Kapitel 7 – Schlussbetrachtung

Die vorstehende Untersuchung hat gezeigt, dass die Blockchain-Technologie zwar eine sehr einfach verfügbare Datengrundlage für systematische Auswertungen bietet. Der Einsatz dieser Auswertungsmöglichkeiten ist allerdings trotz der öffentlichen Verfügbarkeit der ausgewerteten Daten nur teilweise zu Strafverfolgungszwecken zulässig. Denn die einschlägige Ermittlungsbefugnis des § 161 Abs. 1 StPO ermächtigt nur zu geringfügigen Grundrechtseingriffen. Die hier untersuchten Auswertungsmethoden überschreiten allerdings teilweise diese Grenze der Geringfügigkeit. Empfehlenswert ist es daher, in § 98a Abs. 2 StPO eine Befugnis zur Erhebung von öffentlich zugänglichen Daten aufzunehmen.[1902]

A. Die Blockchain-Technologie und ihre Auswertbarkeit

Grundsätzlich wird der Blockchain-Technologie ein enormes Entwicklungspotenzial zugeschrieben, da durch ihren Einsatz einerseits fälschungssicher und andererseits ohne eine zentrale Verwaltungsstelle Daten verwaltet werden können.[1903]

In der öffentlichen Wahrnehmung ist die Blockchain-Technologie zwar vor allem im Zusammenhang mit Bitcoin und anderen Kryptowährungen bekannt, sie ist aber gerade nicht auf diesen Anwendungskontext beschränkt.[1904] Sie kann vielmehr als eine Form dezentraler Datenverwaltung verstanden werden.[1905] So kann die Blockchain-Technologie etwa für Smart-Contracts, die öffentliche Verwaltung, das Crowdfunding oder die digitale Zuweisung von Rechten eingesetzt werden.[1906]

Bei Kryptowährungen wird die Blockchain-Technologie zur Kontobuchführung eingesetzt. Vereinfacht kontrollieren dabei alle Teilnehmer des Blockchain-Netzwerkes, ob neue Transaktionen mit der bisherigen Trans-

1902 Siehe hierzu ausführlich oben unter Kap. 5, F.
1903 Siehe zur technischen Funktionsweise der Blockchain-Technologie im Einzelnen oben unter Kap. 2 m.w.N.
1904 Siehe hierzu oben unter Kap. 2, B.I.
1905 Siehe hierzu oben unter Kap. 2, B.III.
1906 Siehe hierzu mit weiteren Nachweisen und Beispielen oben unter Kap. 2, C.

aktionshistorie übereinstimmen.[1907] Da Bitcoin – wie andere Kryptowährungen auch – als offenes Netzwerk ausgestaltet ist, führt die dezentrale Datenverwaltung dazu, dass alle in der Blockchain enthaltenen Transaktionsdaten öffentlich verfügbare Daten sind.[1908] Dies ist relevant, da Kryptowährungen häufig auch im Zusammenhang mit illegalen Aktivitäten verwendet werden und die in der Blockchain enthaltenen Transaktionsdaten insoweit einen einfach verfügbaren Ansatz für strafrechtliche Ermittlungen bieten. So ist es in der Praxis ohne Umstände möglich, eine *Bitcoin-Adresse* bei Google einzugeben und in der Regel über einen der ersten drei angezeigten Links alle Transaktionen einzusehen, die jemals mit dieser *Bitcoin-Adresse* getätigt wurden, und weitere Informationen zu erhalten.

Die verwendeten *Bitcoin-Adressen* geben grundsätzlich keine Anhaltspunkte über die hinter ihnen stehenden Personen.[1909] Denn einerseits fehlt es auf Grund der Dezentralität eben gerade an einer zentralen Verwaltungsstelle, durch die eine derartige Zuordnung erfolgen könnte. Andererseits ist es bei Bitcoin möglich, sich unzählig viele *Bitcoin-Adressen* zu erstellen.[1910] Die Transaktionsdaten in der Blockchain können aber als Anhaltspunkte für weitere Ermittlungen verwendet werden – etwa um zu ermitteln, ob eine verdächtige *Bitcoin-Adresse* in der Vergangenheit mit einem Diensteanbieter für Kryptowährungen interagiert hat, der zur Identifizierung seiner Kunden verpflichtet ist.

