Entscheidung | Straf- und Strafprozessrecht

Wiss. Ang. Dominik Brodowski, LL.M. (UPenn)

BGH, Urteil v. 4. 6. 2013 – 1 StR 32/13

Vorsätzliches unbefugtes Erheben von Daten durch eine Detektei

BDSG § 28 Abs. 1 S. 1 Nr. 2, § 29 Abs. 1 S. 1 Nr. 1, § 43 Abs. 2 Nr. 1, § 44 Abs. 1; TKG § 148 Abs. 1; EGRL 46/95 Art. 7 lit. f.

1. Zum Vorliegen nicht allgemein zugänglicher personenbezogener Daten bei der Erstellung von sog. Bewegungsprofilen bei Überwachung von Zielpersonen durch Anbringung von GPS-Empfängern an den von diesen genutzten Kraftfahrzeugen durch eine Detektei.

2. Zu den Voraussetzungen einer datenschutzrechtlichen Befugnis zum Erstellen von Bewegungsprofilen mittels GPS-Empfängern in engen Ausnahmefällen.

BGH, Urteil v. 4. 6. 2013 – 1 StR 32/13

Aus den Gründen:[1]

A.

3 Das Landgericht hat folgende Feststellungen und Wertungen getroffen:

I.

4 Fälle 1 bis 29 der Urteilsgründe

5 1. Der Angeklagte H. betrieb eine Detektei, der Angeklagte K. war – ebenso wie der gesondert Verfolgte Kn. – als Detektiv bei ihm angestellt. Die Detektei wurde häufig von Privatpersonen beauftragt, andere Personen (Zielpersonen) zu überwachen. Eine der praktizierten Observationsmaßnahmen bestand in der Erstellung von Bewegungsprofilen der Zielpersonen. Dabei ging die Detektei wie folgt vor: Durch vorangegangene persönliche Observation und Halterabfragen wurde das von den Zielpersonen regelmäßig genutzte Fahrzeug und dessen regelmäßiger Standort ermittelt. Sodann brachte – jeweils auf Anweisung des Angeklagten H. – überwiegend (jedoch nicht in den Fällen 19, 21 und 25 sowie 29 der Urteilsgründe) der Angeklagte K., teilweise gemeinsam mit dem Mitarbeiter Kn., einen GPS-Empfänger (basierend auf Global-Positioning-System = GPS) an diesen Fahrzeugen an. Soweit die Angeklagten für möglich hielten, dass die Zielpersonen mehrere Fahrzeuge benutzten, etwa Fahrzeuge von Personen aus dem familiären Umfeld der Zielpersonen, wurde an jedem dieser Fahrzeuge ein GPS-Empfänger angebracht. Dass die Angeklagten durch ihr Verhalten in die Rechte dieser »unbeteiligten« Familienangehörigen eingriffen, die die Fahrzeuge ebenfalls nutzten, war ihnen bewusst. Die Urteilsgründe enthalten keinen Anhaltspunkt dafür, dass die Angeklagten jemals einen GPS-Empfänger an einem Fahrzeug angebracht hätten, das von mehr als weiteren zwei, in einem Fall von mehr als drei Personen neben der Zielperson benutzt wurde.

6 Zur Anbringung des GPS-Empfängers betrat der Angeklagte K. wiederholt im Bewusstsein, hierzu nicht berechtigt zu sein, Tiefgaragen, die teilweise durch Rolltore oder Gitter gesichert oder nur durch Berechtigte mit einer Karte zu betreten waren.

7 Die GPS-Empfänger zeichneten im Durchschnitt alle zwei Minuten, teils sogar minütlich, das Datum, die Uhrzeit, die geographischen Breiten- und Längenkoordinaten sowie die jeweilige Momentangeschwindigkeit des Fahrzeugs auf. Diese Daten wurden über Mobiltelefone der Angeklagten auf deren Notebooks übertragen und dort mittels eines speziellen Softwareprogramms automatisch zu Bewegungsprotokollen und Kartendarstellungen verarbeitet, wobei auch »Fahrweg und Aufenthaltsort der Zielpersonen« dokumentiert wurden. Diese Arbeiten nahmen im Wesentlichen der Angeklagte K. und der weitere

1 Die Formel lautet:
1. Auf die Revision des Angeklagten H. wird das Urteil des Landgerichts Mannheim vom 18. Oktober 2012, soweit es ihn betrifft, mit den Feststellungen aufgehoben:
a) in den Fällen 13 bis 17, 19, 23 bis 27 und 29 der Urteilsgründe
b) im Ausspruch über die Gesamtfreiheitsstrafe.
2. Auf die Revision des Angeklagten K. wird das vorbezeichnete Urteil, soweit es ihn betrifft, mit den Feststellungen aufgehoben:
a) in den Fällen 13 bis 17, 23, 24, 26 und 27 der Urteilsgründe
b) im Ausspruch über die Gesamtfreiheitsstrafe.
3. Die weitergehenden Revisionen werden verworfen.
4. Im Umfang der Aufhebung wird die Sache zu neuer Verhandlung und Entscheidung, auch über die Kosten der Rechtsmittel, an eine andere Strafkammer des Landgerichts zurückverwiesen.

Mitarbeiter Kn. vor. Die so gewonnenen Daten überließ der Angeklagte H. – teils in Form von Protokollen und Kartendarstellungen, teils in Form von Observationsberichten – den jeweiligen Auftraggebern in Papierform.

8 2. Die Motive der Auftraggeber für die Überwachung der Zielpersonen waren unterschiedlich:

9 a) Fälle 1 bis 12 der Urteilsgründe:

10 Auftraggeber der Observationen waren Geschäftsführer der im Bereich von Labormedizin tätigen L. GmbH. Gegen einen der Geschäftsführer hatte die Kassenärztliche Vereinigung Nordbaden Maßnahmen im Rahmen ihrer Aufgaben ergriffen. Dieser Geschäftsführer wollte kompromittierendes Material aus dem Berufs- und Privatleben von näher bezeichneten Personen, die der Kassenärztlichen Vereinigung Nordbaden angehörten bzw. für diese tätig waren, gewinnen. Dieses Material wollte er dazu einsetzen, um die Zielpersonen in seinem Sinne beeinflussen zu können. Ein weiterer Observationsauftrag betraf mit gleicher Zielrichtung einen Rechtsanwalt, den Insolvenzverwalter über das Vermögen dieses Geschäftsführers. Sowohl an den Fahrzeugen der betroffenen Angehörigen der Kassenärztlichen Vereinigung Nordbaden sowie bei diesem Rechtsanwalt wurden GPS-Empfänger angebracht.

11 Weitere Observationsaufträge betrafen Angehörige der Staatsanwaltschaft Mannheim, die gegen den Geschäftsführer wegen Abrechnungsbetruges ermittelten, sowie Angehörige konkurrierender Labore. Damit im Zusammenhang stehende Vorgänge sind Gegenstand eines gesonderten Verfahrens.

12 b) Fälle 18, 20 bis 22, 28 der Urteilsgründe:

13 Hier wollten die Auftraggeber durch eine Überwachung ihrer Ehegatten (Fälle 18 und 22 der Urteilsgründe) oder der Schwiegertochter (Fälle 20 und 21 der Urteilsgründe) deren Untreue belegen. In einem Fall (Fall 28 der Urteilsgründe erstrebte der Auftraggeber Klärung darüber, ob seine Lebensgefährtin, gegen die wegen dieses Verdachts später auch ermittelt wurde, Beischlaf mit Verwandten gehabt hatte.

14 c) Fälle 13 bis 17, 19, 23 bis 27 sowie 29 der Urteilsgründe:

15 Eine Observation richtete sich gegen einen Mitarbeiter/Berater eines Unternehmens, der bei dem Auftraggeber (Fälle 15 und 16 der Urteilsgründe) in Verdacht stand, hohe Geldbeträge veruntreut und Maschinen unterschlagen zu haben. In zwei weiteren Fällen stand ein Mitarbeiter eines Unternehmens im Verdacht, im Krankenstand »schwarz« einer Nebentätigkeit nachgegangen zu sein (Fälle 23 und 24 der Urteilsgründe) bzw. gegen ein Wettbewerbsverbot verstoßen zu haben (Fall 25 der Urteilsgründe). Hier konnte der Betroffene der »Spionage« zugunsten einer Konkurrenzfirma überführt werden; die Observation diente der Vorbereitung einer Strafanzeige. In den Fällen 26 und 27 der Urteilsgründe hatte der Auftraggeber seine Ehefrau in Verdacht, als Mitarbeiterin eines gemeinsamen Unternehmens Gelder veruntreut zu haben. Eine Auftraggeberin (Fälle 13 und 14 der Urteilsgründe) befürchtete, ihr Ehemann habe im Rahmen einer vermögensrechtlichen Auseinandersetzung ihr zustehende Vermögenswerte beiseite geschafft. Im Fall 17 der Urteilsgründe wollte der Auftraggeber im Interesse zukünftiger Zwangsvollstreckungsmaßnahmen den aktuellen Arbeitsplatz einer ehemaligen Mitarbeiterin, die noch erhebliche Schulden bei ihm hatte, herausfinden. Ein weiterer Auftraggeber versuchte, über die Überwachung zu belegen, dass seine getrennt lebende Ehefrau eine andere Beziehung habe und ihm »das Haus wegnehmen« wolle (Fall 29 der Urteilsgründe); der GPS-Empfänger wurde hier an einem im Eigentum des Auftraggebers stehenden Fahrzeug angebracht. Der Auftraggeber im Fall 19 der Urteilsgründe ließ seine Ehefrau im Rahmen einer Scheidungsauseinandersetzung überwachen.

16 3. Das Landgericht hat in sämtlichen Fällen (bei dem Angeklagten K. nur in den Fällen, an denen er beteiligt war) vorsätzliches unbefugtes Erheben von Daten gegen Entgelt (§ 44 Abs. 1, § 43 Abs. 2 Nr. 1 BDSG) bejaht.

17 Näher hat es ausgeführt:

18 Die GPS-Daten seien personenbezogene Daten (§ 3 Abs. 1 BDSG). Das zunächst fahrzeugbezogene Bewegungsprofil sei entsprechend dem Zweck der Maßnahme den Zielpersonen ohne Weiteres zuzuordnen gewesen.

19 Diese Daten seien nicht allgemein zugänglich gewesen. Durch bloßes Beobachten und/oder »Hinterher-Fahren« wäre schon wegen der Verkehrsdichte und des erhöhten Entdeckungsrisikos die Erstellung eines ebenso vollständigen Bewegungsprofils nicht oder allenfalls theoretisch unter unverhältnismäßigem Aufwand möglich gewesen. Die Datenerhebung bzw. -verarbeitung seien unbefugt gewesen. Namentlich könnten sich die Angeklagten nicht auf Erlaubnissätze, insbesondere nicht auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG berufen.

20 In diesem Zusammenhang sei abzuwägen zwischen

- einerseits dem Interesse der Detektei an der Auftragserfüllung und den dahinter stehenden Interessen der Auftraggeber
- andererseits dem verfassungsrechtlich garantierten Recht der Zielpersonen auf informationelle Selbstbestimmung.

21 Da der GPS-Einsatz bereits für sich genommen widerrechtlich gewesen sei, seien die Interessen der Angeklagten bzw. der Auftraggeber nicht billigenswert. Hierbei sei auch zu berücksichtigen, dass bei keinem der Fälle eine Straftat von erheblicher Bedeutung im Sinne von § 100 h

StPO vorgelegen habe. Selbst Ermittlungsbehörden wären daher nicht befugt gewesen, sich eines GPS-Geräts, das als technisches Mittel im Sinne dieser Vorschrift gelte, zu bedienen. Den Angeklagten, die ohnehin nur über »Jedermanns-Rechte« verfügten, habe dann erst recht keine Befugnis zugestanden. ...

III.

25 Gegen das Urteil richten sich die auf näher ausgeführte Sachrügen gestützten Revisionen der Angeklagten. ...

C.

27 Soweit die Angeklagten wegen vorsätzlichen unbefugten Erhebens von Daten gegen Entgelt (§ 44 Abs. 1, § 43 Abs. 2 Nr. 1 BDSG) verurteilt worden sind, besteht kein Verfahrenshindernis; insbesondere liegen in Bezug auf sämtliche verfahrensgegenständlichen Taten die erforderlichen wirksamen Strafanträge (§ 44 Abs. 2 Satz 1 BDSG) vor.

28 Antragsbefugt ist gemäß § 44 Abs. 2 Satz 2 BDSG neben dem Betroffenen, der verantwortlichen Stelle und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch die Aufsichtsbehörde im Sinne von § 38 BDSG. Die zuständigen Aufsichtsbehörden können per Gesetz von der Landesregierung oder von einer durch diese ermächtigten Stelle bestimmt werden, § 38 Abs. 6 BDSG.

29 Vorliegend hatte, neben einzelnen Geschädigten, am 14. Juli 2010 der Leiter der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich (Innenministerium Baden-Württemberg) in sämtlichen verfahrensgegenständlichen Fällen Strafanträge gestellt.

30 Diese Aufsichtsbehörde war in Baden-Württemberg zu dem Zeitpunkt der Antragstellung bei dem Innenministerium angesiedelt (vgl. Ambs in Erbs-Kohlhaas, 183. Lfg., § 38 BDSG Rn. 1). Erst aufgrund Gesetzes zur Änderung des Landesdatenschutzgesetzes und anderer Rechtsvorschriften vom 7. Februar 2011, das am 1. April 2011 in Kraft trat (GBl. BW Nr. 2, S. 43), wurde die Aufsicht über die nichtöffentlichen Stellen dem Landesbeauftragten für den Datenschutz übertragen (vgl. § 31 Abs. 1 DSG BW nF; Bergmann/Möhrle/Herb, LDSG BW, 43. Lfg., § 31 Anm. 3.1).

31 Die Antragstellung erfolgte damit durch die zuständige Aufsichtsbehörde und ist, weil wenige Tage nach Kenntnisnahme des Sachverhalts gestellt, innerhalb der drei Monate betragenden Antragsfrist, deren Lauf mit Kenntniserlangung von der Tat und der Person des Täters (§ 77 b StGB) beginnt, erfolgt.

