*Vierter Teil*

# Ergebnisse und Zusammenfassung

## K. Kernaussagen des Buches

Der sich anschließenden ausführlichen Darstellung der Ergebnisse und Zusammenfassungen sollen vier zentrale Befunde dieser Arbeit vorangestellt werden:

1. Die Feststellung, dass sich mittels der Überwachung lokaler Funknetzwerke auch eine Überwachung auf dem Übertragungsweg realisieren lässt, die in bestimmten Maße auch mit dem „Problem“ der Verschlüsselung umgehen kann[1606] und deren Erfolgsaussichten nicht unwesentlich geringer sind als die Erfolgsaussichten des Einsatzes eines „Staatstrojaners“, hat Auswirkungen auf die Beurteilung der *Verhältnismäßigkeit von Quellen-Telekommunikationsüberwachung und Online-Durchsuchung*.

2. Die in diversen Bundestagsdrucksachen dokumentierten Durchführungen der Maßnahme des „WLAN-Catchings“ durch staatliche Behörden vor dem 24.08.2017 waren dann *strafprozessual nicht zulässig*, wenn sie zum Zwecke der Strafverfolgung erfolgten und mit Eingriffen in den Datenverkehr einer Netzwerkinfrastruktur und/oder mit Auswirkungen auf IT-Endgeräte einhergingen.

3. Die mit Wirkung vom 24.08.2017 neu eingeführte Eingriffsbefugnis des § 100a I S. 2 StPO bedarf der *verfassungskonformen Auslegung* in dem Sinne, dass von der Maßnahme, sowohl in Bezug auf das Überwachungs-, aber auch

[1606] Diese Aussage wird zunächst konkret nur für den Untersuchungsgegenstand dieser Arbeit, also für die Verschlüsselung im Bereich lokaler Funknetzwerke und für das verschlüsselte World Wide Web (HTTPs) getroffen. Exploitierbare Sicherheitslücken dürfte es aber in allen Einsatzbereichen von Verschlüsselung geben. Die Frage, ob das Ausnutzen von Sicherheitslücken durch staatliche Stellen generell erstrebenswert ist und nicht mit anderen staatlichen Zielstellungen in Konflikt steht, ist eine gänzlich andere. An dieser Stelle geht es ausschließlich darum, dass die Überwachung lokaler Funknetzwerke ein Minus zur Installation eines „Staatstrojaners“ auf einem Endgerät darstellt, welches in der Regel ebenfalls das Ausnutzen von Sicherheitslücken voraussetzt.

in Bezug auf das Eingriffsobjekt der Maßnahme (*gesamter* Gegenstand der Maßnahme), ausschließlich flüchtige Telekommunikationsdaten betroffen sein dürfen.

4. Für die Maßnahme der staatlichen informationstechnologischen Täuschungen, welche die Funktionsweise von IT-Systemen (abweichend vom Interesse des Grundrechtsträgers) in der Art ändert, dass der Betroffene dabei eine Kommunikationsbeziehung zu einer staatlichen Stelle etabliert (wie es etwa beim Spear Phishing, dem gezielten Unterschieben von Schadsoftware über getarnte E-Mails – einem der wichtigsten Installationswege für den „Staatstrojaner“ – der Fall ist), kommt wegen der besonderen Eigenart der Maßnahme *eine Rechtfertigung ausschließlich über § 100b I StPO* in Betracht.

# N. Schlussfolgerung und thesenartiger Überblick

## I. Schlussfolgerung für durchgeführte Maßnahmen des „WLAN-Catchings“ vor dem 24.08.2017

Die soeben dargestellten Ergebnisse der rechtlichen Untersuchung haben aber auch erhebliche Konsequenzen für sämtliche (strafverfolgenden) Überwachungsmaßnahmen, welche die Behörden vor dem 24.08.2017[1618] durchgeführt haben.[1619] Der Befund der Bundesregierung in den regelmäßigen Antworten zu den entsprechenden Anfragen von Bundestagsabgeordneten in Bezug auf den Einsatz computergestützter Kriminaltechnik bei Polizeibehörden und damit die gängige Behördenpraxis, nämlich, dass für das Abhören des WLAN im repressiven Bereich (immer und grundsätzlich) allein § 100a I a.F. StPO einschlägig ist,[1620] kann nicht gestützt werden.

In den betreffenden Drucksachen des Bundestages finden sich leider keine näheren Erläuterungen, wie die Behörden das „WLAN-Catching“ in der Praxis (also mindestens seit 2007) technisch genau umsetzen und tatsächlich handhaben. Darüber können an dieser Stelle daher nur Vermutungen angestellt werden. Drei Szenarien sind denkbar:

- Im ersten Szenario könnte die Maßnahme nur zur Anwendung gekommen sein, wenn der Betroffene lediglich ein unverschlüsseltes WLAN benutzt hat. In solch einer Situation fände wohl ausschließlich die Primärmaßnahme Verwendung, welche auch allein auf § 100a I a.F. StPO gestützt werden konnte.
- Im zweiten Szenario käme auch bei einem verschlüsselten WLAN allein die Primärmaßnahme zum Einsatz. Dann wäre ein staatliches Vorgehen im Einklang mit der Strafprozessordnung möglich, allerdings dürfte der Erkenntnisgewinn der Behörden in diesem Szenario nahezu Null gewesen sein.

[1618] Also bevor das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens seine Wirkung entfaltet hat.

[1619] Dazu näher oben in Abschnitt b) auf Seite 35.

[1620] Vgl. etwa BT-Drucks. 17/8544, S. 16, abrufbar unter: http://dipbt.bundestag.de/dip21/btd/17/085/1708544.pdf (Stand: Dezember 2017).

