DER HEIMLICHE, HOHEITLICHE ZUGRIFF AUF (VERSCHLÜSSELTE) DATEN UND DATENÜBERTRAGUNGEN:

BEWEISFÜHRUNG DURCH SACHVERHALTSAUFKLÄRUNG?

Mit der zunehmenden Nutzung des Internets als Informations- und Kommunikationsmedium ging in den vergangenen Jahrzehnten ein beträchtlicher Ausbau der digitalen Infrastruktur einher: Einerseits wurden informationstechnische Endgeräte (Computer, Smartphones, Tablets) immer kleiner und leistungsfähiger; anderseits ermöglichte der Ausbau der Breitbandtechnik die Übertragung und Vernetzung immer größerer Datenmengen über das Internet.[1] Es überrascht daher nicht, dass immer mehr Informationen in Form von Daten vorliegen und übertragen werden. Insbesondere der Anteil verschlüsselter Kommunikation ist in den vergangenen Jahren rasant gestiegen.[2] Daten haben aber nicht nur als Speicher- und Kommunikationsmedium viele konventionelle Datenträger abgelöst, sondern auch für die Beweisführung im Strafprozess an Bedeutung gewonnen.

Die klassischen Ermittlungsmaßnahmen der Strafprozessordnung (Durchsuchung, 102 ff StPO; Beschlagnahme, §§ 94 ff StPO; Telekommunikationsüberwachung, §§ 100a ff StPO; Vernehmungen und Auskunftsersuchen, § 161a StPO) tragen den Besonderheiten und der Kontrollresistenz moderner Informationstechnik allerdings nur eingeschränkt Rechnung und liefern bei restriktiver Auslegung keine hinreichend bestimmte Grundlage für „moderne" Eingriffe in informationstechnische Systeme[3] – insbesondere nicht für die Durchführung einer Onlinedurchsuchung oder Quellen-Telekommunikationsüberwachung.[4] Nach ständiger Rechtsprechung des BVerfG kann sich der Rechtstaat aber nur dann verwirklichen, „wenn ausreichende Vorkehrungen dafür getroffen sind, dass Straftäter im Rahmen der geltenden Gesetze verfolgt, abgeurteilt und einer gerechten Bestrafung zugeführt werden."[5] Die Praxis behilft sich deshalb mit einer weiten Auslegung der strafprozessualen Ermächtigungsgrundlagen, der Verschleifung repressiver, präventiv-polizeilicher und nachrichtendienstlicher Ermittlungstätigkeit und größtmöglicher Zurückhaltung bei der fachgerichtlichen Kontrolle von Beweiserhebungsvorgängen.[6] Heimliche Überwachungsmaßnahmen sind wegen Fehlens alternativer (offener) Ermittlungsmaßnahmen

---

[1] *Singelnstein*, NStZ, 2012, 593 ff.

[2] *Soiné*, NVwZ 2012, 1585; *Bär*, MMR 1998, 577 (582).

[3] *Bär*, MMR 1998, 577; *Sieber*, Gutachten zum 69. DJT, C62 ff; *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, 2009, S. 262 ff.

[4] *Buermeyer*, StV 2013, 470 (471 f.); *Buemeyer/Bäcker*, StV 2009, 433 (440 f.); *Klesczewski*, ZStW 2011, 744; *Sieber*, Gutachten zum 69. DJT, C104 ff.; *Albrecht/Dienst*, JurPC Web-Dok. 5/2012, Abs. 43.

[5] BVerfGE 33, 367 (383); 46, 214 (222); 122, 248 (272 f.).

[6] *Hefendehl*, GA 2011, 210 f; *Paeffgen*, GA 2003, 650 ff.; *Mitsch*, NJW 2008, 2295 (2298); *Knieriem*, StV 2009, 206 (211).

längst zur Regel avanciert.[7] Ihre Effizienz resultiert aber nicht zuletzt aus einer strukturellen Schwächung von Beschuldigten- und Verteidigerrechten,[8] welche durch die Übertragung der herkömmlichen Beweisverwertungsverbotslehre und Kasuistik – insbesondere die strikte Trennung zwischen Beweiserhebung und -verwertung – auf die heimlichen Überwachungsmaßnahmen mit Technikeinsatz in beträchtlichem Maße verstärkt wird.[9] Das „Effektivitätsdefizit" einzelner strafprozessualer Instrumentarien hat sich damit längst zu einem Legitimationsdefizit repressiv-polizeilicher (Überwachungs-)Tätigkeit ausgeweitet,[10] welches die Rechtsstaatlichkeit und Fairness des Strafverfahrens dauerhaft zu beschädigen droht – in den Worten Jahns: *„Ein Verfassungsverständnis, welches den Bedürfnissen einer funktionstüchtigen Strafrechtspflege […] den prinzipiellen Vorrang vor den Freiheitsrechten des Einzelnen einräumt, kehrt das dem Grundgesetz immanente Verhältnis von Freiheit und staatlicher Gewalt um."*[11]