D.

32 Soweit die Angeklagten wegen Taten nach § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 1 BDSG verurteilt wurden, haben die Revisionen in den aus dem Urteilstenor ersichtlichen Einzelfällen Erfolg, was zugleich zur Aufhebung der Gesamtstrafe führt. Im Übrigen bleiben sie erfolglos. Die für die Entscheidung über die Revisionen beider Angeklagter maßgeblichen Gründe sind weitgehend identisch. Lediglich hinsichtlich des Merkmals der Entgeltlichkeit (§ 44 Abs. 1 BDSG) ist eine differenzierte Betrachtung geboten (unten D. I. 3.).

I.

33 Nach den rechtsfehlerfrei getroffenen Feststellungen haben die Angeklagten zwar jeweils vorsätzlich handelnd gegen Entgelt gemeinschaftlich personenbezogene Daten, die nicht allgemein zugänglich sind, erhoben und verarbeitet. Allerdings hat das Tatgericht bei der Beurteilung des Merkmals »unbefugt« einen nicht in jeder Hinsicht rechtsfehlerfreien Maßstab herangezogen. Aufgrund dessen tragen die bislang getroffenen Feststellungen in den Fällen 13 bis 17, 19, 23 bis 27 sowie 29 der Urteilsgründe die Annahme einer fehlenden Befugnis zur Datenerhebung und -verarbeitung nicht. Dies betrifft mit Ausnahme der Fälle 19, 25 und 29 der Urteilsgründe – hieran hatte der Angeklagte K. nicht mitgewirkt – beide Angeklagte.

34 In den Fällen 1 bis 12 der Urteilsgründe sowie in den Fällen 18, 20 bis 22 und 28 der Urteilsgründe ist das Tatgericht im Ergebnis zutreffend von einem unbefugten Handeln ausgegangen; dies betrifft mit Ausnahme des Falls 21 der Urteilsgründe beide Angeklagten.

35 1. Das Landgericht hat die durch die GPS-Empfänger gewonnenen »Bewegungsdaten« zu Recht als personenbezogene Daten, also als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Legaldefinition des § 3 Abs. 1 BDSG), bewertet.

36 a) Der Begriff der »Angabe« umfasst jede Information. Eine Information ist geistiger Natur (Dammann in Simitis, BDSG, 7. Aufl., § 3 Rn. 5 mwN). Reale Vorgänge und Zustände sind daher für sich genommen keine derartigen Angaben; sie können aber etwa durch Aufzeichnen oder Messen Ausgangspunkt für das Herstellen solcher Einzelangaben sein (Dammann aaO).

37 Auf persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person beziehen sich Einzelangaben dann, wenn sie über die Bezugsperson selbst etwas aussagen oder mit der Bezugsperson in Ver-

bindung zu bringen sind, weil sie einen auf sie beziehbaren Sachverhalt enthalten (Gola/Schomerus, BDSG, 11. Aufl., § 3 Rn. 5 und 7). Daher zählen nicht nur einer Person als solcher zukommende Eigenschaften und Merkmale zu deren persönlichen und sachlichen Verhältnissen, sondern auch ihre Beziehungen zur Umwelt, wie u. a. ihr Aufenthaltsort (vgl. Dammann aaO Rn. 11; Gola/Schomerus aaO Rn. 7; Schaffland/Wiltfang, BDSG, Lfg. 4/11, § 3 Rn. 5; Backu, ITRB 2009, 88, 90).

38 Werden geografische Standort- oder Positionsdaten (hier GPS-Positionsdaten) erhoben, verarbeitet oder genutzt, vermitteln diese, weil sie sich in erster Linie auf Gegenstände – wie vorliegend den GPS-Empfänger bzw. das Fahrzeug, an dem der GPS-Empfänger angebracht ist – beziehen, unmittelbar keine Aussage über die persönlichen oder sachlichen Verhältnisse einer natürlichen Person (vgl. Schrey/Meister, K&R 2002, 177, 180). Durch den Einsatz satellitengestützter Positionsbestimmungs-Systeme lassen sich mit einer horizontalen und vertikalen Genauigkeit von wenigen Metern (vgl. Jandt/Schnabel, K&R 2008, 723, 724) Positionsdaten »lediglich« darüber gewinnen, wo sich ein GPS-Empfänger befindet (zu den technischen Gegebenheiten vgl. Jandt/Schnabel aaO).

39 Gegenstände, wie die hier verwendeten GPS-Empfänger, können aber einem bestimmten Einfluss durch Personen unterliegen, so dass etwa aufgrund der physischen oder räumlichen Nähe des GPS-Empfängers zu einer Person oder zu anderen Gegenständen, etwa dem von einer bestimmten/bestimmbaren Person genutzten Fahrzeug, an dem der GPS-Empfänger angebracht ist, eine indirekte Beziehung zu einer Person hergestellt werden kann. Fahrzeugortungsdaten als Sachdaten werden daher als Verhaltensdaten zu personenbezogenen Daten, wenn der Insasse dem Fahrzeug zugeordnet werden kann (zum Personenbezug von GPS-Standortdaten vgl. Dammann aaO § 3 Rn. 15 und 59, 69; zur Ortung von Arbeitnehmern bei der Anbringung von GPS-Empfängern an Dienst-Fahrzeugen vgl. Meyer, K&R 2009, 14, 19; zur GPS-Ortung im Arbeitsverhältnis vgl. auch Gola, NZA 2007, 1139, 1143).

40 b) Gemessen hieran stellten die durch den Angeklagten H. und seine Mitarbeiter gewonnenen GPS-Positionsdaten der von den Zielpersonen benutzten Fahrzeuge personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG dar. Das gilt sowohl für Standortdaten solcher Fahrzeuge, die lediglich von einer Person genutzt wurden, als auch solcher mit Nutzung durch weitere den Angeklagten aufgrund der vorausgegangenen Recherchen *namentlich bekannte* Personen.

41 Bei Nutzung des jeweiligen Fahrzeugs ausschließlich durch die Zielperson war es den Angeklagten ohne weiteres möglich, die GPS-Daten den entsprechenden Zielpersonen zuzuordnen. Die GPS-Daten enthielten damit eine Information über den jeweiligen Aufenthaltsort und das Fahrverhalten der jeweiligen Zielperson, mithin über eine für die Angeklagten bestimmbare natürliche Person im Sinne von § 3 Abs. 1 BDSG. Auf die in Einzelheiten kontrovers beurteilten Maßstäbe der Bestimmbarkeit der Person im Zusammenhang mit der Zuordnung von zunächst Sachdaten zu einer Person (dazu Forgó/Krügel, MMR 2010, 17, 18 ff. mwN) kommt es vorliegend dabei nicht an.

42 Aber auch soweit eine Nutzung der überwachten Fahrzeuge durch eine oder zwei weitere Personen aus dem Umfeld der Zielpersonen erfolgte, handelte es sich bei den Standortdaten um personenbezogene Daten. Die Angeklagten stellten in diesen Fällen personenbezogene Informationen selbst her, indem sie die GPS-Positionsdaten einer bestimmten Person zuordneten und damit Aussagen über deren Aufenthaltsort trafen.

43 Die Angeklagten hatten die GPS-Empfänger nicht wahllos an Fahrzeugen angebracht; vielmehr hatten sie »Vorfeldermittlungen« angestellt und in deren Verlauf die Halterdaten erhoben sowie die Zielpersonen persönlich observiert. Soweit die Angeklagten zur Beobachtung einer »Zielperson« aufgrund ihrer Erkenntnisse an mehreren Fahrzeugen jeweils einen GPS-Empfänger anbrachten, um Bewegungsprofile der Zielpersonen auch im Falle eines Fahrzeugwechsels zu erhalten, war es ihnen bewusst, dass auch »Unbeteiligte« mitobserviert wurden (UA S. 7). Teilweise überwachten sie auch Angehörige der Zielpersonen (UA S. 15). Soweit drei weitere Personen im familiären Umfeld der Zielpersonen dasselbe Fahrzeug nutzten, war auch dies den Angeklagten bekannt. Verfolgungstechnische »Leerläufe« konnten die Angeklagten im Übrigen dazu nutzen, ergänzende Erkenntnisse zur betreffenden Zielperson zu erlangen. Es liegt angesichts dieser begleitenden Ermittlungen der Angeklagten nicht nahe, dass sie nicht in der Lage gewesen wären, eine zutreffende Zuordnung der GPS-Daten zu dem jeweiligen Fahrzeugführer vorzunehmen. Selbst wenn sie aber in Einzelfällen die GPS-Daten fehlerhaft zugeordnet haben sollten, ändert dies an der Beurteilung als personenbezogene Daten nichts.

44 Ein fehlender Wahrheitswert des Datums bzw. der Daten schließt das Vorliegen einer Angabe im Sinne des § 3 Abs. 1 BDSG nämlich nicht aus. Nur dann, wenn aus dem Kontext heraus eindeutig ist, dass die Angaben »reine Fantasie des Autors« sind, sagen sie über eine Person nichts aus (Dammann aaO § 3 Rn. 6). Dies war hier aber im Hinblick auf die umfassenden »Vorfeldermittlungen« der Angeklagten gerade nicht der Fall.

45 Eine Aufklärungsrüge wurde insoweit im Übrigen nicht erhoben.

46 2. Das Landgericht ist auch zutreffend davon ausgegangen, dass die Angeklagten, indem sie sich die GPS-Daten beschafften und die so erlangten Daten computergestützt automatisiert zu Bewegungsprotokollen zusammenfügten, Daten im Sinne von § 3 Abs. 3 BDSG erhoben.

47 a) Unter dem Erheben von Daten im Sinne von § 3 Abs. 3 BDSG ist deren zielgerichtete Beschaffung zu verstehen; es bedarf daher einer Aktivität, durch die die erhebende Stelle Kenntnis von dem betreffenden Sachverhalt erhält (Dammann aaO § 3 Rn. 102, Schaffland/Wiltfang, BDSG, Lfg. 1/11, § 3 Rn. 105). Gemäß § 3 Abs. 4 Satz 1 BDSG unterfällt dem Verarbeiten unter anderem das Speichern von Daten, d. h. das Erfassen, Aufnehmen und Aufbewahren der Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Daneben stellt die Veränderung von Daten, d. h. das inhaltliche Umgestalten gespeicherter Daten (§ 3 Abs. 4 Satz 2 Nr. 2 BDSG), eine weitere Form der Datenverarbeitung dar.

48 b) Indem die Angeklagten mittels der GPS-Empfänger minütlich oder alle zwei Minuten in geografischen Breiten- und Längenkoordinaten ausgedrückte Positionsdaten der GPS-Empfänger sammelten, erhoben sie im Sinne des § 3 Abs. 3 BDSG Daten. Durch die Erfassung dieser Positionsdaten über ihre Mobiltelefone auf ihren Notebooks speicherten sie – im Zuge ihrer Erhebung – diese Daten im Sinne von § 3 Abs. 4 Satz 2 Nr. 1 BDSG. Da diese Daten computergestützt mittels der von den Angeklagten eingesetzten Software automatisch zu Bewegungsprotokollen und Kartendarstellungen einschließlich der Dokumentation von Fahrweg und Aufenthaltsort des GPS-Empfänger zusammengefügt wurden, verarbeiteten die Angeklagten diese Daten zudem im Sinne des § 3 Abs. 4 Satz 2 Nr. 2 BDSG automatisiert weiter. Dass das Landgericht nicht ausdrücklich auch auf die weitere Verarbeitung (vgl. § 3 Abs. 4 BDSG) der erhobenen Daten abgehoben hat, belastet die Angeklagten nicht.

49 3. Dass der Angeklagte H., der von den Auftraggebern eine monetäre Gegenleistung verlangte, entgeltlich (vgl. § 11 Abs. 1 Nr. 9 StGB) handelte, bedarf keiner Erörterung.

50 Es mag dahinstehen, ob der Hinweis der Revision auf das dem Angeklagten K. ohnehin gewährte Gehalt für diesen ein entgeltliches Handeln im Sinne von § 44 Abs. 1 BDSG auszuschließen vermag. Die Revision vertritt insoweit die Auffassung, ein entgeltliches Handeln verlange einen Zusammenhang des Gehalts mit den konkreten Fällen, in denen er tätig war. Daran fehle es.

51 Selbst wenn dem zu folgen und wegen fehlenden Zusammenhangs entgeltliches Handeln zu verneinen wäre, hätte der Angeklagte K. jedenfalls in der Absicht gehandelt, den Mitangeklagten H. um das von den Auftraggebern bezahlte Honorar zu bereichern.

52 Dies trägt den Schuldspruch. Die Möglichkeit, dass sich der Angeklagte K. bei entsprechendem Hinweis (§ 265 StPO) erfolgversprechender als bislang geschehen hätte verteidigen können, ist auszuschließen.

53 4. Die Wertung des Landgerichts, die erhobenen Daten seien nicht im Sinne von §§ 43, 44 BDSG allgemein zugänglich gewesen, ist entgegen der Auffassung der Revision ebenfalls nicht zu beanstanden. Die Möglichkeit, dass ein nicht beschränkter Kreis von Personen die Zielpersonen in der Öffentlichkeit hätte wahrnehmen können, diesen unter Umständen sogar hätte »nachfahren« können, führt nicht dazu, dass die aufgezeichneten und weiterverarbeiteten (wie dargelegt personenbezogenen) GPS-Positionsdaten allgemein zugänglich waren. Die Erhebung und die Verarbeitung der hier konkret mit Hilfe technischer Mittel erhobenen personenbezogenen Daten waren lediglich unter Überwindung rechtlicher Zugangshindernisse möglich. Das steht einer allgemeinen Zugänglichkeit entgegen. Dies ergibt sich sowohl aus dem Wortlaut als auch und vor allem aus der Entstehungsgeschichte der geltenden gesetzlichen Regelung, die die Wendung »nicht allgemein zugänglich« enthält.

