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.