Im Fokus bisheriger Untersuchungen standen vorwiegend die Ermächtigungsgrundlagen und Anordnungsvoraussetzungen der heimlichen Ermittlungsmaßnahmen mit Technikeinsatz, nicht aber der Umgang mit den dabei gewonnenen Erkenntnissen.[12] Restriktionen, welche die Auswahl an technischen Mitteln und die Art und Weise ihres Einsatzes begrenzen, erscheinen auf den ersten Blick zwar am geeignetsten, um einen wirksamen Grundrechtsschutz im Ermittlungsverfahren zu gewährleisten, gehen bei genauer Betrachtung aber zu Lasten der Durchführbarkeit und Effizienz der Überwachungsmaßnahmen, ohne dass eine solche, generelle Beschränkung verfahrens- oder verfassungsrechtlich zwingend erforderlich wäre. Die Beachtung von Beweiserhebungsvorschriften im Ermittlungsverfahren ist wegen der Heimlichkeit der Maßnahmen zudem nur schwer überprüfbar;[13] ebenso die faktische Nutzung rechtswidrig gewonnener Erkenntnisse durch die Polizei.[14] Der Grundsatz der Verwertbarkeit, die generelle Ablehnung der h.M. gegenüber der Annahme von Fernwirkung und die Präklusion von Verfahrensrechten infolge der Widerspruchslösung ermöglichen darüber hinaus auch die (mittelbare) Verwertung gesetzeswidrig erlangter Beweismittel im Strafverfahren (zuletzt: Kennzeichenüberwachung zur Ermittlung des sog. „Autobahnschützen"[15], aber auch die Verwertung privatdeliktisch erlangter Beweismittel in Filesharingverfahren[16]).[17] Und selbst dann, wenn das Gericht ein Beweisverwertungsverbot

---

[7] *Singelnstein*, NStZ, 2012, 593; *Buermeyer*, StV 2013, 470 (472).

[8] *Schünemann*, ZIS 2009, 484 (488); *Hefendehl*, GA 2011, 210 (211).

[9] *Paeffgen*, GA 2003, 650 (656).

[10] *Roxin/Schünemann*, Strafverfahrensrecht, § 2 Rn. 9.

[11] *Jahn*, Gutachten zum 67. DJT, C48; so auch: *Dallmeyer*, Beweisführung im Strengbeweisverfahren, 2002, S. 128 ff.; *Mitsch*, NJW 2008, 2295 (2296).

[12] *Barte*, Die Quellen-Telekommunikationsüberwachung im Strafverfahren, 2013, S. 321 ff; *Schäfer*, Präventive Telekommunikationsüberwachung, S. 228 ff; *Seebauer*, Die Zulässigkeit des Spähangriffs zu Strafverfolgungszwecken, 2010, S. 147 ff; *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, S. 264 ff.

[13] *Paeffgen*, GA 2003, 650 (669 ff.).

[14] *Knieriem*, StV 2009, 206 (211).

[15] LG Würzburg, Urt. v. 30.10.2014, Az. 801 Js 9341/13.

[16] Vgl. *Kubiciel*, GA 2013, 226 (227).

im Ergebnis bejaht, geht der Erörterung dieser Frage in der Praxis oft eine Beweisaufnahme über das möglicherweise gesperrte Beweismittel voraus.[18] Der Beweiswert der im Rahmen heimlicher Spähangriffe auf informationstechnische Systeme gewonnenen Daten mag gering sein,[19] ihre Bedeutung für eine lückenlose Aufklärung des Sachverhaltes und das Auffinden weiterer („immunisierter") Beweismittel kann aber kaum überschätzt werden.[20] Auf die Umstände und den ursprünglichen Zweck ihrer Erhebung kommt es, jedenfalls bei Ablehnung einer Fernwirkung von Beweisverwertungsverboten, nicht an.[21] Die heimlichen Ermittlungsmaßnahmen mit Technikeinsatz erweitern nicht bloß das bestehende Ermittlungsinstrumentarium, sondern eröffnen völlig neue Möglichkeiten der Beweiserhebung und Beweisführung, die dem in der Literatur häufig verwendeten Begriff der „Verpolizeilichung" eine völlig neue Dimension geben und zunehmend als „Vernachrichtendienstlichung" oder gar „Entfesselung" des Strafverfahrens wahrgenommen werden;[22] sie bedürfen deshalb der umfassenden rechtstaatlichen Kontrolle.