54 a) Allgemein zugänglich sind diejenigen Daten, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang zu den Daten rechtlich beschränkt ist (Gola/Schomerus aaO § 43 Rn. 18). Über die Begrifflichkeit der »allgemein zugänglichen Daten«, die aufgrund Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl. I 2001, S. 904) auch zum Zwecke der Vereinheitlichung des Sprachgebrauchs (vgl. BT-Drucks. 14/5793 S. 64) an verschiedenen Stellen des BDSG aufgenommen wurde (vgl. § 10 Abs. 5, § 28 Abs. 1 Satz 1 Nr. 3 BDSG) und auch im 5. Abschnitt des BDSG insoweit das frühere Merkmal »offenkundig« ersetzte, soll der Informationsfreiheit desjenigen Rechnung getragen werden, der Daten erhebt und verarbeitet. Das Recht auf informationelle Selbstbestimmung des von dieser Datenerhebung Betroffenen findet damit in dem Recht, sich aus Quellen, die jedermann offen stehen, zu informieren, seine Grenze (vgl. Gola/Schomerus aaO § 28 Rn. 45; vgl. auch Forgó/Krügel/Müllenbach, CR 2010, 616, 620 Fn. 39).

55 Rechtliche Schranken jedweder Art des Zugangs zu den Daten, auch wenn die rechtlichen Hürden nicht besonders hoch sind und mittels Falschangaben einfach umgangen werden können, schließen die allgemeine Zugänglichkeit aus. Auskünfte, die mittels einer einfachen Registerauskunft erteilt werden könnten, sind nicht »all-

gemein zugänglich«, wenn die Auskunft von rechtlichen Voraussetzungen abhängt. So setzt etwa die Erteilung von Auskünften nach § 39 Abs. 1 StVG die Geltendmachung eines berechtigten Interesses im Sinne von § 39 Abs. 1 Halbsatz 2 StVG voraus; dementsprechend sind die im entsprechenden Register enthaltenen Daten nicht »allgemein zugänglich« (vgl. BGH, Urteil vom 8. Oktober 2002 – 1 StR 150/02, NJW 2003, 226, 227, dort in Bezug auf das insoweit ausdrücklich gleich behandelte Merkmal der Offenkundigkeit im Zusammenhang mit § 203 Abs. 2 Satz 2 StGB; Gola/Schomerus aaO § 43 Rn. 18; anders OLG Hamburg, NStZ 1998, 358 [ebenfalls zur »Offenkundigkeit« im Zusammenhang mit § 203 Abs. 2 Satz 2 StGB]; BayObLG, NJW 1999, 1727; vgl. auch Schaffland/Wiltfang, BDSG, Lfg. 2/11, § 43 Rn. 26). Die Ersetzung des früheren Begriffs »offenkundig« durch die Wendung »nicht allgemein zugänglich« in §§ 43, 44 BDSG bezweckte gerade auch, Fallgestaltungen, in denen der Zugang zu den Daten rechtlich beschränkt ist, eindeutig als strafbar zu erfassen (BT-Drucks. 14/4329 [Anl. II; Stellungnahme des Bundesrates] S. 59 sowie Beschlussempfehlung und Bericht des Innenausschusses, BT-Drucks. 14/5793, S. 67; vgl. auch Krauskopf in NJW-Sonderheft für Gerhard Schäfer, S. 40 f.; Gola/Schomerus aaO).

56 Eine strafrechtliche Ahndung ist somit nach dem Wortlaut der §§ 43, 44 BDSG (lediglich) in denjenigen Fällen ausgeschlossen, in denen es sich um Daten handelt, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang aus rechtlichen Gründen beschränkt ist (»Jedermanns-Dateien«, vgl. Weichert, NStZ 1999, 490).

57 b) Bei der Bestimmung des Bezugspunkts der allgemeinen Zugänglichkeit personenbezogener Daten ist zu berücksichtigen, dass Informationen ihrerseits geistiger Natur sind und ein finales, auf Vermittlung oder Aufbewahrung gerichtetes Element in sich tragen (vgl. hierzu Dammann aaO § 3 Rn. 5). Unter Berücksichtigung dessen sind Daten allgemein zugänglich, die sowohl in ihrer Zielsetzung als auch in ihrer Publikationsform geeignet sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln (Simitis in ders., BDSG, 7. Aufl., § 28 Rn. 151; vgl. auch BVerfGE 103, 44, 60). Die allgemeine Zugänglichkeit bezieht sich also auf Informationen und daher auf Vorgänge und Zustände, die bei einem anderen als demjenigen, auf den sie sich beziehen, schon als Information vorhanden sind oder zumindest sein könnten. Diese sind dann allgemein zugänglich, wenn »jedermann«, ohne rechtlichen Zugangsbeschränkungen unterworfen zu sein, hierauf zugreifen kann, wie dies z. B. bei Angaben in Massenmedien, auf Internetseiten oder in Registern der Fall sein kann, die nicht lediglich einem wie auch immer abgegrenzten Personenkreis zur Verfügung stehen (etwa das Handels- oder das Vereinsregister, vgl. Simitis aaO § 28 Rn. 153 mwN).

58 c) Gemessen an diesen Maßstäben ist die Annahme des Landgerichts, die Angeklagten hätten Daten erhoben, die nicht allgemein zugänglich waren, im Ergebnis nicht zu beanstanden.

59 Allerdings entfällt die allgemeine Zugänglichkeit entgegen der Auffassung des Landgerichts nicht allein deswegen, weil das Erreichen des Aufklärungsziels (Bewegungsprofil im öffentlichen Straßenverkehr), etwa durch bloßes »Nachfahren«, wegen vorhandener Verkehrsdichte etc. allenfalls theoretisch erreichbar gewesen wäre. Maßgebend für die Beurteilung der »allgemeinen Zugänglichkeit« sind nach dem Vorstehenden rechtliche Zugangsbeschränkungen. Bereits der Anbringung eines GPS-Empfängers als notwendige technische Voraussetzung für die Gewinnung der Personenbezug aufweisenden Geodaten an einem fremden Fahrzeug stehen aber grundsätzlich rechtliche Grenzen entgegen. Dem betroffenen Fahrzeugeigentümer bzw. -besitzer stehen regelmäßig Abwehransprüche (vgl. §§ 1004, 859, 862 BGB) gegen die Störung seines Eigentums oder Besitzes zu. Dementsprechend wäre diese Möglichkeit der Erhebung und späteren Verarbeitung von Daten der Allgemeinheit verschlossen.

60 5. Das Landgericht ist jedoch bei der Beurteilung, ob die Handlungen der Angeklagten unbefugt waren, nicht von einem zutreffenden rechtlichen Maßstab ausgegangen. Aufgrund dessen hat es nicht in sämtlichen der Verurteilung gemäß §§ 43, 44 BDSG zugrunde liegenden Fällen ein unbefugtes Handeln der Angeklagten rechtsfehlerfrei angenommen.

61 a) Unbefugtes Handeln im Sinne des § 43 Abs. 2 Nr. 1 BDSG liegt vor, wenn nicht Rechtssätze das Verhalten erlauben (vgl. Ambs in Erbs/Kohlhaas, 164 Lfg., § 43 BDSG Rn. 19; Sokol in Simitis, BDSG, 7. Aufl., § 4 Rn. 3; Gola/Schomerus aaO § 43 Rn. 20, 26).

62 Das Datenschutzrecht ist zum Schutze des Rechts des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, von dem Grundsatz des Verbots mit Erlaubnisvorbehalt geprägt, d. h. die Erhebung, Speicherung, Verarbeitung und Weitergabe personenbezogener Daten ist grundsätzlich verboten (Helfrich in Hoeren/Sieber, Handbuch Multimedia-Recht, 26. Lfg. Teil 16.1 Rn. 35 mwN). Befugt ist sie nur dann, wenn der Betroffene wirksam seine Einwilligung erklärt oder wenn das BDSG oder eine andere Rechtsvorschrift eine Erlaubnis beinhalten oder gar eine Anordnung zur Erhebung, Speicherung, Verarbeitung oder Weitergabe personenbezogener Daten enthalten. Als Erlaubnissätze kommen neben datenschutzrechtlichen Erlaubnissen auch allgemeine Rechtfertigungsgründe, wie etwa § 34 StGB, in Betracht.

63 Aufgrund seiner Ausgestaltung als grundsätzliches Verbot der Erhebung bzw. Verarbeitung personenbezogener Daten gehen die im BDSG selbst enthaltenen Erlaubnissätze in der Regel in ihrer Reichweite über diejenigen der allgemeinen Rechtfertigungsgründe hinaus und gewähren damit typischerweise in größerem Umfang die Befugnis, in das Recht auf informationelle Selbstbestimmung des Betroffenen einzugreifen, als dies nach allgemeinen Rechtfertigungsgründen der Fall ist.

64 b) Als solche sich aus dem Datenschutzrecht selbst ergebende Erlaubnissätze kamen vorliegend namentlich Rechtfertigungsgründe nach dem 3. Abschnitt des BDSG in Betracht, der die legislativen Anforderungen an die Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich konkretisiert (vgl. Simitis aaO § 27 Rn. 1).

65 Dass die tatbestandlichen Voraussetzungen des den Anwendungsbereich dieses Abschnitts eröffnenden § 27 BDSG vorlagen, namentlich der Angeklagte H. als Inhaber der Detektei als eine nicht-öffentliche Stelle im Sinne von § 27 Abs. 1 Satz 1 Nr. 1 BDSG handelte und die Datenerhebung und Verarbeitung nicht im Sinne von § 27 Abs. 1 Satz 2 BDSG ausschließlich für persönliche oder familiäre Tätigkeiten erfolgte, bedarf keiner weiteren Erörterung.

66 c) Als spezifische datenschutzrechtliche Erlaubnisse kommen der vom Tatgericht herangezogene § 28 BDSG oder aber § 29 BDSG in Betracht. Das Datenschutzrecht grenzt die Anwendungsbereiche der beiden Vorschriften im rechtlichen Ausgangspunkt danach ab, ob der in Rede stehende Datenumgang zu eigenen Geschäftszwecken (§ 28 BDSG) erfolgt oder es sich um eine geschäftsmäßige Datenverarbeitung zur Übermittlung an Dritte (§ 29 BDSG) handelt. Maßgebend für die Abgrenzung ist dementsprechend die jeweilige Zweckbestimmung. Erweist sich die Datenverarbeitung für Dritte als Selbstzweck, kann sich eine Erlaubnis zum Umgang mit »fremden« personenbezogenen Daten aus § 29 BDSG ergeben. Ist die Datenverarbeitung bloßes Hilfsmittel zur Erfüllung anderer Zwecke, greift dagegen regelmäßig § 28 BDSG als möglicherweise zugunsten der datenverarbeitenden nicht-öffentlichen Stelle wirkende Befugnisnorm. Diese Grundsätze über das Verhältnis der Anwendungsbereiche von § 28 BDSG einerseits und § 29 BDSG andererseits erlauben allerdings im konkreten Einzelfall nicht ohne weiteres, die als Erlaubnissatz in Frage kommende datenschutzrechtliche Vorschrift zu bestimmen. Dementsprechend wird die Anwendbarkeit der beiden in Betracht kommenden Vorschriften auf die mit der Erhebung bzw. Verarbeitung personenbezogener Daten verbundene überwachende Tätigkeit von Detektiven in der datenschutzrechtlichen Literatur auch nicht einheitlich beurteilt.

67 aa) Wird ein Detektiv damit beauftragt, gegen eine natürliche Person Ermittlungen anzustellen, so sammelt und verwendet der Detektiv »gewerblich« personenbezogene Daten der überwachten Personen, um sie seinem Auftraggeber, also Dritten, gegen Entgelt weiterzugeben (vgl. Kloepfer/Kutzschbach, MMR 1998, 650). Die observierende Tätigkeit des Detektivs und der damit verbundene Datenumgang stellt sich, obwohl für die Zwecke des Auftraggebers erfolgend, für den Detektiv wegen des eigenen verfolgten wirtschaftlichen Zwecks der Auftragserfüllung als Selbstzweck dar. Diese Tätigkeit ist auch auf Wiederholung ausgerichtet.

68 Konkret auftragsbezogene Observationstätigkeit eines Detektivs bzw. der damit einhergehende Umgang mit personenbezogenen Daten der überwachten Personen könnte sich daher als geschäftsmäßige Datenverarbeitung zur Übermittlung im Sinne von § 29 BDSG erweisen. Als Erlaubnisvorschrift in Fällen der vorliegenden Art käme dann § 29 Abs. 1 Satz 1 Nr. 1 BDSG in Betracht. Der Angeklagte würde hiernach befugt handeln, wenn für ihn kein Grund zu der Annahme besteht, dass die überwachte Person ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung seiner Daten hat.

69 bb) Gegen eine Anwendung des § 29 BDSG wird allerdings vorgebracht, dass konkret auftragsbezogene Ermittlungstätigkeiten eines Detektivs bei vorausschauender Betrachtungsweise – anders als dies etwa bei eindeutig von § 29 BDSG erfassten Tätigkeiten klassischer Auskunfteien der Fall ist – nicht darauf gerichtet seien, Daten in einer Vielzahl von Fällen zu übermitteln (vgl. Duhr in Roßnagel, Handbuch Datenschutzrecht, 7.5 Rn. 6; Ehmann in Simitis, BDSG, 7. Aufl., § 29 Rn. 97; Bergmann/Möhrle/Herb, BDSG, 41. Lfg., § 29 Rn. 38; aA ohne nähere Begründung Gola/Schomerus aaO § 29 Rn. 8; Fricke, VersR 2010, 308, 313; vgl. auch LG Lüneburg, Beschluss vom 28. März 2011 – 26 Qs 45/11; Maisch/Seidl, jurisPR-ITR 1/2012 Anm. 2). Bei einem Detektiv wäre die Zulässigkeit der Verarbeitung personenbezogener Daten der beobachteten Personen stattdessen anhand von § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu prüfen. Dieser Datenumgang wäre ihm auf der Grundlage dieser Vorschrift gestattet, wenn er zur Wahrung berechtigter Interessen des Detektivs erforderlich wäre und kein Grund zur Annahme bestünde, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

70 cc) Der Senat braucht im Ergebnis nicht zu entscheiden, ob die Befugnis zu konkret auftragsbezogener Ermittlungstätigkeit von Detekteien in Fällen der vorliegenden Art anhand der sich aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG oder anhand der sich aus § 29 Abs. 1 Satz 1 Nr. 1 BDSG ergeben-

den, nach dem Wortlaut der Vorschriften divergierenden Abwägungsmaßstäbe zu beurteilen ist. Beide grundsätzlich in Betracht kommende Erlaubnissätze müssen im Hinblick auf die Voraussetzungen einer Befugnis zum Umgang mit »fremden« personenbezogenen Daten anhand der unionsrechtlichen Vorgaben aus Art. 7 lit. f) der am 13. Dezember 1995 in Kraft getretenen Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG 1995 Nr. L 281 S. 31; im Folgenden: Datenschutzrichtlinie) ausgelegt werden. Um diese Auslegung anhand der Datenschutzrichtlinie vornehmen zu können, bedarf es keiner Vorlage an den Gerichtshof der Europäischen Union (EuGH) bezüglich des Verständnisses von Art. 7 lit. f) der Richtlinie selbst. Der EuGH hat mit Urteil vom 24. November 2011 (verbundene Rechtssachen C-468/10, C-469/10, LS veröffentlicht in ABl. EG 2012 Nr. C 25 S. 18, EuZW 2012, 37) die Bestimmung der Richtlinie eindeutig ausgelegt. Auf der Grundlage dieser Rechtsprechung, die sich als gesicherte Rechtsprechung zu der hier relevanten Rechtsfrage der aus dem Unionsrecht resultierenden Befugnis zur Datenverarbeitung erweist (acte éclairé), vermag der Senat die Auslegung des nationalen Rechts selbst vorzunehmen.

