsermittlung ist aber anders als bei der Observation keine eigenständige Maßnahme, die den Polizeieinsatz eher nur begleitet, sondern sie ist die entscheidende Ermittlungsarbeit. Zwar können die Ermittlungen allein mit einer Live-Ortung des entwendeten Gegenstandes noch nicht als abgeschlossen angesehen werden, dennoch kann die Live-Ortung als eigenständige Maßnahme erfolgen, auf der dann weitere Ermittlungsansätze aufbauen können. Eine möglichst genaue Sendefrequenz ist daher auch hier wünschenswert. Dennoch sind häufig genaue Rückschlüsse auf ein Verhalten nicht notwendig. Oft reicht es aus, den Aufenthaltsort des Gegenstandes zu ermitteln und danach weitere Ermittlungstätigkeiten vorzunehmen. Dies spricht für eine geringere Sendefrequenz und damit auch eine geringere Akkuleistung.

## 5. Fazit

Die Gegenüberstellung hat diverse Unterschiede und Parallelen zwischen der Positionsdatennutzung im Rahmen der Diebstahlssachbearbeitung und der zur Observation aufgezeigt. Daraus wird deutlich, dass Erfahrungswissen aus der Observation auf die Live-Ortung zur Diebstahlsaufklärung übertragen werden kann. Teilweise ist die Zielrichtung jedoch so unterschiedlich, dass sich gänzlich andere technische Anforderungen ergeben.

Hinsichtlich der Qualität des Trackingmoduls wird deutlich, dass bei der Diebstahlsaufklärung insbesondere die Relation von Wert des Gegenstandes und die Kosten für das Trackingmodul eine entscheidende Bedeutung haben. So müssten unterschiedliche Trackingmodule für unterschiedliche Gegenstände angeboten werden. Bei (ideell oder materiell) wertvollen Gegenständen könnte es daher gerechtfertigt sein, auf die hochwertigen Trackingmodule zurückzugreifen, die die Polizei nutzt.

Geringwertige Module sind aber für die Diebstahlsaufklärung nicht zwingend ein unüberwindbares Hindernis, da, anders als bei der Observation, ein Trackingmodul ohne Zeitdruck und sogar festverbaut werden kann. So kann nicht nur ggf. die Signalstärke und Sendefrequenz durch eine Stromzufuhr erhöht werden, sondern die Geräte können auch so verbaut werden, dass sie nicht ohne weiteres aufgefunden werden können. So wäre es möglich, entsprechende Module direkt bei der Produktion zu verbauen, etwa in einem Kfz, in einem Fahrrad (insbesondere in einem E-Bike) oder in einem Mobiltelefon. So wäre es möglich, auf Besonderheiten des Gegenstandes und die Anforderungen bzgl. einer möglichst effektiven Live-Ortung direkt einzugehen und dies in einem Umfang zu tun, der bei der Observation nicht möglich ist. Möglicherweise fallen hierbei die Kosten nicht so stark ins Gewicht, weil ohnehin ein Ortungsmodul verbaut wird, da es aus anderen Gründen erforderlich ist, beispielsweise zur Navigation oder um Bewegungsabläufe festzuhalten (etwa zur Abbildung der eigenen sportlichen Leistung).

Kann ein Festeinbau und damit eine dauerhafte Stromzufuhr nicht sichergestellt werden, erscheint es jedoch sinnvoll, auf die Erkenntnisse über die Bewegungssensorik aus dem Observationseinsatz zurückzugreifen. So könnten die Eigentümer*innen einen Sensor aktivieren, wenn sie einen Gegenstand abgestellt haben, beispielsweise ein Fahrrad, und diesen bei der bestimmungsgemäßen Nutzung wieder deaktivieren. Auch auf die Erkenntnisse hinsichtlich der Akkulaufzeit kann auf die Erfahrungen aus der Observation zurückgegriffen werden, da dort auch Module mit einer längeren Akkulaufzeit benötigt werden. Weil die Sendefrequenz zur Live-Ortung von Diebesgut in der Regel nicht so hoch wie bei der Observation sein muss, wäre die Akkulaufzeit sogar noch höher.

Zudem ist deutlich geworden, dass zur Unterstützung der Live-Ortung auch ein GSM-Modul und Bluetooth-Technologie enthalten sein sollte. Dies scheint für die Fälle, in denen ein GPS-Modul nicht sendet eine sinnvolle Unterstützung zu sein.

## Literaturverzeichnis

*Glitza, Klaus-Henning* (2014) Observation. Praxisleitfaden für private und behördliche Ermittlungen. 4. Aufl. Stuttgart: Boorberg.

*Gola* (2012) Die Ortung externer Beschäftigter - Abwägung zwischen Überwachungsinteresse und schutzwürdigen Arbeitnehmerinteressen, ZD. 2. Jg., Nr. 7, S. 308–311.

*Imping* (2018) Compliance – Überwachung – Investigation. In: Kilian, W. (Hg.): Computerrechts-Handbuch. Computertechnologie in der Rechts- und Wirtschaftspraxis. 34. Aufl. München: Beck.

*Singelnstein* (2012) Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen. Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ, 32. Jg., Nr. 11, S. 593–606.

*Vahle* (2003) Rechtliche Aspekte der Gefahrenabwehr in Entführungsfällen, NVwZ, 22. Jg., Nr. 5, S. 513–521.

*Weisser/Färber* (2015) Rechtliche Rahmenbedingungen bei Connected Car. Überblick über die Rechtsprobleme der automobilen Zukunft, MMR, 18. Jg., Nr. 8, S. 506–512.

*Christian Matzdorf*[1]

# Fahrraddiebstahl – ein Delikt mit niedrigen Aufklärungsquoten

Der nachfolgende Text befasst sich mit der Position des Fahrraddiebstahls als Kriminalitätsphänomen im System der Kriminalitätskontrolle und als Gegenstand der kriminalistischen Prioritätensetzung. Dies geschieht vor dem Hintergrund der folgenden Fragen:

Warum wird Fahrraddiebstahl auch heute noch als ein „nachrangiges" Delikt im Rahmen der Kriminalitätskontrolle betrachtet?
Woraus resultieren die anhaltend niedrigen Aufklärungsquoten beim Fahrraddiebstahl?
Warum werden diese niedrigen Quoten augenscheinlich als gegeben akzeptiert?
Kann Fahrraddiebstahl wirkungsvoll bekämpft werden?
Welche Herausforderungen bestehen, um eine nachhaltige Bekämpfung zu realisieren?

## 1. Einleitung

Der Besitz von Fahrrädern ist ubiquitär, unabhängig von ländlichen/urbanen Räumen, Sozialstrukturen oder geografischen Bedingungen. Lediglich die Verbreitungsdichte und die faktische Verfügbarkeit für Dieb*innen variiert.

Was das Fahrrad als Stehlobjekt interessant macht, ist neben der Verbreitung die gute Eignung als Tatobjekt:

Es handelt sich bei Fahrrädern um relativ wertvolle (oder zumindest mit einem kalkulierbaren Mindesterlös weiter zu veräußernde) Objekte, die überwiegend mit verhältnismäßig einfach zu überwindenden Sicherungseinrichtungen versehen sind. Die Fahrräder können mit einem geringen Entdeckungsrisiko (im Regelfall auch durch eine „nicht vorhandene" Spurenlage mit verursacht, da grundsätzlich weder Diebesgut noch Tatmittel oder Reste der Sicherungseinrichtungen am Ort verbleiben) entwendet werden. Das Pönalisierungsrisiko im Entdeckungsfall ist für Täter*innen fast vollkommen zu vernachlässigen.

1 Prof. Christian Matzdorf hat in dem Projekt kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

Diese Konstellation (hohe Verfügbarkeit des Stehlguts in Verbindung mit einem geringen Entdeckungsrisiko bzw. einer marginalen Strafandrohung im Entdeckungsfall) bedingt zwei für das Kriminalitätsphänomen relevante Teilphänomene:

Qualifizierte Diebstähle hochwertiger Fahrräder durch fachkundige Täter*innen auf Bestellung oder zum Angebot in einschlägigen Internetforen (geringe Fallzahlen – hohe Schadensumme im Einzelfall) einerseits und Fahrraddiebstahl als Massendelikt häufig bei „günstiger Gelegenheit" durch nicht bzw. gering spezialisierte Täter*innen (hohe Fallzahlen bei geringer/mittlerer Schadenshöhe im Einzelfall, aber hohes Gesamtschadensvolumen) andererseits.

Die Hintergründe der Tatsache, dass trotz der bekannten Dimension des Kriminalitätsphänomens Fahrraddiebstahl wenig zielführende Aktivitäten der Strafermittlungsbehörden zur Eindämmung bzw. Kriminalitätskontrolle getroffen werden, werden im Folgenden skizziert.

## 2. Allgemeine Einflussvariablen auf das Phänomen Fahrraddiebstahl

Niedrige Aufklärungsquoten beim Fahrraddiebstahl sind kein kurzzeitiges, temporäres Phänomen, sondern seit Jahrzenten ein Faktor, der sich als Bestandteil der Kriminalitätsstatistiken etabliert hat. Das ist bemerkenswert, da diese Tatsache bisher zu keiner nachhaltigen Resonanz bei Strafermittlungsbehörden oder in der öffentlichen Diskussion (Fachforen wie beispielsweise des ADFC[2] ausgenommen) führte.

Anders als bei „neuartigen" Kriminalitätsphänomenen (beispielsweise einiger Erscheinungsformen der unter Zuhilfenahme des Internets begangenen Kriminalität) scheidet hier als Erklärungsansatz der Umstand aus, dass die Strafverfolgungsbehörden sich erst näher mit dem Kriminalitätsphänomen befassen müssen, um strategische Festlegungen zu treffen und geeignete taktische Ausformungen der Ermittlungsarbeit zu finden.

Fahrraddiebstahl gehört auch nicht zu dem Kreis der typischen Kontrolldelikte, bei denen sich lediglich die Aktivitäten der Ermittlungsbehörden in der Polizeilichen Kriminalstatistik (PKS) abbilden. Die daraus resultierenden Schwankungen sind regelmäßig Ursache für Fehlinterpretationen, die häufig auch politisch genutzt werden, um „Erfolge" oder „Misserfolge" zu belegen. Auf die dauerhaft niedrigen Aufklärungsquoten im Deliktsfeld Fahrraddiebstahl trifft dies allerdings ebenfalls nicht zu.

2 Allgemeiner Deutscher Fahrrad Club.

Auch veränderte Erfassungsmodalitäten der PKS wie beispielsweise bei der Umstellung der Erfassung von Mehrfachtaten als Einzelfälle bei einem grundlegenden Tatentschluss (wie beispielsweise im Zusammenhang mit dem Betrug mittels gestohlener EC- und Kreditkarten) spielen beim Phänomen Fahrraddiebstahl keine Rolle.

Vielmehr handelt es sich bei den signifikant niedrigen Quoten der Aufklärung von Fahrraddiebstahlstaten um ein anhaltendendes, seit Jahrzehnten statisches Phänomen. Lediglich die saisonbedingten Unterschiede zwischen warmer und kalter Jahreszeit (bei einer nachvollziehbaren Korrelation von Fahrradnutzung im öffentlichen Raum und Diebstahlstaten sowie der häufigeren Identifizierung von Täter*innen) drücken sich in den Monatsstatistiken der strategischen Auswertung[3] aus. Diese fallen jedoch in dem jährlichen Kriminalitätsstatistikzyklus nicht auf.

Daran hat auch eine differenziertere Erfassung bzw. getrennte Darstellung in der PKS („einfacher Fahrraddiebstahl“ und „schwerer Fahrraddiebstahl“) nichts geändert.

Vor diesem Hintergrund wirkt die augenscheinliche Akzeptanz der fehlenden Ermittlungserfolge über einen langen Zeitraum ebenso befremdlich, wie der Umstand, dass die Ursachen dafür bisher kaum näher wissenschaftlich betrachtet wurden.

Tatsächlich sind eine Vielzahl von Erklärungsansätzen denkbar, die jedoch in der Qualität ihrer Auswirkungen auf das in Rede stehende Phänomen nur eingeschätzt, aber tatsächlich nicht präzise beschrieben werden können.

Zur groben Orientierung können mögliche Erklärungsansätze unter folgende Überschriften eingeordnet werden:

1. Objektbezogene Aspekte
2. Personenbezogene Aspekte
3. Rahmenbedingungen
4. Tatgelegenheitsstrukturen
5. Straftatenverfolgung

Allerdings verbietet sich eine getrennte Betrachtung angesichts der Tatsache, dass die einzelnen Punkte sich gegenseitig in einer Art netzkausaler Struktur beeinflussen. So korreliert beispielsweise die Verfügbarkeit des Diebesgutes

3 Die strategische Auswertung unterstützt Führungskräfte in Ermittlungsbehörden bei der Feststellung von Entwicklungstrends und dient als Entscheidungsgrundlage für die Steuerung von Personal und weiteren Ressourcen. Sie ist von der operativen Auswertung abzugrenzen, die dem Zweck der Erstellung eines kurzfristigen Lagebildes dient, beispielsweise um zeitnah auf bestimmte Kriminalitätsphänomene angemessen zu reagieren, indem entsprechende Einsätze konzipiert werden.

und die Eignung als Tatobjekt, die Aufmerksamkeit potenzieller Straftäter*innen und das Entdeckungsrisiko, welches wiederum abhängig vom Verfolgungsdruck ist.

Das Objekt Fahrrad ist (von hochwertigen Ausnahmen abgesehen) ein Massenprodukt, das sich in einem Großteil der privaten Haushalte und insbesondere fast überall im öffentlichen Raum findet. Durch den hohen Anteil an Fahrrädern aus dem preiswerten oder mittleren Preissegment steigt die Verfügbarkeit für jedermann und eine aufwändige Sicherung oder ein allgemein diebstahlspräventiver Umgang mit dem Objekt „lohnt" sich nicht. Dies könnte die hohe Anzahl an „einfachen Diebstählen" erklären, bei denen keine oder kaum relevante Sicherungseinrichtungen genutzt wurden.

Auf der anderen Seite sind insbesondere Fahrräder im öffentlichen Raum dennoch als Diebstahlsobjekt für Täter*innen interessant, da sie (sofern es sich um preiswerte bis mittelpreisige Modelle handelt) für einen niedrigen aber relativ konstanten Wert weiterverkauft werden können und somit als Hehlerware einen „festen Marktwert" haben. Werden Fahrräder entwendet, erfolgt häufig keine Strafanzeige durch die Betroffenen. Dafür gibt es verschiedene Erklärungsansätze:

Der Wert des entwendeten Rades wird als nicht relevant angesehen und die Wiederbeschaffung ist ebenfalls preiswert. Eine Abwägung von Aufwand und Nutzen einer Information der Polizei fällt zu Ungunsten der Anzeigenerstattung aus. Dabei spielt auch die Einschätzung der Geschädigten hinsichtlich eines zu erwartenden Ermittlungserfolges (Wiederbeschaffung inbegriffen) der Polizei eine Rolle, die auch als Indikator für das Vertrauen in eine funktionierende Strafverfolgung mit erfolgreicher Ermittlungstätigkeit angesehen werden kann.

So ist auf der Seite der Geschädigten häufig ein Desinteresse an der Strafverfolgung anzunehmen. Dies auch vor dem Hintergrund, dass sich in den letzten zehn Jahren Veränderungen in den Bedingungen der Versicherer ergeben haben. Während ältere Verträge noch Konditionen vorsehen, die eine Erstattung des Wertes des entwendeten Rades im allgemeinen Rahmen der Hausratversicherung vorsehen, wurde in den späteren Verträgen die Erstattungssumme pauschal reduziert festgelegt oder an einen geringen Prozentsatz der Gesamtversicherungssumme gebunden. Neuere Verträge schließen eine Erstattung im Diebstahlsfall entweder ganz aus bzw. vom Versicherer wird eine gesonderte Fahrradversicherung angeboten oder es wird an spezialisierte Anbieter verwiesen.

## 3. Organisatorische Perspektive der Kriminalitätskontrolle

Auch unter der Prämisse des Legalitätsprinzips (und damit dem theoretischen Ausschluss betriebswirtschaftlicher Grundsätze in der Strafverfolgung) ist es als gegeben anzusehen, dass eine effektive Kriminalitätskontrolle nur im Rahmen von Aufgabenpriorisierungen möglich ist. Auf den Priorisierungsprozess, der häufig mit behördlichen Zielsetzungsverfahren korreliert, wirken eine Vielzahl von Einflussvariablen ein, die zwar genannt aber nicht quantifiziert werden können. Sie können mit folgenden Überschriften versehen werden:

Interne Determinanten:

- Personelle Ressourcen
- Finanzielle Ressourcen
- Räumliche Ressourcen
- Technische Ressourcen

Externe Determinanten:

- Veränderte Kriminalitäts-Lagebilder und veränderte/neue Tatgelegenheitsstrukturen
- Erwartungen und Tendenzen in der Öffentlichkeit/öffentliche Wahrnehmung

Politische Determinanten:

- Strategische Vorgaben (beispielsweise als Ergebnis von Koalitionsverhandlungen und politischen Willenserklärungen)
- Konkrete Einwirkungen in Form von Vorgaben seitens der Hauptverwaltung

Da sich diese Variablen in einem Wirkgeflecht gegenseitig beeinflussen und zu schnell veränderten Lagen führen, stellt der Priorisierungsprozess nicht immer das (dem Idealbild entsprechende) Ergebnis einer ausgewogenen Betrachtung und strategischen Planung dar, sondern ist häufig taktisch und intuitiv-reaktiv basiert.

Beispielhaft wird dies am Kriminalitätsphänomen Wohnraumeinbruch, welches über mehr als ein Jahrzehnt auf Länder- und Bundesebene bei den Strafverfolgungsbehörden trotz dramatischer Zahlen (und in Vernachlässigung des erheblichen Viktimisierungspotenzials und der kriminalistischen Bedeutung der Organisationsstrukturen der Täter*innen) als nachrangig betrachtet und erst auf politischen Druck hin priorisiert wurde. Ein weiteres Beispiel sind öffentlichkeitswirksame Kriminalitätsphänomene wie der sexuelle Missbrauch von Kindern/pädopornografisches Material, wo einzelne Fälle für einen erheblichen öffentlichen Druck und damit einhergehend zu entsprechenden Priorisie-

rungen führten, die die Aufbauorganisationen von Strafermittlungsbehörden beeinflussen. Das wohl deutlichste Beispiel stellt das Phänomen „islamistischer Terrorismus“ dar, welches zu erheblichen Veränderungen der Allgemeinen Aufbauorganisation (AAO) und der Besonderen Aufbauorganisationen (BAO) von polizeilichen Ermittlungsbehörden mit gravierenden Auswirkungen auf andere Bereiche der Kriminalitätskontrolle führte.

Das Kriminalitätsphänomen Fahrraddiebstahl hat in den vergangenen 30 Jahren zu keiner Zeit eine relevante Rolle bei Priorisierungs- und Entscheidungsprozessen gespielt.[4] Dies spiegelte sich bspw. in Berlin in der Bezeichnung als Bagatelldelikt bzw. später als Delikt der „einfachen“ bzw. „leichten“ Kriminalität wider, deren Bearbeitung möglichst „ressourcenneutral“ erfolgen soll.

Behördenorganisatorisch hatte dies im System der dreistufigen Kriminalitätskontrolle[5] der Polizei Berlin eine Anbindung der polizeilichen Bearbeitungszuständigkeit bei den jeweils untersten Bearbeitungsinstanzen zur Folge. Diese Dienststellen verfügen im Regelfall auch nur über (aus kriminalistischer Sicht) fachlich geringer qualifiziertes Personal und deutlich eingeschränkte personelle und materielle Ressourcen im Vergleich zu Organisationseinheiten mit spezialisierten Zuständigkeiten. Dies erklärt, warum auch heute noch einfache Fahrraddiebstahlsdelikte (ohne Täteranhalte, Hinweise auf Tatserienzusammenhänge oder einen Hehlereiverdacht) im Rahmen der sog. „einfachen“ (oder auch verharmlosend „schlank“ genannten) Bearbeitung als sogenannte „Stempelvorgänge“ betrachtet werden, d.h. sie werden mit dem Stempel „keine Ermittlungsanhalte“ versehen ohne weitere Ermittlungen der Amtsanwaltschaft zur Einstellung übersandt. Eine fundierte Strafverfolgung durch (kriminal-)polizeiliche Ermittlungsarbeit findet faktisch nicht statt.

Neben der organisatorischen Einstufung (und eben auch verstärkt durch diese) muss im Rahmen einer ganzheitlichen Betrachtung auch eine psychologische Komponente betrachtet werden:

Mit der Bearbeitung von Fahrraddiebstahlsvorgängen oder gar mit einer konzeptionellen Bekämpfung des Phänomens waren in Berlin keine positiven Effekte für eine innerbehördliche Anerkennung oder gar positive Karriereentwicklung verbunden. Ganz im Gegenteil: Es war in der Vergangenheit nicht

4 Diese Feststellung ist eine erfahrungsbasierte Aussage des Autors angesichts über dreißigjähriger praktischer Erfahrungen in der Kriminalitätskontrolle.

5 In der Landespolizei Berlin liegt die Zuständigkeit für schwere Kriminalität und ausgesuchte Kriminalitätsphänomene beim LKA Berlin; für die sog. mittlere Kriminalität die Referate K (Kriminalitätsbekämpfung) der örtlich zuständigen Polizeidirektionen und für die sog. einfache Kriminalität die Abschnittskommissariate der jeweils örtlich zuständigen Polizeiabschnitte innerhalb einer Polizeidirektion (unter Fachaufsicht der genannten Kriminalreferatsleitungen).

unüblich, missliebiges, weniger qualifiziertes oder schlecht beurteiltes bzw. auch durch disziplinarische oder strafrechtliche Ermittlungen belastetes Personal in Diebstahlskommissariaten zusammenzufassen (was auch Führungskräfte betreffen konnte). Eine Befassung mit dem Thema Fahrraddiebstahl konnte also seinerzeit zu einer innerbehördlichen negativen Stigmatisierung beitragen oder diese verstärken.

Auch die polizeiliche Präventionsarbeit war durch diesen Effekt gekennzeichnet: Während polizeiliche Kriminalprävention relevant erachteter Themen organisatorisch beim Landeskriminalamt verortet ist, beschränkt sich häufig auch heute noch die Prävention des Fahrraddiebstahls auf „Fahrrad-Codieraktionen" oder mündliche Aufklärungsarbeit bezüglich der Sicherung von Fahrrädern an Brennpunkten, durchgeführt durch schutzpolizeiliche Kräfte. Diese Aktivitäten sind anerkannt als öffentlichkeitswirksam und gut geeignet, einen Dialog zwischen der Bevölkerung und der Polizei zu fördern. Wissenschaftlich begründet oder zumindest in ihren Auswirkungen auf das Kriminalitätslagebild Fahrraddiebstahl evaluiert sind sie jedoch nicht.

Es ist nachvollziehbar, dass diese Rahmenbedingungen nicht zu einer engagierten und zielorientierten Kontrolle des Kriminalitätsphänomens Fahrraddiebstahl führten und führen. Nur bedingt nachvollziehbar ist allerdings, dass ein verändertes Bewusstsein für urbane Mobilität, der ökologischen Nutzen des Fahrrades und die positiven Auswirkungen der mit der Radnutzung verbundenen körperlichen Aktivität,[6] bisher keinen Niederschlag in Form einer veränderten strafermittlungsbehördlichen Priorisierung gefunden haben. Die Aufgabenfülle und die nach wie vor angespannte personelle und finanzielle Situation von Staatsanwaltschaft und Polizei könnten Erklärungen dafür sein, dass nach wie vor eine Vernachlässigung dieses Bereiches der Kriminalitätsbekämpfung besteht. Tatsächlich sollten diese Herausforderungen nicht zu einer Fortsetzung der nachrangigen Priorisierung des Kriminalitätsphänomens führen.

## 4. Fazit

Im Sinne der eingangs aufgeworfenen Fragen ist festzustellen, dass trotz deutlich veränderter gesellschaftlicher Rahmenbedingungen (u.a. gesellschaftliche Aufwertung des Rades/der Aktivität Radfahren unter der Prämisse eines ökologisch korrekten Fortbewegungsmittels mit entsprechender Statusaufwertung; politische Wahrnehmung und öffentliche Thematisierung des Fahrrades mit

6 Aspekte, die im politischen Raum beispielsweise durch Planungen zur gezielten Förderung des Radfahrverkehrs als Ergebnis von Koalitionsvereinbarungen in Berlin ihren Niederschlag fanden.

dem Ergebnis einer – zumindest auf dem Papier – vorrangigen Förderung) bisher kein nachhaltiger Perspektivwechsel seitens der Strafverfolgungsbehörden wahrzunehmen ist. Dies begründet sich aus dem Nachwirken einer überkommenen Einschätzung des Fahrraddiebstahls als nachrangiges Delikt und der entsprechenden Verortung im dreistufigen System der Kriminalitätskontrolle. Begünstigt wird diese Tatsache durch die objektiv angespannte Situation bei Polizei und Staatsanwaltschaft angesichts hoher Anforderungen und daran nicht angepasster Ressourcenausstattung.

Vor diesem Hintergrund wurde bei behördlichen Priorisierungsverfahren die Strategie der vergangenen Jahrzehnte fortgeschrieben, was sich nicht nur auf die strategische Zielsetzung und organisatorische Zuständigkeitsverortung, sondern auch auf die taktische Ausformung von Personaleinsatz (sowohl in quantitativer wie qualitativer Hinsicht) und Sachmittelausstattung bezog.

Zudem sind weitere Determinanten zu betrachten: die breite Verfügbarkeit von Fahrrädern, die wenig ausgeprägten Bemühungen um Sicherung des potentiellen Stehlguts seitens der Nutzenden und die damit verbundene Auswirkung auf Tatgelegenheitsstrukturen. Der geringe Aufwand für Ersatz bei Diebstahl und veränderte Versicherungsbedingungen (was einen geringen Anreiz für eine Anzeigenerstattung bei der Polizei bedingt) sowie letztlich der insbesondere im Bereich der sogenannten Bagatelldelikte vermutete Vertrauensverlust in der Bevölkerung hinsichtlich einer effektiven Strafverfolgung (oder gar Rückgewinnung). Das daraus resultierende ausgeprägte Dunkelfeld trägt ebenfalls zu einer Negativentwicklung bei, da so das Lagebild Fahrraddiebstahl eher spekulativ als fundiert ist und grundlegende Informationen für eine gezielte Kriminalitätskontrolle des Deliktfeldes fehlen.

Die scheinbare „Akzeptanz“ dieser Bedingungen resultiert möglicherweise aus einem Gewohnheitsverhalten, das über Jahrzehnte gewachsen ist und sich etabliert hat.

Dabei könnte eine ausgeprägte öffentliche Diskussion auf der Basis der formulierten und teilweise in Umsetzung befindlichen politischen Willenserklärungen vor dem Hintergrund der sich derzeit verändernden gesellschaftlichen Rahmenbedingungen eine völlig andere Situation schaffen:

Öffentlicher Druck auf Strafverfolgungsbehörden, das Phänomen Fahrraddiebstahl angemessen zu behandeln einerseits und andererseits die Betonung der Verantwortung von Nutzenden bezüglich der Themen „Sicherung des Fahrrades“, „Registrierung von ermittlungsgeeigneten Daten zum Rad“ und im Diebstahlsfall „Anzeigeverhalten“ (Vergrößerung des statistischen Hellfeldes) wären geeignet, grundlegende Veränderungen hervorzubringen. In diesem Zusammenhang ist auch das Themenfeld „Fahrradtrackingsysteme“ zu betrachten, da deren Entwicklung, Markteinführung und Verfügbarkeit für breitere Käufer-

schichten, Auswirkungen auf das Entdeckungsrisiko und die Strafverfolgung haben und damit eine generalpräventive Wirkung erzielen könnte.

Dieser Effekt wäre insbesondere dann zu erwarten, wenn die Polizeibehörden technisch in die Lage versetzt würden, die Vorteile der Trackingsysteme für die Strafverfolgung und Wiedergewinnung angemessen (d.h. ohne Systembrüche) zu nutzen. Erfolge auf diesem Gebiet würden nicht nur eine Außenwirkung entfalten, sondern auch innerbehördlich Signale setzen, die zu einer veränderten Wahrnehmung der Thematik und damit zum Einsatz von qualifiziertem Personal in geeigneten Organisationsformen (beispielsweise spezielle und nicht nur temporär eingerichtete Ermittlungseinheiten mit Auswertungs-, Sachbearbeitungs- und operativen Komponenten) führen könnten.

*Jan Fährmann[1]/Annika Höfner[2]/Christian Matzdorf[3]*

# Wie und von wem werden Fahrräder gestohlen? Kriminalistische und kriminologische Erkenntnisse

## 1. Einleitung

Der Diebstahl von Fahrrädern ist ein weit verbreitetes Phänomen, das als Massendelikt eingestuft wird.[4] Die Aufklärungsquoten sind gering[5] und das Verhältnis von Hell- zu Dunkelfeld unbestimmt. Daher gibt es auch wenige Erkenntnisse dazu, wer für den Diebstahl der Fahrräder verantwortlich ist und wie die Täter*innen vorgehen. Das Phänomen wurde bisher nur im geringen Umfang wissenschaftlich untersucht, sodass ein erheblicher Forschungsbedarf besteht. Erkenntnisse aus der Praxis dringen selten nach außen. In diesem Beitrag werden Erkenntnisse über Abläufe sowie Täter*innen von Fahrraddiebstählen aus einer kriminalistischen als auch kriminologischen Perspektive betrachtet und Thesen bezüglich Täter*innen bzw. Tätergruppierungen, die Fahrraddiebstähle begehen, aufgestellt.

Zur Phänomenologie von Fahrraddiebstählen gibt es zahlreiche Fragen: Handelt es sich dabei in erster Linie um gewerbs- und/oder bandenmäßige Diebstähle, die aus organisierten Strukturen heraus erfolgen? Sind überwiegend einzelne Personen für die Diebstähle verantwortlich? In welchem Umfang und wo sind Fahrraddiebstähle verbreitet? Von welchen Faktoren wird die Verbreitung beeinflusst? Zur Beantwortung dieser Fragen werden unterschiedliche Erkenntnisquellen ausgewertet. Zunächst erfolgt eine Analyse der polizeilichen Kriminalstatistik (PKS), wobei zu berücksichtigen ist, dass auf ihrer Grundlage nur begrenzte Aussagen möglich sind. Anschließend werden kriminalistische Erkenntnisse aus der Praxis dargestellt. Dabei wird in erster Linie ein deskrip-

---

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

2 Annika Höffner war zum Zeitpunkt des Projektes FindMyBike im LKA Brandenburg beschäftigt und stand im Austausch mit dem Projektteam.

3 Prof. Christian Matzdorf hat in dem Projekt FindMyBike kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

4 Jitschin 2002, S. 261; vgl. Bartenschlager/Buchmin/Dörrer et al. 2020; Church/Birkel/Leitgöb-Guzy, Die Polizei 2020, S. 44-45; S. 296.

5 Zu diesem Phänomen und den Ursachen vgl. Matzdorf, in diesem Band, S. 69ff.

tiver Ansatz verfolgt. In einem weiteren Schritt werden die gewonnenen Erkenntnisse zusammengeführt.

## 2. Betrachtungen zur Polizeilichen Kriminalstatistik (PKS)

### *2.1 Fahrraddiebstahl in der PKS am Beispiel der Stadt Hamburg*

Die in der Kriminalitätsstatistik enthaltenen Daten zum Thema Fahrraddiebstahl lassen mehrere Interpretationsmöglichkeiten zu. Das soll an dieser Stelle exemplarisch für die Stadt Hamburg gezeigt werden. Die Hamburger Polizei hat sich intensiv mit dem Thema auseinandergesetzt und daraus bereits Folgerungen für ihre Ablauforganisation gezogen.

Eine Auswertung der Hamburger PKS 2020 durch die Hamburger Polizei ergab folgende Erkenntnisse:[6]

Bekanntgewordene Täter*innen von Fahrraddiebstählen waren vorwiegend Erwachsene (59,9%). Jugendliche (21,3%) sowie Heranwachsende (12,3%) waren weniger vertreten, Kinder (6,4%) nur zu einem sehr geringen Prozentsatz. 92% der Delikte wurden von männlichen Tätern und 68% der Delikte wurden von deutschen Staatsangehörigen begangen. Täter*innen aus dem Ausland hatten vorwiegend die rumänische, polnische, syrische und türkische Staatsangehörigkeit (in dieser Reihenfolge). Kriminalpolizeilich aufgefallen waren bereits 73,6% der Täter*innen. Die Polizei Hamburg nahm 2019 eine genauere Auswertung von Fahrraddiebstählen vor und kam zu folgenden Ergebnissen: Eine Abhängigkeit von „harten Drogen“[7] bestand bei 8% der Täter*innen. Bei 40% der Taten handelten die Täter*innen nicht allein. In Hamburg lebten 67% der Täter*innen (davon besaßen 61% die deutsche Staatsbürgerschaft); 33% der Täter*innen lebten außerhalb von Hamburg (davon besaßen 28% die deutsche Staatsbürgerschaft).

Daraus können folgende Schlussfolgerungen gezogen werden: Beschaffungskriminalität zur Finanzierung des Drogenkonsums scheint beim Fahrraddiebstahl eine untergeordnete Rolle zu spielen, wobei nicht ausgeschlossen werden kann, dass Delikte zur Finanzierung von Cannabis- oder Alkoholkonsum erfolgten, was nicht als Beschaffungskriminalität gewertet wurde.

---

6 Diese wurden den Autor*innen im Rahmen eines Experteninterviews zur Verfügung gestellt.

7 In der PKS werden harte Drogen als Stoffe definiert, die in den Anlagen I-III BtMG enthalten sind, wobei Cannabisprodukte, Psilocybin und „ausgenommene Zubereitungen“ nicht umfasst sind. Diese Einordnung ist kritisch zu bewerten, da die gesundheitlichen Auswirkungen von psychoaktiven Substanzen in erster Linie von der Art und Weise des Konsums abhängen. Dieser Aspekt wird in der PKS aber ausdrücklich nicht berücksichtigt.

Aus dem Umstand, dass 2019 40% der Täter*innen nicht alleine handelten, folgt, dass der Diebstahl oft nach vorheriger Absprache mit zumindest einer anderen Person zustande kommt (spontanes, gemeinsames Vorgehen erscheint eher unwahrscheinlich). Insofern scheint bei den Diebstählen häufig ein planmäßiges Vorgehen stattzufinden. Dies spricht auch dafür, dass ein Teil der Diebstähle gewerbs- oder bandenmäßigen Strukturen zuzuordnen ist, da diese einen höheren Organisationsgrad voraussetzen. Darauf deuten auch die geringen Aufklärungsraten hin, die zudem entsprechende Diebstähle lukrativ machen. Zudem spricht die hohe Zahl der Fahrraddiebstähle für gewerbsmäßige und bandenmäßige Diebstähle, da Einzeltäter*innen kaum für entsprechend hohe Fallzahlen verantwortlich sein können. Entwendungen zum Eigengebrauch müssten vor diesem Hintergrund allerdings gesondert betrachtet werden.

Darüber hinaus scheinen die Diebstähle teilweise einen Bezug zum Ausland aufzuweisen. Dass ein Teil der Täter*innen nicht die deutsche Staatsbürgerschaft besitzt, besagt für sich allein noch nicht viel, da dies nicht zwingend auch für die Tat einen Auslandsbezug bedeuten muss. Betrachtet man jedoch den Umstand, dass 33% der Täter*innen außerhalb von Hamburg lebten und davon nur ein untergeordneter Teil die deutsche Staatsbürgerschaft besaß, spricht dies für einen gewissen Anteil an im Ausland lebenden Personen. Insofern kann vermutet werden, dass in Hamburg international operierende Täter*innengruppierungen agieren und Fahrräder ins Ausland verbringen. Entsprechende Tätergruppierungen könnten zum Diebstahl von Fahrrädern nach Deutschland kommen, um diese anschließend ins Ausland zu transportieren.[8] Dabei muss allerdings auch beachtet werden, dass die Personen genauso gut im Hamburger Umland leben können. Auch spricht eine fehlende deutsche Staatsangehörigkeit nicht zwingend dafür, dass die betreffende Person nicht in Deutschland lebt. Insofern deuten allenfalls Indizien auf international operierende Gruppierungen hin. Aus der PKS allein, sprich ohne weitere Ermittlungsergebnisse, kann diese Annahme deshalb nicht verifiziert werden.

Letztlich lässt sich aus der PKS keine trennscharfe Abgrenzung zwischen Einzeltäter*innen sowie kriminell agierenden Gruppen vornehmen. Allerdings deuten die Zahlen darauf hin, dass zumindest für einen Teil der Delikte Täter*innengruppierungen verantwortlich sind.

8 Dafür sprechen Erkenntnisse aus anderen Ermittlungsverfahren, die sich beispielsweise auf eine in Deutschland operierende polnische Tätergruppierung oder auf große Handelsplätze für gestohlene Fahrräder beispielsweise in Vilnus und Kaunas beziehen. Vor diesem Hintergrund sind Analogien zur internationalen Kraftfahrzeugdiebstahlskriminalität zu ziehen. Diese ist jedoch, im Gegensatz zum Fahrraddiebstahl, deutlich besser durch Erfahrungswerte im Rahmen von Ermittlungstätigkeit und im Rahmen von Forschung ausgeleuchtet.

### 2.2 Kritische Betrachtung der PKS

Die PKS bildet nur das Hellfeld ab, d.h. die von der Polizei registrierten Straftaten. Damit gibt sie in erster Linie die Arbeitsweise der Polizei bzw. das wieder, was die Polizei als Kriminalität einstuft.[9] Das muss allerdings nicht mit der tatsächlich vorhandenen Kriminalität übereinstimmen.[10] Wird beispielsweise bei der polizeilichen Arbeit ein Schwerpunkt auf die Ermittlung von Diebstählen gelegt, steigt damit regelmäßig die Zahl der in diesen Bereichen erfassten Fälle an (sog. Kontrolldelikte). Dieser Effekt ist besonders im Zusammenhang mit Rauschgiftkriminalität relevant. Parallel dazu können die Fallzahlen der im Gegenzug weniger beachteten Delikte abnehmen, weil dort die polizeiliche Kontrolldichte sinkt.[11] Darüber hinaus wird die PKS sehr stark vom Anzeigeverhalten der Bevölkerung beeinflusst, da die Polizei zumeist Kenntnis von Straftaten durch Bürger*innen erhält.[12] Von der Bevölkerung werden zudem nur ein Teil der tatsächlich stattgefunden Straftaten wahrgenommen und als Kriminalität bewertet. Demzufolge wird nicht alles, was als Kriminalität wahrgenommen wird, auch zur Anzeige gebracht und dann auch mit entsprechender Ermittlungstiefe bearbeitet.[13] Auch die Akzeptanz bestimmter Formen von Kriminalität, die Annahme einer Opferrolle sowie demografische Aspekte können das Anzeigeverhalten beeinflussen. Alle diese Faktoren beeinflussen die PKS. Dies ist bei ihrer Interpretation zu berücksichtigen.[14] Zudem sollte das Hellfeld immer in Relation zum Dunkelfeld betrachtet werden, was Gegenstand der kriminologischen Forschung sein sollte.[15] Jedoch sind die empirischen Erkenntnisse zum Fahrraddiebstahl beschränkt.

Das spezifische Anzeigeverhalten für einzelne Deliktgruppen wird insbesondere auch davon beeinflusst, welche Folgen eine Anzeige für die Opfer der Straftaten hat und was sie sich davon versprechen. Einerseits können sie die Erwartung haben, dass nach ihrer Anzeige die Straftat aufgeklärt wird. Ebenso gut kann es auch sein, dass sie kein (hohes) Aufklärungsinteresse haben, sondern für sie der Ersatz des materiellen Schadens im Vordergrund steht. Dies kann insbesondere der Fall sein, wenn ein gestohlener Gegenstand versichert ist.[16] Insofern wird das Anzeigeverhalten auch davon abhängig sein, wie viele Perso-

9 Eisenberg 2005, S. 143.
10 Bock 2019, S. 318.
11 Kunz/Singelnstein 2021, S. 239-240.
12 Bock 2019, S. 320; Kunz/Singelnstein 2021, S. 239-240.
13 Kunz/Singelnstein 2021, S. 240.
14 Schwind 2016, S. 59; Kunz/Singelnstein 2021, S. 240.
15 Bock 2019, S. 321.
16 Vgl. Schwind 1989, S. 252; zur Übersicht: Jitschin 2002,S. 62-63. m.w.N.

nen ihr Fahrrad versichert haben.[17] Veränderungen in der Gestaltung der Hausratsversicherungsverträge durch die Versicherungsgesellschaften stellen daher ebenfalls eine relevante Determinante des Anzeigenverhaltens dar. So enthält etwa eine in der Hausratsversicherung inkludierte Fahrradversicherung oft eine Wertobergrenze, die zumeist an die Gesamtversicherungssumme gekoppelt ist. In anderen Fällen wird die Versicherung in gesonderte Fahrradversicherungen vollständig ausgelagert – teilweise sogar außerhalb der herkömmlichen Versicherungsgesellschaften auf spezialisierte Anbieter übertragen. Diese können für die Versicherten unterschiedlich attraktiv sein. Zu berücksichtigen ist auch, dass Menschen aus finanziell besser gestellten Personenkreisen eher zur Anschaffung höherwertiger Fahrräder tendieren und demzufolge auch eher geneigt und finanziell in der Lage sein werden, kostenpflichtige (Zusatz-)Versicherungen abzuschließen. Von dieser Gruppe ist ein stärker ausgeprägtes Anzeigeverhalten zu erwarten als aus Personenkreisen, die günstige Fahrräder erwerben. Bei einem nicht versicherten Fahrrad steht nach einer Anzeige vermutlich das Aufklärungsinteresse im Vordergrund, da sich die Opfer möglicherweise Schadensersatz oder die Rückgabe des Fahrrades erhoffen.[18]

Das geringe Ausmaß des Schadens kann ein Grund sein, der die Opfer eines Diebstahls von einer Anzeige abhält.[19] Ebenso stellt das Vertrauen der Bevölkerung eine variable Determinante dar, die Einfluss auf das Anzeigeverhalten haben kann. Die geringen Aufklärungsquoten von Fahrraddiebstählen können z.B. dazu beitragen, dass der Diebstahl geringwertiger und nicht versicherter Fahrräder oftmals gar nicht angezeigt wird, da dies aus Sicht der Opfer aufgrund der geringen Aufklärungsquote keinen Mehrwert hat.[20]

Andererseits kann die geringe Aufklärungsquote die Erstattung von Anzeigen fördern, selbst wenn tatsächlich kein Diebstahl begangen wurde. Dies macht nämlich auch den Versicherungsbetrug attraktiver, da die Schlussfolgerung gezogen werden kann, dass dieser ebenso wenig aufgeklärt werden wird, wie eine Diebstahlshandlung, d.h. das Entdeckungsrisiko gering ist. Insofern ist es denkbar, dass Fahrräder als gestohlen gemeldet werden, obwohl diese noch im Gewahrsam der Betroffenen oder weiterveräußert worden sind. Dadurch könnte das Hellfeld mehr Delikte aufweisen, als eigentlich stattgefunden haben. Diese Annahme bezieht sich aber eher auf höherwertige Fahrräder, bei denen die Aufwand-Nutzen-Relation aus Sicht der Versicherungsbetrüger*innen günstiger ausfällt.

17 Vgl. Schwind 1989, S. 260.
18 Vgl. Schwind 1989, S. 253.
19 Schwind 1978, S. 207; Jitschin 2002, S. 62 m.w.N.
20 Jitschin 2002, S. 63; vgl. Balschmiter/Roll 2016, S. 223.

Insgesamt sprechen die Umstände dafür, dass das Dunkelfeld der Fahrraddiebstähle deutlich höher ist als das Hellfeld.[21] Gerade die fehlende Aufklärungsquote im Zusammenhang mit dem oftmals geringen Wert der Fahrräder trägt dazu bei, dass viele Opfer von einer Anzeige absehen. Auch werden Fahrräder oftmals länger genutzt oder sind preisgünstig im Handel zu erwerben, weshalb es viele Fahrräder aus dem unteren Preissegment gibt. Die geringe Aufklärungsquote besteht bei Fahrraddiebstählen schon länger, sodass davon auszugehen ist, dass sie einem größeren Teil der Bevölkerung bekannt ist.

### *2.3 Schlussfolgerungen*

Letztlich ergeben sich aus dem Hellfeld nur wenige Hinweise hinsichtlich der Täter*innen von Fahrraddiebstählen und ihren Vorgehensweisen. Es bestehen – insbesondere vor dem Hintergrund kriminalistischer Erfahrungswerte – Hinweise darauf, dass bei vielen Fahrraddiebstählen mehrere Personen zusammenwirken und dass ein Bezug zum Ausland besteht. Letztere Annahme kann im Zusammenhang mit den Tatbegehungsmodalitäten stehen: Modus Operandi, kriminelle Intensität und Serientatenbegehung haben bei organisiert vorgehenden Gruppen eine besondere Ausformung.

Mit großer Wahrscheinlichkeit kann davon ausgegangen werden, dass die Anzahl der in der PKS aufgeführten Fahrraddiebstähle (Hellfeld) nur einen Teil der Gesamtzahl darstellt. Aus der kriminalistischen Praxis heraus scheint es realistisch zu sein, von einem je hälftigen Hellfeld-Dunkelfeld-Verhältnis auszugehen. Je nachdem, wie die unterschiedlichen Einflussvariablen (etwa Anzeigeverhalten und Verfolgungsdruck) gewichtet werden, wird sich dieses Verhältnis zugunsten des Dunkelfeldes oder des Hellfeldes verlagern.

## 3. Erkenntnisse aus Wissenschaft und Praxis

Hinsichtlich der einzelnen Akteur*innen beim Diebstahl und deren Vorgehensweise kann die PKS und ihre Auswertung allenfalls Anhaltspunkte liefern. Für konkrete Schlussfolgerungen müssen einzelne Taten genauer betrachtet werden. Einerseits sind daher kriminologische Erkenntnisse zum Fahrraddiebstahl auszuwerten, auf der anderen Seite Erkenntnisse aus der Praxis einzubeziehen.

Aus einer wissenschaftlichen Perspektive heraus gibt es nur wenige Erkenntnisse zum Fahrraddiebstahl. In einigen älteren kriminologischen Untersuchungen wurde der Fahrraddiebstahl zwar mit abgefragt,[22] tiefergehend hat sich

21 Vergleiche dazu auch Jitschin 2002, S. 60-64.
22 Z.B. Schwind 1975.

aber lediglich *Jitschin* mit dem Delikt beschäftigt. Neben der Aufbereitung der bisherigen Erkenntnisse führte er eine Aktenanalyse der Bestände eines Polizeikommissariats in Braunschweig aus dem Jahre 1996 durch, die einen Bezug zum Fahrraddiebstahl aufwies. Zusätzlich führte er Interviews mit Polizeibeamt*innen der Polizeiinspektionen Göttingen und Braunschweig, die sich ausschließlich mit dem Delikt des Fahrraddiebstahls bzw. Zweiraddiebstahls beschäftigt hatten.[23] Zusammenfassend geht *Jitschin* davon aus, dass das Delikt überwiegend von jungen Menschen begangen wird; Jugendliche und Heranwachsende würden die Hälfte aller Tatverdächtigen stellen. Es handele sich fast ausschließlich um männliche Täter, wobei das Delikt überwiegend von Personen aus einkommensschwachen Schichten der Bevölkerung begangen würde. Die Diebstähle und der anschließende Verkauf würden regelmäßig im Nahraum der Täter*innen stattfinden. Ein häufiges Motiv sei der finanzielle Gewinn, daneben würden aber auch der Geltungsdrang sowie konkrete Gebrauchswünsche eine Rolle spielen.[24] Es würden zudem auch Einzelteile der Fahrräder gestohlen werden.[25]

Hinsichtlich der Erkenntnisse von *Jitschin* ist anzumerken, dass diese bereits mehr als 20 Jahre alt sind. Außerdem bietet seine empirische Basis allenfalls Hinweise. In erster Linie handelt es sich dabei um Grundlagenforschung, die neben ersten Erkenntnissen den weiteren Forschungsbedarf offenbart. Daher ist ein Blick in die aktuelle kriminalistische Praxis erforderlich.

Im Rahmen des Forschungsprojektes FindMyBike wurden Polizeibeamt*innen aus Hamburg und Berlin befragt. Dabei handelte es sich ausschließlich um Beamt*innen, die einen besonderen Bezug zum Fahrraddiebstahl aufwiesen. Insgesamt wurden drei Interviews mit jeweils mehreren Personen durchgeführt. Dabei ging es u.a. um deren kriminalistische Erkenntnisse über die Täter*innen bzw. Tätergruppierungen und deren Vorgehen beim Fahrraddiebstahl. Als Erhebungsinstrument diente ein leitfadengestütztes[26] Expert*inneninterview mit einer Mischung aus offenen und geschlossenen Fragen.[27] Da die Hintergründe von Fahrraddiebstählen bislang wenig erforscht wurden, ging es in den Interviews allein darum, dass die Expert*innen ihre Erkenntnisse überwiegend deskriptiv darstellen.

Darüber hinaus wurde gemeinsam mit der Polizei Cottbus deren Erfahrungen aus einem Großverfahren hinsichtlich Fahrraddiebstählen aufgearbeitet. Auch gab die Polizei Oldenburg einen Überblick über ihre Ermittlungstätigkeit.

---

23 Jitschin 2002, S. 230.
24 Jitschin 2002, S. 263-264.
25 Jitschin 2002, S. 150.
26 Zur Konstruktion eines Leitfadens vgl. Gläser/Laudel 2010, S. 142.
27 Zur Methodik von Expert*inneninterviews vgl. Gläser/Laudel 2010, S. 112-199.

Bei der Auswahl der zu beforschenden polizeilichen Organisationseinheiten stellte sich die Problematik, dass die Zuständigkeiten für die Bearbeitung von Fahrraddiebstählen sehr unterschiedlich geregelt sind. In Berlin wurden daher die Fahrradstaffel[28] und Angehörige eines Polizeiabschnitts befragt, in denen oft Fahrraddiebstähle vorkommen. Eine Einheit, die sich ausschließlich mit Fahrraddiebstählen beschäftigt, befand sich während des Projektzeitraums noch in der Gründungsphase. Die Fahrradstaffel beschäftigt sich zwar nicht vorrangig mit der Aufklärung von Diebstählen, dafür aber mit der Prävention, weshalb die Angehörigen der Staffel im regen Austausch mit anderen Dienststellen der Polizei standen und daher über Erkenntnisse hinsichtlich der Diebstähle verfügten.

In Hamburg wurden Angehörige der „Arbeitsrate Fahrrad" befragt, die sich ausschließlich mit Fahrraddiebstählen beschäftigten. Von ihnen war zu erwarten, dass sie vertieftes Wissen über Täter*innen von Fahrraddiebstählen besitzen. Die Kontaktaufnahme zu entsprechend spezialisierten Einheiten gestaltete sich schwierig, da in vielen Polizeien solche Dienststellen temporär gegründet und nach einem gewissen Zeitraum wieder aufgelöst werden. Im Zeitpunkt der Erstellung des Beitrages gab es in mehreren Städten bzw. Bundesländern entsprechend spezialisierte Einheiten, die seit 2016 auch untereinander vernetzt sind.

Die Polizei Brandenburg fiel durch einen Ermittlungserfolg hinsichtlich bandenmäßig strukturierter Fahrraddiebstähle an der Grenze zu Polen auf. Daher war sie von besonderem Interesse, weil von ihr Informationen zur grenzüberschreitenden Fahrraddiebstahlskriminalität und zu strukturiert agierenden Täter*innen- und Täter*innengruppierungen zu erwarten waren.

### *3.1 Erkenntnisse über Fahrraddiebstähle in Berlin*

Die Kriminalitätskontrolle in Berlin basiert auf einem dreistufigen System von Bearbeitungszuständigkeiten, die sich überwiegend an der „Schwere" der in Rede stehenden Kriminalität orientieren. Dabei spielen entweder deliktsbezogene Kriterien (Wohnraumeinbruch, Kraftfahrzeugdiebstahl, Betrug u.a.) oder phänomenbezogene Kriterien (Organisierte Kriminalität, Staatsschutzdelikte u.a.) eine Rolle. Lediglich bei den in den Kriminalreferaten der örtlichen Direktionen verorteten „Täterorientierten Ermittlungen" (TOE) begründet die Person eines Täters oder einer Täterin die Zuständigkeit.

Schwere Kriminalität und besondere Kriminalitätsphänomene (wie beispielsweise „Rockerkriminalität" oder Staatsschutzdelikte) werden im Landeskriminalamt (LKA) Berlin bearbeitet (1. Stufe der Kriminalitätskontrolle). Bei

28 Dabei handelt es sich um eine Organisationseinheit, die auf Fahrrädern ihren Dienst versieht.

den besonderen Kriminalitätsphänomenen muss es sich nicht zwangsläufig um schwere Kriminalität handeln. Beispielsweise ist im LKA auch die Zuständigkeit für die Bearbeitung von Betrugsfällen zentralisiert, die früher in den Kriminalreferaten der örtlichen (regionalen) Polizeidirektionen angesiedelt war.

Schließlich werden auch im Berliner LKA Fälle der leichten Kriminalität in Form der „vereinfachten" Bearbeitung (d.h. ohne weitere Ermittlungen) verwaltet, was an sich einen Bruch mit der ursprünglichen Konzeption der Kriminalitätskontrolle darstellt. Dieser Umstand zeigt jedoch, dass die Zuständigkeit für den Fahrraddiebstahl theoretisch auch anders verortet werden könnte, sogar im Landeskriminalamt selbst, beispielsweise bei banden- oder gewerbsmäßiger Begehung in ausgesuchten Fällen mit Vorgangsauswahlrecht.

Tatsächlich werden Fahrraddiebstähle allerdings weder im LKA Berlin noch in den Kriminalreferaten der örtlichen (regionalen) Polizeidirektionen[29] (2. Stufe der Kriminalitätskontrolle) zentralisiert bearbeitet. Lediglich die in den Referaten verorteten Einheiten zur Ermittlung von Hehlereistraftaten könnten in ausgesuchten Fällen von Tatserien mit Fahrraddiebstahl befasst sein.

Die Fahrraddiebstähle werden in den sogenannten Abschnittskommissariaten (3. Stufe der Kriminalitätskontrolle) bearbeitet. Diese Kommissariate sind eine verhältnismäßig neue Einrichtung innerhalb der örtlich/regional zuständigen Polizeiabschnitte.[30] Während diese rein schutzpolizeiliche Gliederungseinheiten darstellen, werden die Abschnittskommissariate durch Kriminalbeamt*innen geführt, die der Fachaufsicht der Kriminalreferate in den örtlichen Direktionen unterstehen. Die Sachbearbeitung selbst – also auch die von Fahrraddiebstahlsfällen – wird durch Schutzpolizist*innen vorgenommen. Insgesamt sind die Abschnittskommissariate für die Bearbeitung von Fällen der „einfachen" Kriminalität zuständig, zu denen beispielsweise Beleidigungen, Sachbeschädigungen oder einfache Körperverletzungen zählen.

Eine gesonderte Zuständigkeit für Fahrraddiebstähle ist nicht vorgesehen und auch nicht vorhanden. Denkbar wären kurzzeitige Fahrraddiebstahlschwerpunkteinsätze auf der Ebene der Dienstgruppen eines Polizeiabschnitts oder auch die Gründung einer temporären Ermittlungsgruppe beim Vorliegen besonderer Ermittlungsanhalte, was aber lediglich aus der Alltagsorganisation der Dienststellen heraus in eigener Zuständigkeit erfolgen kann.

Die Fahrradstaffel kommt berlinweit zum Einsatz,[31]stellt aber keine „Ermittlungsgruppe Fahrraddiebstahl" dar. Sie sieht sich primär als Einheit, die im

29 Davon unterhält die Landespolizei Berlin fünf, eine weitere Direktion ist für den (überwiegend) schutzpolizeilichen Einsatz als „Direktion Einsatz/Verkehr" zuständig.

30 Polizeiabschnitte gehören als Gliederungseinheiten zu den genannten Polizeidirektionen.

31 Diese wurde, hervorgehend aus einer regional agierenden Polizeieinheit, mit entsprechender Personalausstattung sukzessive berlinweit ausgebaut.

Straßenverkehr überwiegend präventive Aufgaben wahrnimmt und Verkehrsordnungswidrigkeiten (wie Rotlichtfahrten von Radfahrern o.a.) im Rahmen des allgemeinen polizeilichen Auftrages verfolgt und ahndet.

Die Initiative einer Polizeidirektion, den Einsatz von mit Sendern präparierten „Lockfahrrädern" in einem ihrer Polizeiabschnitte zu untersuchen, stellt eine Ausnahme im Umgang mit der Thematik dar. In einigen Polizeiabschnitten wurde mit entsprechenden Fahrrädern experimentiert. Die polizeilichen Bemühungen zum Fahrraddiebstahl beschränken sich ansonsten durchweg auf präventive Maßnahmen der Polizeiabschnitte (selten auch des Präventionsbereiches des LKA Berlin), bspw. die nicht unumstrittenen Aktionen zur „Fahrradcodierung bzw. Fahrradkennzeichnung" sowie Bürgerberatungen.

Insgesamt sind die Erkenntnisse zu den Fahrraddiebstählen aufgrund der beschriebenen Organisationsstruktur begrenzt. Eine systematische Verfolgung von berlinweit operierenden Fahrraddieb*innen findet nicht statt. Das Phänomen wurde bisher nicht bezirksübergreifend systematisch und zielgerichtet ausgewertet. Insofern gingen die Erkenntnisse aus den Interviews nicht über den Bericht von Einzelfällen und Beobachtungen hinaus.

So gibt es Hinweise darauf, dass mehrere Personen bei Fahrraddiebstählen zusammenwirken, was auf gewerbs- und bandenmäßigen Diebstahl hindeutet, wobei bisher keine entsprechenden Ermittlungserfolge erzielt werden konnten. Konkrete *Modi Operandi* bestimmter Gruppierungen konnten nicht festgestellt werden, wobei aufgrund der teilweise sehr schlecht gesicherten Fahrräder gezielt vorgehende Täter*innen nicht vor großen Herausforderungen stehen.. Dabei kommt den Täter*innen auch die Anonymität der Großstadt zugute, da das soziale Umfeld kaum auf fremdes Eigentum achtet. Zudem werden Fahrräder in großer Anzahl auf Fahrradparkplätzen abgestellt, was die „Anonymität der Gegenstände" noch erhöht.

Gestohlene Fahrräder wurden im Rahmen von Stichproben oftmals und auch in größerem Umfang auf Flohmärkten aufgefunden, was zumindest in Ansätzen auf organisierte Vertriebsstrukturen hindeutet. Es wurde beobachtet, dass die Fahrräder unmittelbar nach dem Diebstahl oder zumindest zeitnah direkt zu den Flohmärkten verbracht wurden. Teilweise wurden die Fahrräder aber auch im öffentlichen Raum abgestellt – dabei werden mehrere Fahrräder zusammengeschlossen – oder direkt nach dem Diebstahl in Wohnungs- oder Kellerräume verbracht. In Einzelfällen konnte festgestellt werden, dass gestohlene Fahrräder auf Internetplattformen zum Verkauf angeboten wurden. Zudem ergaben Ermittlungen, dass es auch Fälle gibt, in denen die Fahrräder auseinandergebaut werden, um die (teilweise hochwertigen) Einzelteile gesondert zu veräußern.

Vor dem Hintergrund der beschränkten und regional bezogenen Erkenntnisse bezüglich dieses Kriminalitätsphänomens scheint es sinnvoll, diese in

einer Einheit zusammenzuführen, die berlinweit operiert, um die strukturellen Defizite zu überwinden und das Hellfeld zu vergrößern.

### *3.2 Erkenntnisse über Fahrraddiebstähle in Hamburg*

Die „Arbeitsrate Fahrrad" war eine Ermittlungsgruppe des Hamburger LKA. Ziel der Gruppe war eine Erhöhung der Aufklärungsquote bei gleichzeitiger Senkung der Fallzahlen von Fahrraddiebstählen durch eine teilzentralisierte Sachbearbeitung. Dazu wurden die Fahrraddiebstahlsanzeigen gezielt hinsichtlich Mehrfachtäter*innen analysiert.

Die Ermittlungen der „Arbeitsrate Fahrrad" fokussierten sich nicht nur auf die Dieb*innen, sondern auch auf dahinterstehende Strukturen und die anschließende Hehlerei. Aufgrund der Ermittlungen konnten in Hamburg große Mengen gestohlener Fahrräder in mehreren Großeinsätzen sichergestellt werden. Nachdem bei einem Einsatz im Jahre 2017 2000 Fahrräder sichergestellt werden konnten und Verhaftungen erfolgten, ging die Zahl der Fahrraddiebstähle in Hamburg zurück. Dies deutet auf ein „Wegbrechen" von Teilen der Vertriebsstruktur hin.

Die Täter*innen lassen sich in folgende Gruppen einteilen:

- Gelegenheitstäter*innen, die sich an den aktuellen, objektiven Tatgelegenheitsumständen orientieren und das Fahrrad entweder veräußern oder selbst behalten.
- Beschaffungskriminalität, d.h. die Täter*innen finanzieren mit den Diebstählen und der anschließenden Weiterveräußerung ihre Sucht. Diese Form der Kriminalität ist allerdings nicht zwingend auf Fahrräder gerichtet. Jedoch gab es in Hamburg einen entsprechenden Absatzmarkt für Fahrräder.
- Regional ansässige Täter*innen, die gezielt vorgehen und das Fahrrad entweder selber nutzen oder im regionalen Bereich weiterverkaufen, etwa auf Flohmärkten oder Internetplattformen.
- Überörtlich organisierte Täter*innen, die Fahrräder in größerem Umfang stehlen und diese dann ins Ausland transportieren. Diese fahren etwa mit einem Kleintransporter durch Hamburg und stehlen im größeren Umfang Fahrräder. Einzelne Ermittlungserkenntnisse deuten zudem darauf hin, dass mehrere Städte abgefahren werden. Bei einem polizeilichen Einsatz wurden 100 gestohlene Fahrräder aus Dänemark sichergestellt, was darauf hindeutet, dass gestohlene Fahrräder auch durch Deutschland transportiert werden. Es scheint ein Absatzmarkt in an Deutschland angrenzende Länder zu bestehen.

Wie hoch der Anteil von Täter*innengruppen an der Gesamtzahl der Fahrraddiebstähle ist, lässt sich aufgrund der aktuellen Erkenntnislage nicht feststellen.

Grundsätzlich gingen die Mitglieder der „Arbeitsrate Fahrrad“ davon aus, dass Fahrraddiebstähle sehr lukrativ sind, weil ein geringes Entdeckungsrisiko bestehe und die Fahrräder leicht weiterveräußert werden können. Bei den Diebstählen wurden auch öffentliche Verkehrsmittel zum Transport genutzt. Die Straftaten wurden regelmäßig durch das Wegtragen eines abgeschlossenen Fahrrades oder durch das Öffnen eines Fahrradschlosses mittels eines Bolzenschneiders durchgeführt. Dabei kam den Täter*innen zugute, dass Fahrräder oft unzureichend gesichert sind. Zudem waren die Täter*innen auch mit „Profi-Werkzeug“ ausgestattet, d.h. mit hydraulischen Bolzenschneidern oder schweren Werkzeugen. Das scheint aber eher die Ausnahme zu sein, da ein solcher Aufwand bei vielen Schlössern gar nicht nötigt ist. Es kam auch vor, dass Fahrräder zunächst gestohlen, an einem Ort zwischengelagert und anschließend zusammen abgeholt wurden. Außerdem wurden Fahrräder teilweise zeitnah nach dem Diebstahl auseinandergenommen, damit nur die Einzelteile verkauft werden können. Für Einzelteile scheint also auch ein Absatzmarkt zu bestehen, der sich insbesondere auf höherwertige Komponenten bezieht.

Zur Diebstahlsprävention bedarf es aus Sicht der „Arbeitsrate“ einer gezielten Öffentlichkeitsarbeit, um die Bevölkerung für Risikofaktoren des Fahrraddiebstahls zu sensibilisieren und zu effektiveren Sicherungsmaßnahmen anzuhalten. Diebstähle ließen sich durch die Verwendung von besseren Schlössern oder geeigneten Abstellplätzen vermeiden.

### *3.3 Erkenntnisse über Fahrraddiebstähle in Brandenburg*

In den Jahren 2012 und 2013 stiegen die Fallzahlen bei Diebstahlsdelikten im besonders schweren Fall von Fahrrädern im Süden des Landes Brandenburg stark an. Die Schäden bewegten sich dabei im sechsstelligen Bereich. Zudem wurden neben den ortsansässigen Fahrraddieb*innen, welche vorrangig dem Bereich der Beschaffungskriminalität zuzuordnen sind, vermehrt polnische Staatsangehörige beim Fahrraddiebstahl angetroffen. Daher war es aus polizeilicher Perspektive geboten, sich vertiefter mit diesem Phänomen des massenhaften Fahrraddiebstahls zu beschäftigen. Aufgrund einer näheren Betrachtung der Diebstahlshandlungen konnten unterschiedliche Vorgehensweisen bei ortsansässigen und auswärtigen Täter*innen festgestellt werden.

Während in Deutschland lebende Täter*innen oftmals alleine oder mit einer Mittäterin oder einem Mittäter agierten und das Fahrrad als Zufallsfund auf dem Beutezug entwendet wurde, richteten die polnischen Fahrraddieb*innen ihre Beutezüge nach dem konkret erwarteten Diebesgut (z.B. Fahrradtypen und -modellen) aus.

Nach Erkenntnissen der Polizei Brandenburg fand der Fahrraddiebstahl vorwiegend im städtischen Raum statt. Hier wurden die Fahrräder meist ein-

zeln, in öffentlichen oder leicht zugänglichen Bereichen gestohlen, etwa an Fahrradsammelplätzen oder aus Gemeinschaftskellern. Mit dem Erscheinen und dem systematischen Vorgehen einer Diebesbande, die nachstehend weiter beschrieben wird, erweiterte sich der Beschaffungsraum erheblich, insbesondere in den privaten Bereich der Bestohlenen.

Als systematisch kann das Vorgehen insofern bezeichnet werden, weil beim Übertreten der Grenze bereits die Tatörtlichkeit feststand und je nach Wahl der Örtlichkeit in einem fest eingespielten Modus Operandi vorgegangen wurde.

Aufgrund der Vorgänge wurde in der Polizei Brandenburg eine bislang einzigartige Ermittlungsgruppe zur Aufklärung dieser Diebstähle gegründet, die intensive Ermittlungen unter Einbeziehung operativer Maßnahmen führte. Hierbei wurden die strafprozessualen Möglichkeiten umfassend ausgeschöpft. Aufgrund der hohen Fallzahlen lagen die Prioritäten bei der Aufklärung grenzüberschreitender Kriminalität sowie den Verfahren mit konkreten Ermittlungsansätzen. Zudem wurde der Ermittlungsgruppe für eine optimale Verfahrensbearbeitung sowie -begleitung ein Staatsanwalt zugeordnet. Ferner arbeitete sie im Rahmen der grenzüberschreitenden Zusammenarbeit mit der polnischen Polizei zusammen.

Anzumerken ist, dass diese Ermittlungsgruppe lediglich temporär und aus Kräften einer ohnehin personell schwächer ausgestatteten Polizeidienststelle bestand. Sie verfügte über eine operative Auswerte- sowie Fahndungskomponente, welche nicht aus entsprechend spezialisierten Organisationseinheiten herangezogen werden konnten, sondern zu Lasten der Alltagsorganisation bereitgestellt wurden.

Die Initiative zur Gründung dieser Einheit ging von Kräften der mittleren Führungsebene aus. Sie beruhte auch nicht auf einer kriminalstrategischen Entscheidung. Somit kann daraus kein behördlicher Perspektivwandel bezüglich der Wahrnehmung des Fahrraddiebstahls als ernstzunehmendes Kriminalitätsphänomen abgeleitet werden. Grundsätzlich sind Schwerpunktsetzungen im Rahmen der Kriminalitätskontrolle ein Ergebnis eines politischen und gesamtbehördlichen Priorisierungsprozesses, der bis in die nachgeordneten Einheiten der Ermittlungsdienststellen und des Basisdienstes durchwirkt. Der Erfolg der Brandenburger Ermittlungseinheit zeigt allerdings deutlich, dass bereits geringe Veränderungen in den Priorisierungsprozessen nachgeordneter Gliederungseinheiten zu erheblichen Verbesserungen in der phänomenbezogenen Kriminalitätskontrolle führen können.

Diese stellen sich in folgender Weise dar:

- Verschiebungen des Dunkelfeldes zugunsten des Hellfeldes
- Dadurch bedingter Erkenntnisgewinn über Vorgehensweisen von Täter*innen bzw. Täter*innengruppierungen und deren Strukturen
- Gezielterer Einsatz von Polizeikräften zur Unterbindung weiterer Tatserien
- Gerichtsfeste Beweisführung, um eine Verurteilung sicherzustellen
- Generalpräventive Wirkung durch entsprechende Öffentlichkeitsarbeit und daraus resultierende erhöhte Aufmerksamkeit in der Bevölkerung für das Thema (im Sinne von Prävention und Mitwirkung bei der Straftatenaufklärung)
- Teilweise Rückgewinnung von Diebesgut

Den nachfolgenden Erkenntnissen liegen die umfassenden Ermittlungen der Ermittlungsgruppe zugrunde, welche bis ins Jahr 2013 zurückreichen.

### *3.3.1 Täterinnen und Täter*

Haupttäter*innen der o.g. Bande waren Jugendliche, Heranwachsende und jungen Erwachsene, die aus sozial schwachen Bevölkerungsschichten stammten. Die Diebstähle wurden akribisch organisiert. Die Gruppe umfasste ca. 40 Mitglieder, wobei die Organisation und Koordination der Diebstähle durch fünf Brüder erfolgten, die als „Hintermänner" agierten und die Strukturen zusammenhielten. Es gab Dieb*innen, Personen für den Transport und dahinterstehende Organisations- und Verkaufsstrukturen. Die Täter*innen kannten sich untereinander und kamen alle aus derselben Gegend, in der eine hohe Arbeitslosigkeit herrschte. Daher können die sozioökonomischen Strukturen als schwach eingestuft werden. Für die Ausführung der Diebstähle wurden vielfach Jugendliche und suchtkranke Menschen angeworben.

### *3.3.2 Tatörtlichkeiten*

Für ihr Vorhaben mussten sich die Täter*innen einer stetigen Verfügbarkeit an qualitativ hochwertigen Fahrrädern gewiss sein. Dafür bezogen sie neben der Jahreszeit auch die örtlichen Gegebenheiten in die Planung ein.

Betrachtet man die Bevölkerungsverteilung im Land Brandenburg, wird deutlich, dass im Berliner Umland die Einwohnerzahl stetig steigt, während der Rest des Landes eher dünn besiedelt ist und dörfliche sowie kleinstädtische Siedlungsstrukturen aufweist. Ausnahmen bilden die Großstädte Potsdam und Cottbus sowie vereinzelte größere Städte wie Brandenburg/Havel oder Frankfurt/Oder.

Während die größeren Städte auf Grund der hohen Einwohnerzahlen tagsüber in den Zentren und zentrumsnahen Stadtteilen eine gewisse Anonymität

für Täter*innen versprachen, verfügen die Kleinstädte zumeist nur über einen relativ überschaubaren Raum, welcher sich zum Fahrraddiebstahl eignet. Die Gefahr aufzufallen und bei der Tathandlung angetroffen zu werden, ist daher in kleineren Städten bzw. Dörfern wesentlich größer. Daher suchte die Bande zur Tageszeit oft nur Kleinstädte auf, welche unmittelbar an der Grenze lagen. Im Falle der Entdeckung konnten die Bandenmitglieder schnell zu Fuß über die Grenze fliehen.