- Im dritten Szenario erfolgte ein Vorgehen auch mit Hilfe von Maßnahmen, die in dieser Arbeit in die Kategorie der Sekundärmaßnahmen II eingeordnet worden sind.[1621] In diesem Falle war aber eine Rechtfertigung des damit verbundenen Grundrechtseingriffs nicht mehr allein über § 100a I a.F. StPO möglich. Die nunmehr einschlägigen Eingriffsbefugnisse des § 100a I S. 2 StPO und § 100b I StPO sind jedoch erst mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens neu in die Strafprozessordnung eingefügt worden. Bis dahin war ein entsprechendes Vorgehen somit gar nicht zulässig.

Es muss daher final festgestellt werden: Ging eine von den Strafverfolgungsbehörden vor dem 24.08.2017 durchgeführte WLAN-Überwachungsmaßnahme bei der praktischen Umsetzung mit Eingriffen entweder in die Netzwerkinfrastruktur oder gar mit Auswirkungen auf das IT-Endgerät eines Betroffenen einher, was angesichts der ansonsten geringen Erfolgsaussichten einer Maßnahme nicht unwahrscheinlich ist, erfolgte ihre Durchführung *nicht rechtmäßig*.

## II. Thesenartiger Überblick

Abschließend sollen die gefundenen Ergebnisse noch einmal thesenartig im Überblick dargestellt werden:

1. Der Schutzbereich von Art. 10 I GG ist *weit* zu verstehen. Umfasst ist insbesondere die gesamte Bandbreite der vorstellbaren Nutzung des Internet-Netzwerkes, soweit sie durch zumindest eine Person wenigstens entfernt *initiiert* wurde (auch wenn im konkreten Fall automatisiert ohne aktuellen Willen und Wissen des Betroffenen). Es sei denn, die Wahrnehmung der übertragenen Informationen ist *nicht* in irgendeiner Form *Zugangshindernissen* ausgesetzt und erfolgt *auf dem dafür vorgesehenen Weg*.[1622]
2. Der gesamte Datenverkehr in lokalen Funknetzwerken ist von Art. 10 I GG geschützt, ausgenommen ist allein eine reine Maschine-zu-Maschine-Kommunikation.
3. Art. 10 I GG ist alleiniger Prüfungsmaßstab für Eingriffe in Form des *passiven* Mitschneidens und Speicherns des Datenverkehrs eines lokalen Funknetzwerks *von außen*.
4. Das *passive* Mitschneiden und Speichern des Datenverkehrs eines lokalen Funknetzwerks *von außen* lässt sich, soweit die übrigen Anordnungsvoraussetzungen erfüllt sind, auf § 100a I S. 1 StPO stützen.

[1621] Präziser in die zweite und dritte Unterkategorie der Sekundärmaßnahme II, also die Eingriffe in den Datenverkehr einer Netzwerkinfrastruktur und die Maßnahmen mit Auswirkungen auf IT-Endgeräte.

[1622] Ausgenommen ist lediglich die reine Maschine-zu-Maschine-Kommunikation.

5. Das selbständige, isolierte Erheben von Verkehrsdaten eines lokalen Funknetzwerkes lässt sich auf § 100g III StPO stützen.

6. Das Lokalisieren und Zuordnen eines WLAN oder die Ermittlung der MAC-Adresse des Access Points mittels passiver Scanner sind ohne den Rückgriff auf eine strafprozessuale Rechtfertigungsnorm zulässig.

7. Das Verwenden aktiver Scanner oder das Einloggen in ein offenes WLAN sind ebenfalls ohne Weiteres zulässig, wenn sie auf dem technisch dafür vorgesehenen Weg erfolgen und das betreffende IT-System sich dafür geöffnet hat (Regelfall).

8. Das Wahrnehmen der Maschine-zu-Maschine-Kommunikation eines lokalen Funknetzwerkes, ohne dass dafür Sicherheitsvorkehrungen überwunden werden müssen, lässt sich auf die Ermittlungsgeneralklausel in §§ 161, 163 StPO stützen.

9. Das alleinige, isolierte Überwinden („Knacken“) von Verschlüsselung, etwa durch das Dechiffrieren mit Hilfe eines anderweitig erlangten kryptographischen Schlüssels oder auf dem Wege einer reinen Kryptanalyse, stellt bereits einen eigenständigen Eingriff in Art. 10 I GG dar, der (nur) als Annexkompetenz zu § 100a I S. 1 StPO gerechtfertigt werden kann.

10. Für Eingriffe in den Datenverkehr einer Netzwerkinfrastruktur zur Überwindung von Sicherheitsvorkehrungen scheidet eine Rechtfertigung über § 100a I S. 1 StPO ebenso wie über § 100a I S. 3 StPO und § 100b I StPO aus. § 100a I S. 2 StPO ist allein einschlägig.

11. Für Maßnahmen mit Auswirkungen auf IT-Endgeräte ist § 100a I S. 2 StPO nach gebotener, verfassungskonformer Auslegung nicht anwendbar. Vielmehr kann diese (Teil-)Maßnahme nur auf § 100b I StPO gestützt werden.

12. Für staatliche informationstechnologische Täuschungen, welche die Funktionsweise von IT-Systemen (abweichend vom Interesse des Grundrechtsträgers) in der Art ändern, dass der Betroffene dabei eine Kommunikationsbeziehung zu einer staatlichen Stelle etabliert, kommt ebenfalls ausschließlich eine Rechtfertigung über § 100b I StPO in Betracht.