71 (1) Art. 7 lit. f) der Datenschutzrichtlinie erklärt eine Verarbeitung personenbezogener Daten u.a. für rechtmäßig, wenn sie erforderlich ist »zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Art. 1 Abs. 1 (der Datenschutzrichtlinie) geschützt sind, überwiegen«.

72 Abweichend von dem Wortlaut von § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfordert Art. 7 lit. f) der Datenschutzrichtlinie, in die Interessenabwägung nicht lediglich die berechtigten Interessen des Datenverarbeitenden, sondern auch die Interessen von Dritten, die als Empfänger der Daten in Betracht kommen, einzubeziehen. Zudem schließt Art. 7 lit. f) der Datenschutzrichtlinie eine Befugnis zur Verarbeitung »fremder« personenbezogener Daten erst dann aus, wenn die Interessen des davon Betroffenen gegenüber den Interessen desjenigen, der die Daten verarbeitet, überwiegen. Dagegen führen nach dem Wortlaut von § 29 Abs. 1 Satz 1 Nr. 1 BDSG bereits entgegenstehende Interessen des Betroffenen zu einer Unzulässigkeit der Datenerhebung bzw. -verarbeitung (vgl. hierzu Schaffland/Wiltfang, BDSG, Lfg. 5/12, § 29 Rn. 8). Diese ist danach bereits dann unzulässig, wenn die Interessen des Betroffenen diejenigen des Datenverarbeitenden nicht überwiegen.

73 Das nationale Recht darf allerdings jedenfalls im Verhältnis zwischen dem auf der Grundlage von § 44 BDSG (möglicherweise) strafenden Staat und dem von Strafe bedrohten »Datenverarbeiter« nicht hinter den durch Art. 7 lit. f) der Datenschutzrichtlinie gewährten Befugnissen zur Verarbeitung personenbezogener Daten der Betroffenen zurückbleiben. Dabei ist es für die Anwendung der Erlaubnissätze des nationalen Datenschutzrechts jedenfalls in ihrer Bedeutung als strafrechtliche Rechtfertigungsgründe unerheblich, ob in die Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG die Interessen von Dritten, hier der Auftraggeber des Angeklagten, einbezogen werden oder auf der Grundlage von § 29 Abs. 1 Satz 1 Nr. 1 BDSG, der solche Drittinteressen ohnehin berücksichtigt, die Interessenabwägung anhand des durch die Datenschutzrichtlinie vorgegebenen Maßstabs (»Überwiegen der Interessen des Betroffenen«) erfolgt. Auf beiderlei Weise trägt das nationale Recht dem insoweit bindenden Unionsrecht vollumfänglich Rechnung.

74 (2) Nach der Rechtsprechung des EuGH enthält Art. 7 lit. f) der Richtlinie 95/46/EG »inhaltlich unbedingte und hinreichend genau(e)« Vorgaben, um selbst im Fall fehlender oder fehlerhafter Vorschriften der Mitgliedstaaten unmittelbar anwendbar zu sein, so dass sich der Einzelne direkt auf diese Bestimmung der Richtlinie berufen dürfte (vgl. hierzu EuGH aaO Rn. 51f.). Nach Maßgabe der verbindlichen Auslegung von Art. 7 lit. f) der Datenschutzrichtlinie durch den EuGH (aaO) ergeben sich für Fälle der auftragsbezogenen Detektivarbeit folgende Maßstäbe der Zulässigkeit (Befugnis) damit einhergehender Verarbeitung personenbezogener Daten:

75 (a) Die Zulässigkeit der Datenverarbeitung erfordert zum einen, dass die Verarbeitung personenbezogener Daten zur Verwirklichung des von dem Detektiv oder dessen Auftraggeber wahrgenommenen berechtigten Interesses erforderlich ist, und zum anderen, dass die Grundrechte und Grundfreiheiten der von der Observation betroffenen Person nicht überwiegen.

76 (b) Auf Seiten des von der Observation Betroffenen sind sämtliche in Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union (nachfolgend: GrCh) gewährleisteten Interessen einzustellen. Erfasst sind damit sowohl das Recht des Betroffenen auf Schutz der ihn betreffenden personenbezogenen Daten (Art. 8 GrCh) als auch sein Recht auf Schutz seiner Privatsphäre (Art. 7 GrCh). Auch vor dem Inkrafttreten der Grundrechtecharta wurden diese Rechte im Kontext des Datenschutzes bereits (zumindest) sekundärrechtlich durch die Datenschutzrichtlinie gewährleistet (vgl. Art. 1 Abs. 1 der Datenschutzrichtlinie).

77 (c) Stammen die verarbeiteten Daten – wie hier – aus nicht öffentlich zugänglichen Quellen, ist zu berücksichti-

gen, dass der Detektiv und sein Auftraggeber zwangsläufig Informationen über die Privatsphäre der betroffenen Person erlangen. Diese schwerwiegendere Beeinträchtigung der verbürgten Rechte der betroffenen Person ist zu berücksichtigen, indem sie gegen das berechtigte Interesse, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, im Einzelfall abgewogen wird. Dies bedeutet, dass sämtliche Rechtspositionen des von der Observation Betroffenen, die der Privatsphäre zuzuordnen sind, zu gewichten und in die Abwägung einzustellen sind.

78 d) Nach diesen Vorgaben ist eine umfassende Abwägung der gegenläufigen Interessen vorzunehmen.

79 Entgegen der von dem Tatgericht vertretenen Rechtsauffassung darf eine Abwägung mit den Interessen des Detektivs bzw. seines Auftraggebers in Fällen des Einsatzes von Mitteln, die im Anwendungsbereich der Strafprozessordnung der Vorschrift des § 100 h StPO unterfallen, nicht lediglich dann vorgenommen werden, wenn die Voraussetzungen für einen staatlichen Ermittlungseingriff gemäß § 100 h Abs. 1 StPO vorgelegen hätten. Eine solche Beschränkung der auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG oder § 29 Abs. 1 Satz 1 Nr. 1 BDSG vorzunehmenden Abwägung wird den unionsrechtlichen Vorgaben aus Art. 7 lit. f) der Datenschutzrichtlinie nicht ausreichend gerecht. Sie ist aber auch im System des nationalen Rechts nicht tragfähig. Sie machte insoweit die Informationsgewinnung durch Private von tatsächlichen und rechtlichen Voraussetzungen abhängig, die lediglich für den Staat und seine Organe, nicht aber für den privaten Bürger gelten.

80 aa) Die Unvereinbarkeit der vom Tatgericht vorgenommenen Auslegung von § 28 Abs. 1 Satz 1 Nr. 2 BDSG mit der Datenschutzrichtlinie ergibt sich bereits daraus, dass die Zulässigkeit der Datenverarbeitung an Kriterien geknüpft würde, die das Datenschutzrecht der Union nicht vorsieht. Eine Erhöhung der Zulässigkeitsanforderungen im Recht der Mitgliedstaaten gegenüber der Richtlinie schließt die Rechtsprechung des EuGH aber gerade aus (EuGH aaO Rn. 45 f.).

81 bb) Auf der Ebene des nationalen Rechts kann das Verhalten Privater nicht an den tatbestandlichen Voraussetzungen der Beweiserhebungsvorschriften der StPO gemessen werden. Privatpersonen sind grundsätzlich nicht Adressaten dieser Normen (Eisele, Compliance und Datenschutzrecht, S. 56; Weißgerber, NZA 2003, 1005, 1007; siehe auch Kaspar, GA 2013, 206, 208; Greeve, StraFo 2013, 89). Die StPO beschränkt hoheitliches Handeln (vgl. Kubiciel GA 2013, 226, 228; Fricke, VersR 2010, 308, 309) und schützt den Bürger vor staatlicher Willkür. Der Gedanke, dass staatliche Einrichtungen für ihr Handeln grundsätzlich einer Ermächtigung bedürfen, ist auf Private nicht unmittelbar übertragbar (vgl. Kaspar, GA 2013, 206, 208 f.; Kubiciel GA 2013, 226, 227 f.).

82 Die berechtigten Interessen des Detektivs bzw. seines Auftraggebers an der Datenverarbeitung müssen daher auch dann einer Abwägung mit den Interessen des Betroffenen zugänglich sein, wenn es nicht um die Aufklärung von Straftaten besonderer Bedeutung im Sinne von § 100 h Abs. 1 Satz 2 StPO handelt.

83 e) Die Abwägung der gegenläufigen Interessen setzt das tatsächliche Bestehen berechtigter Interessen des Detektivs bzw. seines Auftraggebers an der Datenverarbeitung – bezogen auf den Zeitpunkt ex-ante bei Vornahme der Datenerhebung bzw. Datenverarbeitung – voraus.

84 Dient etwa die Datenverarbeitung der Erstellung eines Bewegungsprofils, so müssen daher Anhaltspunkte dafür bestehen, dass ein berechtigtes Interesse gerade an einem solchen Bewegungsprofil bzw. an seiner Erstellung zur Durchsetzung berechtigter Interessen besteht. Art. 7 lit. f) der Datenschutzrichtlinie bringt diesen Zusammenhang mit dem Abstellen auf die Erforderlichkeit der Datenverarbeitung zur Durchsetzung berechtigter Interessen zum Ausdruck.

85 Beweisführungsinteressen zur Klärung des Vorliegens von zivilrechtlichen Ansprüchen oder zu deren Durchsetzung (Vollstreckung) können dabei zwar, anders als bloße Neugier oder rein negative Interessen (wie etwa in den Fällen 1 bis 12 der Urteilsgründe), unter bestimmten weiteren Voraussetzungen ein berechtigtes Interesse an der Datenverarbeitung begründen. Dies gilt aber nur dann, wenn gerade das Bewegungsprofil zur Durchsetzung des Beweisführungsinteresses benötigt wird. Es bedarf also einer Konnexität zwischen den Interessen des Detektivs bzw. seines Auftraggebers an dem Bewegungsprofil und den Interessen des von der Observation Betroffenen am Schutze seiner Privatsphäre, weil ansonsten eine Abwägung der einander gegenüberstehenden Interessen nicht stattfinden kann (vgl. auch BGH, Urteil vom 15. Dezember 1983 – III ZR 207/82, NJW 1984, 1889 ff.; Schaffland/Wiltfang, aaO Lfg. 1/12, § 28 Rn. 89).

86 f) Ob die Interessen des Betroffenen am Schutz seiner Privatsphäre und »seiner« (personenbezogenen) Daten überwiegen, ist eine Frage des Einzelfalls, die durch den Tatrichter zu beantworten ist. Das Revisionsgericht kann in Fällen, in denen ein unterschiedliches Ergebnis der Würdigung vertretbar wäre, die vom Tatrichter vorgenommene Würdigung nicht durch eine eigene ersetzen. Es ist vielmehr auf die Prüfung beschränkt, ob der Tatrichter die in die Abwägung einzubeziehenden Gesichtspunkte gesehen und einen rechtlich zutreffenden Abwägungsmaßstab

angelegt hat. Dementsprechend kann das Revisionsgericht im Grundsatz auch nicht eine durch den Tatrichter unterbliebene Abwägung selbst nachholen (BGH, Beschluss vom 17. August 1999 – 1 StR 390/99, NStZ 1999, 607). Etwas anderes gilt aber dann, wenn auf der Grundlage der getroffenen Feststellungen ohnehin lediglich ein rechtlich vertretbares Ergebnis möglich ist (vgl. BGH, Urteil vom 14. März 2003 – 2 StR 239/02).

87 Bei dem Einsatz von GPS-Empfängern zu Observationszwecken bedarf es im Hinblick auf die vorgenannten Maßstäbe regelmäßig der Berücksichtigung der folgenden, teils gegenläufigen Gesichtspunkte:

88 aa) Einerseits sind die Eingriffe in das Persönlichkeitsrecht des Observierten durch den Einsatz von GPS-Sendern zunächst weniger schwerwiegend als etwa durch das heimliche Abhören des gesprochenen Wortes (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 581/01, BVerfGE 112, 304; vgl. auch EGMR, Urteil vom 2. September 2010 – Beschwerde-Nr. 35623/05, NJW 2011, 1333, 1335 Rn. 52). Dennoch reicht auch hier ein »schlichtes« Beweisführungsinteresse des Auftraggebers nicht aus, um den Eingriff in die Rechte des vom GPS-Einsatz Betroffenen zu gestatten.