Im städtischen Bereich fokussierten sich die Täter*innen auf Fahrradsammelplätze, wie sie an Schulen, Bahnhöfen, Freizeiteinrichtungen, Einkaufszentren, Krankenhäusern oder vor Mehrfamilienhäusern zu finden sind. In der fahrradfreundlichen Jahreszeit ist tagsüber die Auswahl an diesen Sammelplätzen groß. Nachts oder in der kalten Jahreszeit befinden sich die meisten Fahrräder unbenutzt in Kellern oder Garagen.

### *3.3.3 Tatgegenstand*

Die Tatsache, dass im zunehmenden Maße Damenfahrräder gestohlen wurden, offenbart die Nachfrage, die im Rahmen der Ermittlungen insbesondere für den osteuropäischen Markt belegt werden konnte. So entwendete die Bande in erster Linie sog. Citybikes für Damen mit „Ein-Rohr-Rahmen-Konstruktion“ namhafter Hersteller, gefolgt von Rennrädern und Mountainbikes. Klassische Trekkingbikes sowie Herrenfahrräder waren anscheinend für den ausländischen Markt weniger interessant. Bei den für den Verkauf im Ausland gestohlenen Fahrrädern handelte es sich meist um solche in „neuwertigem Originalzustand mit hochwertigen Teilkomponenten“. Da die Fahrräder größtenteils für den Gebrauchtwarenhandel von „Westwaren“ oder für Fahrradverleihe bestimmt waren, war der Originalzustand für die Auswahl und die anschließende Veräußerung (teilweise auch im Internet) von großer Bedeutung. Fahrräder unter einem Verkaufswert von 500 Euro (Massenware aus dem Großhandel) waren für die Bande nicht interessant. Man hielt sich insbesondere an Marken der ZEG (Zweirad-Einkaufs-Genossenschaft) aus dem Mittelpreissegment, die in vielen Fahrradläden zu finden sind. Diese Fahrradmarken sind weitläufig bekannt und für die Abnehmer auf dem östlichen Markt erschwinglich.

Die entwendeten Fahrräder wurden meist im Originalzustand belassen. Nur für den Transport wurden vorhandene Körbe oder Kindersitze entfernt, die Lenker um 90 Grad verdreht und bei Raumknappheit das Vorderrad ausgebaut.

Den Ermittlungsergebnissen entsprechend nahmen die Täter*innen keine Manipulationen an den Rahmennummern vor. Diese sind auch aus zweierlei Sicht entbehrlich. Zum einen erhärtet eine Manipulation selbst schon für den Laien, dass es sich bei dem angebotenen Fahrrad um Diebesgut handeln könnte; zum anderen ist dies nicht notwendig, da Fahrräder zur Sachfahndung nicht

in das Schengener Informationssystem (SIS) eingepflegt werden, sodass die Abfrage der Rahmennummer eines in Deutschland entwendeten Fahrrades im Ausland stets negativ ausfällt.

Im Gegensatz dazu stehlen die ortsansässigen Fahrraddieb*innen, meist im Rahmen der Beschaffungskriminalität, Fahrräder, die bei jungen Menschen gefragt sind, z.B. Mountainbikes, Rennräder oder die populären Singlespeeds, Urbanbikes oder Crossbikes. Der Beschaffungsmarkt orientiert sich hier an der Nachfrage in der „Szene". Die entwendeten Fahrräder werden entweder als Währung in der Betäubungsmittelszene eingesetzt oder zeitnah nach dem Diebstahl in die Einzelteile zerlegt (teilweise werden auch nur einzelne Komponenten gestohlen), um entweder die hochwertigen Komponenten zu veräußern oder komplett neue Fahrräder zusammenzustellen. Gerade Mountainbikes und Rennräder sind durch ihre Beschaffenheit und ihren Verwendungszweck für schnelle Umbauten prädestiniert. Eine mögliche Wiedererkennung bei der Veräußerung wird durch aufwendige Manipulationen der Rahmennummern sowie Lackierarbeiten entgegengewirkt.

### *3.3.4 Tatfahrzeuge*

Die Mitglieder der Bande wählten ihre Tatfahrzeuge gezielt aus. Erfahrungsgemäß wurden durch die Polizei im grenznahen Raum vorwiegend Transporter oder neuere Fahrzeuge höherwertiger Marken kontrolliert, weil diese primär im Verdacht standen, selbst gestohlen zu sein. Daher wählten die Täter*innen Fahrzeuge mit einer hohen Ladekapazität aus, die unauffällig im alltäglichen Grenzverkehr waren und in das geringe Budget der Täter*innen passten. So fiel ihre Wahl auf Großraumlimousinen/Familienvans und Kombis. Zunächst wurden vor allem Kombifahrzeuge der Marke Opel (Typen Omega und Vectra) genutzt, später bevorzugt Personenkraftwagen (Pkw) der Marken Ford Galaxy und Chrysler Voyager.

Teilweise wurden die Rücksitze ausgebaut und mehrere Decken hineingelegt, welche das Diebesgut vor möglichen Einblicken von außen schützen sollten.

Während die Täter*innen anfänglich die Fahrzeuge noch auf sich registrieren ließen, änderte sich dies im Laufe der Zeit. Bedingt durch den teilweise den niedrigen Kaufpreis begründenden schlechten bautechnischen Zustand der Fahrzeuge, kam es zu Ausfällen, und die Fahrzeuge wurden zeitnah wieder abgestoßen. Die durchschnittliche Nutzungsdauer als Tatfahrzeug betrug nur wenige Wochen. Eine Ummeldung der neu erworbenen Fahrzeuge erfolgte nicht mehr, was die Ermittlungen zusätzlich erschwerte.

### *3.3.5 Die ermittelten Modi Operandi der Bande*

Für die Bande konnten vier unterschiedliche Vorgehensweisen ermittelt werden.

**Modus Operandi I:**

Im Sommer nutzte die Bande den Umstand der ausgesprochen langen Sommerferien in Polen und warb Jugendliche aus sozial schwachen Familien für ihre Tathandlungen an. Diese Jugendlichen wurden gemeinsam mit den Haupttäter*innen im Pkw zur Tageszeit über die Grenze in die Peripherie der Zielstadt gebracht. Für die Einreise wurden die offiziellen Grenzübertrittstellen genutzt.

Um bei einer Fahrzeugkontrolle nicht aufzufallen, führten sie die Tatwerkzeuge (Bolzenschneider) nicht mit. Diese wurden bei vorherigen Diebstählen oder zur Tatvorbereitung an verschiedenen Stellen im Stadtgebiet „gebunkert", etwa im Buschwerk oder in anderen Verstecken. Nach dem Absetzen der Täter*innen holten diese den Bolzenschneider aus dem Versteck, anschließend gingen die Täter*innen gemeinsam zu Fuß auf die Suche nach hochwertigen Fahrrädern. Zur Tarnung, aber auch zum Transport des Tatmittels, wurden Rucksäcke mitgeführt. Mit ihrer eher sportlichen Bekleidung und teilweise in weiblicher Begleitung erweckten die Täter für Außenstehende eher den Eindruck von Schülern auf dem Schulweg oder bei gemeinsamen Freizeitaktivitäten.

Entwendet wurden die Fahrräder entweder an Fahrradsammelplätzen sowie vor Eingängen von Mehrfamilienhäusern. Vormittags wurden gezielt Schulhöfe oder Fahrradständer vor Unternehmen aufgesucht, nachmittags Freizeiteinrichtungen oder Einkaufszentren. Die Taten wurden arbeitsteilig begangen. Mindestens eine Person stand „Schmiere" (d.h. sicherte den Entwendungsvorgang ab), während eine andere das Fahrrad entwendete. Oftmals lagen die Tatorte unmittelbar nebeneinander. Der Bolzenschneider wurde anschließend zurück in das Versteck gebracht.

Der Abtransport erfolgte entweder direkt mit dem Fahrrad, wozu die Täter*innen auf Radwegen und Nebenstraße bis zur Grenze fuhren oder das Diebesgut außerhalb der Stadtgrenze in eher unzugänglichen Flurstücken deponierten. Besonders an Tagen mit hohem Beuteaufkommen konnte so die Verbringung der Fahrräder abgesichert werden. Die Wahl der Verbringungsrouten über die Radwege versprach Sicherheit vor Kontrollen, da diese nur teilweise mit Pkw befahrbar waren und ggf. nahender Fahrzeugverkehr frühzeitig erkannt werden konnte. So kam es vor, dass am Wegesrand Fahrräder ohne die Dieb*innen angetroffen wurden, da diese sich rechtzeitig fußläufig entziehen konnten.

Nachdem die Fahrräder über offizielle, aber auch inoffizielle Grenzübertrittstellen, wie etwa Eisenbahnbrücken oder Wehranlagen, außer Landes gebracht worden waren, erfolgte das Verladen der Fahrräder auf polnischem Staatsgebiet. Die Täter*innen wurden entweder nach Hause gefahren oder zu einer weiteren Tathandlung zurück auf deutsches Staatsgebiet.

Dieser Modus Operandi war insbesondere im grenznahen Bereich zu verzeichnen (bis zu einer Entfernung von ca. 40 Kilometern bis zur Grenze).

**Modus Operandi II:**

Mit Eintritt der kälteren Jahreszeiten agierte die Bande verstärkt zur Nachtzeit. Neben den bisher begangenen besonders schweren Diebstählen von Fahrrädern an Fahrradsammelpunkten sowie vor Mehrfamilienhäusern beging sie nun auch Diebstähle aus Kellern.

Nach der gemeinsamen Einreise nach Deutschland mit zwei Pkw wurden die Fahrzeuge am äußeren Rand der Zielstadt abgestellt. Ein Pkw (oftmals ein Kombi) diente dabei für die Verbringung des Diebesgutes, der andere Pkw für den Transport der Täter.

Der Tatortbereich, bei dem es sich vorrangig um sog. „Plattenbausiedlungen" handelte, wurde durch die Gruppe zu Fuß ausgekundschaftet. Hierbei zeigte man sich offen mit einem jugendtypischen Auftreten. Die Gruppe besichtigte nacheinander Eingänge der Mehrfamilienhäuser und wartete eine günstige Gelegenheit ab. Die einzelnen Mitglieder sicherten sich gegenseitig durch „Schmierestehen" ab. Aus dem Schutz der Gruppe heraus wurde das Fahrrad vor dem Hauseingang entwendet oder sich gewaltsam Zugang mittels Schraubendreher oder Stechbeitel zum Hauseingang bzw. zum Kellerbereich des Mehrfamilienhauses verschafft. Ausschließlich wurden die Fahrräder aus den Gemeinschaftskellern mitgenommen. Hierbei machte man sich u.a. den Umstand zu Nutze, dass vielgenutzte Fahrräder häufig nicht gesichert waren. Mit den entwendeten Fahrrädern bewegte sich die Gruppe zum nächsten Hauseingang, um dort auf dieselbe Art und Weise vorzugehen. Anschließend wurde das Diebesgut in den mitgeführten Pkw verladen oder in Depots zwischengelagert.

Die Zwischenlagerung fand an unauffälligen Orten, bspw. Fahrradständern vor Mehrfamilienhäusern oder Haltestellen, statt. Hier wurden sie mit eigens mitgeführten Schlössern gesichert. Bei der späteren Abholung des Diebesgutes konnte so etwaigen Beobachtern der Eindruck vermittelt werden, dass es sich um das eigene Fahrrad handle.

Vor dem Verladen wurde das Diebesgut selektiert, die aussortierten Fahrräder wurden vor Ort zurückgelassen. Das Verladen der Fahrräder erfolgte in den bereits wartenden Pkw. Dazu wurden die Vorderräder ausgebaut, sperriges

Zubehör (z.B. Fahrradkörbe) entfernt und die Lenker um 90 Grad verdreht. Zum Sichtschutz wurden die Fahrräder mit Decken und Planen abgedeckt. Die beiden Pkw, jeweils beladen mit Diebesgut und Täter*innen, verließen im Konvoi gemeinsam auf kürzestem Weg das Stadtrandgebiet und anschließend über weniger frequentierte Nebenstraßen das Bundesgebiet.

Dieser Modus Operandi wurde im grenznahen Raum, aber auch in Städten vollzogen, welche bis zu 150 Kilometer von der Grenze entfernt liegen. Bei den weiter entfernt liegenden Tatörtlichkeiten kehrten die Täter*innen später nicht wieder zum Tatort zurück.

**Modus Operandi III:**

Bei dieser Vorgehensweise reisten die Täter (ausschließlich männlich) mit einem oder zwei Pkw-Kombis nachts in die Bundesrepublik ein. Die Fahrzeuge waren mit jeweils zwei Personen besetzt und dienten zum einen dem Transport der Bandenmitglieder und zum anderen zum Transport des Diebesguts. Die Tatfahrzeuge fuhren fast ausnahmslos gemeinsam den Zielort an und stellten die Fahrzeuge am Rande von Wohngebieten in der Nähe von Ausfallstraßen ab. Fußläufig näherte man sich in Zweierteams den Hauseingangsbereichen der Mehrfamilienhäuser an, vorrangig sog. Plattenbauten.

Eine Person stand „Schmiere“, während die andere die Eingangstür mittels Schraubendreher oder Stechbeitel aufhebelte und sich Zutritt zum Haus verschaffte. Im Anschluss wurden gemeinsam die Kellerabteile besichtigt, gewaltsam geöffnet und hauptsächlich hochwertige Räder entnommen, aber auch andere Gebrauchsgegenstände, z.B. Elektrowerkzeuge. Die privaten Keller (oftmals nur einfache Holzlattenabteile) waren zumeist nur mit Bügelschlössern gesichert, die vergleichsweise einfach mit Bolzenschneidern überwunden werden konnten.

Die Täter verbrachten das Diebesgut aus den Tatobjekten zu vorher verabredeten Sammelstellen in der Nähe der abgestellten Pkw. Nachdem der Beutezug die Ladekapazität der Pkw erreicht hatte, wurde dieser herangefahren und das Diebesgut verladen. Dafür wurden wieder die Vorderräder ausgebaut und die Lenker um 90 Grad verdreht, um mehrere Fahrräder übereinander in den Pkw stapeln zu können. Anschließend wurden die Räder mit Decken abgedeckt, um ein eventuelles verdächtiges Anleuchten der reflektierenden Fahrradteile nach außen zu verhindern.

Der Tatort wurde zeitnah über die nahegelegenen Ausfallstraßen auf direktem und schnellstem Weg zur polnischen Grenze verlassen, wobei im Laufe der Zeit der erste Wagen als „Pilotfahrzeug“ diente, um dem nachfolgenden vor eventuellen Polizeistreifen bzw. Kontrollen (insbesondere im Grenzbereich) zu

warnen. So stellte die Bande sicher, dass mindestens einer der beiden Pkw über die Grenze gelangte.

Dieser Modus Operandi wurde vor allem in Städten mit guter Autobahnanbindung und einer Entfernung von ca. 30 bis 100 Kilometern bis zur Grenze praktiziert.

**Modus Operandi IV:**

Nachdem viele Plattenbausiedlungen wiederholt aufgesucht worden waren, wechselte die Bande auf andere Tatörtlichkeiten. Anstelle von Kellern in Mehrfamilienhäuser konzentrierte sie sich nun auf Nebengelasse von Einfamilienhäusern, die sie in Stadtrandsiedlungen oder stadtnahen Dörfern aufsuchten. Hierbei machte sie sich den Umstand zu Nutze, dass diese Örtlichkeiten zur Nachtzeit sehr wenig frequentiert werden. Regelmäßig gibt es weder Anwohner- noch Durchgangsverkehr, allenfalls wird in den frühen Morgenstunden die Zeitung geliefert. In diesen Wohngegenden leben finanziell eher bessergestellte Menschen, weshalb dort auch teure Fortbewegungsmittel vermutet werden können.

In diesem vorwiegend ländlich geprägten Raum waren zuvor kaum Fahrrad- und sonstige Diebstähle vorgekommen, sodass die Bewohner*innen nicht damit gerechnet und allenfalls ihre Pkw besonders gesichert hatten. Die Nebengelasse waren oft nicht gegen unbefugten Zugriff gesichert, geschweige denn die darin abgestellten Fahrräder. So hatten die Täter*innen vergleichsweise leichten Zugang zu einer großen Auswahl an höherwertigen Fahrrädern; auf einem Grundstück waren meistens mehrere Fahrräder vorhanden.

Für den entsprechenden Beutezug wurden die Täter*innen nachts mit einem Pkw über die Grenze gebracht und in größerer Distanz (ca. 2 Kilometer) zum Tatort abgesetzt. Sie agierten gemeinsam aus einer Gruppe von drei bis vier Personen heraus, wobei sie sich gegenseitig bei der Tatbegehung absicherten. Zunächst liefen sie die Straßen der Siedlungen ab und hielten nach Hunden, Bewegungsmeldern und unter Aspekten der Zugänglichkeit und Belebtheit Ausschau. Erst danach betraten sie die Grundstücke über das unverschlossene Hoftor oder überstiegen Zäune um die Grundstücke zu betreten.

Für die eigentliche Tathandlung wurden keine Tatmittel mitgeführt, da man auf fehlende Sicherungen hoffte. Waren die Nebengelassene jedoch verschlossen, wurden die Schutzvorrichtungen auf kreative Art und Weise überwunden. Hierfür bediente man sich vorhandener Gartenwerkzeuge, etwa Heckenscheren oder Schaufeln. Aus den Nebengelassen wurden oftmals neben den Fahrrädern auch weitere Gegenstände entwendet, z.B. Motorsägen oder Motorradhelme. Die von den Grundstücken entwendeten Fahrräder wurden in einer gewissen Entfernung vom Tatort zwischengelagert. Danach kehrten die Täter*innen zu-

rück, um die Nachbargrundstücke zu betreten. Dieser Vorgang konnte mehrere Stunden in Anspruch nehmen. Anschließend wurden die entwendeten Räder mitsamt dem weiteren Diebesgut auf Radwegen in Richtung Grenze verbracht. Der Grenzübertritt (per Fahrrad) erfolgte zumeist in den frühen Morgen- und Vormittagsstunden über offizielle oder inoffizielle Übertrittstellen. Bei entsprechender Beute wurde das Depot danach erneut aufgesucht und die restlichen Fahrräder zur Grenze gefahren.

Dieser Modus Operandi war insbesondere im grenznahen Bereich zu verzeichnen (bis zu einer Entfernung von 40 Kilometern bis zur Grenze).

### *3.3.6 Bandenkriminalität vs. Organisierte Kriminalität*

Das gemeinschaftliche Agieren der Täter stellt noch keine Organisierte Kriminalität (OK) im kriminalpolizeilichen Sinne dar, sondern ist zunächst lediglich als bandenmäßiges Handeln anzusehen und einzustufen. Letztendlich diente der Diebstahl der Fahrräder durch die in Rede stehende Bande der Beschaffung eines Tageseinkommens, welches jedoch nicht (wie von der OK-Definition des BKA[32] gefordert) dem Gewinn- oder Machtstreben unter Verwendung von gewerbe- oder geschäftsähnlicher Strukturen diente, sondern lediglich dem „Broterwerb“ oder dem anschließenden Kauf von Rauschmitteln, sei es Alkohol oder andere berauschende Mittel.[33] Die Beutezüge endeten jeweils mit der Direktabgabe der entwendeten Fahrräder beim Zwischenhändler und der sofortigen Aufteilung des Erlöses unter den Tatbeteiligten. Fast täglich erfolgte ein erneuter Beutezug mit identischer Zielsetzung.

### *3.3.7 Erschwerte Abgrenzung zwischen den heutigen Täter*innen*

Im Laufe der letzten Jahre entdeckten zunehmend deutsche, suchtkranke Betäubungsmittelkonsumierende den Absatzmarkt des osteuropäischen Auslands für ihre Beschaffungskriminalität. Auch sie passen sich in der Auswahl der zu entwendenden Fahrrädern der Nachfrage aus dem Ausland an. Gleichzeitig entwickeln sich Anfänge strukturierten Vorgehens, ähnlich jenen der Bande: Es wird gemeinsam arbeitsteilig gehandelt und die Lagerung sowie Verbringung organisiert. Entweder werden noch in Deutschland die Fahrräder an Zwischenhändler*innen aus dem Ausland weiterverkauft oder das Diebesgut ins Ausland transportiert. Hierbei arbeiten deutsche und polnische Kriminelle verstärkt zusammen.

---

32 BKA 2019.

33 Schon allein der Nachweis des bandenmäßigen Vorgehens, insb. der Bandenabsprache, stellt in der polizeilichen Ermittlungsarbeit eine Herausforderung dar. Im Fall der hier beschriebenen Bande ist dies gelungen.

Dieser Umstand erschwert es den Ermittlungsbehörden zusehends, zwischen deutschen und ausländischen Täter*innen zu unterscheiden. In Zukunft sind weitere Herausforderungen für die kriminalpolizeiliche Ermittlungsarbeit sowie insbesondere die deutsch-polnische Zusammenarbeit der Ermittlungsbehörden zu erwarten.

### *3.4 Erkenntnisse über Fahrraddiebstähle in Oldenburg*

In der Stadt Oldenburg hatte und hat nach wie vor der Fahrradverkehr eine große Bedeutung. Als sich Ende der 70er Jahre die Zahl der Fahrraddiebstähle auf über 6000 summierte, machte dies einen erheblichen Teil aller bekannt gewordenen Straftaten aus. Um diesen Entwicklungen entgegenzuwirken, wurde Anfang der 80er Jahre ein Pilotprojekt eingeführt. Dieses bestand aus fünf Beamt*innen, die für eine zentrale Bearbeitung der Fahrraddiebstähle im gesamten Stadtgebiet zuständig waren. Aufgrund dieser zentralen Bearbeitung konnten schneller Tatzusammenhänge und Täter*innenprofile erkannt werden, was zu einer erheblichen Steigerung der Aufklärungsquote führte. Daher wurde die zentrale Bearbeitung verstetigt und die entsprechende Sachbearbeitung war teilweise sogar mit sechs Beamt*innen besetzt. Zudem wurde eine eigene Fahndungsdatei für Fahrraddiebstähle konzipiert, die auf die Besonderheiten von Fahrraddiebstählen ausgerichtet war und in der jeder Fahrraddiebstahl gespeichert wurde. So konnte festgestellt werden, dass 40-50 % der Personen, die einen Fahrraddiebstahl anzeigten, keine Rahmennummer angeben konnten. Um auch solche Fahrräder zuordnen zu können, konnten nun im Rahmen der Anzeige auch eine Beschreibung des Fahrrades angegeben werden. Nach der Einführung des Programms wurde nicht nur Zuordnung von entwendeten Fahrrädern effektiver durchgeführt, sondern es konnten auch leichter Zusammenhänge zwischen dem Wohnort der Täter*innen und aufgefunden Fahrrädern nachvollzogen werden. Weiterhin werden anhand des Programms Diebstahlschwerpunkte erkannt. Ferner wurden die Registrierung und die Präventionsarbeit von Fahrrädern stark vorangetrieben.

Durch die intensive Bearbeitung konnten die Fallzahlen bis 2020 auf ca. 1240 angezeigte Fahrraddiebstähle gesenkt werden. Die Aufklärungsquote konnte von ehemals 3 % auf 21% im Jahr 2020 gesteigert werden.

Die Polizei in Oldenburg geht allerdings davon aus, dass von einer erheblichen Dunkelziffer auszugehen ist. Vielfach können die Eigentümer*innen nachträglich festgestellt und informiert werden. Diese zeigen sich regelmäßig erstaunt, dass die Polizei ihr Rad sicherstellen konnte, obwohl sie keine Anzeige erstattet hatten. Als Grund für die fehlende Anzeige identifizierte die Polizei sechs Hauptaussagen:

„Ich bin ja selbst Schuld, ich habe mein Fahrrad ja nicht angeschlossen."
„Ich habe keine Versicherung, dann lohnt sicher keine Anzeige."
„Ich habe mein Fahrrad ja nicht vorher registrieren lassen."
„Die Aufklärungsquote der Polizei ist schlecht, wie man immer hört und liest."
„Das ist doch ein Massendelikt (oder auch Bagatelldelikt), dass bei der Polizei und Staatsanwaltschaft nicht beachtet und bearbeitet wird."
„Mein Fahrrad war kaum noch etwas wert. Da lohnt sich keine Anzeige."

Zudem kam es auch vor, dass Anzeigen als zu aufwendig angesehen wurden oder dass die Bestohlenen damit rechneten, dass die Fahrräder ohnehin nicht wiedergefunden würden, da diese alle ins Ausland verbracht würden.

## 4. Schlussfolgerungen

Die Täter*innen sowie deren Vorgehensweisen scheinen sich zu unterscheiden. Neben Beschaffungskriminalität und Gelegenheitstäter*innen gibt es auch beim Fahrraddiebstahl gewerbs- und bandenmäßige Strukturen. Vor allem die Vorgehensweise ist von den regionalen Besonderheiten abhängig (etwa der Nähe zur Bundesgrenze). Die Fahrraddiebstähle scheinen für die Täter*innen im Regelfall einfach zu begehen sein, da viele Fahrräder unzureichend gesichert sind. Eine Sensibilisierung der Bevölkerung für Sicherungsmaßnahmen wäre daher nach wie vor erfolgsversprechend.

Obwohl es sich beim Fahrraddiebstahl um ein Massendelikt handelt, ist letztlich ein Mangel an kriminologischen und kriminalistischen Erkenntnissen erkennbar. Das Dunkelfeld wird als groß eingeschätzt, da zahlreiche Delikte vermutlich nicht angezeigt werden.

Auch wurde deutlich, dass durch einzelne Täter*innengruppierungen beträchtliche Schäden verursacht werden können und dass diese Gruppierungen teilweise für einen Großteil der Delikte verantwortlich sind. Ein gezielter Einsatz von polizeilichen Kräften hätte vermutlich großen Einfluss auf die Entwicklung des Kriminalitätsphänomens.

Fahrraddiebstähle scheinen in erster Linie im städtischen Raum vermehrt aufzutreten. In mehreren Großstädten ist der Fahrraddiebstahl offenbar weit verbreitet, was auch auf die erhöhte Anonymität zurückgeführt werden kann. Zudem sind in Großstädten mehr Fahrräder vorhanden, die an bestimmten Orten gehäuft stehen (z.B. Hinterhöfe oder Fahrradparkplätze), sodass die Täter*innen leicht zahlreiche Fahrräder auf einmal stehlen können. Zudem lassen sich in größeren Städten leichter Vertriebsstrukturen für Diebesgut (Hehlerei) aufbauen und unterhalten. Jedoch ist nicht ausgeschlossen, dass Banden auch im ländlichen Raum agieren oder diesen zumindest mit einbeziehen. Dies trifft

insbesondere dort zu, wo abgelegene Objekte wie einzelnstehende Wohnhäuser oder Gehöfte günstige Tatgelegenheitsstrukturen bieten.

Zudem zeigte sich, dass suchtkranke oder als sozioökonomisch benachteiligt einzustufende Menschen des Öfteren an Fahrraddiebstählen beteiligt sind. Diese scheinen aber eher als ausführende Organe zu agieren. Entweder werden sie ausgenutzt, oder sie nutzen diese Möglichkeit, ihre Sucht zu finanzieren bzw. ihren finanziellen Status zu verbessern.

Offenbar gibt es kriminelle Strukturen mit Verbindung nach Osteuropa, wo Absatzmärke für gestohlene Ware aus Deutschland und anderen westlichen Ländern zu bestehen scheinen. Diese Strukturen weisen teilweise einen hohen Organisationsgrad auf, der in den beschriebenen Vorgehensweisen seinen Ausdruck findet.

Ein wesentlicher Faktor für kriminalpolizeiliche Ermittlungserfolge sind die polizeilichen Organisationsstrukturen. Nur wenn die Polizei systematisch bei ihren Ermittlungen vorging und die Gesamtsituation strategisch bewertete, konnte vertieftes Wissen über die Diebstähle gewonnen werden. Daher ist es bei Ermittlungen hinsichtlich gewerbs- und/oder bandenmäßiger Diebstähle zwingend erforderlich, dass die Delikte systematisch betrachtet und ausgewertet werden. Andernfalls sind Ermittlungserfolge allenfalls hinsichtlich lokal operierender Gruppierungen denkbar oder vom Zufall abhängig. Dem werden temporäre oder nur in einem begrenzten Umfang ermittelnde Polizeieinheiten nicht gerecht, da diese Gruppierungen anscheinend sowohl über die Grenzen der Bundesländer als auch der Bundesrepublik Deutschland agieren. Deshalb wäre der Ausbau der bundesländerübergreifenden Zusammenarbeit deutscher Polizeibehörden sowie der internationalen polizeilichen Zusammenarbeit empfehlenswert. Dazu gehören auch die Sachfahndungsmaßnahmen, die im europäischen Kontext zwar eine Vielzahl von Gegenständen (insbesondere Kraftfahrzeuge) berücksichtigen, jedoch keine gestohlenen Fahrräder. Eine reguläre grenzüberschreitende Fahndung nach gestohlenen Fahrrädern ist damit derzeit ausgeschlossen, das Entdeckungsrisiko für Straftäter*innen somit gering.

## Literaturverzeichnis

Bartenschlager, Christopher/Buchmin, Thomas/Dörrer, Linda/Hiendl, Laura/ Hoffmann, Maria/Michalowski, Lena/Ridel, Magdalena/Rieder, Marlene/Rückerl, Raphaele/Theimer, Theresa/Vogelmeier, Bettina/Müller, Henning (2020) Sicherheit von Frauen im öffentlichen Raum, in: https://epub.uni-regensburg.de/43430/ (letzter Aufruf: 01.12.2021).

Balschmiter, Peter/Roll, Holger (2016) Dunkelfelduntersuchung in Mecklenburg-Vorpommern – Teil II, Die Polizei, S. 222-232.

BKA (2019) Organisierte Kriminalität (OK), in: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html (letzter Aufruf: 03.04.2019).

Bock, Michael (2019) Kriminologie. Für Studium und Praxis. 5. Aufl., München: Verlag Franz Vahlen.

Church, Daniel/Birkel, Christoph/Leitgöb-Guzy, Nathalie (2020) Der Deutsche Viktimisierungssurvey 2017, Die Polizei, S. 293-300.

Eisenberg, Ulrich (2005) Kriminologie. 6. Aufl., München: Beck.

Gläser, Jochen/Laudel, Grit (2010): Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. 4. Aufl., Wiesbaden: VS Verlag.

Jitschin, Oliver (2002) Der Fahrraddiebstahl: ein Beitrag zur kriminologischen, kriminalpolitischen und strafprozessualen Problematik eines Delikts der Massenkriminalität, Göttingen.

Kunz, Karl-Ludwig/Singelnstein, Tobias (2021) Kriminologie. Eine Grundlegung. 8. Aufl. Stuttgart, Bern: utb.

Schwind, Hans-Dieter (1975) Dunkelfeldforschung in Göttingen 1973/74. Wiesbaden: Bundeskriminalamt.

Schwind, Hans-Dieter (1978) Empirische Kriminalgeographie, Wiesbaden.

Schwind, Hans-Dieter (1989) Dunkelfeldforschung in Bochum 1986/87, Wiesbaden: Bundeskriminalamt.

Schwind, Hans-Dieter (2016) Kriminologie. Eine praxisorientierte Einführung mit Beispielen. 23. Aufl. Heidelberg, Hamburg: Kriminalistik Verl.-Gruppe Hüthig Jehle Rehm.

*Hanno Brandt[1]/Christian Matzdorf[2]/Katharina Noeske[3]*

# Abläufe bei der polizeilichen Bearbeitung von Fahrraddiebstählen – bisherige Praxis und Varianten

## 1. Einleitung

Die Ablauforganisation der Polizei für ihreArbeit in der Strafverfolgung muss für eine Vielzahl unterschiedlich gelagerter Lebenssachverhalte standardisierte Modelle vorenthalten. Sie differenziert anhand von Kriterien wie der Schwere der Straftat, der Deliktsgruppe (Delikte am Menschen, Eigentumsdelikte u.a.), der Eilbedürftigkeit von polizeilichen Maßnahmen (hier spielen ggf. auch Aspekte der Gefahrenabwehr eine Rolle), aber auch dem Vorliegen von besonderen Umständen des Einzelfalls (wie beispielsweise Tatserienzusammenhänge, besondere Öffentlichkeitswirkungen und polizeiliche Priorisierungen). Die Ablauforganisation variiert darüber hinaus abhängig davon, auf welchem Weg die Polizei von der Straftat beziehungsweise des eine solche vermuten lassenden Sachverhalts Kenntnis erlangt. Im Wesentlichen sind dies die in diesem Beitrag dargestellten vier Wege. Die fünfte Möglichkeit ist die Kenntniserlangung durch Aktenzusendung seitens der Staats- oder Amtsanwaltschaft, dies kommt jedoch selten vor und ist für die Betrachtung der Arbeitsabläufe in der Praxis nachrangig.

In diesem Beitrag werden die typischen Abläufe bei der polizeilichen Bearbeitung von Diebstählen am Beispiel der Fahrraddiebstahlsbearbeitung der Polizei Berlin untersucht. So können die Wege der Kenntniserlangung in den Blick genommen und ein wesentlicher Teil der Differenzierungskriterien berücksichtigt werden. Die Aussagen dazu können – trotz der bei den Länderpolizeien individuell bestehenden Regelungen – als im Wesentlichen repräsentativ für die Arbeit anderer Länderpolizeien angesehen werden.

Hintergrund der Forschungsfrage: In welchen Schritten bearbeitet die Polizei Berlin Fahrraddiebstähle?, ist die für das FindMyBike-Projekt entscheidende Fragestellung: Über welche Schnittstelle lassen sich Zugangsdaten für

1 Hanno Brandt war in dem Projekt FindMyBike wissenschaftlicher Mitarbeiter für die rechtlichen Forschungsfragen.

2 Prof. Christian Matzdorf hat in dem Projekt FindMyBike kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

3 Katharina Noeske war in dem Projekt FindMyBike studentische Hilfskraft an der Hochschule für Wirtschaft und Recht Berlin.

GPS-basierte Positionsbestimmungen in den Bearbeitungsprozess einspeisen? Die Bearbeitung der hier betrachteten Straftat durch die Polizei beginnt zumeist mit der Feststellung des Diebstahls eines Fahrrades durch Eigentümer*innen bzw. rechtmäßige Nutzer*innen und deren Kontaktaufnahme mit der Polizei. Die Kenntniserlangung der Polizei begründet einen polizeilichen Ermittlungsvorgang mit weiteren Maßnahmen bzw. Bearbeitungsschritten; dem hier untersuchten Workflow.

Präventive Maßnahmen, wie sie insbesondere von Verkehrsbeauftragt*innen der Polizeiabschnitte und selten auch von der Präventionsdienststelle des Landeskriminalamtes Berlin (LKA) vorgenommen werden (Fahrradcodierung, Fahrradpass, Aufklärung über Sicherungsarten von Fahrrädern u.a.), sind nicht Teil dieser Betrachtung.

Die Polizei hat, wenn sie vom Diebstahl eines Fahrrads Kenntnis erlangt, zwei Funktionen. Sie versucht Tatverdächtige festzustellen und ggf. das Fahrrad als Beweismittel sicherzustellen. Neben diesen strafverfolgenden Maßnahmen zielen ihre Handlungen aber auch darauf ab, den mit dem Diebstahl eingetretenen rechtswidrigen Zustand und die darin liegende fortdauernde Verletzung der Rechte des Bestohlenen zu beenden; also Rückgewinnungshilfe zu leisten. Beide Ausrichtungen werden bei den herausgearbeiteten Workflows beachtet.

Der Beitrag skizziert, wie die Polizei von Fahrraddiebstählen Kenntnis erlangt und welche Workflows sich daran anschließen. Grundlage sind Expertengespräche sowie Erkenntnisse aus langjähriger polizeilicher Tätigkeit des Mitverfassers Matzdorf.[4]

## 2. Varianten der Fallbearbeitung

Vier relevante Wege der Kenntniserlangung werden hier unterschieden: über den Polizeinotruf („110“), über eine Online-Anzeige, durch eine sonstige Kenntnisnahme durch Polizeikräfte (insbesondere durch sogenannte eigene Feststellung, beispielsweise im Rahmen der Streifentätigkeit) und im Rahmen einer persönlichen Anzeige auf einem Polizeiabschnitt. Diese vier Varianten sind in den folgenden Abbildungen (Nr. 2-5) dargestellt. Zum besseren Verständnis fasst Abbildung Nr. 1 die vier Varianten zusammen und verdeutlicht die zentrale Rolle der Einsatzleitzentrale (ELZ) im Rahmen der Informationssteuerung.

4 Unter anderem sowohl in kriminalpolizeilicher Verwendung im Landeskriminalamt Berlin und innerhalb örtlicher Polizeidirektionen im Kriminalreferat als auch in schutzpolizeilicher Verwendung im Stab des Polizeipräsidenten und innerhalb örtlicher Polizeidirektionen in Polizeiabschnitten; jeweils in strategischer und taktischer Hinsicht u.a. mit Eigentumsdelikten befasst.

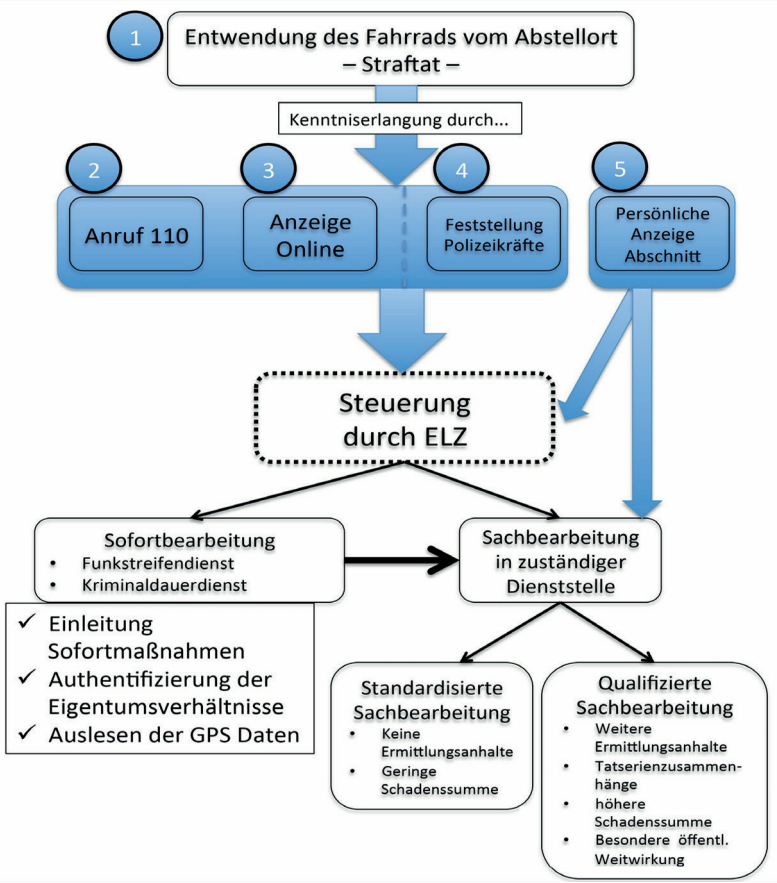


*Abbildung 1: Workflow der Fahrraddiebstahlsbearbeitung in der Polizei Berlin*[5]

5 Abbildung erstellt von Matzdorf, Noeske.

Nach der initialen Kenntniserlangung steuert grundsätzlich die ELZ die weitere Bearbeitung, indem sie den Ermittlungsvorgang[6] entweder zur Sofortbearbeitung an den Funkstreifendienst oder den Kriminaldauerdienst weiterleitet oder in zeitlich weniger dringenden Fällen der jeweils zuständigen sachbearbeitenden Dienststelle zuweist. Erhalten hingegen die Mitarbeiter*innen eines Polizeiabschnitts als erste Kenntnis von einem Fahrraddiebstahl (insbesondere bei persönlicher Anzeige auf dem Abschnitt), wird von dort aus in zeitlich nicht dringenden Fällen der Vorgang direkt an die zuständige Dienststelle zur Sachbearbeitung verwiesen, in akuten Fällen aber wiederum eine Einsatzsteuerung durch die ELZ veranlasst.

Die Sofortbearbeitung erfolgt also durch den Funkstreifendienst oder beim Vorliegen entsprechender Ermittlungsanhalte (wesentlich seltener) durch den Kriminaldauerdienst. Sie umfasst Maßnahmen wie das Anfahren des Tatorts, die Befragung (ggf. Vernehmung) von Zeugen, die Sicherung von Videomaterial und ggf. auch schon die Feststellung von Eigentumsverhältnissen. Nach Abschluss der Sofortmaßnahmen (die in seltenen Fällen auch Beschuldigtenermittlung und -vernehmungen, Durchsuchungsmaßnahmen, erkennungsdienstliche Maßnahmen und ggf. Einlieferungen/Vorführungen beim Bereitschaftsgericht u.a. beinhalten können) leitet der Funkstreifendienst bzw. der Kriminaldauerdienst den Vorgang an die zuständige Dienststelle zur Sachbearbeitung weiter. Die Maßnahmen des Funkstreifendienstes werden generell an die Leitung des Kriminaldauerdienstes kommuniziert.

Bei der Sachbearbeitung durch die zuständige Dienststelle lässt sich zwischen der sogenannten standardisierten und der qualifizierten Sachbearbeitung unterscheiden. Es bleibt bei einer standardisierten Sachbearbeitung, wenn es keine Ermittlungsanhalte gibt und die Schadenssumme verhältnismäßig gering ist. Hier wird die Fallbearbeitung regelmäßig bald eingestellt bzw. im Sinne von Ermittlungshandlungen gar nicht erst aufgenommen und der Vorgang der Amtsanwaltschaft zugeleitet, die dann das Ermittlungsverfahren einstellt. Qualifiziert, also zeitlich und inhaltlich intensiver, wird der Vorgang nur bearbeitet, wenn mindestens eines der folgenden Kriterien vorliegt:

- Hohe Schadenssumme
- Vorhandene Ermittlungsanhalte (beispielsweise bezüglich Täteridentitäten oder Tatserienzusammenhängen)
- Besondere öffentliche Weitenwirkung

6 Ein „Vorgang“ im engeren Sinne setzt die Anlage im polizeilichen Datenverarbeitungssystem POLIKS (Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung) voraus.

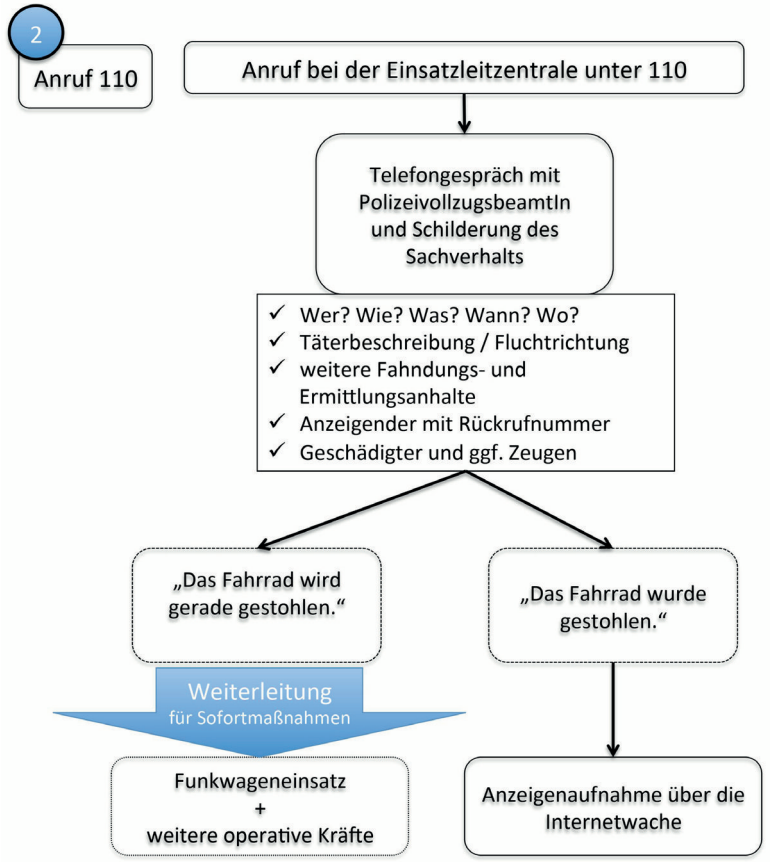


*Abbildung 2: Workflow der Fahrraddiebstahlsbearbeitung in der Polizei Berlin / Anruf über „110"*

Bei einer Kenntniserlangung über den Polizeinotruf werden im ersten Schritt Polizeivollzugsbeamt*innen in der ELZ, sich an den Fragen „Was? Wo? Wann? Wer? Wie?" orientierend, den Sachverhalt für eine Entscheidung über die nächsten Schritte aufklären. Standardmäßig werden Informationen zur Identität der Anrufenden (Rückrufnummer etc.), der Geschädigten und eventuellen Zeug*innen aufgenommen. Für die Entscheidung über die weiteren Schritte relevant sind aber insbesondere das Vorhandensein von Informationen bezüg-

lich der Täter*innen, über Fluchtrichtungen und sonstige Fahndungs- und Ermittlungsanhalte und – das wird zu Anfang geklärt – die Frage, ob der Fahrraddiebstahl gegenwärtig ist oder bereits der Vergangenheit angehört. Im ersten Fall („Fahrraddiebstahl gegenwärtig") sowie bei besonderen Konstellationen, werden grundsätzlich Sofortmaßnahmen (durch Funkstreifendienst und eventuell weitere operative Kräfte) eingeleitet. Wird lediglich über einen bereits geschehenen Diebstahl berichtet, so werden die Anrufenden in der Regel auf die Möglichkeit einer Internetanzeige verwiesen.

Über die Internetwache der Polizei Berlin[7], die bei der ELZ organisatorisch angebunden ist, lässt sich online eine Strafanzeige erstatten. Hierbei werden Anzeigende bei der Wahl des Menüfeldes „Anzeigen rund um das Fahrrad" zu den Feldern „Mein Fahrrad ist gestohlen worden" und „Von meinem Fahrrad sind Teile gestohlen worden" geführt. Nach Auswahl des passenden Feldes erfolgen rechtliche Hinweise und Belehrungen, es werden umfassende Angaben zum Sachverhalt erhoben, inklusive Angaben zum Tatobjekt, dem (möglichen) Tatablauf, den Anzeigenden und den Geschädigten. Schließlich lässt sich ein gegebenenfalls erforderlicher Strafantrag stellen, um das Strafverfolgungsinteresse der Geschädigten zu manifestieren.

Die derart erhobenen Informationen werden in der ELZ parallel zu den Notrufen (Ruf 110) zur Kenntnis genommen. In der Regel leitet die ELZ den Vorgang dann an den zuständigen Polizeiabschnitt beziehungsweise das zuständige Abschnittskommissariat zur Sachbearbeitung weiter. In Ausnahmefällen wird der Vorgang zur Sofortbearbeitung an den Kriminaldauerdienst gegeben. Aus den Sachverhalten mit Täter*innenhinweisen ergeben sich in seltenen Fällen weitere Zuständigkeiten, beispielsweise die einer kriminalpolizeilichen Dienststelle für Intensivtäter*innen, kiezorientierte Mehrfachtäter*innen und Schwellentäter*innen oder die des Landeskriminalamtes Berlin mit Zuständigkeit für größere Hehlereifälle oder Hehlerei mit Bezug zur sog. organisierten Kriminalität.

Wenn Polizeivollzugsbeamt*innen vor Ort auf den Diebstahl eines Fahrrades angesprochen werden oder sonst davon Kenntnis erlangen, werden gegebenenfalls unmittelbar Sofortmaßnahmen eingeleitet. Ansonsten werden die Strafanzeige aufgenommen und ein Vorgang angelegt (d.h. ein sogenannter „Anwendungsfall" im polizeieigenen Informations- und Vorgangsverwaltungssystem POLIKS eröffnet und mit den betreffenden Informationen gespeist). Hierbei werden die gleichen Informationen wie bei der Internetanzeige erhoben. Ebenfalls kommt es zu vergleichbaren rechtlichen Hinweisen und Belehrungen. Darüber hinaus können noch weitere Ermittlungsanhalte festgehalten werden. Es folgt, gesteuert über die ELZ, eine Weiterleitung an den Kriminal-

7 https://www.internetwache-polizei-berlin.de (letzter Aufruf: 13.04.2021).

dauerdienst zur Sofortbearbeitung oder an die zuständige Sachbearbeitungsstelle.

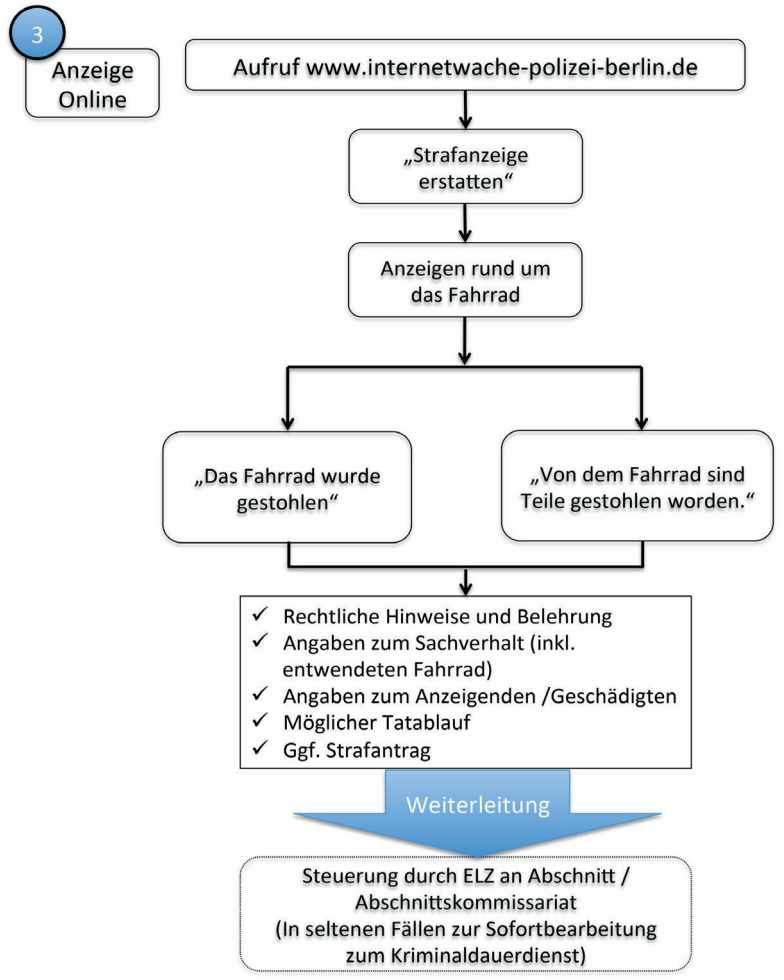


*Abbildung 3: Workflow der Fahrraddiebstahlsbearbeitung in der Polizei Berlin / Online Anzeige*

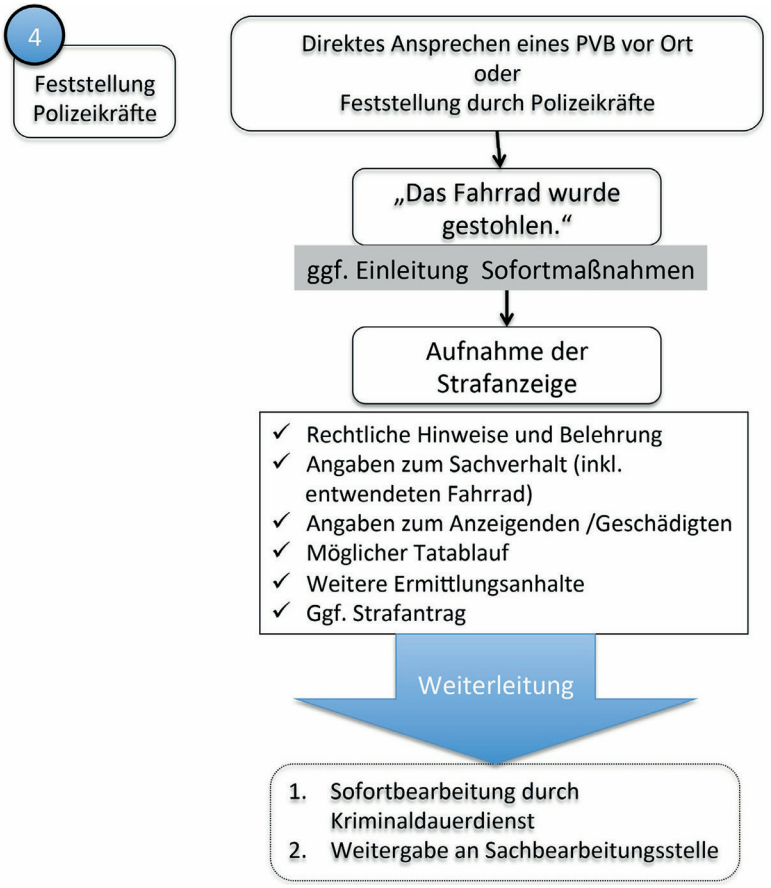


*Abbildung 4: Workflow der Fahrraddiebstahlsbearbeitung in der Polizei Berlin / Feststellung durch Polizeikräfte*

Teilweise erhält die Polizei Kenntnis von Fahrraddiebstählen, indem Betroffene eine Polizeidienststelle persönlich aufsuchen, um eine Strafanzeige zu erstatten. Inhaltlich unterscheidet sich diese nicht von der Anzeige über die Internetwache. Anders als bei der Anzeige gegenüber Polizeivollzugsbeamt*innen vor Ort entscheidet hier die die Anzeige aufnehmende Polizeikraft nach Aufnahme der Anzeige in Rücksprache mit zuständigen Vorgesetzt*innen darüber, ob es sich um einen der ELZ zuzuleitenden Fall handelt, der Sofortmaßnahmen verlangt,

oder der Fall dem Abschnittskommissariat im zuständigen Polizeiabschnitt zur Sachbearbeitung überlassen wird.

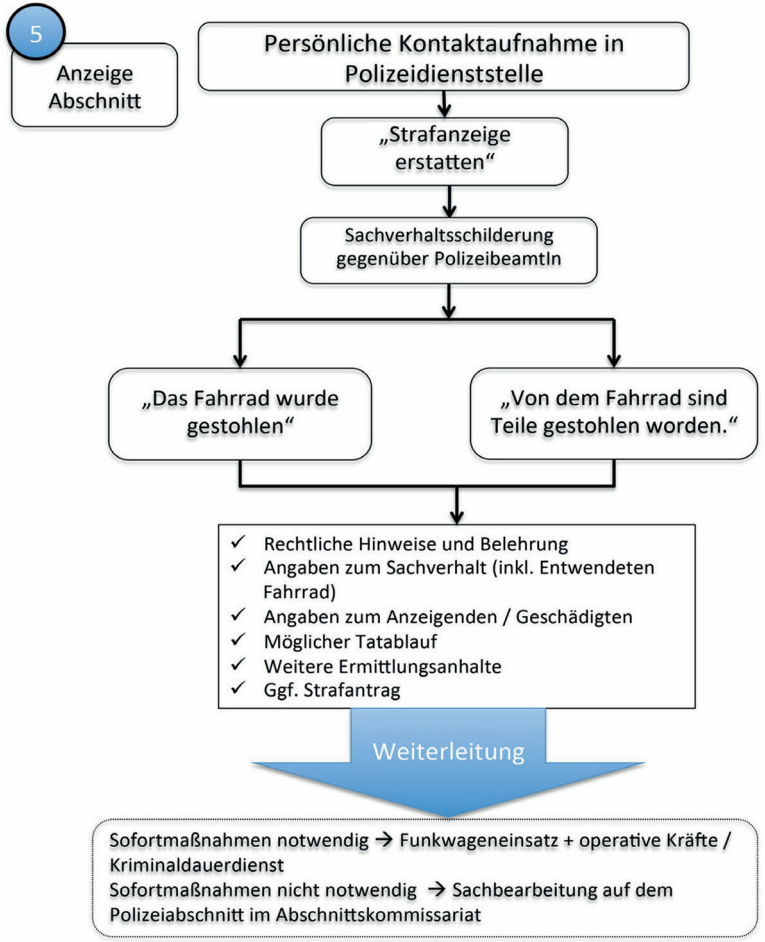


*Abbildung 5: Workflow der Fahrraddiebstahlsbearbeitung in der Polizei Berlin / Anzeige auf einem Polizeiabschnitt*

## 3. Fazit

Es gibt vier typische Wege, über die die Polizei von Fahrraddiebstählen Kenntnis erlangt. Der sich anschließende Workflow variiert abhängig von diesen Wegen sowie jeweils davon, ob der Diebstahl aktuell ist und Ermittlungsansätze vorhanden sind. Eine Gemeinsamkeit ist, dass die ELZ eine zentrale Stellung im Workflow einnimmt, insbesondere in Fällen mit der Notwendigkeit einer Sofortbearbeitung. Davon unbenommen ist die direkte Weiterleitung durch die erstbearbeitende Vollzugskraft an eine sachbearbeitende Dienststelle nach entsprechender Rücksprache. Hervorzuheben ist die Anzeige über die Internetwache, da diese bei Fahrraddiebstählen häufig verwendet wird und da bei anderen Wegen der polizeilichen Kenntniserlangung Hinweise auf die Möglichkeit einer Anzeigeerstattung per Internet erfolgen.

Die hier dargestellten Abläufe können in den meisten Länderpolizeien vorgefunden werden. Unterschiede bestehen lediglich in der Bearbeitungszuständigkeit (Schutz- oder Kriminalpolizei). In Flächenbereichen mit einer geringen Personalausstattung können zudem die Erstbearbeitung und die eigentliche Sachbearbeitung innerhalb einer Dienststelle erfolgen, was die grundsätzliche Gültigkeit der Darstellung jedoch nicht berührt.

*Sophie v. Stockhausen*[1]

# Trackingdaten und ihre Nutzung durch Fahrradflottenanbieter

## 1. Einleitung

Seit seiner Gründung im Jahr 2014 beschäftigt sich das Berliner Startup Noa Technologies mit der Entwicklung von Flottenmanagement-Lösungen für Fahrradflotten. Durch eine effizientere Verwaltung und Wartung der Leihfahrräder soll deren Praktikabilität und Attraktivität verbessert werden. Dafür wurde ein leistungsstarkes GPS-Tracking-Modul entwickelt, welches direkt am Fahrrad verbaut ist. Mit Hilfe einer selbst entwickelten Software-Lösung, kann jedes Rad dank exakter GPS-Standortbestimmungen in Echtzeit nachverfolgt werden. Dank dieser von Noa entwickelten Tracking-Lösung konnte die Verlustrate von Fahrrädern im laufenden Betrieb deutlich verringert werden. Für Noa Technologies entwickelte sich das System zur Prävention und Aufklärung von Fahrraddiebstählen als zusätzlicher Geschäftszweig. Dabei arbeitet die Firma eng mit der Polizei Berlin sowie der Beuth Hochschule für Technik Berlin und der Hochschule für Wirtschaft und Recht Berlin zusammen.

## 2. Generelle Anwendergruppen und Anforderungsprofile

In großen Städten beobachten wir einen wachsenden Bedarf an alternativen Mobilitäts-Angeboten. Neben dem Autoverkehr, dem öffentlichem Personennahverkehr (ÖPNV) und Carsharing-Angeboten, werden zunehmend Fahrradflotten im öffentlichen Raum verfügbar gemacht. Für Alternativen zum Autoverkehr ist vor allem die Erschließung der sogenannten *ersten und letzten Meile* wichtig, um ein möglichst nahtloses Verkehrsangebot bereitzustellen und es Pendler*innen zu erleichtern, auch kurze Wege autonom überbrücken zu können. Neben Angeboten für die breite Öffentlichkeit planen bzw. nutzen bereits einige Unternehmen neuerdings den Ausbau von Fahrradflotten für ihre Angestellten. Für deren Mitarbeitende ist das ein attraktives Zusatzangebot, das ihnen das Pendeln von und zum Arbeitsplatz, zu Kundenterminen sowie

1 Sophie v. Stockhausen vertrat in dem FindMyBike Projekt den unternehmerischen Projektpartner Noa Technologies

die Mobilität auf großen Firmengeländen erleichtert. Neben Zeitersparnis und Kosteneffizienz spielen aber auch die gesundheitsfördernden Aspekte des Fahrradfahrens eine Rolle, die einen zusätzlichen Vorteil darstellen.

Die Firma Noa Technologies hat ihren Hauptsitz in San Francisco, an der Westküste der Vereinigten Staaten. Sie entwickelte sich aus einer Vorgängerfirma, die ursprünglich ein elektronisches Schloss[2] zur Diebstahlsicherung von privat genutzten Fahrrädern entwickeln wollte. Im Frühjahr 2015 startete die Firma mit Großkonzernen im Silicon Valley erste Pilotprojekte zur Implementierung ihrer Hard- und Software-Produkte in Fahrradflotten. Dabei handelte es sich um Firmenfahrräder, die auf großen Firmengeländen zum Einsatz kommen. Die Firma Noa lieferte dabei sowohl die Hardware-Technologie als auch die nötige Software zum digitalen Flottenmanagement. Das von Noa entwickelte System bietet eine hohe Kompatibilität mit möglichst vielen Fahrradtypen und eine große Flexibilität für die Nachrüstung von Rädern. Es ist sowohl für frei zugängliche als auch für in sich geschlossene (definierte) Benutzerkreise nutzbar. Optional verfügt es über ein Bluetooth gesteuertes Speichenschloss, welches an das Tracking-Modul gekoppelt ist. Über eine Smartphone-Applikation kann die Nutzerin oder der Nutzer sich nicht nur den jeweils genauen Standort eines Fahrrads vom System anzeigen lassen, sondern auch den dynamischen Verleihvorgang ortsungebunden abwickeln.

Die auf die jeweiligen Kundenbedürfnisse zugeschnittenen Angebote für den Datenservice und die Flottenlösungen richten sich bislang nur an Geschäftskunden (*B2B*[3]). Für den operativen Einsatz steht den Flottenbetreibenden eine Cloud-basierte Software zur Verfügung, die sowohl auf dem Desktop als auch auf mobilen Endgeräten funktioniert. Derzeit entwickelt Noa eine Trackinglösung für Endverbraucher*innen (*B2C*), für die eine Kooperation mit einem Fahrradhersteller und einem Versicherer angestrebt wird.

### *2.1 Herausforderung und Bedarfsanalyse*

Obwohl Fahrräder im Vergleich zu anderen Verkehrsmitteln wie PKW, Busse und Bahnen günstig in der Anschaffung sind, gestaltet sich deren Verwaltung und Pflege im öffentlichen Einsatz vergleichsweise kostenintensiv, da sie baulich bedingte Schwachstellen besitzen, bisweilen an entlegenen Orten abgestellt werden und zudem ganzjährig im Freien stehen, wo sie nicht nur der Witterung, sondern auch Vandalismus und Diebstahl ausgesetzt sind.

2 Elektronische Schlösser (auch: Smart Lock) lassen sich durch Eingaben eines autorisierten Codes sperren oder entsperren. Zur Authentifizierung werden oft drahtlose Übertragungstechniken genutzt, die zudem den Versand entsprechender Benachrichtigungen erlauben.

3 B2B: englisch für Business-to-Business.

Neben der Vielzahl an typischen Problemen im Betrieb von Fahrradflotten stellt auch die Bereitstellung der benötigten Infrastruktur oftmals eine Herausforderung für öffentliche wie private Betreiber dar. Eine besondere Schwierigkeit bei den Kund*innen im Silicon Valley war beispielsweise der Wunsch der Unternehmen, dass die Fahrräder nicht abgeschlossen, sondern frei zugänglich sein sollten. Einige Unternehmen verzeichneten vor der Implementierung der Tracking-Technologie hohe Verlustraten, welche sich beispielsweise bei Google auf jährlich bis zu 70% beliefen. Nachdem dies anfangs noch durch Neuanschaffungen ausgeglichen wurde, überstiegen die zusätzlichen Investitionskosten aber schnell die verfügbaren Budgets. Um die hohen Investitions- und Betriebskosten in den Griff zu bekommen, wurde daher eine Lösung gesucht, welche die Verlustraten minimieren und zugleich eine maximale Flexibilität im Zugang zu den Fahrrädern (ohne Schlösser) ermöglichen konnte.

Die positiven Auswirkungen einer gut organisierten und bedarfsgerecht bereitgestellten Fahrradflotte liegen auf der Hand: In vielen Teilen der Vereinigten Staaten existiert nur ein unzureichendes Angebot an Öffentlichem Nahverkehr. So ist auch im Silicon Valley die überwiegende Mehrheit der Menschen auf das Auto angewiesen, woran auch ein vor Jahren eingeführtes Park & Ride System mit Bussen nur geringfügige Abhilfe schaffen konnte. Daher verbringen die Menschen dort täglich mehrere Stunden im Stau. Dank dem kalifornischen Engagement im Klimaschutz wurden endlich alternative Mobilitätskonzepte und Sharing-Angebote gefördert, was sich auch in einem Wandel des öffentlichen Transportwesens niedergeschlagen hat. Die lokale Infrastrukturpolitik achtet seitdem vermehrt auf den Aus- und Neubau von Radwegen und Abstellmöglichkeiten für Fahrräder.

### *2.2 Genauigkeit der GPS-Daten bei Fahrradflotten*

Bisher wurden Fahrradverleihsysteme üblicherweise stationsbasiert betrieben, um den logistischen wie finanziellen Aufwand für das Umstellen und die Wartung der Räder so gering wie möglich zu halten. Räder konnten also lediglich an festen Stationen entliehen und wieder zurückgegeben werden, wobei der Anbieter beziehungsweise Betreiber des Verleihsystems gewährleisten musste, dass Stationen mit einer ausreichenden Anzahl an Rädern bestückt und diese in einem verkehrssicheren sowie fahrbereiten Zustand sind.

In den letzten Jahren stieg die Nachfrage nach flexiblen, nicht stationsbasierten Fahrradflotten sowohl bei öffentlichen Anbietern als auch bei privatwirtschaftlich betriebenen Flotten. Durch intelligentes *Geofencing*[4] können die

4 Geofencing bezeichnet das automatisierte Auslösen einer Aktion durch das Überschreiten einer gedachten Begrenzung auf der Erdoberfläche oder in der Luft. In den meisten Fällen handelt es

Betreiber*innen im System von Noa virtuelle Zonen festlegen, in denen der Einsatz sowie das Abstellen der Fahrräder erlaubt sind. Damit kann ein wahlloses Parken und Verwenden der Fahrräder vermieden werden. Im Gegensatz zu stationsbasierten Systemen haben die Nutzerinnen bzw. Nutzer die Möglichkeit, das Fahrrad innerhalb der definierten Einsatzbereiche abzustellen oder auszuleihen. Bei zahlungspflichtigen Angeboten kann die Mietdauer auch nur dann beendet werden, wenn das Fahrrad in der dafür vorgesehenen Zone sachgerecht geparkt wurde. Dabei wird zwischen der *Service Area* (innerhalb der ein Fahrrad ausgeliehen und gefahren werden kann) und einer *Drop Zone* (der Ausleih- und Rückgabe-Zone) unterschieden. Andere Anbieter von Fahrradverleihsystemen haben ebenfalls GPS-Sender an ihren Verleih-Fahrrädern verbaut. In den meisten Fällen werden dabei lediglich Start- und Endpunkt der Mietzeit erfasst und während restlichen Mietzeit die GPS-Lokalisierung ausgesetzt, um Strom zu sparen.

Wirksames Geofencing erfordert präzise Angaben der GPS-basierten Standort- sowie Trackingdaten, die in kurzen Intervallen aktualisiert werden müssen. Nur dann können die Daten sowohl beim Betreibenden als auch beim Nutzenden einen tatsächlichen Mehrwert erlangen. Viele Anbieter von gebührenpflichtigen Fahrradverleihsystemen nutzen für die Standortermittlung die Lokalisierungsdaten des Smartphones der Nutzerinnen bzw. Nutzer bei der Beendigung des Leihvorganges. Diese Daten sind aber häufig ungenau. Ebenso verhält es sich mit einem Großteil der GPS-basierten Tracking-Systeme, welche nur grobe Positionsdaten in vergleichsweise großen zeitlichen Abständen übermitteln. Dabei ist für die Betreiber*innen der Fahrradflotten eine möglichst exakte Bestimmung des Standorts entscheidend, weil bei offenen Systemen die Nutzerinnnen oder Nutzer lediglich gebeten, oftmals aber gar nicht dazu angehalten werden, den jeweils ermittelten Abstellort nochmals zu überprüfen. Somit sind die Betreiber*innen darauf angewiesen, falsch oder ungünstig geparkte Räder möglichst genau lokalisieren zu können, um diese gegebenenfalls umzupositionieren. Damit dies effizient und zeitsparend erledigt werden kann, ist die genaue Standortbestimmung von zentraler Bedeutung. Zu welchen Problemen es führt, wenn die Standortdaten von Flottenfahrrädern ungenau sind, kann man in vielen Großstädten beobachten, wo ungünstig und schwer lokalisierbare Leihfahrräder oftmals wochenlang verwaist herumstehen und somit weder vom Betreibenden noch von potentiellen Nutzer*innen gefunden werden. Derart vernachlässigte Räder verursachen auf Betreiberseite nicht nur wirtschaftliche Ausfälle, sondern tragen auch zu einem erhöhten Risiko von Vandalismus oder Diebstahl bei.

---

sich um geschlossene Bereiche, so dass zwischen innen und außen unterschieden werden kann; s.a.: https://de.wikipedia.org/wiki/Geofencing (letzter Aufruf: 20.07.2023).

Ein GPS-Tracking-Modul zu entwickeln, welches den Ansprüchen moderner Fahrradverleihsysteme gerecht wird, stellte für die Ingenieure eine Herausforderung dar. Die Genauigkeit des GPS-Signals sollte unter guten Bedingungen bei weniger als fünf Metern liegen, um eine präzise Lokalisierung zu gewährleisten. Darüber hinaus war bei der Installation des Tracking-Senders darauf zu achten, dass dieser einerseits gut versteckt und sicher am Fahrrad verbaut ist, andererseits aber auch eine hervorragende Sendeleistung bietet. Außerdem musste die Batterieleistung so bemessen sein, dass sie das gesamte System auch in Ruhephasen mindestens 60 Tage lang mit der nötigen Energie versorgen kann. Sobald das Fahrrad bewegt wird, sollte die Batterie innerhalb kurzer Zeit wieder aufgeladen werden. Langlebigkeit sowie Hitze- und Kältebeständigkeit (für den Einsatz bei extremen Witterungsverhältnissen) sind bei der Entwicklung von Fahrradkomponenten ohnehin selbstverständliche Maßgaben.

Im folgenden Kapitel soll auf konkrete technische Spezifikationen sowie die Umsetzung der Flottenmanagement-Lösung genauer eingegangen werden.

## 3. Systembeschreibung

### *3.1 Hardware*

Als Diebstahlsicherung sind inzwischen zahlreiche Tracking-Lösungen für Fahrräder erhältlich (s. Abschnitt 2). Doch nur wenige eignen sich tatsächlich für nachhaltige oder präventive Maßnahmen gegen den Fahrraddiebstahl. Eine Grundvoraussetzung für ein qualitativ aussagekräftiges GPS-Tracking ist die oben beschriebene Genauigkeit der Standort- und Bewegungsdaten. Dabei muss das Sendemodul so am Fahrrad verbaut werden, dass es bei maximaler Sendeleistung nicht leicht wieder zu entfernen ist und zudem eine optimale Stromversorgung hat. Dies wurde von den Ingenieur*innen erst durch intensive Entwicklungsarbeit und zahlreiche Testreihen erreicht. Die Tracking-Einheit nutzt den fahrradeigenen Nabendynamo als Stromquelle, schon nach einer kurzen Fahrt von 10 bis 20 Minuten ist der eingebaute Akku wieder voll aufgeladen. Neben der bereits erwähnten Hitze- sowie Kältebeständigkeit aller verbauten Materialien war die Entwicklung einer möglichst leistungsstarken und gleichzeitig wartungsarmen Bewegungs- und Beschleunigungssensorik eine weitere Herausforderung. Außerdem sollte das System eine größtmögliche Kompatibilität zu typischen Baureihen sämtlicher Fahrradhersteller aufweisen, um auch bereits bestehende Flotten mit der Technologie nachrüsten zu können.