Daher wurden mittlerweile verschiedenste Auswertungsmöglichkeiten entwickelt, mit denen die Transaktionsdaten der Blockchain systematisch ausgewertet werden können. So ist es etwa durch die sog. *Entitäts-Clustering*-Verfahren möglich, mehrere *Bitcoin-Adressen* einer einzelnen sog. *Entität* zuzuordnen.[1911] Darüber hinaus ist es möglich, die Transaktionsdaten der *Bitcoin-Adressen* und *Entitäten* systematisch auszuwerten und zu ermitteln, welches Transaktionsverhalten typisch ist und welches Transaktionsverhalten hiervon abweicht.[1912] Außerdem können auch Transaktionsmuster ermittelt werden, die auf einen bestimmten Hintergrund der Transaktionen hindeuten.[1913] Ferner können auch die Daten über die Weiterleitung von Transaktionsnachrichten im Netzwerk der Blockchain und sog. *Bloom-*

1907 Siehe hierzu im Einzelnen oben unter Kap. 2, A.III.
1908 Siehe hierzu im Einzelnen oben unter Kap. 2, A.IV.
1909 Siehe hierzu oben unter Kap. 2, A.II. m.w.N.
1910 Siehe hierzu oben unter Kap. 2, A.II. m.w.N.
1911 Siehe hierzu oben unter Kap. 3, A.I. m.w.N.
1912 Siehe hierzu oben unter Kap. 3, A.II. m.w.N.
1913 Siehe hierzu oben unter Kap. 3, A.III. m.w.N.

Filter ausgewertet werden, um *Bitcoin-Adressen* einer IP-Adresse zuzuordnen.[1914] Schließlich ist es auch möglich, diese Daten auch mit anderweitig verfügbaren Daten zu verknüpfen, um so weitere Informationen zu erhalten.[1915]

Dabei muss allerdings berücksichtigt werden, dass die hier dargestellten Auswertungsmöglichkeiten nur eine Momentaufnahme sind, denn die technische Funktionsweise von Bitcoin und anderen Kryptowährungen wird fortlaufend angepasst – auch, um derartige Auswertungsmöglichkeiten zu verhindern. So haben sich mittlerweile schon mehrere weitere Kryptowährungen herausgebildet, bei denen eine Auswertung der Transaktionsdaten noch schwieriger ist. Insoweit unterliegt sowohl die technische Funktionsweise von Blockchains und Kryptowährungen als auch die technische Funktionsweise von Ermittlungsmöglichkeiten einem fortlaufenden Wandel. Die herausgearbeiteten rechtlichen Bewertungsmaßstäbe können aber bei technischer Vergleichbarkeit entsprechend angewendet werden.

B. Die Auswertungsmethoden als Eingriff in das Recht auf informationelle Selbstbestimmung

Zunächst lässt sich festhalten, dass beim Einsatz der hier untersuchten Auswertungsmethoden nur ein Eingriff in das Recht auf informationelle Selbstbestimmung (nachfolgend als „RiS" bezeichnet) vorliegt.[1916]

Denn einerseits liegen auch bei den ausgewerteten Daten personenbezogene Daten vor.[1917] Andererseits kann auch bei öffentlich verfügbaren Daten ein Eingriff in das RiS vorliegen.[1918]

Der Personenbezug liegt nach hier vertretener Auffassung vor, wenn die jeweils verarbeitende Stelle rechtlich und tatsächlich dazu in der Lage ist, einen Personenbezug mit einem nicht unverhältnismäßigen Aufwand herzustellen.[1919] Dies ist für die von Auswertungsmethoden betroffenen Daten insoweit der Fall, als dass die in einer Blockchain enthaltenen Transaktionsdaten etwa nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG

1914 Siehe hierzu oben unter Kap. 3, B. m.w.N.
1915 Siehe hierzu oben unter Kap. 3, C. m.w.N.
1916 Siehe hierzu insgesamt unter Kap. 4, B.II. m.w.N.
1917 Siehe hierzu unter Kap. 4, B.II.1. m.w.N.
1918 Siehe hierzu unter Kap. 4, B.II.2. m.w.N.
1919 Siehe hierzu unter Kap. 4, B.II.1.b)(4) m.w.N.

einer Person zugeordnet werden können.[1920] Dieses Ergebnis wird auch von der datenschutzrechtlichen Einordnung unterstützt, die überwiegend davon ausgeht, dass die in Blockchains enthaltenen Daten personenbezogene Daten sind.[1921] Soweit darüber hinaus (dynamische) IP-Adressen von den Auswertungsmethoden betroffen sind, liegen eindeutig personenbezogene Daten vor.