89 Nach der Rechtsprechung des Bundesverfassungsgerichts und der neueren Rechtsprechung des Bundesgerichtshofs genügt in Fällen, in denen das von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG – u. a. – geschützte Recht am gesprochenen Wort beeinträchtigt ist, das stets bestehende »schlichte« Interesse, sich ein Beweismittel für zivilrechtliche Ansprüche zu sichern, nicht, um bei der Güterabwägung trotz Verletzung des Persönlichkeitsrechts der anderen Prozesspartei zu einer Schutzbedürftigkeit des Beweisführungsinteresses zu gelangen (vgl. BVerfG, Beschluss vom 9. Oktober 2002 – 1 BvR 1611/96, 805/98, BVerfGE 106, 28 unter C.II. 4.a.bb; BGH, Urteile vom 17. Februar 2010 – VIII ZR 70/07, NJW-RR 2010, 1289, 1292; und vom 20. Mai 1958 – VI ZR 104/57, BGHZ 27, 284, 290). Die Rechtsprechung verweist insoweit auf notwehrähnliche Situationen, die für eine beweisbelastete Person im Zivilprozess bestehen können, wenn die Beeinträchtigung des Persönlichkeitsrechts aus schwerwiegenden Gründen mangels anderer in Betracht kommender Beweismittel im Interesse einer wirksamen Rechtspflege erforderlich ist (vgl. BVerfG aaO; BGH, Urteile vom 18. Februar 2003 – XI ZR 165/02, NJW 2003, 1727 unter II. 1. und 2. mwN; vom 13. Oktober 1987 – VI ZR 83/87, BGHR BGB § 1004 Abs. 1 Satz 1 Abwehranspruch 2; vom 24. November 1981 – VI ZR 164/79, NJW 1982, 277, 278; vom 20. Mai 1958 – VI ZR 104/57, BGHZ 27, 284, 290; vgl. auch Fischer, StGB, 60. Aufl., § 201 Rn. 11; kritisch Schünemann in Leipziger Kommentar zum StGB, 12. Aufl., § 201 Rn. 40; Lenckner/Eisele in Schönke/Schröder, StGB, 28. Aufl., § 201 Rn. 32).

90 Es müssen jedenfalls in diesen Fällen neben dem allgemeinen Beweisführungsinteresse weitere Gesichtspunkte hinzutreten, die das Interesse an der Beweiserhebung trotz der Verletzung des Persönlichkeitsrechts als schutzbedürftig erscheinen lassen. So kann etwa die Anfertigung heimlicher Tonbandaufnahmen zur Feststellung der Identität eines anonymen Anrufers (vgl. BGH, Urteil vom 24. November 1981 – VI ZR 164/79, BGH NJW 1982, 277 ff.) oder zur Feststellung erpresserischer Drohungen (BGH, Urteil vom 20. Mai 1958 – VI ZR 104/57, BGHZ 27, 284) oder im Fall eines auf andere Weise nicht abwehrbaren Angriffs auf die berufliche Existenz (vgl. hierzu BGH, Urteil vom 27. Januar 1994 – I ZR 326/91, NJW 1994, 2289, 2292 f.) hinzunehmen sein, wenn nicht durch andere, weniger belastende Methoden der Sachverhalt anderweit aufgeklärt werden kann.

91 bb) Die von der Rechtsprechung geforderten erhöhten Anforderungen sind jedoch nicht auf Fälle der Beeinträchtigung des Rechts am gesprochenen Wort beschränkt. Auch bei anderweitigen ähnlich gewichtigen Beeinträchtigungen des Persönlichkeitsrechts gelten vergleichbare Maßstäbe (vgl. BVerfG, Urteil vom 13. Februar 2007 – 1 BvR 421/05, BVerfGE 117, 202 Rn. 96 zu heimlichen Vaterschaftstests; vgl. auch die Rechtsprechung des Bundesarbeitsgerichts zur verdeckten Videoüberwachung am Arbeitsplatz: zuletzt BAG, Urteil vom 21. Juni 2012 – 2 AZR 153/11 unter III. 1.a. und b.; vgl. auch BAG, Beschluss vom 14. Dezember 2004 – 1 ABR 34/03; sowie Landesarbeitsgericht Düsseldorf, Beschluss vom 7. März 2012 – 4 TaBV 87/11).

92 cc) Werden aus Gründen der Beweisführung Detektive zur Observation eingesetzt, so kann das Beweisführungsinteresse die Beeinträchtigung des Persönlichkeitsrechts des Observierten etwa dann zulässig machen, wenn ein konkreter Verdacht gegen diesen besteht, die detektivische Tätigkeit zur Klärung der Beweisfrage erforderlich ist und nicht andere, mildere Maßnahmen als genügend erscheinen (vgl. OLG Köln, Urteil vom 3. August 2012 – I-20 U 98/12, 20 U 98/12; vgl. auch BGH, Urteil vom 20. Mai 2009 – IV ZR 274/06 mwN; zu den Maßstäben der Pflicht des Observierten zur Übernahme der Detektivkosten vgl. auch BAG, Urteil vom 28. Oktober 2010 – 8 AZR 547/09 mwN; OLG Karlsruhe, Urteil vom 23. September 2009 – 6 U 52/09, OLG Düsseldorf, Beschluss vom 24. Februar 2009 – II-10 WF 34/08; vgl. auch OLG Oldenburg, Beschluss vom 20. Mai 2008 – 13 WF 93/08; Zöller, ZPO, 29. Aufl., § 91 Rn. 13 [Sb. Herget] sowie § 788 Rn. 13 [Sb. Stöber] zum Stichwort Detektivkosten jew. mwN).

93 dd) In den Fällen des Einsatzes von GPS-Empfängern zum Zwecke der Erstellung eines Bewegungsprofils darf schließlich die Art und Weise der Datenerhebung und -ver-

arbeitung nicht unberücksichtigt bleiben. Eine qualitativ schwerwiegende Beeinträchtigung der Privatsphäre des Observierten liegt nämlich vor, wenn mit der Anbringung eines GPS-Empfängers ein Eindringen in befriedetes Besitztum des zu Observierenden verbunden ist (Beispiel: Der GPS-Empfänger wird am Fahrzeug angebracht, indem sich unberechtigt Zutritt zu Tiefgaragen verschafft wird). Gleiches gilt, wenn das Observationsmittel an Fahrzeugen angebracht wird, die für den Detektiv bzw. dessen Auftraggeber eigentumsrechtlich fremd bzw. nicht auf diese zugelassen sind. Es werden dann zwangsläufig auch wesentlich mehr Vorgänge aufgezeichnet, die in die Privatsphäre des Fahrzeugführers erheblicher eingreifen, als dies etwa der Fall wäre, wenn beispielsweise der Eigentümer an seinem eigenen Fahrzeug einen GPS-Empfänger anbringen ließe. In solchen Fällen müssen daher die den Interessen des Observierten gegenüberstehenden Interessen des Detektivs bzw. seines Auftraggebers umso höher sein, um die Datenverarbeitung rechtfertigen zu können (vgl. EuGH, aaO Rn. 44 f.). Gleiches gilt, wenn von den Observationsmaßnahmen unbeteiligte Dritte betroffen sind.

94 Im Übrigen ist es eine Frage des Einzelfalls, inwieweit Erkenntnisse darüber, wann und wo sich eine Person mit dem Fahrzeug aufgehalten hat, geeignet sein können, die angestrebte Beweisführung (etwa zu finanziellen Fragen) wesentlich zu erleichtern.

95 g) Die Strafkammer hat derartige Abwägungen – von ihrem rechtlichen Ausgangspunkt aus konsequent – für keinen der verfahrensgegenständlichen Fälle vorgenommen. Das erweist sich für die aus dem Tenor ersichtlichen Fälle der Verurteilung der Angeklagten als rechtsfehlerhaft. In den nicht der Aufhebung im Schuldspruch unterliegenden Fällen boten die insoweit rechtsfehlerfreien und ausreichenden Feststellungen dagegen keine Veranlassung, eine aus den genannten datenschutzrechtlichen Vorschriften resultierende Befugnis der Angeklagten zur Überwachung der betroffenen Fahrzeuge und der damit einhergehenden Erhebung bzw. Verarbeitung personenbezogener Daten in Erwägung zu ziehen.

96 Für die einzelnen Fälle der Urteilsgründe ergeben sich folgende Konsequenzen:

97 aa) Fälle 1 bis 12 der Urteilsgründe:

98 Hier ging es den Auftraggebern der Angeklagten um die Verfolgung »illegaler« Zwecke – letztlich um die Ermöglichung wenigstens von Nötigungshandlungen. Denn das erhoffte »kompromittierende Material« sollte allein dazu dienen, die Zielpersonen von ihren gesetzlichen bzw. satzungsmäßigen Aufträgen abzuhalten oder ihr berufliches Verhalten durch Erkenntnisse über ihr berufliches oder ihr Privatleben im Sinne der Auftraggeber des Angeklagten zu beeinflussen.

99 bb) Fälle 18, 20 bis 22, 28 der Urteilsgründe:

100 Bei den entsprechenden Taten beschränkte sich das Interesse der jeweiligen Auftraggeber, ohne dass bereits gerichtliche Verfahren, etwa Unterhaltsrechtsstreitigkeiten, im Raume gestanden hätten, auf die Aufklärung über die Treue des eigenen Ehegatten (Fälle 18 und 22), des Lebensgefährten (Fall 28) oder der Schwiegertochter (Fälle 20 und 21). In diesen Fällen ist ausgeschlossen, dass die unterbliebene Abwägung dazu geführt hätte, den Einsatz eines GPS-Empfängers als gerechtfertigt anzusehen.

101 Da auch im Übrigen Rechtsfehler nicht ersichtlich sind, hat der Schuldspruch in diesen Fällen Bestand. Dies wird durch den von der Revision vorgebrachten urteilsfremden Vortrag zu Lebenssachverhalten, die einzelnen Observationsmaßnahmen zu Grunde gelegen hätten, nicht in Frage gestellt.

102 cc) Fälle 13 bis 17, 19, 23 bis 27 sowie 29 der Urteilsgründe:

103 In den verbleibenden Fällen ging es den Auftraggebern um die Wahrung finanzieller Interessen. Der Senat, dem eine eigene Beweiswürdigung verwehrt ist, kann nach den bisherigen Feststellungen nicht ausschließen, dass sich weitere Erkenntnisse ergeben können, die ein durch die Erstellung von Bewegungsprofilen zu bedienendes Beweisführungsinteresse und daraus resultierend im Rahmen der gebotenen Abwägung eine Befugnis zur Erhebung und Verarbeitung der personenbezogenen Daten ergeben können. Um dem Tatrichter zu ermöglichen, in jedem dieser Fälle einheitliche und in sich geschlossene Feststellungen zu treffen, hebt der Senat in diesen Fällen auch die Feststellungen auf.

104 h) Weitergehende Befugnisse zu der Vornahme der gemäß § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 1 BDSG straftatbestandsmäßigen Datenerhebung bzw. -verarbeitung als die durch die vorstehend erörterten datenschutzrechtlichen Erlaubnissätze auf der Grundlage anderer Rechtfertigungsgründe kommen vorliegend nicht in Betracht.

II.

105 Entgegen dem Vorbringen der Revision hatte das Landgericht keinen Anlass, der Möglichkeit einer Strafmilderung nach §§ 17, 49 Abs. 1 StGB näher zu treten. Nach den Feststellungen rechneten die Angeklagten zumindest damit, dass die »GPS-Einsätze« ungerechtfertigt gewesen sein könnten. Für die Annahme eines § 17 StGB unterfallenden sog. Erlaubnisirrtums bezüglich einer sich aus datenschutzrechtlichen oder sonstigen Erlaubnissätzen ergebenden Befugnis war daher kein Raum.

III.

106 Die Aufhebung des Schuldspruchs in den Fällen 13 bis 17, 19, 23 bis 27 und 29 der Urteilsgründe – hiervon ist mit Ausnahme der Fälle 19, 25 und 29 der Urteilsgründe auch der Angeklagte K. betroffen – zieht bei beiden Angeklagten die Aufhebung des Ausspruchs über die jeweilige Gesamtstrafe nach sich. Anhaltspunkte dafür, dass die Einzelstrafen in den Fällen, in denen der Schuldspruch Bestand hat, durch die Fälle, in denen der Schuldspruch keinen Bestand haben kann, zum Nachteil der Angeklagten beeinflusst sind, bestehen nicht. Da die Einzelstrafen auch ansonsten rechtsfehlerfrei festgesetzt sind, können sie daher Bestand haben.

E.

107 Sollte das neue Tatgericht auf der Grundlage seiner Feststellungen bei Anwendung der vorstehend dargestellten Grundsätze über eine mögliche Befugnis zu der hier vorliegenden Datenerhebung bzw. -verarbeitung im Einzelfall von einem erlaubten Vorgehen der Angeklagten ausgehen, wird es auch die Notwendigkeit eines subjektiven Rechtfertigungselements (häufig sog. Rechtfertigungsvorsatz) in den Blick zu nehmen haben. Bei Heranziehung der einschlägigen datenschutzrechtlichen Bestimmungen als im Strafrecht wirkende Rechtfertigungsgründe bedarf es eines solchen Elements stets. Dieses verlangt wenigstens, dass dem Täter die rechtfertigenden Gründe bekannt sein und sich im Motiv seines Handelns niedergeschlagen haben müssen (BGH, Beschluss vom 25. Oktober 2010 – 1 StR 57/10, BGHSt 56, 11, 22 Rn. 32 mwN).

Anmerkung

In das Datenschutzstrafrecht ist Bewegung gekommen: Weltweit führen die Enthüllungen über die weitreichende Datensammlung, -weitergabe und -auswertung durch die Geheimdienste zu einer Debatte über die digitale Privatsphäre im 21. Jahrhundert. Auf europäischer Ebene ist eine umfassende Reform des Datenschutzrechts in der Diskussion.[2] Auf nationaler Ebene schließlich setzt sich der *1. Strafsenat* des BGH mit diesem Urteil – die GPS-gestützte Erstellung von Bewegungsprofilen durch Privatdetektive betreffend – in bislang detailliertester Weise mit der zentralen datenschutzrechtlichen Strafvorschrift, § 44 BDSG, auseinander[3] und wirkt damit auch dem viel kritisierten Vollzugsdefizit im Datenschutzstrafrecht entgegen.[4] Einerseits zeigt der *1. Strafsenat* in seinem Urteil privaten Akteuren bei der Erhebung, Verarbeitung und Weitergabe personenbezogener Daten strafrechtliche Grenzen auf (sogleich I.). Andererseits aber räumt er ihnen auf methodisch zweifelhaftem Wege Freiräume zu Datenerhebungen ein, selbst wenn hierzu verdeckte technische Mittel eingesetzt werden. Dies ist nicht nur für Detektive, sondern auch allgemein für den Umgang mit personenbezogenen Daten – etwa im Bereich der Compliance und bei Internal Investigations – von erheblicher Bedeutung. Zudem lässt die Entscheidung eine Abkehr des *1. Strafsenats* von der »Versuchslösung« bei fehlendem subjektivem Rechtfertigungselement vermuten (II.). Abschließend sei diese Entscheidung im Lichte der geplanten Neuregelung des Datenschutzrechts auf europäischer Ebene eingeordnet (III.).