Über ein zusätzliches GSM-Modul in der Tracking-Einheit werden heute alle am Rad erhobenen Informationen an das Backend des Cloud-Servers übermittelt, von wo aus die Daten dann weiterverarbeitet und im Frontend

einer Flottenmanagement-Software (FMS) abgebildet werden. Der Flottenbetreibende kann zur Verwaltung der Räder entweder die von Noa angebotene Flottenmanagement-Software oder eine Schnittstelle (API[5]) nutzen, um die Datenpakete in eine andere Frontend-Software zu integrieren. Auf diese Weise wird sichergestellt, dass die Kund*innen für das Flottenmanagement sowohl die von uns angebotene Software mit ihrem eigenen Firmenbranding als auch mit bereits in ihrem Betrieb vorhandenen IT-Systemen nutzen können.

### *3.2 Firmware*

Für die Verbindung zwischen der im Fahrrad verbauten Hardware und der Software-Anwendung für das Flottenmanagement ist eine entsprechende Firmware nötig. Es handelt sich dabei um eine spezielle Software, die für bestimmte Aufgaben einer aus verschiedenen Modulen bestehenden Hardware programmiert wird. Dieses sogenannte *Embedded System*[6] kann in den meisten Fällen nur durch ein spezielles Verfahren überschrieben werden und ist in den von Noa entwickelten Geräten vorinstalliert (*pre-embedded*). Die Firmware verarbeitet alle vom GPS-Modul empfangenden Signale, macht Angaben zum Batterieladezustand und weiteren intelligenten Sensoren, verpackt diese in entsprechende Datenpakete und sendet Informationen über das GSM-Netz an das Backend. Aus den dort ankommenden Daten können wiederum für das Flottenmanagement relevante Informationen abgeleitet werden, wie zum Beispiel Positions- und Bewegungsdaten oder nützliche Angaben über die Kapazitätsauslastung einer bestimmten Fahrradflotte.

Die speziell für diesen Anwendungsfall entwickelte Firmware kann als Alleinstellungsmerkmal der Noa-Lösung angesehen werden. Sie trägt wesentlich zur Genauigkeit der Positionsdaten, der enormen Strapazierfähigkeit des Systems und der geringen Ausfallrate der Geräte bei. Welche Algorithmen dabei Anwendung finden, kann an dieser Stelle nicht weiter erörtert werden.

Üblicherweise merkt man als normaler Anwendende dem fertigen Produkt nicht mehr an, wie viele Arbeitsschritte (vom Bestücken einer Leiterplatine bis zum Einbau auf engstem Raum) in einem Tracking-System stecken – letztlich auch, weil es versteckt platziert und unscheinbar ist, denn der Anwender bzw. die Anwenderin kommen damit nie in Berührung. Dabei ist es oftmals gerade die Firmware, welche bei elektronischen Geräten mit ihren ausgereiften Algorithmen den entscheidenden Wettbewerbsvorteil des Endproduktes ausmacht.

---

5 API: Application Programming Interface = Programmierschnittstelle.

6 Embedded System: ein auf einen Festwertspeicher (ROM, Flash-Speicher) „eingebranntes" Computerprogramm, das alle auf einer Leiterplatine verbauten, daten-generierenden Komponenten kontrolliert, koordiniert und überwacht.

### *3.3 Flottenmanagement Software (FMS)*

Mit der Flottenmanagement-Software können die Betreibenden ihre Fahrradflotte verwalten. Sie enthält verschiedene Funktionalitäten: So können beispielsweise in der Kartenansicht in Echtzeit (dank Live-Daten) alle im System registrierten Fahrräder an ihren genauen Standorten mit aktuellen Zeitstempeln (der letzten Datenübertragung) angezeigt werden. Ebenso kann überprüft werden, wie viel die Räder insgesamt (oder in einem bestimmten Zeitraum) gefahren sind und welchen Ladezustand die Batterie aufweis. Für eine effiziente Wartung sowie für das Wiederauffinden verlorener oder gestohlener Fahrräder können hier auch Informationen zum Fahrradtyp (inklusive Foto), Rahmen- oder Seriennummern und Angaben zu den Besitzer*innen hinterlegt werden. In der Kartenansicht können auch die für das Geofencing benötigten Park- und Einsatzzonen definiert werden (s. Abschnitt 2.2).

Neben den Kartenansichten gibt es für die Verwaltung sämtlicher registrierter Nutzerinnen bzw. Nutzer und Fahrräder weitere Module, welche die übrigen Daten abbilden. Durch das Erstellen von konditionalen Benachrichtigungen kann der Betreibende leicht festlegen, wer beispielsweise im Falle eines außerhalb der Parkzone abgestellten oder eines nicht sachgemäß verschlossenen Fahrrades je nach Region zu benachrichtigen ist. Sobald die Bewegungssensoren melden, dass sich ein Fahrrad mit untypischer Geschwindigkeit bewegt, kann sich der Betreibende einen Alarm schicken lassen. Bei zu hoher Geschwindigkeit kann hier der Schluss gezogen werden, dass das betroffene Fahrrad in einem PKW oder Lieferwagen geladen und eventuell gerade entwendet wird.

Das funktionale Herzstück der Flottenmanagement-Software bildet das sogenannte Dashboard. Es bildet sämtliche Parameter der gesamten Flotte entsprechend gewünschter Wertebereiche grafisch ab, um einen schnellen Überblick über die „vitalen Funktionen" – also den laufenden Betrieb – zu erlangen. Davon ausgehend bietet es die Möglichkeit, tiefere Einblicke in einzelne Details vornehmen zu können.

#### *3.3.1 Datenauswertung und Data Science als Flottenlösung*

Die reine Darstellung von Echtzeit-Tracking-Daten in einer Flottenmanagement-Anwendung bringt noch keinen Mehrwert, solange der jeweilige Betreibende diese Informationen nicht für sich zu nutzen weiß. Erst die Kombination aus aktuellen Positions- und Bewegungsdaten erlaubt es, im Verlustfall wirksame Gegenmaßnahmen zu ergreifen. Die Analyse sämtlicher Daten des Flottenmanagement-Systems fördert weitere Erkenntnisse zu Tage: Daraus lassen sich beispielsweise Erkenntnisse über häufig gefahrene Strecken zu bestimmten

Uhrzeiten, über die Ansammlungen von Fahrrädern an bestimmten Bahnhöfen (etwa am Freitagabend) oder die durchschnittlich benötigte Verteilung von Fahrrädern am Montagmorgen gewinnen. Solche Daten(analysen) sind die Grundlage für eine *vorausschauende Re-Distribuierung* und *bedarfsgerechte Bereitstellung* von Fahrrädern innerhalb der Flotte. Die über einen gewissen Zeitraum gesammelten Datensätze werden durch ein Team von Datenanalysten ausgewertet. Idealerweise entsteht daraus eine klare Prognose, zu welchem Zeitpunkt und an welcher Stelle man eine gewisse Anzahl Fahrräder zur Verfügung stellen muss, damit das System maximal ausgelastet und mit größtmöglicher Effizienz betrieben werden kann.

Um die Verlustraten bei frei verfügbaren Flotten zu minimieren, ermitteln die Datenanalyst*innen auch jene Zonen, die ein besonders hohes Diebstahlrisiko aufweisen. Damit lassen sich Folgeschritte automatisieren, wie zum Beispiel individuelle Warnungen an die Nutzerin bzw. den Nutzer (über einen Push-Dienst), um vom Abstellen in einer gefährlichen Zone abzuraten. Durch intelligente Datenanalyse können die Aufklärung von begangenen Diebstählen und deren Vermeidung (durch Prävention) langfristig miteinander verknüpft werden.

Die Visualisierung der Daten in übersichtlichen Schaubildern oder Heatmaps[7] ist für Anwender*innen- und Kund*innenkreise besonders hilfreich, da auf Grundlage dieser Informationen eigene Entscheidungen abgeleitet werden können. Dabei geht es nicht nur um die bedarfsgerechte Bereitstellung der Räder, sondern auch um die Planung der Infrastruktur auf dem Firmengeländen oder im Stadtbild. Durch das zusätzliche Einspeisen der während der Wartung erhobenen Daten in das System lassen sich zudem auch die Qualität und die durchschnittliche Lebensdauer einzelner Fahrradkomponenten kontrollieren. In Kombination mit weiteren Daten, beispielsweise zu klimatischen Bedingungen oder zur Nutzungsart, lassen sich Wartungs-Engpässe vorausschauend vermeiden.

Hinzu kommt, dass Daten über das Fahrverhalten (etwa gefahrene Kilometer insgesamt, pro Tag oder pro Fahrrad), sowie die durch die Fahrradnutzung eingesparte Zeit oder die positive $CO_2$-Bilanz (im Vergleich zu einer PKW-Nutzung) gezielt ausgewiesen werden können. Die Datenauswertung kann dabei je nach Problemstellung individuell an die Bedürfnisse der Betreibenden angepasst werden und ihnen damit wichtige Zusammenhänge aufzeigen bzw. hilfreiche Hinweise und Handlungsempfehlungen liefern.

7 Heatmap: Eine farbige Darstellung in Diagrammform zur Visualisierung von Daten um eine zweidimensionale Definitionsmenge abzubilden.

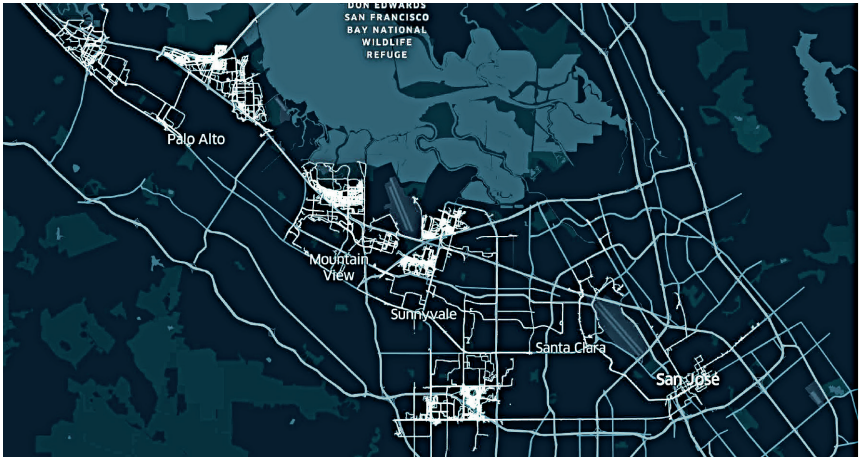


*Abbildung 1: Heatmap-Übersicht verschiedener Fahrradflotten aus dem Silicon Valley, Kalifornien (Stand: Februar 2019). Dargestellt sind diejenigen Gebiete, in denen die Fahrradnutzung besonders hoch ist.*

### *3.4 Applikationen für Smartphone und Tablet*

In der Desktop-Version der Flottenmanagement-Software erhält der Betreibende alle Funktionen auf einen Blick angezeigt. Da im mobilen Einsatz viele der verfügbaren Funktionen erfahrungsgemäß nicht benötigt werden, lässt sich der Umfang der mobilen Applikation (die überwiegend auf Smartphones und Tablets genutzt wird) entsprechend anpassen. Relevant sind hier meist nur die Positionsdaten für die bestmögliche Verteilung und etwaige Um-Positionierungen der Fahrräder sowie Informationen über deren Reparatur- und Wartungsbedarf, welche entsprechend reduziert und nutzerfreundlich abgebildet werden.

Für die Endanwender*innen steht eine eigenständige Smartphone-Applikation zum Download bereit, welche bedarfsweise sowohl die mitgelieferten Fahrradschlösser entriegeln kann, als auch Bezahlsysteme für klassische Mietmodelle beinhaltet. Nach der Installation der Applikation und der einmaligen Registrierung kann sich die Anwenderin bzw. der Anwender mit der App im System anmelden und das vom Betreibenden konfigurierte Angebot nutzen. Eine Kartenansicht zeigt eingangs gleich die verfügbaren Flottenfahrräder in der unmittelbaren Umgebung, etwaige Begrenzungen des Einsatzgebietes sowie die Abstell-Zonen an, sofern diese vom Betreibenden via Geofencing vor-

gegeben wurden. Je nach Konfiguration des Angebots können beispielsweise Warnungen über nicht korrektes Parken oder über die anfallenden Nutzungskosten als Push-Nachrichten informieren.

Als Zusatzfunktion bietet die App knappe Statistiken über die zurückgelegte Strecke und die gefahrenen Kilometer pro Zeit. Über die „Feedback-Funktion" kann die Nutzerin oder der Nutzer Probleme oder Wartungsbedarf samt Foto am Fahrrad melden, welche in der Verwaltung mit einem Bonus in Form eines Nutzungs-Guthabens für die damit verbundenen Mühen honoriert werden können.

Die von der Beuth Hochschule eigens für das FindMyBike-Projekt entwickelte Lösung mit einer Daten-Schnittstelle zur Polizei wird an anderer Stelle[8] genauer beschrieben.

## 4. Schlussbemerkung / Ausblick

Die Nachfrage nach cleveren Flottenmanagement-Lösungen, welche die oben genannten Anforderungen erfüllen und eine vorausschauende Datenanalyse ermöglichen, steigt. Mit dem zu erwartenden Ausbau der Netze und einer besseren Netzabdeckung sowie den höheren Datenübertragungsraten durch den kommenden 5G-Standard steht der weiteren Entwicklung von Anwendungen für das „Internet der Dinge" nichts im Wege.

Angesichts des Pionier-Geistes amerikanischer Technologie-Unternehmen, welche sich seit Jahren mit großem Interesse an der Weiterentwicklung und Verfügbarmachung von Mobilitäts-Konzepten beteiligen, können wichtige Entwicklungen erst auf dem US-Markt entwickelt werden. Hierzulande ist die Nachfrage von Firmenkunden und privaten Endverbrauchern nach einem wirksamen Schutz vor Fahrraddiebstählen ungebrochen hoch, zugleich steigt die Nachfrage nach Lösungen zur Verbrechensaufklärung. Bisher haben aber weder die größeren Konzerne noch die Fahrradhersteller ein gestiegenes Interesse an der Implementierung von erweiterten, Tracking-basierten Diebstahlsicherungen erkennen lassen. Deshalb braucht es die Zusammenarbeit mit kleinen und mittelständischen Fahrradherstellern, um ein entsprechendes Produkt für den Endverbrauchenden auf den Markt zu bringen.

Es ist mit Sicherheit davon auszugehen, dass in den kommenden Jahren auch sogenannte *Smartbikes*[9] - mit dem Internet verbundene Fahrräder, die auf die eine oder andere Weise getrackt werden können – auf den Markt

8 Vgl. Vollmar/Görlitz/Kober in diesem Band, S. 227ff.

9 Smartbike: darunter versteht man mit dem Internet verbundene Fahrräder, die entweder GPS-Tracking oder GSM-Technologie direkt in das Fahrrad verbauen.

kommen. Deshalb ist es an der Zeit, die gesellschaftliche Auseinandersetzung mit den sich daraus ergebenden Implikationen voranzutreiben, um zu einer verträglichen gesetzlichen Regulierung zu kommen. Dabei geht es sowohl um die Fragen, wer zum Zugriff auf die Tracking-Daten berechtigt ist, wer diese weiterverarbeiten darf –(beispielsweise zum Erstellen von Profilen für Marketingzwecke), aber auch, wann und wie diese zur Aufklärung von Straftaten (etwa im Falle eines Diebstahls) genutzt werden dürfen.

Es liegt auf der Hand, dass bestimmte Daten auch das Interesse von weiteren Akteuren (beispielsweise von Versicherungen oder Dienstleistern) wecken. Deshalb zeichnet sich bereits heute ein ähnlich breiter Bedarf an einer gesellschaftlichen Debatte über den Umgang mit diesen Daten und eine entsprechende gesetzliche Regulierung ab, wie dies bereits bei der Entwicklung selbstfahrender Automobile sichtbar wurde.

Gemeinsam mit unterschiedlichsten Unternehmen in Europa hat Noa Technologies in den vergangenen Jahren die Erfahrung gemacht, dass eine steigende Zahl moralischer, ethischer sowie noch offene rechtliche Fragestellungen im Umgang mit erhobenen Daten nicht mehr vom Tagesgeschäft zu trennen sind und daher nach detaillierten Antworten verlangen. Nicht erst seit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 ist die Frage nach dem richtigen Umgang mit gesammelten Daten im Allgemeinen, und dem Schutz personenbezogener Daten im Bereich des *Internets der Dinge* im Besonderen, zum Sorgenkind unter Anbietern wie Anwenderinnen und Anwendern geworden. Das rasante Entwicklungstempo im Bereich digitaler Dienstleistungen und Angebote hat in den vergangenen Jahren zahlreiche Lücken in den rechtlichen Regelwerken hinterlassen, welche nun mit Bedacht und realistischen Vorschlägen zu schließen sind. Studien und Forschungsprojekte wie FindMyBike tragen nicht nur dazu bei, Diskussionsbedarfe und Regulierungslücken in realistischen Szenarien aufzudecken; durch den Austausch zwischen wirtschaftlichen, wissenschaftlichen und gesellschaftlichen Akteurinnen und Akteure helfen sie auch, zentrale Regelungsbedarfe für die notwendigen rechtlichen Regeln im Umgang mit neuen Technologien zu identifizieren und konkrete Regulierungsvorschläge zu entwickeln. Ohne die Unterstützung durch Forschung und Hochschulen wäre eine derart umfangreiche Transferleistung von kleinen Unternehmen allein nicht zu leisten. Im Sinne einer aufgeklärten, gesellschaftlichen Teilhabe an der Ausgestaltung neuer Technologien ist jene Art von projektbezogener Zusammenarbeit unverzichtbar.

*Martin Scholz[1]/Gudrun Görlitz[2]*

# Räumliche und zeitliche Verdichtungen von Fahrraddiebstählen durch Visualisierungen mit Markern oder als Heatmap auf interaktiven Karten

## 1. Einleitung

Straftaten, auch Fahrraddiebstähle, sollen nicht nur verfolgt, sondern bereits im Vorfeld verhindert werden. Gelingt es die Vorgehensweise krimineller Banden und typischer Einzeltäter*innen zu erfassen, können Vorhersagen zu möglichen Diebstählen getroffen und Diebstähle dadurch vorgebeugt werden. Bei entsprechender Sensibilisierung der Radbesitzer*innen helfen geeignete Präventionsmaßnahmen, Fahrraddiebstähle zu erschweren und zu verhindern.

Die Vorhersage von Straftaten basiert auf der Auswertung historischer Deliktsdaten vergleichbarer Straftaten. Die Computertechnik ist heutzutage mittels verschiedener softwaregestützter Vorhersagemodelle und visueller Darstellungen in der Lage praxistaugliche Hilfsmittel für den Polizeieinsatz zur Verfügung zu stellen. Die Datenvisualisierung erfolgt mit Hilfe mathematischer Algorithmen. Zur Anwendung kommen dabei Visualisierungen mittels Markern und Heatmaps. Heatmaps sind zweidimensionale Abbildungen, ähnlich den Aufnahmen von Wärmebildkameras. Heatmaps ermöglichen einen schnellen Überblick über große Datenmengen. Eine Farbkodierung lässt Diebstahlschwerpunkte deutlich erkennen.

## 2. Zielstellung

Ziel ist die Konzeption und Umsetzung einer prototypischen Webanwendung zur Visualisierung von Trackingdaten gestohlen gemeldeter Fahrräder auf einer interaktiven Karte für Berlin. Damit soll der zuständigen Polizei die Möglichkeit gegeben werden, Standorte und Transportwege dieser Fahrräder effektiv zu erfassen und nachzuvollziehen. Ausgegangen wird von der These, dass eine solche kartografische Sichtbarmachung zeitlicher und räumlicher Häufung von Diebstählen einen Mehrwert für die präventive Polizeiarbeit bringt. Anonymi-

1 Martin Scholz hat seine Bachelorarbeit begleitend zum Projekt FindMyBike geschrieben.
2 Prof. Dr. Gudrun Görlitz hat das Projekt FindMyBike für den Bereich Informatik geleitet.

sierte GPS-Trackingdaten werden so in einer Webanwendung visualisiert, dass Gegenden und Zeiten mit hoher Diebstahldichte schnell erkannt werden können und damit eine Entscheidungshilfe für polizeiliche Präventionsmaßnahmen zur Verfügung steht. Solche Maßnahmen können Hinweise auf Diebstahl-Hotspots im öffentlichen Raum oder eine Erhöhung der Polizeipräsenz an einschlägigen Orten und zu diebstahlintensiven Zeiten sein. Die Darstellung des Endpunktes eines Fahrrad-Tracks gibt Aufschluss über die aktuelle Position des identifizierten Fahrrades. Anhand der Position kann ein gestohlen gemeldetes Fahrrad aufgefunden werden.

Die Webanwendung soll so personalisiert werden können, dass zwischen verschiedenen Darstellungsformen (Marker, Heatmaps und Marker-Cluster) gewählt werden kann. Die Eingabe von Zeitabschnitten lässt unterschiedliche Fahrraddiebstahlaktivitäten an bestimmten Tagen oder Tageszeiten sichtbar werden. Eine Datenauswertung in Form eines Warnhinweises soll zusätzliche Informationen liefern. Die Benutzerin oder der Benutzer wird beim Start der Anwendung informiert, wenn ein beliebig einstellbarer Schwellenwert (z. B. Zahl der Diebstähle im Zeitraum der letzten sieben Tage) überschritten wird.

Die Basis der Anwendung ist eine Datenbank mit den GPS-Trackingdaten gestohlen gemeldeter Fahrräder. Die Kartierung soll es ermöglichen, Diebstahlswahrscheinlichkeiten kleinräumig zuzuordnen.

## 3. Prävention Fahrraddiebstahl

Unterschiedliche Strategien und Konzepte, die im Folgenden vorgestellt werden, helfen Fahrraddiebstählen vorzubeugen.

### *3.1 Fahrradsicherung*

Zur Verhinderung von Fahrraddiebstählen tragen die Eigentümer*innen durch eine geeignete Sicherung ihrer Fahrräder bei. Der Allgemeine Deutsche Fahrrad Club (ADFC)[3] und die Polizei informieren auf ihren Webseiten aktuell über Sicherungskonzepte für Fahrräder. Die Polizei betreibt ein bundesländerübergreifendes Webportal „Polizeiliche Kriminalprävention der Länder und des Bundes“[4], um die örtlichen Polizeibehörden online und mit Flyern bzgl. der Sicherung von Fahrrädern zu unterstützen.

3 ADFC, o.J.

4 Polizeiliche Kriminalprävention der Länder und des Bundes, 2021.

### *3.1.1 Anschließen von Fahrrädern*

Die Polizei berät in ihrem Webportal „Polizeiliche Kriminalprävention der Länder und des Bundes“, dass Fahrräder mit „stabilen Bügelschlössern und Panzerkabeln […] am Rahmen und an beiden Rädern an einem festen Gegenstand“ angeschlossen werden sollen.[5]

An manchen Diebstahlschwerpunkten weisen auf den Boden gesprühte Piktogramme auf die Gefahr des Fahrraddiebstahls hin und erinnern an das Sichern von Fahrrädern.

### *3.1.2 Fahrradcodierung und Fahrradpass*

Bei der Fahrradcodierung wird nach Vorlage eines Eigentumsnachweises ein alphanumerischer Code mit einem ablösegesicherten Klebeetikett angebracht oder in den Rahmen eingeprägt. Die personenbezogene Codierung enthält die verschlüsselte Anschrift anhand derer die Polizei und Fundbüros den Eigentümer bzw. die Eigentümerin des Fahrrads feststellen können. Eine Fahrradcodierung erschwert den Weiterverkauf eines gestohlenen Rades und trägt zur Senkung der Diebstähle bei.[6][7]

Die Fahrradcodierung wird zusätzlich zu den von den Herstellern eingestanzten Rahmennummer angebracht. Da die Hersteller die Rahmennummern nicht systematisch und eindeutig vergeben und es keine zentrale Nummerndatei gibt, ist eine Zuordnung eines Fahrrads zu seinem Eigentümer oder seiner Eigentümerin nicht immer gewährleistet, wie der Allgemeine Deutsche Fahrrad-Club (ADFC) bemängelt.[8]

Die Polizei empfiehlt deshalb die Codierung in einen sogenannten Fahrradpass zusammen mit der Rahmennummer des Fahrrads und den persönlichen Daten der Eigentümerin oder des Eigentümers einzutragen. Darüber hinaus gehört ein Foto des Fahrrads dazu. Den Fahrradpass gibt es als Printversion und App[9].

### *3.1.3 Trackingsysteme für Fahrräder*

Fahrradflottenunternehmen statten ihre Fahrräder mit GPS-Trackern aus, um das Flottenmanagement (Ausleihen, Abrechnen) zu vereinfachen. Auch werden höherpreisige Fahrräder zunehmend mit GPS-Trackern ausgerüstet, um Zusatz-

5 Polizeiliche Kriminalprävention der Länder und des Bundes 2021.
6 ADFC o.J.
7 Polizeiliche Kriminalprävention der Länder und des Bundes o.J.
8 ADFC o.J.
9 Polizeiliche Kriminalprävention der Länder und des Bundes o.J.

leistungen durch verschiedene App-Services anzubieten zu können. Hierzu gehört auch eine Verfolgung im Diebstahlfall. Mittels GPS-Technologie können Gegenstände in Echtzeit geortet werden. Der Eigentümer bzw. die Eigentümerin wird per SMS informiert, wenn das Fahrrad beispielsweise über einen definierten Bereich hinaus bewegt wird. Die Benutzerinformation mit der genauen Position des Fahrrades erfolgt mit Hilfe von GPS und über Mobilfunk (GSM). In einstellbaren Zeitintervallen können die Positionsdaten an autorisierte Handys oder an ein Trackingportal übertragen und visualisiert werden. Der Service des Anbieters beinhaltet eine Routen-Aufzeichnung und Speicherung im GPX-Format.

Der Tracker, der aus einer relativ kleinen Leiterplatine besteht, wird häufig so im bzw. am Fahrrad verbaut, dass dieser sich nicht von gängigem Fahrradzubehör unterscheidet. Der Tracker muss hierzu mit einer SIM-Karte bestückt sein. Die Stromversorgung erfolgt über Batterien unterschiedlicher Kapazität oder es wird der Dynamo über einen zusätzlich zu montierenden Laderegler genutzt.

### *3.2 Predictive Policing*

Unter Predictive Policing, übersetzt „vorhersagende Polizeiarbeit“, versteht man die IT-gestützte Ermittlung der Auftrittswahrscheinlichkeit zukünftiger Straftaten an bestimmten Orten zu bestimmten Zeiten. Durch diesen Raum- und Zeitbezug erhält die strategische polizeiliche Einsatzplanung zur Prävention eine konkrete Unterstützung.[10,11] „Grundlage dieses Vorgehens ist die Verarbeitung großer Datenmengen aus detaillierten Lagebildern, aktuellen Ereignissen,“ geografischen und soziologischen sowie „allgemein zugänglichen Daten und zukünftig auch Sensordaten auf Basis von wissenschaftlichen Theorien zur Mustererkennung.“[12] Um verlässliche Prognosen zu erhalten, muss die Datenbasis ständig aktuell und fehlerfrei sein. Fehlerhafte und unvollständige Daten führen zu falschen Prognosen. Data Mining ist die Methode, die zur Gewinnung von Informationen aus den Daten (Strukturen, Zusammenhänge) angewendet wird. Die Data-Mining-Methode lässt sich vereinfachend als eine Verbindung aus statistischer Modellbildung, Datenspeicherung und Techniken der künstlichen Intelligenz beschreiben. Data-Mining umfasst demzufolge mehrere Schritte, von der Zusammenstellung der Daten, beispielsweise dem Anlegen einer Datenbank, über die Analyse der Daten, bis zum Ergebnis, das zum Beispiel aus Begriffslisten oder Clusterdarstellungen bestehen kann. Visuali-

10 Landeskriminalamt NRW 2018.
11 Rolfes 2017, S. 52
12 Tiemann 2016.

sierte Datenbezüge wie etwa Cluster oder auch Kartierungen unterstützen beim Predictive Policing das Aufdecken krimineller Muster[13].

In Deutschland wurde im Landeskriminalamt Nordrhein-Westphalen im Zeitraum von 2015 bis 2018 im Rahmen des SKALA-Projekts die Nutzung der vorhersagende Polizeiarbeit im praktischen Polizeieinsatz erforscht. Dabei ging es darum, durch Korrelation von Einbruchdiebstählen mit Geodaten vorherzusagen, wo und wann sich Einbruchserien voraussichtlich fortsetzen werden, um diese zu stoppen. Für solche Analysen werden polizeiliche Daten wie Tatzeiten, Tatorte und Vorgehensweisen bei Einbrüchen genutzt. Diese Daten werden durch soziostrukturelle Daten von Wohngebieten wie beispielsweise Bebauung, Einkommensstruktur oder Verkehrsinfrastruktur erweitert.[14][15]

## 4. Datenvisualisierung

Um Muster, Strukturen und Beziehungen in Datenmengen besser zu erkennen als in textlichen Datenauswertungen, werden Daten grafisch aufbereitet, um sie visuell erfassbar zu machen. Unterstützt wird der Prozess der Datenvisualisierung durch zahlreiche Computerprogramme. Demzufolge ist die Palette der grafischen Darstellungsmöglichkeiten breit gefächert und umfasst neben den bekannten Balken- und Kreisdarstellungen auch Flächendiagramme, verschiedenartige Kurvenabbildungen, geografische Karten, Marker- und Heatmap- sowie Clusterdarstellungen.

### *4.1 Prozess der IT-gestützten Datenvisualisierung*

Eine Visualisierung stellt bereits eine Interpretation dar. Sie soll die ausgewählten Daten zunächst sinnvoll anordnen bzw. strukturieren (Datenexploration) und sie dann in anschaulicher Form visualisieren, wodurch sich Muster in großen Datenmengen erkennen lassen. Die Verknüpfung von Visualisierungstechniken mit Data-Mining wird als „Visual Data-Mining" bezeichnet.[16] Das Referenzmodell von Shneidermann[17] schlägt für den Transformationsprozess von den Rohdaten zur visualisierten Darstellung, folgende drei Schritte vor:

13 Nath 2006, S. 41-44.
14 Landeskriminalamt NRW 2018.
15 Schürmann 2015.
16 Krypczyk 2014.
17 Card/Mackinlay/Shneiderman 1999, S. 321ff

1. Transformation der Rohdaten in strukturierte Daten

Die Rohdaten liegen meist in sehr unterschiedlichen Formaten, oftmals auf verschiedenen Datenträgern vor. Im ersten Schritt sind die Rohdaten deshalb in ein computerlesbares, strukturiertes Format zu überführen.

2. Visuelles Mapping

Im zweiten Schritt wird die grafische Visualisierung (visuelles Mapping) ausgewählt. Anhand der zahlreichen grafischen Möglichkeiten ist ein inhaltlich adäquates und ausdrucksstarkes Mapping zu entwickeln.

3. View-Transformation

Im dritten Schritt werden die unter 2. erarbeiteten grafischen Visualisierungen in konkrete Darstellungen umgesetzt. Hierzu gehört auch die Implementierung der Benutzerinteraktionen wie beispielsweise die Möglichkeit in die Abbildungen hinein zu zoomen.

### *4.2 Verbrechenskartierung*

Verbrechenskartierung (engl. crime mapping) bezeichnet die kartographische Visualisierung kriminalitätsbezogener Daten. In zahlreichen Polizeidienststellen wurde Software installiert, mittels derer Kriminalgeografen Lagebilder durch Verknüpfung von zeitbasierten Geodaten mit tatbezogenen und täterbezogenen Daten auf einer Landkarte erstellen. Die „geographische Komponente erweitert die Analyse- und Darstellungsmöglichkeiten durch schnelle visuelle Erfassung und die Integration wichtiger räumlicher Basisdaten.“[18] „Der entscheidende Vorteil liegt vor allem in der gelungenen Verbindung zwischen optisch leicht zu erfassendem und schnell zu generierendem Ergebnis sowie dem darin enthaltenen Analysevorgang. Die verfügbaren kriminalitätsbezogenen Daten können dabei unter räumlichen Aspekten in einer Vielzahl von Kombinationen abgefragt und aufbereitet werden.“[19].

Mittels Verbrechenskartierung wird der präventive Bereich der Polizeiarbeit unterstützt. Durch Verbrechenskartierung sind Gebiete mit hoher Straftatenkonzentration, sogenannte Hotspots, identifizierbar.[20] Dabei können auch Serien von Taten identifiziert werden, die den vor Ort tätigen Spurensuchern nicht auffallen würden. Verbrechenskartierung wird von Polizeibehörden für

18 Orkon/Weinreich 2013.
19 Orkon/Weinreich 2013.
20 Zou 2014, S. 227.

die interne Informationsverarbeitung genutzt. Es existieren auch öffentliche Webseiten, auf denen zur Anzeige gebrachte Straftaten auf einer Karte visualisiert werden können, filterbar nach Art der Straftat, Region und Zeitraum.

Eine Verbrechenskarte mit den Daten der „City of London Police" lässt sich beispielsweise auf deren Webseite im Bereich „Community Policing" aufrufen[21]. Nachdem ein Polizeiabschnitt ausgewählt wurde, erscheint eine Auswahlliste für Monate und eine für den „crime type". Beispielhaft sind in Abbildung 1 links Fahrraddiebstähle auf einer Karte mit Marker-Clustern innerhalb polizeilicher Abschnittsgrenzen visualisiert, die rechte Abbildung zeigt die Diebstähle im Umkreis von einer Meile, ausgehend von einem definierten Abschnittsmittelpunkt.

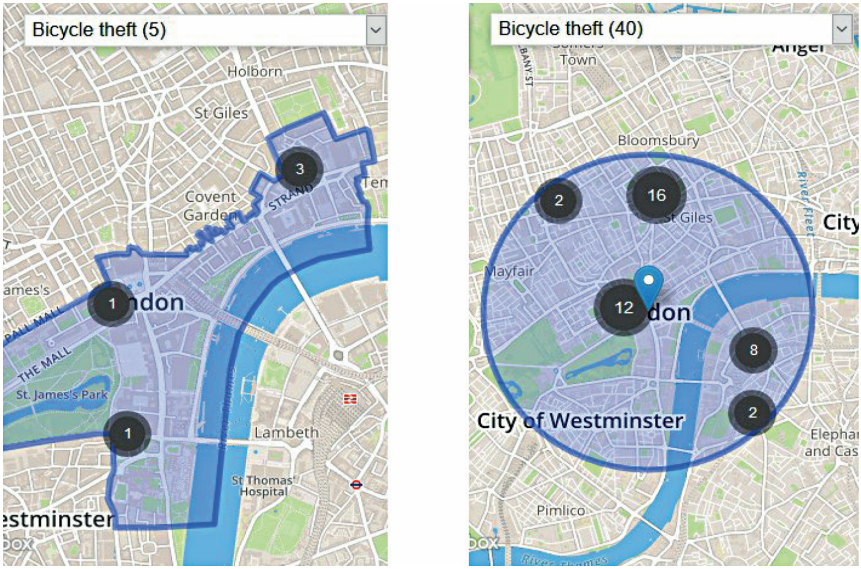


*Abb. 1: Visualisierung von Fahrraddiebstählen durch Marker-Cluster (Beispiel London): Links in einem ausgewählten Polizeiabschnitt, rechts im 1-Meilen-Radius*[22]

21 City of London Police o.J.
22 City of London Police o.J.

Neben den positiven Aspekten sich mittels Verbrechenskarten im Internet informieren zu können, soll auch auf die Gefahren hingewiesen werden. So werden mit Verbrechenskarten Orte vermeintlich als „objektiv sicher oder unsicher" eingestuft, was der sozialen Ausgrenzung Vorschub leisten kann.[23] Wenn Betreibende privater Mapping-Webseiten unter Missachtung von Datenschutz und ohne überprüfbare Kriterien, Delikte auf interaktiven Karten veröffentlichen, werden schnell Einzelpersonen diskriminiert.

## 5. Konzeption einer Webanwendung zur interaktiven Visualisierung von Fahrraddiebstählen

Die IT-Vorgehensweise zur Konzeption und Implementierung einer interaktiven Webanwendung zur Visualisierung von Trackingdaten gestohlen gemeldeter Fahrräder wird in diesem und dem folgenden Kapitel dargelegt.

### *5.1 Szenarien*

Jedem Diebstahl liegt ein Tatverhalten zugrunde, das durch die Visualisierung der Positions- und der Trackingdaten teilweise nachvollzogen werden kann. Jedem Tatverhalten einer Fahrraddiebin, eines Fahrraddiebes oder einer Gruppe von Dieb*innen steht ein Wissensbedarf der Strafverfolgungsbehörden gegenüber. Durch eine geeignete Darstellung der Daten kann das Wissen der Behörde erweitert werden. Bei einer kartografischen Auswertung von Trackingdaten gestohlener Fahrräder auf einer interaktiven Karte sind elf verschiedene Szenarien denkbar (siehe Abbildung 2).

23 Rötzer 2009.

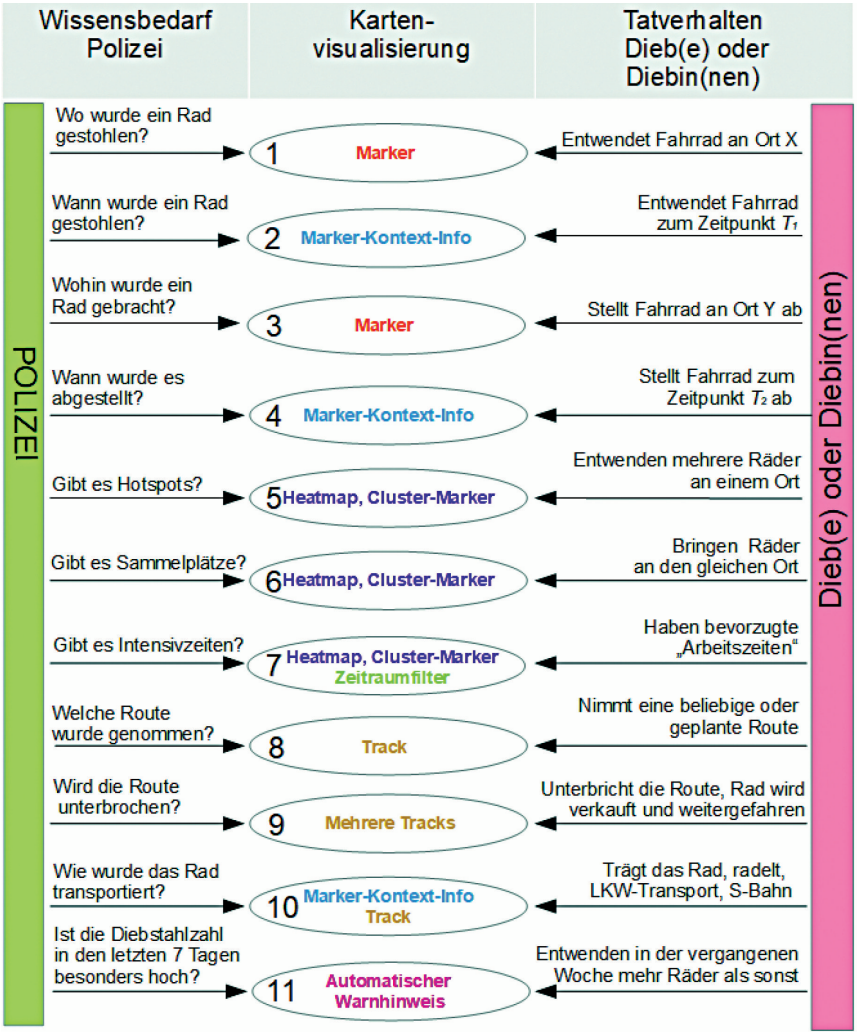


*Abb. 2: Szenarien zur Visualisierung von Daten gestohlen gemeldeter Fahrräder (Grafik: M. Scholz)*

### *5.2. Darstellungsmöglichkeiten*

Aus den 11 Szenarien werden folgende sechs Darstellungsmöglichkeiten abgeleitet:

1. **Marker** visualisieren den Diebstahlort oder den Standort eines Fahrrades.
2. **Kontextinformationen** liefern Information darüber
   - um welches Fahrrad es sich handelt (Fahrrad-ID)
   - wie das Rad transportiert wurde (Geschwindigkeit)
   - wann das Rad gestohlen und wann es abgestellt wurde.
3. **Heatmaps** und **Cluster-Marker** visualisieren die geografische Verteilung von Diebstählen.
4. **Heatmaps** und **Cluster-Marker** in Verbindung mit **Zeitraumfilter** visualisieren die zeitliche Verteilung von Diebstählen.
5. **Tracks** in Form von Polygonzügen sowie **Start- und Endmarker** visualisieren den Transportweg eines gestohlenen Fahrrades und können einen Hinweis auf die Transportart geben.
6. Ein modales Fenster mit einem **Warnhinweis** und der **Anzahl der gestohlenen Fahrräder** der vergangenen Woche wird automatisch angezeigt.

### *5.3 Softwarearchitektur*

Die Architektur der entwickelten Anwendung basiert auf einem dreischichtigen Client-Server-Modell, bestehend aus der Präsentationsschicht, der Fachlogikschicht und der Datenhaltungsschicht, die an ein Datenbanksystem angebunden ist.

Die oberste Schicht ist die Präsentationsschicht, in der alle Komponenten realisiert werden, mit denen der Benutzende mit dem Programm interagiert.

Die mittlere Schicht ist die Fachlogikschicht, in der die Benutzereingaben verarbeitet, die Benutzerausgaben erzeugt und die Zugriffe auf die Datenbank verwaltet werden. Da die Fachlogik größtenteils clientseitig stattfindet, handelt es sich bei dieser Anwendung um eine Client-zentrierte Webanwendung (Rich Internet Application). In dieser Schicht befinden sich alle statischen Ressourcen (JavaScript, CSS) und alle Abfrage-Routinen zur Erstellung von Aggregationen, wie z. B. die Arrays mit den Koordinaten der Diebstahlorte für einen bestimmten Zeitraum.

In der unteren Ebene, der sogenannten Datenhaltungsschicht, erfolgt das Speichern der Trackingdaten und eines Schwellenwertes für den Warnhinweis in einer MongoDB-Datenbank. Mit *NodeJS* wird eine Ausführungsumgebung für JavaScript genutzt, die unabhängig von einem Browser lauffähig ist und sich deshalb für die Implementierung eines Webservers eignet.

Die Anwendung besteht idealerweise aus einer einzigen HTML-Seite (single-page application), deren Inhalte dynamisch nachgeladen werden.

## 6. Implementierung

Für die verschiedenen Visualisierungen von Fahrraddiebstählen mit Markern, Heatmaps und Marker-Clustern wurden drei Ebenen (vgl. Abbildung 3) implementiert:

- Marker-Ebene
- Heatmap-Ebene
- Marker-Cluster-Ebene

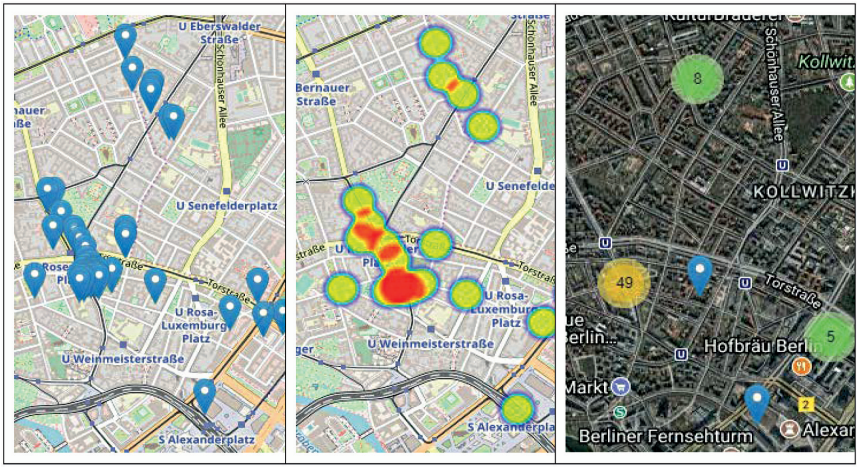


*Abb. 3: Screenshots der prototypischen Anwendung: Karten-Ausschnitte mit Markern (links), als Heatmap (mitte), mit Cluster-Markern (rechts)*

Abbildung 4 zeigt einen Screenshot mit der Seitenstruktur der Anwendung. Im rechten Teil wird die Straßenkarte mit den Positionen gestohlen gemeldeter Fahrräder angezeigt. Der linke Bereich ist als Sidebar mit Eingabe- und Steuerelementen realisiert. Hier kann bezüglich eines Zeitraums gefiltert, durch Eingabe der Fahrrad-ID nach einem einzelnen Rad gesucht oder ein Schwellenwert für die Zahl der Diebstähle in den letzten sieben Tagen festgelegt werden. Im

Screenshot ist ein Warnhinweis zu sehen, wie er im Fall einer Überschreitung des Schwellenwerts angezeigt wird.

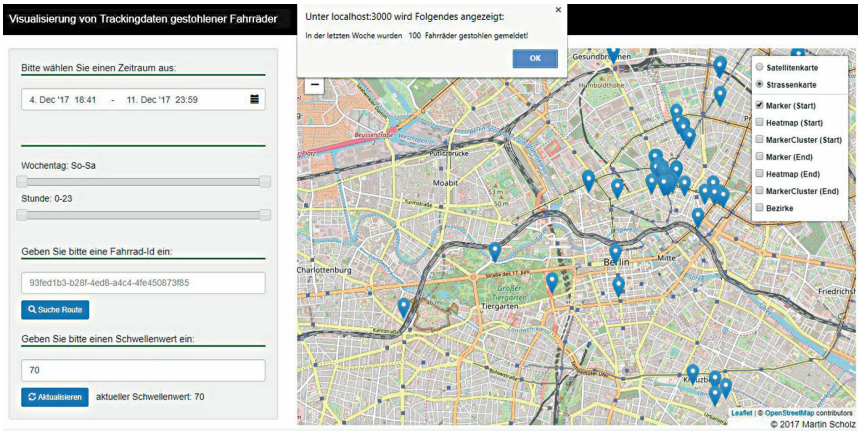


*Abb. 4: Screenshot der prototypischen Anwendung: Seitenstruktur und Alert-Box mit Warnhinweis*

Für die Visualisierung der Route eines Fahrrads (siehe Abbildung 5) werden jeweils zwei Marker durch eine Linie verbunden, so dass die Route durch einen Polygonzug abgebildet wird. Durch Klicken auf einen Marker wird die Route auf der Karte angezeigt. Eine Route kann auch mittels einer Routensuche durch Eingabe einer Fahrrad-ID angezeigt werden. Zusätzliche Textinformationen zu Zeitpunkt, Fahrrad-ID und Transportart sind mittels Pop-ups an den Markern abrufbar. Auf die Transportart wird aus der Geschwindigkeit geschlossen. Höhere Geschwindigkeiten lassen beispielsweise auf eine Beförderung per Autotransporter schließen. Durch die Pop-ups erhalten die Textinformationen einen eindeutigen Raumbezug und die Marker durch Start- und Endzeiten ihren Zeitbezug.


*Abb. 5: Screenshot der prototypischen Anwendung: Karten-Ausschnitt einer Routenvisualisierung*

## 7. Zusammenfassung

Die vorgestellte prototypische Anwendung zeigt, wie die Visualisierung von Tracking-Daten gestohlener Fahrräder auf einer interaktiven Karte zum Auffinden gestohlener, mit GPS-ausgestatteter Fahrräder sowie als Entscheidungsgrundlage für Präventionsmaßnahmen bei der Polizei dienen kann.

Der praxistaugliche Einsatz einer solchen Anwendung im Polizeibetrieb setzt voraus, dass eine Datenbank mit Trackingdaten gestohlener Fahrräder vorhanden ist. Alle Diebstahldaten sind zeitnah einzupflegen, andernfalls sind die vom System erzeugten Visualisierungen nicht hinreichend aussagefähig und gegebenenfalls sogar fehlerhaft. Wiederaufgefundene Fahrräder sind ebenfalls zeitnah im Datensystem einzutragen, da sonst Fahrräder gesucht (und gefunden) werden, die nicht mehr als gestohlen gemeldet sind.

Als Prototyp mit eigenem Webserver und eigener Datenbank ist die Anwendung unabhängig von einem polizeilichen Verwaltungssystem lauffähig. Unter Beibehaltung der Datenstruktur der verwendeten Trackingdaten ist die Anbindung des Prototyps über seine HTTP-Schnittstellen an ein polizeiliches Softwaresystem möglich.

## Literatur

ADFC (o. J.-a) Thema: Diebstahl vermeiden. ADFC Allgemeiner Deutscher Fahrrad-Club e. V. https://www.adfc.de/themen/im-alltag/diebstahlvermeidung (letzter Aufruf: 20.02.2019).

ADFC (o. J. -b) Fahrrad-Codierung. ADFC Allgemeiner Deutscher Fahrrad-Club https://www.adfc.de/artikel/fahrrad-codierung (letzter Aufruf: 20.02.2019).

Card, Stuart K., Mackinlay, Jock, Shneiderman, Ben (1999) Readings in Information Visualization: Using Vision to Think (Interactive Technologies). Morgan Kaufman-Verlag.

City of London Police (o. J.): Crime map. Police.uk. https://www.police.uk/pu/your-area/city-of-london-police/community-policing/?tab=CrimeMap (letzter Aufruf: 20.02.2019).

Landeskriminalamt NRW (2018) Abschlussbericht Projekt SKALA. Düsseldorf. https://polizei.nrw/sites/default/files/2018-07/180628_Abschlussbericht_SKALA.PDF (letzter Aufruf: 20.02.2019).

Nath, Shyam Varan (2006) Crime Pattern Detection Using Data Mining, in 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops. Hong Kong: IEEE 2006, S. 41–44. doi: 10.1109/WI-IATW.2006.55.

Okon, Günter; Weinreich, Ralf (2013) Darstellung der Kriminalitätslage unter Verwendung von GIS. https://archive.is/20130122163137/http://proceedings.esri.com/library/userconf/europroc99/html/vortraege/v05/v0504/v0504.html (letzter Aufruf: 20.02.2019).

Rolfes, Manfred (2017) Predictive Policing: Beobachtungen und Reflexionen zur Einführung und Etablierung einer vorhersagenden Polizeiarbeit in: Potsdamer Geographische Praxis. S. 51-76. Universitätsverlag Potsdam.

Polizeiliche Kriminalprävention der Länder und des Bundes (o. J.) Fahrradpass als App - Polizei-Beratung. https://www.polizei-beratung.de/themen-und-tipps/diebstahl/diebstahl-von-zweiraedern/fahrradpass-app/ (letzter Aufruf: 20.02.2019).

Polizeiliche Kriminalprävention der Länder und des Bundes (2021) Diebstahl von Zweirädern - Polizei-Beratung. https://www.polizei-beratung.de/themen-und-tipps/diebstahl/diebstahl-von-zweiraedern/ (letzter Aufruf: 20.02.2019).

Rötzer, Florian. (2009) Verbrechenskarten (fast) in Echtzeit. heise online. https://www.heise.de/tp/features/Verbrechenskarten-fast-in-Echtzeit-3381970.html (letzter Aufruf: 02.2019).

Schürmann, Dieter (2015) SKALA. Predictive Policing als praxisorientiertes Projekt der Polizei NRW.“ in Forum KI 2015. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2015/kiforum2015SchuermannPositionspapier.html (letzter Aufruf: 20.02.2019).

Tiemann, Jens (2016) Vorhersagende Polizeiarbeit, In: Jens Fromm und Mike Weber (Hrsg.): 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT.

Zhou, Guiyun/Lin, Jiayuan/Ma, Xiujun (2014) A Web-Based GIS for Crime Mapping and Decision Support. In: Gregory A. Elmes, George Roedl and Jamison Conley.(ed.): Forensic GIS. Geotechnologies and the Environment, S. 221-243. Dordrecht, Heidelberg, New York, London: Springer.

*Jan Fährmann*[1]

# Rechtliche Rahmenbedingungen der Nutzung von Positionsdaten durch die Polizei und deren mögliche Umsetzung in die Praxis– zwischen Strafverfolgung und Hilfe zur Wiedererlangung des Diebesguts

## 1. Problemaufriss

Die Anwendungsmöglichkeiten von Ortungssystemen sind zahlreich. Die IT-Technik zur Positionsermittlung wird in vielen Lebensbereichen genutzt, z. B. in den Navigationssystemen in PKW, LKWs und Bussen. Auch sehr viele Apps für Smartphones liefern ortsbezogene Informationen.[2] Die Einbeziehung von Positionsdaten in die Ermittlungsarbeit und die Gefahrenabwehr gewinnt in der Polizeiarbeit dementsprechend zunehmend an Bedeutung.[3] Mittels solcher Daten lassen sich Positionen von gestohlenen Gegenständen nachvollziehen, die mit einem GPS Sender verbunden sind.[4] So wird die Ortungstechnik bereits zum Auffinden gestohlener PKW eingesetzt,[5] wobei hier vielfach noch nicht auf GPS Daten zugegriffen wird, sondern Funkzellen abgefragt werden, was gerade im ländlichen Raum viel zu ungenau zum Auffinden des Gegenstandes ist. Auch Anbieter von Fahrradflotten nutzen diese Technik bereits zum Auffinden ihrer abhandengekommenen Fahrräder.

Die Nutzung von Positionsdaten könnte das Auffinden von mit Sendern ausgestatteten, gestohlenen Gegenständen durch die Polizei erheblich erleichtern. Dies ist in verschiedenen Situationen denkbar. Einerseits könnte die Polizei zum Standort des Diebesgutes fahren, um dieses sicherzustellen und vor Ort Beweise erheben, um die Täter*innen zu ermitteln (Strafverfolgung). Gleichzeitig könnte die Polizei den rechtswidrigen Zustand beenden und den Geschädigten ihr Eigentum zurückgeben (Gefahrenabwehr). Zudem könnte sie

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

2 Vgl. Weichert, SVR 2009, S. 348-350.

3 Vgl. zum Interesse am Zugang zu neuen Datenquellen: Kudlich 2016-Kölbel § 161 Rn. 26; Singelnstein, NStZ 2012, S. 599, 602; vgl. zur Gefahrenabwehr etwa Faßnacht 2011; Neumann 2014, S. 136-142; Fährmann, MMR 2020, S. 288.

4 Vgl. Kilian 2018, 1. Abschnitt., Rn. 17; Nickel/Gwehenberger, VW 1994, S. 134.

5 Vgl. Singelnstein, NStZ 2012, S. 594.

auch die Bewegungen des Gegenstandes beobachten oder Bewegungsdaten speichern und diese auswerten, um daraus Rückschlüsse für die strafrechtlichen Ermittlungen zu ziehen, etwa auf hinter dem Diebstahl stehende kriminelle Strukturen. Denkbar wäre auch, dass der Polizei aufgrund von Ermittlungen (etwa Zeug*innenaussagen) bekannt ist, wer den Diebstahl begangen und die tatsächliche Sachherschafft über den Gegenstand innehat. Insofern können neben der Beobachtung der Position des Gegenstandes noch weitere Ermittlungsmaßnahmen wie die Überwachung der Telekommunikationsdaten (TKÜ) zusätzlich eingesetzt werden. Letzterer Fall dürfte aber nicht oft vorkommen und bleibt daher hier außen vor. In diesem Beitrag wird daher ausschließlich die Konstellation rechtswissenschaftlich untersucht, in der die Polizei nur die Bewegungen eines Gegenstandes beobachtet.

Sowohl die Polizei als auch private Personen könnten (theoretisch) Positionsdaten gestohlener Gegenstände erheben (wobei bei der Polizei ggf. die Datenverarbeitung entsprechend anzupassen ist). Zum Tracking oder zu dessen Veranlassung berechtigte Privatpersonen können z. B: Eigentümer*innen, Inhaber*innen einer eigentümer*innenähnlichen Position (z. B. einer Anwartschaft) oder berechtigte Besitzer*innen – z. B. aus einem Leasing- oder Mietvertrag –, sein, die durch den Diebstahl den Besitz bzw. Zugriffsmöglichkeiten auf den Gegenstand eingebüßt haben. Im Folgenden werden diese als Geschädigte bezeichnet. Zudem können sowohl Dieb*innen, Hehler*innen (als bösgläubige Besiter*innen) als auch gutgläubige Besitzer*innen die tatsächliche Sachherrschaft über den Gegenstand ausüben. Sofern unklar ist, welche Eigenschaft diese Besitzer*innen innehaben, wird nur von Besitzer*innen gesprochen.

Für behördliche Eingriffe in Form der Datenerhebung sowie -verarbeitung bedarf es einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang des Eingriffs klar ergeben.[6] Ferner kann auch die Verarbeitung personenbezogener Daten durch die Geschädigten einen Verstoß gegen das Datenschutzrecht darstellen. So können durch die Positionsdaten des Gegenstandes sowohl umfangreiche Rückschlüsse auf das Verhalten der Dieb*innen, Hehler*innen als auch von gutgläubigen Besitzer*innen gezogen werden, was schwerwiegende Eingriffe in die Persönlichkeitsrechte bedeuten kann, insbesondere, wenn Gegenstände über einen längeren Zeitraum beobachtet werden. Im Rahmen des Beitrages wird analysiert, ob die Polizei über eine Ermächtigungsgrundlage zur Ortung gestohlener Gegenstände verfügt. Zudem wird untersucht, ob Geschädigte berechtigt sein können, entsprechende Daten gestohlenen Gegenstände zu erheben und ob diese Daten an die Polizei übertragen werden können.

6 St. Rspr. des BVerfG, vgl. grdl. BVerfGE 65, 1 ff.; zur obergerichtlichen Rspr. Z. B. OVG Hamburg NJW 2008, 96 (97).

## 2. Ermächtigungsgrundlagen für die polizeiliche Datenerhebung

Es wird vertreten, dass eine Ermächtigungsgrundlage vorliegend nicht erforderlich sei. Sollten die Geschädigten die Polizei zur Erhebung der Daten berechtigt haben, hätten diese wirksam auf ihr Grundrecht der informationellen Selbstbestimmung verzichtet. Den Dieb*innen ständen weder der gestohlene Gegenstand noch die Positionsdaten zu, sodass sie nicht in die Datenerhebung einwilligen bräuchten.[7] Auch sei es nicht angemessen, wenn sich Straftäter*innen auf das Grundrecht der informationellen Selbstbestimmungsrecht berufen dürften.[8] Dagegen spricht sehr eindeutig die Rechtsprechung des BVerfG, welches die Notwendigkeit einer Ermächtigungsgrundlage bei jeder Beeinträchtigung des Rechts auf informationelle Selbstbestimmung voraussetzt.[9]

Vorliegend liegt ein Eingriff in die informationelle Selbstbestimmung der Dieb*innen bzw. der (ggf. gutgläubigen) Besitzer*innen des Gegenstandes vor. Das Recht auf informationelle Selbstbestimmung gewährleistet den Bürger*innen, selbst über die Preisgabe und Verwendung von persönlichen Daten zu entscheiden.[10] Personenbezogene Daten liegen hier vor. Personenbezogen sind Daten, die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person ermöglichen.[11] Dazu zählen nicht nur einer Person zukommende Eigenschaften und Merkmale, sondern auch ihre Beziehungen zur Umwelt, wie unter anderem ihr Aufenthaltsort.[12] Auch Gegenstände können dem Einfluss einer Person unterliegen, so dass über sie eine indirekte Beziehung zur Person hergestellt werden kann.[13] Gerade leicht bewegliche Gegenstände, die im Alltag verwendet werden (Fahrräder, Autos, Mobiltelefone etc.), ermöglichen bei ihrer Nutzung Rückschlüsse auf die Besitzer*innen. Beispielsweise wo diese wohnen oder welche Orte sie aufsuchen.[14] Entsprechende „Sachdaten" können also einer konkreten Person zugeordnet werden, wodurch sie zu personenbezogenen Daten werden.[15] Je mehr Daten gespeichert werden, desto leichter lassen sich Rückschlüsse ziehen. Es ist auch gleichgültig, ob es sich um Daten von Straftäter*innen handelt - was vielfach

7 AG Friedberg NStZ 09/2006, 517 (518); Jordan, Der Kriminalist 2005, S. 353.
8 Ladeur, DÖV 2009, S. 47-48; Lesch, JA 2000, S. 727-728.
9 Grundlegend dazu BVerfG 65, 1 ff.
10 Z. B. BVerfGE 130, 1 (35).
11 BVerfG 65, 1 (42); Gasch 2012, S. 97.
12 BGH NJW 2013, 2530 (2532) m. w. N.
13 BGH NJW 2013, 2530 (2532) m. w. N.; Cornelius, NJW 2013, S. 3341.
14 Vgl. LG Lüneburg NJW 2011, 2225; Steinmetz, NStZ 2001, S. 347.
15 Vgl. BGH NJW 2013, 2530 (2532) m. w. N.; Weichert, DuD 2009, S. 348-350; Gasch 2012, S. 98-99, 127; Neumann 2014, S. 319.

offen sein wird -, da auch diese Positionsdaten dem Schutz der informationellen Selbstbestimmung unterliegen.[16] Daran vermag auch die Einwilligung der Geschädigten nichts zu ändern, da diese nicht über das informationelle Selbstbestimmungsrecht der Besitzer*innen des gestohlenen Gegenstandes disponieren können.[17] Von einer konkludenten Einwilligung der Dieb*innen in die Datenerhebung ist ebenfalls nicht auszugehen, da diese kein Interesse an Eingriffen haben dürften.[18] Auch widerspricht die beschriebene Ansicht der Grundkonzeption des Strafverfahrensrechts, welches Eingriffe in die Rechtssphäre der Tatverdächtigen an konkrete Anforderungen knüpft.[19] Die Ansicht ist überdies nicht mit der in Art. 6 Abs. 2 EMRK garantierten Unschuldsvermutung vereinbar.[20] Die Ortung und Speicherung von Positionsdaten gestohlener Gegenstände stellt damit einen Eingriff in das informationelle Selbstbestimmungsrecht dar,[21] der einer Ermächtigungsgrundlage bedarf.

### *2.1 § 100h StPO als Ermächtigungsgrundlage für die Ortung von Diebesgut*

Die Positionsdaten gestohlener Gegenstände könnten direkt von der Polizei zur Strafverfolgung erhoben werden, die die Daten selbstständig speichert und verwendet. Die Ermächtigung dazu könnte sich aus § 100h Abs. 1 S. 1 Nr. 2 StPO ergeben. Dies erfordert Observationszwecke, und bei dem Ortungssystem müsste es sich um sonstige technische Mittel handeln. Zusätzlich muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert sein. Nach S. 2 ist weiterhin notwendig, dass Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

#### *2.1.1 Tatbestandsvoraussetzungen § 100h StPO*

Die Erhebung von Positionsdaten müsste also eine Observation darstellen. Eine Observation ist die regelmäßige, unauffällige und planmäßige Beobachtung einer Person oder eines Objekts, um für das Ermittlungsverfahren relevante

16 Auch ist darauf hinzuweisen, dass im Strafverfahren erhobene Daten immer personenbezogen sind, da es stets darum geht, einen Verdächtigen zu überführen; Gusy, StV 1998, S. 527.

17 Vgl. LG Hildesheim, Besch. v. 12. März 2008, 12 Qs 12/08, Rn. 16; Gasch 2012, S. 142 m. w. N.; Bosch, JA 2006, S. 749.

18 Gasch 2012, S. 136.

19 Abdallah/Gercke, CR 2003, S. 298-299.

20 Abdallah/Gercke, CR 2003, S. 298.

21 BVerfGE 97, 319 (404 f.); Jarass/Pieroth-Jarass 2022, Art. 2, Rn. 59; vgl. Börner, K&R Beilage 2015, S. 3.

Daten zu erheben,[22] vgl. die Legaldefinition aus § 163f Abs. 1 S. 1 StPO. Dazu muss die Person nicht direkt von den Beamten*innen wahrgenommen werden, sondern es reicht aus, sie mittels technischer Einrichtungen zu beobachten.[23]

Geht es der Polizei darum, den gestohlenen Gegenstand zu orten, um diesen sicherzustellen, dann erfolgt keine regelmäßige Beobachtung des Gegenstandes oder der Tatverdächtigen. Es geht vielmehr darum, den Gegenstand aufzufinden, ggf. als Beweismittel. Auch kann nicht von einer planmäßigen Herangehensweise gesprochen werden, da sich die Polizei lediglich an der aktuellen Position des Gegenstandes orientiert und ansonsten nichts unternimmt. Folglich ist die bloße Ortung nur zur Sicherstellung des Gegenstandes keine Observation.[24] Eine Observation durch das Tracken von Positionsdaten liegt demnach nur dann vor, wenn die Polizei die Bewegungen des gestohlenen Gegenstandes über einen gewissen Zeitraum nachverfolgt, um etwa Muster bei den Diebstählen zu erkennen, Rückschlüsse auf Beteiligte zu ziehen oder um auf Bandenstrukturen schließen zu können.

Des Weiteren müssten die Ortungssysteme sonstige technische Mittel darstellen. Technische Mittel im Sinne des § 100h Abs. 1 S. 1 Nr. 2 StPO sind technische Anwendungen mittels derer Überwachungsmaßnahmen durgeführt werden, die weder das Aufzeichnen von Bildern noch von Worten betreffen, da diese bereits durch andere Ermächtigungsgrundlagen abgedeckt sind. § 100h Abs. 1 S. 1 Nr. 2 StPO stellt damit eine Generalklausel für den Einsatz von technischen Geräten dar, die nicht unter konkrete Ermächtigungsgrundlagen der StPO gefasst werden können.[25] D. h., falls es eine speziellere Regelung geben sollte, würde diese eine Sperrwirkung entfalten.[26] Die Verwendung und Erhebung von GPS- oder anderen Positionsdaten in dieser Situation ist aber in keiner anderen Norm der StPO genannt. Lediglich zu anderen Zwecken können Positionsdaten erhoben werden[27] (allenfalls gestohlene Mobiltelefone könnten geortet werden).

22 BGH NJW 1998, 1237 (1237); Kudlich-Günther 2016, § 163f Rn. 7; Steinmetz, NStZ 2001, S. 347.

23 Steinmetz, NStZ 2001, S. 347.

24 A. A. Bär 2007, S. 198, der diese Ansicht aber nur damit begründet, dass die Ortung auch zur Observation gehöre, ohne sich damit zu beschäftigen, ob jede Ortung auch als Observation zu verstehen ist. Nur weil die Ortung Teil einer Observation sein kann, muss nicht jede Ortung eine Observation darstellen.

25 Vgl. Kühne, JZ 2001, S. 1148.

26 Kudlich-Kölbel 2016, § 161 Rn. 6 ff.

27 Ausführlich dazu Fährmann/Matzdorf/Höffner in diesem Band, S. 29ff.

In der höchstrichterlichen Rechtsprechung ist anerkannt, dass Ortungssysteme technische Mitteln nach 100h Abs. 1 S. 1 Nr. 2 StPO darstellen.[28] Dem hat sich die überwiegende Literatur angeschlossen.[29] Grundsätzlich kann festgehalten werden, dass vom Wortlaut der Norm der Einsatz von Ortungstechnologie umfasst ist,[30] da die Norm sehr weit gefasst ist. In Teilen der Literatur wird jedoch der Einsatz von GPS-Sendern aufgrund von 100h StPO kritisiert, insbesondere, weil sich aus der Norm kein konkreter Hinweis auf den Einsatz von Ortungssystemen ergebe. Entsprechende Eingriffe müsse der Gesetzgeber klarer und bestimmter regeln.[31] Insbesondere, weil mittels GPS ein weitaus intensiverer Eingriff möglich sei, da Bewegungsbilder deutlich präziser erstellt werden könnten als bei der bloßen Beobachtung durch Beamt*innen ohne technische Hilfsmittel.[32] Die gesteigerte Eingriffsintensität könne auch daraus erwachsen, dass diese Daten mit weiteren Daten verknüpft werden.[33] Aus dem Bestimmtheitsgebot folgt aber nicht, dass sich jede kriminaltechnische Neuerung ausdrücklich aus einer Norm ergeben muss.[34] Vielmehr ist auch eine Umschreibung der Tätigkeit möglich, um der Polizei die Möglichkeit zu geben, auf technische Entwicklungen reagieren zu können und verbesserte Systeme einzusetzen.[35] Dementsprechend ist es Aufgabe der Rechtsprechung, den Anwendungsbereich von weiten Normen durch Präzisierung und Konkretisierung im Wege der Auslegung auszudifferenzieren (Präzisierungsgebot), d. h. deren Inhalte durch Auslegung zu bestimmen.[36] Dies ist dem Umstand geschuldet, dass es letztlich nicht möglich ist, für jede technische Neuerung und jeden technischen Anwendungsbereich eine eigene Norm zu kreieren, weshalb entsprechend weite Normen notwendig sind. Die Normen dürfen aber nicht so weit sein, dass der Inhalt beliebigen Interpretationen zugänglich ist, bzw. unter sehr weite Normen dürfen keine intensiven Eingriffe subsumiert werden. Der Eingriffsgehalt muss sich bei intensiven Eingriffen so präzise wie möglich aus der Norm ergeben. Inwieweit Eingriffe durch Generalklauseln oder weite Normen gerechtfertigt werden können oder präziser in speziellen Normen um-

28 BVerfG NJW 2005, 1338 (1339 f.); BGH NJW 2001, 1658 (1659) m. w. N.; OLG Düsseldorf NStZ 1998, 268 (268 ff.)

29 Gercke 2006, S. 404 m. w. N.; Soiné, NStZ 2014, S. 600

30 Gercke 2006, S. 404; Kühne, JZ 2001, S. 1148.

31 Zur Übersicht Gercke/Julius/Temming/Zöller-Gercke 2012, § 100h, Rn. 5 m. w. N.; Gercke 2006, S. 404 ff; Kühne, JZ 2001, S. 1148.

32 Gercke 2006, S. 405.

33 Vgl. dazu Schomberg/Stroscher 2020, 07074.

34 BVerfG NJW 2005, 1338 (1349); Graf-Hegmann (Stand 2016), StPO § 100h Rn. 5.

35 BGH NStZ 2001, 386 (387); zu dieser Problematik Aden/Fährmann, Vorgänge 2019, S. 101 f.; an Hand von Drohnen Tomerius, LKV 2020, 486.

36 BVerfG Beschl. v. 23.6.2010 – 2 BvR 2559/08, 105, 491/09, BeckRS 2010, 51599, Rn. 81.

schrieben werden müssen, hängt damit im Wesentlichen davon ab, wie schwer die Eingriffe wiegen. Um das beurteilen zu können, müssen die Norm und ihre Tatbestandsvoraussetzungen als Ganzes mit Blick auf den konkreten Eingriff bewertet werden. Die Schwere des Eingriffs hängt aber maßgeblich davon ab, welche Form der Datenverarbeitung von § 100h StPO umfasst ist. Dies wird sogleich aus Gründen der Übersichtlichkeit im folgenden Abschnitt *2.1.2* betrachtet und daran schließt sich dann auch die Bewertung der Schwere des Eingriffs an.