Im Rahmen der Untersuchung soll deshalb ein *Restriktionsmodell* entwickelt werden, welches verbindliche Regelungen für die Nutzung der gewonnenen Erkenntnisse im Ermittlungsverfahren und ihre spätere (mittelbare) Verwertung in einem Strafverfahren beinhaltet. Dabei soll es keinen Unterschied machen, ob die technische Überwachungsmaßnahme ursprünglich zu repressiven, präventiv-polizeilichen oder nachrichtendienstlichen Zwecken angeordnet wurde. Jedwede Nutzung und Verwertung heimlich gewonnener Daten zu Ermittlungs- oder Beweiszwecken stellt einen eigenständigen Eingriff in das Recht des Beschuldigten auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG) dar, dessen Eingriffsintensität wiederum untrennbar mit der Art und Weise ihrer Erhebung verbunden ist.[23] Die Regelungen der §§ 161 I, 163 I StPO (für die Datennutzung im Ermittlungsverfahren), § 261 StPO oder § 244 II StPO (für die Beweisverwertung) beinhalten ebenso wenig eine Differenzierung nach der Art, dem Inhalt oder den Umstände der Erhebung verfahrensrelevanter Datensätze, wie die pauschale Behauptung, selbst die Verwertung rechtswidrig gewonnener Erkenntnisse sei dem deutschen Strafverfahren immanent. [24]

Stattdessen ist zu fragen, ob dem Grundsatz der Verwertbarkeit und der Widerspruchslösung nicht vielmehr die Idee einer Kompensation von solchen Verfahrensnachteilen zu Grunde

---

[17] *Jahn*, StraFo 2011, 117 ff.

[18] BVerfGE 80, 367 (375); OLG München mit Anm. *Satzger*, JR 2007, 336 (337); *Jahn*, Gutachten zum 67. DJT, C87 f.

[19] *Bär*, MMR 1998, 577 (582).

[20] Vgl. *Hefendehl*, GA 2011, 210 (216, 225 f.).

[21] *Hefendehl*, GA 2011, 210 (216 f.).

[22] *Paeffgen*, GA 2003, 650 (669 ff.); *Schoreit*, StV 1989, 449 ff.; *Hefendehl*, GA 2011, 210 (225 f.).

[23] *Hefendehl*, GA 2011, 210 (215); *Singelnstein*, NStZ, 2012, 593 (605).

[24] Satzger/Schluckebier/Widmaier/*Eschelbach*, StPO, 2014, § 136 Rdnr. 83 m.w.N.; *Jahn*, Gutachten zum 67. DJT, C66 [Beweisbefugnislehre].

liegt, die den Strafverfolgungsbehörden im Rahmen offener Ermittlungsmaßnahmen und bei Beachtung sämtlicher Anordnungsvoraussetzungen zwangsläufig entstehen. Die grundsätzliche Verwertbarkeit würde sich dann aus der Rechtsmäßigkeit der Maßnahme ableiten; eine rechtswidrige Beweiserhebung müsste die Unverwertbarkeit des Beweismittels zur Folge haben, sofern die Umstände, welche die Rechtswidrigkeit im Einzelfall begründen, nicht ausnahmsweise einen kompensationsfähigen „Verfahrensnachteil" darstellen. Erkenntnisse aus heimlichen Überwachungsmaßnahmen, denen die typischen Risiken für den Verlust oder eine Verschlechterung des Beweismittels nicht in demselben Maße anhaften wie offenen Maßnahmen, könnten diesem Ansatz zufolge nur dann verwendet und verwertet werden, wenn die Rechtmäßigkeit ihrer Erhebung sichergestellt ist. Dies könnte in einem der Beweisaufnahme vorgelagerten Verfahren unter Beteiligung des Verteidigers oder einer unabhängigen Institution überprüft und sichergestellt werden.[25] Es versteht es sich von selbst, dass ein Verfahren, welches den spezifischen Risiken heimlicher Spähangriffe auf informationstechnische Systeme Rechnung tragen soll, nicht oder nur eingeschränkt auf andere Ermittlungsmaßnahmen übertragbar ist, zumal ein harmonisch abgestimmtes System der Beweisverbote ohnehin reine Illusion ist.[26]