I. Zum strafrechtlichen Datenschutz

1. Bestandsaufnahme. Der strafrechtliche Schutz der Privatsphäre ist im doppelten Wortsinne fragmentarisch: Er ist auf eine Vielzahl von Vorschriften verteilt, die teils im StGB (vorrangig[5] §§ 201 ff. StGB), teils im Nebenstrafrecht (neben § 44 Abs. 1 BDSG sei exemplarisch auf § 33 Abs. 1 KunstUrhG verwiesen) zu finden sind, und er ist – wie jede dem Gebot des Art. 103 Abs. 2 GG genügende Strafvorschrift – notwendigerweise lückenhaft, weil diese Strafvorschriften nur bestimmte Angriffe gegen die Privatsphäre inkriminieren. In diesem »komplexe(n) Normensystem«[6] hat § 44 Abs. 1 BDSG insoweit eine besondere Stellung inne, als

0 Vorschlag für [eine] Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg. v. 25. 1. 2012 sowie Vorschlag für [eine] Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endg. v. 25. 1. 2012. Zur bisherigen Datenschutzrichtlinie s. noch unten bei und mit Fn. 36 f.

1 S. zuvor BGH StV 2002, 26 m. Anm. *Behm*; BGH NJW 2013, 401 m. Bespr. *Cornelius*, NZWiSt 2013, 166; *Wessing*, NZG 2013, 494.

2 S. nur *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 98; *Sieber*, Straftaten und Strafverfolgung im Internet, 2012, C 29.

3 Daneben weisen mehrere Tatbestände oder Qualifikationen einen engen Bezug zum persönlichen Lebens- und Geheimbereich auf, namentlich etwa Hausfriedensbruch (§ 123 StGB) oder Wohnungseinbruchsdiebstahl (§ 244 Abs. 1 Nr. 3 StGB).

4 *Sieber* (Fn. 4) C 47.

dass sich diese Vorschrift allgemein auf *personenbezogene Daten* bezieht, während bei den sonstigen Strafvorschriften nur bestimmte Daten oder Informationen – etwa Bildaufnahmen aus dem höchstpersönlichen Lebensbereich (§ 201a StGB) oder besonders gesicherte Daten[7] (§ 202a Abs. 1 StGB) – geschützt werden. Damit kann § 44 Abs. 1 BDSG durchaus als zentrale, wenn auch reformbedürftige[8] Vorschrift des Persönlichkeitsschutzes angesehen werden.

2. Zum geschützten Tatobjekt. Dreh- und Angelpunkt dieser Vorschrift ist – jedenfalls bei § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 1 bis Nr. 4 BDSG – das datenschutzrechtlich determinierte Tatbestandsmerkmal der »personenbezogene(n) Daten, die nicht allgemein zugänglich sind«. Zur Konturierung dieser Begriffe trägt dieses Urteil wesentlich bei:

a) Bereits der *Personenbezug* der erhobenen – also von den Angeklagten beschafften (§ 3 Abs. 3 BDSG) – Daten war hier umstritten, denn die an verschiedenen Kfz befestigten GPS-Sensoren übermittelten nur die Position dieses Sensors und folglich auch des Kfz. Wer das Kfz jeweils nutzte, lässt sich diesen sachbezogenen Daten selbst nicht entnehmen.[9] Allerdings reicht es nach der Legaldefinition personenbezogener Daten in § 3 Abs. 1 BDSG aus, dass sich solche (Positions-)Daten auf eine »bestimmbare[...] natürliche[...] Person« beziehen. Nach allgemeiner Auffassung richtet sich die *Bestimmbarkeit* im mikrosystematischen Umkehrschluss zur in § 3 Abs. 6 BDSG definierten Anonymisierung danach, ob Daten mit noch darstellbarem Aufwand »an Zeit, Kosten und Arbeitskraft« durch den Datenverarbeiter einer bestimmten Person zugeordnet werden können.[10] Auf dieser Grundlage trägt der genannte Einwand des Sachbezugs nicht: Durch die Befestigung der Sensoren an bestimmten Kfz, die von den auszuforschenden Zielpersonen genutzt wurden, schufen die Angeklagten – wie der *1. Strafsenat* überzeugend ausführt – eine hinreichende »indirekte Beziehung« zwischen den erhobenen Daten und der Zielperson. Mehr noch: die gesamte Datenerhebung verfolgte nur diesen einen Zweck, Erkenntnisse über den Aufenthaltsort bestimmter Zielpersonen zu erlangen.[11]

b) Auch der zweite Einwand, mit dem sich der BGH auseinanderzusetzen hatte, ist fadenscheinig: Einige der überwachten Kfz wurden von mehreren Personen genutzt, so dass gelegentlich die Zuordnung, wer das Kfz für eine konkrete Fahrt genutzt hatte, erschwert war. Gelegentlich soll auch möglicherweise eine falsche Zuordnung getroffen worden sein. Hierzu führt der *1. Strafsenat* lediglich aus, es liege erstens »nicht nahe, dass [die Angeklagten] nicht in der Lage gewesen wären, eine ... Zuordnung der GPS-Daten zu dem jeweiligen Fahrzeugführer vorzunehmen«, dass zweitens eine (teilweise) falsche Zuordnung unschädlich sei und dass drittens eine Aufklärungsrüge nicht erhoben wurde – der es indes nicht bedarf, wenn die Feststellungen lückenhaft sind, mithin den Schuldspruch nicht tragen.[12] Im Ergebnis ist jedoch dem BGH auch bei dieser Sachfrage zuzustimmen, wenn auch nicht in dieser zu knappen Argumentation. Drei alternative Begründungsstränge bieten sich hingegen an:

(1) Erstens ließe sich darauf abstellen, dass der *1. Strafsenat* den gesamten Ausforschungsvorgang einer Zielperson als *eine* Tat des § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 1 BDSG wertete, selbst wenn sich dieser über etliche Fahrten verteilt auf mehrere Wochen erstreckte und neben dem Einsatz des GPS-Sensors auch noch die Auswertung (sprich: Verarbeitung) der gewonnenen Rohdaten umfasste.[13] Dann aber sind sämtliche Tatbestandsmerkmale des § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 1 Alt. 2 BDSG – also der entgeltlichen bzw. mit Bereicherungs- oder Schädigungsabsicht vorgenommenen,[14] unbefugten Verarbeitung personenbezogener Daten – jedenfalls dann erfüllt, wenn die Angeklagten in jedem der Fälle *irgendeine* Fahrt irgendeiner Person (korrekt oder inkorrekt) zuordneten.

(2) Zweitens und dogmatisch stimmiger ist es, vollständig auf den Zeitpunkt der Daten*erhebung* abzustellen. Wann immer aber das Zielfahrzeug in Bewegung war, wäre es den Angeklagten jeweils möglich gewesen, durch vertretbaren Einsatz von »Zeit, Kosten und Arbeitskraft« – etwa durch eine kurzfristige Observation des Zielfahrzeugs während der gemeldeten Fahrt –, den Personenbezug mit einiger Treffsicherheit herzustellen. Dass diese konkrete Möglichkeit zur im Strafrecht maßgeblichen Tatzeit be-

7 Hier allerdings Daten i. S. d. § 202a Abs. 2 StGB.

8 Zum Reformbedarf s. *Sieber* (Fn. 4) C 93 ff.

9 Vgl. *Dammann*, in: Simits (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl. 2011, § 3 Rdn. 15, 59, 69.

10 S. nur *Ambs*, in: Erbs/Kohlhaas (Hrsg.), Strafrechtliche Nebengesetze, 194. Erg.Lfg. 2013, § 3 BDSG Rdn. 3; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rdn. 10 m. w. N., auch zur einen objektiven Maßstab vertretenden Gegenauffassung; relativierend *Cornelius*, NJW 2013, 3340, 3341.

11 Infolgedessen wäre auch der engere und subjektivierte Maßstab für Positionsdaten, wie ihn *Forgó/Krügel*, MMR 2010, 17, 18 ff. vorschlagen, erfüllt.

12 Vgl. nur *Kuckein*, in: Karlsruher Kommentar StPO, 6. Aufl. 2008, § 337 Rdn. 28.

13 Jedenfalls europarechtlich ist die Erhebung von Daten ein Unterfall der Verarbeitung von Daten (Art. 2 lit. b 95/46/EG); strafrechtlich dürfte das Verhältnis zwischen Erhebung und nachfolgender – von demselben Tatvorsatz erfasster – Verarbeitung personenbezogener Daten das einer tatbestandlichen Handlungseinheit sein.

14 Zur Bereicherungsabsicht und Entgeltlichkeit in diesem Fall vgl. *Cornelius*, NJW 2013, 3340, 3341; *Wybitul*, ZD 2013, 509, 511.

stand, ist für die in § 3 Abs. 1 BDSG geforderte Bestimmbarkeit ausreichend;[15] für den diesbezüglichen Vorsatz reicht es aus, dass der Täter jedenfalls ein entsprechendes sachgedankliches Mitbewusstsein hatte.

(3) Drittens und meines Erachtens am überzeugendsten ist es jedoch, für einen Personenbezug von Daten auch Wahrscheinlichkeitsaussagen ausreichen zu lassen: Die von den Angeklagten erhobenen Daten – »Die Zielperson nutzt häufig das Kfz K« sowie »Das Kfz K befindet sich derzeit in X« – ergeben nämlich in ihrer Kombination die »persönliche oder sachliche Verhältnisse« der Zielperson betreffende und damit § 3 Abs. 1 BDSG unterfallende Aussage, dass sich diese derzeit mit einer nicht geringen Wahrscheinlichkeit in X aufhält.[16] Solche Wahrscheinlichkeitsaussagen sind dem Datenschutzrecht indes nicht nur aus der *Scoring*-Problematik (vgl. § 28b BDSG) bestens bekannt, sondern geradezu täglich Brot des *data mining*[17] und der personalisierten Werbung[18]: Aus dem Surfverhalten des Benutzers im Internet werden dabei beispielsweise Wahrscheinlichkeiten errechnet, für welche Produkte oder Produktgruppen sich der Benutzer interessieren *könnte*. Das ist ebenso »nur« eine Wahrscheinlichkeitsaussage wie die Aussage, dass sich die Zielperson derzeit in X aufhalten *könnte*; hier wie dort ist diese unsichere Aussage aber datenschutzrechtlich höchst relevant.

c) Schließlich wendet sich der *1. Strafsenat* noch gegen den Einwand, dieselben Daten hätten hypothetisch auch dadurch erhoben werden können, dass die Angeklagten den Zielpersonen »nachgefahren« wären, diese also im Wortsinne verfolgt hätten. Dennoch seien die erhobenen Daten nicht »allgemein zugänglich[...]« gewesen: Unter Hinweis auf die Gesetzgebungsgeschichte weist er darauf hin, dass maßgebliches Kriterium für »allgemein zugängliche Daten« sei, dass »›jedermann‹, ohne rechtlichen Zugangsbeschränkungen unterworfen zu sein«, auf diese zugreifen könne.[19] Die von den Angeklagten konkret erhobenen Geodaten setzten aber die Installation eines GPS-Sensors an ihnen fremden Fahrzeugen voraus, was ihnen zivilrechtlich nicht gestattet gewesen sei.

Diese Argumentation ist spitzfindig und so nicht anzugreifen. Sie ist aber dahingehend zu ergänzen, dass in der Automatisierung der elektronischen Auswertung, des nur geringen Zeit- und Kostenaufwands solcher technischer Überwachungsmaßnahmen und der daraus resultierenden Multiplikatoreffekte ein gänzlich anderes Gefahrenpotential für die Privatsphäre geschaffen ist: Aus diesem Grund ist die verdeckte technische Überwachung einer Zielperson nicht gleichzusetzen mit personalintensiven alternativen Ermittlungsmethoden wie dem »Nachfahren« im öffentlichen Straßenverkehr.[20]

d) Der *1. Strafsenat* definiert daher den Personenbezug von Daten weit und erstreckt – im Einklang mit der Systematik des BDSG (arg. ex § 35 Abs. 1 S. 1 BDSG) – den Schutzbereich der Strafvorschriften auch auf *unzutreffende* personenbezogene Daten (arg. ex § 35 Abs. 1 S. 1 BDSG).[21] Das überzeugt, jedoch ließ er dabei die Chance verstreichen, auf die besonderen Gefahren einer technikbasierten Datenerhebung und einer automatisierten Auswertung explizit hinzuweisen; auch wäre eine Klarstellung wünschenswert gewesen, dass bereits eine Möglichkeitsangabe – etwa, dass entweder A oder B sich an einem bestimmten Ort aufhalten – ein personenbezogenes Datum darstellt.

3. Zur Bedeutung von Vorbereitungs- und Begleithandlungen. Den Schutz der Privatsphäre – auch mit strafrechtlichen Mitteln – hält der *1. Strafsenat* schließlich noch an anderer Stelle hoch, indem er das Gewicht deren Beeinträchtigung[22] maßgeblich daran misst, welche Vorbereitungs- und Begleiteingriffe zur Durchführung einer Observation notwendig sind. In diesem Kontext führt er einen unberechtigten Zutritt in eine Tiefgarage (!) als Beispiel an für eine »qualitativ schwerwiegende Beeinträchtigung der Privatsphäre des Observierten« (!).