Der Eingriff in das RiS bei öffentlich verfügbaren Daten liegt nach hier vertretener Auffassung vor, wenn über die bloße Kenntnisnahme hinaus, öffentlich verfügbare Daten erhoben und gespeichert werden und sich eine Persönlichkeitsgefährdung des Einzelnen daraus ergibt, dass er nicht mehr überblicken kann, welche Daten über ihn erhoben werden und welche Schlüsse sich durch weitergehende Datenverarbeitungsmaßnahmen ergeben können.[1922] Dies ist bei allen hier untersuchten Auswertungsmethoden der Fall. Eine Besonderheit ergibt sich allerdings für das Herunterladen der jeweiligen Blockchain-Daten. Dies stellt noch keinen Eingriff in das RiS dar, da zwar umfangreiche Daten, die bereits chronologisch geordnet sind, den Strafverfolgungsbehörden verfügbar gemacht werden, dies hat aber lediglich den technischen Hintergrund der Funktionsweise der Blockchain-Technologie und darf insoweit rechtlich nicht anders bewertet werden als die bloße Kenntnisnahme öffentlich verfügbarer Daten.[1923] Anders ist dies jedoch im Rahmen des Datenschutzrechts der DSGVO zu bewerten, da hier nach Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 2 DSGVO bereits in der bloßen Teilnahme an dem *Peer-to-Peer*-Netzwerk der Blockchain und dem Herunterladen der Blockchain-Daten ein datenschutzrechtlich relevanter Verarbeitungsvorgang vorliegt, für den ein Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO erfüllt sein muss.[1924] Zu beachten ist allerdings, dass das Datenschutzrecht der DSGVO nur für den Einsatz der Auswertungsmethoden durch Private gilt.[1925]

Zwar kommt auch ein Eingriff in den Schutzbereich des Telekommunikationsgeheimnisses und des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (nachfolgend als „IT-Grundrecht“ bezeichnet) in Betracht.[1926]

1920 Siehe hierzu unter Kap. 4, B.II.1.c) m.w.N.
1921 Siehe hierzu im Einzelnen unter Kap. 6, A.I.1. m.w.N.
1922 Siehe hierzu im Einzelnen unter Kap. 4, B.II.2.b). m.w.N.
1923 Siehe hierzu im Einzelnen unter Kap. 4, B.II.2.c)(1).
1924 Siehe hierzu oben unter Kap. 6, A.I.1.
1925 Siehe zum Anwendungsbereich der DSGVO bereits oben unter Kap. 6, A.I., II.
1926 Siehe hierzu insgesamt oben unter Kap. 4, B.I., III.

Allerdings ist vom Schutzbereich des Telekommunikationsgeheimnisses nur Individualkommunikation erfasst. Nicht von Art. 10 Abs. 1 GG geschützt wird dagegen Massenkommunikation. Problematisch kann diese Abgrenzung zwar bei der Telekommunikation im Internet auf Grund der zu unterscheidenden Kommunikationsebenen sein.[1927] Für die hier gegenständliche Untersuchung wurde die geschützte Individualkommunikation von der nicht geschützten Massenkommunikation dahingehend abgegrenzt, ob auf die jeweilige Kommunikation ohne weitere Autorisierung von außen zugegriffen wurde.[1928] Für die Auswertungsmethoden bedeutet das, dass jedenfalls die in der Blockchain enthaltenen Daten keine geschützte Individualkommunikation sind, sondern nicht geschützte Massenkommunikation darstellen.[1929] Dies gilt auch für die Auswertung anderweitig verfügbarer Daten, soweit nicht von außen unautorisiert auf Telekommunikation zugegriffen wird. Gleiches gilt für die Auswertung der Verbreitung von Transaktionsnachrichten, die sog. Bloom-Filter-Attacks und die Auswertung des Datenverkehrs durch das Tor-Netzwerk, da auch bei diesen nicht von außen auf individuelle Telekommunikationsvorgänge zugegriffen wird.[1930] Da außerdem nach hier vertretener Auffassung vom Schutzbereich des Telekommunikationsgeheimnisses nicht das Verschlüsseln von Telekommunikation erfasst ist, kann in entsprechender Anwendung auch das Verschleiern von Telekommunikationsumständen nicht vom Schutzbereich des Telekommunikationsgeheimnis erfasst sein, sodass der Schutzbereich nicht eröffnet ist, wenn die Nutzung des Tor-Netzwerkes unterbunden wird.[1931]