Zudem bedarf es des Tatbestandsmerkmals einer Straftat von erheblicher Bedeutung, welches sich an dem Katalog des § 100a Abs. 2 StPO orientiert.[37] Solche Taten sind anzunehmen, wenn sie mindestens dem Bereich der mittleren Kriminalität zuzurechnen sind. Darüber hinaus müssen sie den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit in der Bevölkerung erheblich zu beeinträchtigen.[38] Die Delikte müssen dazu eine gewisse Schwere aufweisen.[39] Mithin scheiden Antrags- und Bagatelldelikte aus.[40] Auch ein einfacher Diebstahl genügt in der Regel nicht.[41] Etwas anderes kann nur dann gelten, wenn die gestohlene Sache einen erheblichen Wert hat (etwa ein LKW mit wertvoller Ladung).[42] Dies folgt aus dem Sinn und Zweck der Norm, da das Tatbestandsmerkmal dazu dient, den Anwendungsbereich von technischen Überwachungsmaßnahmen zu begrenzen.[43] Daher muss sich der Wert des entwendeten Gegenstandes im Regelfall im Bereich von mehreren zehntausend Euro bewegen. Andere Diebstähle haben grundsätzlich nicht die beschriebenen Auswirkungen auf den Rechtsfrieden. Einfache Diebstähle, z. B. ein Fahrraddiebstahl, können daher nicht unter § 100h Abs. 1 S. 1 Nr. 2 StPO subsumiert werden. Daher können nur die organisierte Kriminalität, Bandenkriminalität oder Seriendiebstähle bzgl. Fahrrädern, Handys oder vergleichbaren Tatobjekten als Straftaten von erheblicher Bedeutung eingestuft werden.[44] Das Gewicht der Straftaten ergibt sich dabei aus der Vielzahl der Delikte und aus dem Umstand, dass durch die arbeitsteilige Herangehensweise ein sehr hoher Schaden angerichtet wird.[45] Durch die Vielzahl der Delikte wird der

37 Vgl. Graf-Hegmann (Stand 2016), StPO § 100h Rn. 12.
38 BVerfG NStZ 2003, 441; 2004, 270; BVerfG NJW 2005, 1338 (1339).
39 Vgl. EGMR NJW 2011, 1333 (1335); BVerfG NStZ 2003, 441 (442); BVerfG NJW 2005, 1338 (1339).
40 Kudlich-Günther 2014, § 100h Rn. 16.
41 LG Hildesheim, Beschl. V. 12.03.2008 - 12 Qs 12/08.
42 Kudlich-Günther 2014, 2014 - Günther § 100g Rn. 25; AG Friedberg NStZ 09/2006, 517 (518).
43 Vgl. EGMR NJW 2011, 1333 (1335).
44 Vgl. Vassilaki, Computer und Recht 2005, S. 572.
45 Vgl. BGH NStZ 2001, 386, 387.

Rechtsfrieden zudem erheblich gestört. Insofern sind bei einfachen Diebstählen mit geringwertigen Sachwert die Voraussetzungen von § 100h Abs. 1 S. 1 Nr. 2 StPO nicht gegeben; bei organisierter oder Bandenkriminalität sowie Serien-diebstählen bzw. wertvollem Diebesgut ist dies hingegen der Fall.

Die Ortung und die Auswertung von Positionsdaten gestohlener Gegenstände, insbesondere von beweglichen Sachen wie Fahrrädern und Autos, sind zur Aufklärung des Diebstahls zudem nützlich, da gerade bei zahlreichen Diebstählen, wenn keine Zeug*innen vorhanden sind, diese auf andere Weise kaum aufgeklärt werden können, sodass auch dieses Tatbestandsmerkmal erfüllt ist.[46] Die Polizei hat bei zahlreichen Diebstahlsdelikten in der Regel keine oder kaum Ermittlungsansätze, sodass die Ermittlungen ohne den Einsatz von Ortungstechnologie deutlich weniger erfolgversprechend bzw. normalerweise zum Scheitern verurteilt sind (etwa beim Fahrraddiebstahl). Durch die Standorte und die Bewegungen der Gegenstände sind Rückschlüsse auf die Tatverdächtigen möglich. Beispielsweise können sich gestohlene Gegenstände in einer Halle befinden, die einer bestimmten Person gehört, die damit dann als Verdächtige in Betracht kommt.

Zusammenfassend kann festgehalten werden, dass der Tatbestand nur bei höherwertigen Gegenständen oder bei banden- oder gewerbsmäßigen Diebstählen erfüllt ist. Allerdings stellt sich bei vielen Diebstählen das Problem, dass gewerbs- und/oder bandenmäßige Diebstähle oft nicht ohne weitere Ermittlungsmaßnahmen erkennbar sind. Jedoch fehlen oft Ermittlungsansätze, sodass nur in seltenen Fällen am Tatort erkennbar ist, ob es sich um eine Straftat von erheblicher Bedeutung handelt. Oft ist ein Gegenstand nur verschwunden, ohne dass es Hinweise auf das Vorgehen der Dieb*innen gibt, weshalb dann auch keine weiteren Ermittlungen angestellt werden. So werden die Voraussetzungen von 100h Abs. 1 Nr. 2 StPO in diesen Fällen nicht vorliegen, wenn die Gegenstände keinen höheren Wert aufweisen. Bei zahlreichen Diebstählen dürfte der Tatbestand dementsprechend nicht erfüllt sein.

### *2.1.2 Welche Maßnahmen sind von § 100h Abs. 1 S. 1 Nr. 2 StPO umfasst?*

Fraglich ist, welche Maßnahmen von 100h Abs. 1 S. 1 Nr. 2 StPO umfasst sind. Dürfen die Positionsdaten erhoben und gespeichert werden? Dies hängt, wie festgestellt, von dem Wortlaut der Norm, der Schwere des Grundrechtseingriffs und der damit verfolgten Zwecke ab.

Die längere Beobachtung der Bewegungen von Diebesgut mittels Ortungstechnologie ist vom Wortlaut vergleichsweise präzise beschrieben. Bei der Be-

46 Vgl. Bosch, JA 2006, S. 748; Bär 2007, S. 196-197; Kilian 2018, Computerrecht, 1. Abschnitt. Erläuterungen Teil 7, Rn. 17.

obachtung von Positionsdaten handelt es sich um einen klassischen Fall der Observierung mit Hilfe von technischen Mitteln. Werden die technischen Mittel länger als 24 Stunden oder an mehr als zwei Tagen eingesetzt, dann müssen zusätzlich die Voraussetzungen von § 163f. StPO erfüllt sein.[47] Insbesondere ist nach § 163f Abs. 3 S. 1 StPO die Genehmigung des zuständigen Gerichts einzuholen.[48] Längerfristige Beobachtungen folgen damit auch aus dem Gesetz. Somit sprechenden Wortlaut und Systematik dafür, dass die Positionsdaten von Gegenständen von der Polizei beobachtet werden können. Zwar ist auch eine längere Beobachtungen von Gegenständen, um Rückschlüsse auf das Verhalten einer Person zu ziehen, ein Eingriff von einiger Intensität, aber die Norm beschreibt dieses ausreichend präzise, schränkt die Fälle ein und sieht zudem noch einen Schutzmechanismus gegen einen rechtswidrigen Einsatz vor (in Form des Richter*innenvorbehalt). Ein Ausufern der Eingriffe wird also mittels Verfahren und dem Wortlaut verhindert.[49] Dementsprechend ist Beobachtung mittels Ortungssystemen ausreichend bestimmt beschrieben.

Hinsichtlich der Speicherung ist allerdings unklar, ob die Norm eine ausreichende Ermächtigungsgrundlage darstellt. Die Speicherung wäre gerade im Bereich der bandenmäßigen und gewerbsmäßigen Kriminalität kriminalistisch sinnvoll, da so Bewegungsprofile vom Diebstahl bis hin zu den Hehler*innen oder zu einem Abtransport ins Ausland erstellt werden könnten.[50] Dadurch wäre die Polizei in der Lage, Strukturen der Kriminalität zu erkennen und nachzuvollziehen. In der Rspr. zur Nutzung von GPS-Daten wird nicht ausdrücklich erwähnt, ob die Daten gespeichert und ob Bewegungsprofile erstellt werden dürfen. Es wird vertreten, dass die Speicherung von GPS-Daten nicht von § 100h Abs. 1 S. 1 Nr. 2 StPO umfasst sei.[51] Zur Begründung wird auf den Wortlaut der Regelung Bezug genommen, in dem das Speichern von Daten nicht erwähnt wird.[52] Für die Ansicht spricht, dass in den §§ 100a StPO ff. vielfach explizit die Aufzeichnung der Daten genannt wird. Insofern könnte daraus der Umkehrschluss zu ziehen sein, dass dies bei § 100h StPO gerade nicht vorgesehen ist.

47 Steinmetz, NStZ 2001, S. 349; Soiné, NStZ 2014, S. 600.
48 Vgl. BGH NJW 2001, 1658 (1669); Singelnstein, NStZ 2014, S. 310.
49 Vgl. dazu BVerfG NJW 2016, 1781, 1786.
50 Umfangreich zu Persönlichkeitsprofilen und deren Risiken Hornung, ZD 2005, S. 159-162.
51 Gercke 2006, S. 405.
52 Gercke 2006, S. 405.

Auf der anderen Seite ging es in der Fallkonstellation, in der das OLG Düsseldorf,[53] der BGH,[54] das BVerfG[55] und der EGMR[56] die Verwertbarkeit von GPS-Daten prüften und für rechtmäßig befanden, darum, dass diese Daten auch gespeichert wurden. Also geht die höchstrichterliche Rechtsprechung offensichtlich davon aus, dass auch die Speicherung als logische Konsequenz der Erhebung umfasst ist. Für eine solche Interpretation spricht, dass § 100h Abs. 1 S. 1 Nr. 2 StPO gerade als Generalklausel konzipiert wurde, die es ermöglichen soll, auf neue technische Entwicklungen zu reagieren. Auch wenn sich aus dem Wortlaut der Vorschrift damit nicht direkt die Speicherung ergibt, so könnte diese aus dem Sinn und Zweck der Norm folgen, neue technische Entwicklungen abzudecken. Viele technische Neuerungen und auch die GPS-Technologie umfassen gerade die Speichermöglichkeit.[57] Die Generalklausel bezüglich technischer Anwendungen könnte damit den Willen des Gesetzgebers ausdrücken, dass diese technischen Neuerungen auch effektiv eingesetzt werden.[58] Zudem bestände andernfalls nur die Möglichkeit, dass sich die beobachtenden Polizeibeamt*innen Notizen über die Bewegungen machen, was aber aufgrund der technischen Möglichkeiten realitätsfremd erscheint.

Gegen eine solche Auslegung könnte sprechen, wenn die Speicherung von Bewegungsdaten ein so schwerer Grundrechtseingriff ist,[59] dass er nicht mehr unter diese Norm subsumiert werden kann, weil die Vorschrift in Relation zur schwere des Eingriffs zu unpräzise ist. Je höher die Eingriffsintensität ist, desto präziser muss die Ermächtigungsgrundlage ausgestaltet sein.[60] Dementsprechend könnte § 100h Abs. 1 S. 1 Nr. 2 StPO als Generalklausel für technische Observation ungeeignet[61] und eine speziellere Norm erforderlich sein.

Schwer wiegen etwa Eingriffe in die Privatsphäre[62] oder die Tangierung des Kernbereichs der Persönlichkeit.[63] Von einem Eingriff in die Privatsphäre ist dann auszugehen, wenn Informationen umfasst sind, die typischerweise dem privaten Bereich zugeordnet werden.[64] Ferner sind bei der Beurteilung

53 OLG Düsseldorf, NStZ 05/1998, 268 (268 ff.).
54 BGH NStZ 2001, 386 (386 ff.).
55 BVerfG NJW 2005, 1338 (1338 ff.).
56 EGMR NJW 2011, 1333 (1333 ff.).
57 Vgl. Gercke 2006, S. 505 m. w. N.
58 Vgl. BGH NStZ 2001, 386 (387).
59 So etwa Fock/Möhle, GSZ 2021, 174.
60 BVerfG, NVwZ 2007, 688 (690).
61 Vgl. Faßnacht 2011, S. 82.
62 BGH NJW 2013, 2530 (2536); BGH NStZ-RR 2014, 187 (189).
63 Vgl. Gusy, StV 1998, S. 527; Jarass/Pieroth-Jarass 2022, Art. 2, Rn. 47 ff.,74; Rückert ZStW 2017, S. 321.
64 BVerfG, Beschl. V. 24.2.2015 - 1 BvR 472/14 - Rn. 29.

die Eingriffsschwelle die betroffenen Personen sowie die Art und der Umfang der erhobenen Daten zu berücksichtigen. Dabei ist vor Allem entscheidend, wie viele Rückschlüsse aus den Daten auf eine bestimmte oder bestimmbare Person(en) gezogen werden können.[65] Ferner wirkt sich die Heimlichkeit der Maßnahme auf die Intensität des Eingriffes aus. Bei heimlichen Maßnahmen ist es den Betroffenen weder möglich, sich direkt gerichtlich gegen die Maßnahme zur Wehr zu setzen, noch auf andere Weise die Ermittlungen zu beeinflussen.[66] Auch kann der Einsatz von technischen Hilfsmitteln den Eingriff erschweren, da Daten gezielter und effektiver erhoben und anschließend zusammengefügt werden können.[67]

Zunächst ist eine Speicherung bei Positionsdaten zu betrachten, die zur Aufklärung von banden- und gewerbsmäßiger Kriminalität erfolgen. Für einen schweren Grundrechtseingriff spricht die Heimlichkeit der Überwachungsmaßnahme und die Fixierung der Daten durch die Speicherung. Dadurch sind mehr Rückschlüsse auf die Besitzer*innen möglich. Allerdings sind die erhobenen Daten zwar personenbezogen, weisen aber in erster Linie einen Objektsbezug auf.[68] Genaue Rückschlüsse auf eine Person lassen sich also nur ziehen, wenn diese den Gegenstand oft bzw. regelmäßig nutzt.[69] Im Rahmen von gewerbs- oder bandenmäßiger Kriminalität ist vielfach nicht davon auszugehen, dass die Gegenstände oft von den Täter*innen genutzt werden. Insbesondere scheidet eine private Nutzung regelmäßig aus, die den Eingriff intensivieren würde, da oft die Gegenstände möglichst schnell verkauft werden sollen. Es ist damit zu rechnen, dass in erster Linie der Weg des Gegenstandes vom Ort des Diebstahls bis zu den Hehl*innen oder gutgläubigen Besitzer*innen nachvollzogen werden kann. Diese Wege lassen, wenn überhaupt, nur wenige Rückschlüsse auf den privaten Bereich der betroffenen Personen zu und erst Recht keine auf den Kernbereich der Persönlichkeit. Vielmehr wird nur das kriminelle Verhalten dokumentiert.[70] Ferner können Daten einzelner Personen nur verarbeitet werden, solange sie den Gegenstand im Besitz haben. Es ist jedoch damit zu rechnen, dass die Gegenstände zügig an andere weitergegeben werden. Für die Polizei ist im Regelfall gar nicht ersichtlich, wer den Gegenstand gerade nutzt, bei wem sich dieser befindet bzw. wer diesen transportiert, wodurch der Eingriff deutlich

65 Vgl. BVerfGE 65, 1 (45); BVerfG SVR 09/2008, 344 (344 f.); BGH NStZ-RR 2014, 187 (189); Gasch 2012, 97; Weichert, SVR 2009, S. 350.

66 Arzt 2006, S. 231; Kilian 2018, S. 1. Abschnitt. Teil 13, Rn. 16 f.; Rückert, ZStW 2017, S. 320.

67 Vgl. BVerfGE 65, 1 (45); OLG Koblenz NJW 2007, 2863 (2863); Gasch 2012, S. 97; Müller/Schwabenbauer 2021, G Rn. 796.

68 Abdallah/Gercke, CR 2003, S. 300; vgl. Neumann 2014, S. 317.

69 Neumann 2014, S. 318.

70 Vgl. Vgl. BVerfG, Urt. v. 16. 6. 2009, 2 BvR 902/06; BVerfG, NJW 1990, 563 (564).

weniger schwerwiegend ist.[71] Rückschlüsse auf Personen sind folglich nur begrenzt möglich, wenn mehrere Personen an den Diebstählen beteiligt sind. Dies macht aber gerade das Wesen der gewerbs- und bandenmäßigen Kriminalität aus. Auch ist weder das Interesse am Persönlichkeitsschutz der Mitglieder von kriminellen Organisationen als besonders schutzwürdig einzustufen, da sie selbst durch den Diebstahl die Ursache für die Datenerhebung gesetzt haben.

Zu berücksichtigen ist aber auch, dass die Polizei vielfach nicht wissen kann, ob gutgläubige Besitzer*innen betroffen werden. In diesem Fall ist von einer gesteigerten Eingriffsintensität auszugehen. Das Risiko, dass gegen Unschuldige ermittelt wird, ist dem Strafverfahren jedoch stets immanent. Gegen diese Risiken müssen aufgrund der möglichen schweren Eingriffe nach der StPO Schutzmechanismen vorgesehen werden. Eine längere Observierung ist an einen Richtervorbehalt geknüpft, dementsprechend muss es eine Speicherung der Daten über einen längeren Zeitraum erst recht sein. Von der Polizei muss fortlaufend geprüft werden, ob eine längere Speicherung noch kriminalistisch sinnvoll und mit den Grundrecht auf informationelle Selbstbestimmung vereinbar ist. Sofern es sich um längere Beobachtung handelt, wird diese Entscheidung von einem Gericht überprüft. Dabei muss das Risiko, dass gutgläubige Besitzer*innen und damit Unschuldige von der Speicherung betroffen sind, gewichtet werden. So muss aus den bisherigen Ermittlungstätigkeiten hervorgehen, dass die Gegenstände mit einer hohen Wahrscheinlichkeit noch im Besitz von Personen aus kriminellen Strukturen sind. Die längere Speicherung macht aus ermittlungstaktischer Sicht zudem vielfach keinen Sinn, da die Daten auch ausgewertet werden müssten und die begrenzte Aussagekraft in vielen Situationen bekannt sein dürfte, insbesondere, weil viele Gegenstände schnell weitergeben werden können. Dies wirkt sich insbesondere auf die Geeignetheit und die Erforderlichkeit der Maßnahme aus, die vielfach nicht gegeben sein dürften, wenn die Diebstähle länger zurückliegen. Insofern ist von einem ausreichenden Schutzmechanismus auszugehen.

Dies gilt auch für wertvolle Gegenstände. Dabei muss geprüft werden, welche Rückschlüsse aus dem Gegenstand auf die Person möglich sind und wie weit sie die Persönlichkeit betreffen. Auch hier ist die Wahrscheinlichkeit zu prüfen, dass der Gegenstand an Unschuldige weitergegeben wurde. Intensive Rückschlüsse auf die Persönlichkeit sind auch bei wertvollen Gegenständen in der Regel nur bei längeren Zeiträumen zu erwarten. Dementsprechend scheint eine differenzierte Lösung im Einzelfall möglich.

Vor diesem Hintergrund ist insgesamt durch die Speicherung von Positionsdaten gestohlener Gegenständen unter den Voraussetzungen des 100h StPO vielfach nicht von einem Eingriff auszugehen, der so schwer wiegt, dass die

71 Vgl. BGH NJW 2013, 2530 (2537).

Norm zu unbestimmt erscheint.[72] Eine differenzierte Betrachtung im Einzelfall ist möglich. Da die Speicherung an enge Voraussetzungen geknüpft ist und es bei technischen Neuerungen wesensfremd erscheint, dass Daten grundsätzlich nicht gespeichert werden dürfen, ist es vertretbar durch Auslegung der Norm eine Speicherung von Positionsdaten in § 100h StPO mit der höchstrichterlichen Rechtsprechung anzunehmen. Auch wenn die Norm gleichwohl oft ausreichen wird, ist es im Interesse der Bestimmtheit und der Klarheit sinnvoll, die Normen hinsichtlich der Beobachtung von Gegenständen zu konkretisieren und entsprechend nach zu schärfen. Dies würde die Anwendung erheblich erleichtern und der Gesetzgeber könnte rechtsstaatliche Grenzen für die Ortung klarer definieren. Gelungen erscheint die Norm nicht. Zumindest sollte klar ersichtlich sein, was unter einer Verwendung technischer Mittel zu verstehen ist.

### *2.1.3 Zusammenfassung*

Abschließend lässt sich festhalten, dass die Polizei im Falle von banden- und gewerbsmäßigen Diebstählen und bei besonders wertvollem Diebesgut die Bewegungen des Diebesgutes mit Ortungstechnologie beobachten und die dazugehörigen Daten vielfach fallbezogen speichern und verwenden darf. Beobachtungen über 24 Stunden müssen vom Gericht genehmigt werden. Der Richter*innenvorbehalt ist nicht nur auf die Beobachtung beschränkt, sondern findet auch dann Anwendung, wenn Datenmaterial durchgehend über 24 Stunden oder länger erhoben wurde und erst nachträglich gesichtet werden soll. Eine Auswertung der Daten ist nur im Rahmen der konkreten Observation möglich; Daten dürfen nicht auf Vorrat gespeichert werden.

## *2.2 § 163 Abs. 1 StPO als Ermächtigungsgrundlage für das GPS-Tracking?*

Ferner ist zu prüfen, ob die Polizei mittels Ortungstechnologie den Standort gestohlener Gegenstände feststellen kann und diese Daten speichern und verwenden darf, wenn es sich nur um einen einfachen Diebstahl handelt.

In diesem Fall kommt mangels einer anderen Eingriffsgrundlage nur die Ermittlungsgeneralklausel aus den §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO in Betracht.[73]

72 Vgl. EGMR NJW 2011, 1333 (1335 ff.); Bär 2007, S. 196-197.

73 BVerfG NJW 2009, 1405 (1407); Verfassungsgerichtshof Rheinland-Pfalz, Urteil v. 24. Februar 2014 – VGH B 26/13 –, Rn. 48.

### 2.2.1 Anwendbarkeit der Generalklausel

§ 100h Abs. 1 S. 1 Nr. 2 StPO stellt keine speziellere Norm dar, weil explizit von Observation gesprochen wird, die nicht vorliegt (s. o.). Andere Ermächtigungsgrundlagen zur Ortung sind nicht ersichtlich.

Der Einsatz von technischen Mitteln könnte generell ausgeschlossen sein, da in § 100h StPO ausdrücklich von technischen Mitteln gesprochen wird und in den §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO nicht.[74] Dagegen spricht aber, dass nach § 163 Abs. 1 StPO der Polizei der Einsatz von Hilfsmitteln grundsätzlich nicht verwehrt ist, etwa ein Fernglas.[75] Auch muss im Rahmen der teleologischen Auslegung der Gegenwartszweck der Norm berücksichtigt werden. Die Hilfsmittel werden aufgrund der technischen Entwicklung auch immer mehr technische Funktionen aufweisen. Auch hat die technische Entwicklung dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürgerinnen und Bürger von zentraler Bedeutung ist.[76] So wird sich auch die Ermittlungsarbeit zunehmend in den digitalen Raum verlagern, was ohne den Einsatz von technischen Mitteln nicht möglich ist.[77] Diese Maßnahmen werden sich nicht alle spezifisch gesetzlich normieren lassen (vor Allem Eingriffe mit einer sehr geringen Intensität), sodass auch dazu Generalklauseln erforderlich sind. Solange der Einsatz der technischen Mittel nur zu leichten Grundrechtseingriffen führt, können diese auch durch die §§ 161 Abs. 1. S. 1, 163 Abs. 1 StPO gerechtfertigt sein.[78]

### 2.2.2 Tatbestandvoraussetzungen der Generalklausel

Die Generalklausel legitimiert lediglich Ermittlungsmaßnahmen mit geringer Eingriffsintensität,[79] etwa die nicht eingriffsintensiven visuellen kurzzeitige Beobachtung von Tatverdächtigen im öffentlichen Raum.[80] Im Hinblick auf die Datenerhebung und die Datenverarbeitung gilt, dass die Generalklausel nur einschlägig sein kann, wenn aufgrund eines konkreten Anlasses Daten eines eng begrenzten, verdächtigen Personenkreises erhoben werden.[81]

---

74 Vgl. Gercke/Julius/Temming/Zöller-Zöller 2012, § 163f. Rn. 2

75 Keller/Kay 2016, 45; Gercke/Julius/Temming/Zöller-Zöller 2012, § 163f, Rn. 3.

76 BVerfG NJW 2008, 822 (824).

77 Vgl. BVerfG NJW 2008, 822 (836); Rückert, ZStW 2017, S. 303-304; Soiné, NStZ 2014, S. 251.

78 Vgl. Soiné, NStZ 2014, S. 251.

79 Z. B. BGHSt 51, 211, 218.

80 Vgl. dazu BVerfG NJW 2009, 1405 (1407); BGH, NStZ 1992, 44 (44f.); Verfassungsgerichtshof Rheinland-Pfalz, Urteil vom 24. Februar 2014 – VGH B 26/13 –, Rn. 48.

81 Spernath, NStZ 2010, S. 311; BVerfG NJW 2009, 1405 (1407).

Zunächst ist zu prüfen, ob die Ortung, die bezweckt einen gestohlenen Gegenstand sofort sicherzustellen, als schwerer Eingriff einzustufen ist. D. h. es geht um Fälle, in denen die Polizei diesen ortet, um danach direkt zu dessen Standort zu fahren, um diesen zu beschlagnahmen, ohne Daten zu speichern oder die Bewegungen beispielsweise eines Fahrrades oder eines PKWs länger als zur Ortung nötig zu beobachten.

Im Falle der Ortung erfolgt diese heimlich und ermöglicht eine Beobachtung aus der Ferne, ohne dass die Betroffenen davon Kenntnis nehmen können.[82] Allerdings steht die Heimlichkeit einer Maßnahme der Anwendung der §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO dann nicht entgegen, wenn die Maßnahme insgesamt nur geringfügig in die Grundrechte Betroffener eingreift.[83] Es muss beachtet werden, dass eine Ortung nicht überraschend für die Täter*innen ist, da heutzutage jeder und jede damit rechnen muss, dass Ortungstechnologie in Gegenständen verbaut ist. Ferner wird ein sehr konkreter Tatverdacht dadurch begründet, dass die Person im Besitz des gestohlenen Gegenstands ist und die Maßnahme bezieht sich nur auf diese Person.

Der Ort des Gegenstandes weißt regelmäßig eine geringere Persönlichkeitsrelevanz auf.[84] Die Rückschlüsse, die aus einem einmaligen Aufenthalt an einem Ort geschlossen werden können, sind überwiegend gering, da der Aufenthalt dort auch zufällig sein kann. Für vertiefte Schlussfolgerungen über die Person sind üblicherweise längere Beobachtungen erforderlich. Auch geht der Persönlichkeitsbezug verloren, wenn sich der Gegenstand an Orten befindet, die keine Rückschlüsse auf Personen zulassen.[85] Werden nur Bewegungen im öffentlichen Raum beobachtet, wird allein dadurch die Eingriffsqualität gesenkt. Daher ist gerade bei Fahrzeugen der Eingriff durch deren Ortung gering, da diese sich vorwiegend im öffentlichen Straßenverkehr bewegen.

Auch bei Personen, die den Gegenstand ohne Kenntnis vom Diebstahl im Besitz haben, ist der Eingriff durch die Ortung gering. Zwar wiegt er schwerer als bei den Dieb*innen oder Hehler*innen, da diese Personen nicht mit einer Ortung rechnen mussten. Aber letztlich ist der Eingriff nur sehr kurz und lässt kaum Rückschlüsse auf die Person zu, die über die Nutzung des Gegenstandes hinausgehen, wobei dies abhängig von der Art des Gegenstandes auch anders beurteilt werden kann.

Durch den eindeutig festgelegten und beschränkten Zweck der Maßnahme, wird deren Gewicht also erheblich verringert. Dies kann auch technisch sichergestellt werden, indem die IT-Anwendung erst gar nicht ermöglicht, Be-

82 Vgl. Hornung/Schindler, ZD 2017, S. 206.
83 BVerfG NJW 2009, 1405 (1407); vgl. Rückert, ZStW 2017, S. 320.
84 BVerfG, Urteil vom 11.3.2008 - 1 BvR 2074/05 - Rn. 88.
85 Vgl. Weichert, DuD 2009, S. 350.

wegungsmuster nachzuverfolgen. So kann die aktuelle Position lediglich als Punkt auf einer Karte dargestellt werden, der sich bewegt, ohne, dass die zurückgelegte Route anzeigt wird.

Insgesamt ist der Eingriff durch die bloße Ortung daher als nicht intensiv einzustufen.[86] Dementsprechend fällt die bloße Ortung zur einmaligen Ermittlung des Standortes des Gegenstandes unter §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO.

Allerdings darf die Polizei aber nach §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO keine Bewegungsprofile nachvollziehen und diese schon gar nicht speichern. Ein entsprechender Eingriff würde Rückschlüsse auf die Person eröffnen, die durch die Ermittlungsgeneralklausel nicht gerechtfertigt werden können. Auch die Generalklausel zur Datenverarbeitung aus § 483 Abs. 1 1. und 2. Alt. StPO umfasst nicht die Berechtigung, zusätzliche Daten zu erheben, dies muss aus speziellen Ermächtigungsgrundlagen folgen.

Es stellt sich allerdings die Frage, ob bei der Ortung ebenfalls Speichervorgänge ablaufen. Die Visualisierung von Positionsdaten erfolgt in der Regel so, dass die letzte ermittelte Position auf einer Karte solange angezeigt wird bis ein neues Signal eingeht. Solange befinden sich die Positionsdaten im Arbeitsspeicher und werden anschließend überschrieben. Dies ist auf den Umstand zurückzuführen, dass ansonsten eine Ortung nicht praktikabel durchführbar wäre; die Beamt*innen müssten andernfalls immer auf das gesendete Signal warten ohne Positionen auf der Karte zu sehen. So ist es sehr schwierig den Standort zu ermitteln. Auch eine Erhöhung der Sendefrequenz erscheint nicht immer sinnvoll, da so der Akku des Gerätes zu stark beansprucht würde. Insofern stellt sich die Frage, ob das kurzzeitige Verbleiben des Standortes im Arbeitsspeicher ein „Speichern" darstellt, für das eine gesonderte Ermächtigungsgrundlage nötig wäre.

Dafür könnte sprechen, dass eine kurzzeitige Fixierung auch im Arbeitsspeicher erfolgt. Insofern ist anerkannt, dass eine Speicherung im Arbeitsspeicher auch eine Vervielfältigung im Sinne des Urheberrechtsgesetzes darstellt.[87] Allerdings muss dabei der konkrete Vorgang betrachtet werden, da es nicht sachgerecht erscheint, jede Form der kurzfristigen Fixierung als ermächtigungsgrundlagenbedürftige Speicherung einzustufen. Vorliegend verbleibt der letzte Standort für kurze Zeit im Arbeitsspeicher bis der nächste Standort gesendet wird. Hierbei geht es gerade nicht darum, dass Datum dauerhaft zu fixieren, sondern nur um die Praktikabilität der Ortung sicherzustellen, die gerade ein dauerhaftes Speichern ausschließen soll. Auch in anderen Rechtsgebieten wer-

86 Vgl. BVerfG, Urteil vom 11.3.2008 – 1 BvR 2074/05.

87 OLG Hamburg ZUM 2001, 512 (513); Wandtke/Bullinger 2022, § 16 Rn. 18 m. w. N.; Dreier/Schulze-Schulze 2022, UrhG § 16 Rn. 13 m. w. N.

den daher bewusst an die kurzfristige Fixierung eines Datums keine Konsequenz geknüpft. So ist hinsichtlich des Tatbestandes der Fälschung von beweiserheblichen Daten nach § 269 StGB anerkannt, dass ein Datum im flüchtigen Arbeitsspeicher nicht als Datum im Sinne der Vorschrift anzusehen ist, da dieses automatisch gelöscht wird, wenn der Bearbeitungsvorgang beendet ist oder die Stromzufuhr unterbrochen wird.[88] Auch müssen Daten aus dem Arbeitsspeicher erst noch gesondert gespeichert werden, damit sie im Sinne der §§ 94 StPO ff. beschlagnahmt werden können. Bei einem flüchtigen und kurzen Aufenthalt im Arbeitsspeicher besteht auch keine wesentliche Gefahr für das Recht auf informationelle Selbstbestimmung. Von einer solchen ist nur auszugehen, wenn das Ziel des „Speichervorganges" auf eine dauerhafte Fixierung des Datums oder seine Verbreitung gerichtet ist. Dies kann im Rahmen der Urheberrechtsverletzung der Fall sein, da bei einigen Onlineplattformen die Nutzer*innen auf den Arbeitsspeicher zahlreiche Personen zugreifen können und anschließend das Datum speichern können. Um keine Regelungslücken offen zu lassen, hat sich der Gesetzgeber daher entschieden, mit § 16 Abs. 1 UrhG auch den kurzfristigen Aufenthalt im Arbeitsspeicher mit zu umfassen.[89] Im Rahmen der Ortung ist aber weder vorgesehen, dass andere auf den Arbeitsspeicher zugreifen können, noch sollen die Positionsdaten dauerhaft gespeichert werden. Damit kann nicht von der Möglichkeit einer dauerhaften Fixierung und damit auch nicht von einer Speicherung gesprochen werden.

Insgesamt kann festgehalten werden, dass der kurzfristige Aufenthalt des Standortdatums im Arbeitsspeicher keine Speicherung darstellt.

### *2.3 Ortung und Datenerhebung nach Gefahrenabwehrrecht?*

Ferner ist zu klären, ob die Polizei auch berechtigt wäre, zur Gefahrenabwehr Gegenstände zu orten, diese zu beobachten und die Daten zu speichern. Exemplarisch wird dies am Beispiel des Berliner ASOG geprüft.

Die Ortung zur Sicherstellung kann über § 18 Abs. 1 Satz 2 ASOG erfolgen. Da keine Spezialermächtigung vorhanden ist[90] und der Eingriff mangels Speicherung der Daten nur sehr gering ist (siehe vorheriger Abschnitt), kann hier auf die Datenerhebungsgeneralklausel zurückgegriffen werden. Durch die Entwendung des Gegenstandes ist ein rechtswidriger Zustand geschaffen worden, sodass eine Gefahr für die öffentliche Sicherheit vorliegt. Die Ortung stellt eine Datenerhebung dar. Der Anwendung der Norm steht auch nicht entgegen,

88 Kindhäuser/Neumann/Paeffgen/Albrecht/Altenhain-Puppe-Schumann 2017, § 269 Rn. 20; Hefendehl-Erb 2022, § 269 Rn. 32 m. w. N.

89 Drucksache 15/38, S. 18; vgl. Dreier-Schulze 2022 § 16 Rn. 13.

90 Vgl. Knape/Schönrock 2016, § 18, Rn. 39.

dass die Ermittlungen entgegen § 18 Abs. 2 Satz 1 ASOG verdeckt durchgeführt werden, die Polizei tritt für die Betroffenen nicht in Erscheinung,[91] da die Polizei mangels Kenntnis von der Person des Besitzers des Gegenstandes die Ermittlungen gar nicht offen durchführen kann. Insofern wäre zwingend der Erfolg der Maßnahme gefährdet, vgl. § 18 Abs. 2 Satz 2 ASOG. Insgesamt ist die Datenerhebungsgeneralklausel aus dem ASOG auch weniger problematisch anwendbar als die Ermittlungsgeneralklausel aus der StPO, da § 18 ASOG eindeutig auf Datenerhebung ausgerichtet ist und diese klarer umschreibt.

Eine Speicherung der Positionsdaten kann nicht nach § 42 Abs. 2 S. 1 ASOG erfolgen, da die GPS-Daten für die bloße Wiedererlangung des Gegenstandes nicht gespeichert werden müssen. Dazu ist es ausreichend, wenn die Polizei zu dem Standort des Diebesgutes fährt. Für die Dokumentation des Einsatzes sind die Daten ebenfalls nicht erforderlich, da dafür der Bericht der Polizeibeamt*innen ausreichend ist.

Auch § 25 Abs. 1 Satz 1. Nr. 2 ASOG ist nicht anwendbar, da die Gegenstände damit vor dem Diebstahl und damit auch vor dem rechtswidrigen Zustand beobachtet werden müssten. Zu diesem Zeitpunkt befinden sie sich aber noch im Besitz der Geschädigten.

Zur Gefahrenabwehr ist also nur eine Ortung zur Sicherstellung möglich.

Fraglich ist aber, ob die Maßnahme sich nach dem Gefahrenabwehr- oder dem Strafverfolgungsrecht richtet. Nach der neueren Rechtsprechung des BGH können strafprozessuale und gefahrenabwehrrechtliche Maßnahmen nebeneinander angewendet werden.[92] Dies vermag allerdings nicht zu überzeugen, da die Polizei so in die Lage versetzt wird, die Ermächtigungsgrundlage auszuwählen, die geringere tatbestandliche Anforderungen aufweist.[93] In solchen Konstellationen könnten also die jeweils strengeren tatbestandlichen Anforderungen unterlaufen werden, die gerade den besonderen Umständen der Situation (etwa der sehr eingriffsintensiven Strafverfolgung) Rechnung zollen und daher von der Legislative bewusst ausgewählt worden sind. Auch kann sich die Polizei so der verfahrenslenkenden Funktion der Staatsanwalt entziehen, wenn sie bewusst auf Maßnahmen der Gefahrenabwehr zugreift. Mithin bedarf es klarer Kriterien zur Abgrenzung. In der verwaltungsgerichtlichen Rechtsprechung ist seit langem anerkannt, dass sich die rechtliche Einordnung der Maßnahme nach dem damit verfolgten Schwerpunkt bemisst.[94] Auch wenn dadurch die Abgrenzung im Einzelfall schwierig sein kann, so überzeugt diese Herangehensweise mehr als das völlig konturlose Vorgehen des BGH. Auch

91 Baller/Eiffler/Tschisch 2004 § 18, Rn. 11.

92 BGH Urteil v. 26.04. 2017 - 2 StR 247/16, Rn. 25 ff.

93 Lenk, StR 2017, S. 695 m. w. N.; Aden/Fährmann 2021, S. 595 f.

94 Z. B. BVerwGE 47, 139 (147); BVerwGE 121, 345 (348).

die Ansichten, die einen generellen Vorrang der Strafverfolgung sehen, wenn diese begonnen hat,[95] oder die Meinung, die im Zweifel der Gefahrenabwehr Vorrang einräumt,[96] vermögen nicht zu überzeugen. Dies rührt daher, dass dadurch nicht auf die besonderen Umstände des Einzelfalles reagiert werden kann. So sind beispielsweise Situationen denkbar, in denen im Rahmen der Strafverfolgung aufgrund veränderter Umstände Gefahrenabwehrmaßnahmen notwendig werden. Auch überzeugt der BGH insofern, dass die Grenzen zwischen präventivem Handeln und repressivem Vorgehen fließend sein können.[97] Es wird daher auch Maßnahmen mit einer doppelten Zielrichtung geben. Diese müssen aber aus den beschriebenen Gründen auf Fälle begrenzt werden, in denen eine Abgrenzung nicht geleistet werden kann, was in den meisten Fällen aber möglich sein wird. In allen anderen Konstellationen ist auf den Schwerpunkt der Maßnahme abzustellen.

Wo liegt aber der Schwerpunkt bei der Ortung zur Sicherstellung des Diebesgutes? Durch eine schnelle Ortung und Sicherstellung wird die Polizei einerseits in die Lage versetzt, den Geschädigten den gestohlenen Gegenstand möglichst schnell und unkompliziert wieder zu geben. Auf der anderen Seite dient der Gegenstand und dessen Zuordnung zu einer bestimmten Person aber auch dazu, um die Täter*innen zu identifizieren. Auch kann es sein, dass der Gegenstand noch auf weitere Hinweise untersucht wird, sodass die Geschädigten ihren Gegenstand nicht zwingend sofort wiedererhalten. Daher können sich nach dem Auffinden des Gegenstandes noch weitere strafprozessuale Maßnahmen wie eine Beschuldigtenvernehmung oder Zeug*innenbefragung anschließen. Allerdings kann ein Gegenstand durch die Ortung aber auch ohne die Täter*innen aufgespürt werden, z. B. wenn sich der Gegenstand im öffentlichen Raum befindet. In so einem Fall wird die Polizei den Geschädigten den Gegenstand üblicherweise zeitnahe aushändigen und keine weiteren Maßnahmen der Strafverfolgung mehr einleiten. Der Zeitpunkt der Ortung ist mithin neutral, da die Polizei noch gar nicht genau weiß, ob sich an das Auffinden des Gegenstandes noch weitere strafprozessuale Maßnahmen anschließen. Vor diesem Hintergrund ist eine Doppelfunktionalität zu bejahen.

### 3. Kann die Polizei die Tracking-Daten von Privatpersonen verwenden?

Die Geschädigten könnten allerdings die Trackingdaten gestohlener Gegenstände auch selbst speichern oder vom Trackingservice-Anbieter*innen speichern

95 Gubitz, NStZ 2016, S. 128; Müller/Römer, NStZ 2012, S. 546.
96 Pieroth/Schlink/Kniesel/Kingreen/Poscher 2016, S. 24-25.
97 BGH Urteil v. 26.04. 2017 - 2 StR 247/16, Rn. 30.

lassen und diese an die Polizei übertragen, damit diese das Diebesgut aufspüren kann. Insofern hätte die Polizei selbst keine Daten erhoben, sondern würde nur vorhandene Daten verwenden.

Vorliegend obliegen der Einbau und zumindest die Datenerhebung direkt nach dem Diebstahl den (potenziell) Geschädigten. Schließlich kann die Polizei die Gegenstände mangels Zuständigkeit im Vorfeld eines Diebstahlsdelikts nicht mit Trackingsendern ausstatten und erst Daten erheben, wenn sie vom Diebstahl erfährt. Da die Geschädigten zur Erhebung und Verarbeitung der Positionsdaten aber selbst größtenteils nicht in der Lage sind, werden sie einen entsprechenden Vertrag mit einer Anbieter*in für den Trackingservice abschließen und diese wird dann aufgrund ihrer vertraglichen Verpflichtung die Daten erheben und an die Geschädigten weitergeben. Daher ist zu prüfen, ob sowohl die Trackingservice-Anbieter*innen als auch die Geschädigten berechtigt sind, die Positionsdaten gestohlener Gegenstände zu erheben und an die Polizei weiterzugeben. Dabei ist besonders zu berücksichtigen, ob und wann eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Besitzer*innen des gestohlenen Gegenstandes vorliegt.

### *3.1 Sind Privatpersonen von Ermittlungsmaßnahmen grundsätzlich ausgeschlossen?*

Die Durchführung von Ermittlungsmaßnahmen und die dazu nötige Beweissammlung ist nach der StPO Aufgabe der Polizei. In der beschriebenen Konstellation würden wesentliche Beweise aber von Privatpersonen erhoben und die Polizei würde diese nur entgegennehmen. Grundsätzlich sind Privatpersonen jedoch nicht von eigenen Ermittlungsmaßnahmen ausgeschlossen.[98] Vielmehr ergibt sich für die Strafverfolgungsorgane aus dem strafprozessualen Untersuchungsgrundsatz (§§ 155 Abs. 2, 244 Abs. 2 StPO) die Pflicht zur umfassenden Sachverhaltsaufklärung, sodass sämtliche Erkenntnis- und Informationsquellen auszuwerten sind, d. h. auch solche, die von Privatpersonen stammen.[99] Allerdings können gewisse Ermittlungsmaßnahmen nur durch staatliche Institutionen durchgeführt[100] und nicht in den privaten Bereich ausgegliedert werden.[101] Vorliegend kann bei dem Erhebung von Positionsdaten dieser Bereich aber gar nicht betroffen sein, da es sich um eine Maßnahme handelt, die dazu dient, das Eigentum oder den Besitz der Geschädigten besonders zu sichern, indem das Auffinden von gestohlenen Gegenständen erleichtert

98 Stoffer 2014, S. 144.
99 Eckhardt 2009, S. 147; Stoffer 2014, S. 147.
100 Stoffer 2014, S. 143.
101 OLG Frankfurt NStZ-RR 2017, 188, (189 ff.)

wird. Dies ist aber gerade keine staatliche Aufgabe, sondern obliegt jeder Privatperson selbst, wie etwa die Installation einer Alarmanlage oder die Videoüberwachung des eigenen Grundstückes. Die Grundlage für solche Maßnahmen können nur im Vorfeld der Straftat geschaffen werden, sodass die Polizei in der Regel noch gar nicht zuständig sein kann. Außerdem besteht auch ein zivilrechtliches Interesse an den Positionsdaten, da diese auch als Beweise zur Durchsetzung von zivilrechtlichen Ansprüchen genutzt werden können. Demensprechend können Privatpersonen die Positionsdaten gestohlener Gegenstände grundsätzlich erheben.

### *3.2 Haben Privatpersonen die rechtliche Befugnis zum Tracking?*

Allerdings könnten die Geschädigten nicht berechtigt sein, die Positionsdaten zu erheben bzw. zu speichern. Auch auf der zivilrechtlichen Ebene liegt ein Eingriff in das Allgemeine Persönlichkeitsrecht (im zivilrechtlichen Sinne) und damit in eine Rechtsposition der Besitzer*innen der gestohlenen Gegenstände vor. Dementsprechend kann eine entsprechende Datenverarbeitung rechtswidrig sein. Eine rechtmäßige Bearbeitung könnte aus Art. 6 Abs. 1 Satz 1 f DS-GVO folgen.

#### *3.2.1 Anwendbarkeit der DS-GVO?*

Damit Art. 6 Abs. 1 Satz 1 f DS-GVO Anwendung finden kann, müsste die DS-GVO aber zunächst einschlägig sein. Der sachliche Anwendungsbereich bestimmt sich nach Art. 2 DS-GVO. Dazu ist nach Abs. 1 eine Verarbeitung von personenbezogenen Daten erforderlich. Ein Fall der Datenverarbeitung liegt nach der Legaldefinition aus Art. 4 Nr. 2 DS-GVO vor, da eine Erhebung von Positionsdaten bzw. deren Veranlassung durch die Geschädigten erfolgt. Diese sind auch personenbezogen (siehe dazu ausführlich unter 2). Allerdings könnte Art. 2 Abs. 2 c DS-GVO der Anwendbarkeit entgegenstehen. Diese sogenannte Haushaltsausnahme[102] liegt vor, wenn Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten verarbeitet werden.[103] Dies ist der Fall, wenn die Verarbeitung ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit erfolgt.[104] Solange die Nutzung einen auch nur teilweisen beruflichen Bezug aufweist (Mischnutzung), findet die DS-GVO Anwendung.[105] Es wird also die soziale Sphäre in Form

102 Gola/Heckmann 2022, Art. 2, Rn. 15.
103 Kritisch zur Weite der Ausnahme Gola/Lepperhoff, ZD 2016, S. 11.
104 Paal/Pauly-Ernst 2018, DS-GVO Art. 2 Rn. 16.
105 Wybitual- Rauer/Ettig 2017, Art. 2, Rn. 12.

des privaten Bereichs aus der DS-GVO ausgenommen.[106] Dies bezweckt den Schutz der privaten Datenverarbeitung, da diese aufgrund des bestehenden Autonomieanspruches als grundsätzlich schutzwürdiger angesehen wird als die Rechtssphäre der von der Verarbeitung Betroffenen.[107] Einerseits werden durch eine rein private Verarbeitung die Interessen von Betroffenen kaum berührt. Andererseits würde die private Lebensführung, etwa das Tätigen von Urlaubsaufnahmen, auf denen eine andere Person zwangsläufig zu sehen ist, so durch die DS-GVO unverhältnismäßig beeinträchtigt. Mithin ist zu prüfen, ob die Veranlassung oder die Erhebung der Positionsdaten dem privaten Aktionskreis der Geschädigten zuzuordnen ist.[108]

Sämtliche Verarbeitungsvorgänge, die der privaten Kommunikation dienen oder dem Privathaushalt zuzurechnen sind, fallen unter die Haushaltsausnahme.[109] Zu den typischen persönlichen Tätigkeiten, auch im familiären Bereich, gehören beispielsweise Freizeitverhalten, privater Konsum oder Sport. Für die Zuordnung zum privaten Bereich kommt es aber auch auf die Zugriffsmöglichkeit auf die Daten an. Sofern die Nutzung in der Gestalt erfolgt, dass lediglich ein begrenzter Personenkreis, d. h. das persönliche und familiäre Umfeldes der Privatperson, von den Daten Kenntnis erlangt, kann die Ausnahme einschlägig sein.[110] Die Haushaltsausnahme liegt überdies nur vor, wenn die Daten auch in "persönlicher" Art und Weise verwendet werden.[111] Wenn die Daten auch Dritten zur Verfügung gestellt werden - etwa in einem gerichtlichen Verfahren – kann damit der ausschließlich private Charakter entfallen.[112]

Zwar werden die Positionsdaten nicht für eine wirtschaftliche oder geschäftliche Tätigkeit erhoben. Jedoch werden sie gerade erhoben, um sie ggf. im Rahmen des Ermittlungsverfahrens an die Polizei weiterzugeben und um sie ggf. auch im straf- oder zivilgerichtlichen Verfahren zu verwenden. Zwar kann der Vorgang der Speicherung von Positionsdaten grundsätzlich auch dem privaten Bereich zuzuordnen sein.[113] Jedoch spricht die Weitergabe an die Justiz dafür, dass der private Raum gerade verlassen wird.[114] Auch werden perso-

106 von Lewinski 2018, Rn. 21.
107 Sydow-Ennöckl 2022, Art. 2, Rn. 11.
108 Vgl. OLG Celle Beschl. v. 4.10.2017 – 3 Ss (OWi) 163/17, BeckRS 2017, 131819, Rn. 23.
109 Gola/Heckmann 2022, Art. 2, Rn. 15; Lauber-Rönsberg/Hartlaub, NJW 2017, S. 1060.
110 Kühling/Buchner-Buchner 2020, Art. 22, Rn. 25 m. w. N.; Lauber-Rönsberg/Hartlaub, NJW 2017, S. 1060.
111 Gola/Lepperhoff, ZD 2016, S. 12.
112 OLG Celle Beschl. v. 4.10.2017 – 3 Ss (OWi) 163/17, BeckRS 2017, 131819, Rn. 23 m. w. N.; OLG Stuttgart NJW 2016, 2280 (2281).
113 Vgl. Fuchs, ZD 2015, S. 215-216.
114 VG Ansbach SVR 06/2015, 235 (237); VG Göttingen NJW 2017, 1336 (1337); vgl. OLG Stuttgart NJW 2016, 2280 (2281); Froizheim, NZV 2018, S. 115.

nenbezogene Daten einer Person verarbeitet, die nicht zur privaten Sphäre der Geschädigten gehört. Daran vermag auch der Umstand nichts zu ändern, dass ein privatgenutzter Gegenstand im Regelfall der privaten Sphäre zuzuordnen ist. Ferner werden auch Daten über Bewegungen im öffentlichen Raum, sofern der Gegenstand dort bewegt wird, oder aus der Sphäre der Besitzer*innen verarbeitet, sofern der Gegenstand sich dort befindet. Dies spricht ebenfalls gegen eine Zuordnung zum privaten Bereich.[115] So wird die Haushaltsaufnahme auch nicht bei Dash-Cam-Aufzeichnungen angenommen, die durch Kameras entstehen, die sich am KFZ befinden, um Beweise im Falle eines Unfalls festzuhalten. Auch hier wird argumentiert, dass diese Aufnahmen (anders als z. B. Helmkameras eines Sportlers) nicht dazu gedacht sind, das eigene Erleben oder die eigene Leistung zu dokumentieren. Das Erheben von Beweismitteln sei keine „persönliche" Tätigkeit.[116]

Für eine entsprechende Interpretation würde ebenfalls sprechen, wenn im Interesse des Datenschutzes der private Bereich eng auszulegen wäre, wovon die überwiegende Ansicht ausgeht.[117] Dies ergäbe sich aus dem Wortlaut der Norm, in der bewusst von „ausschließlich" gesprochen wird.[118] Daher dürften nur solche Datenverarbeitungen aus dem Anwendungsbereich der DS-GVO ausgenommen werden, bei denen dies wegen des beschränkten Verwendungszwecks unter Berücksichtigung der Interessen der Betroffenen und der Datenerhebenden geboten ist.[119] Dagegen könnte allerdings angeführt werden, dass die Beobachtung des eigenen, gestohlenen Gegenstandes dazu führen würde, dass damit sämtliche Verpflichtungen der DS-GVO einhergehen würden, d. h. abhängig von der Zählweise ca. 46 Verpflichtungen.[120] Dies sind etwa umfassende Dokumentations- und Informationspflichten. Kann von einer Privatperson in einer solchen Konstellation verlangt werden, sämtlichen Pflichten aus der DS-GVO nachzukommen?[121] Dies könnte nicht zuletzt abgelehnt werden, da bei einigen Pflichten der Eindruck entstehen könnte, dass diese sich in erster Linie an große Unternehmen richten und somit für Privatpersonen oftmals kaum zu schultern sind.[122]

115 Vgl. EuGH Urt. 11.12.2014 –C-212/13 Rn. 33.
116 OLG Celle ZD 2018, 86, (86).
117 Z. B. Sydow-Ennöckl 2022, Art. 2, Rn. 10 m. w. N.
118 Vgl. EuGH EuZW 2015, 234 (235) m. w. N.; OLG Celle Beschl. v. 4.10.2017 – 3 Ss (OWi) 163/17, BeckRS 2017, 131819, Rn. 23.
119 Sydow-Ennöckl 2022, Art. 2, Rn. 10.
120 Vgl. Veil, NVwZ 2018a, 9.
121 Kritisch zu den Pflichten von Privatpersonen etwa Veil, NVwZ 2018b, S. 692-693.
122 Veil, NVwZ 2018b, S. 693; vgl. Härting, CR 2013, S. 717.

Somit könnte es angebracht sein, die Ausnahmeregelung doch weiter zu interpretieren. Anhaltspunkte dafür könnten sich auch aus den Erwägungsgründen ergeben. Dort heißt es, dass auch die Nutzung sozialer Netze und Online-Tätigkeiten dem persönlichen oder familiären Bereich zuzuordnen sein können, solange sie nicht im beruflichen Kontext verwendet werden.[123] Ein beruflicher Kontext liegt zumindest für die Geschädigten nicht vor, solange es sich nicht um Gegenstände handelt, die im Kontext der Erwerbstätigkeit eingesetzt werden. Die von der Ortung Betroffenen wären auch nicht schutzlos gestellt, da es in so einem Fall immer noch möglich wäre, Ansprüche gegen die Anbieter des Ortungsservices geltend zu machen.[124]

Gegen eine weite Auslegung der Haushaltsausnahme kann wiederum angeführt werden, dass so der Zweck der DS-GVO, einen möglichst wirksamen und umfassenden Datenschutz zu erreichen,[125] umgangen wird. Auf der anderen Seite muss aber auch gewährleistet sein, dass es generell möglich ist, den Pflichten aus der DS-GVO nachzukommen.[126] Andernfalls wäre der Gesetzeszweck verfehlt und den Geschädigten verbliebe nur die Möglichkeit, von der Ortung abzusehen, um sich keinen rechtlichen Risiken auszusetzen, unabhängig davon, ob ein berechtigtes Interesse besteht. In so einem Fall muss das berechtigte Interesse aber in einem angemessenen Verhältnis zu den Datenschutzinteressen stehen,[127] etwa muss ein wirksamer Schutz des Eigentums gegen rechtswidrige Beeinträchtigungen gewährleistet sein.[128]

Allerdings muss aber auch beachtet werden, dass in der DS-GVO Ausnahmen von bestimmten Pflichten in einzelnen Kontexten vorgesehen sind und dass auch die Möglichkeit einer einschränkenden Auslegung der Vorschriften besteht. So könnte eine Einschränkung auch auf der Ebene der Verantwortlichkeit im Sinne des Art. 4 Nr. 7 DS-GVO stattfinden, um bestimmte Akteure von den Pflichten der DS-GVO auszunehmen. Gleichzeitig könnten gewisse Pflichten auch anders verteilt oder in bestimmten Situationen anders interpretiert werden.[129] So ist eine weite Auslegung der Haushaltsausnahme gar nicht zwingend erforderlich, um den Interessen der Geschädigten Rechnung zu zollen.

Vor diesem Hintergrund erscheint es nicht sinnvoll, die Haushaltsausnahme weit zu interpretieren und auch Vorgänge darunter zu subsumieren, bei denen es

123 Erwägungsgrund 18 Satz 2.
124 Vgl. Erwägungsgrund 18 Satz 3.
125 EuGH Urt. v. 13.5.2014 – C-131/12 – Rn. 33 f.
126 Vgl. Marosi 2016, S. 392.
127 Veil, NVwZ 2018b, S. 694.
128 Vgl. intensiv zum Verhältnis des Datenschutzinteresses im Verhältnis zu anderen Rechten: Veil, NVwZ 2018b, S. 693-696.
129 Fährmann/Vollmar/Görlitz in diesem Band, S. 177ff.

darum geht, andere Personen zu beobachten, insbesondere ohne deren Wissen und entgegen deren Willen. Dafür spricht ferner, dass mittlerweile auch durch natürliche Personen, die in privatem Kontext handeln, beträchtliche Risiken für den Datenschutz entstehen.[130] Auch diese haben mittlerweile Zugang zu technischen Möglichkeiten, mit denen sie beträchtlich in die Sphäre anderer Personen eingreifen können. Daher sollte eine Haushaltsausnahme nur dann vorliegen, wenn der private Bereich nicht verlassen wird.[131] Dies mag im Einzelfall schwierig zu beurteilen sein, da die Grenzen fließend sind. Im Falle der Beobachtung gestohlener Gegenstände ist die Situation aber nicht so. Auch wenn der Gegenstand der privaten Sphäre zuzuordnen ist, wird eine fremde Person, die dem Geschädigten zudem meist noch nicht einmal bekannt ist, beobachtet bzw. deren Bewegungsdaten gespeichert. So spiegelt die Beobachtung keinerlei persönlichen oder familiären Bezug wider.[132] Eine unbekannte Person, mit der im privaten Kontext keinerlei Interaktion stattfindet, kann üblicherweise nicht zur privaten Sphäre gehören. Außerdem befindet sich der Gegenstand nicht mehr in der Einflusssphäre der Geschädigten, sodass nicht mehr von der privaten Sphäre gesprochen werden kann.[133]

Daher ist die DS-GVO auf die Geschädigten anwendbar.

Hinsichtlich der Trackingservice-Anbieter*innen ist unproblematisch der Anwendungsspielraum der DS-GVO eröffnet, da die Daten aus der Perspektive der Anbieter*innen ausschließlich zu geschäftlichen Zwecken – nämlich zur Erfüllung vertraglicher Verpflichtungen – erhoben werden.

### *3.2.2 Interessenabwägung zwischen Geschädigten bzw. Trackingsystemanbieter sowie (unberechtigten) Besitzer*innen*

Die Datenerhebung müsste nach Art. 6 Abs. 1 Satz 1 f DS-GVO rechtmäßig sein. Dieser Art. ermöglicht die Datenverarbeitung im Anschluss an eine Abwägung der berührten Interessen, soweit die Interessen an der Verarbeitung die Interessen an deren Unterlassung überwiegen. Zunächst ist ein berechtigtes Interesse zu prüfen, zu dessen Wahrung die Verarbeitung erforderlich ist. Dieses Interesse ist weit zu verstehen[134] und umfasst jegliches rechtliches, wirtschaftli-

130 von Lewinski 2018, Rn. 22.

131 Siehe dazu auch EuGH ZD 2015, 212, 215.

132 Vgl. BGH Urteil v. 15.5.2018 – VI ZR 233/17; OLG Nürnberg, Beschl. v. 10.8.2017 – 13 U 851/17 –, Rn. 63 ff.

133 Mienert/Gipp, ZD 2017, S. 515; Lohse 2016.958; im Ergebnis auch EuGH EuZW 2015, 234 (235) m. w. N.

134 Vgl. Erwägungsgrund 47 S. 2, 6, 7; Erwägungsgrund 75; Schantz/Wolff 2017-Wolff Rn. 643; Gierschmann, MMR 2018, S. 9-10.

ches oder ideelles Interesse.[135] Bei der Bestimmung des berechtigten Interesses sind insbesondere die Grundrechte[136] sowie die GRCh[137] heranzuziehen.

Das berechtigte Interesse der Geschädigten folgt meist aus dem Eigentumsrecht aus Art 14 GG bzw. Art. 17 GRCh[138] sowie aus dem einfachen Recht, nämlich, den gestohlenen Gegenstand nach § 985 BGB wiederzuerlangen bzw. Ansprüche aus dem Eigentümer*in-Besitz*in-Verhältnis (§§ 987 BGB ff.) gegen die Besitzer*innen oder Schadensersatz nach § 823 Abs. 1 BGB gegen die Dieb*innen geltend zu machen. Ohne die Ortung des Gegenstandes wären diese Ansprüche vielfach mangels Hinweisen auf die Besitzer*innen nicht durchsetzbar, sofern es keine anderen Ermittlungsansätze gibt. Dadurch bleibt vom Eigentumsrecht im Regelfall nichts mehr übrig. Aber auch bei anderen Ermittlungsansätzen ist die Kenntnis des Standortes des Gegenstandes ein Umstand, der die Geltendmachung von Ansprüchen erheblich erleichtern kann. Dementsprechend wird regelmäßig kein milderes gleichgeeignetes Mittel ersichtlich sein, sodass das notwendige Kriterium der Erforderlichkeit[139] erfüllt ist. Auch kann nicht nur die Ortung der gestohlenen Gegenstände notwendig sein, sondern auch, etwaige Bewegungsdaten zu erheben und zu speichern. Diese ermöglichen Rückschlüsse auf die Person der Besitzer*innen, um zivilrechtliche Ansprüche gegen sie geltend zu machen. Gerade wenn eine Ortung aus technischen Gründen nicht mehr möglich sein sollte, sind die Geschädigten auf die bereits erfassten Bewegungsdaten angewiesen.

In Bezug auf die Besitzer*innen sind sämtliche entgegenstehenden Interessen beachtlich, die einen Bezug zur DS-GVO aufweisen. Vor allem sind Art. 8 GRCh sowie das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG relevant.[140]

Diese beiden gegenläufigen Interessen sind nun gegeneinander abzuwägen. Dabei kommt es auf die Art der Datenverarbeitung an und das Gewicht der damit einhergehenden Interessenbeeinträchtigung bzw. der Beeinträchtigungsrisiken bei den Besitzer*innen.[141] Neben den Rechtspositionen der Beteiligten sind zudem auch Interessen der Allgemeinheit zu berücksichtigen.[142] Damit ist die Funktionstüchtigkeit der Straf- und Zivilrechtspflege aus Art. 20 Abs. 3

135 Gierschmann, MMR 2018, S. 9 f. m. w. N.; Mäsch/Ziegenrücker, JuS 2018, S. 751.
136 Vgl. Prütting/Wegen/Weinreich 2016, § 12, Rn. 37 m. w. N.; Mäsch/Ziegenrücker, JuS 2018, S. 751.
137 Paal/Pauly-Frenzel 2018, Art. 6 Rn. 28.
138 Abdallah/Gercke, CR 2003, S. 300.
139 Gierschmann, MMR 2018, S. 10; Mäsch/Ziegenrücker, JuS 2018, S. 751.
140 Mäsch/Ziegenrücker, JuS 2018, S. 752.
141 Gierschmann, MMR 2018, S. 11.
142 Mäsch/Ziegenrücker, JuS 2018, S. 752.

GG[143] in der Abwägung als besonders geschütztes Rechtsgut zu beachten,[144] da durch die erhobenen Datensätze beide Verfahren gefördert werden können. Bei der Abwägung ist auch zu beachten, ob die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass eine Verarbeitung für berechtigte Zweck erfolgen kann.[145]

Dieb*innen und Hehler*innen können damit rechnen, dass Sicherheitsmaßnahmen zum Schutz des Eigentums bestehen. Wie bereits festgestellt, wiegen die bloßen Ortungseingriffe zudem nicht schwer, da im Regelfall nur beschränkte Rückschlüsse auf eine bestimmte Person möglich sind (siehe dazu ausführlich unter 2.). Auch die Speicherung der Daten erlaubt oftmals nur beschränkte Rückschlüsse auf eine Person, da meistens nicht erkennbar ist, wer den Gegenstand gerade im Besitz hat. Keinesfalls darf der Diebstahl dazu führen, dass nunmehr ein umfassendes Bewegungsprofil von Dieb*innen oder Hehler*innen über einen längeren Zeitraum erstellt wird. Daran besteht allerdings in der vorliegenden Konstellation seitens der Geschädigten kein Interesse, da diese lediglich das Diebesgut zurückerlangen bzw. Schadensersatzansprüche geltend machen wollen. Ein längeres Zuwarten und Beobachten steigert das Risiko, dass das Diebesgut nicht gefunden oder die Zuordnung zu einer bestimmten Person schwieriger wird, insbesondere falls irgendwann der Ortungs-Sender nicht mehr funktioniert. Insofern wird die Datenerhebung im Regelfall nicht lange andauern, was die Erstellung eines umfassenden Profils sehr unwahrscheinlich macht.

Solange das Interesse der Geschädigten also darauf gerichtet ist, so schnell wie möglich den gestohlenen Gegenstand zurückzuerlangen und nur zur Durchsetzung von Ansprüchen oder zum Auffinden des Gegenstandes dieser geortet oder dessen Bewegungsdaten gespeichert werden, überwiegen damit die Interessen der Geschädigten die Interessen der Dieb*innen.[146]

Zwar sind die Interessen von gutgläubigen Besitzer*innen höher zu werten als die der Dieb*innen bzw. Hehler*innen, was aber regelmäßig nicht dazu führen wird, dass auch die Interessen der Geschädigten überwogen werden. Einerseits erwerben sie kein Eigentum nach § 935 Abs. 1 BGB. Zudem muss auch beachtet werden, dass die Geschädigten sonst im Regelfall keine Möglichkeit haben, ihr Eigentum zurückzuerlangen. Dies spricht dafür, dass die Interessen

143 BVerfG NJW 1977, 1489 (1490); Jarass/Pieroth-Jarass 2022, Art. 20 Rn. 128 ff.; 137 ff. m. w. N.

144 BVerfG NJW 2002, 3619 (3214); BGH NJW 2013, 2530 (2536); vgl. BVerfG, NJW 1990, 563 (564); Landau NStZ 2007, S. 126.

145 Erwägungsgrund 47 Satz 3; vgl. Lachenmann, ZD 2017, S. 409.

146 Vgl. Abdallah/Gercke, CR 2003, S. 300.

an dem Eigentum auch in dieser Konstellation überwiegen müssen. Die Geschädigten können zudem nicht wissen, wann ein gestohlener Gegenstand von einer Person gutgläubig in Besitz genommen wurde. Wenn die Interessen einer gutgläubigen Besitzer*in grundsätzlich überwiegen würden, dann würden die Geschädigten bei jeder Datenerhebung das Risiko eingehen, dass diese rechtswidrig ist und damit entsprechende Konsequenzen für sie hat. Dies könnte dazu führen, dass auch in Fällen, in denen das Diebesgut tatsächlich noch im Besitz der Dieb*innen ist, auf eine Datenerhebung verzichtet wird.

Die Geschädigten sind also im Regelfall berechtigt, die Daten zu erheben und sogar von Bewegungsprofilen der Gegenstände nach dem Diebstahl zu speichern.[147]

Die Rechtmäßigkeit der Datenverarbeitung der Trackingservice-Anbieter*innen folgen grundsätzlich ebenfalls direkt aus Art. 6 Abs. 1 f. 2 Variante DS-GVO, unabhängig davon, ob sie als datenschutzrechtlich Verantwortliche oder Auftragsverarbeiter*innen tätig werden, was von der vertraglichen Ausgestaltung abhängt.[148]

### *3.3 Darf die Polizei die Trackingdaten verwenden?*

Nunmehr stellt sich die Frage, ob die Polizei die privat erhobenen Daten verarbeiten darf: d. h. insbesondere speichern oder auswerten. Diese Vorgänge können unabhängig voneinander rechtswidrig sein.[149] Die grundrechtliche Schutzwirkung von der informationellen Selbstbestimmung erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an die Kenntnisnahme von Daten anschließt.[150] Jede Verwendung und Verarbeitung personenbezogener Daten tangiert grundrechtliche Positionen der Betroffenen.[151]

Gegen eine Annahme und Verwendung könnte vorgebracht werden, dass so die Voraussetzungen der §§ 100h bzw. 163f StPO unterlaufen würden, vor allem der Richtervorbehalt aus § 163f Abs. 3 S. 1 StPO. Letztlich werden jedoch nur von Privatpersonen Daten an die Polizei herangetragen. Dazu hat die Polizei die Privatpersonen weder beauftragt noch ersucht.[152] Daher erfolgt

147 Vgl. Bär 2007, S. 200; AG Friedberg NStZ 2006, 517, (518); Jordan, Der Kriminalist 2005, S. 353.

148 Fährmann/Vollmar/Görlitz in diesem Band, S. 177ff.

149 Vgl. Kaiser, NStZ 2011, S. 386; Kölbel, NStZ 2008, S. 242.

150 BVerfG NJW 2000, 55 (57).

151 Singelnstein, NStZ 2012, S. 606.

152 Woraus ein Verwertungsverbot erwachsen könnte, wenn die Polizei unzulässig ihre Befugnisse erweitert Kölbel, NStZ 2008, S. 242 m. w. N.; vgl. BGH NJW 1998, 3506 (3507).

keine Umgehung der strafprozessualen Vorschriften, da Privatpersonen nicht an die StPO gebunden sind.[153]

Die Polizei müsste aber berechtigt sein, die Daten anzunehmen. Wie dargelegt, sind die Erkenntnisse aus den Positionsdaten begrenzt, da diese sich vornehmlich auf ein Objekt beziehen und nicht eindeutig ist, wer dieses Objekt im Besitz hatte (siehe ausführlich unter 2.). Insofern könnte auch die Entgegen- und Kenntnisnahme nur einen geringen Eingriff darstellen, der durch die Ermittlungsgeneralklausel des §§ 161 Abs. 1 S. 1, 163 Abs. 1 StPO gerechtfertigt ist. Wendet sich eine Privatperson mit einer rechtswidrig erlangten „Steuer-CD" an die Polizei, so ist nach der überwiegenden Ansicht sogar deren Ankauf mit staatlichen Mitteln durch die Ermittlungsgeneralklausel gerechtfertigt.[154] Insofern könnte erst recht die Kenntnisnahme von legalen Daten umfasst sein. Diese Problematik ist aber bisher nur wenig untersucht.

Mittlerweile können von Privatpersonen beträchtliche Mengen an Daten erhoben werden und zwar in einem Umfang, wie es früher noch nicht einmal von behördlicher Seite möglich war.[155] Dadurch werden die Gefahren für das Allgemeine Persönlichkeitsrecht immer größer. Daher ist es dringend notwendig, dass sowohl die Datenerhebung durch Privatpersonen als auch der staatliche Umgang mit solchen Daten eindeutig geregelt wird, da die Generalklausel für zahlreiche Konstellationen ungeeignet sein und der tatsächlichen Entwicklung und der zunehmenden Eingriffstiefe nicht gerecht wird.[156] Die aktuelle Rechtslage kann so interpretiert werden, dass sie eine Annahme über die Generalklausel der StPO zulässt. Da diese Rechtslage die aktuellen Entwicklungen nicht berücksichtigt, besteht hier dringender Bedarf, von Seiten der Gesetzgebung nachzusteuern.

Die Berechtigung zum Speichern und zur Nutzung der Daten könnte aus der Generalklausel für Datenverarbeitung aus § 483 Abs. 1 1. Und 2. Alt. StPO folgen. Die Vorschrift ist weit zu verstehen.[157] Zwar besteht danach nicht die Berechtigung, Beweismittel zu speichern.[158] Erlaubt ist aber das Speichern von Daten, die aufgrund der Auswertung von Beweismitteln erstellt wurden, d.