Das ist bemerkenswert, weil in der Strafrechtspflege bislang eine gegenläufiger Tendenz zu verzeichnen war, solche Vorbereitungs- und Begleiteingriffe zu marginalisieren, jedenfalls wenn sie von Ermittlungsbehörden bei strafprozessualen Ermittlungen – etwa im Zuge einer sogenannten Quellen-Telekommunikationsüberwachung –

15 Vgl. oben bei und mit Fn. 10

16 In diese Richtung auch *Gola/Schomerus* (Fn. 10) § 3 Rdn. 3; skeptisch für Aggregation und einen solchen Mehrpersonenbezug Simitis/*Dammann* (Fn. 9) § 3 Rdn. 14, 20.

17 S. hierzu allgemein *Weichert*, ZD 2013, 251.

18 S. hierzu allgemein *Skistims/Voigtmann/David/Roßnagel*, DuD 2012, 31.

19 BGH JR 2003, 290, 291 m. Anm. *Brehm*, JR 2003, 292.

20 Allerdings setzt die Strafvorschrift § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nr. 1 BDSG nicht notwendigerweise eine automatisierte Verarbeitung personenbezogener Daten i.S.d. § 3 Abs. 2 BDSG voraus. Dies hindert jedoch nicht, das genannte teleologische Argument durch § 3 Abs. 2 BDSG und die hierauf Bezug nehmenden Vorschriften des BDSG systematisch zu untermauern.

21 Der Schutz vor der Verarbeitung unzutreffender personenbezogener Daten ist teilweise sogar wichtiger als der Schutz vor der Verarbeitung zutreffender Daten, etwa wenn aus falschen Daten unzutreffende Schlüsse im Rahmen eines Scoring (§ 28b BDSG) gezogen werden.

22 Hier im Zusammenhang mit der erforderlichen Abwägung der gegenläufigen Interessen; s. hierzu unten II. 3. c.

ergriffen werden.[23] Es bleibt zu hoffen, dass der *1. Strafsenat* auch in solch strafprozessualem Kontext an diesem grundrechtsbewussten Maßstab festhält.

II. Die Relativität des strafrechtlichen Datenschutzes

1. Zu den Rechtfertigungsgründen im Datenschutzstrafrecht. Indes ist der strafrechtliche Schutz gegen eine GPS-basierte Observation durch Privatdetektive nicht absolut; neben einem kurzen Hinweis auf die allgemeinen Rechtfertigungsgründe – das Urteil nennt hier ausdrücklich § 34 StGB – konzentriert sich der *1. Strafsenat* dabei auf die spezifischen, aber weitreichenden datenschutzrechtlichen Erlaubnissätze, die er ebenfalls als (spezifische) Rechtfertigungsgründe ansieht.[24]

a) Auf eine Konsequenz dieser dogmatischen Einordnung weist der *1. Strafsenat* zum Ende seiner Entscheidung ausdrücklich hin: Neben einer objektiven Komponente sei auch »stets« ein subjektives Rechtfertigungselement erforderlich; »(d)ieses verlangt wenigstens, dass dem Täter die rechtfertigenden Gründe bekannt sein und sich im Motiv seines Handelns niedergeschlagen haben müssen«. Allerdings: fehlt es dem Täter an einem subjektiven Rechtfertigungselement, so soll er nach vorherrschender Auffassung in Rechtsprechung[25] und Literatur[26] nur wegen *Versuchs* zu bestrafen sein. Doch der Versuch ist – mangels ausdrücklicher Anordnung der Strafbarkeit – bei dem Vergehen des § 44 Abs. 1 BDSG nicht strafbar, so dass der Täter hier auch dann straflos ist, wenn er allein objektiv gerechtfertigt handelt. Diese – nicht tragenden – Erwägungen ergeben somit nur Sinn, soweit der *1. Strafsenat* erwägt, von der sogenannten »Versuchslösung« bei fehlendem subjektivem Rechtfertigungselement wieder Abstand zu nehmen und den Täter wegen eines vollendeten Delikts zu verurteilen. Zu dieser Rechtsfrage hatte er sich in den vergangenen Jahren ohnehin bemerkenswert zweideutig verhalten.[27]

b) Daneben erinnert die Einordnung als Rechtfertigungsgrund auch an die klassische Diskussion über die Rechtfertigungsgründe tragenden Prinzipien.[28] Hieraus können indes nur begrenzte Schlüsse gezogen werden, wenn ein Rechtfertigungsgrund – wie bei den §§ 28 ff. BDSG der Fall – in detaillierter Weise durch den Gesetzgeber konkretisiert wurde.[29] Ein wiederkehrender Abwägungstopos bei auf dem Prinzip des überwiegenden Interesses beruhenden Rechtfertigungsgründen ist es allerdings, bei einem Eingriff in Schutzgüter Privater zu hinterfragen, ob der Täter stattdessen staatliche Hilfe in Anspruch hätte nehmen können.[30] Darauf wird zurückzukommen sein;[31] bereits jetzt ist aber darauf hinzuweisen, dass der *1. Strafsenat* kein »staatliches Gewaltmonopol« dahingehend anerkennt, dass verdeckte Überwachungen unter Einsatz technischer Mittel allein staatlichen Stellen vorbehalten wären.

c) Das BDSG bietet mit § 28 Abs. 1 S. 1 Nr. 2 BDSG – eine Datenerhebung für *eigene* Geschäftszwecke betreffend – und § 29 Abs. 1 S. 1 Nr. 1 BDSG – eine Datenerhebung *zum Zwecke der Übermittlung* betreffend – zwei Rechtfertigungsgründe, die bei der vorliegenden Fallgestaltung zumindest erwägenswert sind. Die Abgrenzung zwischen diesen beiden Vorschriften ist auch allgemein[32] und insbesondere betreffend Detekteien[33] umstritten, und sie ist bei isolierter Betrachtung beider Normen auch po-

23 LG Hamburg wistra 2011, 155, 156 ff. Zu BGHSt 46, 266, 273 f. s. die abl. Anm. *Kühne* JZ 2001, 1148; *Schäfer*, in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 100 c Rdn. 8 m. w. N.; vgl. ferner *Wolter* in: SK StPO, 4. Aufl. 2010, § 100 a Rdn. 29.

24 So auch *Gola*/*Schomerus* (Fn. 10) § 43 Rdn. 26; *Becker* in: Plath (Hrsg.), BDSG, 2013, § 43 Rdn. 13; *Eisele*, Computer- und Medienstrafrecht, 2013, § 17 Rdn. 67; a. A. *Heghmanns*, in: Achenbach/Ransiek (Hrsg.), Handbuch Wirtschaftsstrafrecht, 3. Aufl. 2012, Kap. 6/1 § 95; *Tiedemann*, NJW 1981, 945 (946 f., 949 f). Zur rechtfertigenden Wirkung der Vorschriften des BDSG für Strafvorschriften des StGB vice versa vgl. *Eisele*, Compliance und Datenschutzstrafrecht, 2012, S. 76 ff.

25 BGHSt 38, 144, 155; OLG Celle, Beschl. v. 25. 1. 2013, 2 Ws 17–21/13 u. a. m. Anm. *Jahn*, JuS 2013, 1042; OLG Sachsen-Anhalt, StraFo 2013, 344; a. A. noch die frühere Rspr., etwa BGHSt 2, 111, 114.

26 Statt vieler *Kühl*, AT, 7. Aufl. 2012, § 6 Rdn. 14 ff.; *Wessels*/*Beulke*/*Satzger*, AT, 43. Aufl. 2013, Rdn. 278 f.; a. A. *Heinrich*, AT, 3. Aufl. 2013, Rdn. 392; jew. m. w. N.

27 Vgl. BGHSt 56, 11, 22 f. sowie BGH NStZ 2005, 332 (334); zu letzterer Entscheidung vgl. die Darlegung in OLG Celle, Beschl. v. 25. 1. 2013, 2 Ws 17–21/13 u. a., warum dies nicht als Abweichung von der »Versuchslösung« zu sehen sei.

28 Siehe nur *Roxin*, AT I, 4. Aufl. 2006, § 14 Rdn. 38 ff.; *Lenckner*/*Sternberg-Lieben* in: Schönke/Schröder, StGB, 28. Aufl. 2010, Vor § 32 Rdn. 6 ff.; jew. m. w. N.

29 Vgl. *Kühl* (Fn. 26) § 6 Rdn. 10; Schönke/Schröder/*Lenckner*/*Sternberg-Lieben* (Fn. 28) Vor § 32 Rdn. 7 a. E.

30 So insbesondere bei § 32 StGB – s. hierzu nur Schönke/Schröder/*Perron* (Fn. 28), § 32 Rdn. 41; einschränkend aber etwa *Erb*, in: Münchener Kommentar StGB, 2. Aufl. 2011, § 32 Rdn. 140 ff. – sowie bei § 34 StGB – s. hierzu nur *Fischer*, StGB, 60. Aufl. 2013, § 34 Rdn. 9.

31 S. hierzu unten II. 3. a.

32 Vgl. hierzu *Gola*/*Schomerus* (Fn. 10) § 28 Rdn. 4 ff.; Simits/*Ehmann* (Fn. 9) § 29 Rdn. 20 ff.; *Wolff*, in: Wolff/Brink, Datenschutzrecht, 2013, § 28 Rdn. 12 ff.

33 Für § 28 BDSG tendenziell etwa Simits/*Ehmann* (Fn. 9) § 29 Rdn. 97 f.; Plath/*Plath* (Fn. 24) § 29 Rdn. 29; für § 29 BDSG etwa LG Lüneburg NJW 2011, 2225 m. Anm. Ernst; *Vahle* DSB 2013, 207; Wolff/Brink/*Buchner* (Fn. 32) § 29 Rdn. 32.

tentiell entscheidungserheblich: Auf den ersten Blick ist – so der *1. Strafsenat* – bei § 28 Abs. 1 S. 1 Nr. 2 BDSG eine Interessenabwägung vorzunehmen, bei der auf der einen Seite nur[34] Interessen des Datenverarbeiters – hier der Detekteien –, auf der anderen Seite die Interessen des Betroffenen einzustellen sind; bei § 29 Abs. 1 S. 1 Nr. 1 BDSG sind auch Interessen Sonstiger – etwa der jeweiligen Auftraggeber – berücksichtigungsfähig,[35] allerdings sieht der Wortlaut keine Interessenabwägung vor, sondern lässt ein »schutzwürdiges Interesse« des Betroffenen ausreichen, um den Datenumgang zu verwehren.[36]

2. Europarechtlich überformte Interessensabwägung. Diese Differenzierungen des deutschen Datenschutzrechts wischt der *1. Strafsenat* indes mit einem Federstrich beiseite und fordert das Tatgericht auf, eine Interessenabwägung allein am Maßstab des Art. 7 lit. f RL 95/46/EG (EG-Datenschutzrichtlinie)[37] vornehmen. Diese Regelung enthält ihrerseits den wenig normenklaren und normenbestimmten Maßstab, dass eine Datenerhebung gestattet ist, soweit diese erforderlich »ist zur Verwirklichung des berechtigten Interesses« des Detektivs und seines Auftraggebers, »sofern nicht das Interesse oder die Grundrechte oder Grundfreiheiten der betreffenden Person … überwie[g]en«.[38]

a) Das *methodisches Vorgehen* des *1. Strafsenats* überzeugt dabei nicht:[39] So spricht er zwar richtigerweise von der Notwendigkeit, die genannten Bestimmungen des BDSG »anhand der unionsrechtlichen Vorgaben« auszulegen; dies vermischt er aber sodann mit einer unmittelbaren Anwendbarkeit von Art. 7 lit. f RL 95/46/EG und dem Postulat, das »nationale Recht« dürfe »nicht hinter den durch Art. 7 lit. f [RL 95/46/EG] gewährten Befugnissen zur Verarbeitung personenbezogener Daten der Betroffenen zurückbleiben«. Diese beiden Methoden sind jedoch voneinander zu trennen: In einem ersten Schritt sind Vorschriften wie §§ 28, 29 BDSG, die ihrem Sinn und Zweck nach auch der Umsetzung unionsrechtlicher Vorgaben dienen, auszulegen. Lässt dabei der klassische Methodenkanon (Wortlaut, Genese, Systematik, Teleologie, aber auch Verfassungskonformität) mehrere Auslegungsvarianten zu, ist diejenige zu wählen, die mit den unionsrechtlichen Vorgaben im Einklang steht (sog. *europarechtskonforme Auslegung*).[40] In einem zweiten Schritt ist sodann zu überprüfen, ob das nationale Recht in seiner Auslegung den Vorgaben des Unionsrechts entspricht. Nur wenn sich hierbei eine fehlerhafte oder fehlende Umsetzung des Unionsrechts ergibt, lässt sich in einem dritten Schritt die – das nationale Recht ersetzende – unmittelbare Anwendbarkeit bzw. unmittelbare Wirksamkeit der unionsrechtlichen Vorgaben diskutieren.[41] Dann und nur dann kann sich der Einzelne unmittelbar auf die Richtlinie berufen; andernfalls ist er – sowohl aus europarechtlicher wie aus national-verfassungsrechtlicher Sicht – auf das unionsrechtskonforme nationale Recht zu verweisen.

b) Zunächst zum ersten Schritt: Der *1. Strafsenat* blickt zielgerichtet auf *eine* unionsrechtliche Vorgabe – Art. 7 lit. f RL 95/46/EG –, der zufolge die Mitgliedstaaten vorsehen müssen, dass »die Verarbeitung personenbezogener Daten lediglich erfolgen darf«, wenn die genannte Interessenabwägung zu Gunsten des Datenverarbeitenden ausfällt. Eine weitere unionsrechtliche Vorgabe verdient jedoch ebenfalls, betrachtet zu werden: Art. 5 RL 95/46/EG führt aus, dass die »Mitgliedstaaten nach Maßgabe [der Art. 5 ff.] die Voraussetzungen näher [bestimmen], unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist«; hierzu bestimmt ferner Erwägungsgrund 22 RL 95/46/EG, dass die Mitgliedstaaten »besondere Bedingungen für die Datenverarbeitung in spezifischen Bereichen … vorsehen« dürfen.