Auf diese Weise könnten zugleich ein wirksamer *Kernbereichsschutz* sowie die Erhaltung von Verfahrens- und Verteidigungsrechten des Beschuldigten innerhalb der heimlichen technischen Überwachungsmaßnahmen erreicht werden. Berücksichtigt man, dass Daten bei technischer Betrachtung nur erkennungsfähige Ketten von Zeichen oder physikalischen Zuständen sind, deren Informationsgehalt sich dem Betrachter erst im Wege ihrer Verarbeitung erschließt, so wird man dem bloßen Ausleiten von Daten aus einem informationstechnischen System allenfalls geringe Eingriffsintensität beimessen können. Erst die spätere Verarbeitung der Daten ermöglicht eine sinnliche Wahrnehmung der gespeicherten Informationen durch Dritte und damit die Verletzung des Kernbereichs persönlicher Lebensgestaltung. Gem. § 110 StPO liegt die Befugnis zur Durchsicht und Auswertung von Daten bei der Staatsanwaltschaft, wird jedoch regelmäßig auf deren Ermittlungspersonen – und damit auf die Polizei – delegiert.[27] Einer unzulässigen Suche nach Zufallsfunden, der Durchsicht kernbereichsrelevanter Datensätze sowie der faktischen Nutzung dieser Erkenntnisse im Ermittlungsverfahren sind nahezu keine Grenzen gesetzt;[28] nicht zuletzt, weil eine Teilnahme des Beschuldigten oder seines Verteidigers an der Durchsicht nach § 110 StPO nach neuer Rechtslage nicht mehr vorgesehen ist.[29] Zwar ist nach der Rechtsprechung des BVerfG durch „technische Vorkehrungen" sicherzustellen, dass erst gar keine kernbereichsrelevanten Daten erhoben werden, allerdings erscheint die Konstruktion solcher „Vorkehrungen" aus technischer und rechtlicher Sicht unmöglich, denn eine Filtersoftware, die von vorne herein auf die Erlangung belastenden Beweismaterials

---

[25] *Schünemann*, ZIS 2009, 484 (488 f).

[26] *Mitsch*, NJW 2008, 2295 (2299); a.A. Hefendehl, GA 2011, 210 (227 ff), der ein einheitliches Wertungssystem favorisiert.

[27] Satzger/Schluckebier/Widmaier/*Hadamitzky*, StPO, 2014, § 110 Rdnr. 11.

[28] *Singelnstein*, NStZ, 2012, 593 (587, 605).

[29] BVerfGE 124, 43 (72); zur Notwendigkeit in begründeten Einzelfällen: BVerfGE 113, 29 (58).

unter Ausfilterung entlastender, weil kernbereichsrelevanter Umstände, ausgerichtet ist, wäre wohl weder mit dem Recht auf ein faires und rechtstaatliches Strafverfahren (Art. 6 III EMRK, Art. 2 I i.V.m. 20 III GG), noch mit der Menschenwürdegarantie des Art. 1 I GG, vereinbar. Ein wirksamer Kernbereichsschutz ist deshalb nur im Anschluss an den Zugriff auf das beweisrelevante Datenmaterial möglich.

ARBEITSGLIEDERUNG

A. Daten als Beweismittel

I. Begriffsbestimmung

II. Merkmale von Daten im informationstechnischen Sinne

1. Fehlende Verkörperung
2. Ubiquitous Computing
3. Routing
4. Kryptografie

III. Auswirkungen auf die Beweiserhebung de lege lata

1. Durchsuchung und Beschlagnahme, §§ 94 ff, 102 ff StPO
2. Staatsanwaltschaftliche Auskunftsersuchen / Vernehmungen, § 161a StPO
3. Telekommunikationsüberwachung, §§ 100a ff StPO
4. Repressive Onlinedurchsuchung / Quellen-TKÜ (nach wohl h.M. unzulässig)
5. Ermittlungsgeneralklauseln; insbesondere die Nutzung kriminal-, steuer-, verwaltungspolizeilicher und geheimdienstlicher Erkenntnisse auf Grundlage der §§ 161 I, 163 I StPO (hier ist auf Onlinedursuchung und Quellen-TKÜ einzugehen)
6. Nutzung privatdeliktisch erlangter Beweismittel (insb. Filesharing etc.)

B. „Entfesselung“ des Strafverfahrens oder „erforderliche Strafrechtspflege“?

I. Unbestimmtheit grundrechtssichernder Anordnungsvoraussetzungen

II. Bevorzugte Anordnung heimlicher Maßnahmen

III. Fehlende Zweckbindung gewonnener Ermittlungserkenntnisse

IV. Verpolizeilichung und Vernachrichtendienstlichung des Ermittlungsverfahrens

V. Verletzung des Trennungsgebots

VI. Lückenhafter Kernbereichsschutz

VII. Eingriffe in die Rechte Unbeteiligter