153 Kölbel, NStZ 2008, S. 242 m. w. N.

154 VerfGH Rheinland-Pfalz NJW 2014, 1434, 1437; Kölbel, NStZ 2008, S. 243; dies ist allerdings umstritten vgl. zur Übersicht: Stoffer 2014, S. 553-562 m. w. N.; Spernath, NStZ 2010, S. 311.

155 Vgl. Singelnstein, NStZ 2012, S. 599.

156 Vgl. hinsichtlich des Ankaufes von „Steuer-CDs" Stoffer 2014, S. 554 m. w. N.

157 Gercke/Julius/Temming/Zöller-Temming 2012, § 483, Rn. 4; Wolter-Weßlau 2013, § 483, Rn. 5.

158 OLG Karlsruhe NStZ 2015, S. 606 (608).

h. Fall- und Spurendokumentationsdateien.[159] Die Vorschrift setzt eine legale Erhebung voraus. Vorliegend werden die einzelnen GPS-Daten zusammengefasst, um erkennen zu können, wo sich der Gegenstand befunden hat. Diese Zusammenfassung ist bereits auf dem privaten Rechner erstellt worden, sodass die Polizei diese dann entsprechend speichern und auswerten kann. Es handelt sich bei den gespeicherten Bewegungsdateien also um eine Spurendokumentation. Demnach besteht die Berechtigung zum Speichern und zur fallbezogenen Verarbeitung, sofern die rechtmäßige Annahme der Daten angenommen wird.

Insgesamt darf die Polizei nach der heutigen Rechtslage Positionsdaten gestohlener Gegenstände, die von einer Privatperson gespeichert wurden, speichern und auswerten.

## 4. Zusammenfassung und Ausblick

Die Ausführungen belegen, dass der Einsatz von Ortungstechnologie zur Aufklärung von Diebstählen nur mit beträchtlichem Aufwand unter Heranziehung von zahlreichen Generalklauseln gerechtfertigt werden kann. Dadurch wird die Rechtsanwendung erheblich erschwert. Vor dem Hintergrund, dass die Ortungstechnik alles andere als neu ist, sollte die Legislative in absehbarer Zeit aktiv werden und Regelungen schaffen, die den Umgang mit dieser Technologie eindeutig regeln und begrenzen. Zwar ist der gezielte Einsatz von Ortungstechnologie zur Diebstahlsaufklärung, jedenfalls in größerem Umfang, ein neueres Phänomen, sodass aufgrund der geringfügigen Grundrechtseingriffe die Generalklauseln vorliegend noch vertretbar zum Einsatz kommen können. Das Bestimmtheitsgebot verlangt vom Gesetzgeber jedoch, dass technische Eingriffsinstrumente genau bezeichnet werden, wodurch sichergestellt wird, dass die Adressat*innen den Inhalt der jeweiligen Norm erkennen können. Zwar ist es nicht erforderlich, dass jede Einbeziehung kriminaltechnischer Neuerungen ausdrücklich normiert wird. Wegen der schnellen und für den Grundrechtsschutz riskanten technischen Entwicklung muss der Gesetzgeber aber die technischen Entwicklungen aufmerksam beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch ergänzende Rechtsetzung korrigierend eingreifen. Es liegt in der Verantwortung des Gesetzgebers auf neue Situationen auch mit entsprechenden Ermächtigungsgrundlagen zu reagieren.[160] Der Rechtfertigungsaufwand macht deutlich, dass der Einsatz von Ortungstechnologie zur Diebstahlsaufklärung von der

159 Gercke/Julius/Temming/Zöller-Temming 2012, § 483, Rn. 2; Wolter-Weßlau 2013, § 483, Rn. 6.

160 BVerfG NJW 2005, 1338, 1340.

Legislative zukünftig klarer normiert werden sollte. Insbesondere bestehen zahlreiche Unklarheiten. Wie lange soll die Berechtigung zur Speicherung bestehen? Kann die Polizei auch gegen den Willen der Geschädigten auf diese Daten zugreifen? Wegen der mit einem System der geheimen Überwachung verbundenen Missbrauchsgefahr müssen solche Maßnahmen auf bestimmt gefassten Rechtsvorschriften beruhen, insbesondere weil sich die Technik ständig und rasant weiterentwickelt und damit immer neue Eingriffsmöglichkeiten geschaffen werden.[161]

Die fehlenden eindeutigen Ermächtigungsgrundlagen führen überdies dazu, dass die Polizei in der vorliegenden Konstellation weniger Kompetenzen hat als Privatpersonen. Da die Strafverfolgung die Aufgabe der Polizei ist, stellt sich die Frage, ob dieser Zustand so beibehalten werden sollte. Diese Fragen werden sich in Zukunft bei immer mehr Gegenständen stellen, an die ein Ortungssender angebracht werden können oder in denen ein solcher bereits vorhanden ist.

## Literaturverzeichnis

Abdallah, Tarek/Gercke, Björn (2003) Verwertbarkeit privat veranlasster GPS-Peilung von gestohlenem Gut. Ist die privat veranlasste GPS-Peilung eines Fahrzeugs strafprozessual zulässig? in: CR, 18. Jg., Nr. 8, S. 298-300.

Albrecht, Jan P./Jotzo, Florian (2017) Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse.

Aden, Hartmut & Fährmann, Jan (2019) Wie lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen., in: Vorgänge Nr. 227, S. 95–106.

Aden, Hartmut & Fährmann, Jan (2021) Argumente für einen besseren Musterentwurf für einheitliche Polizeigesetze: Kritische Analyse von Entwicklungen im Polizeirecht aus rechtsstaatlicher und bürgerrechtlicher Perspektive, S. 580–615 in M. H. W. Möllers & R. C. van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit 2020/2021. Frankfurt am Main: Verlag für Polizeiwissenschaft.

Arzt, Clemens (2006) Automasierte Kfz-Kennzeichenerkennung. In: Roggan, F./Aden, H. (Hg.): Handbuch zum Recht der Inneren Sicherheit. 2. Aufl. Berlin: BWV Berliner Wissenschafts-Verl., S. 229–244.

Baller, Oesten/Eiffler, Sven/Tschisch, Andreas (2004) Allgemeines Sicherheits- und Ordnungsgesetz Berlin - ASOG Bln - Zwangsanwendung nach Berliner Landesrecht - UZwG Bln. Stuttgart: Boorberg.

Bär, Wolfgang (2007) Handbuch zur EDV-Beweissicherung. Stuttgart u.a.: Boorberg.

Börner, Fritjof (2015) Datenschutz im Auto der Zukunft, in: K&R Beilage, 18 Jg., Nr. 2, S. 2–6.

Bosch, Nikolaus (2006) Verwertung von Telekommunikationsverbindungsdaten, in: JA, 38 Jg., Nr. 10, S. 747–749.

161 2012 – 1 BvR 22/12 -, Rn. 25.

Cornelius, Kai (2013) Schneidiges Datenschutzrecht: Zur Strafbarkeit einer GPS-Überwachung, in: NJW, 66 Jg., Nr. 46, S. 3340–3343.

Damm, Matthias (2017) Der Zugang zu staatlichen Geodaten als Element der Daseinsvorsorge. Berlin: Duncker & Humblot.

Dreier, Thomas/Schulze, Gernot (2022) Urheberrechtsgesetz. Verwertungsgesellschaftenrecht, Kunsturhebergesetz: Kommentar. 7. Aufl. München: C.H. Beck.

Eckhardt, Jens (2017) DS-GVO: Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer, in: CCZ, 10. Jg., Nr. 03, S. 111–117.

Eckhardt, Sebastian (2009) Private Ermittlungsbeiträge im Rahmen der staatlichen Strafverfolgung, Zugl.: Freiburg im Breisgau, Univ., Diss., 2009. Frankfurt am Main, Wien u.a.: Lang.

Ehmann, Eugen/Selmayr, Martin (2018) Datenschutz-Grundverordnung. 2. Aufl. München: C.H.Beck.

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

Faßnacht, Ute (2011) Rechtsfragen bei der Verwendung von Ortungstechnologien und einsatzunterstützender Systeme durch Feuerwehr und THW. Rechtlicher Rahmen und Haftungsfragen. Münster.

Frenz, Walter (2013) Das Grundrecht auf informationelle Selbstbestimmung – Stand nach dem Antiterrordatei-Urteil des BVerfG, in: JA, 45. Jg., 2013, S. 840–845.

Fock, Merle & Möhle, Jan-Peter (2021) Viel Fahndung, wenig Strategie? – Verfassungsrechtliche Beurteilung der strategischen Fahndung in § NRWPOLG § 12a PolG NRW. In: GSZ, 04 Jg., Nr. 04, S. 170–175.

Froizheim, Oliver (2018) Dash Cams, das allgemeine Persönlichkeitsrecht und Beweisverwertung, in: NZV, 31 Jg., Nr. 03, S. 109–115.

Fuchs, Daniel (2015) Verwendung privater Kameras im öffentlichen Raum - Datenschutz bei Dash-Cams, Helm-, Wildkameras & Co., in: ZD, 05 Jg., Nr. 05, S. 212–217.

Gasch, Patrick (2012) Grenzen der Verwertbarkeit von Daten der elektronischen Mauterfassung zu präventiven und repressiven Zwecken. Berlin: Duncker & Humblot.

Gercke, Björn (2006) Einsatz des „Global-Positioning-System“ (GPS). In: Roggan, F./Aden, H. (Hg.): Handbuch zum Recht der Inneren Sicherheit. 2. Aufl. Berlin: BWV Berliner Wissenschafts-Verl., S. 403–409.

Gercke, Björn/Julius, Karl/Temming, Dieter/Zöller, Mark (2012) Strafprozessordnung. 5. Aufl. Heidelberg u.a.: Müller.

Gierschmann Sibylle (2018) Gestaltungsmöglichkeiten bei Verwendung von personenbezogenen Daten in der Werbung. Auslegung des Art. EWG_DSGVO Artikel 6 Abs. EWG_DSGVO Artikel 6 Absatz 1 lit. F DS-GVO und Lösungsvorschläge, in: MMR, 21 Jg., Nr. 01, S. 7–12.

Gola, Peter/Heckmann, Dirk (2022) Datenschutz-Grundverordnung VO (EU) 2016/679. 3. Aufl. München.

Gola, Peter/Lepperhoff Niels (2016) Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbietung. Aufnahme und Umfang der Ausnahmeregelung in der DS-GVO, in: ZD, 6 Jg., Nr. 01, S. 9–12.

Graf, Jürgen (Stand 2016) Beck'scher Online-Kommentar StPO mit RiStBV und MiStra. 24. Aufl. München.

Gubitz, Michael (2016) Praxiskommentar, in: NStZ, 36 Jg., Nr. 02, S. 128.

Gusy, Christoph (1998) Anmerkung, in: StV, S. 526–527.

Härting, Niko (2013) Datenschutzreform in Europa: Einigung im EU-Parlament. Kritische Anmerkungen, in: CR, 29 Jg., Nr. 11, S. 715–721.

Hefendehl, Roland (2022) Münchener Kommentar zum Strafgesetzbuch. Band 5. 4. Aufl. München: Beck.

Hornung, Gerrit/Schindler, Stephan (2017) Das biometrische Auge der Polizei. Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, in: ZD, 07 Jg., Nr. 05, S. 203–209.

Hornung, Gerrit (2005) Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Zugl.: Kassel, Univ., Diss., 2005. Baden-Baden: Nomos.

Jarass, Hans/Pieroth, Bodo (2022) Grundgesetz für die Bundesrepublik Deutschland. Kommentar. 17. Aufl. München: C.H. Beck.

Jordan, Stefan (2005) Polizeiliche Nutzbarkeit der Mautdaten zur Strafverfolgung, in: Der Kriminalist, S. 351–354.

Kaiser, Ingo (2011) Zulässigkeit des Ankaufs deliktisch erlangter Steuerdaten, in: NStZ, 31 Jg., Nr. 7, S. 383–390.

Keller, Christoph/Kay, Wolfgang (2016) Bußgeldverfahren. Eingriffsbefugnisse der Verwaltungsbehörden und der Polizei im Ermittlungsverfahren. Stuttgard: Kohlhammer Verlag.

Kilian, Wolfgang (2018) Computerrechts-Handbuch. Computertechnologie in der Rechts- und Wirtschaftspraxis. 34. Aufl. München: Beck.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans/Albrecht, Hans/Altenhain, Karsten (2017) Strafgesetzbuch. 5. Aufl. Baden-Baden: Nomos.

Knape, Michael/Schönrock, Sabrina (2016) Allgemeines Polizei- und Ordnungsrecht für Berlin. Kommentar für Ausbildung und Praxis. 11. Aufl. Hilden: Deutsche Polizeiliteratur.

Kölbel, Ralf (2008) Zur Verwertbarkeit privat-deliktisch beschaffter Bankdaten. – Ein Kommentar zur causa „Kieber" –, in: NStZ, 28 Jg., Nr. 05, S. 241–244.

Kudlich, Hans (2014) Münchener Kommentar zur Strafprozessordnung Gesamtwerk. Band 1. München: Beck C H.

Kudlich, Hans (2016) Münchener Kommentar zur Strafprozessordnung Gesamtwerk. Band 2. München: Beck C H.

Kühling, Jürgen/Buchner, Benedikt (2020) Datenschutz-Grundverordnung. BDSG Kommentar. 3. Aufl. München.

Kühne, Hans (2001) Anmerkung, in: JZ, S. 1148.

Lachenmann, Matthias (2017) Neue Anforderungen an die Videoüberwachung. Kritische Betrachtungen der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu, in: ZD, 07 Jg., Nr. 9, S. 407–411.

Ladeur, Karl-Heinz (2009) Das Recht auf informationelle Selbstbestimmung. Eine juristische Fehlkonstruktion?, in: DÖV, 2009, Nr. 2, S. 45–55.

Landau, Herbert (2007) Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege, in: NStZ, 27 Jg., Nr. 3, S. 121–129.

Lauber-Rönsberg, Anna/Hartlaub, Anneliese (2017) Personenbildnisse im Spannungsfeld zwischen Äußerungs- und Datenschutzrecht, in: NJW, 70 Jg., Nr. 15, S. 1057–1062.

Lenk, Heiko (2017) Vertrauen ist gut, legendierte Kontrolle ist besser. -zugleich Anmerkung zum Urteil des BGH v. 26.04. 2017 – 2 StR 247/16, StV 2017, 643, in: StV, S. 692–699.

Lesch, Heiko (2000) Zu den Rechtsgrundlagen des V-Mann-Einsatzes und der Observation im Strafverfahren, in: JA, S. 725–728.

Eßer, M./Kramer, P./Lewinski, K. von (2018.) DSGVO BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. 6. Aufl. Köln.

Lohse, Kai (2016) Alles auf Aufnahme? Dashcam im Fokus, in: VersR, S. 953–963.

Marosi, Johannes (2016) Mehrstufige Anbieterverhältnisseim Datenschutz: letzte Station Unionsrecht? . Zugliech Kommentar zu BVerwG, Beschl. v. 25.3.2016 - 1 X 28.14, K&R Nr. 6, S. 437 ff., in: K&R, Nr. 6, S. 389–392.

Mäsch, Gerald/Ziegenrücker, Daniel (2018) Kameras vor Gericht – Zur Verwertbarkeit von Dashcam-Aufnahmen im Zivilprozess in Zeiten der Datenschutz-Grundverordnung, in: JuS, 58 Jg., Nr. 8, S. 750–754.

Mienert, Heval/Gipp, Bela (2017) Dashcam, Blockchain und der Beweis im Prozess. Kriterien für einen Privacy by Design-Lösungsansatz bei Dashcams, in: ZD, 7 Jg., Nr. 11, S. 514–519.

Müller, Wolfgang/Römer, Sebastian (2012) Legendierte Kontrollen. Die gezielte Suche nach dem Zufallsfund, in: NStZ, 32 Jg., Nr. 10, S. 543–547.

Neumann, Conrad (2014) Zugang zu Geodaten. Neue Impulse für das Informationsverwaltungsrecht durch die INSPIRE-Richtlinie. Berlin: Duncker & Humblot.

Nickel, Friedhelm/Gwehenberger, Johann (1994) Aktive Diebstahlsicherung für Personenkraftwagen, in: VW, S. 134–141.

Paal, Boris/Pauly, Daniel (2018) Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. 2. Aufl. München: Beck.

Pieroth, Bodo/Schlink, Bernhard/Kniesel, Michael/Kingreen, Thorsten/Poscher, Ralf (2016) Polizei- und Ordnungsrecht. Mit Versammlungsrecht. 9. Aufl. München: Beck, C H.

Roßnagel, Alexander/Kroschwald, Steffen (2014) Was wird aus der Datenschutzgrundverordnung? Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, in: ZD, 04 Jg., Nr. 10, S. 495–500.

Rückert, Christian (2017) Zwischen Online-Streife und Online (Raster)Fahndung. Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, in: ZStW, 129 Jg., Nr. 2, S. 302–333.

Schantz, Peter/Wolff, Heinrich A. (2017) Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis.

Schmidt, Bernd/Freund, Bernhard (2017) Perspektiven der Auftragsverarbeitung. Wegfall der Privilegierung mit der DS-GVO?, in: ZD, 7 Jg., Nr. 1, S. 14–18.

Schönke, A./Schröder, H./Eser, A. (2019) Strafgesetzbuch. Kommentar. 30. Aufl. München: Beck.

Simitis, Spiros (2014) Bundesdatenschutzgesetz. 8. Aufl. Baden-Baden: Nomos.

Singelnstein, Tobias (2012) Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen. Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in: NStZ, 32 Jg., Nr. 11, S. 593–606.

Singelnstein, Tobias (2014) Bildaufnahmen, Orten, Abhören – Entwicklungen und Streitfragen beim Einsatz technischer Mittel zur Strafverfolgung, in: NStZ, 34 Jg., Nr. 6, S. 305–311.

Soiné, Michael (2014) Kriminalistische List im Ermittlungsverfahren, in: NStZ, 34 Jg., Nr. 06, S. 596–602.

Spernath, Valentin (2010) Strafbarkeit und zivilrechtliche Nichtigkeit des Ankaufs von Bankdaten, in: NStZ, 30 Jg., Nr. 06, S. 307–312.

Steinmetz, Jan (2001) Zur Kumulierung strafprozessualer Ermittlungsmaßnahmen, in: NStZ, 21 Jg., Nr. 07, S. 344–349.

Stoffer, Hannah (2014) Wie viel Privatisierung "verträgt" das strafprozessuale Ermittlungsverfahren? Tübingen: Mohr-Siebeck.

Sydow, G. (2022) Europäische Datenschutzgrundverordnung. 3. Aufl. München.

Tomerius, Carolyn (2020) „Drohnen“ zur Gefahrenabwehr – Darf die Berliner Polizei nach jetziger Rechtslage Drohnen präventiv-polizeilich nutzen? LKV 30: 481–489.

Vassilaki, Irini (2005) Anmerkung, in: Computer und Recht, Nr. 33, S. 569–574.

Veil, Winfried (2018a) Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, in: ZD, 09 Jg., Nr. 01, S. 9–16.

Veil, Winfried (2018b) Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, in: NVwZ, 37 Jg., Nr. 10, S. 686–986.

Wandtke, A.-A./Bullinger, W (2022) Praxiskommentar zum Urheberrecht. 6. Aufl. München: C.H.Beck.

Weichert, Thilo (2009) Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, in: Datenschutz und Datensicherheit, 33 Jg., Nr. 6, S. 347–352.

Weichert, Thilo (2014) Datenschutz im Auto – Teil 1, in: SVR, 14 Jg., Nr. 01, S. 201–207.

Wolter, Jürgen (2013) Systematischer Kommentar zur Strafprozessordnung. Mit GVG und EMRK, Band VIII. 4. Aufl. Köln.

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

# Rechtliche und technische Rahmenbedingungen für die datenschutzkonforme Verarbeitung von Ortungsdaten durch Private und die Polizei unter besonderer Berücksichtigung des Datenschutzrechts

## 1. Einleitung

Im interdisziplinären Forschungsprojekt *FindMyBike* wurde eine datenschutzkonforme Software (*FindMyBike-System*)[4] zur Übertragung von Positionsdaten gestohlener, mobiler und mit ortbaren Sendern ausgestatten Gegenstände an die Polizei konzipiert. Die Software wurde auf Basis des Wissens über Fahrraddiebstähle entwickelt (wobei auch andere Positionsdaten gestohlener Gegenstände übertragen werden können). Sobald die Besitzer*innen den Diebstahl bemerken, können sie bei der jeweiligen Trackingservice-Anbieter*in eine Uniform Ressource Locator (URL) anfordern, die durch das *FindMyBike-System* generiert und von der Trackingservice-Anbieter*in mit dem Fahrrad verknüpft wird, sodass dessen Live-Position auf einer Karte angezeigt wird. Über einen längeren Zeitraum erhobene Positionsdaten (Bewegungsdaten) können auch über die Software an die Polizei übertragen werden, müssen aber gesondert angefordert werden. Die URL mit der Live-Position können die Bestohlenen bei der Anzeigeerstellung in der Internet-Wache in das zugehörige Online-Formular kopieren. Die Polizei kann mit Hilfe dieser URL die *FindMyBike-Anwendung* aufrufen und hat damit Zugriff auf die Live-Positionsdaten des Fahrrades. Diese Positionsdaten können bei der Aufklärung von Diebstählen sehr hilfreich bzw. die wesentliche Voraussetzung zur Ermittlung der Dieb*innen sein und auch in einem zivilgerichtlichen Verfahren – z. B. auf Schadensersatz gegen die Dieb*innen – als wichtiges Beweismittel dienen.[5] Immer mehr Gegenstände

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 Die Implementierung des FindMyBike-Systems ist in Vollmar/Görlitz/Kober in diesem Band, S. 227ff, dargelegt.

5 Fn. einfügen: Fährmann/Vollmar/Görlitz in diesem Band: S. 177ff.

sind ortbar, sodass zukünftig damit zu rechnen ist, dass private Anbieter zunehmend in der Lage sind, diese bei einem Diebstahl zu orten.

Mit der Übertragung von Positionsdaten gestohlener Gegenstände an die Polizei gehen aber auch verschiedene datenschutzrechtliche Risiken einher. Da sensible Daten von Personen betroffen sein können, die keinen Anlass zur Datenerhebung gegeben haben, sind erhöhte Anforderungen zum Schutz der Daten an die Ausgestaltung einer solchen Software zu stellen. Zwar sind sowohl Dieb*innen als auch bösgläubige Besitzer*innen wenig schutzwürdig, sodass ihre Interessen gering zu gewichten sind. Aber es ist möglich, dass (ggf. tage- oder wochenlang) Positionsdaten von gutgläubigen Besitzer*innen erhoben und ausgewertet werden, weil Fahrräder sehr schnell weitergegeben werden können. Positionsdaten – insbesondere, wenn sie über einen längeren Zeitraum erhoben werden – können ein Bewegungsbild der Person wiedergeben, die den Gegenstand bei sich führt. Daher kann es sich um sensible Daten handeln, die weitreichende Einblicke in die Privatsphäre der Betroffenen ermöglichen, gerade wenn sie mit anderen Daten kombiniert werden, was im strafrechtlichen Ermittlungsverfahren üblich ist. Grundsätzlich lassen Trackingdaten damit weitreichende Rückschlüsse auf eine Person und ihre Lebensumstände zu, etwa bezüglich des Wohnorts, besuchter Geschäfte oder Bekannter. Die Bewegungsdaten von Fahrrädern können allerdings nicht immer einer konkreten Person oder Örtlichkeit zugeordnet werden, gerade weil das Fahrrad leicht weitergegeben werden kann, was für eine geringere Schutzwürdigkeit spricht. Die Bewegungsdaten beziehen sich außerdem zumeist auf Vorgänge, die in der Öffentlichkeit ablaufen, wodurch sie auch der weniger eingriffsintensiven Sozialsphäre zugeordnet werden können. Auch ist im Regelfall ein eingeschränkter Lebensbereich betroffen, da Fahrräder meist nur zum Fortkommen oder zu sportlichen Aktivitäten verwendet werden, wobei der Bewegungsradius nicht unerheblich sein kann, zumal Fahrräder im Rahmen von Mobilitätskonzepten immer mehr an Bedeutung gewinnen. Entscheidend für die gesteigerten datenschutzrechtlichen Anforderungen ist aber der Umstand, dass die Positionsdaten für ein strafrechtliches Verfahren relevant sein können, in dem sie in eingriffsintensiver Weise verwendet werden und stigmatisierende Wirkungen bis hin zu einer (ggf. ungerechtfertigten) Verurteilung entfalten können.[6] Die Beteiligung mehrerer Akteure führt außerdem zu speziellen Risiken für das Recht auf informationelle Selbstbestimmung. Haben mehrere Personen Zugriff auf die Daten, so steigt auch das Risiko individuellen Fehlverhaltens.

Im Rahmen des Beitrages wird auf Basis dieser Risikobewertung erläutert, welche datenschutzrechtlichen Anforderungen und Pflichten bei der Konzepti-

6 Vgl. Borell/Schindler, DuD 2019, S. 772; zur Bestimmung der Sensibilität der Positionsdaten ausführlich Fährmann in diesem Band, S. 141 ff.

on der Software zu berücksichtigen sind und wie diese technisch umgesetzt wurden bzw., welche Umsetzungsmöglichkeiten es gibt. Die Konzeption der Software wurde insbesondere von den Datenschutzgrundsätzen der Datensparsamkeit sowie Privacy by Design und Default getragen, um einen wirksamen Datenschutz bereits in der Software und ihren Funktionen anzulegen. Zudem wird in diesem Beitrag auf die rechtliche Stellung und die daraus resultierenden gesetzlichen Verpflichtungen der an der Datenverarbeitung beteiligten Akteure eingegangen, die bei einer Umsetzung eines solchen Systems in der Praxis zugrunde gelegt werden müssten.

Die Software ist für die Berliner Polizei entwickelt worden. Auf Grund der hohen Datenschutzanforderungen an polizeiliche IT-Systeme konnte die Software im Zeitrahmen eines Forschungsprojektes nicht in das vorhandene IT-System integriert werden, sondern wurde als Softwareschnittstelle zur Berliner Polizei implementiert. Daraus ergibt sich der Vorteil, dass die Software auch in anderen Bundesländern ohne größeren Aufwand an die dort im Einsatz befindlichen IT-Systemen angebunden und in die polizeiliche Arbeit integriert werden kann. Wenn die Auswertung von Positionsdaten regelmäßig in die Ermittlungsarbeit einbezogen wird, dann sollte eine integrierte Implementierung in den polizeilichen Workflow und die IT-Systeme erfolgen.

## 2. Beteiligte Akteure an der Datenverarbeitung

An dem Prozess der Erhebung und Weiterleitung der Positionsdaten der gestohlenen Gegenstände sind folgende Personen(-gruppen) mit ihren jeweils spezifischen Interessen und rechtlichen Positionen beteiligt:

- Berechtigte zur Ortung des Diebesgutes (kurz: Tracking-Berechtigte): Berechtigt sind Eigentümer*innen der Gegenstände (hier und im Folgenden des Fahrrades). Zusätzlich kann auch aus anderen Rechtposition eine Befugnis zur Ortung folgen, etwa aus einer Anwartschaft an dem Fahrrad oder einem Fahrrad-Leasingvertrag.
- Trackingservice-Anbieter*in: Dies könnte z. B. eine Firma sein, die gegen Gebühr Tracking-Daten für die Tracking-Berechtigten verarbeitet und dafür passende Applikationen bereitstellt. Anknüpfungspunkt der Datenverarbeitung muss dabei nicht die Diebstahlsaufklärung sein, sondern kann auch – nach Entscheidung der Tracking-Berechtigten – die Auswertung gefahrener Strecken etc. sein.
- Betreiber*in des *FindMyBike-System* (kurz: System-Betreiber*in): Dies könnte ebenfalls eine Firma oder eine sonstiger Betreiber*in (z. B. ein Verein) sein. Die Aufgabe besteht speziell in der Verarbeitung und Übertragung

der Trackingdaten an die Polizei im Falle eines Diebstahls. Dieser Service muss sich nicht auf ortbare Fahrräder beschränken, sondern kann für zahlreiche Gegenstände (Autos, Mobiltelefone etc.) zur Verfügung gestellt werden. Der Trackingservice-Anbieter sowie der Betreiber eines Systems zur Übertragung von Positionsdaten an die Polizei könnten auch übereinstimmen,[7] von einem solchen Fall wird vorliegend aber nicht ausgegangen.
- Polizei
- Dieb*innen bzw. Hehler*innen.

## 3. Datenschutzrechtliche Anforderungen an die Erhebung von Trackingdaten und ihre Übermittlung an die Polizei

Die datenschutzrechtlichen Vorgaben folgen für die beteiligten Akteure aus unterschiedlichen Gesetzen. Für die privaten Trackingservice-Anbieter*innen, die Tracking-Berechtigten sowie für die Betreiber*in des FindMyBike-Systems folgen die Datenschutzgrundsätze aus Art. 5 DS-GVO, dessen Vorgaben in verschiedenen Normen konkretisiert werden. Art. 5 DS-GVO enthält die allgemeinen datenschutzrechtlichen Grundprinzipien, die zugleich Konkretisierungen der grundrechtlichen Vorgaben aus Art. 8 Abs. 2 GRCh und Art. 8 EMRK sind. Für die Polizei ergeben sich datenschutzrechtliche Grundsätze im Rahmen der strafverfolgenden Tätigkeit aus § 47 BDSG, wobei diese im Lichte der europarechtlichen Vorgaben aus der Richtlinien (EU) 2016/680 (JI-Richtlinie) auszulegen sind.[8] Auch diese Grundsätze werden teilweise durch speziellere Regelungen konkretisiert.[9] Die Grundsätze aus DS-GVO und BDSG/JI-Richtlinie weisen zahlreiche Parallelen auf,[10] auch wenn es Unterschiede im Detail gibt.[11]

Im Folgenden wird die Umsetzung der Datenschutzgrundsätze im *FindMyBike-System* und im gesamten Datenverarbeitungsvorgang von der Erhebung bis zur Übertragung an die Polizei erörtert und analysiert. Dabei konnten nicht alle möglichen technischen Funktionen im *FindMyBike-System* umgesetzt werden, da einige Spezifikationen davon abhängen, ob und inwieweit das System mit dem jeweiligen polizeilichen System verknüpft wird. Sofern eine Ver-

7 Wie etwa die Firma Ubinam; https://www.ubinam.de/ (letzter Aufruf: 20.07.2023).

8 Zur Abgrenzung von DS-GVO und BDSG Johannes/Weinhold 2018, S: 52; Schantz/Wolff-Wolff 2017, S. 75 f.; Kühling/Buchner-Schwichtenberg 2020, § 45 Rn. 3 f. m. w. N.

9 Johannes/Weinhold 2018, S. 63 f.

10 Paal/Pauly-Frenzel 2021, BDSG § 47, Rn. 3; Johannes/Weinhold 2018, S. 6; vgl. Johannes ZD-Aktuell 2017, 05852; Kühling/Buchner-Schwichtenberg 2020, § 47 Rn. 2.

11 Vgl. z. B. Johannes, ZD-Aktuell 2019, 06875; Aden/Fährmann, TATuP 2020, S. 26.

knüpfung erforderlich ist, werden diesbezüglich Vorschläge formuliert. Auch bzgl. der Erhebung der Positionsdaten durch Trackingservice-Anbieter*innen werden Vorschläge erarbeitet, um ein hohes Datenschutzniveau sicherzustellen. Hinsichtlich des *FindMyBike-Systems*, welches losgelöst von den polizeilichen Datenverarbeitungssystemen funktioniert, sind die Funktionen zur Umsetzung der Datenschutzgrundsätze alle in der im Forschungsprojekt konzipierten Software implementiert.

Im Folgenden werden die Datenschutzgrundsätze zunächst beschrieben und danach erläutert, wie diese in dem *FindMyBike-System* umgesetzt wurden, bzw. wie sie bei der Trackingservice-Anbieter*in und bei einer Verknüpfung mit dem polizeilichen IT-System umgesetzt werden könnten.

### *3.1 Privacy bei Design and Default*

Zunächst ist auf die Grundsätze „Privacy by Design" und „Default" einzugehen. „Privacy by Design" bedeutet nach Art. 25 Abs. 1 DS-GVO bzw. 71 BDSG,[12] dass technische Anwendungen so ausgestaltet werden müssen, dass die Datenschutzgrundsätze effektiv umgesetzt werden.[13] Dazu müssen nicht nur zum Zeitpunkt der eigentlichen Verarbeitung, sondern bereits bei der Einrichtung der Datenverarbeitungssysteme geeignete technische und organisatorische Maßnahmen getroffen werden, um eine datenschutzrechtskonforme Datenverarbeitung zu unterstützen oder zu ermöglichen. Damit soll erreicht werden, dass die Einhaltung datenschutzrechtlicher Grundsätze möglichst nicht von Entscheidungen der Nutzer*innen abhängt, sondern das IT-System bereits im Design nur eine rechtskonforme Nutzung zulässt.[14] Privacy by Default bedeutet, dass Datenverarbeitungsprozesse so voreinzustellen sind, dass ein möglichst optimaler Datenschutz gewährleistet wird (z. B. im Sinne der Datenminimierung so wenig Daten wie möglich erhoben werden), die Nutzer*innen sich also nicht erst aktiv für datenschutzfreundliche Einstellungen entscheiden müssen, Art. 25 Abs. 2 DS-GVO.[15]

Im *FindMyBike-System* wird durch technische Voreinstellungen und Funktionen sichergestellt, dass die Datenschutzgrundsätze soweit wie möglich automatisch umgesetzt werden, indem Daten nur über einen gewissen Zeitraum an die Polizei übertragen, Positionsdaten im System nur übergangsweise und nicht

12 BT-Drs. 18/11325, S. 118.

13 Baumgartner/Gausling, ZD 2017, S. 310; Auernhammer-Kramer/Meints 2020, Art. 24 Rn. 1.

14 Anwendungsbeispiele bei Fährmann, MMR 2021, S. 778 ff.; Bosch/Fährmann/Aden, ZKKW 2021, S. 206 ff.

15 Schenk/Mueller-Stöfen, GWR 2017, S. 177; Auernhammer-Brüggemann 2020, Art. 25 Rn. 23; Gola/Heckmann-Nolte/Werkmeister 2022, Art. 25 Rn. 27.

dauerhaft gespeichert, Bewegungsdaten nur auf Anforderungen an die Polizei übertragen und Daten im System pseudonomisiert und verschlüsselt werden. Auf die genaue Umsetzung wird bei dem jeweiligen Datenschutzgrundsatz eingegangen.

### *3.2 Zweckbindung*

Der Zweckbindungsgrundsatz, der bereits in den 1980er Jahren durch das Bundesverfassungsgericht etabliert wurde,[16] besagt, dass personenbezogene Daten nur für eindeutig festgelegte, rechtmäßige Zwecke erhoben und weiterverarbeitet werden dürfen (Art. 5 Abs. 1 b DS-GVO). Bei offener Datenerhebung kennen die Betroffenen in der Regel den Erhebungszweck. So ist z. B. beim Einbau eines GPS-Senders in ein Fahrrad oder einen anderen mobilen Gegenstand bekannt, dass der Sender die Ortung des Gegenstands ermöglicht. Der Zweckbindungsgrundsatz schützt das Vertrauen der Betroffenen, dass bei der Verarbeitung keine anderen, ihnen unbekannte Nutzungszwecke hinzukommen.

#### *3.2.1 Datenübertragung durch das FindMyBike-System an die Polizei*

Das *FindMyBike-System* stellt eine Software-Schnittstelle zur Polizei dar, damit die Positionsdaten gestohlener Fahrräder an die Polizei übertragen werden können. Da durch die Betätigung der Pedale die aufladbaren Batterien von GPS-Sendern immer wieder aufgeladen werden können, bestünde die Möglichkeit, dass für längere Zeit weiterhin Positionsdaten an die Polizei übertragen werden. Daher muss im *FindMyBike-System* sichergestellt werden, dass die Daten nur solange an die Polizei übertragen werden, wie sie für die Strafverfolgung bzw. straftatenbezogene Gefahrenabwehr, d. h. die Wiedererlangung des gestohlenen Fahrrades, benötigt werden. Wenn z. B. das Fahrrad wiedergefunden und an die rechtmäßigen Eigentümer*innen oder andere Berechtigten zurückgegeben wurde, muss die Datenübertragung an die Polizei beendet werden, was im Sinne von Privacy by Design möglichst sowohl im *FindMyBike-System* als auch in der polizeilichen IT technisch angelegt sein sollte.

Technisch voreingestellte zeitliche Grenzen könnten sich an den Verjährungsregeln für die Verfolgbarkeit des Diebstahls orientieren.[17] Eine Datenübertragung der Live-Positionsdaten an die Polizei kann nur solange erfolgen, wie der Diebstahl auch verfolgt werden kann, d. h. nach §§ 78 Abs. 3 Nr. 5 i. V. m. 242 Abs. 1 StGB üblicherweise drei Jahre. Dies erscheint allerdings zu lang. Einerseits ist nicht zu erwarten, dass die Polizei nach einem längeren

16 BVerfGE 65, 1 (Volkszählungsentscheidung).
17 Vgl. Keppeler/Berning, ZD 2017, S. 315 m. w. N.

Zeitraum noch eine Verfolgung beginnt, da in diesem Fall das Fahrrad oft nicht mehr im Zugriffsbereich der Polizei befindet oder bereits in seine Einzelteile zerlegt wurde. Gleichzeitig ist kaum noch mit einer wirksamen Ermittlungsarbeit zu rechnen, u. a. weil sich etwaige Zeug*innen in der Regel nicht mehr erinnern werden oder andere Spurenansätze nicht mehr verfolgt werden können. Allerdings könnte die Polizei auch nach einem längeren Zeitraum das Fahrrad immer noch im Rahmen der Gefahrenabwehr zurückholen, jedenfalls solange das Fahrrad nicht ins Ausland verbracht wurde. Auch könnte es sein, dass das Fahrrad länger steht und deswegen nicht geortet werden kann. Wenn aber dann der Akku wieder durch den Betrieb des Dynamos aufgeladen wird, könnte das Fahrrad wieder geortet werden. Der Betreiber des *FindMyBike-Systems* und die Trackingservice-Anbieter*in stehen damit vor dem Problem, dass sie selbst nicht beurteilen können, wie lange die Daten für die polizeilichen Verfahren von Bedeutung sind.

Ein gangbarer Weg könnte sein, dass das System nach sechs und neun Monaten automatisch anfragt, ob das Verfahren noch läuft, was von Polizei-Seite in der Fallbearbeitungssoftware zu bestätigen ist. Im Sinne eines wirkungsvollen Datenschutzes sind auch kürzere Zeiträume denkbar. Hierzu könnte etwa ein Dialogfenster in die Web-View integriert und möglicherweise in das polizeiliche Vorgangsbearbeitungssystem eingebunden werden. Nach einem Jahr sollte die Datenübertragung eingestellt werden, und es bedarf dann einer erneuten Aufforderung durch die Polizei oder die Tracking-Berechtigten zur Wiederaufnahme der Übertragung. So hat die Polizei einerseits die Möglichkeit, bei konkreten Hinweisen den Sachverhalt weiter aufzuklären, gleichzeitig wirkt das System darauf hin, unnötige Datenverarbeitungsprozesse zu beenden (Privacy by Design). Die Festlegung von Zeiträumen für den Abbruch der Datenübertragung ist im *FindMyBike-System* vorgesehen, sollte aber an den jeweiligen Workflow der Polizeien bei der Diebstahlsbearbeitung individuell angepasst werden.

Zudem ist den Tracking-Berechtigten bekannt, ob die Ermittlungsverfahren noch laufen. Werden sie als Geschädigte von der zuständigen Staatsanwaltschaft über die Einstellung des Verfahrens informiert, so sind sie verpflichtet, den Übertragungsvorgang abzubrechen, soweit dies nicht bereits die Polizei veranlasst hat, da die Daten nunmehr nicht mehr seitens der Polizei benötigt werden. Dementsprechend muss auch eine Abbruchmöglichkeit der Übertragung für den Bestohlenen vorhanden sein, etwa in der jeweiligen App der Trackingservice-Anbieter*in. Sofern das *FindMyBike-System* mit einem polizeilichen Datenverarbeitungssystem verknüpft ist, könnte ein Abbruch erfolgen, wenn die Polizei das Verfahren abschließt und an die Staatsanwaltschaft gibt.

### *3.2.2 Datenerhebung durch die Trackingservice-Anbieter*

Die Datenverarbeitung durch die Trackingservice-Anbieter*in kann mit Blick auf den Diebstahlsfall zwei Zwecke verfolgen, die rechtlich getrennt zu betrachten sind. Die Trackingservice-Anbieter*in erhebt die Daten, damit die Tracking-Berechtigten ihr Fahrrad wiedererhalten. Dies kann einerseits durch die Polizei andererseits aber auch auf dem zivilgerichtlichen Wege geschehen, d. h. die Tracking-Berechtigten können versuchen einen Herausgabetitel zu erlangen, wenn ihnen bekannt ist, wer das gestohlene Fahrrad in Besitz genommen hat. Alternativ können die Bestohlenen Schadensersatz verlangen, falls ihnen eine zu verklagende Person, insbesondere die Dieb*in bekannt ist. Insofern ist vom DS-GVO-konform verfolgten Zweck erfasst, dass die Daten solange erhoben werden, bis die Bestohlenen ihr Fahrrad zurückerhalten, bzw. bis sie das Fahrrad einer Person eindeutig zugeordnet haben.

Zivilrechtlich verjähren Herausgabeansprüche und andere dingliche Rechte erst nach 30 Jahren, siehe § 197 Abs. 1 Nr. 2 BGB. Dementsprechend könnte auch gerechtfertigt sein, die Daten solange durch den Trackingservice-Anbieter erheben zu lassen. Dies ist aber gerade im Hinblick darauf, dass es wahrscheinlich ist, dass das Fahrrad innerhalb von 30 Jahren – sollte es solange benutzbar sein - mehrfach die Besitzer*innen wechselt, höchst problematisch, da so diese meist über einen sehr langen Zeitraum beobachtet werden können. Geht es nur um die Herausgabe des Fahrrades oder um Schadensersatzansprüche, so sollten diese aufgrund des schnellen Wertverlustes von Fahrrädern zeitnah geltend gemacht werden. Wie lange eine Erhebung zur Förderung eines zivilrechtlichen Verfahrens erfolgen sollte, lässt sich aber nicht abstrakt, sondern nur im Einzelfall beurteilen. Sofern sich aus den Gesamtumständen ergibt, dass ein zivilrechtlicher Herausgabeanspruch nicht ernsthaft verfolgt wird, ist die Datenerhebung rechtswidrig. Dafür würde sprechen, dass über einen längeren Zeitraum weder zivilrechtliche Ansprüche geltend gemacht werden, noch die Polizei informiert wird. Dies wird oft spätestens nach sechs bis neun Monaten naheliegend sein. Daher sollten auch in diesem Fall die technischen Voreinstellungen die Übertragung zeitlich begrenzen und die Wiederaufnahme an gesondert zu begründende Software-Befehle geknüpft werden.

### *3.3 Transparenz*

Der Grundsatz der Transparenz gewährleistet, dass Betroffene Datenschutzvorgänge nachvollziehen können. Das Gebot der Transparenz bezweckt ein umfassendes Angebot an Informationen gegenüber den Betroffenen über die

Datenverarbeitung.[18] Dadurch soll ein effektiver Daten- und Rechtsschutz gewährleistet werden, da die betroffenen Personen nur so wirksam von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen können und so die Möglichkeit erhalten, entweder die Datenerhebung zuzulassen oder sich gegen diese zur Wehr zu setzen.[19]

Für die polizeiliche Arbeit gibt es kein umfassendes Transparenzgebot, was bereits aus zahlreichen Ermächtigungen zur heimlichen Überwachung in der StPO folgt.[20] D. h. aber nicht, dass die Polizei keine Pflichten zum transparenten Handeln hat, diese folgen vielmehr aus zahlreichen Vorschriften sowie verfassungsrechtlichen Vorgaben.[21] Entsprechende Pflichten bestehen aber oftmals nicht während der strafrechtlichen Ermittlung bzw. nur bei offenen Ermittlungsmaßnahmen unter die eine Ortung regelmäßig nicht fällt. Hinsichtlich der Polizei werden sich bei dem Anwendungsfall des *FindMyBike-Systems* regelmäßig nur nachträgliche Informationspflichten ergeben.

Allerdings muss nach der DS-GVO die Datenverarbeitung transparent ablaufen, Art. 5 Abs. 1 a und 13 ff. DS-GVO. Eine Datenverarbeitung nach dem Fairness-Grundsatz setzt voraus, dass Datenverarbeiter*innen den betroffenen Personen ermöglichen, von der Datenverarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden.[22]

Insofern stellt sich die Frage, inwieweit die heimliche Beobachtung von den Bewegungen von Diebesgut überhaupt mit der DS-GVO zu vereinbaren ist. In Teilen der Literatur wird davon ausgegangen, dass durch die Transparenz- und Informationspflichten der DS-GVO ein prinzipielles Verbot heimlicher Überwachung begründet wird.[23] Verdeckte Beobachtungen wären demnach nur möglich, wenn das Transparenzgebot durch einen Rückgriff auf Art. 23 Abs. 1 DS-GVO oder durch Normen beschränkt wird, die aufgrund von der Öffnungsklausel aus Art. 88 DS-GVO erlassen werden.[24] Weder ist aber Art. 88 DS-GVO einschlägig, noch sind Regelungen nach Art. 23 Abs. 1 DS-GVO erlassen worden, sodass heimliche Überwachungen nach der DS-GVO nicht gestattet wären.

---

18 Vgl. Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11 f.

19 Paal/Pauly- Frenzel 2021 , DS-GVO Art. 5 Rn. 21; Gierschmann/Schlender/Stentzel/Veil-Veil 2018, Art. 13 und 14, Rn. 2; Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11.

20 Erwägungsgrund 26 zur Justiz Richtlinie.

21 Aden/Fährmann/Bosch 2020, S. 6 ff.; Aden/Fährmann, TATuP 2020, S. 24 ff.

22 Gierschmann/Schlender/Stentzel/Veil-Veil 2018, Art. 13 und 14, Rn. 2.

23 Kühling/Buchner-Herbst 2020, Art. 5 Rn. 18; Byers, NZA 2017, S. 1887 f.; vgl. Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11.

24 Vgl. Kort, RdA 2018, S. 31; Byers NZA 2017, S. 1887 ff.; Lachenmann, ZD 2017, S. 411; Kühling/Buchner-Bäcker 2020, Art. 13 Rn. 14.

Allerdings könnte die DS-GVO auch so auszulegen sein, dass heimliche Überwachungen nicht grundsätzlich ausgeschlossen sind. Dafür könnte Art. 6 Abs. 1 f DS-GVO sprechen, der die zentrale Abwägungsklausel der DS-GVO darstellt.[25] Nach dieser Norm ist eine Interessenabwägung durchzuführen, bei der die jeweiligen Interessen der Beteiligten zu gewichten sind. Ein ausnahmsloses Verbot von heimlichen Kontrollen würde eine Interessenabwägung in Konstellationen unmöglich machen, in denen eine Partei die andere nicht kennt. So zeigt etwa der Diebstahl von Gegenständen, die geortet werden können, dass in diesem Bereich eine Interessenabwägung notwendig ist, da vielfach die Bestohlenen keine andere Möglichkeit haben, die entwendeten Gegenstände anders zurückzuerhalten. Bei einem ausnahmslosen Verbot von heimlicher Überwachung würde das aus Art. 14 Abs. 1 GG erwachsene Interesse am Schutz des Eigentums gänzlich unberücksichtigt bleiben. Es sind aber auch weitere Konstellationen denkbar, in denen das berechtigte Interesse an einer heimlichen Überwachung, die Interessen der Betroffenen überwiegen kann.[26] Verdeckte Überwachungen können etwa das einzige effektive Mittel sein, um einen konkreten Straftatverdacht im Unternehmen nachzugehen[27] oder um zivilrechtliche Ansprüche zu beweisen.[28] Dieb*innen können zudem damit rechnen, dass Fahrräder und anderes Diebesgut ortbar sind, da es entsprechende technische Lösungen und Produkte mittlerweile seit geraumer Zeit gibt. Vor dem Hintergrund, dass Dieb*innen Überwachungsrisiken kennen und diese in Kauf nehmen, werden ihre Interessen vielfach kaum überwiegen. Daher wird eine umfassende Berücksichtigung der Interessen, insbesondere der Eigentümer*innen oder anderer Berechtigter, nur dann ermöglicht, wenn eine Bewertung der Verhältnismäßigkeit im konkreten Einzelfall nicht pauschal ausgeschlossen wird.[29] Andernfalls wäre es nicht möglich, Eigentum und Besitz wirksam durch Ortungsfunktionen zu schützen, die auch eine präventive Wirkung entfalten können, gerade, wenn Dieb*innen die Sender nicht ohne weiteres stören oder entfernen können.

Auch deutet der Wille der Legislative darauf hin, dass heimliche Maßnahmen nicht zwingend ausgeschlossen sind. Aus dem Erwägungsgrund 47 Satz 3 geht hervor, dass bei der Interessenabwägung zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Datenverarbeitung erfolgen wird. Daraus wird

25 Byers, NZA 2017, S. 1089; vgl. Gola/Heckmann-Schulz 2022, DS-GVO Art. 6 Rn. 59.
26 Z. B. BAG NJW 2012, 49/2012, S. 3594 (3596).
27 Byers, NZA 2017, S. 1090.
28 Z. B. BGH NZV 2018, 08/2018, S. 367 (370 ff.) m. w. N.
29 Vgl. Byers, NZA 2017, S. 1090.

deutlich, dass auch heimliche Datenerhebungen vorgesehen sind, da diese Erwägung bei einer zwingenden Transparenz keinen Anwendungsfall hätte.

Zusätzlich lässt sich die Zulässigkeit von heimlichen Kontrollen im Einzelfall auch durch eine analoge Anwendung des Ausnahmetatbestands aus Art. 14 Abs. 5 b DS-GVO begründen. Diese Norm bezieht sich auf die Informationspflichten der datenschutzrechtlich Verantwortlichen (Art. 26 DS-GVO ff.), wenn die Datenerhebung bei Dritten und nicht unmittelbar beim Betroffenen erfolgt. Von den Informationspflichten sieht Art. 14 Abs. 5 b DS-GVO eine Ausnahme vor, wenn die vorherige Information der Betroffenen die Verwirklichung der Ziele der Datenverarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde. In Art. 13 DS-GVO, der die Informationspflichten der Verantwortlichen bei der direkten Datenerhebung regelt, fehlt eine solche Ausnahmeregelung, womit eine Regelungslücke vorliegt. Es ist auch davon auszugehen, dass diese planwidrig ist, da kein nachvollziehbarer Grund ersichtlich ist, weshalb bei der Datenerhebung bei Betroffenen keine Ausnahme von der Informationspflicht aus Art. 13 Abs. 1 DS-GVO gemacht werden kann, wenn die Informationen den Zweck der Datenerhebung vereiteln oder ernsthaft beeinträchtigen würden.[30] Diese Lücke erscheint zudem im vorliegenden Anwendungsfall besonders widersprüchlich, da es bei der Ortung gestohlener Gegenstände gar nicht möglich wäre, die Informationsverpflichtung einzuhalten, da die Ortung gerade dazu dient, die Dieb*innen aufzuspüren. Entsprechende Fallkonstellationen sind offenbar in der DS-GVO nicht mitgedacht worden. Es ist jedoch kaum vorstellbar, dass mit der DS-GVO bezweckt wird, Dieb*innen bzw. unberechtigte Besitzer*innen in ihrer rechtswidrigen Besitzposition umfassend zu schützen und damit die Aufklärung von Diebstählen mittels Positionsdaten unmöglich zu machen. Wäre diese Konstellation mitgedacht worden, hätte die Legislative für die Konstellation eine Ausnahmeregelung gestaltet.

Insgesamt steht die DS-GVO dem nicht-offenen Tracken gestohlener Fahrräder durch Privatpersonen oder –firmen sowie der Datenübertragung an die Polizei grundsätzlich nicht entgegen. Da die Interessen der Dieb*innen hier nicht überwiegen und Transparenz gegenüber den vom Tracking Betroffenen kaum gewährleistet werden kann, sind keine besonderen Transparenzanforderungen im *FindMyBike-System* umzusetzen. Anders ist dies indes zu beurteilen, wenn die Datenerhebung durch die Polizei erfolgt, die an die aus rechtsstaatlichen Gründen engeren Voraussetzungen der Strafprozessordnung gebunden ist.

Es wäre wünschenswert, wenn der Gesetzgeber von seinen Regelungsmöglichkeiten aus Art. 23 Abs. 1 DS-GVO Gebrauch machen würde. So könnten die Grenzen und die Pflichten im Zusammenhang mit einer heimlichen Datenerhebung eindeutiger festgelegt werden. Die bisherigen Ausführungen zeigen,

30 Byers, NZA 2017, S. 1090.

dass eine heimliche Datenerhebung in gewissen Konstellationen notwendig sein und auf die Betroffenenrechte unterschiedlich umfangreiche Auswirkungen haben kann. Da diese aber auch sehr eingriffsintensiv sein kann,[31] sollten dafür klare Regelungen bestehen.[32] Die Legislative könnte sich dabei etwa auf Art. 23 Abs. 1 d, j oder die Generalklausel aus e[33] stützen.

### *3.4 Datenminimierung, Speicherbegrenzung und Löschkonzepte*

Eine besondere Bedeutung für den Datenschutz hat der Grundsatz der Erforderlichkeit. Die Erhebung, Verarbeitung und Übermittlung personenbezogener Daten ist nur dann gestattet, wenn sie zur rechtmäßigen Aufgabenerfüllung der datenverarbeitenden und erhebenden Stelle für den jeweils damit verbundenen Zweck das mildeste, gleich geeignete Mittel ist. Gerade bei der automatisierten Verarbeitung personenbezogener Daten ist ein Verfahren auszuwählen oder zu entwickeln, welches die zur Zweckerreichung nötige Menge personenbezogener Daten so gering wie möglich hält. Diese Gedanken drücken sich im Grundsatz der Datenminimierung oder der Datensparsamkeit aus, Art. 5 Abs. 1 c DS-GVO. Der Grundsatz der Datenminimierung stellt einen zentralen Grundsatz des Datenschutzrechts dar[34] und drückt sich in verschiedenen Vorschriften aus und wird dort konkretisiert.[35]

Art. 5 Abs. 1 c DS-GVO vereint insgesamt drei eng miteinander verbundene Anforderungen unter dem Begriff der Datenminimierung. Personenbezogene Daten müssen für den mit der Erhebung und Verarbeitung verfolgten Zweck angemessen und erheblich sein und dabei zweckorientiert auf das nötige Maß beschränkt werden.[36] Dem Zweck angemessen sind Daten dann, wenn ihre Zuordnung zu dem angestrebten Zweck nicht zu beanstanden ist.[37] Aus der Kombination von Angemessenheit und Erheblichkeit ergibt sich schließlich, dass die Daten nicht nach der Präferenz der datenschutzrechtlich Verantwortlichen erhoben und verarbeitet werden dürfen, sondern vielmehr für die Zweckerreichung förderlich sein müssen.[38] Das Wort „Minimierung“ schreibt eine möglichst weite Begrenzung vor,[39] die Anforderungen wurden insofern mit der DS-GVO gegenüber der vorherigen Rechtslage konkretisiert und verschärft.

31 Z. B. BVerfG NJW 2016, 25/2016, 1781 (1785).
32 Vgl. Byers, NZA 2017, S. 1088.
33 Paal/Pauly-Paal 2021, Art. 23 Rn. 31a.
34 Vgl. Simitis-Scholz 2014, § 3 a Rn. 1.
35 Ehmann/Selmayr-Hebelein 2018, Art. 5 Rn. 23.
36 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 34.
37 Schantz/Wolff 2017, Rn. 421.
38 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 36.
39 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 34.

Also sind so wenige Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.[40] Der Grundsatz Datenminimierung lässt sich bereits beim Design eines IT-Systems umsetzen, indem das System so konzipiert wird, dass nur die Eingaben zugelassen werden, die für den Verarbeitungszweck unbedingt erforderlich sind. Insofern hängen Datenminimierung und *Privacy by Design* eng zusammen.

In § 47 Nr. 3 BDSG wird zwar nicht explizit von dem Grundsatz der Datenminimierung gesprochen, jedoch ergibt sich dieser Grundsatz aus dieser Norm und weiteren des BDSG und der JI-Richtlinie. So wird in § 47 Nr. 3 BDSG betont, dass von mehreren gleich geeigneten Maßnahmen stets diejenige zu wählen ist, die den geringsten Eingriff darstellt.[41] Dieser Grundsatz drückt sich auch in § 483 Abs. 1 StPO aus, nach dem nur Daten gespeichert werden dürfen, die für das Strafverfahren erforderlich sind. Auch wird in § 71 Abs. 1 Satz 1 BDSG von dem Grundsatz der Datensparsamkeit gesprochen, der mit der Datenminimierung teilidentisch ist. Zudem sind die in der JI-Richtlinie vorgeschriebenen Datenschutzgrundsätze wie die Datenminimierung im Hinblick auf den Anwendungsvorrang des Rechts der EU wirksam umzusetzen,[42] was für das gesamte BDSG gilt, unabhängig davon, ob der Anwendungsbereich der JI-Richtlinie oder der DS-GVO betroffen ist.

Der Grundsatz der Datenminimierung wird in zeitlicher Hinsicht durch den Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 e DS-GVO ergänzt.[43] Die eigenständige Betonung dieses Grundsatzes neben dem Grundsatz der Datenminimierung verleiht ihm ein besonderes Gewicht.[44] Aus ihm resultieren Pflichten zur Definition der für die jeweiligen Daten im Hinblick auf den konkreten Verarbeitungszweck erforderlichen Speicherdauer sowie Löschpflichten, die in Art. 17 DS-GVO zugleich als Löschanspruch der Betroffenen ausgestaltet sind. Zugleich folgt aus dem Zweckbindungsgrundsatz, dass keine Löschpflicht besteht, solange ein mit der Verarbeitung verfolgter rechtmäßiger Zweck vorliegt. Die sich aus der Verpflichtung zur Löschung ergebenden und anzuwendenden Löschfristen sind zu dokumentieren und nachzuweisen.[45]

Gerade bei den Grundsätzen der Datenminimierung und Speicherbegrenzung haben datenschutzfreundliche Voreinstellungen von Systemen eine beson-

40 Vgl. Landessozialgericht Berlin-Brandenburg, Urteil vom 01. Dezember 2011 – L 3 U 7/10 –, Rn. 48.

41 Wolff/Brink-Hertfelder Stand 2021, BDSG, § 47 Rn. 18; vgl. Johannes/Weinhold 2018, S. 66; Schantz/Wolff 2017, Rn. 440.

42 BT-Drs 18/11325, S. 98; Kühling/Buchner-Schwichtenberg 2020. § 47 BDSG Rn. 2.

43 Albrecht/Jotzo 2017, S. 52 f.; Wolff/Brink Stand-Schantz 2018, DS-GVO Art. 5 Rn. 32.

44 Wolff/Brink Stand-Schantz 2021, DS-GVO Art. 5 Rn. 32; vgl. Erwägungsgrundsatz 39 Satz 8.

45 Keppeler/Berning, ZD 2017, S. 315.

dere Bedeutung, die sich auch im *FindMyBike-System* niederschlagen müssen, Art. 25 Abs. 1 und Abs. 2 DSGVO[46] bzw. §§ 47 Nr. 3 und 71 BDSG. Daraus folgt, dass das *FindMyBike-System* und damit zusammenhängenden Systeme zur Verarbeitung von Positionsdaten bereits so zu gestalten sind, dass so wenig wie möglich personenbezogene Daten erhoben werden und gleichzeitig ein angemessenes Konzept für eine soweit wie möglich automatisierte Löschung besteht.[47]

### *3.4.1 Live-Postions- und Bewegungsdaten im FindMyBike-System*

Die Datenverarbeitung im *FindMyBike-System* dient dem Zweck, die Positionsdaten gestohlen gemeldeter Fahrräder an die Polizei zu übertragen, um die Strafverfolgung und eine Wiedererlangung des Fahrrades zu ermöglichen. Mithin sind nach dem Grundsatz der Datenminimierung nur die Daten zu übertragen, die für die Ermittlungsarbeit bzw. die Gefahrenabwehr notwendig sind. Dabei ist zwischen Live-Positionsdaten und gespeicherten Bewegungsdaten zu unterscheiden.

Um eine Live-Ortung zu ermöglichen, werden Live-Positionsdaten an die Polizei übertagen. Diese beinhalten den jeweils letzten, durch das Tracking der Positionsdaten bekannten Standort des gestohlenen Fahrrades (geographische Länge und Breite), den zugehörige Zeitstempel sowie einen Wert, der die Genauigkeit der jeweiligen Standortbestimmung beschreibt (*accuracy*). Diese Daten können als Kreis um einen Punkt (mit den oben erwähnten geographischen Koordinaten) visualisiert werden. Der Radius des Kreises entspricht dem Wert der *accuracy* in Metern. Weiterhin wird der genaue Zeitpunkt der letzten Standortbestimmung übermittelt. Diese Daten sind für die Ermittlungsarbeit erforderlich, weil die Polizei im Regelfall keine anderen Ansätze für das Ermittlungsverfahren bei gestohlenen Fahrrädern hat, soweit nicht ausnahmsweise andere Tatspuren oder Zeug*innen verfügbar sind. Die Kenntnis über den Standort des Fahrrades ermöglicht der Polizei nicht nur einen ersten Ermittlungsansatz, sondern kann im besten Falle zum Aufspüren der Dieb*innen führen, wenn diese das Fahrrad im Besitz haben.

Der Grundsatz der Datenminimierung wird im *FindMyBike-System* umgesetzt, indem die Ortungsdaten nur im Arbeitsspeicher verbleiben und nach der Speicherung eines (über den entsprechenden Datensatz berechneten) Hashwertes nicht dauerhaft gespeichert werden. Damit findet kein aktives Speichern von Ortungsdaten im *FindMyBike-System* statt. Aus dem Hashwert allein ergibt sich kein Personenbezug. Der Hashwert ermöglicht die Authentizität der

46 Baumgartner/Gausling, ZD 2017, S. 312.
47 Keppeler/Berning, ZD 2017, S. 318.

Daten nachzuweisen, was insbesondere für die Beweisqualität der Daten in einem späteren Strafverfahren relevant ist.[48] Zwar kann es aus Gründen des Integritätsschutzes (Datensicherung) sinnvoll sein, die Datensätze an mehreren Stellen zu speichern. Dies erfordert aber nicht zwingend, eine Speicherung bei unterschiedlichen Akteuren. Durch eine solche Speicherung wird zudem dem Grundsatz der Datenminimierung widersprochen und das Risiko eines illegalen Zugriffs erhöht. Eine sichere Speicherung mit den üblichen Backups beim Trackingservice-Anbieter reicht vorliegend aus. So ist gewährleistet, dass das *FindMyBike-System* selbst datenarm ausgestaltet ist, und es auch keines gesonderten Löschkonzepts bedarf, da die Daten nicht im *FindMyBike-System* verbleiben.

Durch den Umstand, dass im *FindMyBike-System* selbst keine Daten gespeichert werden, wird dem Grundsatz der Datenminimierung noch nicht vollständig entsprochen, da das System die Übertragung von beim Trackingservice-Anbieter gespeicherten Bewegungsdaten an die Polizei ermöglicht. Daher muss das System aus Gründen der Datenminimierung eine solche Datenübertragung nur dann umsetzen, wenn und solange die Polizei die Bewegungsdaten zwingend benötigt. So wird sichergestellt, dass die Daten auf das notwendige Mindestmaß beschränkt werden und gleichzeitig die Systeme der Polizei nicht mit unnötigen Daten belastet werden. Andernfalls bestünde auch ein Risiko, dass die Polizei aufgrund der Datenmenge relevante Hinweise übersieht[49] oder dass die Daten irrtümlich in den polizeilichen Systemen für andere Zwecke verarbeitet werden. Gleichzeitig wird so einer Speicherung auf Vorrat entgegengewirkt, da die Polizei selbst aktiv werden muss, um die Daten zu erlangen. Ein Abbruch des Vorganges wird durch den Vorgang ermöglicht, der unter 3.2.1 beschrieben wird.

Da nur die Polizei erkennen kann, wann die Bewegungsdaten für das Ermittlungsverfahren erforderlich sind, muss die Polizei diese über das *FindMyBike-System* anfordern. Eine automatische Übersendung wäre mit dem Grundsatz der Datenminimierung unvereinbar. Dies wurde im *FindMyBike-System* umgesetzt.

### *3.4.2 Speicherung der Bewegungsdaten bei der Polizei und beim Trackingservice-Anbieter*

Die stärkste Beeinträchtigung der Betroffenenrechte erfolgt durch die Speicherung der Bewegungsdaten bei Trackingservice-Anbieter*innen und bei der Polizei. Daher muss dort gewährleistet werden, dass die Daten gelöscht werden,

48 Näher hierzu Fährmann/Vollmar/Görlitz in diesem Band, S. 211ff.
49 Vgl. dazu Fährmann, MMR 2020, S. 231ff.

wenn sie nicht mehr für zivil- bzw. das strafrechtliche Verfahren benötigt werden.

Bei der Polizei können die Daten nur gespeichert werden, wenn sie konkret an ein Ermittlungsverfahren anknüpfen, vgl. § 483 Abs. 1 StPO. Die Löschfristen ergeben sich aus § 489 StPO, was sich in erster Linie danach beurteilt, ob die Daten für die Polizeiarbeit (noch) erforderlich sind. Auch die Polizei muss eine Infrastruktur vorhalten, die die Löschung von nicht mehr benötigten und rechtswidrigen Daten umsetzt,[50] vorrangig in einem automatisierten, im System-Design voreingestellten Verfahren. Das *FindMyBike-System* kann durch die beschriebene datensparsame Übertragungsform den Grundsatz der Datenminimierung und der Speicherbegrenzung auch für die polizeilichen Systeme lediglich fördern. Die genaue Umsetzung obliegt aber der Polizei.

Wie lange müssen die Bewegungsdaten aber von Trackingservice-Anbieter*innen für Polizei und Tracking-Berechtigte vorgehalten werden? Es kann sein, dass Fahrradbewegungen länger beobachtet werden müssen, um das Fahrrad oder den Diebstahl einer Person oder Personengruppe zuordnen zu können, insbesondere wenn es darum geht, Rückschlüsse auf bandenmäßige oder gewerbsmäßige Kriminalität zu ziehen. Ferner kann es sein, dass die Polizei das Fahrrad erst nach einiger Zeit auffinden kann, insbesondere, wenn die Polizeiressourcen stark ausgelastet sind. Daher müssen die Daten solange gespeichert werden, wie das Ermittlungsverfahren andauert. Hier ist auch zu beachten, dass eine Veranlassung der Löschung durch die Tracking-Berechtigten bzw. die Trackingservice-Anbieter*in unter Umständen eine Strafvereitlung nach § 258 Abs. 1 StGB bzw. eine versuchte Strafvereitlung[51] darstellen könnte. Die endgültige Löschung von Daten kann eine Vernichtung von Beweisen darstellen.[52] Vor diesem Hintergrund kann, solange das Verfahren läuft, von beiden nicht erwartet werden, dass sie Daten löschen, sodass die Speicherung durch ein Überwiegen der Interessen nach Art. 6 Abs. 1 f DS-GVO gerechtfertigt ist. Sollten allerdings bereits Daten an die Polizei übertragen worden sein, so sollten diese auch von den Trackingservice-Anbieter*innen gelöscht werden, wenn diese nicht für ein zivilrechtliches Verfahren oder für andere rechtlich zulässige Zwecke benötigt werden. Auch hierfür ist eine automatisierte Kennzeichnung der betreffenden Datensätze und die ebenfalls automatisierte Löschung zu empfehlen.

Wenn ein Ermittlungsverfahren mehr als ein Jahr in Anspruch nimmt, sollten sich Trackingsystem-Anbieter*innen und/oder Tracking-Berechtigte an

50 BT-Drs. 18/11325, S. 114 f.

51 Kapp/Schlump, BB 2008, S. 2482.

52 Vgl. Kapp/Schlump, BB 2008, S. 2482; Altenhain/Brunhöber/Cierniak-Cramer 2017, § 258 Rn. 24.

die Polizei wenden, um sicherzugehen, dass die Daten noch benötigt werden. Dazu sollten entsprechende niedrigschwellige Kommunikationsmöglichkeiten geschaffen werden und automatische Meldungen aus dem System erfolgen.

### *3.4.3 Pseudonomysierung personenbezogener Daten im FindMyBike-System*

Ein effektiver Datenschutz kann zudem über eine Pseudonymisierung unterstützt werden. Diese ist Ausdruck der Datenminimierung und kann ein wesentlicher Teil der datenschutzfreundlichen Gestaltung technischer Systeme sein.[53] Art. 4 Nr. 5 DSGVO definiert die Pseudonymisierung als Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen (Schlüssel) nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen gesondert, d. h. räumlich getrennt aufbewahrt werden. Die Informationen und Daten dürfen sich also nicht am selben Ort oder im selben System befinden oder zusammen weitergegeben werden.[54] Beim Einsatz von Pseudonymisierungsverfahren ist stets im Vorfeld zu klären, wer über Zuordnungstabellen bzw. das Verschlüsselungsverfahren verfügen soll, wer das Pseudonym generiert, ob ein Re-Identifizierungsrisiko ausgeschlossen werden kann und unter welchen Voraussetzungen eine Zusammenführung von Schlüssel und den personenbezogenen Daten gestattet ist.[55] Auch setzt die Pseudonymisierung voraus, dass technische und organisatorische Maßnahmen erfolgen, die die Nichtzuordnung sicherstellen.[56]

Ob eine Pseudonymisierung notwendig und sinnvoll ist, hängt davon ab, ob überhaupt Daten im System enthalten sind, die Rückschlüsse auf Personen zulassen. Die Positionsdaten werden im *FindMyBike-System* nicht gespeichert und können von den Betreibern keiner Person zugeordnet werden, da diese nur als Fall-ID übertragen werden, die keine Zuordnung erlaubt. Diese Fall ID-stellt damit eine Pseudonymisierung dar und setzt sich im *FindMyBike-System* aus einem beliebigen String aus Hexadezimal-Zeichen mit einer Länge von 64 Zeichen zusammen. Insofern ist die ID gegen Rückschlüsse abgesichert.

Insofern sind die Fahrradortungsdaten im *FindMyBike-System* gut geschützt.

Zusätzlich stellt sich die Frage, ob es sinnvoll ist, dass weitere Daten im System enthalten sind, die Rückschlüsse erlauben und ggf. eine Pseudonymisierung notwendig machen. Dies könnten die Daten der Bestohlenen sein. Da das

53 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 41; Marnau, DuD 2016, S. 431 f.
54 Auernhammer-Eßer 2020, Art. 4 Rn. 69; Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 43.
55 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 44.
56 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 46.

*FindMyBike-System* eine Softwareschnittstelle darstellt, um Daten an die Polizei weiterzuleiten, sind die Daten der Bestohlenen im System eigentlich nicht erforderlich, da die Polizei selbst über diese Daten aufgrund der Onlineanzeige verfügt. Bei einer Schnittstelle soll nämlich gerade gewährleistet werden, dass diese von verschiedenen Anbietern genutzt werden kann, ohne dass sich das System auf jeden Anbieter gesondert einstellen muss. Daher ist es ausreichend, das System zu konfigurieren, dass die eindeutige Zuordnung der jeweiligen Trackingdaten zu der dazugehörenden Diebstahlsanzeige möglich ist.