Ebenfalls nicht eröffnet ist der Schutzbereich des IT-Grundrechts, da bei dem staatlichen Zugriff auf eine Blockchain weder Vertraulichkeits- noch Integritätserwartungen verletzt werden. Maßgeblicher Grund hierfür ist, dass die Daten aus offenen Netzwerken zur Kenntnis genommen werden.[1932]

1927 Siehe hierzu Kap. 4, B.I.1.c)(1).
1928 Siehe hierzu Kap. 4, B.I.1.c)(5).
1929 Siehe hierzu Kap. 4, B.I.2.a).
1930 Siehe hierzu Kap. 4, B.I.2.b).
1931 Siehe hierzu Kap. 4, B.I.2.b)(3).
1932 Siehe hierzu Kap. 4, B.III.3.

C. Verfassungsrechtliche Rechtfertigung dieses Eingriffs

Als Rechtfertigung für diesen Grundrechtseingriff kann zum Zweck der Strafverfolgung nur § 161 Abs. 1 StPO herangezogen werden, der jedoch einen Anfangsverdacht voraussetzt und nur zu geringfügigen Grundrechtseingriffen ermächtigt.

I. § 161 Abs. 1 StPO als einschlägige Ermittlungsbefugnis

§ 161 Abs. 1 StPO ist als Ermächtigungsgrundlage einschlägig, da keine der speziellen Ermittlungsbefugnisse der StPO einschlägig ist und auch keine Vergleichbarkeit mit besonders geregelten Ermittlungsbefugnissen vorliegt.[1933]

So ermächtigen etwa die Vorschriften zur Sicherstellung und Beschlagnahme nach §§ 94ff. StPO zwar auch zur Auswertung von sichergestellten Daten. Bei den hier gegenständlichen Auswertungsmethoden steht allerdings nicht das Verfügbarmachen von Daten im Vordergrund steht, sondern deren Auswertung.[1934]

Ebenfalls nicht einschlägig ist die Ermittlungsbefugnis zur Rasterfahndung nach § 98a StPO. Zwar ermächtigt § 98a StPO grundsätzlich zu einem maschinellen Datenabgleich personenbezogener Daten, erforderlich ist jedoch, dass sich dieser Datenabgleich auf Daten bezieht, die entweder zuvor freiwillig herausgegeben wurden oder nach § 98a Abs. 2 StPO erhoben wurden. Für die von den Auswertungsmethoden betroffenen Daten ist keine dieser Varianten auf Grund des begrenzten Wortlauts von § 98a Abs. 2 StPO der Fall.[1935]

Schließlich sind auch §§ 98c StPO, 100a, 100b, 100g, 100j StPO nicht einschlägig. § 98c StPO bezieht sich nur auf den internen maschinellen Datenabgleich.[1936] § 100a StPO ist nicht einschlägig, da bereits der Schutzbereich des Art. 10 Abs. 1 GG nicht eröffnet ist.[1937] § 100b StPO ermächtigt nur zu einem Zugriff auf informationstechnische Systeme auf einem technisch nicht dafür vorgesehenen Weg.[1938] Schließlich liegen in den erhobenen Da-

1933 Siehe hierzu insgesamt Kap. 5, B.
1934 Siehe hierzu im Einzelnen unter Kap. 5, B.I.
1935 Siehe hierzu im Einzelnen unter Kap. 5, B.II.
1936 Siehe hierzu im Einzelnen unter Kap. 5, B.III.
1937 Siehe hierzu im Einzelnen unter Kap. 5, B.IV.
1938 Siehe hierzu im Einzelnen unter Kap. 5, B.V.