Im zentralen Urteil[42] zu diesen Bestimmungen führte der *EuGH* aus, dass es den Mitgliedstaaten verwehrt ist,

34 S. nur Simits/*Simitis* (Fn. 9) § 28 Rdn. 22; Plath/*Plath* (Fn. 24) § 28 Rdn. 48.

35 S. nur Wolff/Brink/*Buchner* (Fn. 32) § 29 Rdn. 55.

36 Simits/*Simitis* (Fn. 9) § 29 Rdn. 155 m. w. N.

37 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (AblEU 1995 Nr. L 281 v. 23.11.95, S. 31) i. d. F. CONSLEG 1995L0046 v. 20. 11. 2003.

38 Im Original: »überwiesen«; dieser offensichtliche Schreibfehler wurde, soweit ersichtlich, bislang nicht korrigiert.

39 *Cornelius*, NJW 2013, 3340, 3341 hält das Vorgehen des BGH für »zumindest missverständlich«.

40 S. nur *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 50. Erg.Lfg. 2013, Art. 288 Rdn. 133 ff.; *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 4. Aufl. 2011; Art. 288 AEUV Rdn. 77 ff.; aus dem Bereich der Literatur des Europäischen Strafrechts s. *Ambos*, Internationales Strafrecht, 3. Aufl. 2011, § 11 Rdn. 46 ff.; *Safferling*, Internationales Strafrecht, 2011, § 11 Rdn. 43 ff.; *Satzger*, Internationales und Europäisches Strafrecht, 6. Aufl. 2013, § 9 Rdn. 88 ff.; *Schramm*, Internationales Strafrecht, 2011, S. 125 f.; vgl. ferner *Rönnau/Wegner*, GA 2013, 561, 562 ff.

41 S. erneut nur Grabitz/Hilf/*Nettesheim* (Fn. 40) Art. 288 Rdn. 142 ff., insb. Rdn. 143 (»nur …, wenn es zu einer *Verletzung der Umsetzungspflicht* gekommen ist«, Herv. dort); Calliess/*Ruffert* (Fn. 40) Art. 288 Rdn. 47, insb. Rdn. 52; *Safferling* (Fn. 40) § 11 Rdn. 46; *Satzger* (Fn. 40) § 9 Rdn. 78 (»soweit … Umsetzungsfrist *fruchtlos* abgelaufen ist«, Herv. hier); vgl. ferner *Rönnau/Wegner*, GA 2013, 561, 566 ff.

42 EuGH, Urt. v. 24. 11. 2011, Rs. C-468/10 und C-469/10 = EuZW 2012, 37 m. Anm. u. Bespr. *Diedrich*, CR 2013, 408; *Freund*, CR 2012, 33; *Grimm*, ArbRB 2012, 48; *Kunczik*, ITRB 2012, 51; *Lang*, K&R 2012, 43; *Schüßler*, jurisPR-ITR 2/012 Anm. 3.

»neben den beiden … kumulativen Voraussetzungen« des Art. 7 lit. f RL 95/46/EG – Erforderlichkeit und Interessenabwägung – »zusätzliche Erfordernisse« aufzustellen (Rz. 39). Andererseits aber, so der *EuGH*, »ist es Sache der Mitgliedstaaten, bei der Umsetzung … darauf zu achten, … ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten und Grundfreiheiten sicherzustellen« (Rz. 43), so dass »nichts dagegen spricht, dass die Mitgliedstaaten in der Ausübung ihres Ermessens nach Art. 5 der Richtlinie 95/46 Leitlinien für diese Abwägung aufstellen« (Rz. 46).

All dies lässt sich bei der Auslegung der §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 S. 1 Nr. 1 BDSG berücksichtigen: So ist es durchaus mit dem Wortlaut des § 28 Abs. 1 S. 1 Nr. 2 BDSG vereinbar, bei der Prüfung der Erforderlichkeit – die sich dort dem Wortlaut nach nur auf die »berechtigte(n) Interessen der verantwortlichen Stelle« bezieht – auch Interessen der Auftraggeber einzubeziehen, die durch das zwischen ihm und der verantwortlichen Stelle bestehende Band mittelbar auch deren Interessen werden.[43] Bei § 29 Abs. 1 S. 1 Nr. 1 BDSG wiederum gestattet, ja verlangt die Norm – entgegen der Auffassung des *1. Strafsenats* – nach einer Interessenabwägung,[44] die allerdings hier zugunsten des Betroffenen verschoben ist. Doch solch eine Gewichtung, solange sie nicht kategorisch ist und Raum für Einzelfallwertungen belässt,[45] verbietet die bisherige Rechtsprechung des *EuGH* im Lichte des Art. 5 RL 95/46/EG gerade nicht.[46]

c) Somit erscheint eine europarechtskonforme Auslegung möglich; folgt man dieser Auffassung, so sind §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 S. 1 Nr. 1 BDSG mit Unionsrecht vereinbar. Dann aber geht es fehl – weil den Umsetzungsspielraum des nationalen Gesetzgebers übergehend –, einer Harmonisierungsvorschrift wie hier Art. 7 lit. f RL 95/46/EG unmittelbare Wirkung anzuerkennen,[47] oder in ihr – mit dem *1. Strafsenat* – einen zwingenden strafrechtlichen Mindest-Rechtfertigungsstandard zu sehen.[48]

3. Zur Interessenabwägung bei GPS-basierten Observationen. Hinsichtlich der vorzunehmenden Interessenabwägung sind drei Kernaussagen des *1. Strafsenats* herauszuarbeiten:

a) Zunächst weist er darauf hin, dass sich diese nicht schematisch an den strafprozessrechtlichen Regelungen wie § 100 h Abs. 1 StPO orientieren darf, wie dies noch das Landgericht vertreten hatte. Dem ist zuzustimmen, denn hier ist ein horizontales Verhältnis zwischen Privaten betroffen, die sich nicht auf Hoheitsrechte berufen können und die auch nur in sehr begrenztem Umfang an Stelle der Strafverfolgungsbehörden tätig werden dürfen (vgl. nur § 127 Abs. 1 S. 1 StPO), um den sogenannten »staatlichen Strafanspruch« durchzusetzen. Ist aber eine Datenerhebung auf strafprozessualer Grundlage möglich, so wird regelmäßig ein Tätigwerden von privater Seite – und damit auch eine Zuhilfenahme von Privatdetektiven – nicht erforderlich sein.

b) Sodann ist im Lichte des Koinzidenzprinzips (§ 8 StGB) zu berücksichtigen, dass die Interessenabwägung aus einer ex ante-Perspektive, also auf den Zeitpunkt der Tathandlung des Täters (hier: Installation des GPS-Sensors) bezogen, vorzunehmen ist.

c) Schließlich zu den Abwägungsgesichtspunkten: Unter Verweis auf die Rechtsprechung zum Einsatz verdeckter technischer Observationsmittel durch Private[49] fordert der *1. Strafsenat*, dass über ein allgemeines (zivilprozessuales) Beweisführungsinteresse hinausgehend »weitere Gesichtspunkte hinzutreten« müssen; diese sieht er für gegeben an, »wenn ein konkreter Verdacht … besteht, die detektivische Tätigkeit zur Klärung der Beweisfrage erforderlich ist und nicht andere, mildere Maßnahmen als genügend erscheinen«. Mit Ausnahme des *konkreten* Verdachts ist das indes wenig Neues, denn die Erforderlichkeit der Datenerhebung und damit auch eine Berücksichtigung möglicher Alternativen ist ohnehin bereits gesetzliche Voraussetzung sowohl des Art. 7 lit. f RL 95/46/EG als auch der §§ 28 Abs. 1 S. 1 Nr. 2, 29 Abs. 1 S. 1 Nr. 1 BDSG. Mehr Aufschluss liefert hingegen der beachtliche Abwägungstopos der Vorbereitungs- und Begleitmaßnahmen[50] sowie ein neuerer Beschluss des *XII. Zi-*

43 So auch Simits/*Simitis* (Fn. 9) § 28 Rdn. 106; Plath/*Plath* (Fn. 24) § 28 Rdn. 48.

44 So auch Simits/*Ehmann* (Fn. 9) § 29 Rdn. 160; *Gola*/*Schomerus* (Fn. 10) § 29 Rdn. 10 f.; Plath/*Plath* (Fn. 24) § 29 Rdn. 37; Wolff/Brink/*Buchner* (Fn. 32) § 29 Rdn. 51 ff.; jew. m. w. N.

45 S. auch *Ehmann*/*Helfrich*, EG-Datenschutzrichtlinie, 1999, Art. 5 Rdn. 4: »gesetzliche Vermutungen« seien in bestimmten Sektoren zulässig; unkritisch *Cornelius*, NJW 2013, 3340, 3342.

46 Andernfalls gerieten auch sonstige Strafvorschriften wie §§ 201 ff. StGB in Gefahr, welche bestimmte Datenerhebungen (z. B. Ton- oder Bildaufnahmen) bei Kriminalstrafe kategorisch verbieten und bei denen allenfalls in Ausnahmefällen nach allgemeinen Grundsätzen eine Rechtfertigung eintreten kann.

47 Vor einer Überbewertung des EuGH-Urteils ebenfalls warnend *Lang*, K&R 2012, 43, 44 sowie *Kunczik*, ITRB 2012, 51: Es wäre »vermessen, sich … auf den Standpunkt zu stellen, dass fortan nur noch die relevanten europarechtlichen Vorgaben des Datenschutzrechts zu beachten und weitergehende nationale Vorgaben nahezu irrelevant sind.«

48 So aber *Wybitul*, ZD 2013, 509, 510.

49 Vorrangig BVerfGE 106, 28; BGH NJW 2003, 1727.

50 S. hierzu bereits oben I. 3.

vilsenats:[51] Dieser hatte den Maßstab betreffend GPS-basierter Observationen dahingehend konkretisiert, dass die hierdurch gewonnenen Beweismittel im Zivilprozess nur dann verwertbar sind, »wenn sich der Beweisführer in einer Notwehrsituation oder einer notwehrähnlichen Lage i. S. von § 227 BGB bzw. § 32 StGB befindet«; ferner erachtet er eine GPS-basierte Observation regelmäßig für nicht erforderlich, wenn sich durch eine »punktuelle persönliche Beobachtung« ebenfalls das Beweisziel hätte verfolgen lassen können.

Im konkreten Fall verneint der *1. Strafsenat* die Möglichkeit einer Rechtfertigung bei der Verfolgung (straf-) rechtswidriger Zwecke, aber auch bei einem Informationsinteresse in Konstellationen, bei denen noch keine »gerichtliche(n) Verfahren, etwa Unterhaltsrechtsstreitigkeiten, im Raume gestanden hätten«. Lediglich eine GPS-basierte Observation zur »Wahrung finanzieller Interessen« hält er für potentiell rechtfertigbar und verwies nur insoweit die Sache zur weiteren Aufklärung des Sachverhalts an das Tatgericht zurück.

4. Fazit. Der strafrechtliche Datenschutz des § 44 Abs. 1 BDSG ist ein relativer: Selbst beim Einsatz verdeckter technischer Mittel durch Private ohne Wissen der Betroffenen sind Konstellationen denkbar, in denen eine solche Datenerhebung rechtlich zulässig ist. Allerdings sind an die Erforderlichkeit der Datenerhebung und an die Interessenabwägung – bei der auch Vorbereitungs- und Begleitmaßnahmen zu berücksichtigen sind – hohe Maßstäbe anzusetzen. Die Erstellung von Bewegungsprofilen durch verdeckte technische Mittel ist daher nur »in einer Notwehrsituation oder einer notwehrähnlichen Lage i. S. von § 227 BGB bzw. § 32 StGB« rechtmäßig, andernfalls – unter den besonderen Voraussetzungen des § 44 Abs. 1 BDSG – bei Kriminalstrafe verboten.

III. Zur europäischen Neuregelung

Abschließend noch zur geplanten Neuregelung des Datenschutzrechts auf europäischer Ebene und zur Frage, ob diese die Maßstäbe, die dieser Entscheidung des BGH zugrunde lagen, wesentlich verändern wird. Zwar befindet sich die Datenschutz-Grundverordnung[52] noch in einem frühen Stadium des Gesetzgebungsverfahrens; dennoch lassen sich erste Leitlinien erkennen:

1. Das gewählte Instrument der *Verordnung* führt dazu, dass der erste Blick des Rechtsanwenders in die europäische Norm führt; normativer Ausgangspunkt der Beurteilung einer GPS-basierten Observation wird daher zukünftig die Datenschutz-Grundverordnung sein.

2. Der Kommissionsvorschlag hält ebenso wie das Europäische Parlament bzw. dessen LIBE-Ausschuss hinsichtlich der »Rechtmäßigkeit der Verarbeitung« personenbezogener Daten am selben *Abwägungsmaßstab* fest, wie er bereits in Art. 7 lit. f RL 95/46/EG enthalten war (Art. 6 Abs. 1 lit. f VO-E).

3. Dennoch dürfte auch in Zukunft die unmittelbare Anwendung dieser abstrakt gehaltenen Abwägung die Ausnahme bleiben: Eine nähere Regelung der Anwendung von Art. 6 Abs. 1 lit. f VO-E und damit eine *Konkretisierung des Abwägungsmaßstabs*, wie sie etwa in § 29 Abs. 1 S. 1 Nr. 1 BDSG vorgenommen wird, soll entweder über delegierte Rechtsakte der Kommission (so Art. 6 Abs. 5 VO-E) oder aber über Regelungen in den Mitgliedstaaten (so Art. 6 Abs. 3 S. 3 VO-E i. d. F. des LIBE-Ausschusses) erfolgen.

4. Zu spezifisch *strafrechtlichen Sanktionen* schweigt sowohl der Kommissionsvorschlag als auch die Positionierung des Europäischen Parlaments. Den Mitgliedstaaten soll es daher auch zukünftig überlassen sein, ob sie in Erfüllung der Maßgabe, wirksame, verhältnismäßige und abschreckende Sanktionen für Verstöße gegen die Datenschutz-Grundverordnung bereitzuhalten (Art. 78 Abs. 1 VO-E), allein auf bußgeldrechtliche oder aber auch auf genuin strafrechtliche Sanktionen setzen.

51 BGH NJW 2013, 2668 m. Anm. u. Bespr. *Bruns*, FamRZ 2013, 385; *Hausen/Haußleiter*, NJW 2013, 2671; *Schlünder*, FamRZ 2013, 1389.

52 S. hierzu oben bei und mit Fn. 2.