Jedoch könnten die Bestohlenen wirksam einwilligen, dass ihre Daten im System hinterlegt werden. Die polizeiliche Fahndung könnte etwa dadurch unterstützt werden, dass – soweit verfügbar – ein Foto oder eine Beschreibung des Fahrrades mit übertragen werden, was die Wahrscheinlichkeit eines Auffindens erhöhen dürfte. Diese Daten müssen aber ebenfalls nicht im *FindMyBike-System,* sondern bei der Polizei gespeichert werden. Die Bestohlenen könnten im Rahmen der Online-Anzeige, ein Bild des Fahrrades und eine Beschreibung an die Polizei senden. Noch effektiver erscheint es, dass die Daten des Fahrrades, inklusive Beschreibung und Foto, bereits im Vorfeld gespeichert werden. Andernfalls besteht die Gefahr, dass die notwendigen Daten bei der Anzeigeerstellung nicht griffbereit sind. Dazu könnte etwa die Fahrradpass-App der Polizei genutzt werden, in der sich sämtliche relevante Daten speichern lassen, die dann im Falle eines Diebstahls leicht an die die Polizei weitergeleitet werden können.[57] Im besten Fall könnte man in dieser App auch noch eine Verbindung zur Onlineanzeige herstellen, sodass die Daten automatisiert mit der Online-Anzeige versandt und automatisch mit dem polizeilichen Vorgang verknüpft werden. Auf die App könnte beim Kauf von GPS-Sendern oder entsprechend ausgestatten Fahrrädern direkt hingewiesen werden.

Hinsichtlich der Trackingservice-Anbieter*innen wäre eine Pseudonymisierung der Daten der Bestohlenen aus datenschutzrechtlichen Gründen sinnvoll, sofern diese nicht für die Abwicklung der vertraglichen Beziehungen vonnöten sind. Dies hängt aber von der Ausgestaltung des konkreten Service ab.

Allerdings ist es gegenwärtig bei der Online-Anzeige an die Berliner Polizei noch nicht möglich, Bilder des gestohlenen Gegenstandes (z. B. Fahrrad) im Rahmen der Onlineanzeige hochzuladen. Allerdings sollte diesem Umstand dringend abgeholfen werden, da dies die Ermittlungstätigkeit, nicht nur bei Fahrrädern, vereinfachen würde. So hätte die Polizei sofort Zugang zu Fotos gestohlener Gegenstände und diese auch digital zur Verfügung, sodass sie bei Bedarf unmittelbar für Fahndungs- und Ermittlungszwecke genutzt werden

57 https://www.polizei-beratung.de/themen-und-tipps/diebstahl-und-einbruch/diebstahl-von-zweiraedern/fahrradpass-app/ (letzter Aufruf: 26.02.2023).

können. Auch lassen sich Polizeibeamt*innen in Ermittlungsverfahren schon oft Bilder und Videos per Mail oder über spezielle Portale zusenden, was den Bedarf verdeutlicht. Für eine effektive Beweissicherung ist es sinnvoll, eine sichere Möglichkeit zur Übertragung von Bildern an die Polizei zu schaffen. Andernfalls müssten die Bürger*innen im Falle von vorhandenen Fotos immer noch extra zur Wache kommen, wodurch es sein kann, dass einige Bilder nicht zur Polizei gelangen. Eine Erleichterung der Arbeit durch die Online-Anzeige würde so nur partiell erreicht. Auch würde dem Grundsatz der Datenminimierung entsprochen, wenn Daten nur dort gespeichert würden, wo sie tatsächlich benötigt werden. Ziel sollte es also sein, der Polizei die für den Diebstahl notwendigen Daten einfach verfügbar zu machen.

### *3.5 Integrität der Daten*

Aus Art. 5 Abs. 1 f DS-GVO und § 47 Nr. 6 BDSG folgt, dass die Integrität und Vertraulichkeit der Daten vor unbefugter oder unrechtmäßiger Verarbeitung und durch geeignete technische und organisatorische Maßnahmen vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen ist. Die Schutzmechanismen sind nicht verbindlich festgelegt und orientieren sich am konkreten Einzelfall.[58] Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten gehören zu den Schlüsselelementen moderner IT-Sicherheitsmechanismen. In der DS-GVO wird der Grundsatz der Integrität in Art. 32 und Art. 24 Abs. 1 DS-GVO konkretisiert.[59] Nach Art. 32 Abs. 1 DS-GVO sind nach dem Risikoprinzip[60] geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, der Umfang sowie der Zweck der Verarbeitung, die Implementierungskosten und die Eintrittswahrscheinlichkeit sowie die Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigten. Auch hier orientiert sich das Schutzniveau daran, was nach dem Grundsatz der Verhältnismäßigkeit im konkreten Fall von den Datenverarbeiter*innen gefordert werden kann und welche Risiken für die Betroffenen bestehen.[61]

Integrität lässt sich als „Unversehrtheit" definieren. „Unversehrtheit" bedeutet, dass keine Veränderung der Daten durch unbefugte Zugriffe erfolgt ist, d. h. keine Verfälschung, Ergänzung oder Beschränkung. Die Datensätze

58 Vgl. BT-Drs. 18/11325, 111; Kühling/Buchner-Schwichtenberg 2020, BDSG § 47 Rn. 2.
59 Baumgartner/Gausling, ZD 2017, S. 310.
60 Gola/Heckmann-Piltz 2022, Art. 32 Rn. 22.
61 Gola/Heckmann-Piltz 2022, Art. 32 Rn. 13.

müssen aber auch gegen Schadensereignisse geschützt werden.[62] Vom Integritätsschutz ist damit der Schutz vor Zugriffen Dritter, etwa durch Hacker*innen, aber auch die technisch reibungslose Gewährleistung des Regelbetriebs umfasst. So ist etwa eine Überlastung informationstechnischer Systeme oder eine fehlerhafte Datenverarbeitung zu vermeiden.[63]

Ein Datum ist nur vertraulich, wenn personenbezogene Daten nur einem befugten Empfängerkreis bekannt werden.[64] Auch aus Gründen der Vertraulichkeit ist also ein unbefugter Zugriff auf die Daten auszuschließen.[65] Maßnahmen zur Umsetzung der Vertraulichkeit sind beispielsweise eine Zutritts-, Zugriffs-, Zugangskontrolle oder die Verschlüsselung von Daten, Art. 32 Abs. 1a DS-GVO.[66]

Ein manipulativer Zugriff auf die Positionsdaten gestohlener Fahrräder erscheint zunächst eher unwahrscheinlich. Allerdings handelt es sich um Daten, die für ein strafrechtliches Verfahren relevant sein können. Eine Manipulation könnte damit beträchtliche Folgen haben. Etwa könnte es zu einem unberechtigten Strafverfahren kommen, was wiederum Zwangsmittel bis hin zu einer unberechtigten Festnehme fälschlich eines Diebstahls bezichtigter Personen führen könnte. Wenn ein umfassender Schutz vor Zugriffen von außen nicht gewährleistet ist, muss die Polizei die Integrität der Daten deswegen allein aufgrund ihrer rechtsstaatlichen Verpflichtung aus 20 Abs. 3 GG genau prüfen.

Bei der Trackingservice-Anbieter*in gespeicherte Bewegungsdaten sind hinsichtlich der personenbezogenen Informationen deutlich sensibler als die im *FindMyBike-System* verarbeitete Live-Position, so dass hier gesteigerte Pflichten zur Gewährleistung eines adäquaten Zugriffsschutzes bestehen.

Das *FindMyBike-System* ist gegen unbefugten Zugriff von außen durch die folgenden technisch-organisatorischen Vorkehrungen geschützt: Der Zugriff auf die Ortungsdaten erfolgt über einen URL. Es ist daher sicherzustellen, dass von außen nicht auf die URL zugegriffen werden kann. Dies wird durch die Beschränkung des IP-Bereichs erreicht, d. h. nur Rechner aus dem Netzwerk der Polizei Berlin können mittels der URL auf das *FindMyBike-System* zugreifen, für alle andern IP-Adressen ist der Zugriff nicht möglich. Weiterhin verhindert

62 Paal/Pauly-Frenzel 2021, DS-GVO Art. 5 Rn. 47; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 43.

63 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 35.

64 Auernhammer-Kramer/Meints 2020, Art. 32 Rn. 33; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 45.

65 Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 36; vgl. BVerfGE 120, 274 (315).

66 Paal/Pauly-Martini, 2021 DS-GVO Art. 32 Rn. 35; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 30 ff.

die Firewall einen Zugriff auf andere Ports als Port 443 (HTTPS, Hypertext Transfer Protocol Secure).

Auch sind die Daten auf dem risikobehafteten Übertragungsweg gegen unautorisierte Zugriffe und Veränderungen zu schützen. Dazu muss eine Verschlüsselung der Daten erfolgen,[67] wozu das kryptografische Verfahren in Betracht kommt.[68] Aus Art. 32 Abs. 1 DS-GVO könnte folgen, dass die BSI-Standards der Verschlüsselung zu Grunde gelegt werden können. In Art. 32 Abs. 1 a 2. Alt. DS-GVO wird unter anderem als Maßnahme die Verschlüsselung der Daten genannt. Anhaltspunkte für den Stand der Technik bieten die Technischen Richtlinien des Bundesamts für die Sicherheit in der Informationstechnik (BSI). Den vom BSI ausgearbeiteten IT-Schutzmaßnahmen kommt zwar keine unmittelbare rechtlich verbindliche Wirkung zu.[69] Die Richtlinien geben aber eine Orientierung zu den aktuellen Möglichkeiten der IT-Sicherheit und damit für den Stand der Technik.[70] Art. 32 Abs. 1 DSGVO enthält keine konkreten Angaben, wie die Verschlüsselung auszugestalten ist, sondern orientiert sich, wie bereits festgestellt, am Risikoprinzip. Daher ist es naheliegend, hier die BSI-Richtlinien als Stand der Technik zu Grunde zu legen, wie dies auch nach Rechtslage vor Inkrafttreten der DS-GVO der Fall war (§ 9 BDSG alt[71] und Anlagen).[72] Zudem ist es sinnvoll, die aktuellen Vorgaben an dynamische Regelungen anzupassen, die sich u. a. in den jeweils aktuellen technischen Anforderungen in den BSI-Richtlinien widerspiegeln.[73]

Die Umstände, unter denen die Daten übertragen werden, sowie die Art der Daten und die Wahrscheinlichkeit einer Rechtsgutsverletzung erfordern eine sichere Verschlüsselung. Auch wenn ein unbefugter Zugriff auf den Datenübertragungsprozess eher unwahrscheinlich ist, ist wiederum entscheidend, dass die Daten ein polizeiliches und ggf. gerichtliches Handeln nach sich ziehen. Daher sind hohe Verschlüsselungsstandards anzulegen, gleichgültig ob es sich um Bewegungsdaten oder einzelne Live-Positionsdaten handelt. Die Verschlüsselung der Datenübertragung richtet sich daher nach BSI TR-02102. Zur Verschlüsselung wird das Verschlüsselungsprotokoll „Transport Layer Security“ (TLS)

67 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 36; Roßnagel 2003, 3.4 Rn. 77.
68 Heinson 2015, S. 149; Marnau, DuD 2016, S. 431.
69 Vgl. Kilian-Illies/Lochter/Stein 2018, Kryptografie Rn. 58.
70 Mitterer/Wiedemann/Zwissler, BB 2018, S. 7; Günther, VV 2018, S. 52; Paal/Pauly-Nolden 2021, BDSG § 64 Rn. 3; Kühling/Buchner-Schwichtenberg 2020, BDSG § 64 Rn. 3.
71 Wolff/Brink Stand-Paulus 2021, DS-GVO Art. 32 Rn. 3.
72 Baumgartner/Gausling, ZD 2017, S. 311.
73 Vgl. Baumgartner/Gausling, ZD 2017, S. 311; Grosskopf/Momsen, CCZ 2018, S. 105; Roßnagel/Nebel, NJW 2014, S. 887; Bartsch/Rieke, EnWZ 2017, S. 437; Roßnagel, MMR 2018, S. 34.

verwendet. Hierbei werden vom BSI grundsätzlich die Versionen TLS 1.2 und TLS 1.3 empfohlen.[74]

Für den Aufbau einer gesicherten Datenverbindung im TLS-Protokoll wird eine Cipher-Suite, eine standardisierte Sammlung der zu verwendenden kryptographischen Algorithmen für Schlüsseleinigung (und ggf. für die Authentisierung), für die Verschlüsselung der Daten sowie eine Hashfunktion für die Integritätssicherung der Datenpakete verwendet. Für das *FindMyBike-System* wurde eine Cipher-Suite mit Perfect Forward Secrecy (gewählt, mit der „eine Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden kann".[75] Alle in den Technischen Richtlinien TR-02102-2 aufgeführten Cipher-Suites[76] sind für den Aufbau von gesicherten Datenverbindungen geeignet.

Ferner können sogenannte Eingabekontrollen zum Schutz der Integrität beitragen. Durch diese werden Protokolldaten in IT-Systemen ausgewertet. Dadurch wird ermöglicht, nachträglich zu überprüfen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.[77]

Vergleichbare Standards sind auch bei der Datenübertragung durch die Trackingservice-Anbieter*in einzuhalten. Für die Übertragung an die Polizei ergibt sich die Anwendbarkeit der BSI-TR zudem aus § 64 Abs. 1 S. 2 BDSG. Aus dieser Norm folgt, dass der Gesetzgeber die BSI-TR als Standard zur Umsetzung von den datenschutzrechtlichen Vorgaben sieht, der zumindest zu berücksichtigen ist.

Überdies stellt sich die Frage, inwieweit Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung im *FindMyBike-System* zu gewährleisten sind. Grundsätzlich ist es eine wirksame Maßnahme zum Schutz der Integrität der Daten, regelmäßig Kopien der Datensätze zu erstellen und diese sicher zu speichern.[78] Dabei ist allerdings zu beachten, dass das Erstellen von Kopien im Konflikt zum Grundsatz der Datenminimierung steht.[79] Weitere Kopien an verschiedenen Orten erhöhen außerdem das Risiko, dass auf die Daten unbefugt zugegriffen wird. Daher sind die Kopien ebenfalls gesondert zu sichern, und die Anzahl der Kopien muss in einem angemessenen Verhältnis zu

74 Bundesamt für Sicherheit in der Informationstechnik 2021.
75 Bundesamt für Sicherheit in der Informationstechnik 2021, S. 8.
76 Bundesamt für Sicherheit in der Informationstechnik 2021, S. 8 ff.
77 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 37.
78 Sydow/Marsch-Mantz 2022. Art. 32, Rn. 18 m. w. N.; Paal/Pauly-Martini 2021, Art. 32 Rn. 38a; vgl. Härting 2016, S. 38.
79 Paal/Pauli-Martini 2021, DS-GVO Art. 32 Rn. 38a.

der Bedeutung der Daten und den erfolgten Arbeitsschritten stehen. Es dürfen daher nicht mehr Kopien erstellt werden als unbedingt notwendig sind.

Wie dargelegt, ist das *FindMyBike-System* bewusst darauf angelegt, dass auf die Speicherung von Daten innerhalb des Systems verzichtet wird, um in erster Linie eine Softwareschnittstelle bereitzustellen, die von unterschiedlichen Anbieter*innen genutzt werden kann. Dies schließt nicht aus, dass bei der Trackingservice-Anbieter*in und bei der Polizei entsprechende Kopien angelegt werden und ist sogar insbesondere mit Blick auf die Beweisqualität der Daten empfehlenswert.

Neben diesen „datenbezogenen Maßnahmen" sind die Normadressaten dauerhaft und kontinuierlich verpflichtet,[80] den ungestörten Betrieb der Datenverarbeitungsanlage sicherzustellen. Dazu muss das System im Sinne des Art. 32 Abs. 1 b 5. Var. DS-GVO belastbar sein. Dazu ist z. B. eine unterbrechungsfreie Stromversorgung sicherzustellen, um einem Datenverlust vorbeugend entgegenzuwirken.[81] Die Datenverarbeitungssysteme müssen so belastbelastbar sein, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gewährleistet ist. Dazu muss das System auch vor Angriffen von außen, etwa durch die gezielte Überlastung von Servern mittels sog. DoS- oder DDoS-Attacken geschützt sein.[82] Dies müsste bei einer Umsetzung des *FindMyBike-Systems* in der Praxis beachtet werden. Hinsichtlich der Polizei und der Trackingservice-Anbieter*in bleibt festzuhalten, dass die betroffenen Systeme insgesamt wenigstens ein dem *FindMyBike-System* vergleichbares Schutzniveau aufweisen sollten, wobei gerade bei der Polizei ein deutlich höheres Schutzniveau zu erwarten wäre.

## 4. Rechtliche Einordnung der Datenverarbeitung beteiligten Akteure

An dem *FindMyBike-System* partizipieren unterschiedliche Akteure (Übersicht unter 2.), die zueinander in unterschiedlichen rechtlichen Verhältnissen stehen. Um die gegenseitigen Rechte und Pflichten sowie die rechtlichen Risiken zu klären, die für die einzelnen Akteure bestehen, wird der rechtliche Rahmen untersucht. Dabei ist zu beachten, dass die Rechtsverhältnisse wesentlich durch vertragliche Absprachen bestimmt werden. Empfehlungen für die vertragliche Ausgestaltung sollen an dieser Stelle nicht ausgesprochen werden (diese ori-

80 Paal/Pauly-Martini 2021, DS-GVO Art. 32 DS-GVO Rn. 40.

81 Auernhammer-Kramer/Meints 2020, DS-GVO Art. 32 Rn. 41 f.; Paal/Pauly Martini 2021, DS-GVO Art. 32 Rn. 38b.

82 Sydow/Marsch-Mantz 2022, Art. 32, Rn. 17; vgl. Gerlach 2015, S. 585.

entieren sich an den Leistungen im Einzelfall), sondern nur der rechtliche Rahmen, der aus der DS-GVO folgt.

Zu klären ist insbesondere die Frage, wer in einem solchen mehrstufigen Datenverarbeitungsprozess bei mehreren Beteiligten die Verantwortung für die Einhaltung von datenschutzrechtlichen Vorgaben trägt und für Fehlverhalten potenziell haftet. Verantwortliche sind natürliche oder juristische Personen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Sie sind neben den Auftragsverarbeiter*innen die zentralen Normadressaten der DS-GVO und für die Einhaltung der Datenschutzbestimmungen rechtlich verantwortlich, haften für Schäden und machen sich ggf. bußgeldpflichtig.[83] Mit der Verantwortlichkeit gehen zahlreiche Prüf-, Rechenschafts- und Dokumentationspflichten einher.[84] So sind die Verantwortlichen nach Art. 5 Abs. 2 DS-GVO für die Einhaltung der Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO verantwortlich. Auch müssen sie nach Art. 24 Abs. 1 DS-GVO nachweisen, dass die Datenverarbeitung DS-GVO-konform erfolgt. Zudem haben sie nach Art. 24 Abs. 2 DS-GVO für angemessene Datenschutzvorkehrungen zu sorgen.

Die DS-GVO sieht ausdrücklich vor, dass es mehrere Verantwortliche geben kann (Art. 4 Nr. 7). In diesem Rahmen können mehrere Personen gemeinsame Entscheidungen fällen. Aber es können auch Personen mit verschiedenen Verantwortungsbereichen arbeitsteilig zusammenwirken.[85] So werden vielfach Infrastrukturen von Anbieter*innen zur Verfügung gestellt, die dann wiederum von anderen Dienstleister*innen genutzt werden.[86] Auch wird der Prozess der Datenverarbeitung zunehmend nicht mehr von den Personen durchgeführt, die diesen veranlasst haben, sondern dieser wird an entsprechend spezialisierte Anbieter*innen ausgelagert. Erschwerend kommt teilweise hinzu, dass die Anbieter*innen von Infrastrukturen selbst Zugang auf die dabei verarbeiteten Daten haben, z. B. im Rahmen der Systemadministration. Auch Privatpersonen greifen auf Datenverarbeitungsangebote von externen Anbietern zurück. Insofern sind oft verschiedene Akteure an einem Datenverarbeitungsprozess beteiligt, die in unterschiedlichem Maße Einfluss auf die einzelnen Verarbeitungsschritte haben.

83 Auernhammer–Eßer 2020, Art. 4 Rn. 77; Schwartmann/Jaspers/Thüsing/Kugelmann- Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 128 f.

84 Radtke 2021, S. 36.

85 Schwartmann/Jaspers/Thüsing/Kugelmann-Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 139 f.

86 Berlit 2016, Anm. 3.

Maßgeblich für die Einstufung als Verantwortliche ist, dass die betreffenden Akteure über den Zweck und die Mittel der Verarbeitung mitentscheiden.[87] Für eine Verantwortlichkeit ist erforderlich, dass eine tatsächliche Einflussnahme auf das „Ob", „Warum" und das „Wie" der Datenverarbeitung erfolgt.[88] Dabei ist zu berücksichtigen, dass der Einfluss auf den Zweck und die Mittel unterschiedlich ausgeprägt sein kann;[89] gerade bei mehreren Beteiligten. Daher muss ein Grad an Einfluss auf Zweck und Mittel erreicht werden, der es rechtfertigt, die jeweiligen Beteiligten im konkreten Einzelfall als Verantwortliche einzustufen. Abhängig vom Kontext der Verarbeitung können die Zwecke oder die Mittel stärker im Vordergrund stehen.[90]

Auftragsverarbeiter*innen sind nach Art. 4 Nr. 8 DS-GVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag der Verantwortlichen verarbeiten. Die Auslagerung von Datenverarbeitungsprozessen an externe Anbieter kommt mittlerweile sehr oft vor. Den Rahmen hierfür definiert Art. 28 DS-GVO, der aufgrund der mit der Auslagerung verbundenen datenschutzrechtlichen Risiken die Zulässigkeit der Auftragsverarbeitung an strenge Voraussetzungen knüpft.[91] Maßgeblich sind vertragliche Vereinbarungen für das Verhältnis, Art. 28 Abs. 3 S. 1 DS-GVO, wobei in S. 3 zahlreiche Inhalte der Verträge geregelt sind, z. B. mit Blick auf die Datensicherheit c oder der Pflicht aus f, die Verantwortlichen bei gewissen Verpflichtungen zu unterstützen. Auch die Haftung auf Schadensersatz ist bei der Auftragsverarbeitung möglich, Art. 82 Abs. 1 DSGVO. Allerdings ist die Haftung in Art. 82 Abs. 2 S. 2 DS-GVO eingeschränkt und geht nicht so weit wie bei den Verantwortlichen.

Die Verantwortlichen haben indes mehr Verpflichtungen als die Auftragsverarbeiter*innen. Ihre Pflichten werden in Art. 24 DS-GVO konkretisiert. Sie haben im Rahmen eines risikobasierten Ansatzes dafür einzustehen, dass die Datenverarbeitung in zulässiger Art und Weise abläuft, wobei sie für die notwendigen technischen und organisatorischen Maßnahmen zu sorgen haben.[92] Sie tragen auch dann die Verantwortung für die Einhaltung der Vorgaben der

87 WP 169, S. 15; BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 Rn. 28; Däubler/Wedde/Weichert/Sommer–Weichert 2020, DSGVO Art. 4 Rn. 87; Schwartmann/Jaspers/Thüsing/Kugelmann-Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 153; Auernhammer-Eßer 2020, Art. 4 Rn. 79.

88 WP 169, S. 11; Gierschmann/Schlender/Stentzel/Veil- Kramer 20218, Art. 4, Rn. 2; Martini/Fritsche, NVwZ-Extra 2015, S. 5 m. w. N.

89 Vgl. BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 Rn. 28.

90 WP 169, S. 16.

91 Wolff/Brink-Spoerr 2021, DS-GVO Art. 28 Rn. 1 ff.; Däubler/Wedde/Weichert/Sommer-Weichert 2020, Art. 4 Rn. 96.

92 Gola/Heckmann-Gola 2022, Art. 4 Rn. 63.

DS-GVO, wenn sie personenbezogene Daten durch Auftragsverarbeiter verarbeiten lassen.[93]

### *4.1 Tracking-Berechtigte*

Die Tracking-Berechtigten bestimmen über das „Ob" der Datenverarbeitung, da sie durch die Installation der Trackinghard und Software und den Abschluss eines Vertrages mit einem Trackingservice-Anbieter die wesentliche Ursache für die Verarbeitung setzen. Auch erfolgt das Tracken, damit sie mit Hilfe der Polizei ihr Fahrrad zurückerlangen können oder um in einem etwaigen zivilrechtlichen Prozess Herausgabe- oder Schadensersatzansprüche beweisen können („Warum").

Allerdings stellt sich die Frage, ob die Tracking-Berechtigten Einfluss auf das „Wie" der Datenverarbeitung haben. Die Kontrolle über die technischen Abläufe obliegt den Trackingservice-Anbieter*innen bzw. dem System-Betreiber*innen. Diese Abläufe werden die Tracking-Berechtigten im Regelfall nicht nachvollziehen können. Damit stellt sich die Frage, inwieweit sie – als die den Datenverarbeitungsprozess veranlassende Person – Kontrolle über die Vorgänge der konkreten Datenverarbeitungsprozesse haben müssen.

Gegen die Verantwortung der Tracking-Berechtigten könnte der begrenzte Einfluss auf die Datenverarbeitung sprechen, da diese den Prozess lediglich starten und beenden können,[94] ohne ausreichenden Einfluss auf die Verarbeitung zu haben, um eine Verantwortlichkeit zu begründen.[95] Eine bloße Mitursächlichkeit für das Aufkommen der personenbezogenen Daten würde dementsprechend nicht für eine Verantwortung ausreichen.[96] Eine solche Rechtsauslegung wäre jedoch mit Blick auf die Gewährung eines effektiven Datenschutzes problematisch. Der Begriff der Verantwortlichen ist zentral für die Anwendung der datenschutzrechtlichen Vorgaben, sodass im Regelfall kein Raum für eine einschränkende Auslegung besteht.[97] Andernfalls könnten sich Betroffene nicht ausreichend gegen Eingriffe zur Wehr setzen. Für einen effektiven Schutz der Rechte und Freiheiten der betroffenen Personen bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer Zuteilung der Verantwortlichkeiten, einschließlich der Fälle, in denen Verantwortliche die Verarbeitungszwecke und -mittel gemeinsam mit anderen

93 Gierschmann/Schlender/Stentzel/Veil-Kramer 2018, Art. 4 Nr. 7 Rn. 2 m. w. N.
94 Vgl. Voigt/Alich, NJW 2011, S. 3543; Hoffmann/Schulz/Brackmann, ZD 2013, S. 123 f.
95 Vgl. BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 - Rn. 28.
96 Martini/Fritsche, NVwZ-Extra 2015, S. 5; Voigt/Alich, NJW 2011, S. 3543; OVG Schleswig, ZD 2014, S. 644.
97 Karg, ZD 2014, S. 55 m. w. N.

Verantwortlichen festlegen oder ein Verarbeitungsvorgang im Auftrag von Verantwortlichen durchgeführt wird. Dies spricht dafür, die Verantwortlichkeit zunächst möglichst weit zu interpretieren, da andernfalls das Datenschutzniveau von vornherein reduziert würde.

Die Anforderungen an die Verantwortlichen sind hoch. Insbesondere müssen sie nach Art. 5 Abs. 2 DS-GVO die Einhaltung der DS-GVO Vorschriften nachweisen können. Dies können Privatpersonen - also Verbraucher/innen - kaum leisten, insbesondere wenn sie keinen Zugriff auf das IT-System haben. Wenn es aber möglich wäre, dass eine Verantwortung bereits dadurch ausgeschlossen wäre, dass die beauftragende Personen die Datenverarbeitungsprozesse nicht beeinflussen kann, dann könnte dies dazu führen, dass sich auch Unternehmen, Organisationen und sogar staatliche Stellen durch die Auswahl entsprechender Anbieter*innen einer datenschutzrechtlichen Verantwortung entziehen könnten.[98] Bewusste Unwissenheit könnte also dazu führen, dass keine Verantwortung besteht, während Personen, die sich trotz externer Anbieter um die Steuerung des Datenverarbeitungsprozesses bemühen, verantwortlich wären.[99] Dies erscheint widersprüchlich. Der Umstand, dass ein eingerichteter Service genutzt wird, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann die Nutzer*innen also nicht von ihren Verpflichtungen zum Schutz personenbezogener Daten befreien.[100]

Eine Verantwortlichkeit kann dementsprechend nur dann mit Sicherheit abgelehnt werden, wenn keinerlei rechtlicher oder tatsächlicher Einfluss auf die Verarbeitung besteht.[101] Die Tracking-Berechtigten können das Tracking starten und bestimmen, wann es beendet wird. Sie können entscheiden, dass die Daten an die Polizei übertragen werden und die Daten auch mehrfach speichern bzw. speichern lassen. Ohne sie würde der Trackingvorgang nicht stattfinden, und das Tracking erfolgt ausschließlich in ihrem Interesse. Somit rechtfertigen ihr Handlungsspielraum und die Steuerungsmöglichkeiten, sie als Verantwortliche zu behandeln. Die Möglichkeiten, auf das Tracking Einfluss zu nehmen, sind so groß, dass sie als Verantwortliche einzustufen sind.

Allerdings können die Pflichten der Tracking-Berechtigten bei einer gemeinsamen Verantwortlichkeit (etwa mit der Trackingservice-Anbieter*in) auch einschränkend interpretiert werden. Dies folgt aus dem risikobasierten

98 Karg, ZD 2014, S. 56.

99 Karg, ZD 2014, S. 56; Caspar, ZD 2015, S. 14; Martini/Fritsche, NVzW-Extra 2015, S. 4 f., die darin allerdings keinen Widerspruch sehen und allein an objektiven Kriterien anknüpfen wollen.

100 EuGH Urt. v. 5.6.2018 – C-210/16, BeckRS 2018, 10155.

101 WP 169, S. 15.

Ansatz.[102] Dieser Ansatz zieht sich durch die Vorschriften der DS-GVO[103] und drückt sich damit als zentrale Ausprägung des Verhältnismäßigkeitsprinzips in zahlreichen Vorschriften aus.[104] So spiegelt sich dieses Prinzip etwa in den Art. Art. 24 Abs. 1 S. 1, Abs. 2, Art. 25 Abs. 1, Art. 30 Abs. 5, Art. 32 Abs. 1, 2, 35 und 39 Abs. 2 i. V. m. 38 Abs. 2 DS-GVO wider, die die Pflichten der Verantwortlichen konkretisieren. Daraus folgt auch, dass die Pflichten bei privater Datenverarbeitung im Vergleich zu Datenverarbeitung im Rahmen geschäftlicher Tätigkeiten weniger weit reichen. So ist es denkbar, dass von Großkonzernen höhere Datenschutzstandards zu erwarten sind als von kleineren Unternehmen oder gar von Privatpersonen. Insbesondere muss dabei berücksichtigt werden, dass die einzuleitenden Schritte wirtschaftlich vertretbar sind, solange die Rechte der Betroffenen angemessen gewürdigt werden.[105] Insofern können abhängig vom konkreten Einzelfall einzelne Verantwortliche auch anders behandelt werden als andere, je nachdem, was sie leisten können. Dies folgt auch aus Art. 26 DS-GVO, der bei mehreren Verantwortlichen auch bewusst von verschiedenen Pflichten ausgeht. Das Bestehen einer gemeinsamen Verantwortlichkeit hat damit nicht zwangsläufig gleichwertige Pflichten zur Folge.[106]

Die Tracking-Berechtigten dürften in der Regel als Kunden nur sehr beschränkt prüfen können, ob datenschutzrechtliche Vorgaben bei dem Trackingservice-Anbieter*innen eingehalten werden. So kann etwa die Datensicherheit kaum überprüft werden, wenn die Hard- und Software ausschließlich beim Anbieter betreiben wird. Auch werden die Daten meist im Zugriffsbereich der Trackingservice-Anbieter*innen verbleiben, sodass die Bestohlenen nicht kontrollieren können, was mit den Daten passiert. Dieses Argument gilt umso mehr, wenn es sich bei den Tracking-Berechtigten um Verbraucher*innen handelt. Daher kann im Wesentlichen von den Tracking-Berechtigten nur zwingend erwartet werden,

- dass Sie Auftragsverarbeiter*innen auswählen, bei denen sie davon ausgehen können, dass diese die datenschutzrechtlichen Vorgaben einhalten; dies kann durch die Gestaltung von Musterverträgen und die Bestellung speziell versierter Datenschutzbeauftragter für die Trackingdienste-Anbieter*in erfol-

102 Ausführlich dazu Veil, ZD 2015, S. 347 ff.; Veil, ZD 2018, S. 13 ff.; Gola/Heckmann-Piltz 2022, Art. 24 Rn. 23.

103 Gola/Heckmann-Piltz 2022, Art. 24 Rn. 23; Schantz/Wolff 2017-Wolf, S. 149; Kühling/Buchner-Bergt 2020, Art. 39, Rn. 23; vgl. Veil, ZD 2015, S. 348.

104 Gola/Heckmann 2022-Piltz Art. 24 Rn. 23; Veil, ZD 2015, S. 350 ff.; vgl. Veil, ZD 2018, S. 15.

105 Sydow/Marsch-Raschauer 2022, Art. 24, Rn. 32.

106 EuGH EuZW 2018, 13/2018, 534 (537).

gen. Außerdem ist es nach Art. 28 Abs. 5 DS-GVO durch die Wahl einer nach Art. 42 DS-GVO zertifizierten Auftragsverarbeiter*innen (der Schutz der Betroffenen wird durch die Zertifizierung sichergestellt) möglich, die Erfüllung der Pflichten aus Art. 28 Abs. 1 – 4 DS-GVO als Verantwortliche nachweisen. In Art. 28 Abs. 5 DS-GVO drückt sich der Gedanke aus, dass die Vorteile der Auftragsverarbeitung nicht durch zu hohe Anforderungen an die Verantwortlichen faktisch unmöglich gemacht werden sollen. Damit soll ermöglicht werden, dass die Verantwortlichen einen Datenverarbeitungsprozess ausgliedern können, ohne dass sie im Einzelnen die Verarbeitung der Daten nachvollziehen oder kontrollieren können. Für private und nicht-kommerzielle Auftraggeber gilt dies in besonderem Maße. Zudem kann sich die Wahl einer zertifizierten Anbieter*in auch auf ein etwaiges Bußgeldverfahren auswirken, § 83 Abs. 2 j DS-GVO. Es ist daher damit zu rechnen,

- dass entsprechende Zertifikate in der Praxis eine hohe Bedeutung haben werden, wodurch allerdings ggf. Kosten entstehen, die in der Regel von den Auftraggeber*innen, hier also von den Tracking-Berechtigten zu tragen sein werden.
- dass sie im Falle einer erkennbar rechtswidrigen Datenverarbeitung die Verarbeitung stoppen und etwaiger rechtswidrig erhobenen Daten löschen und/oder die Löschung veranlassen, Art. 17 Abs. 1 d DS-GVO;
- dass sie gem. der Art. 13 DS-GVO ff. den Informations- und Auskunftsrechten nachkommen, sofern die Betroffenen von der Datenerhebung erfahren haben und die Betroffenen ihnen bekannt sind.[107] Daher sind sämtliche Vorgänge sowohl im *FindMyBike-System* als auch bei den Trackingservice-Anbieter*innen zu dokumentieren, Art. 30 DS-GVO.

### *4.2 Trackingservice-Anbieter*in*

Ob die Trackingservice-Anbieter*innen Verantwortliche im Sinne DS-GVO sind, hängt im Wesentlichen von der vertraglichen Ausgestaltung ab. Sofern die vertragliche Ausgestaltung nicht eindeutig ist, gibt es aber gewisse Indikatoren, die auf eine Verantwortlichkeit der Trackingservice-Anbieter*innen hinweisen. Diese Indikatoren müssen im Rahmen einer wertenden Gesamtbetrachtung aller Umstände beurteilt werden.

---

107 Da dies im Regelfall erst nach Abschluss der polizeilichen Ermittlungen der Fall sein wird oder wenn der Betroffene von Ermittlungen der Polizei erfährt, steht dies nicht im Konflikt zu den polizeilichen Ermittlungen. In diesen Fällen ist vielmehr damit zu rechnen, dass die Polizei das Fahrrad entweder beschlagnahmt hat oder den Betroffenen bereits als Beschuldigten eingestuft hat. Ggf. haben die Betroffenen im Rahmen eines Strafverfahrens ohnehin Akteneinsicht.

Als wesentliches Abgrenzungskriterium zwischen Auftragsverarbeiter*innen und Verantwortlichen dient die Weisungsbindung gem. Art. 28 Abs. 3 a und Art. 29 DS-GVO. Die Auftragsverarbeiter*innen werden demnach abhängig vom Verantwortlichen tätig. Die Auftragsverarbeitung setzt damit voraus, dass die Auftragsverarbeiter*innen auf Grundlage eines definierten Auftrags gem. Art. 28 DS-GVO in Bezug auf die Daten für die Verantwortlichen fremdbestimmt tätig werden.[108] Ob eine solche Abhängigkeit besteht, bemisst sich danach, wie groß der Entscheidungsspielraum der Auftragsverarbeiter*innen ist. Wenn ihre Rolle auch Entscheidungen enthält, die den Verantwortlichen vorbehalten sind, wie beispielsweise „Welche Daten werden verarbeitet?“, „Wie lange werden sie verarbeitet?“, „Wer hat Zugang zu ihnen?“,[109] kann eine Trackingservice-Anbieter*in auch selbst Verantwortlicher im Sinne von Art. 24 DS-GVO sein. Für eine entsprechende Einstufung kann beispielsweise sprechen, wenn sie die Daten auch für eigene Zwecke verarbeitet, beispielsweise um Rückschlüsse auf die Nutzung bestimmter Fahrradrouten oder die Auslastung von Leihrädern zu ziehen.[110] Für eine alleinige Verantwortung der Tracking-Berechtigten kann sprechen, wenn die Trackingservice-anbieter*innen nur einen engen Entscheidungsrahmen haben und die wesentlichen Entscheidungen vom Tracking-Berechtigten gefällt werden.

### *4.3 Betreiber*in des FindMyBike-Systems*

Auch für die Betreiber*in des *FindMyBike-Systems* stellt sich die Frage, ob sie als Auftragsverarbeiter*in oder als Verantwortliche einzustufen ist. In erster Linie werden durch das *FindMyBike-System* Daten von den Trackingservice-Anbieter*innen zur Polizei weitergeleitet, was dafür spräche, dass es sich um eine Auftragsverarbeitung handelt, da keine wesentlichen Entscheidungen getroffen werden. Das System agiert in erster Linie durch den Datentransport eher passiv, sodass eine Verantwortlichkeit fernliegend ist, wobei sich dies auch durch entsprechende vertragliche Absprachen ändern kann.

108 Paal/Pauly-Ernst 2021, DS-GVO Art. 4 Rn. 56.

109 WP 169, S. 17.

110 Vgl. EuGH Urteil v. 13.5.2014 – C-131/12 -, Rn. 28 ff.; WP 169, S. 18; wobei auch nur eine Verantwortlichkeit im Hinblick auf die für eigene Zwecke erhobenen Daten bestehen könnte, vgl. Martini/Fritsche NVwZ-Extra 2015, S. 8 f. Eine entsprechende Differenzierung erscheint aber wenig praxistauglich, da sich die Datensätze nicht immer klar trennen lassen.

### *4.4 Polizei*

Für die Einhaltung der Datenschutzvorgaben bei der polizeiinternen Verarbeitung der übermittelten Positionsdaten ist die Polizei zuständig. Dies folgt unmittelbar aus den Art. 4 Abs. 4 i. V. m. 3 Nr. 8 der JI-Richtlinie und dem Gebot der Gesetzmäßigkeit der Verwaltung aus Art. 20 Abs. 3 GG.[111]

## 5. Wesentliche Schlussfolgerungen

Es ist deutlich geworden, dass eine Softwareschnittstelle mit hohen Datenschutzstandards umgesetzt werden kann, nicht zuletzt durch interdisziplinäre Forschungsarbeit. Damit können gesteigerte datenschutzrechtliche Risiken durch die Übertragung von Positionsdaten gestohlener Gegenstände an die Polizei wirksam begrenzt werden. Die zunehmende Bedeutung der Grundsätze Privacy by Design und Default kann an diesem Beispiel verdeutlicht werden und es wird erkennbar, wie wenige Daten für eine Übertragung tatsächlich erforderlich sind.

Auch die Rechte, Pflichten und Risiken für die beteiligten Akteure erscheinen überschaubar. Die DS-GVO eröffnet auch in dieser spezifischen Konstellation einen Rahmen, der für Verantwortliche eine sachgerechte Aufteilung der Pflichten und Risiken mit Auftragsverarbeiter*innen oder anderen Verantwortlichen ermöglicht. Das Risiko, von Betroffenen in Anspruch genommen zu werden, erscheint gering und auf grob datenschutzrechtliche Mängel beschränkt. Auch wenn die Pflichten der Tracking-Anbieter*innen an und der Systembetreiber*in höher sind, können diese – wie dargelegt – durch eine entsprechende System- und Organisationsgestaltung wirksam und dauerhaft minimiert werden.

Eine Umsetzung in der Praxis steht aus einer datenschutzrechtlichen Perspektive nichts entgegen, wobei auch der Datenschutz bei der Polizei durch eine Verknüpfung mit dem *FindMyBike-Stystem* verbessert werden könnte.

## Literaturverzeichnis

Aden, H./Fährmann, J. (2020) Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, in: TATuP, 29 Jg., Nr 3, S. 24–28.

111 Johannes/Weinhold 2018, S. 68.

Aden, H./Fährmann, J./Bosch, A. (2020) Intransparente Polizeikontrollen – rechtliche Pflichten und technische Möglichkeiten für mehr Transparenz. In: Hunold, D./Ruch, A. (Hg.): Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts. Wiesbaden: Springer VS, S. 3–22.

Albrecht, J. P./Jotzo, F. (2017) Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse. Baden Baden: Nomos.

Barlag, C. (2017) Anwendungsbereich der Datenschutz-Grundverordnung. In: Roßnagel, A. (Hg.): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts. Baden-Baden, S. 108–117.

Bartsch, A./Rieke, I. (2017) Das neue Datenschutzrecht mit Auswirkungen auch auf Energieversorger, in: EnWZ 06 Jg. Nr. 12, S. 435–441.

Baumgartner, U./Gausling, T. (2017) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Was Unternehmen jetzt nach der DS-GVO beachten müssen, in: ZD 07 Jg., Nr. 07, S. 308–313.

Berlit, U.-D. (2016): Anmerkung zu BVerwG 1. Senat, Beschluss vom 25.02.2016 - 1 C 28/14, jurisPR-BVerwG (13), Anmerkung 3.

Borell, A./Schindler, S. (2019) Polizei und Datenschutz, Datenschutz und Datensicherheit,– in: DuD 43. Jg. Nr. 12, S. 767–773.

Bosch, A./Fährmann, J./Aden, H. (2021) Kontrollquittungen und -statistiken – Ein Instrument zur Durchsetzung des Diskriminierungsverbots bei Polizeikontrollen, in: ZKKW 7 Jg. Nr. 1, S. 186–218.

Bundesamt für Sicherheit in der Informationstechnik (2021) Technische Richtlinie TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2021-01. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2 (letzter Aufruf: 21.02.2023).

Byers, P. (2017) Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, in: NZA 34. Jg., Nr. 17, S. 1086–1091.

Caspar, J. (2015) Nutzung des Web 2.0- zwischen Bürgernähe und Geschwätzigkeit? Einsatz von Web 2.0-Plattformen durch öffentliche Stellenam Beispiel der Polizei, in: ZD 5 Jg., Nr. 1, S. 12–17.

Däubler, W./Wedde, P./Weichert, T./Sommer, I. (2020) EU-Datenschutz-Grundverordnung und BDSG-neu. 2. Auflage. Frankfurt am Main.

Ehmann, E./Selmayr, M. (2018) Datenschutz-Grundverordnung. 2. Aufl. München: C.H.Beck.

Eßer, M./Kramer, P./von Lewinski, K. (2020) DSGVO BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. 7. Aufl. Köln.

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

Fährmann, J. (2021) Mehr Transparenz durch technische Innovationen? Wie Technik polizeiliche Personenkontrollen effektiver und transparenter machen könnte, in: MMR 24 Jg., Nr. 10, S. 775–779.

Gerlach, C. (2015) Sicherheitsanforderungen für Telemediendienste - der neue § 13 Abs. 7 TMG, CR 31. Jg., Nr. 9, S. 581–589.

Gierschmann, S./Schlender, K./Stentzel, R./Veil, W. (2018) Kommentar Datenschtuz-Grundverodnung. Köln: Bundesanzeiger Verlag.

Gola, P./Heckmann, D. (2022): DS-GVO. Datenschutz-Grundverordnung VO (EU) 2016/679. 3. Aufl. München.

Gola, P./Schomerus, R. (2015) Bundesdatenschutzgesetz. 12. Aufl. München.

Grosskopf, L./Momsen, C. (2018) Outsourcing bei Berufsgeheimnisträgern – strafrechtliche Verpflichtung zur Compliance?, in: CCZ 11 Jg., Nr. 3), S. 98–108.

Günther, D.-C. (2018) Auf dem Stand der Technik, in: VV, S. 50–52.

Härting, N. (2016) Datenschutz-Grundverordnung. Köln: Otto Schmidt.

Heinson, D. (2015) IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen. Tübingen: Mohr Siebeck.

Hoffmann, C./Schulz, S./Brackmann, F. (2013) Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten, in: ZD 3 Jg., Nr. 3, S. 122–126.

Johannes, P. C. (2017) Unterschiede in der Datenschutz-Folgenabschätzung für Polizei und Strafverfolgungsbehörden nach europäischem und deutschem Recht, in: ZD-Aktuell 7 Jg., Nr. 19, S. 5852.

Johannes, P. C. (2019) Sicherheit der Datenverarbeitung nach § 64 BDSG im Vergleich zur JI-Richtlinie und DS-GVO, in: ZD-Aktuell, 09 Jg., Nr. 19, S. 6875.

Johannes, P. C./Weinhold, R. (2018) Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Baden-Baden: Nomos.

Kapp, T./Schlump, A. (2008) Ist die Vernichtung von (kartellrechtlich relevanten) Unternehmensunterlagen zulässig?, in: BB Nr. 46, S. 2478–2486.

Karg, M. (2014) Anmerkung, in: ZD 4 Jg., Nr. 1, S. 54–56.

Keppeler, L. M./Berning, W. (2017) Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten. Anforderungen an Löschkonzepte und Datenbankstrukturen, in: ZD 7 Jg., Nr. 7, S. 314–319.

Kilian, W. (2018) Computerrechts-Handbuch. Computertechnologie in der Rechts- und Wirtschaftspraxis. 34. Aufl. München: Beck.

Koós, C./Englisch, B. (2014) Eine „neue" Auftragsverbeitung? Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs, in: ZD 4 Jg., Nr. 06, S. 276–285.

Kort, M. (2018) Neuer Beschäftigtendatenschutz und Industrie 4.0, in: RdA 71. Jg., Nr. 1, S. 24–33.

Kühling, J./Buchner, B. (2020) Datenschutz-Grundverordnung. BDSG Kommentar. 3. Aufl. München.

Kühling, J./Klar, M./Sackmann, F. (2021) Datenschutzrecht. 5. Aufl. Heidelberg.

Lachenmann, M. (2017) Neue Anforderungen an die Videoüberwachung. Kritische Betrachtungen der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu, in: ZD 4 Jg., Nr. 9, S. 407–411.

Marnau, N. (2016) Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung, in: DuD Nr. 7, S. 428–433.

Martini, M./Fritsche, S. (2015) Mitverantwortung in sozialen Netzwerken. Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, in: NVwZ-Extra, 34. Jg., Nr. 21, S. 1–16.

Mitterer, K./Wiedemann, M./Zwissler, T. (2018: BB-Gesetzgebungs- und Rechtsprechungsreport zu Industrie 4.0 und Digitalisierung 2017, in: BB 08.01.2018, Nr. 01-02, S. 3–15.

Paal, B./Pauly, D. (2021) Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. 3. Aufl. München: Beck.

Radtke, T. (2021): Gemeinsame Verantwortlichkeit unter der DSGVO. Unter besonderer Berücksichtigung von Internetsachverhalten. Baden-Baden: Nomos.

Roßnagel, A. (2003) Handbuch Datenschutzrecht. München: C. H. Beck.

Roßnagel, A. (2018) Das Vertrauensdienstegesetz. Neue Regelungen zur Anpassung des deutschen Rechts an die EU-eIDAS-VO, in: MMR 21. Jg., Nr. 1, S. 31–35.

Roßnagel, A./Nebel, M. (2014) Beweisführung mittels ersetzend gescannter Dokumente, in: NJW, S. 886–891.

Sander, G. M./Joecks, W./Miebach, K. (2017) Münchener Kommentar zum Strafgesetzbuch. Band 4, §§ 185-262. 3. Aufl. München: C.H.Beck.

Schantz, P./Wolff, H. A. (2017) Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis.

Schenk, S. von/Mueller-Stöfen, T. (2017) Die Datenschutz – Grundverordnung: Auswirkungen in der Praxis, in: GWR 9 Jg., Nr. 9, S. 171–179.

Schwartmann, R./Jaspers, A./Thüsing, G./Kugelmann, D. (2020) DS-GVO/BDSG. Datenschutz-Grundverordnung/Bundesdatenschutzgesetz. 2. Auflage. Heidelberg.

Sydow, G./Marsch, N. (2022) Europäische Datenschutzgrundverordnung. 3. Auflage. München.

Veil, W. (2015) DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip. Eine erste Bestandsaufnahme, in: ZD 05 Jg., Nr. 08 , S. 347–353.

Veil, W. (2018) Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, in: ZD 9 Jg., Nr. 1, S. 9–16.

Voigt, P./Alich, (2011) Facebook-Like-Button und Co. - Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, in: NJW 64 Jg., Nr. 49, S. 3541–3544.

Wolff, H. A./Brink, (2022) BeckOK Datenschutzrecht. 41. Edition. München.

*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.

*Alexander Vollmar[1]/Gudrun Görlitz[2]/Kevin Kober[3]*

# IT-System zur Echtzeitverfolgung von mit GPS-Trackern ausgestatteten Fahrrädern bei Diebstahl unter Berücksichtigung der rechtlichen Rahmenbedingungen

## 1. Einführung

Im FindMyBike-Projekt wurde in einem interdisziplinären, rechtlich-verwaltungswissenschaftlichen und informationstechnischen Ansatz in Zusammenarbeit mit dem in Berlin ansässigen Unternehmen Noa Technologies GmbH und dem Landeskriminalamt Berlin ein modulares Softwaresystem entwickelt, welches das Auffinden gestohlener Fahrräder mit Hilfe von Positionsbestimmung mittels GPS erleichtert.

Das zu entwickelnde Softwaresystem – im Folgenden *FindMyBike-System* genannt – soll dazu dienen Fahrrad-Live-Positionsdaten von unterschiedlichen Flottenbetreibern bzw. GPS-Trackingservice-Providern[4] über eine standardisierte Schnittstelle datenschutz- und rechtskonform an die Polizei zu übertragen.

Der Einsatz dieses Systems erfordert Änderungen am bisherigen polizeilichen Workflow bei Anzeige und Verfolgung von Fahrraddiebstählen. Bereits heute kann die Erstellung einer Anzeige nach einem Fahrraddiebstahl über die Internet-Wache der Polizei Berlin erfolgen. Mit der Einführung des *FindMyBike-Systems* muss das entsprechende Internet-Formular um neue Felder erweitert werden. Diese Erweiterung umfasst insbesondere die Möglichkeit einer rechtsverbindlichen Freigabe des Gebrauchs der Live-Positionsdaten des gestohlenen Fahrrades.

---

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

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

3 Kevin Kober war in dem Projekt FindMyBike studentische Hilfskraft für den Bereich Informatik.

4 Im weiteren Verlauf wird der Begriff “Trackingservice-Anbieter” zusammenfassend für alle Flottenbetreiber und GPS-Trackingservice-Provider verwendet.

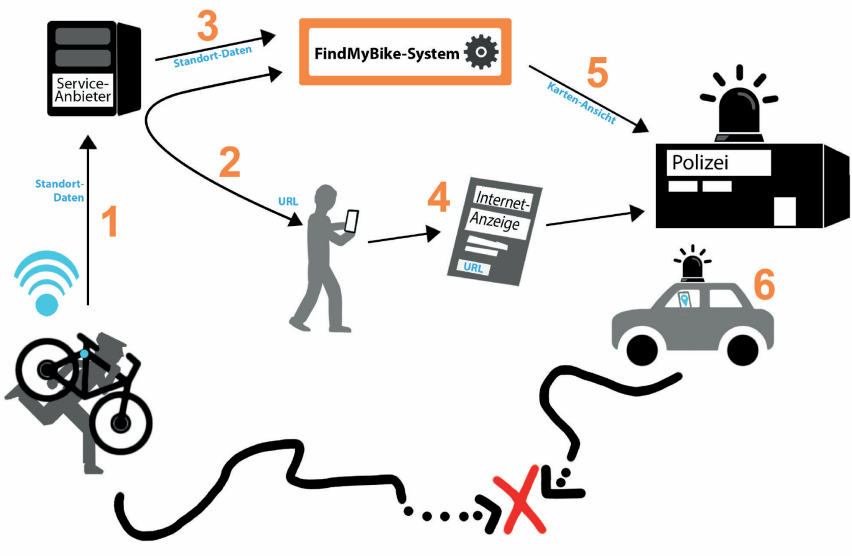


*Abbildung 1: Schematische Darstellung der Anzeige und der Verfolgung von Fahrraddiebstählen mit Unterstützung von GPS-Daten (Grafik: Mark Gebler, Alexander Vollmar)*

In Abbildung 1 ist die zukünftige Vorgehensweise bei Anzeige und Verfolgung eines Fahrraddiebstahles schematisch dargestellt: Nachdem ein mit einem GPS-Tracker ausgestattetes Fahrrad gestohlen wurde (‚1' in Abbildung 1), bemerkt der*die Besitzer*in den Diebstahl und fordert beim jeweiligen Trackingservice-Anbieter eine URL an (2). Diese URL wird durch das *FindMyBike-System* generiert und vom Trackingservice-Anbieter mit dem Fahrrad verknüpft. Unmittelbar nach dem Abrufen der URL beginnt der Anbieter die Positionsdaten des Fahrrades (mit der URL als ID) an das *FindMyBike-System* zu übermitteln (3). Die bestohlene Person erstellt daraufhin eine Anzeige über die Internet-Wache der Polizei (4) und fügt die vorher abgefragte URL in ein dafür vorgegebenes Feld des Internet-Formulars ein. Die Polizei kann mit Hilfe der URL das *FindMyBike-System* aufrufen und hat damit Zugriff auf eine Kartenansicht, auf der die jeweils letzte bekannte Position des Fahrrades dargestellt wird (5). Mit Hilfe der Anwendung führt die Polizei die Suche nach dem Fahrrad durch und findet im Idealfall sowohl das gestohlene Fahrrad als auch den Dieb (6).

## 2. Systembeschreibung

Die Hauptaufgabe des *FindMyBike-Systems* besteht im Bereitstellen einer standardisierten Schnittstelle für die Übertragung von Live-Positionsdaten von gestohlenen Fahrrädern von Trackingservice-Anbietern zur Polizei. Diese Schnittstelle soll sämtlichen Anbietern zur Verfügung stehen und die datenschutz- und rechtskonforme Übertragung von Live-Positionsdaten an die Polizei ermöglichen.

### *2.1 Ablauf der Datenverarbeitung*

Die Verarbeitung der Live-Positionsdaten im Gesamtsystem wird von drei unterschiedlichen Akteuren*innen durchgeführt: dem jeweiligen Trackingservice-Anbieter, dem zentralen *FindMyBike-System* sowie der Polizei (siehe Abbildung 2).

Um das System nutzen zu können, muss ein mit einem GPS-Tracker ausgestattetes Fahrrad bei einem Trackingservice-Anbieter angemeldet sein und kontinuierlich seine Positionsdaten an diesen Provider übermitteln. Nachdem ein solches Fahrrad gestohlen und der Diebstahl bemerkt wurde, benötigt die oder der Bestohlene eine URL, die beim *FindMyBike-System* abgerufen werden kann. Dieses Abrufen der URL sollte innerhalb der App des Trackingservice-Anbieters geschehen können, z.B. durch das Drücken eines hierfür vorgesehenen Buttons. Hierdurch wird beim *FindMyBike-System* eine URL angefragt, generiert und an die App weitergeben. Die URL verweist auf eine fahrradspezifische Kartenansicht des *FindMyBike-Systems* und wird zusammen mit dem zugehörigen Zeitstempel in einer Datenbank abgespeichert.

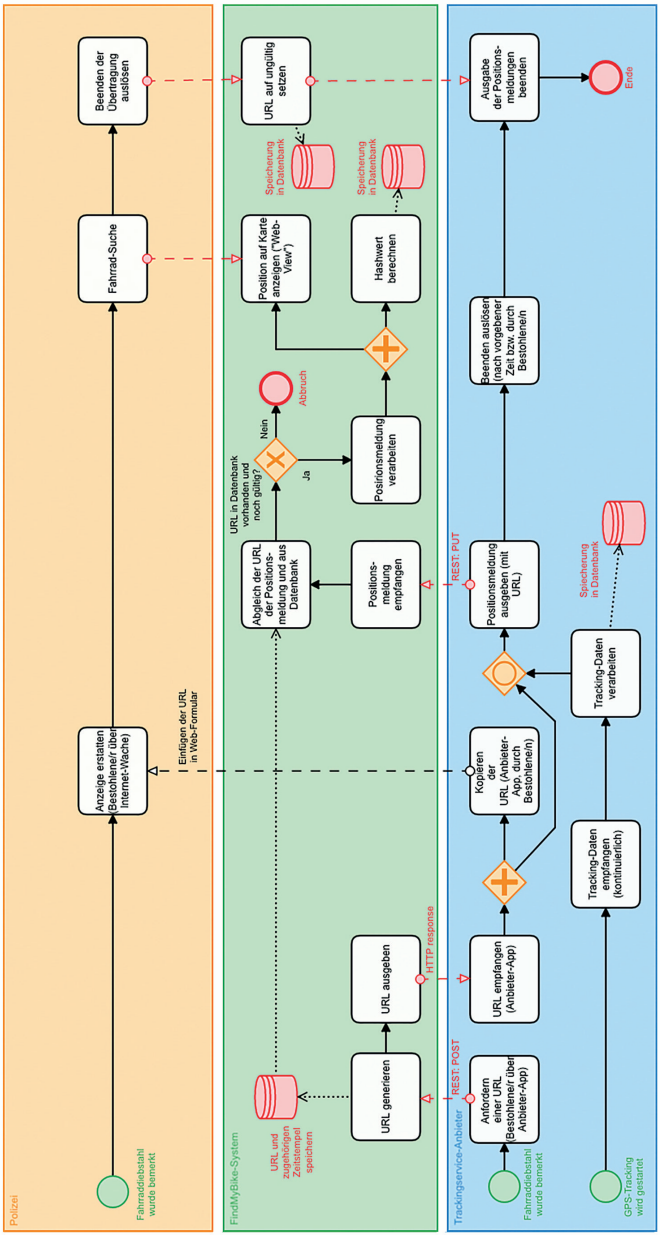


*Abbildung 2: FindMyBike-System: Verarbeitung von Positionsdaten (nahezu) in Echtzeit (Grafik: Alexander Vollmar)*

Nach dem Abrufen der URL kann mit deren Hilfe eine Diebstahlanzeige über das Internet-Formular der Internet-Wache der Polizei erstattet werden. Die URL wird beim Erstellen der Anzeige in ein eigens dafür vorgesehenes Feld des Webformulars eingefügt.

Sobald die URL vom Trackingservice-Anbieter empfangen wurde, beginnt dieser die Positionsdaten des gestohlenen Fahrrades an das *FindMyBike-System* zu übertragen. Hierbei werden Push-Nachrichten an die oben generierte URL und somit an das *FindMyBike-System* gesendet. Dieses nimmt die Nachrichten mit den Positionsdaten entgegen und fragt in der Datenbank ab, ob die URL existiert und wann sie erstellt wurde. Die URL ist nur innerhalb eines aus rechtlichen Überlegungen festgelegten maximalen Zeitraums gültig. Nach dem Ablauf dieses Zeitraums lehnt es das System ab, Nachrichten mit der jeweiligen URL zu verarbeiten. Falls die URL jedoch in der Datenbank vorhanden und noch gültig ist, wird die Nachricht verarbeitet. Hierbei wird zum einen ein Hashwert über die gesamte Nachricht berechnet und in einer Datenbank abgelegt, zum anderen wird die Position, die aus der Nachricht extrahiert wurde, der URL zugeordnet, so dass dieser bei Aufruf der URL in einer von einem weiteren Service erzeugten Web-View dargestellt werden kann. Der hierbei generierte Hashwert wird später für das nachträgliche Abrufen von Live-Positionsdaten benötigt (siehe 3.3).

Nachdem die Anzeige empfangen wurde, kann die Polizei unter Verwendung der übermittelten URL eine Web-View des *FindMyBike-Systems* öffnen, welche eine Kartenansicht beinhaltet. Auf dieser Karte wird die jeweils letzte bekannte Position des gestohlenen Fahrrades angezeigt. Falls die Position des Gerätes, auf dem das *FindMyBike-System* genutzt wird, und damit auch die Position der Person, die das *FindMyBike-System* gerade verwendet, mit Hilfe der W3C Geolocation API[5] bestimmt werden kann, wird auch dieser auf der Karte visualisiert. Die Angabe der jeweiligen eigenen Position ist insbesondere bei der Suche nach einem Fahrrad im Gelände hilfreich.

## *2.2 Der Aufbau des FindMyBike-Systems*

Das *FindMyBike-System* besteht aus zahlreichen Softwaremodulen, welche die verschiedenen Services realisieren (siehe Abbildung 3). Zentrales Element des Systems ist die Message Broker-Software RabbitMQ, eine nachrichtenorientier-

5 Die Spezifikation der W3C Geolocation API findet sich unter https://www.w3.org/TR/geolocation-API

te Middleware, über die ein großer Teil der internen Kommunikation abgewickelt und eine Parallelisierung von Prozessen umgesetzt wird.

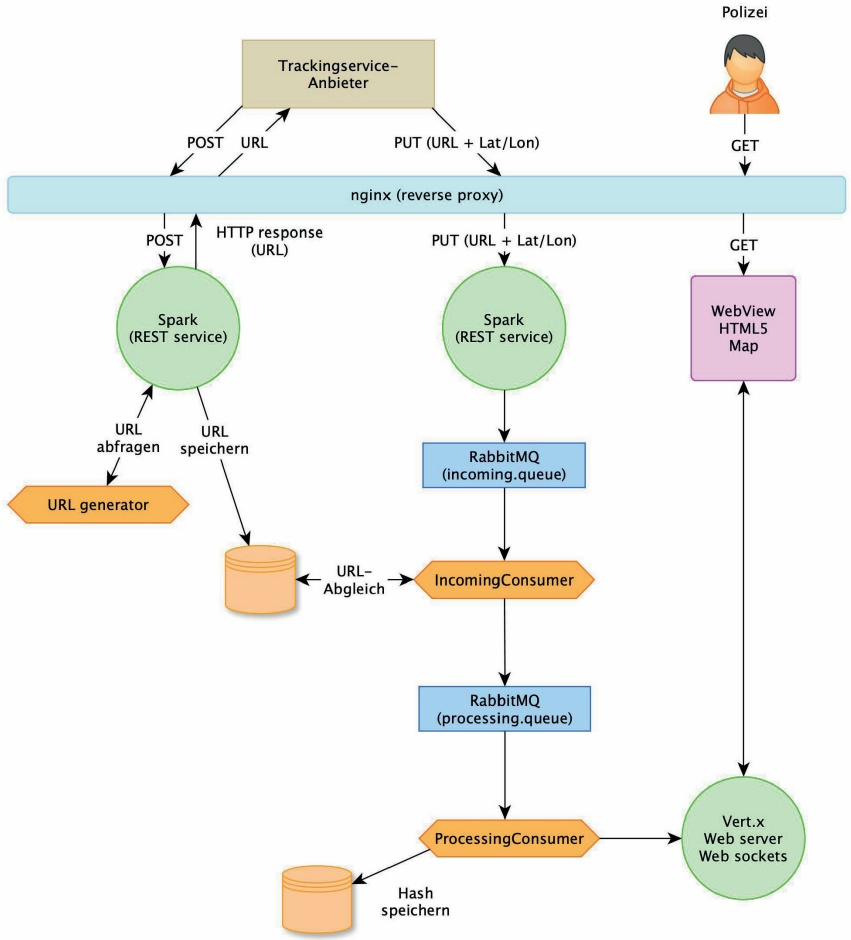


*Abbildung 3: Die Zusammenarbeit der verschiedenen Komponenten des FindMyBike-Systems (Grafik: Alexander Vollmar)*

Durch das Konzept der Microservice-Architektur ist eine unabhängige Programmierung der verschiedenen Komponenten möglich gewesen. Darüber hi-

naus unterstützt dieser Architekturstil eine agile Entwicklung und ermöglicht insbesondere eine einfache Wartbarkeit eines Systems (und somit die unabhängige Änderbarkeit, Erweiterbarkeit und Ersetzbarkeit der einzelnen Microservices[6]). So kann das Gesamtsystem leicht horizontal skaliert werden, indem die Services auf verschiedene Hostsysteme verteilt und ausgeführt werden. Hierdurch bleibt das System flexibel und es ist sichergestellt, dass es auch bei einer umfangreicheren Nutzung durch eine Vielzahl von Trackingservice-Anbietern, bei einer großen Anzahl an gestohlenen Fahrrädern bzw. bei sehr häufigem Abrufen der Fahrradpositionen performant einsetzbar ist.

Die Kommunikation mit dem *FindMyBike-System* von außen verläuft über einen nginx[7]-Webserver, der als Reverse Proxy fungiert, die HTTP-Requests verarbeitet und diese Anfragen an die verschiedenen Services weiterleitet. Das Web-Application-Framework Spark[8] wird eingesetzt um verschiedene REST[9]-Schnittstellen zur Verfügung zu stellen.

Ein erster Service stellt URLs für die anfragenden Trackingservice-Anbieter bereit. Hierbei wird eine Anfrage nach einer URL zuerst vom Webserver an einen Spark-Service weitergeleitet. Daraufhin erzeugt ein in Kotlin realisierter URL-Generator eine URL und liefert sie an den Spark-Service zurück, der diese wiederum an den Trackingservice-Anbieter weitergibt und zusätzlich in einer dokumentbasierten Datenbank (MongoDB[10]) abspeichert.

Ein weiterer Service dient der Entgegennahme der Positionsdaten. Hierbei beginnt der Trackingservice-Anbieter unmittelbar nach dem oben beschriebenen Empfangen der URL mit der Übertragung der Positionsdaten. Die Positionsnachrichten werden wiederum vom Webserver entgegengenommen und dem Spark-Service übergeben. Dieser Service reicht die Live-Positionsdaten kontinuierlich in eine mit der Message Broker-Software RabbitMQ[11] realisierte Warteschlange weiter, welche die Nachrichten asynchron für die Verarbeitung einem weiteren Kotlin-Programm, dem "incoming consumer" aushändigt. Dieser Consumer gleicht die jeweilige URL mit der Datenbank ab und reicht (falls die URL gültig ist) die Nachricht an eine weitere RabbitMQ-Queue weiter. Von dort wird die Positionsnachricht einem weiteren Consumer ("processing consumer") übergeben, der daraufhin aus der Nachricht einen Hashwert berechnet und diesen in einer weiteren MongoDB-Datenbank speichert. Daneben werden

6 Dowalil 2018, S. 4.
7 nginx unter https://nginx.org
8 http://sparkjava.com
9 REST: Representational State Transfer; ein Programmierparadigma für verteilte Systeme, das häufig für Webservices eingesetzt wird.
10 https://www.mongodb.com
11 https://www.rabbitmq.com

die Positionsdaten aus dieser Message-Queue vom WebServer-Service zum Browser der bzw. des Nutzenden gesendet. Die Übertragung der verschlüsselten Live-Positionsdaten erfolgt dabei über das WebSocket-Protokoll, welches es ermöglicht aktuelle Fahrradpositionen vom Server zum Client zu senden, ohne dass ein kontinuierliches Aktualisieren der Webanwendung durch die Nutzenden erforderlich wäre.

## *2.3 Sicherheit*

### *2.3.1 Verschlüsselung der Datenübertragung*

Zur Verschlüsselung der Datenübertragung zwischen dem Trackingservice-Anbieter, dem *FindMyBike-System* und der Polizei wird das Verschlüsselungsprotokoll "Transport Layer Security" (TLS) eingesetzt. Hierbei wird die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene TLS-Version 1.2. genutzt. Für die TLS-Version 1.3, die seit dem 21.03.2018 als "proposed standard"[12] gilt, enthalten die Technischen Richtlinien bisher noch keine Einschätzung.[13]

Den Aufbau einer gesicherten Datenverbindung im TLS-Protokoll wird mit Hilfe einer Cipher-Suite, einer standardisierten Sammlung der zu verwendenden kryptographischen Algorithmen für Schlüsseleinigung (und gegebenenfalls auch für die Authentisierung), für die Verschlüsselung der Live-Positionsdaten sowie eine Hashfunktion für die Integritätssicherung der Datenpakete durchgeführt. Das *FindMyBike-System* verwendet eine Cipher-Suite mit Perfect Forward Secrecy (mit der "eine Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden kann"[14]) und zwar die Cipher-Suite TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. Diese Cipher-Suite ist, wie alle durch das BSI in den Technischen Richtlinien aufgeführten Cipher-Suites,[15] für den Aufbau von gesicherten Datenverbindungen geeignet, wobei der empfohlene Verwendungszeitraum bis über das Jahr 2024 hinaus reicht.

### *2.3.2 IP-Adress-Bereich*

Die URLs mit denen die entsprechenden Kartenansichten des FindMyBike-Systems zur Darstellung derPosition eines gestohlenen Fahrrades aufgerufen werden können, bestehen jeweils im letzten Segment aus einem 64-stelligen

12 Internet Engineering Task Force 2018.
13 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 5.
14 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 7.
15 Bundesamt für Sicherheit in der Informationstechnik 2018, S. 6 ff.

Hexadezimal-String. Eine solche URL ist nur äußerst schwer zu erraten. (Es sind hierbei insgesamt $2^{256} \approx 10^{77}$ verschiedene URLs möglich.) Um einen unberechtigten Zugriff auf die Positionsdaten darüber hinaus auszuschließen, soll die Kartenansicht weiterhin nur aus dem Rechnernetz der Polizei aufrufbar sein. Hierzu wird in der Konfiguration des nginx-Webservers die Möglichkeit des Aufrufs auf Adressen aus dem IP-Bereich der Polizei begrenzt.

## 3. Die Schnittstellen

Das *FindMyBike-System* benötigt verschiedene Datenschnittstellen für die Kommunikation mit den Trackingservice-Anbietern auf der einen Seite und der Polizei auf der anderen Seite. Diese müssen für das Funktionieren des Gesamtsystems von den verschiedenen Kommunikationspartnern implementiert bzw. genutzt werden. Nachfolgend werden diese Schnittstellen als Vorschlag für eine mögliche Standardisierung des Datenaustauschs ausführlicher beschrieben. Allen Schnittstellen ist gemein, dass der Grundsatz der Datenminimierung beachtet wird, d.h. es werden nur solche Daten übertragen, die für den Betrieb des Systems und die Ermittlungsarbeit der Polizei auch wirklich notwendig sind. Auf eine Speicherung von personenbezogenen Daten durch das *FindMyBike-System* kann dabei vollständig verzichtet werden.

### *3.1 Übertragung von Tracking-Daten an das FindMyBike-System*

Um Positionsdaten übertragen zu können, muss der jeweilige Trackingservice-Anbieter über eine erste Schnittstelle eine fallbezogene URL beim *FindMyBike-System* abfragen. Über eine zweite Schnittstelle sendet der Anbieter nahezu in Echtzeit Nachrichten mit den jeweils aktuellen Positionsdaten des gestohlenen Fahrrads an das *FindMyBike-System*.