ten weder Verkehrs- noch Bestandsdaten im Sinne der §§ 100g, 100j StPO vor, sodass auch diese nicht einschlägig sind.[1939]

II. Einsatz der Auswertungsmethoden nur bei bestehendem Anfangsverdacht

Auf Grund des für § 161 Abs. 1 StPO erforderlichen Anfangsverdachts können die Auswertungsmethoden jeweils nur dann eingesetzt werden, wenn bereits aus anderen Gründen der Verdacht einer Straftat besteht.[1940] Ein Einsatz zur (unmittelbaren) Begründung eines Anfangsverdachts ist dagegen nicht zulässig – selbst wenn die Blockchain-Daten nach Transaktionsmustern durchsucht werden, die mit sehr hoher Wahrscheinlichkeit im Zusammenhang mit illegalen Aktivitäten stehen.[1941] Denn grundsätzlich ist für den Anfangsverdacht das Vorliegen zureichender tatsächlicher Anhaltspunkte erforderlich, die auf eine Straftat hindeuten.

Dies ist weder beim proaktiven Aufklären von Dunkelfeldern noch bei sog. Vorermittlungen der Fall.[1942] Darüber hinaus nahm das BVerfG im MIKADO-Fall zwar einen Anfangsverdacht für die Abfrage von bestimmten Kreditkartendaten an, die sich auf konkrete Tatumstände, wie etwa ein bestimmter Buchungsbetrag zugunsten eines bestimmten Zahlungsempfängers unter Angabe einer bestimmten Merchant-ID, bezog.[1943] Dies kann jedoch hier keine Anwendung auf die Suche nach Transaktionsmustern finden, da im MIKADO-Fall des BVerfG nach Tätern bei bereits bestehendem Anfangsverdacht gesucht wurde, wohingegen bei der Suche nach bestimmten Transaktionsmustern eine *Tat*- und keine *Tätersuche* vorliegt.[1944]

III. Nur geringfügige Grundrechtseingriffe nach § 161 Abs. 1 StPO

Ein noch geringfügiger Grundrechtseingriff liegt vor, wenn beim sog. *Entitäts-Clustering* lediglich eine bereits aus anderen Gründen verdächtige

1939 Siehe hierzu im Einzelnen unter Kap. 5, B.VI., VII.
1940 Siehe hierzu unter Kap. 5, D.I.2.b).
1941 Siehe hierzu unter Kap. 5, D.I.2.a), c).
1942 Siehe hierzu unter Kap. 5, D.I.1.a), d).
1943 Siehe hierzu unter Kap. 5, D.I.1)g).
1944 Siehe hierzu unter Kap. 5, D.I.2.c).

Transaktion oder *Bitcoin-Adresse* betrachtet wird.[1945] Hinsichtlich der Auswertungsmethoden, die darüber hinaus Transaktionsverhalten und -muster ermitteln und vergleichen, liegt ein geringfügiger Grundrechtseingriff allenfalls vor, wenn diese in der Form eines „Treffer-/Nichttreffer-Modells" eingesetzt werden, um zu vermeiden, dass eine große Anzahl Unbeteiligter von weiteren strafrechtlichen Ermittlungen betroffen wird.[1946] Nicht mehr geringfügig sind die mit diesen Auswertungsmethoden verbundenen Grundrechtseingriffe allerdings, wenn die Blockchain-Daten insgesamt anlassunabhängig durch eine dieser Auswertungsmethoden systematisch analysiert werden.[1947]

Denn bei der Auswertung von unmittelbaren Blockchain-Daten ist die Grundrechtsintensität zwar insbesondere dadurch erhöht, dass bei den ausgewerteten Blockchain-Daten eine insgesamt große Datenmenge vorliegt, die heimlich erhoben wird, systematisch und technikgestützt ausgewertet wird und auf Grund ihrer Nähe zu Kontoinformationen wohl eine besondere Persönlichkeitsrelevanz aufweisen kann.[1948] Intensitätsverringernd ist jedoch zu beachten, dass die Erhebung der Blockchain-Daten selbst noch keinen Grundrechtseingriff begründet, die Blockchain-Daten öffentlich verfügbar sind und erst durch Zusatzwissen einer Person zugeordnet werden können.[1949]