#### *3.1.1 Schnittstelle zur Abfrage einer URL durch einen Trackingservice-Anbieter beim FindMyBike-System*

Für die eindeutige Zuordnung der Anzeige über die Internet-Wache zu den zugehörigen Positionsmeldungen wird eine ID benötigt. Als ID wird eine URL genutzt, die über eine REST-Schnittstelle beim *FindMyBike-System* abgefragt wird. Für das Durchführen dieser Abfrage wird die HTTP-Methode POST

genutzt. Diese Methode wird hierbei eingesetzt, da sie für nicht idempotente[16] Anfragen, bei denen eine neue Ressource unterhalb der jeweils angegebenen Ressource erstellt wird, verwendet werden soll[17].

Der Abruf einer URL könnte z.B. mit curl[18], einem Programm zum Übertragen von Dateien in Rechnernetzen, wie folgt durchgeführt werden:

```
curl·-X·POST·-k·https://ip029248.beuth-hochschule.de/bike
```

Der Server liefert als Antwort (im Body der HTTP response) eine in ein JSON[19]-Format gekapselte URL. Diese URL muss beim Erstatten einer Anzeige über die Internet-Wache der Polizei in das hierfür vorgesehene Feld eingegeben werden. Nachfolgend ist ein Beispiel für den response body der Antwort des Servers (mit dem zugehörigen HTTP-Statuscode 201, "created") aufgeführt:

```
{
··"url":··"https://[findmybikeserver.de]/bike/77DEED7EE6D42DAB96F0764096CBD0FBA
E4AEFDDFA121FE480F75D9B85851554"
}
```

Die vom *FindMyBike-System* generierte URL setzt sich wie folgt zusammen:

```
https://[findmybikeserver.de]/bike/[ID]
```

Das letzte Segment der URL (oben mit [ID] bezeichnet) besteht aus einem beliebigen 64-stelligen Hexadezimalstring. Falls bei einer Fehlfunktion des Systems die Ausgabe einer URL durch den Spark-Webservice nicht möglich sein sollte, wird eine Antwort mit einem leeren response body und dem HTTP-Statuscode 503 ("service unavailable") zurückgegeben.

Die URL wird zusammen mit dem zugehörigen Zeitstempel (dem Erstellungszeitpunkt der URL) durch das *FindMyBike-System* abgespeichert. Mit Hilfe dieses Zeitstempels kann später ermittelt werden, ob mittels der jeweiligen URL das Abrufen von Positionsdaten zu einem späteren Zeitpunkt noch möglich ist. Hierzu wird im *FindMyBike-System* gemäß rechtlicher Vorgaben eine maximale Gültigkeit für die URLs hinterlegt. Nach Ablauf dieser Frist

16 Idempotenz: Das mehrmalige Ausführen einer Anfrage führt zum gleichen Ergebnis wie eine einzige Ausführung. Die angegebene Methode ist nicht idempotent, d.h. jedes Ausführen führt zu einem neuen Ergebnis, hier dem Generieren einer neuen URL.

17 Richardson/Amundsen/Ruby 2013, S. 37.

18 https://curl.haxx.se

19 JavaScript Object Notation, siehe http://json.org

wird das Abrufen von Positionsdaten für das entsprechende Fahrrad durch das System verweigert.

### *3.1.2 Schnittstelle zum Versand von Positions-Nachrichten an das FindMyBike-System*

Trackingservice-Anbieter, die das *FindMyBike-System* nutzen wollen, müssen Live-Positionsdaten von gestohlenen Fahrrädern mittels Push-Nachrichten an das *FindMyBike-System* übermitteln (auch hier wiederum über die REST-Schnittstelle).

Der Versand der Live-Positionsdaten muss dabei kontinuierlich erfolgen, d.h. es wird, sobald vom Trackingservice-Anbieter eine neue Positionsmeldung des GPS-Trackers eines betroffenen Fahrrads empfangen wurde, eine entsprechende Nachricht mit der letzten Positions-Meldung an das *FindMyBike-System* gesendet. Die Positionsnachrichten umfassen lediglich die folgenden Felder:

*Tabelle 1: Positionsnachricht*

| Feld-Bezeichnung | Beschreibung |
|---|---|
| *location* | JSON-Objekt mit zwei Feldern für die geographische Länge (*longitude*) und Breite (*latitude*) der Position des Fahrrads |
| *timestamp* | Der Zeitpunkt, auf den sich die Positionsmeldung bezieht (Unixzeit) |
| *Accuracy* | Genauigkeit des GPS-Geräts (in Metern)[20] |

Als Format für die Positionsmeldungen wird wiederum JSON eingesetzt. Nachfolgend ist eine Beispiel-Nachricht dargestellt:

```
{
··"location":·{
····"longitude":·13.351520729064941,
····"latitude":·52.539655456542969
},
··"timestamp":·1531927644,
··"accuracy":·14
}
```

20 Die Genauigkeit eines GPS-Trackers beschreibt den Radius in dem sich das Gerät mit einer bestimmten Wahrscheinlichkeit befindet. Diese Wahrscheinlichkeit ist nicht normiert und kann bei verschiedenen Geräten unterschiedlich sein.

Positionsnachrichten mit der oben aufgeführten Struktur können mittels der HTTP-Methode PUT an die REST-Schnittstelle des *FindMyBike-Systems*, d.h. an die oben abgerufene URL (siehe 3.1.1), gesendet werden:

Die Methode PUT wird im REST-Architekturstil zum Anlegen von Ressourcen verwendet und ist idempotent. Wird eine identische Nachricht also mehrmals an den Server gesendet, so wird sie nur beim ersten Mal verarbeitet und sie hinterlässt den Server im jeweils selben Zustand.

Nach dem Empfangen einer Positionsnachricht durch den Trackingservice-Anbieter, wird dem *FindMyBike-System* somit eine neue Nachricht mittels der PUT-Methode übermittelt und damit eine neue Ressource mit den jeweiligen Positionsdaten erstellt. Das System berechnet mittels einer kryptographischen Hashfunktion (aus der SHA-2-Familie, SHA-512/256[21]) aus der Positionsnachricht einen Hashwert. Dieser Hashwert, eine ID (das letzte Segment der URL) sowie der entsprechende Zeitstempel werden in einer Datenbank abgelegt. Die eigentlichen Positionsdaten werden also aus datenschutzrechtlichen Gründen nicht in der Datenbank abgespeichert. Mit Hilfe des Hashwerts kann bei einem erneuten Abrufen der Positionsdaten überprüft werden, ob die zugehörigen Daten beim Anbieter verändert wurden.

Beispiel für das Versenden einer Push-Nachricht an das *FindMyBike-System* mit curl:

```
curl·-H·'Content-Type: ·application/json'·-X ·PUT·-d·'{·"location":·{·"longitude":
·13.351520729064941, ·"latitude":·52.539655456542969·},·"timestamp":·1531927644,
·"accuracy":·14}'·-k https:// [findmybikeserver.de]/bike/77DEED7EE6D42DAB96F07
64096CBD0FBAE4AEFDDFA121FE480F75D9B85851554
```

Der Server liefert, falls er die Nachricht entgegennehmen kann, eine HTTP-Antwort mit einem “ok” im response body und dem HTTP-Statuscode 202 (“accepted”). Falls die Positions-Meldung nicht entgegengenommen werden kann, wird als Antwort ein leerer response body und der HTTP-Statuscode 503 (“service unavailable”) zurückgegeben.

### *3.2 Darstellung der Positionsdaten auf einer Karte*

Mit Hilfe der erstellten URL kann die Polizei auf die jeweils aktuelle Position eines gestohlenen Fahrrades zugreifen. Diese Position wird auf einer Web-View visualisiert (siehe Abbildung 4). Wenn neue Positionsdaten des Fahrrades vor-

21 Siehe hierzu Gueron/Johnson/Walker 2010; eine genaue Beschreibung der Hashfunktionen nach dem SHA-Standard findet sich in *National Institute of Standards and Technology* (2015); Informationen zur Berechnung eines SHA-512/256-Hashs ebenda S. 26.

liegen, wird die Anzeige der Position in dieser Kartenansicht automatisch aktualisiert (also jeweils nachdem eine neue, aktuelle Meldung verarbeitet wurde).

Beim Öffnen der Kartenansicht wird, soweit sich die entsprechende Information im Arbeitsspeicher des FindMyBike-Servers befindet, die letzte Position, die dem System bekannt ist, auf der Karte dargestellt. Diese Information wird allerdings nicht dauerhaft durch das System gespeichert und geht z.B. nach einem Neustart des Servers verloren. Wenn seit dem Start des *FindMyBike-Systems* keine neuen Positionsdaten übermittelt wurden, kann solange kein Position visualisiert werden, bis eine erste Positionsmeldung empfangen wurde. Falls sich das Fahrrad z.B. in einem abgeschirmten Raum befindet, kann eine solche Meldung damit auch ganz ausbleiben.

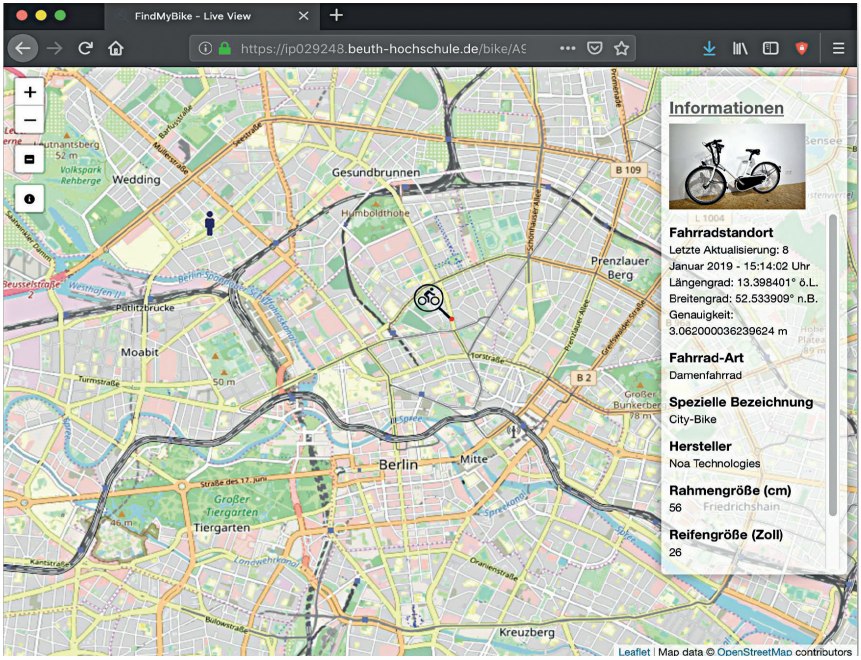


*Abbildung 4: Screenshot der FindMyBike-Anwendung: Karteansicht mit Symbolen für das gestohlene Fahrrad und die Position des jeweilig genutzten Gerätes*

Der Abruf der Karte kann mittels eines gewöhnlichen Web-Browsers durch Eingabe der URL erfolgen. (Es wird hierbei also die HTTP-Methode GET verwendet.) Auf der Karte kann zusätzlich zur Position des jeweiligen Fahrrades auch die Position des entsprechenden Tablets oder sonstigen mobilen Endgeräts (und somit auch der Standpunkt der Person, welche das *FindMyBike-System* gerade einsetzt) dargestellt werden. Die Kartenansicht wird auf Grundlage von OpenStreetMap[22] bereitgestellt. Die HTML5-basierte Webanwendung verwendet die Bibliothek Leaflet[23] um die Web Map Tiles ("Karten-Kacheln") von OpenStreetMap anzuzeigen.

### *3.3 Schnittstelle zum rückwirkenden Abruf von Positionsdaten durch die Polizei beim Trackingservice-Anbieter – vermittelt durch das FindMyBike-System*

Neben der oben dargestellten Möglichkeit des Empfangens von Positionsdaten nahezu in Echtzeit kann die Polizei, wenn die Positionsdaten für die Beweisführung vor Gericht benötigt werden, rückwirkend beim Trackingservice-Anbieter anfragen (siehe Abbildung 5).

22 https://www.openstreetmap.org
23 https://leafletjs.com

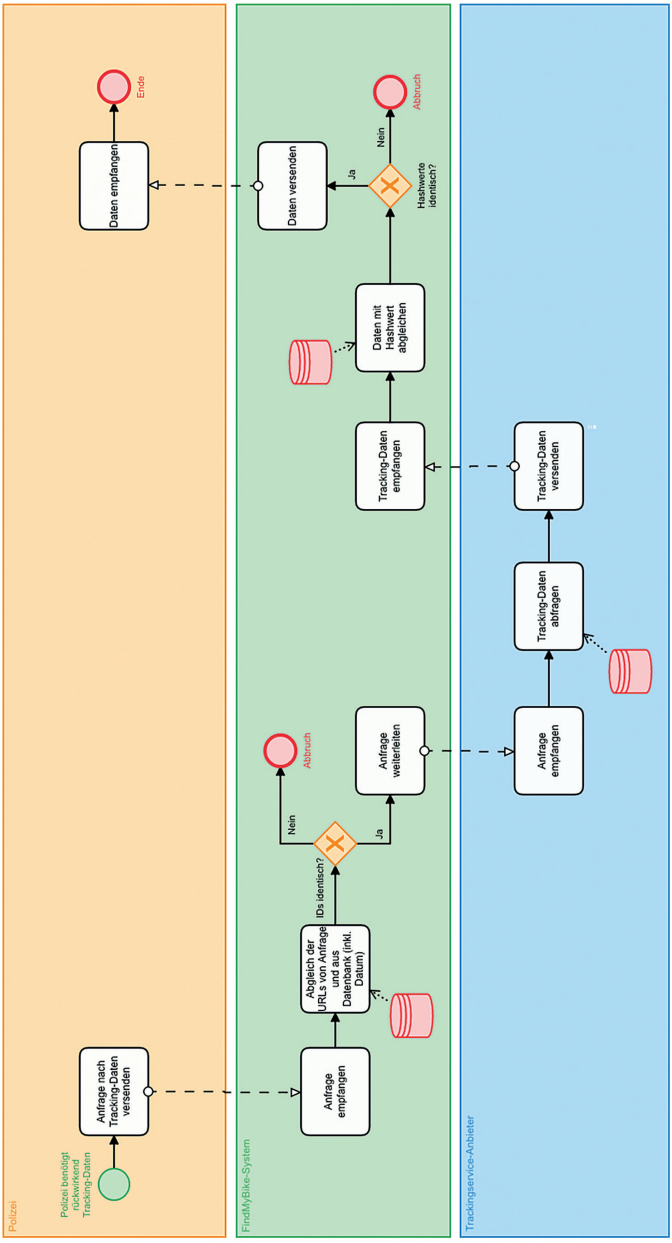


*Abbildung 5: FindMyBike-System: Rückwirkender Abruf von Positionsdaten durch die Polizei (Grafik: Alexander Vollmar)*

Die Live-Positionsdaten werden durch das *FindMyBike-System* mit den zwischengespeicherten Hashwerten abgeglichen und bei Übereinstimmung in standardisierter Form an die Polizei weitergereicht. Die Abfrage ist frühestens ab dem Zeitpunkt der Erstellung der URL möglich.

Für diesen rückwirkenden Abruf wird eine Nachricht (Aufbau siehe Tabelle 2), welche die URL und den Zeitpunkt, ab dem die Freigabe besteht, beinhaltet, von der Polizei an das *FindMyBike-System* gesendet. Das *FindMyBike-System* gleicht die URL mit der Datenbank ab und leitet, falls diese in der Datenbank vorhanden ist, die Anfrage an den Trackingservice-Anbieter weiter. Der Provider versendet hierauf alle Nachrichten (siehe Tabelle 3) mit den zu dem Fahrrad vorhandenen Positionsdaten – ab dem entsprechenden, angegebenen Zeitpunkt.

*Tabelle 2: Anfrage an den Trackingservice-Anbieter*

| **Feld-Bezeichnung** | **Beschreibung** |
|---|---|
| *url* | wurde beim FindMyBike-System abgefragt (siehe 3.1.1) |
| *timestamp* | Zeitpunkt ab dem die Positionsdaten abgerufen werden sollen |

*Tabelle 3: Beispiel für eine erneut gesendete Positionsmeldung (vom Trackingservice-Anbieter an das FindMyBike-System)*

| **Feld-Bezeichnung** | **Beschreibung** |
|---|---|
| *location* | JSON-Objekt mit zwei Feldern für die geographische Länge (*longitude*) und Breite (*latitude*) der Position des Fahrrads |
| *timestamp* | Der Zeitpunkt, auf den sich die Positionsmeldung bezieht (Unixzeit) |
| *accuracy* | Genauigkeit des GPS-Geräts (in Metern) |

Die Positionsmeldungen, die erneut gesendet werden, müssen identisch zu den unter 3.1.2 versandten Nachrichten sein. Aus diesen nochmals versendeten Positionsnachrichten werden durch das *FindMyBike-System* wiederum Hashwerte berechnet und mit den entsprechenden, in der Datenbank abgespeicherten Hashwerten abgeglichen. Mit Hilfe der Hashwerte kann gezeigt werden, dass die Positionsdaten zwischen der ersten und der erneuten Übertragung nicht verändert wurden, d.h. die Gleichheit der Datensätze kann somit nachgewiesen

werden[24]. Bei Übereinstimmung der Hashwerte werden alle Positionsnachrichten in einem Arbeitsgang, z.B. als zip-Archiv, an die Polizei weitergeleitet.

### *3.4 Schnittstelle für die Beendigung der Datenübertragung*

Die Übertragung von Positionsdaten vom Trackingservice-Anbieter über das *FindMyBike-System* an die Polizei kann auf verschiedenen Wegen beendet werden (siehe auch Abbildung 2). Zum einen sollte der Serviceanbieter die Übertragung der Live-Positionsdaten automatisch nach einer vorgegebenen Zeit beenden. Diese Zeit sollte aus den rechtlichen Vorgaben abgeleitet werden und prinzipiell verhindern, dass Daten über eine rechtlich abgesicherte Zeitspanne hinaus an die Polizei übertragen werden können. Zum anderen sollte auch die bestohlene Person die Übertragung abbrechen können. Ein einfacher Weg dies zu realisieren ist das Integrieren eines Schalters in die App des jeweiligen Providers, über welchen die Datenübertragung direkt abgebrochen werden kann, z.B. nach dem Auffinden des Fahrrads. Diese beiden Abbruchmöglichkeiten müssen bei Nutzung des FindMyBike-Systems durch den entsprechenden Anbieter implementiert werden.

Weiterhin wird in die Web-View zur Darstellung der Positionsdaten eines gestohlenen Fahrrads bei der Polizei ein Schalter integriert, über den der Wunsch zum Abbruch der Datenübertragung an das *FindMyBike-System* gemeldet und von diesem an den jeweiligen Anbieter weitergeleitet wird. Hiermit wird die Polizei in die Lage versetzt zu jedem beliebigen Zeitpunkt den Prozess abbrechen zu können, z.B. wenn ein Fahrrad wieder aufgefunden oder eine Anzeige zurückgezogen wurde und somit die rechtliche Grundlage für die Datenübertragung nicht mehr besteht.

## 4. Ausblick

Für den zukünftigen Einsatz des *FindMyBike-Systems* durch die Polizei wäre es über die oben beschriebenen Anpassungen vorteilhaft, wenn die Fahrrad-Diebstahlsanzeige direkt aus der Fahrradpass-App[25] der "Polizeilichen Kriminalprävention der Länder und des Bundes"[26] (oder einer ähnlichen Anwendung)

24 *Heinson* (2015), S. 146ff.

25 Informationen zur Fahrradpass-App finden sich unter https://www.polizei-beratung.de/themen-und-tipps/diebstahl-und-einbruch/diebstahl-von-zweiraedern/fahrradpass-app

26 Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes ist ein Verbund zwischen den Polizeien der Bundesländer, der Bundespolizei, des Bundeskriminalamts und der Deutschen Hochschule der Polizei. Siehe hierzu https://www.polizei-beratung.de

erstattet werden könnte. Diese App sollte zu diesem Zweck so erweitert werden, dass sie alle für eine Anzeige benötigten Daten zum Fahrrad (inklusive Fotos) und seinem*seiner Besitzer*in bereitstellen kann. Hierzu müsste der oben beschriebene Ablauf der Datenverarbeitung des Gesamt-Systems jedoch verändert werden, da die Anzeige direkt in der Fahrradpass-App erstellt werden sollte. Weiterhin könnte die App die für die Anzeige benötigte URL direkt beim *FindMyBike-System* abrufen und an den Trackingservice-Anbieter übermitteln. Die Nutzung der Internet-Wache für die Erstellung der Anzeige könnte damit vollständig entfallen. In einem weiteren Schritt sollte die Fahrradpass-App für die Nutzung durch die verschiedenen Polizeibehörden aller Bundesländer angepasst werden, so dass die Anzeige durch die App (dem Ort des Diebstahls entsprechend) an die zuständige Polizeistelle im jeweiligen Bundesland weitergeleitet wird.

## Literatur

Bundesamt für Sicherheit in der Informationstechnik (2018) Technische Richtlinie TR-02102–2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen Teil 2 – Verwendung von Transport Layer Security (TLS), (Version 2018–01). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=6, zuletzt besucht am 20.02.2019.

Dowalil, Herbert (2018) Grundlagen des modularen Softwareentwurfs – Der Bau langlebiger Mikro- und Makro-Architekturen wie Microservices und SOA 2.0. München: Carl Hanser Verlag.

Gueron, Shay.; Johnson, Simon; Walker, Jesse (2010) SHA-512/256. International Association for Cryptologic Research. https://eprint.iacr.org/2010/548.pdf; zuletzt besucht am 20.02.2019.

Heinson, Dennis (2015) IT-Forensik. Veröffentlichungen zum Verfahrensrecht 199. Tübingen: Mohr Siebeck.

Internet Engineering Task Force (2018) Protocol Action: 'The Transport Layer Security (TLS) Protocol Version 1.3' to Proposed Standard. https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html, zuletzt besucht am 20.02.2019.

National Institute of Standards and Technology – Information Technology Laboratory (2015) Secure Hash Standard (SHS). Federal Information Processing Standards, FIPS PUB 180–4. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS. 180-4.pdf, zuletzt besucht am 20.02.2019.

Richardson, Leonard; Amundsen, Mike; Ruby, Sam (2013) RESTful Web APIs – Services for a Changing World. Sebastopol CA.: O'Reilly Media.

*Hanno Brandt[1]/Alexander Vollmar[2]/Gudrun Görlitz[3]*

# Erkenntnisse aus den Feldversuchen des FindMyBike-Systems

## 1. Einführung

Neben der logisch korrekten Arbeitsweise und dem Zusammenspiel aller Softwarekomponenten, spielt die Gebrauchstauglichkeit (engl. Usability) bei der Nutzerakzeptanz eine wesentliche Rolle. Unter Gebrauchstauglichkeit von Software versteht man das Ausmaß, in dem eine Software für bestimmte Benutzerinnen und Benutzer „in einem bestimmten Nutzungskontext genutzt werden kann, um bestimmte Ziele effektiv, effizient und zufriedenstellend zu erreichen".[4] Um die Gebrauchstauglichkeit von Software zu beurteilen, sind Nutzerevaluationen eine geeignete Methode. Dabei nehmen potenzielle Anwenderinnen und Anwender an Tests teil, in denen die Software im Arbeitskontext eingesetzt wird. Zur Erfassung und Auswertung der Ergebnisse aus den Evaluationen können verschiedene Verfahren genutzt werden:

- Beobachtung der Proband*innen während der Softwarenutzung
- Ausfüllen von Evaluationsfragebögen durch die Proband*innen nach dem Testende persönlich oder online
- Interviews mit den Proband*innen nach dem Testende

Da Beobachtungen und Interviews zeitaufwändige, schwierig zu standardisierende Verfahren sind, haben sich Evaluationen mittels Fragebögen breit etabliert. Die Fragebögen können statistisch ausgewertet und die Ergebnisse visualisiert werden.

1 Hanno Brandt war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die rechtlichen 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. DIN EN ISO 9241-11:2018-11,2018, S. 6

## 2. Zielstellung der Evaluation des FindMyBike-Systems

Das Ziel bestand darin, das im Rahmen des IFAF geförderten *FindMyBike-Projekts* entwickelte Softwaresystem im polizeilichen Einsatz zum Wiederauffinden entwendeter Fahrräder zu testen. Das *FindMyBike-System* zeigt in der Benutzeroberfläche eine Kartenansicht, in der die Position eines gestohlenen Fahrrads angezeigt wird.[5] Getestet werden sollte dabei zum einen, inwieweit die Arbeitsabläufe eine Unterstützung durch das *FindMyBike-System* erfahren und wo Optimierungen der Anwendung, der Arbeitsabläufe und des Zusammenspiels von Anwendung und Abläufen erfolgen können. Dafür wurde ein besonderes Augenmerk auf die Handhabung der Kartenansicht des *FindMyBike-Systems* durch Polizeikräfte gelegt. Zum anderen sollte die Schnittstelle des *FindMyBike-Systems*, über die Standortdaten von gestohlenen Fahrrädern von Trackingservice-Anbietern*innen an das *FindMyBike-System* gelangen, gründlich getestet werden.

## 3. Versuchsplanung

Die IFAF-Projektförderung der Hochschulen bot den Rahmen für gründliche Großfeldversuche, die im Kontext von Lehrveranstaltungen an der Hochschule für Wirtschaft und Recht und der Polizeiakademie Berlin mit Polizeistudierenden des gehobenen Diensts im Wintersemester 2018/2019 geplant wurden. Die Lehrveranstaltungen ermöglichten die Einweisungen der Studierenden in die Tests und Auswertungen in Gruppengesprächen. Das kooperierende Fahrradflottenunternehmen Noa stellte für die Testtage mit GPS-Trackern ausgestattete Fahrräder zur Verfügung.

Für die Feldversuche wurden verschiedenartige Fahrraddiebstahlszenarien entworfen. Es gab Szenarien, in denen die Fahrräder abgestellt waren (z. B. an der Hauswand, im Hinterhof). In anderen Szenarien wurde das „entwendete" Fahrrad bewegt (z. B. auf dem Fahrrad fahrend, das Fahrrad schiebend, das Fahrrad in einem Transporter oder der S-Bahn bewegend).

Der Arbeitsprozess des Fahrraddiebstahls bei der Polizei Berlin wurde in den Feldversuchen in folgenden Teilprozessen[6] betrachtet:

5 Bei Vollmar/Görlitz/Kober, in diesem Band, S. 227ff, wird das FindMyBike-System aus IT-Sicht erläutert.

6 Der Workflow beim Fahrraddiebstahl bei der Polizei Berlin wird bei Matzdorf/Brandt/Noeske, in diesem Band, S. 105ff ausführlich dargelegt.

1. Diebstahlmeldung des Geschädigten über das Online-Formular bei der Internetwache
2. Bearbeitung der Diebstahlanzeige in der Einsatzleitzentrale der Polizei Berlin
3. Tätigkeit der Einsatzleitung zum Auffinden gestohlener Fahrräder
4. Tätigkeiten verschiedener Polizeikräfte (Funkwagenbesatzungen, Zivilstreife, Fahrradstaffel, Fußstreife) beim Suchen und Auffinden gestohlener Fahrräder

Das *FindMyBike-System* sollte schwerpunktmäßig beim 4. Punkt getestet werden. Die Polizist*innen wurden dafür mit Tablets ausgestattet. In einem Szenario wurden die suchenden Polizeikräfte von der Einsatzleitung (siehe 3. Punkt) geführt. In diesem Fall wurde die Software in der Einsatzleitung im Zusammenspiel mit der Ortsdatenübermittlung an die suchenden Polizeikräfte getestet.

Die Arbeitsprozesse unter 1. und 2. sind die normalen Arbeitsabläufe bei der Polizei Berlin. Die Arbeitsprozesse unter 3. und 4. wurden für die Feldversuche simuliert, da die Tests auf die Lehrveranstaltungszeit von vier Stunden und die Diebstähle auf einen Abschnitt bei der Polizei Berlin begrenzt wurden. Die Proband*innen waren Polizei-Studierende, die in den Rollen als Geschädigte, Dieb*innen, Einsatzleitzentrale, Einsatzleitung und suchende Kräfte gemäß den Szenarien agierten. In einem Szenario übernahmen zusätzlich erfahrenere Polizeikräfte die Rolle der suchenden Kräfte. Dabei kannten die Proband*innen nur die Bedingungen für ihre eigene Rolle und nicht das gesamte Diebstahlszenario.

Das aktuelle Online-Formular für Fahrraddiebstähle der Internetwache der Polizei Berlin beinhaltet keine Möglichkeit der Freigabe von Trackingdaten seitens der Geschädigten. Für die Großfeldversuche wurde deshalb vereinbart, im Formularfeld „Besondere Merkmale am Fahrrad“ die den Geschädigten vorgegebene, zum Fahrrad gehörige URL einzutragen.

Es war notwendig, die zum Großfeldversuch gehörenden Diebstahlanzeigen aus den während der Versuchszeit bei der Polizei Berlin eingehenden Diebstahlmeldungen herauszufiltern und den Einsatz an die von den Studierenden der Polizeiakademie organisierte Einsatzzentrale weiterzuleiten. Dazu wurde abgestimmt, dass die Geschädigten zur Markierung der Anzeigen für die Großfeldtest Codewörter in der Online-Anzeige einzutragen hatten. Ein E-Mail-Konto wurde für die Tests eingerichtet, an das seitens der Einsatzleitzentrale der Polizei eine PDF-Datei mit der Diebstahlanzeige gesandt wurde. Die Studierenden der Einsatzleitung hatten Zugriff auf dieses E-Mail-Konto.

## 4. Versuchsdurchführung

Insgesamt wurden drei Großfeldversuche durchgeführt. Diese waren im Aufbau ähnlich, unterschieden sich aber in einzelnen Punkten, insbesondere den Versuchsorten, den Versuchspersonen und den eingesetzten technischen Mitteln.

Die Versuchsanordnung stellte zeitlich gegebenenfalls zusammenfallende, aber unabhängig voneinander vorgenommene, (simulierte) Fahrraddiebstähle und die darauffolgenden Reaktionen der Betroffenen und der von diesen Personen informierten Polizei dar. Die Dieb*innen entwendeten die Fahrräder in von der Versuchsleitung vorgegebenen Parametern.

Für die Feldversuche wurden die folgenden, behelfsmäßigen[7] Vorgehensweisen festgelegt: Die Betroffenen waren angewiesen, als Reaktion auf eine Entwendung (zu einem vorgegebenen Zeitpunkt) die Polizei zu kontaktieren, indem sie eine der Form nach echte Online-Anzeige[8] bzgl. der Entwendung „ihres" Fahrrads aufgaben, dabei aber in dem Formularfeld „Besondere Merkmale am Fahrrad" die URL zum Start des *FindMyBike-Systems* eintrugen und die Anzeige durch bestimmte Angaben als dem aktuellen Test zugehörig markierten[9]. Die echte Einsatzleitzentrale der Polizei Berlin hatte die Aufgabe, im Rahmen ihres Echtbetriebs alle markierten Anzeigen als PDF-Dateien an ein vorgegebenes E-Mail-Postfach weiterzuleiten. Über dieses E-Mail-Postfach konnte die Einsatzleitung des Feldversuchs auf die Anzeigen zugreifen und mit Hilfe der jeweils übermittelten URL das *FindMyBike-System* zur Visualisierung der aktuellen Position des entsprechenden Fahrrads starten. Aufgabe der Einsatzleitung war es, einen Zugriff auf das Fahrrad zu ermöglichen. Sie war dazu gegenüber den suchenden Kräften weisungsbefugt und sollte diesen, soweit eine Ausstattung mit Tablets gegeben war, auch die URL zum Starten des *FindMyBike-Systems* zuschicken. Die suchenden Kräfte sollten, den Anweisungen und Hinweisen der Einsatzleitung entsprechend, die als gestohlen gemeldeten Fahrräder suchen und sicherstellen.

Da beim Projektpartner Noa Technologies (dem Trackingservice-Anbieter) notwendige Systemumstellungen bis zu den Feldversuchen nicht zu realisieren waren, mussten die Positionsnachrichten bei diesem abgeholt und an das *Find-*

7 Behelfsmäßig insofern, als dass für die Versuche keine Anpassungen der polizeilichen IT-Systeme, beispielsweise des Formulars der Internetanzeige oder des elektronischen Informationsflusses nach Übermittlung der URL, vorgenommen wurden.

8 Die Anzeigen wurden über die Internetwache der Polizei Berlin (erreichbar unter https://www.internetwache-polizei-berlin.de) erstellt.

9 Die Anzeigen wurden markiert, indem die Anzeigenden als eigenen Namen „FindMyBike, Testeinsatz …" angaben und in das Formularfeld „Besondere Merkmale am Fahrrad" zudem „Test" schrieben.

*MyBike-System* weitergegeben werden. Die Positionsdaten wurden also entgegen der eigentlichen Konzeption nicht direkt vom Trackingservice-Anbieter als Push-Nachrichten an das FindMyBike-System weitergegeben, sondern durch einen Webservice, der zwischen diese beiden Systeme gesetzt wurde, abgeholt. Dieser Service fragte die Tracking-Daten beim Trackingservice-Anbieter aktiv ab (in kurzen Intervallen – alle zehn Sekunden) und gab sie anschließend an die Schnittstelle des *FindMyBike-Systems* weiter. Das *FindMyBike-System* wurde zu diesem Zweck also nicht extra angepasst, es wurde lediglich eine weitere Anwendung vor das System gesetzt. Diese zwischengeschaltete Anwendung verhielt sich gegenüber dem *FindMyBike-System* also wie ein Trackingservice-Anbieter. Weiterhin wurde die URL-Generierung insofern simuliert, als dass die Betroffenen die Generierung der URL nicht selbst veranlassten, sondern eine im Vorfeld erstellte URL nutzten.

Die verschiedenen Rollen (Geschädigte, Dieb*innen, suchende Kräfte und Einsatzleitung) wurden von Versuchspersonen übernommen. Die Versuchspersonen waren beim ersten Feldversuch Polizeistudent*innen des gehobenen Diensts der Hochschule für Wirtschaft und Recht Berlin. Bei den in Kooperation mit der Polizeiakademie Berlin durchgeführten zweiten und dritten Versuchen kamen Polizeistudent*innen des gehobenen Diensts aus dem fünften Semester hinzu, die bereits eine mehrjährige Praxiserfahrung als Beamt*innen des mittleren Dienstes hatten. Beim letzten Versuch wurden zudem Einheiten aus der Fahrradstaffel der Polizei Berlin einbezogen. In der echten Einsatzleitzentrale waren die Beamt*innen jeweils mit der Weiterleitung der markierten Anzeigen betraut.

Die Feldversuche erfolgten mit insgesamt 13 von Noa Technologies mit GPS-Trackern ausgestatteten Fahrrädern. Knapp die Hälfte dieser Fahrräder sendete die Positionsdaten im Zehn-Sekunden-Takt, die anderen hatten eine Minutentaktung. Für die fernmündliche Kommunikation wurden Mobiltelefone, sowie beim zweiten und dritten Feldversuch das Funksystem der Polizei Berlin genutzt. Beim ersten Versuch agierten die simulierten Polizeikräfte zu Fuß, beim zweiten wurden zudem Funkwagen und ein Gruppenwagen, beim letzten Versuch Funkwagen und eine Fahrradstreife eingesetzt. Die suchenden Kräfte[10] waren beim ersten und zweiten Versuch teilweise, beim letzten Versuch vollständig mit Tabletcomputern der Polizei Berlin[11] ausgestattet.

Die Feldversuche dauerten jeweils drei bis vier Stunden. Pro Versuch wurden neun bis zwölf Vorgänge simuliert. Versuchsgebiet war bei dem ersten Versuch der Campus Lichtenberg der Hochschule für Wirtschaft und Recht Berlin,

10 So die Bezeichnung für die mobilen Einheiten.

11 Die eingesetzten Tablets waren vom Typ *Samsung Galaxy Tab Active 2* und *Samsung Galaxy Tab S3*.

bei den weiteren Versuchen das Gebiet des Polizeiabschnitts 15 (welches den westlichen Teil des Ortsteils Prenzlauer Berg, des Bezirks Pankow von Berlin umfasst).

Bei der Evaluation der Feldversuche wurden qualitative und quantitative Methoden eingesetzt. Hierbei wurden sowohl Versuchsbeobachtungen, teilweise ergänzt durch kurze Interviews im Anschluss an die Versuche, als auch Befragungen mit Hilfe von Fragebögen durchgeführt. Außerdem standen die Protokolle der Einsatzleitung zur Verfügung.

## 5. Erkenntnisse

In diesem Abschnitt werden die unterschiedlichen Erkenntnisse aus den verschiedenen Feldversuchen zusammenfassend dargestellt. Hierbei werden auch die Resultate der Evaluation mit Fragebögen sowie Auswertungen aus den Funkprotokollen der Einsatzleitung aufgeführt.

Soweit möglich werden dabei die Ergebnisse der drei Feldversuche zusammengeführt. Neben der Möglichkeit von Freitexteingaben waren die Fragen in den Evaluationsbögen mehrheitlich durch Ankreuzen eines von jeweils fünf Kästchen zu beantworten, wobei das erste mit „trifft nicht zu“ und das letzte mit „trifft voll zu“ beschriftet war. Die Ergebnisse wurden mit Werten von „1“ (trifft nicht zu) bis „5“ (trifft voll zu) kodiert, d.h. der mittlere Wert entspricht einer „3“. Die unten aufgeführten Durchschnittswerte beziehen sich jeweils auf insgesamt 24 ausgewertete Fragebögen.

### *5.1 Funktionsfähigkeit*

Während der Feldversuche wurde die im Projekt FindMyBike prototypisch erstellte Software, insbesondere die Schnittstelle zur Übertragung von Positionsdaten durch Trackingservice-Provider an das *FindMyBike-System* und die Kartenansicht ausgiebig genutzt. Alle getesteten Software-Module funktionierten planmäßig und arbeiteten stabil. Es wurden keine größeren Probleme oder Fehler festgestellt. Pro Versuch wurden ca. 2.000 bis 3.000 Datenbankeinträge und somit auch Standortmeldungen erzeugt und für die Darstellung im *FindMyBike-System* störungsfrei verarbeitet. Die Menge der zu verarbeitenden Nachrichten stellte in keiner Weise und zu keinem Zeitpunkt für das entwickelte System ein Problem dar.

Die Anwendung wurde von den Versuchsteilnehmer*innen als stabil eingestuft (Bewertungen im Mittel 4,0 auf der oben beschriebenen Skala – und dies obwohl bei einem Versuch ein Polizeiserver, über den der Datenverkehr lief, zeitweise ausfiel, was zu negativeren Bewertungen führte). Das Nachladen

der Kartendaten über das Mobilfunknetz wurde nur als mittelmäßig schnell bewertet (im Durchschnitt mit 3,0 auf der Skala von 1 bis 5).

Für den zweiten und dritten Feldversuch lagen die Funkprotokolle der Einsatzleitung vor. Anhand dieser kann eine zeitliche Beurteilung der Fahrradsuche mit dem *FindMyBike-System* erfolgen. In beiden Feldversuchen wurden jeweils neun Fahrräder aus zwölf Diebstahlszenarien gefunden. Das entsprich einer Aufklärungsquote von 75%. Im dritten Feldversuch, in dem die Studierenden mit der Handhabung des *FindMyBike-Systems* am besten vertraut waren, lagen die Auffindungszeiten der Fahrräder zwischen neun und vierzig Minuten. Nach durchschnittlich 19,6 Minuten wurde ein Fahrrad aufgefunden.

### *5.2 Bedienbarkeit*

Die Versuchspersonen konnten die Benutzeroberfläche sicher navigieren. Die Bedienung der Anwendung wurde von fast allen Teilnehmenden als sehr einfach bewertet. Die meisten Personen gaben an, dass für die Bedienung keine zusätzlichen Erklärungen benötigt werden. Auch der Umgang mit den Tablets wurde von den Versuchspersonen als einfach eingeschätzt. Die Teilnehmenden hatten zum Versuchszeitpunkt noch keine Erfahrungen mit den bis dahin noch nicht flächendeckend in Berlin eingeführten Polizei-Tablets gemacht. Der dennoch sichere Umgang mit den Geräten könnte allerdings auf den Umstand zurückzuführen sein, dass es sich um junge Versuchspersonen handelte, die mit der Bedienung mobiler Geräte wie Smartphones vertraut sind.

### *5.3 Starten der Anwendung*

Da die polizeilichen IT-Systeme für die Feldversuche nicht speziell angepasst wurden, ergaben sich Schwierigkeiten beim Öffnen des *FindMyBike-Systems*. Hierzu musste die übermittelte URL von Hand aus der PDF-Datei mit der Anzeige in den Browser kopiert und Umbrüche entfernt werden. Nachdem das Problem erkannt war, behinderte dies die Polizeikräfte jedoch kaum. Dieser Umstand würde allerdings vor einem möglichen Roll-Out des Systems in jedem Falle behoben werden.

### *5.4 Beschränkung auf Anzeige des letzten Standorts*

Da aufgrund von rechtlichen Beschränkungen[12] nicht die gesamte vom Fahrrad zurückgelegte Route sondern nur die jeweils letzte Position einschließlich des

12 Siehe ausführlich zu den datenschutzrechtlichen Anforderungen an das *FindMyBike-System* Fährmann/Vollmar/Görlitz, in diesem Band, S. 211ff.

zugehörigen Zeitstempels auf der Kartenansicht des *FindMyBike-Systems* angezeigt werden durfte, war es fraglich, ob die Versuchspersonen Fahrräder in Bewegung für einen Zugriff ausreichend genau orten könnten. Bei Fahrrädern mit höherer Taktung (Übermittlung der Positionsdaten alle zehn Sekunden) ergaben sich hierbei keine größeren Probleme. Versuchspersonen mit besserer Ortskenntnis und Erfahrung war es bei solchen Fahrrädern möglich, Schlussfolgerungen auf die zukünftige Route der verfolgten Person zu ziehen und ihr den Weg abzuschneiden. Bei Fahrrädern mit langsamer Taktung (60 Sekunden) gab es Berichte über Schwierigkeiten bei der Verfolgung sich bewegender Fahrräder.

Die Beschränkung der Anzeige auf den letzten, zeitlich markierten Standort erwies sich insgesamt also nicht als limitierender Faktor.

### *5.5 Die Kartenansicht der FindMyBike-Anwendung*

Das verwendete Kartenmaterial von OpenStreetMap[13] wurde von den Versuchspersonen durchweg als gut eingeschätzt. So wurde die Karte z.B. als „sehr detailliert", „genau" und „übersichtlich" beurteilt. Es wurde lediglich bemängelt, dass die Hausnummern der Gebäude erst bei stärkerem Hinein-Zoomen in die Karte angezeigt werden.

Die Anzeige des jeweils eigenen Standorts der suchenden Person (bzw. des entsprechenden Mobilgerätes) auf der Karte ermöglicht es, den eigenen Standort in Relation zu dem des gesuchten Fahrrads zu setzen. Diese Standortanzeige wurde als sehr sinnvoll bewertet (im Durchschnitt über die drei Versuche mit 4,4 auf der oben eingeführten Skala). Zum Teil funktionierte bei Selbststeuerung der suchenden Kräfte die Anzeige des eigenen Standorts auf der Karte jedoch nicht zuverlässig. Eine entsprechende Funktion wurde in der Anwendung implementiert, die Aktualisierung der Position konnte aufgrund der jeweiligen Gerätekonfiguration allerdings nicht immer erfolgen.

Neben der Visualisierung der letzten Standortmeldung des Fahrrads auf der Karte wurden die zusätzlichen Angaben zum Fahrrad (Foto des Fahrrads, Fahrradtyp, Hersteller, Rahmengröße, Reifengröße, Gangschaltung) von den Versuchsteilnehmer*innen als besonders hilfreich empfunden (4,5 auf der Skala von 1 bis 5). Die suchenden Kräfte und die Einsatzleitung orientierten sich häufig an diesen Angaben. Das dargestellte Foto des gestohlenen Fahrrades ermöglichte eine effizientere und effektivere Suche. Wäre auch die Rahmennummer dargestellt worden, hätte sich nach einem Zugriff auch auf diesem Weg die Identität des Fahrrads verifizieren lassen. (Die entsprechende Rahmennummer konnte allerdings der Anzeige entnommen werden.) Eine Darstellung von mög-

13 Siehe https://www.openstreetmap.org

lichst umfassenden Informationen über das jeweilige Fahrrad, zumindest aber der Rahmennummer und eines Fotos, ist also sehr sinnvoll.

Die Teilnehmenden fanden, dass Fahrräder mit Hilfe des *FindMyBike-Systems* eher einfach aufzufinden sind (Mittelwert: 3,8) und dass eine solche Anwendung in der Praxis besonders hilfreich wäre (4,5 auf der oben genannten Skala).

### *5.6 Die Übermittlung der URL an die Polizei*

Bei der Übermittlung der URL zum Start des *FindMyBike-Systems* durch die Betroffenen an die Einsatzleitung traten an zwei Punkten Schwierigkeiten auf. Die erste Schwierigkeit resultiert daraus, dass das Online-Formular in seiner jetzigen Form kein eigenes Feld für die Übertragung von Informationen für den Zugriff auf einen Trackingservice vorsieht. Obwohl die Betroffenen um die Bedeutung der URL wussten und schriftlich sowie mündlich angewiesen wurden, diese URL in das Feld „Besondere Merkmale am Fahrrad“ einzutragen, übergingen sie diesen Schritt wiederholt. Sie wussten, dass sie zunächst die URL ihres Fahrrads über eine ihnen mitgeteilte Website abrufen und diese dann in das eben bezeichnete Feld kopieren mussten. Ihnen war auch klar, dass erst über diese URL die Suche nach Ihrem Fahrrad starten könnte. Trotzdem waren in einigen Anzeigen die URLs nicht aufgeführt. In einem Fall hat ein Betroffener die Angabe sogar versäumt, obwohl er unmittelbar zuvor von der Versuchsleitung auf genau diesen Fehler in seiner vorherigen Anzeige hingewiesen wurde. Auch vor dem Hintergrund von entsprechenden Aussagen der Betroffenen kann davon ausgegangen werden, dass der Grund für die fehlende Angabe nicht an einem fehlenden Verständnis der Betroffenen lag. Als Erklärung für das auffällige Versäumnis mehrerer Betroffener lässt sich vielmehr das Fehlen eines dafür vorhergesehenen Feldes für die URL in der Online-Anzeige angeben. Dieses wird dadurch verständlich, dass in dem Online-Formular der Internetwache der Polizei Berlin eine große Anzahl von Feldern auszufüllen ist und vor jedem Feld eine sehr spezifische Frage steht. Daher ist es für die Betroffenen naheliegend, auch jeweils nur die konkret gestellte Frage zu beantworten. Eine Anpassung des Online-Formulars wäre insofern unbedingt ratsam.

Die zweite Problematik lag in der Weiterleitung der Anzeigen von der echten Einsatzleitzentrale zu der in den Versuchen simulierten Einsatzleitung. Beim ersten Feldversuch gelang die Weiterleitung der Anzeigen an die zuvor bei der Einsatzleitzentrale hinterlegte E-Mail-Adresse noch problemlos. Bei den weiteren Versuchen kam es jedoch dazu, dass markierte, dem Versuch zugehörige Anzeigen nicht an die simulierte Einsatzleitung weitergeleitet wurden, sondern zu einem echten Vorgang erklärt und dem zuständigen Abschnitt zu-

geleitet wurden. Dass die Vorfälle sich besonders zum Zeitpunkt von Schichtwechseln ereigneten, spricht dafür, dass eine bessere Einweisung und eine längere Gewöhnungszeit dieser Fehlerquelle entgegenwirken könnten. Allerdings ist zu bedenken, dass dieses Problem der besonderen Versuchskonstellation geschuldet war und in dieser Form bei einem Echtbetrieb des *FindMyBike-Systems* nicht zu erwarten ist.

### *5.7 Genauigkeit und Zuverlässigkeit der Positionsdaten*

Die Positionsdaten waren für Situationen unter freiem Himmel hinreichend genau. Wenn sich die Fahrräder innerhalb von U-Bahnen oder KFZ befanden, wurden nur vereinzelt Positionsdaten empfangen, so dass hier das Auffinden kaum gelang. Somit wurde auch die Genauigkeit der Positionsbestimmung abhängig von den jeweiligen Bedingungen am Auffindungsort sehr unterschiedlich eingeschätzt (von deutlich weniger als zehn Meter bei guten Bedingungen und von 30 bis 100 Meter bei Fahrrädern in Bewegung, in Hinterhöfen und unter Dächern oder Brücken).

Wenn sich der gesuchte Gegenstand in einem mehrstöckigen Gebäude befindet, stößt das System an seine Grenzen, da die verwendeten GPS-Tracker keine Höhenangaben übermittelten und innerhalb von Gebäuden auch nur sehr beschränkt (z.B. in der Nähe eines Fensters) GPS-Satellitensignale zum Ermitteln des Standorts empfangen werden können.

## 6. Schlussfolgerungen und Ausblick

Die Funktionalität und Belastbarkeit des *FindMyBike-Systems* wurden in den Großfeldversuchen eindrucksvoll bestätigt. Auch wenn berücksichtigt wird, dass die Diebstahlszenarien auf einen beschränkten örtlichen Bereich eingegrenzt waren, kann aus der hohen Auffindungsquote und den geringen Auffindungszeiten (siehe 5.1) geschlussfolgert werden, dass polizeiliche Arbeitsabläufe zum Festnehmen von Tatverdächtigen und Sicherstellen von entwendeten Fahrrädern mit GPS-Trackern durch das *FindMyBike-System* eine Unterstützung erfahren können. Aufgrund der zeitlichen Limitierung wurden die Versuche auf das Auffinden der Fahrräder beschränkt, so dass taktische Maßnahmen mit dem Fokus auf dem Ergreifen von Tatverdächtigen nicht im Vordergrund standen. Die Versuche haben jedoch keine Gründe aufgezeigt, die einer entsprechenden Schwerpunktverschiebung entgegenstehen würden. Besonders hervorzuheben ist, dass die Ausgestaltung des *FindMyBike-Systems* gemäß den rechtlichen Anforderungen, wonach die Polizei nur den jeweils letzten Standort

eines Fahrrads sieht, sich als praktikabel erwiesen hat. Die gewählte Anwenderoberfläche erwies sich als gut bedienbar.

Für die Freigabe der Trackingdaten durch die Geschädigten, z. B. durch die Übermittlung der FindMyBike-URL an die Polizei, lässt sich festhalten, dass der bereits existierende Weg über die Internet-Wache grundsätzlich gangbar ist, aber in jedem Falle einer Anpassung des entsprechenden Web-Formulars bedarf.

Im Ausblick lassen sich einige Punkte benennen, an denen eine Weiterentwicklung des Systems oder seiner Anknüpfungspunkte bei der Polizei sinnvoll erscheint. An der grundsätzlichen Ausgestaltung der Anwenderoberfläche kann festgehalten werden. Allerdings ließe sich die Polizeiarbeit mit dem *FindMyBike-System* auch bei Beibehaltung der Beschränkung auf die Anzeige des letzten Standorts durch kleinere Ergänzungen möglicherweise effektuieren. Beispielsweise stellt sich die Frage, ob es nicht möglich und sinnvoll wäre, zusätzlich zu den bereits dargestellten Informationen anzuzeigen, wie schnell das Fahrrad zum letzten bekannten Standort gekommen sein muss. In einem weiteren Schritt wäre ein automatischer Hinweis für den Fall möglich, dass sich der Sender so schnell bewegt, dass von einem Transport des Fahrrads in einem Fahrzeug ausgegangen werden muss. Rechtlich sollte dies kein Problem sein. Es müsste hierbei nur bedacht werden, dass der Wegverlauf zwischen den beiden Punkten nicht mitberücksichtigt wird. So mag ein Transporter zwar schnell durch die Straßen einer Stadt fahren, in der Luftlinie, die alleine ja berechenbar ist, mag die Geschwindigkeit aber dennoch gering erscheinen. Diese Ungenauigkeit wäre bei häufigerem Senden der aktuellen Position durch den Tracker von geringem Ausmaß.

Hilfestellungen wären wohl auch für den Fall sinnvoll, dass vom GPS-Tracker keine aktuellen Daten mehr gesendet werden. Denkbar wäre zunächst eine farbliche Markierung, die anzeigt, wie neu die letzte Standortangabe ist (z.B. von Grün zu Rot). Eventuell ließen sich auch die wahrscheinlichsten Gründe für die Sendepause anzeigen (Statische Lage, Abschirmung, Akkulaufzeit, Defekt).

Die Großfeldversuche wurden mit verschiedenen Szenarien durchgeführt. In weiteren Tests sollte ermittelt werden, ob das *FindMyBike-System* für spezifische Diebstahlsfälle besonders geeignet ist. Ebenso sind die Fälle, in denen die Fahrräder nicht gefunden wurden, detaillierter zu untersuchen, um gegebenenfalls Abgrenzungen zu den Leistungsparametern oder programmtechnische Erweiterungen des *FindMyBike-Systems* vorzunehmen.

Die Polizeiarbeit ist in Deutschland auf Bundesländerebene organisiert. Das *FindMyBike-System* arbeitet bundesländerübergreifend und länderübergreifend. Da insbesondere bei bandenmäßigem Fahrraddiebstahl davon auszugehen ist, dass die gestohlenen Fahrräder über weite Strecken transportiert werden, ist

das *FindMyBike-System* für den Einsatz bei länderübergreifenden Fahndungen geeignet.

Das *FindMyBike-System* wurde für die Visualisierung von Fahrrad-Ortungsdaten optimiert. Grundsätzlich kann die Anwendung auf die GPS- Ortung anderer Gegenstände angepasst werden, die von der Polizei aufgefunden werden sollen.

## Literatur

DIN EN ISO 9241-11:2018-11, Ergonomie der Mensch-System-Interaktion - Teil 11: Gebrauchstauglichkeit: Begriffe und Konzepte (ISO 9241-11:2018)

*Christian Matzdorf*[1]

# Perspektiven für ein Roll-out des FindMyBike-Systems in der Polizeipraxis

## 1. Hintergrund der Systementwicklung

Das FindMyBike-System stellt eine Entwicklung des vom Institut für angewandte Forschung Berlin (IFAF-Berlin) geförderten „FindMyBike-Projekt - Rechtliche und technische Konzepte für die Übertragung von zeitbasierten Geodaten zur Aufklärung von Fahrraddiebstählen“ dar. Dieses Projekt wurde von der Hochschule für Wirtschaft und Recht Berlin und der ehemaligen Beuth Hochschule für Technik Berlin als Forschungspartnern und dem Landeskriminalamt Berlin sowie dem Unternehmen Noa Technologies GmbH getragen. Dem Sitz der Projektbeteiligten entsprechend fiel bei der Entwicklung der Blick zunächst auf das Bundesland Berlin. Wie dem Projektnamen zu entnehmen ist, stand während des Forschungsprozesses das Fahrrad als Diebstahlsobjekt im Mittelpunkt. Es wurden jedoch stets globale Bezüge mitbedacht, geografisch und inhaltlich sowie mit Rücksicht auf die Vielfältigkeit der Voraussetzungen und Anforderungen in verschiedenen Anwendungsgebieten, und für das System ein modularer Aufbau gewählt. Ein solcher lässt Anpassungen und Fortentwicklungen zu. Vor diesem Hintergrund ist sowohl die Verortung der Projektbeteiligten als auch die Bezeichnung „FindMyBike-System“ zu verstehen: Das System ist weder auf ein bestimmtes Bundesland noch auf die Anwendung ausschließlich für die Verfolgung von Fahrraddiebstählen beschränkt.

Dieser Beitrag beleuchtet Perspektiven für ein Roll-out des Systems in die Polizeipraxis. Ziel des Projektes durfte nicht sein, ein unmittelbar gebrauchsfertiges Produkt zu entwickeln. Das ließen die IFAF-Regularien vor dem Hintergrund, dass öffentlich geförderte Forschungsprojekte nicht in Konkurrenz zu privaten Anbietern treten dürfen, nicht zu. Doch die im Projekt entwickelten und in Feldversuchen getesteten Konzepte entstanden mit der Intention, für die Praxis sinnvoll anwendbar und damit auch privatwirtschaftlich umsetzbar zu sein.

Die Projektpartner waren von der Überzeugung getragen, dass eine Übernahme der Erkenntnisse des FindMyBike-Projekts einen Mehrwert für die

1 Prof. Christian Matzdorf hat in dem Projekt kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

Polizeipraxis sowie für Bürger*innen erbringen kann. Eine so oder ähnlich formulierte Frage galt es zu beantworten:

„Warum nutzt die Polizei nicht die durch einen eingebauten GPS-Sender generierten Standortinformationen einer abhandengekommenen Sache (wie mein Fahrrad oder andere Gegenstände von für mich bedeutendem Wert) um mein Eigentum zu sichern und Täter*innen zu stellen?“

Die Beantwortung dieser Frage würde im mutmaßlichen Sinne des Betroffenen stehen. Damit verbunden hätte die Polizei rechtssichere und (informations-)technisch einfache Möglichkeiten, einen technisch basierten und bisher kaum existenten Ermittlungsansatz zu nutzen. Das System wurde mit Blick auf Fahrräder entwickelt, da hier aufgrund der geringen Aufklärungsquote und der hohen Fallzahlen zusätzliche Ermittlungsansätze besonders sinnvoll erschienen. Aber auch bei anderen Gegenständen ist es nicht vermittelbar, warum die Polizei vorhandene und rechtlich zulässige Wege zur Straftatenaufklärung nicht nutzt oder aus rechtlichen oder technischen Gründen nicht nutzen kann. Es bietet sich eine Möglichkeit, auf der Grundlage bestehenden Rechts eingriffsarm auf dem Gebiet der fallzahlenintensiven Alltagskriminalität Bedürfnissen der Bürger*innen zu begegnen. Diesbezüglich wird die amtierende Berliner Polizeipräsidentin Dr. Barbara Slowik zitiert, die feststellt, dass „der Bürger von Bedrohungen des Extremismus […] in den seltensten Fällen direkt betroffen [ist…]. Viel wichtiger ist für ihn […] der Fahrraddiebstahl.“[2]

## 2. Voraussetzungen eines Roll-outs

Die notwendigen Voraussetzungen für ein Roll-out des Systems müssen in vier großen Bereichen gegeben sein: beim Betreiber des Systems, an den (technischen) Schnittstellen zur Polizei, in der polizeiinternen IT-Organisation sowie bei der Software-Anpassung auf Seiten der Polizei.

Der erste dieser Bereiche lässt sich nur indirekt seitens der Polizei beeinflussen und bedarf daher privater Kooperation und/oder politischer Unterstützung. Wesentlich für das FindMyBike-System ist nämlich, dass ein zentraler Bestandteil weder bei der Polizei noch bei den jeweiligen Tracking-Service-Anbietern oder seitens privater Fahrradeigentümer betrieben wird. Das FindMyBike-System im engeren Sinne sollte seitens einer weiteren, unabhängigen

2 Interview mit der Zeit vom 19.12.2018, https://www.zeit.de/gesellschaft/zeitgeschehen/2018-12/barbara-slowik-polizeipraesidentin-berlin-sicherheit-organisierte-kriminalitaet?utm_referrer=https%3A%2F%2Fwww.google.com%2F (letzter Aufruf: 13.04.2021).

Stelle, sozusagen einer FindMyBike-System-Betreibergesellschaft,[3] unterhalten werden. Dieser Systembetreiber muss das Softwaresystem hosten und für eine zentrale Koordination sorgen. Über ihn fließen die Daten an die Polizei und bei ihm werden Maßnahmen getroffen, um Daten für das gerichtliche Verfahren verwertbar zu machen; der Systembetreiber selbst, nicht die Polizei, steht im Kontakt zu allen beteiligten Tracking-Service-Anbietern und -Nutzern. Zwischen ihm und den anderen Beteiligten muss es zivilrechtliche Absprachen und datenschutzrechtliche Regelungen geben. Möglich wäre eine Gestaltung, nach der dieser mit den verschiedenen Tracking-Service-Anbietern Verträge abschließt und datenschutzrechtliche Abreden trifft.[4] Die Herausforderung besteht hierbei darin, eine (juristische) Person zu finden bzw. zu gründen, die bereit ist, das System zu betreiben, weil sie in dem Betrieb ein tragfähiges Geschäftsmodell sieht oder aus sonstigen Gründen, beispielsweise als Interessenvertretung von betroffenen Personengruppen, diese zentrale Aufgabe übernehmen würde.

Schnittstellen müssen zwischen dem FindMyBike-Systembetreiber, den Tracking-Service-Anbietern und den jeweiligen polizeilichen Organisationseinheiten geschaffen werden sowie, je nach Gestaltung, auch direkt zwischen den Betroffenen und der jeweils zuständigen Polizeibehörde. Die notwendigen Schnittstellen zwischen dem FindMyBike-Systembetreiber und den jeweiligen Tracking-Service-Anbietern sollen hier nicht näher beleuchtet werden. Es ist jedoch davon auszugehen, dass ein FindMyBike-Systembetreiber eine standardisierte Schnittstelle entwickeln wird, weil dies ihm die Möglichkeit geben würde, allen interessierten Tracking-Service-Anbietern kostengünstig die Nutzung zu ermöglichen. Auch die Schnittstellen zwischen der Polizei und dem FindMyBike-Systembetreiber brauchen lediglich zur Vollständigkeit erwähnt zu werden, da hier zwischen dem Systembetreiber und den beteiligten Polizeidienststellen auch individuelle Absprachen bzw. Absprachen auf der Ebene der jeweiligen Bundesländer denkbar sind. Diese könnten den Besonderheiten der jeweiligen polizeilichen IT-Systeme Rechnung tragen.

Regelungsbedarf besteht hingegen in Bezug auf die Schnittstelle zwischen der oder dem Betroffenen und den Polizeidienststellen. Die Bearbeitung durch die Polizei beginnt mit einer Anzeige durch das Diebstahlsopfer, weiterer Personen oder durch eigene Wahrnehmung im Rahmen der Bewältigung polizeilicher Aufgaben. Im Rahmen der Anzeigenaufnahme erhebt die Polizei verschiedene Daten, die dann verarbeitet und gespeichert werden: persönliche Geschädigtendaten, Angaben zum Diebesgut (Beschreibung und Wert), Tatzeit

3 Auch hier sei noch einmal darauf hingewiesen, dass der Name „FindMyBike“ nicht dahingehend missverstanden werden darf, dass das System nur fahrradbezogen anwendbar ist. Dazu unter dem Punkt „Perspektiven“ mehr.

4 Fährmann/Vollmar/Görlitz in diesem Band, S. 177 ff.

und Tatort, mögliche Zeugen und weitere Informationen, die sich am Lebenssachverhalt orientieren. Erhoben werden muss aber auch die individuelle Kennung (es handelt sich hierbei um eine URL), die über das FindMyBike-System den Zugriff auf die aktuellen Positionsdaten gewährleistet. Auf welchem Weg geben Betroffene aber die Informationen an die Polizei weiter und welche Informationen sollen über welchen Weg fließen? Aus Sicht der Polizei wäre der einfachste Weg wohl eine Anzeigeerstattung über das Internet (Internetanzeige über die sogenannte Internetwache). Allerdings bestehen hierbei Schwierigkeiten, wenn Betroffene nach erfolgter Internetanzeige doch noch persönlich auf einer Polizeidienststelle erscheinen und sich gesondert zum dem Sachverhalt äußern müssen. Dies ist insbesondere dann der Fall, wenn die Notwendigkeit besteht, weitere strafprozessuale Maßnahmen einzuleiten (beispielsweise Identitätsfeststellungen verdächtiger Personen, Durchsuchungsmaßnahmen und/oder Sicherstellungen/Beschlagnahmen von Diebesgut). Die Internetanzeige hat aber den Vorteil, dass über sie schnell eine Übermittlung der Daten, insbesondere auch der URL möglich ist. Diese kann aufgrund ihrer Länge nur schwer abgeschrieben oder diktiert werden. Um der hohen Wahrscheinlichkeit eines Übermittlungsfehlers durch das Abschreiben der URL entgegenzuwirken, sollte dies auf elektronischem Weg erfolgen.

Weitere Wege, beispielsweise mit der Generierung eines QR-Codes durch Applikationen der Tracking-Service-Anbieter auf Mobilgeräten der Betroffenen, die durch Polizist*innen ausgelesen werden könnten, sind denkbar, aber bedingen weitere technische Voraussetzungen. Schließlich müsste dafür nicht nur eine Software-Schnittstelle geschaffen, sondern auch entsprechende Hardware angeschafft, distribuiert und unterhalten werden. Dabei ist grundsätzlich zu bedenken, dass in Fällen unaufschiebbarer Maßnahmen (wie der Verfolgung auf frischer Tat) Schnelligkeit von höchster Bedeutung ist.

Aber auch bei einer Nutzung der Internetanzeige bleibt ein großer Gestaltungsspielraum. Theoretisch denkbar ist beispielsweise für die Polizei Berlin, die Onlineanzeige in ihrer jetzigen Form zu nutzen. Die Feldversuche des FindMyBike-Systems haben allerdings ergeben, dass dies unpraktisch wäre und geringfügige Modifikationen vorzusehen sind. So ist beispielsweise die Erstellung spezifischer Felder für die URL unabdingbar.

Die Möglichkeiten gehen aber deutlich darüber hinaus. Es hat sich bei den Feldversuchen unter anderem bestätigt, dass es für die nach einem bestimmten gestohlenen Objekt suchenden Polizeibeamt*innen sehr hilfreich ist, nicht nur den aktuellen Standort des Objekts angezeigt zu bekommen, sondern auch die wesentlichen Informationen, die eine Identifizierung des Objekts ermöglichen oder erleichtern. Dazu zählen standardmäßig bei Fahrrädern bereits abgefragte Informationen wie die Rahmennummer und die Fahrradfarbe, aber insbesondere auch ein Foto des Fahrrads, dass beispielsweise in Berlin bei der Online-

anzeige noch nicht hochgeladen werden kann. Die Polizei könnte allerdings durch entsprechende Erweiterungen alle notwendigen Informationen bei der Onlineanzeige erheben und dann im Polizeisystem mit dem Web-View des FindMyBike-Systems verknüpfen.

Eine weitere Möglichkeit wäre, die entsprechenden Daten beim FindMyBike-Systembetreiber zu erheben und von diesem in den Web-View aufzunehmen. Diese Erhebung könnte schon im Vorfeld geschehen – also zu einer Zeit, bei der der Betroffene das Fahrrad noch in seinem Besitz hat und daher in der Lage ist, korrekte und umfassende Angaben zu machen. Das würde jedoch die nach bisherigem Konzept vermiedene Notwendigkeit eines direkten Kontaktes zwischen dem FindMyBike-Systembetreiber und den Fahrradeigentümer*innen schaffen. Die Erhebung könnte auch indirekt durch den FindMyBike-Systembetreiber vorgenommen werden. Denkbar wäre insofern eine Erhebung durch den Trackinganbieter der oder des Betroffenen mit anschließender Weitergabe an den FindMyBike-Systembetreiber. Vielversprechend wäre schließlich auch die Option, die Fahrradpässe nutzbar zu machen. In diesem sind die relevanten Informationen (außer Fotos, was bei einer Neugestaltung vorzusehen wäre) bereits gespeichert. Es bedürfte daher nur einer Verknüpfung, entweder zur Polizei (im Rahmen der Anzeigeerstattung) oder zum FindMyBike-Systembetreiber (im Vorfeld oder im Rahmen der Abfrage der FindMyBike-URL) oder zum Trackinganbieter (der die Informationen zum FindMyBike-Systembetreiber weiterleiten müsste).

Die polizeiinterne Organisation lässt vielfältige Gestaltungsmöglichkeiten offen. Dies gilt in technischer Hinsicht, hinsichtlich der ablauforganisatorischen Einbindung (die sich beispielsweise in Flächenländern anders gestaltet als in städtischen Ballungsräumen und sich in einer zentralen Steuerung durch eine Einsatzleitzentrale oder dezentral durch kleinere polizeiliche Gliederungseinheiten darstellen kann) und bzgl. der Zielsetzung der Anwendung. Je nach der gewählten Gestaltung wird sich das FindMyBike-System eher als Instrument zur Gefahrenabwehr (Restitution des entwendeten Gegenstandes), als Instrument zur Strafverfolgung oder auch als doppelfunktionales Instrument ohne eigentlichen Schwerpunkt erweisen.

Fraglich ist, ob das Instrument des FindMyBike-Systems von speziellen Einheiten genutzt werden soll, wie sie beispielsweise für den Fahrraddiebstahl vereinzelt schon gegründet wurden. Darauf schließt sich die Frage an, ob es ratsam ist, allen Polizeibeamt*innen den Zugriff auf das FindMyBike-System zu eröffnen und damit als zusätzliches Ermittlungs-Tool zur Verfügung zu stellen. Zu diesen strategischen Fragen können in diesem Projekt keine abschließenden Antworten gegeben werden. Abhängig von der Ressourcenausstattung und vom Behördenaufbau ist je nach Bundesland mit unterschiedlichen Ausgangsbedingungen und Zielrichtungen zu rechnen. Die notwendigen Software-Anpassun-

gen auf Seiten der Polizei variieren ebenfalls erheblich; abhängig von den unterschiedlichen polizeilichen Datenverarbeitungssystemen. Die Feldversuche im Rahmen des FindMyBike-Systems haben gezeigt, dass eine Nutzung sogar ohne Anpassungen denkbar ist. Jedoch wäre das Fehlen von Softwarelösungen durch vermeidbare Mehrarbeit der Polizeikräfte auszugleichen. Sinnvollerweise würden insbesondere Anpassungen des elektronischen Informationsflusses vorgenommen werden, beispielsweise um es den eingesetzten Polizeikräften zu ermöglichen, problemlos auf die in der Internetanzeige angegebenen Informationen und den Web-View gleichzeitig zuzugreifen. Dabei sind auch aktuelle technische Veränderungen wie die Einführung von mobilen Endgeräten für die Kräfte des Basisdienstes (aktuell beispielsweise in der Polizei Berlin in Umsetzung) ebenfalls zu bedenken.

## 3. Umsetzung

Eine wesentliche Variable des Changemanagements ist die Akzeptanz der Veränderung von den betroffenen Dienstkräften. Insofern gilt es, ein ausgewogenes Verhältnis zwischen dem Interesse an einer schnellen Umsetzung und den Interessen der an der Umsetzung Beteiligten zu finden. Daher müssen negative Faktoren minimiert und positive Faktoren herausgestellt werden. So mag es ratsam sein, das Roll-Out des FindMyBike-Systems zunächst auf ausgewählte Einheiten zu beschränken, um in diesem begrenzten Rahmen Strategien zur Minimierung von Friktionen zu entwickeln, auftretende Probleme vor der allgemeinen Einführung zu beheben und Erfolge zu sammeln, die organisationsintern den Nutzen der Veränderung nachvollziehbar machen.

Auch aus langjähriger polizeiinterner Erfahrung des Verfassers heraus, ergibt sich die (naheliegende) Erkenntnis, dass Veränderungsprozesse völlig unabhängig von dem tatsächlichen objektiven Nutzen regelmäßig verzögert werden oder sogar scheitern, wenn keine Akzeptanz bei der vorgesehenen Zielgruppe, den späteren Anwender*innen vorhanden ist. Es wäre falsch, dies ausschließlich mit einem behördlichen Beharrungsvermögen oder einer passiven Ablehnung von (insbesondere technischen) Innovationen zu begründen. Vielmehr spielen hier eine Reihe von Variablen eine Rolle, deren Nichtbeachtung aus behördlicher Leitungssicht in der Vergangenheit für erhebliche Umsetzungsprobleme gesorgt haben. Bezogen auf die Polizei Berlin sind beispielhaft zu erwähnen:

Die Einführung eines neuartigen Behördenorganisationsmodells mit grundsätzlich veränderten Aufgabenzuschnitten[5], die Einführung eines neuen polizeilichen Informationssystems[6] oder die Implementierung der DNA-Spurensuche in den Berufsalltag von kriminal- und schutzpolizeilichen Basisdienstkräften[7].