Unterschiedlich ist bei den einzelnen Auswertungsmethoden allerdings die Streubreite zu berücksichtigen, die mit der jeweiligen technischen Funktionsweise einhergeht.[1950]

So kann etwa das einfache *Entitäts-Clustering,* soweit es bezogen auf eine bestimmte *Bitcoin-Adresse* oder Transaktion stattfindet, mit einer einfachen Suchfunktion verglichen werden. Hierbei werden nur Transaktionen und weitere *Bitcoin-Adressen* ermittelt, die im Zusammenhang mit dieser bestimmten Bitcoin-Adresse oder Transaktion stehen.[1951] Insoweit findet zwar grundsätzlich ein Datenabgleich aller in der Blockchain enthaltenen Transaktionen statt, ein Grundrechtseingriff liegt jedoch bei den Nichttreffern

1945 Siehe hierzu im Einzelnen unter Kap. 5, D.II.3.a).
1946 Siehe hierzu im Einzelnen unter Kap. 5, D.II.3.b), c).
1947 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1948 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1949 Siehe hierzu insgesamt unter Kap. 5, D.II.3.a), b), c).
1950 Siehe hierzu jeweils unter Kap. 5, D.II.3.a), b), c).
1951 Siehe hierzu unter Kap. 5, D.II.3.a).

nicht vor, da diese anonym und spurenlos wieder ausgeschieden werden und sich auch kein spezifisches Interesse an diesen Daten verdichtet hat.[1952]

Anders muss dies bewertet werden bei den Auswertungsmethoden, die Transaktionen und *Bitcoin-Adressen* mit bestimmten Transaktionsmustern vergleichen. Denn hierbei ist jeweils erforderlich, dass vor dem Abgleich, ob eine bestimmte Transaktion einem bestimmten Muster ähnelt oder nicht, durch eine systematische Analyse ein entsprechendes Muster überhaupt erst ermittelt wird.[1953] Die derart erhöhte Streubreite führt dazu, dass grundsätzlich kein geringfügiger Grundrechtseingriff mehr vorliegt. Geringfügig kann der Grundrechtseingriff daher allenfalls noch sein, wenn lediglich ein „Treffer-/Nichttreffer-Modell" verwendet wird.[1954]

Zu einem anderen Ergebnis gelangt die Bewertung der Grundrechtsintensität der Auswertungen des Netzwerkverhaltens. Bei diesen Auswertungsmethoden liegt grundsätzlich kein geringfügiger Grundrechtseingriff mehr vor, sodass sie nicht auf § 161 Abs. 1 StPO gestützt werden können.[1955] Denn bei der Auswertung des Weiterleitungsverhaltens von Transaktionsnachrichten liegt bereits ein Grundrechtseingriff durch die Erhebung der Daten vor, sodass insoweit auch eine erhöhte Streubreite vorliegt.[1956] Ähnlich gilt dies für die sog. *Bloom-Filter-Attacks,* da dies in der Ermittlungspraxis nur sinnvoll einsetzbar ist, wenn in einem konkreten Verdachtsfall bei allen *SPV-Clients* abgefragt werden müsste, ob eine verdächtige *Bitcoin-Adresse* in dem jeweiligen *Bloom-Filter* enthalten ist.[1957] Nur so kann die Zuordnung einer verdächtigen *Bitcoin-Adresse* zu einer bestimmten IP-Adresse vorgenommen werden.

Schließlich hängt die Grundrechtsintensität der Auswertung anderweitig verfügbarer Daten wohl von deren konkretem Einsatz ab.[1958] So dürfte ein noch geringfügiger Grundrechtseingriff vorliegen, wenn lediglich im öffentlich verfügbaren Internet nach einer bestimmten *Bitcoin-Adresse* gesucht wird.[1959] Anders ist dies jedoch zu beurteilen, wenn anlassunabhängig mittels *Web-Crawler* die öffentlich verfügbaren Inhalte im Internet nach möglichst vielen Hintergrundinformationen durchsucht werden, um so