Auf den konkreten Fall der beschriebenen Anwendung des FindMyBike-Systems (oder einer vergleichbaren Entwicklung) ergeben sich vor dem Hintergrund der beruflichen Erfahrung mit Implementierungsprozessen in Behörden daraus folgende Punkte, die im Rahmen der Vorbereitung und Realisierung berücksichtigt werden sollten (keine abschließende Aufzählung):

- Vorbereitende interne (ggf. auch externe) Öffentlichkeitsarbeit, mit dem Ziel, eine positive Grundstimmung zu erreichen
- Einbeziehung der Mitarbeiter*innen, insbesondere der Zielgruppen, in grundsätzliche Fragen der Realisierung im Vorfeld, auch bezüglich Fragen zur Zeitplanung, organisatorischen Anbindung, Schulungsbedarf u.a.
- Verdeutlichung des Mehrwertes der technisch-organisatorischen Veränderung für die Polizeibehörde aber auch konkret für die Mitarbeiter*innen
- Weitgehender Ausschluss potenziell imageschädigender Ereignisse (Systeminkompatibilität oder sog. Abstürze) durch gründliche Prüfungen im Testlauf
- Ausschluss von empfundener oder tatsächlicher Mehrarbeit durch parallel laufende Systeme (beispielsweise bei der Datenerfassung) oder durch überdimensionierte Kontroll-, Dokumentations- und Evaluationsmaßnahmen
- Direkte (durch Anerkennung und ggf. Zertifizierung der Leistung) oder indirekte (Zugang zunächst nur für leistungsstarke Förderkandidat*innen) Belohnungssysteme für Innovationswilligkeit

---

5 Das sog. „Berliner Modell", 1998 eingeführt und rund 15 Jahre später erheblich reformiert, war getragen von dem Grundgedanken, weniger spezialisierte und daher generalistische Polizeikräfte im Basisdienst der Schutzpolizei einzusetzen (die auch zahlreiche bis dahin originär kriminalpolizeiliche Aufgaben übernehmen sollten); es scheiterte letztlich auch an der grundlegenden Ablehnung in der Mitarbeiterschaft auf Grund der reinen Top-down-Umsetzungsstrategie.

6 POLIKS (Polizeiliches Landessystem zur Information, Kommunikation und Sachbearbeitung) als teilweise Eigenentwicklung der Polizei Berlin, anfangs mit erheblichen technischen Startschwierigkeiten und ständigem Anpassungsbedarf, führte zu gefühlten und realen Belastungen der Arbeitsprozesse und daraus resultierend zu jahrelangen Widerständen in der Mitarbeiterschaft.

7 Die Suche und Sicherung von DNA-haltigem Spurenmaterial mit entsprechenden Wattestäbchen erforderte nach der Einführung einen mehrjährigen erheblichen Überzeugungsaufwand, da der Arbeitsprozess zunächst als aufwändige und nicht gerechtfertigte Zusatzbelastung angesehen wurde.

- Realistische Aussicht, Mitarbeiter*innen mit der Innovation im Berufsalltag erfolgreich zu machen
- Aussicht auf längerfristige Nutzung bzw. Fortschreibung

Die Berücksichtigung der vorgenannten erfahrungsbasierten Punkte kann die Grundlage für eine erfolgreiche Implementierung des Systems in die polizeibehördliche Arbeitsorganisation darstellen. Bezogen auf das Phänomen Fahrraddiebstahl muss, abweichend von anderen Phänomenen der Alltagskriminalität, ein zusätzlicher Aspekt berücksichtigt werden:

Diese Erscheinungsform wurde in den vergangenen Jahrzehnten als nachrangig zu bearbeitender Teil der einfachen Kriminalität behandelt. Daher ist insbesondere im Rahmen der internen Öffentlichkeitsarbeit die Notwendigkeit der Sensibilisierung der Mitarbeiter*innen für die Bedeutung dieses Kriminalitätsphänomens und für den „Wert" der Befassung mit diesem Phänomen zu berücksichtigen.

## 4. Ausblick

Im Rahmen einer umfassenden Betrachtung muss berücksichtigt werden, welche Möglichkeiten der Erweiterungen im Rahmen des FindMyBike-Systems realisiert werden können. An erster Stelle ist die Erweiterung auf andere Gegenstände zu nennen. Fahrräder werden zwar sehr häufig gestohlen und es fehlt bei solchen Taten auch regelmäßig an Ermittlungsansätzen, sodass die Nutzung des FindMyBike-Systems angesichts der zu erwartenden zunehmenden Verbreitung von in Fahrrädern verbauten Ortungsgeräten zu spürbaren Verbesserungen führen könnte. Aber auch alle sonstigen trackinggeeigneten Gegenstände können von dem System erfasst werden. Kraftfahrzeuge, hochwertige Baumaschinen, Transportgüter und Kabelanlagen bieten, wie zahlreiche andere Bereiche auch, weitere Einsatzmöglichkeiten für das System. Daher wäre zu erwägen, nicht mehr vom FindMyBike-System zu sprechen, sondern einen Namen wie „FindMyStuff", „FindMyItem", „FindMyBelonging" oder schlicht „FindMyObjekt" o.ä. zu prägen. Neben dieser inhaltlichen Erweiterung ist eine geografische Ausbreitung zu erwägen, da sich zwar voraussichtlich einige Bundesländer als Vorreiter etablieren werden, aber eine Anknüpfung an ein laufendes und funktionierendes FindMyBike-System in einer Zeit des „Internets der Dinge" auch von den sonstigen Bundesländern erwartet werden kann.

Interessant ist das System für die Polizei auch vor dem Hintergrund, dass bereits jetzt sogenannte „Lockfahrräder" eingesetzt werden, um in dem Feld des Fahrraddiebstahls zu Ermittlungserfolgen zu kommen. Im Falle der Ent-

wendung eines Fahrrads steht für die Betroffenen vielleicht die Rückgewinnung im Vordergrund. Für die Ermittlungsbehörden liegt der Schwerpunkt jedoch auf der Aufklärung von Straftaten, insbesondere anlässlich von Serientaten und der Entwendung von hochwertigen Fahrrädern. Bei weiterer Verbreitung von Tracking-Technologie wird so potenziell ein Großteil der Fahrräder zwar nicht zu „Lockfahrrädern", aber doch zu Gegenständen, die aufgrund des Ortungssystems einen ähnlichen Nutzen wie diese bieten können. Grundsätzlich lässt sich am FindMyBike-System selbst als Entwicklungsperspektive noch die Erweiterung auf andere Ortungsmethoden nennen, da in bestimmten Ermittlungssituationen die Ortung über GPS oder ein vergleichbares GNSS durch weitere Ansätze erfolgreicher sein kann.

Für die Polizei wird bei der Konstruktion der Schnittstellen ein besonderes Augenmerk auf die Sicherheitsanforderungen polizeilicher Datenverarbeitungssysteme zu legen sein. Eine erfolgreiche polizeiliche Einführung ist dann letztlich eine Frage der Akzeptanzförderung sowohl bei Führungskräften als auch bei der Zielgruppe der Polizeiangehörigen im Basisdienst, die entsprechende begleitende Maßnahmen (insbesondere der internen Öffentlichkeitsarbeit) erforderlich machen wird.

Bei Berücksichtigung der in diesem Beitrag skizzierten Aspekte und der regionalen Besonderheiten der jeweiligen Polizeidienststellen vor dem Hintergrund ihrer aufbauorganisatorischen Rahmenbedingungen kann von einer erfolgversprechenden Lösung für heutige und – nicht zuletzt wegen der Modularität des Systems – zukünftige polizeiliche Aufgabenstellungen ausgegangen werden.

Das Roll-Out ist letztlich eine strategische Entscheidung der polizeilichen (bzw. politischen) Führung. Im Entscheidungsfindungsprozess sollte dabei berücksichtigen werden, dass das Potenzial der hier in Rede stehenden Lösungsansätze bisher noch gar nicht abschließend beschrieben ist. Insbesondere die Übertragbarkeit auf verschiedene Bereiche des Sachwertdiebstahls bietet Raum für zukunftsfähige Visionen.

*Jan Fährmann*[1]

# Rechtliche Folgen der standardisierten Positionsdatenübertragung an die Polizeipraxis - Legalitätsprinzip, Strafvereitelung im Amt und Ermessensreduktion

## 1. Einleitung

Durch die im Rahmen des FindMyBike-Projekts entwickelte Software zur Positionsermittlung können Positionsdaten gestohlener Fahrränder direkt an die Polizei übertragen werden, was die Aufklärung von Diebstählen und die Rückgewinnungshilfe erheblich vereinfachen bzw. erst ermöglichen würde. Insofern lag der Schluss nahe, dass ein entsprechendes Forschungsprojekt in der Polizei ausschließlich positiv aufgefasst würde. Gleichwohl äußerten sich im Rahmen des regelmäßigen Austausches mit dem assoziierten Projektpartner LKA Berlin zahlreiche Beamt*innen überaus skeptisch (mehrere Beamt*innen waren gleichwohl an einer entsprechenden Anwendung interessiert). Sie sorgten sich, dass sie aufgrund der Vielzahl von Fahrraddiebstählen kaum in der Lage wären, alle Diebstähle aufzuklären, selbst, wenn ihnen die Positionen gestohlener Fahrräder bekannt wären. Die Beamt*innen warfen mehrfach die Fragen auf, ob sich die bekannten Positionen auf das Risiko einer Begehung der Strafvereitlung im Amt auswirken würde, und, ob sie zu jedem gestohlenen Fahrrad fahren und es den Bestohlenen zurückbringen müssten. Dies sei nahezu unmöglich.

Dieser Gedanke ist aus einer kriminologischen Perspektive nicht fernliegend. Kriminalität ist ein ubiquitäres Phänomen. So begeht beispielsweise ein großer Teil der männlichen Jugendlichen eine oder mehrere Straftaten, meist ohne, dass dies formelle, staatliche Interventionen durch Polizei und Justiz zur Folge hat.[2] Dies ist – wie bei vielen anderen Straftaten auch – auf verschiedene Gründe zurückzuführen; wesentliche Faktoren dürften aber sein, dass der Polizei viele Delikte gar nicht erst bekannt werden bzw. Ermittlungsansätze fehlen.[3]

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

2 Boers 2008, S. 343 f.; Boers 2007, S. 5 m. w. N.

3 Vgl. Kühne 2015, S. 199; Kunz/Singelnstein 2021, S. 239.

So sind z. B. beim Fahrraddiebstahl Ermittlungsansätze oft nicht vorhanden und viele Bestohlene zeigen das Delikt nicht an, weil sie nicht mit der Aufklärung rechnen. Insgesamt ist davon auszugehen, dass so viele Straften begangen werden, dass die Polizei gar nicht in der Lage ist, jede Straftat zu verfolgen.[4] Vielmehr gibt es natürliche Grenzen der Strafverfolgung, die auf begrenzten Ermittlungsmöglichkeiten und endlichen Ressourcen beruhen. Dementsprechend setzen die Strafverfolgungsorgane ihre Ressourcen bewusst selektiv ein.[5] Selbiges gilt erst recht für die polizeiliche Gefahrenabwehr, da die Polizei dementsprechend nicht alle Straftaten und andere gefährliche Verhaltensweisen, die nicht strafbewehrt sind, verhindern kann. Auch bei der Gefahrenabwehr ist also eine Schwerpunktsetzung erforderlich.[6] Schwerpunktsetzungen führen dazu, dass zahlreiche Delikte faktisch nicht aufgeklärt bzw. verhindert werden können, da Schwerpunkte dazu führen können, dass Ressourcen an anderer Stelle fehlen.[7] Aus den Schwerpunktsetzungen erwachsen entsprechende innerbehördliche Strukturen und Arbeitsweisen. Diese Strukturen können aber erschüttert werden, beispielsweise, wenn neue Ermittlungsansätze vorhanden sind, etwa aufgrund neuer Technologien (die auch das Anzeigeverhalten verändern können). Strukturelle Änderungen werden oft skeptisch betrachtet und sind mit Sorgen verbunden, was wir auch im Berliner LKA beobachten konnten.

Im Rahmen dieses Beitrages soll am Beispiel der im FindMyBike-Projekt entwickelten Software analysiert werden, wie sich technische Neuerungen und damit einhergehende zusätzliche Ermittlungsansätze auf die polizeilichen Pflichten auswirken könnten und ob die Sorgen der Beamt*innen gerechtfertigt sind. Dabei wird untersucht, welche Verpflichtungen die Polizei bzw. einzelne Polizist*innen haben, wenn eine solche Software als mobile Anwendung zur Positionsbestimmung beispielsweise auf dem Smartphone oder Tablet bei der Polizei etabliert würde. Wenn die Position eines gestohlenen Fahrrades der Polizei bekannt ist, ist die Polizei dann zur Rückgewinnungshilfe verpflichtet? Muss sie aufgrund des Legalitätsprinzips sämtliche Fahrraddiebstähle aufklären? Und ist ein Unterlassen der Aufklärung sogar strafbar? Diese Fragen können auf andere, durch neue Technologien entstehende Ermittlungsansätze übertragen werden, die aufgrund der Digitalisierung und technischer Entwicklungen in den kommenden Jahren zunehmend vorhanden sein werden.[8]

---

4 Fährmann, CILIP 2021, S. 38; Erb 1999, S. 88 f; Kühne 2015, S. 199; Schmidt-Jortzig, NJW 1989, S. 134 f.

5 Erb 1999, S. 89; Nestler JA 2012, S. 91; Kühne 2015, S. 200-201 m. w. N.; siehe dazu die empirische Untersuchung Feest/Blankenburg 1972, S. 114-119.

6 Kingreen/Poscher 2020, S. 183.

7 Erb 1999, S. 89 m. w. N.

8 Fährmann, MMR 2020, S. 228.

## 2. Rückgewinnungshilfe

Durch die Positionsdaten der gestohlenen Fahrräder ist die Rückgewinnungshilfe durch die Polizei in vielen Fällen möglich. Die Polizist*innen könnten zur angezeigten Position fahren bzw. mit Hilfe der Positionsdaten das Fahrrad suchen, dieses mitnehmen und den Bestohlenen zurückgeben. Dadurch würden sie einen rechtswidrigen Zustand beenden und verhindern, dass den Bestohlenen der Besitz dauerhaft entzogen wird. Die Rückgewinnungshilfe ist also polizeiliche Gefahrenabwehr. Zur Rückgewinnungshilfe ist die Polizei gleichwohl nur selten verpflichtet.

Um dem Umstand gerecht zu werden, dass die Polizei nicht in der Lage ist, alle Gefahren abzuwehren, liegt dem Polizei- und Ordnungsrechts das Opportunitätsprinzip zugrunde, sodass es grundsätzlich im Ermessen der Polizei liegt, ob und wie sie einschreitet.[9] Die Polizei soll in zeitlicher, räumlicher, personeller und sachlicher Hinsicht Schwerpunkte bei der Gefahrenabwehr setzen und so mit den ihr zur Verfügung stehenden Mitteln ihre Aufgaben möglichst effektiv erfüllen und Einzelfallgerechtigkeit herstellen.[10] Demnach kann ein Nichteinschreiten der Polizei trotz Bestehen einer Gefahr rechtmäßig sein.[11] Das Ermessen ist allerdings nicht gänzlich frei, sondern es gilt der Grundsatz der pflichtgemäßen Ermessensausübung. Demnach muss das Ermessen fehlerfrei ausgeübt werden.[12] Maßstab ist dabei eine effektive Gefahrenabwehr,[13] die sich insbesondere an der Wertigkeit der bedrohten Rechtsgüter und dem Grad der Bedrohung zu orientieren hat; bei Gefahren für höherwertige Rechtsgüter wird das Ermessen dementsprechend eingeschränkt. Relevant ist auch, wie dringend ein Einschreiten erforderlich ist. Außerdem ist zu berücksichtigen, welche Risiken und welcher Aufwand durch das polizeiliche Einschreiten entsteht. Dabei muss eine gewisse Einsatzreserve der Polizei für potenzielle schwere Gefahren bestehen.[14] Dementsprechend kann der Ermessensspielraum auch eingeschränkt sein, wenn der Aufwand gering ist und dabei keine anderen polizeilichen Pflichten vernachlässigt werden.[15] In Einzelfällen kann das Ermessen „auf null reduziert sein", wodurch eine Pflicht zum Einschreiten entsteht, die von der Rechtsprechung allerdings nur selten angenommen wird.[16]

9 Kingreen/Poscher 2020, S. 183.
10 Möstl/Mühl-Müller-Franken 2021, § 5 Rn. 3 m. w. N.
11 Schenke 2021, S. 63.
12 Gusy 2017, S. 239.
13 Zimmermann, NJW1999, S. 3145.
14 Vgl. Kingreen/Poscher 2020, S. 185-186 m. w. N.
15 Schenke 2021, S. 63-64.
16 Gusy 2017, S. 240.

Eine solche Pflicht kann insbesondere bei erheblichen Gefahren für wesentliche Rechtsgüter bestehen.[17]

Somit ist eine Pflicht zum Einschreiten bzw. eine Reduzierung des Ermessens im Falle der Rückgewinnungshilfe von gestohlenen Fahrrädern zwar denkbar, wird aber im Regelfall nicht vorliegen. Die Eigentumsposition ist im Falle eines gestohlenen Fahrrades regelmäßig nicht als wesentliches Rechtsgut anzusehen, sodass eine Ermessensreduzierung „auf null" äußerst selten sein wird. Die Polizei wird bei der Rückgewinnungshilfe vielfach ein weites Ermessen haben, welches oft nicht eingeschränkt sein wird, allein aufgrund der Vielzahl anderer Aufgaben, die in vielen Situationen höherwertige Rechtsgüter betrifft. Allein aus den Positionen des Fahrrades wird sich zudem oft nicht schließen lassen, dass ein Einschreiten besonders dringend ist. Dies kann lediglich der Fall sein, wenn aus den Positionsdaten ersichtlich wird, dass in absehbarer Zeit eine Rückgewinnungshilfe nicht mehr möglich ist, z. B. wenn erkennbar ist, dass Fahrränder über Landesgrenzen gebracht werden sollen. In dieser und auch in anderen Konstellationen ist nicht auszuschließen, dass gerade bei höherwertigen Fahrrändern eine Pflicht zum Einschreiten besteht, insbesondere, wenn gerade keine anderweitige Auslastung der Polizei vorliegt. Auch wenn damit zu rechnen ist, dass die Anzahl von Fällen der potenziellen Rückgewinnungshilfe durch vermehrte Positionsdaten steigen wird, wird die Polizei dennoch im Regelfall einen weiten Entscheidungsspielraum haben, ob sie entsprechend aktiv wird. Vor Allem ist dabei auch zu berücksichtigen, dass eine Rückgewinnungshilfe auch Einfluss auf die strafprozessualen Ermittlungen haben kann, sodass auch ermittlungstaktische Gründe zu berücksichtigen sind, die gegen ein Einschreiten sprechen können.[18]

## 3. Strafverfolgung

Im Bereich der Strafverfolgung ist die Polizei hingegen gemäß der §§ 163 Abs. 1 Satz 1, 160 Abs. 1 StPO verpflichtet, im Falle einer ihr bekanntgewordenen Straftat ausnahmslos tätig zu werden, d. h. diese zu erforschen und ggf. aufzuklären.[19] Das Legalitätsprinzip wird überwiegend mit der Rechtsstaatsgarantie begründet, da die konsequente Durchführung dieses Grundsatzes die notwendige Gleichbehandlung von Betroffenen von Straftaten sowie der Täter*innen und damit allgemein strafrechtliche Gerechtigkeit garantiert.[20] So zielt die

17 Z. B. BVerwGE 11, 95 (97); Schenke 2021, S. 64; zur Übersicht Gusy 2017, S. 240.
18 Siehe dazu ausführlich Fährmann in diesem Band, 141 ff.
19 Schneider-Kölbel 2016, § 160 Rn. 29; Kühne 2015, S. 199.
20 BVerfGE 16, 194 (202); BVerfGE 46, 214 (223); Hannich-Diemer 2019, § 152 Rn. 3.

Pflicht zur Ermittlung auf eine unterschiedslose Strafrechtsimplementierung ab, da sämtlichen Verdachtsfällen ohne Ansehung der Person nachgegangen werden muss.[21] Die Exekutive soll nicht eigenen Strafwürdigkeitserwägungen zugrunde legen; vielmehr soll die demokratisch legitimierte Legislative sowie gerichtliche Normenkonkretisierung vorgeben, was strafwürdig ist.[22] Das Legalitätsprinzip gilt während des gesamten Strafverfahrens.[23]

Sofern diese Erwägungen uneingeschränkt zugrunde gelegt würden, hätte dies zur Folge, dass die Polizei als Strafverfolgungsbehörde bei Kenntnis der Position von gestohlenen Fahrrädern und allen anderen Gegenständen zum Einschreiten verpflichtet wäre, was aufgrund der Vielzahl der Fälle bei einer standardisierten Übertragung von Positionsdaten an die Polizei bei der bisherigen Organisationsstruktur vielfach kaum möglich wäre.[24] Gleichwohl ist zu beachten, dass im Rahmen des Legalitätsprinzips mehrere Aspekte zu berücksichtigen sind, die dazu führen, dass die Polizei bei den Ermittlungen einen gewissen Spielraum hinsichtlich der Frage hat, ob sie im Falle eines Diebstahls ermittelt.

### *3.1 Ermittlungstaktik*

Zunächst ist festzuhalten, dass Raum für ein ermittlungstaktisches Vorgehen besteht. Die StPO legt weder Zeitpunkt noch Art der Ermittlungen fest. So kann etwa ein Zuwarten geboten sein, wenn die Annahme gerechtfertigt ist, dass dadurch ein umfassenderer Aufklärungserfolg zu erwarten ist; beispielsweise hinsichtlich hinter dem*der Täter*in stehenden Strukturen.[25] Die Polizei hat damit einen Ermessensspielraum hinsichtlich der Frage des Zeitpunkts des Einschreitens und im gewissen Sinne hinsichtlich der Art und Weise des Vorgehens,[26] sofern dieses nicht erkennbar ineffizient ist. Die zeitweise Zurückstellung bestimmter Ermittlungshandlungen ist demnach vielfach kein "Aufschieben" der Strafverfolgung, sondern vielmehr eine taktische Variante, um dem Legalitätsprinzip im bestmöglichen Umfang gerecht zu werden.[27] Dieser Spielraum wird als „Grundsatz der freien Gestaltung des Ermittlungsverfahrens" bezeichnet und findet dort seine Grenzen, wo rechtliche Vorgaben verletzt werden.[28] Dies

21 BVerfG NStZ 1982, 430 (430); BGHSt 15, 155 (159).
22 Schneider-Kölbel 2016, § 160 Rn. 31; Erb 1999; BKA 2019, S. 136-137.
23 Kühne 2015, S. 198.
24 Vgl. Erb 1999, S, 89; Nestler JA 2012, S. 91; Kühne 2015, S. 200.
25 Rebmann, NJW 1985, S. 4; Graulich 2021, E Rn. 118.
26 Krause 1978, Rn. 100; Schmidt-Jortzig, NJW 1989, S. 134-135.
27 Rebmann, NJW 1985, S. 4.
28 Schmidt-Jortzig, NJW 1989, S. 134-135. f.

ist beispielsweise der Fall, wenn auf eine Ahndung bekannt gewordener Straftaten völlig verzichtet wird oder verzichtet werden muss, weil sie entweder aufgrund des Zeitablaufs nicht oder nur noch schwer zu rekonstruieren sind.[29] Sofern der Verzicht der Verfolgung eines Diebstahl aufgrund von Ermittlungstaktik erfolgt, stellt dies keinen Verstoß gegen das Legalitätsprinzip dar.[30]

Somit ist es der Polizei regelmäßig gestattet, die Bewegungen gestohlener Gegenstände über einen längeren Zeitraum zu verfolgen, ohne einzugreifen, wenn ermittlungstaktische Aspekte dafürsprechen.[31] Gerade im Rahmen von Seriendiebstählen kann es sinnvoll sein, Bewegungen einzelner Gegenstände länger zu beobachten, da diese Rückschlüsse auf hinter den Diebstählen stehenden Strukturen ermöglichen können. Dabei kann die Polizei aus ermittlungstaktischen Erwägungen auch in Kauf nehmen, dass hinsichtlich einzelner Gegenstände eine Rückgewinnungshilfe nicht mehr zu leisten ist. Andernfalls wäre die Polizei nicht in der Lage, entsprechende Seriendiebstähle vollständig aufzuklären und würde dadurch gegen das Legalitätsprinzip verstoßen.

### *3.2 Schwerpunktsetzung bei der Strafverfolgung*

Der Polizei wird regelmäßig nicht nachweisbar sein, dass ihre Schwerpunktsetzung dazu führt, dass sie gewisse Delikte nicht verfolgen bzw. nicht ausreichend verfolgen kann. Die Schwerpunktsetzung ist daher gerichtlich kaum überprüfbar und daher eher ein theoretisches Problem.

Wie bereits beschrieben, muss die Polizei Schwerpunkte bei der Strafverfolgung setzen. Gewisse Delikte können nur aufgeklärt werden, wenn ausreichende polizeiliche Ressourcen eingesetzt und gebündelt werden.[32] Insofern kann eine gewisse Tendenz beobachtet werden, schwerere Delikte bevorzugt zu verfolgen; etwa Tötungsdelikte.[33] Würde aber eine Bündelung nicht erfolgen, sondern die Ermittlungstätigkeit nach dem „Gießkannenprinzip“ verteilt werden - d. h. dass die Polizei bei jeder Straftat „ein bisschen“ ermittelt -, wäre dies ein Verstoß gegen das Legalitätsprinzip, da so keine effektive Ermittlungsarbeit gewährleistet wäre. Einschränkungen der Verfolgungspflicht sind damit nicht zwingend eine Durchbrechung des Legalitätsprinzips, sondern können die Verfolgung anderer Delikte überhaupt erst ermöglichen.[34]

29 Graulich 2021, E Rn. 128.
30 Sander-Cramer 2021, § 258a Rn. 10
31 Zu den rechtlichen Voraussetzungen siehe Fährmann in diesem Band, S. 141ff.
32 Vgl. Kühne 2015, S. 200.
33 Erb 1999, S. 89; Nestler 2012, S. 91; Rieß, NStZ 1981, S. 4.
34 Vgl. Rieß, NStZ 1981, S. 6.

Eine Verpflichtung nach dem Legalitätsprinzip kann nicht bestehen, wenn in der konkreten Situation entsprechende Ressourcen zur Verfolgung fehlen,[35] beispielsweise weil alle Einheiten aufgrund von bestehenden Ermittlungen ausgelastet sind und diese nicht zurückgestellt werden können. Fehlen diese Ressourcen aber aufgrund einer defizitären Organisationsstruktur oder unterlässt die Polizei die Verfolgung, weil sie das Delikt nicht für relevant hält, ist ein Verstoß gegen das Legalitätsprinzip theoretisch denkbar. Zwar ist der Staat verpflichtet, seine Organisationseinheiten so auszustatten, dass sie ihren (verfassungsrechtlichen) Aufgaben nachkommen können.[36] Die Verteilung und der Einsatz von Ressourcen, Polizeitaktik und die vorhandenen Organisationsstrukturen sind allerding kaum justiziabel. Da sich die Organisationsstruktur der sehr komplexen Behörde Polizei auf sehr viele verschiedene Aufgaben bezieht, kann von gerichtlicher Seite diese Struktur kaum abschließend beurteilt werden, da diese von sehr vielen Faktoren abhängt. Insofern können nur erhebliche und offensichtliche Defizite eine gerichtlich feststellbare Verletzung des Legalitätsprinzips begründen.[37] Insofern würde sich regelmäßig allenfalls die Frage stellen, ob einzelne Polizist*innen gegen das Legalitätsprinzip verstoßen, wenn sie trotz bekannter Position eines gestohlenen Fahrrades nicht einschreiten. Ein solcher Verstoß kann schwer wiegen, weshalb dieser strafbar sein kann.

## 4. Strafbarkeit von Polizist*innen bei Nichtverfolgung

Es kommen zwei Varianten der Strafvereitlung im Amt in Betracht. Polizist*innen schreiten nicht ein, weil sie andere Delikte verfolgen bzw. Gefahren abwehren und dementsprechend einen anderen Schwerpunkt gesetzt haben. Oder sie schreiten nicht ein, obwohl es ihnen mangels anderer Verpflichtungen möglich wäre. Ein Nichteinschreiten trotz der Möglichkeit ist unproblematisch strafbar (was aber keine Besonderheit neuer technischer Entwicklungen ist), während ein Nichteinschreiten bei anderen Aufgaben bzw. einer anderen Schwerpunksetzung regelmäßig gerechtfertigt ist.

Eine Strafbarkeit nach den §§ 258, 258a, 13 StGB kommt in Betracht, wenn die Polizist*innen ihrer aus dem Legalitätsprinzip begründeten Pflicht zur Strafverfolgung im Einzelfall nicht nachkommen.[38] Eine Strafvereitelung durch Unterlassen setzt eine Garantenpflicht nach § 13 Abs. 1 StGB voraus, die sich

35 Erb 1999, 89 m. w. N.

36 Vgl. BVerfGE 40, 276 (284); BVerfG, Beschl. v. 23.5.2013, 2 BvR 2129/11, Rn. 16.

37 Verstöße gegen Verfassungsprinzipien, die sich aus polizeilichen Selektionsprozessen ergeben, können natürlich unabhängig davon rechtswidrig sein.

38 Sander 2021-Cramer, § 258a Rn. 10; vgl. BGH NJW 1960, 1962 1963.

konkret auf das Rechtsgut der Strafvereitelung beziehen muss.[39] Geschütztes Rechtsgut der §§ 258 und 258a StGB ist die staatliche Strafrechtspflege. Die Garantenpflicht trifft daher nur solche Personen, die die rechtliche Verpflichtung haben, Belange der Strafrechtspflege wahrzunehmen, d. h. dafür zu sorgen oder dazu beizutragen, dass Straftaten aufgeklärt werden.[40] Dies betrifft vor Allem Polizist*innen,[41] die auch Amtsträger*innen im Sinne des § 258a StGB sind.[42] Lassen Beamt*innen eine Straftat unbearbeitet, kann ein Unterlassung tatbestandsmäßig i.S. der §§ 258, 258a StGB sein, wenn dadurch Täter*innen für geraume Zeit der Bestrafung entzogen werden.[43] Die Strafbarkeit wird durch die örtliche und sachliche Zuständigkeit sowie durch die Aufgabenzuweisungen innerhalb der Behörde beschränkt.[44] Die innerdienstliche Aufgabenverteilung ist ein wesentlicher Bestandteil einer am Rechtsstaatsgedanken ausgerichteten effektiven Strafrechtspflege sowie zugleich die Grundlage für die Bestimmung der individuellen Leistungspflicht und -fähigkeit der Amtsträger*innen. Eine von der innerdienstlichen Zuständigkeit abgekoppelte strafbewehrte Verpflichtung zur Verfolgung hinsichtlich aller bekannt gewordenen Straftaten würde zu einer praktisch nicht lösbaren Pflichtenkollision führen.[45]

Beamt*innen dürfen nicht über die Grenzen ihrer Leistungsfähigkeit bei der Strafverfolgung in Anspruch genommen werden; mehr als das Mögliche kann nicht verlangt werden.[46] Wenn sie nicht in der Lage sind, alle zugewiesenen Aufgaben zu erfüllen, so kann ihnen nicht der Vorwurf der Pflichtwidrigkeit und damit eines rechtswidrigen Verhaltens gemacht werden.[47] Sie müssen dann Verfolgungsschwerpunkte setzen. Auch wenn in objektiver und subjektiver Weise der Tatbestand erfüllt sein kann, muss die Rechtswidrigkeit in solchen Konstellationen entfallen. Es handelt sich um eine Pflichten-Kollision, die die Beamt*innen kaum auflösen können. Die Pflichtenkollision ist ein selbstständiger übergesetzlicher Rechtfertigungsgrund bei Unterlassungsdelikten.[48] Voraussetzung ist, dass Täter*innen mehrere rechtliche Handlungspflichten treffen, sie aber nur eine erfüllen können,[49] vorliegend die Verfolgung von zwei oder mehreren Delikten gleichzeitig.

---

39 LG NStZ 2021, 544 (544).
40 BGH NJW 31/1997, 2059 (259).
41 Schönke/Schröder-Hecker 2019, § 258a Rn. 10; Dusch/Rommel 2014, S. 189.
42 Schönke/Schröder-Hecker 2019, § 258a Rn. 10.
43 BGH NJW 43/1960, 1962 1963.
44 BGH NJW 43/1960, 1962 1963; BGH NJW 1993, 544 (544).
45 Sander-Cramer 2021, § 258a Rn. 5.
46 Bock 2018, S. 587.
47 BGH NJW 43/1960, 1962 1963.
48 Bock 2018. S. 586, m. w. N. zum dogmatischen Streitstand.
49 Schönke/Schröder-Lieben 2019, vor § 32 Rn. 71/72; Satzer JA 2010, S. 753 ff.

Denkbar wäre eine Strafvereitlung im Amt durch Schwerpunktsetzung nur bei groben Missverhältnissen im Selektionsprozess. Etwa wenn bei bestimmten Kriminalitätsphänomenen nur mit äußerst geringem Aufwand oder überhaupt nicht ermittelt wird. Es kann zudem einen Verstoß gegen das Legalitätsprinzip darstellen, wenn die Polizei nur bestimmte Personengruppen verfolgt und daher andere Gruppen übersieht;[50] eine solche Praxis wird überdies regelmäßig gegen Grund- und Menschenrechte verstoßen.[51] Entsprechende Schwerpunktsetzungen dürfte aber vielfach schwer zu beweisen sein, wenn solche Verstöße nicht offensichtlich sind, da diese einen vertieften Blick in innerbehördliche Abläufe erfordern.

## 5. Fazit

Ob der Polizei Straftaten und Gefahren bekannt werden und wie sie diese aufklären bzw. prognostizieren kann, ist dynamischen Entwicklungen unterworfen. Beispielsweise kann die Polizei aufgrund von technischen Neuerungen über (weitere) Ermittlungsansätze verfügen, die es wahrscheinlicher machen, Straftaten aufzuklären bzw. Gefahren zu verhindern.

Positionsdaten gestohlener Gegenstände können solche neuen Ermittlungsansätze sein, die sowohl Rückgewinnungshilfe als auch Strafverfolgung ermöglichen oder vereinfachen können. Insgesamt ist damit zu rechnen, dass sich durch solche neuen Ansätze Strukturen und Abläufe innerhalb der Polizei ändern, da neue Ermittlungsansätze vielfach nicht ignoriert werden können. Dies wirkt sich aber nur beschränkt auf die rechtlichen Pflichten zum Eingreifen aus, da die Polizei einen großen Spielraum bei der Schwerpunktsetzung hat, der gerichtlich kaum zu kontrollieren ist. Vielmehr ist damit zu rechnen, dass ein gesellschaftlicher bzw. politischer Druck auf die Polizei entsteht, den Ermittlungsansätzen nachzugehen. Da immer mehr Gegenstände mit Ortungstechnologien ausgestattet sind, ist daher zu empfehlen, dass sich die Polizei darauf einstellt, dass immer mehr Personen zu ihnen kommen, die wissen, wo sich gestohlene Gegenstände befinden. Andernfalls verbliebe den Beamt*innen nur die Möglichkeit, sich von den Bestohlenen zu der Position des gestohlenen Gegenstandes hin dirigieren zu lassen oder dies zu verweigern. In einer solchen Situation stellen sich praktisch dieselben Probleme hinsichtlich von Rückgewinnungshilfe, dem Legalitätsprinzip und der Strafvereitlung im Amt.

50 Ein Beispiel wäre die überwiegende Verfolgung von Armutskriminalität, die von Feest/Blankenburg 1972, S. 114-119 beobachtet wurde.

51 Vgl. dazu z. B. Aden, Zeitschrift für Menschenrechte 2017; Aden/Fährmann 2018, S. 18; Cremer 2013.

Insgesamt ist es also sinnvoll, auf neue Ermittlungsansätze zielgerichtet zu reagieren und sich nicht aus Sorge vor einem beträchtlichen Mehraufwand dagegen zu sperren. Eine Möglichkeit wäre, die Etablierung einer entsprechenden Software zur Ermittlung von Positionsdaten.

## Literaturverzeichnis

Aden, Hartmut (2017) Anlasslose Personenkontrollen als grund- und menschenrechtliches Problem in: Zeitschrift für Menschenrechte, 11 Jg., Nr. 2, S. 54–65.

Aden, Hartmut/Fährmann, Jan (2018) Polizeirecht vereinheitlichen? Kriterien für MusterPolizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive. https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf (letzter Aufruf: 21.02.2023).

BKA (2019) Organisierte Kriminalität (OK), in: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html (letzter Aufruf: 21.02.2023).

Bock, Dennis (2018) Strafrecht Allgemeiner Teil. Heidelberg: Springer.

Boers, Klaus (2007) Hauptlinien der kriminologisch Längsschnittforschung. In: Boers, K./Reinecke, J. (Hg.): Delinquenten Jugendalter. Erkenntnisse einer Münsteraner Längsschnittstudie. Münster, S. 5–32.

Boers, Klaus (2008) Die Trias: Ubiquität, spontan Bewährung und Intensität. In: Deutsche Vereinigung für Jugendgerichte und Jugendgerichtshilfe e. V. (Hg.): Fördern, fordern, fallen lassen. Aktuelle Entwicklung im Umgang mit Jugenddelinquent, Dokumentation des 27. deutschen Jugendgerichtstages vom 15. - 18 September 2007 in Freiburg. Mönchengladbach.

Cremer, Hendrik (2013) Studie „Racial Profiling" – Menschenrechtswidrige Personenkontrollen nach § 22 Abs. 1 a Bundespolizeigesetz Empfehlungen an den Gesetzgeber, Gerichte und Polizei, (Hg.): Deutsches Institut für Menschenrechte. https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Racial_Profiling_Menschenrechtswidrige_Personenkontrollen_nach_Bundespolizeigesetz.pdf (letzter Aufruf: 04.02.2021).

Dusch, Christian/Rommel, Sebastian (2014) Strafvereitelung (im Amt) durch Unterlassen am Beispiel von Finanzbeamten in: NStZ, 34 Jg., Nr. 04, S. 188–192.

Erb, Volker (1999) Legalität und Opportunität. Gegensätzliche Prinzipien der Anwendung von Strafrechtsnormen im Spiegel rechtstheoretischer, rechtsstaatlicher und rechtspolitischer Überlegungen, Berlin: Duncker & Humblot.

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

Fährmann, Jan (2021) Soziale Kontrolle durch die Polizei in: CILIP, Nr. 125, S. 32-39.

Feest, Johannes/Blankenburg, Erhard (1972) Die Definitionsmacht der Polizei. Strategien der Strafverfolgung und soziale Selektion. Düsseldorf: Bertelsmann Univ.-Verl.

Graulich, Kurt (2021) E. Das Polizeihandeln. In: Lisken, H./Denninger, E. (Hg.): Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz. 7. Aufl. München: C.H. Beck, S. 341–644.

Gusy, Christoph (2017) Polizei- und Ordnungsrecht. 10. Aufl. Tübingen: Mohr Siebeck.

Hannich, Rolf (2019) Karlsruher Kommentar zur Strafprozessordnung. Mit GVG, EGGVG, EMRK. 8. Aufl. München: Beck C H.

Krause, Dietmar (1978) Strafverfahrensrecht in der Polizeipraxis. Köln: Heymann.

Kühne, Hans (2015) Strafprozessrecht. Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts. 9. Aufl. Heidelberg: C.F. Müller.

Kunz, Karl-Ludwig/Singelnstein, Tobias (2021) Kriminologie. Eine Grundlegung. 8. Aufl. Stuttgart, Bern: utb.

Möstl, Markus/Bäuerle, Michael (Stand 1.10.2021) Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen. 23. Edition. München: Beck.

Nestler, Nina (2012) Strafverfahren zwischen Wirtschaftlichkeit und Legalitätsprinzip in: JA, 44 Jg., Nr. 2, S. 88–95.

Kingreen, Thorsten/Poscher, Ralf (2020) Polizei- und Ordnungsrecht. Mit Versammlungsrecht. 11. Aufl. München: Beck, C H.

Rebmann, Kurt. (1985): Der Einsatz verdeckt ermittelnder Polizeibeamter im Bereich der Strafverfolgung in: NJW, 38 Jg., Nr. 1-2, S. 1–6.

Rieß, Peter (1981) Die Zukunft des Legalitätsprinzips in: NStZ 1 Jg., Nr. 1, S. 2–10.

Sander, Günther (2021): Münchener Kommentar zum Strafgesetzbuch. Band 4. München: Beck.

Satzer, Hartmut (2010) Die Rechtfertigende Pflichtenkollision. In: JA, 42 Jg., Nr. 10, 753-757.

Schenke, Wolf-Rüdiger (2021): Polizei- und Ordnungsrecht. 11. Aufl. Heidelberg: C.F. Müller.

Schmidt-Jortzig, Edzard (1989) Möglichkeiten einer Aussetzung des strafverfolgerischen Legalitätsprinzips bei der Polizei in: NJW, 42 Jg., Nr. 3, S. 129–138.

Schneider, Helmut (2016) Münchener Kommentar zur Strafprozessordnung. Band 2. München: Beck C H.

Schönke, Adolf/Schröder, Horst (2019) Strafgesetzbuch. Kommentar. 30. Aufl. München: C.H. Beck.

Zimmermann, Andreas (1999) Polizeiliche Gefahrenabwehr und das Internet in: NJW, 52 Jg., Nr. 43, S. 3145–3152.

*Hartmut Aden[1]/Jan Fährmann[2]/Christian Matzdorf [3]*

# Technikforschung und Polizei – strukturelle Rahmenbedingungen, Hindernisse und Perspektiven

## 1. Polizei, Technik und Forschung

Die schnelle technische Entwicklung ist auch an der Polizei nicht vorbeigegangen. Begrenzte Haushaltsmittel, bürokratische Schwerfälligkeit und die verfassungsrechtlichen Grenzen zulässiger Grundrechtseingriffe stehen manchen von Praktizierenden gewünschten Innovationen im Wege.[4] Polizeiarbeit basiert zu größeren Teilen auf Tätigkeiten, die vorrangig von Menschen durchgeführt werden, etwa Präsenz von Polizeistreifen im öffentlichen Raum. Dennoch hat die Technisierung dazu geführt, dass sich Polizeiarbeit in den zurückliegenden Jahrzehnten grundlegend verändert hat.[5]

Besonders offensichtlich wird dies – wie in vielen anderen Lebensbereichen auch – am Beispiel der voranschreitende Digitalisierung. Dementsprechend wurde die Polizei für ihre Aufgaben – d. h. zur Gefahrenabwehr und Strafverfolgung – mit technischen Mitteln ausgestattet, da die wachsende Bedeutung digitaler Daten es sowohl erforderlich macht, dass die Polizei selbst über Datenverarbeitungstechnologie verfügt als auch Zugriff auf Vorgänge der Datenverarbeitung von Beschuldigten oder Personen hat, von denen Gefahren ausgehen.[6] Auf Bundesebene wurde im Jahr 2017 die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (ZITIS) gegründet, die Polizeibehörden und Nachrichtendienste des Bundes bei der Telekommunikationsüberwachung, der digitalen Forensik, der Kryptoanalyse und der *Big-Data*-Analyse unterstützen soll.[7]

---

1 Prof. Dr. Hartmut Aden hat das Projekt FindMyBike für den Bereich Rechtswissenschaft geleitet.

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

3 Prof. Christian Matzdorf hat in dem Projekt FindMyBike kriminalistische und kriminaltechnische Forschungsfragen bearbeitet.

4 Näher hierzu Aden, Vorgänge 2019, S. 7 f.

5 Ausführlich Heinrich 2008, S. 203 ff.; Jarolimek 2019, S. 175; Rademacher/Perkowski 2020, S. 713 f.

6 Fährmann, MMR 2020, S. 228; Krüger, ZRP 2016, S. 190.

7 https://www.zitis.bund.de/DE/Home/home_node.html (letzter Aufruf am 04.03.2023).

Eine Besonderheit der *polizeilichen* Techniknutzung besteht in der großen Bedeutung, die Informationen für die Gefahrenabwehr, für Beweiszwecke in Strafverfahren und für die polizeiliche Zusammenarbeit mit Behörden und Dritten im In- und Ausland haben. Für diese Zwecke ist die Polizei – noch wesentlich stärker als andere Verwaltungen – auf Informationen angewiesen.[8] Unter Praktizierenden ist daher der Wunsch zu beobachten, möglichst ohne Reglementierung Zugriff auf möglichst umfangreiche Datenbestände zu haben. Unterstellt wird vielfach, dass die Sicherheitsbehörden umso besser funktionieren, je umfassender der Alltag überwacht wird.[9] Da Gefahrenprognosen möglichst viele Informationen erfordern, können entsprechende Ansätze zu einem nahezu unstillbaren Informationsverlangen hinsichtlich potenzieller Gefahrenherde und Beschuldigter führen.[10] Damit gehen zwangsläufig immer mehr Eingriffe in die Grund- und Menschenrechte einher, selbst wenn weder Gefahren oder Straftaten vorliegen noch Menschen zu den Eingriffen einen Anlass gegeben haben.[11] Betroffen sind besonders die informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und die Telekommunikationsfreiheit (Art. 10 GG). Diese Konfliktlinie spiegelt sich insbesondere in den kontroversen fachlichen, politischen und gesellschaftlichen Diskussionen über den Zugriff auf große Datenbestände wider, die unabhängig von konkreten Ermittlungsverfahren von der Polizei oder Dritten gesammelt werden,[12] etwa in Form der Vorratsdatenspeicherung für Telekommunikationsverbindungsdaten.

Das Bundesverfassungsgericht (BVerfG) hat in zahlreichen Entscheidungen betont, dass der Zugriff auf Datenbestände kein harmloser Grundrechtseingriff ist, wenn ungezielt mit Datenbeständen gearbeitet wird, die Informationen über Unbeteiligte enthalten.[13] In seiner Entscheidung aus dem Mai 2020 zur Auslands-Telekommunikationsüberwachung durch den Bundesnachrichtendienst hat das BVerfG klargestellt, dass nicht nur Menschen, die sich in Deutschland aufhalten, unter dieses Grundrecht fallen, sondern auch Drittstaatsangehörige, die von deutschen Sicherheitsbehörden überwacht werden.[14] Da die Informationstechnik in den zurückliegenden Jahrzehnten immer leistungsfähiger geworden ist, steigt faktisch die Intensität, mit der polizeiliche Technik in die Grundrechte der Menschen eingreift, selbst wenn die gesetzlichen Grundlagen

8 Näher hierzu Aden 2014, S. 58ff.
9 Schaar, HMD 2014, S. 843; Rademacher/Perkowski, JuS 2020, S. 713.
10 Baldus, Die Verwaltung 2014, S. 9 ff.; Schaar 2017, S. 59.
11 Aden/Fährmann, 2018, S. 21; Arzt, DÖV 2017, S. 1027.
12 Vgl. dazu Schaar, HMD 2014; Aden/Fährmann 2018, S. 17 ff.; Rademacher/Perkowski, JuS 2020, S. 713–720.
13 Z. B. BVerfGE 141, 220 ff.; BVerfGE 125, 260 ff.
14 BVerfG, Entscheidung vom 19.5.2020 - 1 BvR 2835/17 = BVerfGE 154, 152 ff.

hierfür gar nicht erweitert werden; denn allein die leistungsfähigere Technik eröffnet mit denselben rechtlich normierten Verfahren mehr Möglichkeiten zu Eingriffen in die Privatsphäre der Menschen.[15] Hinzu kommen Konstellationen, wie sie im *FindMyBike* Projekt für die polizeiliche Nutzung von Positionsdaten untersucht wurden, in denen zwar eine gesetzliche Grundlage vorhanden ist, aber leistungsfähigere Technik die Frage aufwirft, ob ihre Nutzung noch von den bestehenden Normen gedeckt ist.[16] Die Erforschung und Entwicklung polizeilich zu nutzender Technik ist mithin ein sensibles Thema, da die Auswirkungen neuer Technologien auf die Ausübung von Grund- und Menschenrechten gravierend sein können und darüber hinaus weitere Rückwirkungen auf das gesellschaftliche Zusammenleben möglich sind.

Das Interesse der Polizeipraxis an technischen Innovationen liegt auch in der Vereinfachung von Arbeitsabläufen. Die polizeiliche Arbeit kann durch neue Technologien erheblich effektiver gestaltet werden. Zeitaufwendige Arbeiten wie das Suchen in Papierkarteien, die früher von Menschen erledigt wurden, können jetzt von Computern übernommen oder jedenfalls beschleunigt werden. Viele Akteure der Polizeipraxis möchten dementsprechend auf dem neuesten Stand der Technik arbeiten. Es ist anzunehmen, dass die meisten Polizeibediensteten privat über eine leistungsfähige technische Ausstattung verfügen, etwa Smartphones und Notebook-Computer, sodass es für sie kaum einsehbar ist, im Dienst mit wesentlich weniger leistungsfähiger Technik zu arbeiten. Technische Entwicklungen müssen auch nicht zwangsläufig mit schweren Eingriffen einhergehen, da Technik auch so gestaltet werden kann, dass Eingriffe auf das notwendige Maß beschränkt und die Privatsphäre Betroffener gewahrt bleibt. Entscheidend sind technische Lösungen, bei denen die rechtskonforme Nutzung nicht von den Endanwendenden abhängt, sondern bereits in der Ausgestaltung der Technik angelegt ist (*privacy by design* und *legality by design*).

Insgesamt wird deutlich, dass im Rahmen der polizeilichen Technikforschung zahlreiche - teilweise gegenläufige - Aspekte und Interessen zu berücksichtigen sind.

15 Ausführlich zu diesem Effekt: Fährmann/Aden/Bosch, Kriminologisches Journal 2020.

16 Näher hierzu Aden/Fährmann, Vorgänge 2019 und die rechtswissenschaftlichen Beiträge in diesem Band.

## 2. Unabhängige interdisziplinäre Forschung zur polizeilichen Techniknutzung

Polizeibehörden können oft nicht einfach Standardprodukte einkaufen. Zu speziell sind die Anforderungen aufgrund spezifischer Aufgaben und hoher Sicherheitsanforderungen. Bereits seit geraumer Zeit verfügen insbesondere das Bundeskriminalamt und einige Landeskriminalämter über eigene kriminaltechnische Forschungskapazitäten. Parallel hat sich eine intensive Zusammenarbeit mit Universitäten und externen Forschungsinstituten entwickelt. Eine neue Dynamik erreichte die technikbezogene Sicherheitsforschung in der Phase nach den Terroranschlägen in New York und Washington vom 11. September 2001, als Sicherheitsvorkehrungen weltweit einen höheren Stellenwert erhielten.

### *2.1 Varianten der Technikforschung für die Polizei*

Technikforschung für die Polizei kommt in verschiedenen Varianten vor. Eine Variante besteht in der Auftragsforschung, bei der Polizeibehörden – wie andere Behörden auch – gezielt Forschungsaufträge zur Lösung bestimmter Probleme oder zur Klärung bestimmter Fragen ausschreiben. Es handelt sich um öffentliche Aufträge, sodass solche Ausschreibungen den Anforderungen des Vergaberechts unterliegen. Auch Evaluationsforschung fällt hierunter, diese ist allerdings in Deutschland auf anderen Politikfeldern, z.B. in der Sozial- oder Arbeitsmarktpolitik, wesentlich stärker ausgeprägt als in Polizei- und Sicherheitsforschung.[17] Die Möglichkeiten von Polizeibehörden, Forschungsaufträge zu vergeben, sind zumeist durch die verfügbaren Haushaltsmittel begrenzt. In der Regel handelt es sich um kleinere, thematisch stark fokussierte Aufträge.

Die zivile Sicherheitsforschung setzt deutlich andere Akzente. Bei den entwickelten technischen Geräten und Anwendungen kann es allerdings Überschneidungen zwischen ziviler und sicherheitsbehördlicher Nutzung und damit forschungsethische Konflikte geben. In der zivilen Sicherheitsforschung entstanden auch Förderlinien für unabhängige wissenschaftliche Forschung, wobei die Förderung zumeist eine enge Kooperation mit Sicherheitsbehörden als „Endnutzende" der entwickelten Sicherheitslösungen voraussetzt. Zumeist handelt es sich um Polizeibehörden – Nachrichtendienste sind in solchen Forschungsprogrammen kaum vertreten, wohl auch wegen ihrer spezifischen Geheimhaltungskultur, die eine Beteiligung an Forschungsverbünden erschwert. Indes wäre eine Beforschung der nachrichtendienstlichen Techniknutzung keinesfalls ausgeschlossen, solange keine Rückschlüsse auf sicherheitsrelevante

17 Zu Konzepten, Stand und Defiziten der Evaluation von Sicherheitsgesetzen: Weingärtner 2021.

Abläufe oder Einzelfälle möglich sind. Polizeibehörden sind gelegentlich auch selbst Förderungsempfangende, die im Rahmen solcher Verbundprojekte eigene Forschungsleistungen erbringen. Zumeist sind sie aber sogenannte „assoziierte Partner", die mit ihrer Mitwirkung die praktische Relevanz des Vorhabens unter Beweis stellen und am Ende von den entwickelten Lösungen profitieren können.

In Deutschland entwickelte das Bundesministerium für Bildung und Forschung (BMBF) hierzu ein spezielles Forschungsprogramm.[18] Auch die Europäische Union sieht in seinen Forschungsprogrammen spezielle Förderlinien für die zivile Sicherheit vor, mit denen Forschungseinrichtungen und Sicherheitsbehörden in europaweiten Verbünden gemeinsam forschen können. Das verfügbare Grundlagenwissen der Sicherheitsforschung ist daher heute wesentlich solider ausgeprägt als noch in den 1990er Jahren, auch wenn der Anwendungsbezug und die Interessen der Sicherheitsbehörden bei dieser Art der Forschung ein wesentlich höheres Gewicht haben als bei klassischer Grundlagenforschung.

Das *Institut für Angewandte Forschung Berlin (IFAF),* Förderer des *FindMyBike*-Projekts, ist nicht auf bestimmte Forschungsthemen fokussiert. Vielmehr fördert das Land Berlin über das IFAF Forschungsvorhaben, an denen mindestens zwei der vier öffentlichen Berliner Hochschulen für Angewandte Wissenschaften und Praxispartner*innen aus der Region beteiligt sind. Forschung zu polizeilichen Themen ist in diesem Rahmen eher die Ausnahme. Diese spezifische Form der Forschungsförderung ermöglicht indes eine enge Vernetzung der beteiligten Hochschul- und Praxispartner/-innen vor Ort. Im *FindMyBike*-Projekt hat sich dies als klarer Vorteil erwiesen, insbesondere während der intensiven Testphase in Zusammenarbeit mit der Polizei Berlin gegen Ende des Projekts.

### *2.2 Hindernisse und Herausforderungen*

Technikorientierte Forschungsprojekte für die und mit der Polizei stoßen allerdings auf eine Reihe spezifischer Hindernisse und Herausforderungen. Dies gilt in unterschiedlichem Ausmaß für Auftragsforschung und für Projekte, in denen die Polizeibehörden assoziierte Partner sind.

Eine erste Herausforderung besteht darin, dass weite Teile der Polizeipraxis durch Alltagsaufgaben stark absorbiert sind. Aufgrund eines jahrelangen Personalabbaus und vielfältiger gewordener Aufgaben sind viele Polizeidienststellen bereits mit ihren Kernaufgaben überlastet. Eine Beteiligung an Forschung wird daher von manchen Praktizierenden als zeitraubender „Luxus" betrachtet.

18 https://www.sifo.de/sifo/de/home/home_node.html (letzter Abruf: 04.03.2023).

Folglich hängen die polizeilichen Kapazitäten zur Beteiligung an Sicherheitsforschung häufig davon ab, wie die Schnittstellen zwischen Polizei und Forschung auf der polizeilichen Seite organisiert sind. Ein Standardmodell hat sich hierfür bisher nicht entwickelt; die Polizei Berlin etwa hat gleich mehrere Stellen, die für Forschungskoordination (mit-) zuständig sind. Für Forschende führt dies zu besonderen Herausforderungen beim Finden der richtigen Ansprechpartner/-innen, bereits in der Konzeptions- und Beantragungsphase für neue Forschungsprojekte, die aufgrund von Abgabefristen zumeist durch einen gewissen Zeitdruck geprägt ist.

Während eines Forschungsprojektes in Kooperation mit der Polizei sind kompetente und gut vernetzte Ansprechpersonen von großer Bedeutung, da es ohne diese nur sehr schwer möglich wäre, Zugang zu den jeweils zuständigen Dienststellen und Personen zu bekommen. Zudem ist es mit einem erheblichen Koordinationsaufwand verbunden, alle relevanten Ansprechpersonen in der Polizei für ein Vorhaben an einen Tisch zu bekommen, beispielsweise für einen Testlauf für neu entwickelte Technologien. Außerdem ist es für Externe nahezu unmöglich herauszufinden, welche Personen für ein Vorhaben an einem Tisch sitzen müssen, etwa damit sich keine Abteilung übergangen fühlt oder behördeninterne Beteiligungsstrukturen eingehalten werden.

Weitere Hindernisse entstehen dadurch, dass Polizeibehörden stark ausgeprägten hierarchischen Kontrollstrukturen unterliegen. Selbst wenn sich in den letzten Jahrzehnten in vielen Polizeibehörden eine positive Grundhaltung gegenüber Forschung entwickelt hat, prägen oft langwierige Genehmigungsverfahren und hierarchische Kontrollstrukturen den Forschungszugang und das Fortkommen gemeinsamer Projekte. Koordinationsstellen oder Hierarchien fungieren dabei oft als *Gatekeeper,* die auch darauf achten, dass möglichst keine Forschungsvorhaben durchgeführt werden, bei denen die jeweilige Dienststelle oder Praxis in ein negatives Licht geraten könnte. Soweit Forschung auf empirischen Erkenntnissen aus der Polizeipraxis basiert, sind somit auch Verzerrungen zu beachten, die durch einen selektiv gewährten Feldzugang entstehen können.

Für IT- und andere technikorientierte Forschung ergeben sich weitere Hindernisse aus hohen Geheimschutz- und IT-Sicherheitsanforderungen, die für die polizeiliche Techniknutzung gelten. Jede Form der netzbasierten Anbindung von Technikressourcen ist aus Behördensicht mit erheblichen Sicherheitsrisiken für die polizeilichen Netze und Datenbestände verbunden. Die Nutzung polizeilicher Echtsysteme zum Entwickeln neuer technischer Lösung stößt daher auf hohe, zumeist kaum zu überwindende Hürden. Forschungsvorhaben müssen sich daher selbst im fortgeschrittenen Stadium zumeist auf die Entwicklung von Prototypen und „Demonstratoren“ beschränken, die eine mögliche polizeiliche Realität in Testsystemen abbilden. Unter diesem Aspekt ist die Testphase

des *FindMyBike*-Projekts einerseits charakteristisch, da die Schnittstelle zur Polizei im Vergleich zum technisch Möglichen und Wünschenswerten auf eine Minimalversion reduziert werden musste. Aufgrund der intensiven Testphase unter Nutzung polizeilicher Technikinfrastruktur gelang dem Projekt hier aber immerhin ein wichtiger Schritt hin zu realitätsnahen Testszenarien.

Wie bei jeder Form der verwaltungsbezogenen Forschung stößt auch die polizeibezogene Technikforschung auf unterschiedlich ausgeprägte Innovationsfreude in der Praxis. Während manche Akteur/-innen geradezu euphorisch auf die Perspektive technischer Innovationen mit erleichtertem Arbeitsalltag und erweiterten technischen Möglichkeiten reagieren, bleiben viele Praktizierende skeptisch und betonen eher die Schwierigkeiten, die mit neuer Technik und damit zu verändernden Gewohnheiten verbunden sind. Im Rahmen des *FindMyBike*-Projektes wurden insbesondere Bedenken geäußert, dass die Polizei nicht in der Lage sein könnte, alle Dieb/-innen von Fahrrädern zu verfolgen, wenn sie in vielen Fällen mit neuen Ermittlungsansätzen in Form von *Tracking*-Daten versorgt wird. Andere Polizist/-innen waren hingegen der Ansicht, dass entsprechende Herausforderungen aufgrund der technischen Entwicklungen ohnehin auf die Polizei zukämen. Sie bewerteten das Projekt als sinnvoll.

Und schließlich stößt polizeibezogene Technikforschung, die über sehr fokussierte Auftragsforschung hinausgeht, auf die Frage, wie die Forschungsergebnisse am Ende tatsächlich in der polizeilichen Praxis genutzt werden können. Dieser Schritt gelingt längst nicht immer und so manche gute Idee wird nicht realisiert. Forschungstransfer in die Praxis ist in Wissenschaftseinrichtungen seit vielen Jahren ein wichtiges Thema – dennoch scheitern Vorhaben trotz ihrer grundsätzlichen Praxistauglichkeit in der Realisierungsphase.

## 3. Recht, Datenschutz und Ethik – mehr als „Begleitforschung“

Im Ausgangspunkt ist Forschung zu polizeilicher Sicherheitstechnik von technischen Disziplinen geprägt. Mit dem Bedeutungsgewinn von *Big Data* und künstlicher Intelligenz spielt die Informatik eine zentrale Rolle. Je nach Fragestellungen kommen andere technisch-naturwissenschaftliche Disziplinen hinzu.

Nachdem der Fokus der öffentlich geförderten Forschung zur zivilen Sicherheit zunächst sehr stark technisch dominiert war, haben sich die rechtlich-sozialwissenschaftlichen und ethischen Teile inzwischen zu zentralen Bestandteilen von Forschungsverbünden der Sicherheitsforschung entwickelt. Dies ist vor allem der Erkenntnis geschuldet, dass technische Innovationen wenig Nutzen haben, wenn ihre Anwendung rechtlich unzulässig ist, als ethisch unvertretbar eingestuft wird oder bei Betroffenen nicht auf Akzeptanz stößt. In einem demokratisch-rechtstaatlichen System sind diese Aspekte zentral, auch im Hin-

blick auf einen notwendigen politischen und gesellschaftlichen Konsens bezüglich des polizeilichen Technikeinsatzes und seiner Grenzen. Die Forschungen hierzu werden auch unter dem Label *Ethical, Legal and Social Implications (ELSI)* zusammengefasst.

Die Forschung zu Recht, Datenschutz und Ethik im Rahmen der Entwicklung sicherheitstechnischer Innovationen hat sich damit gegenüber ihrem Status als „Begleitforschung" emanzipiert. Die Forschungsarbeiten, die in diesem Rahmen geleistet werden, reichen von der klassisch-rechtswissenschaftlichen Bewertung der Zulässigkeit technischer Innovationen nach der aktuellen Rechtslage und im Rahmen verfassungsrechtlich zulässiger Gesetzesänderungen über die Erarbeitung ethischer Bewertungsmaßstäbe bis hin zur empirischen Akzeptanzforschung. Dabei kann die sozial- und rechtswissenschaftliche Forschung an die seit mehreren Jahrzehnten etablierte Technikfolgenabschätzung[19] anknüpfen, die an der Schnittstelle zwischen Wissenschaft und Politikberatung ansetzt.

Strukturelle Begrenzungen ergeben sich indes aus den divergierenden Interessen der Beteiligten. Wenn die sozial- und rechtswissenschaftliche Forschung aufzeigt, dass besser auf eine Technologie verzichtet werden sollte, kollidiert dies mit dem Interesse sowohl der beteiligten Firmen, die auf die Vermarktung der jeweiligen Technologie ausgerichtet sind, als auch von Akteur/-innen aus den beteiligten Sicherheitsbehörden, die sich von der Technologie eine effektivere Arbeit versprechen.[20]

## 4. Forschung zu polizeilicher Technik als empirische Polizeiforschung

Forschung zu polizeilicher Technik ist notwendig, auch empirische Polizeiforschung.[21] Die praktischen Bedarfe und Hindernisse für die Nutzung neuer Technologien lassen sich kaum abstrakt-generell ermitteln, sondern erfordern empirische Einblicke in die Polizeipraxis und ihre Arbeitsweise. Gleiches gilt für die Erprobung technischer Innovationen, die mit realitätsnahen Testszenarien unter Einbeziehung von Polizeipraktiker/-innen ebenfalls eine Variante empirischer Polizeiforschung ist.

Im Vergleich zu rein sozialwissenschaftlicher empirischer Forschung, bei der die Erforschung polizeilicher Praktiken im Mittelpunkt des Erkenntnisin-

19 Grundlegend zur rechtswissenschaftlichen Perspektive auf die Technikfolgenabschätzung: Roßnagel 1993.

20 Zu dieser und weiteren Grenzen der sozial- und rechtswissenschaftlichen Forschung in Projekten zur Sicherheitstechnik: Rappold/Schuster, Vorgänge 2019.

21 Übersicht zum Begriff und zur Methodik Liebl/Ohlemacher 2000.

teresses steht, ist der Feldzugang bei Verbundforschungsvorhaben zur Entwicklung von Techniklösungen für die Polizeiarbeit tendenziell einfacher. Akteur/-innen, die an den technischen Innovationen und ihrer Nutzung interessiert sind, bilden hier die „Türöffner". Für den wissenschaftlichen Zugang und ein strukturiertes Beforschen der Polizei reichen diese hingegen allein nicht aus.

## 5. Schlussfolgerungen und Ausblick

Die Technisierung der Polizeiarbeit ist ein fortlaufender Prozess mit vielen Aspekten. Die Nutzung von Positionsdaten von Fahrrädern oder anderen Gegenständen für die Aufklärung von Diebstählen ist unter diesem Aspekt ein Forschungsfeld von vielen, auf dem der Nutzen technischer Innovationen für den Sicherheitsgewinn zu eruieren und im Rahmen interdisziplinärer Forschung mit möglichen Risiken zu konfrontieren ist.

So kann sicherheitsbezogene Forschung dazu beitragen, die einfache Dichotomie zu überwinden, bei der sich Sicherheit und Freiheit unversöhnlich gegenüberstehen. Abhängig von ihrem technischen Design, das Risiken für die Betroffen und ihre Datenschutzbelange von vornherein einbezieht, können technische Innovationen einen Sicherheitsgewinn erzeugen und bei Betroffenen auf Akzeptanz stoßen, ohne Rechtsstaatlichkeit in Frage zu stellen. Ohne diesen ganzheitlich-gesellschaftlichen Ansatz liefe Sicherheitstechnik dagegen Gefahr, mehr Schaden als Nutzen zu verursachen.

Auch wenn Verbundprojekte unter Einbeziehung der Polizei gerade im Bereich der polizeilichen Technikentwicklung eine große Bedeutung entfalten und gleichzeitig valide wissenschaftliche Ergebnisse produzieren können, ersetzen sie nicht eine unabhängige externe Polizeiforschung. Externe Forschung hat den Vorteil, dass keine gegenseitigen Verpflichtungen bestehen und die Polizei dementsprechend unabhängiger untersucht werden kann. Durch diesen veränderten Blickwinkel sind möglicherweise andere wissenschaftliche Erkenntnisse zu erwarten.

Es kann konstatiert werden, dass es in der deutschen Polizei seit einiger Zeit starke Tendenzen gibt, sich gegenüber Forschung zu öffnen. Verbundprojekte zeigen, dass dies nicht nur ein Gewinn für die Wissenschaft ist, sondern auch für die Polizei.

## Literatur

Aden, Hartmut (2014) Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem, in: der moderne staat, Zeitschrift für Public Policy, Recht und Management, 7. Jg., Nr. 1, S. 55-73.

Aden, Hartmut (2019) Polizei und Technik zwischen Praxisanforderungen, Recht und Politik, in: Vorgänge 2019, Nr. 227, 58. Jg., Nr. 3, S. 7-19.

Aden, Hartmut/Fährmann, Jan (2018) Polizeirecht vereinheitlichen? Kriterien für Muster- Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, Heinrich-Böll-Stiftung e.V (Hg.). https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf, zuletzt besucht 04.03.2023.

Aden, Hartmut/Fährmann, Jan (2019) Lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen? Ein Ausblick am Beispiel der GPS-Ortung gestohlener Gegenstände, in: Vorgänge 2019, Nr. 227, 58. Jg., Nr. 3, S. 95-106.

Arzt, Clemens (2017) Das neue Gesetz zur Fluggastdatenspeicherung. Einladung zur anlasslosen Rasterfahndung durch das BKA, in: DÖV Nr. 24, S. 1023–1030.

Baldus, Manfred (2014) Entgrenzungen des Sicherheitsrechts – Neue Polizeirechtsdogmatik?, in: Die Verwaltung, 42 Jg., Nr. 1, S. 1–23.

Fährmann, Jan (2020) Digitale Beweismittel und Datenmengen im Strafprozess, in: Multimedia und Recht (MMR), 23. Jg., Nr. 4, S. 228–233.

Fährmann, Jan/Aden, Hartmut/Bosch, Alexander (2020) Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung, in: Kriminologisches Journal, 52. Jg., Nr. 2, S. 135-148.

Heinrich, Stephan (2009) Technik und Systeme der Inneren Sicherheit, in: Lange, Hans-Jürgen u.a. (Hg.): Auf der Suche nach neuer Sicherheit. 2. Aufl., Wiesbaden: Springer, S. 203–219.

Jarolimek, Stefan (2019) Von analog zu digital, vom Kobold zum Thermomix. Thesen zur Zukunft der Polizei zwischen Identität und Anpassung, in: Lange, Hans-Jürgen/Model, Thomas/Wendekamm, Michaela (Hg.): Zukunft der Polizei. Trends und Strategien, Wiesbaden: Springer, S. 173–188.

Krüger, Philipp (2016) Datensouveränität und Digitalisierung. Probleme und rechtliche Lösungsansätze, in: Zeitschrift für Rechtspolitik, S. 190–192.

Kugelmann, Dieter (2001) Die informatorische Rechtsstellung des Bürgers, Tübingen: Mohr Siebeck.

Liebl, Karlhans; Ohlemacher, Thomas (2000) Empirische Polizeiforschung: Forschung in, für und über die Polizei. In: Karlhans Liebl und Thomas Ohlemacher (Hg.): Empirische Polizeiforschung: interdisziplinäre Perspektiven in einem sich entwickelnden Forschungsfeld. Herbolzheim: Centaurus-Verl.

Rappold, Viktoria/Schuster, Susanne (2019) Kritische Reflexionen zur Rolle rechtswissenschaftlicher Forschungspartner*innen in der zivilen Sicherheitsforschung, in: Vorgänge, Nr. 227, 58. Jg., Nr. 3, S. 47-58.

Rademacher, Timo/Perkowski, Lennart (2020) Staatliche Überwachung, neue Technologien und die Grundrechte, in: Juristische Schulung (JuS), S. 713–720.

Roßnagel, Alexander (1993) Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos.

Schaar, Peter (2014) Datenschutz in Zeiten von Big Data, in: HMD, 51. Jg., Nr. 6, S. 840–852.

Schaar, Peter (2017) Trügerische Sicherheit. Wie die Terrorangst uns in den Ausnahmezustand treibt, Hamburg: Edition Körber.

Weber Max (1980) Wirtschaft und Gesellschaft, 5. Aufl., Tübingen: Mohr Siebeck.

Weingärtner, Dieter (2021) Die Evaluation von Sicherheitsgesetzen. Grund- und menschenrechtliche Anforderungen, Berlin: Deutsches Institut für Menschenrechte, https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Analyse_Studie/Analyse_Evaluation_von_Sicherheitsgesetzen.pdf (letzter Aufruf: 04.03.2023).