1952 Siehe hierzu unter Kap. 5, D.II.3.a).
1953 Siehe hierzu jeweils unter Kap. 5, D.II.3.b), c).
1954 Siehe hierzu jeweils unter Kap. 5, D.II.3.b), c).
1955 Siehe hierzu insgesamt unter Kap. 5, D.II.3.d).
1956 Siehe hierzu unter Kap. 5, D.II.3.d).
1957 Siehe hierzu unter Kap. 5, D.II.3.d)(4).
1958 Siehe hierzu insgesamt unter Kap. 5, D.II.3.e)
1959 Siehe hierzu unter Kap. 5, D.II.3.e)(1).

hierauf im Verdachtsfall zurückgreifen zu können.[1960] Hinsichtlich der Auswertung von Dritt-Anbieter-Cookies und IoT-Blockchain-Anwendungen hängt die jeweilige Grundrechtsintensität grundsätzlich von deren konkreter Umsetzung ab.[1961] Dabei dürfte insbesondere relevant werden, ob und welche Rückschlüsse auf die Persönlichkeit gezogen werden können und ob und wie viele Unbeteiligte von den Auswertungsmethoden betroffen werden.

D. Empfehlung und Ausblick

Zusammenfassend lässt sich festhalten, dass die Blockchain-Technologie neben dem Entwicklungspotenzial, das ihr zugeschrieben wird, auch viele Ansatzpunkte für strafrechtliche Ermittlungen bieten kann. Einige dieser Auswertungsmethoden lassen sich zwar als geringfügige Grundrechtseingriffe noch auf die strafprozessualen Ermittlungsgeneralklauseln stützten, andere Auswertungsmethoden übersteigen dagegen die Grenze der Geringfügigkeit. Dies kann zur Rechtsunsicherheit führen. Denn die Untersuchung hat auch gezeigt, dass die Bewertung der Grundrechtsintensität einerseits aufwändig ist und andererseits von vielen einzelnen Faktoren abhängt. Das könnte zur Folge haben, dass bereits bei geringfügigen technischen Anpassungen sowohl der jeweils ausgewerteten Blockchain als auch der eingesetzten Auswertungsmethode der Einsatz der Auswertungsmethoden als nicht mehr nur geringfügiger Grundrechtseingriff zu bewerten ist. Insoweit müsste bei jeder technischen Anpassung auch eine angepasste Bewertung der Grundrechtsintensität vorgenommen werden – immer mit der Gefahr verbunden, dass eine nicht mehr nur geringfügige Intensität vorliegt.

Empfehlenswert ist daher die Neuregelung derartiger Ermittlungsmöglichkeiten in der vorgeschlagenen Form eines § 98a Abs. 2 S. 2 StPO:

> *„Zu diesem Zweck sind die Strafverfolgungsbehörden außerdem ermächtigt, allgemein zugängliche Daten zu erheben und für den Abgleich zu verarbeiten.“*[1962]

Denn hierdurch würde Rechtssicherheit dahingehend geschaffen, dass auch öffentlich verfügbare personenbezogene Daten unter bestimmten Voraus-

1960 Siehe hierzu unter Kap. 5, D.II.3.e)(1).
1961 Siehe hierzu unter Kap. 5, D.II.3.e)(2), (3).
1962 Siehe hierzu im Einzelnen unter Kap. 5, F.

setzungen zur Strafverfolgung maschinell abgeglichen werden dürfen. Das wäre zugleich ein erster Schritt in Richtung auf die grundlegende Frage, wie öffentlich verfügbare Daten zur Strafverfolgung ausgewertet werden dürfen. Denn im Rahmen der vorstehenden Untersuchung ist unter anderem auch aufgefallen, dass die Ermittlungsbefugnisse der StPO vorrangig an die Art und Weise der Datenerhebung anknüpfen. Dagegen stellen sie nicht auf die Art und Weise der Auswertung von Daten ab. Die Art und Weise der Auswertung von Daten kann jedoch – wie die vorstehende Untersuchung gezeigt hat – ähnlich ausschlaggebend für die Intensität von Grundrechtseingriffen sein. Und sie ist erst recht relevant angesichts der technischen Dynamik und der damit verbundenen Möglichkeiten, die in diesem Bereich zu erwarten sind.