Kapitel 6 – Exkurs – Datenschutzrechtliche Einordnung (privater) Auswertungen von Blockchain-Systemen

Blockchains sind mittlerweile auch Gegenstand der juristischen Diskussionen im Rahmen des europäischen Datenschutzrechts der DSGVO. Hierbei stellen sich etwa Fragen, die teilweise Ähnlichkeit zu den bereits diskutierten Fragen der strafprozessualen Zulässigkeit haben.

Diese Fragen sollen nachfolgend kurz dargestellt werden, um zu prüfen, ob und inwieweit sie etwa zur Unterstützung der vorstehenden Ergebnisse der strafprozessualen Zulässigkeit von Blockchain-Auswertungen herangezogen werden können.

So ist etwa auch für die Eröffnung des sachlichen Anwendungsbereichs der DSGVO zunächst erforderlich, dass personenbezogene Daten vorliegen[1789] (hierzu unter A.). Darüber hinaus muss – soweit der Anwendungsbereich der DSGVO eröffnet ist – ein Erlaubnistatbestand für jegliche Datenverarbeitungen im Zusammenhang mit Blockchains einschlägig und erfüllt sein[1790] (siehe hierzu unter B.).

A. Anwendungsbereich der DSGVO

Für die Eröffnung des Anwendungsbereichs der DSGVO ist in sachlicher Hinsicht nach Art. 2 Abs. 1 DSGVO erforderlich, dass eine „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten“[1791] oder

1789 Vgl. Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 DSGVO; *Bechtolf Vogt,* ZD 2018, 66 (68); *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 72.

1790 Vgl. *Hofert,* ZD 2017, 161 (165), der allerdings noch auf die zu diesem Zeitpunkt geltenden Erlaubnistatbestände des BDSG abstellt. Siehe zum Erfordernis von Erlaubnistatbeständen allgemein Simitis-Hornung-Spiecker/*Albrecht,* Einführung zu Art. 6, Rn. 1. Über diese Fragen hinaus werden etwa auch die Fragen nach der datenschutzrechtlichen Verantwortlichkeit bei Blockchains und nach der hinreichenden Umsetzbarkeit von Betroffenenrechte in der Blockchain diskutiert. Siehe hierzu etwa *Janicki/Saive,* ZD 2019, 251 (252f.); ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 171ff; *Bechtolf/Vogt,* ZD 2018, 66 (69f.). Da diese Fragen allerdings keine unmittelbare Relevanz für die hier gegenständliche Untersuchung haben, werden sie hier nicht dargestellt.

1791 So der Wortlaut des Art. 2 Abs. 1 Hs. 1 DSGVO.

eine „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“[1792] vorliegt.[1793] Darüber hinaus darf keiner der in Art. 2 Abs. 2 DSGVO aufgeführten Ausnahmetatbestände vorliegen.

I. Verarbeitung personenbezogener Daten

Sowohl der Begriff der „Verarbeitung“ als auch der Begriff der „personenbezogenen Daten“ werden in Art. 4 Nr. 1, Nr. 2 DSGVO legal definiert.

1. Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO

Art. 4 Nr. 1 DSGVO definiert personenbezogene Daten als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“[1794].

Grundsätzlich ist insoweit erforderlich, dass Daten verarbeitet werden, die sich mindestens auf eine identifizierbare Person beziehen. Daten, die

1792 So der Wortlaut des Art. 2 Abs. 1 Hs. 2 DSGVO.

1793 Die Eröffnung des räumlichen Anwendungsbereichs nach Art. 3 DSGVO ist für die hier gegenständliche Untersuchung nicht relevant, da sie lediglich voraussetzt, dass die für die Datenverarbeitung verantwortliche Stelle oder der Auftragsverarbeiter eine Niederlassung innerhalb der EU hat, vgl. BeckOK-DSR/*Hanloser,* DSGVO Art. 3 Rn. 2. Dies kann zwar für die Frage nach dem anwendbaren Datenschutzrecht beim Fortschreiben der jeweiligen Blockchain relevant werden (siehe zur technischen Funktionsweise des Fortschreibens von Blockchains oben unter Kap. 2, A.III.), bei dem hier gegenständlichen Einsatz der Auswertungsmethoden wird dagegen davon ausgegangen, dass die Datenverarbeitung von einer verantwortlichen Stelle innerhalb der EU vorgenommen wird, sodass jedenfalls der territoriale Anwendungsbereich der DSGVO eröffnet ist.

1794 Art. 4 Nr. 1 DSGVO.

keinerlei Personenbezug aufweisen, sind dementsprechend vom Anwendungsbereich der DSGVO ausgenommen.[1795]

Bisher ist nicht eindeutig geklärt, aus welcher Perspektive die Identifizierbarkeit von natürlichen Personen zu beurteilen ist.[1796] Dies ist auch für die Verarbeitung von Daten in Blockchains besonders relevant. Denn auf Grund der dezentralen Verwaltungsstruktur von Blockchains[1797] verfügt keine zentrale Instanz über die Möglichkeit alle verwendeten *public keys* bzw. *Bitcoin-Adressen* einer natürlichen Person zuzuordnen. Im Umkehrschluss bedeutet dies jedoch nicht, dass die natürlichen Personen nicht identifizierbar sind. Denn etwa der zur Identifizierung verpflichtete[1798] *Exchange-Anbieter* kann die verwendete *Bitcoin-Adresse* eines Kunden mit dessen Kundendaten in Verbindung bringen. Andererseits ist es darüber hinaus insbesondere möglich, bestimmte *Bitcoin-Adressen* einfach zu googlen und hieraus entweder die Identität der natürlichen Person oder weitere Anhaltspunkte hierfür zu erhalten.[1799]

Insoweit ist für die Beurteilung, ob personenbezogene Daten vorliegen oder nicht, insbesondere die Perspektive und die Erkenntnisquellen desjenigen, der die Daten verarbeitet, relevant.[1800]

Umstritten war bereits im Rahmen des BDSG und der RL 95/46/EG (nachfolgend „DS-RL") die Grenze der Bestimmbarkeit bei personenbezo-

1795 Sydow-DSGVO/*Ziebarth,* Art. 4 Rn. 24 m.w.N; BeckOK-DSR/*Schild,* DS-GVO Art. 4 Rn. 15.

1796 Siehe hierzu ausführlich etwa *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 85ff.

1797 Siehe hierzu bereits ausführlich oben unter Kap. 2, B.III. m.w.N.

1798 Die Identifizierungspflicht ergibt sich aus § 1 Abs. 11 Nr. 10 KWG i.V.m. § 2 Abs. 1 Nr. 2, §§ 10ff. GwG.

1799 Gibt man etwa die *Bitcoin-Adresse* „165dtfwNvyMUbLGdqf87w8DfZX7i542Fyr" bei Google ein, führt das erste Suchergebnis zu einer Analyseseite, auf der man sämtliche Ein- und Ausgänge dieser *Bitcoin-Adresse* nachvollziehen kann (https://www.blockchain.com/btc/address/165dtfwNvyMUbLGdqf87w8DfZX7i542Fyr letzter Abruf: 20. Dezember 2021). Als zweites Suchergebnis gelangt man auf die Spendenseite der Tageszeitung „taz" (https://taz.de/1-Zahlen-mit-Bitcoins/!142454/ letzter Abruf: 20. Dezember 2021), auf der erkennbar ist, dass diese *Bitcoin-Adresse* als Spendenkonto der taz verwendet wird.

1800 Vgl. *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 73. Darüber hinaus ist auch maßgeblich relevant, um welche Daten es sich handelt, da der Nutzer einer Blockchain ja gerade durch die Art und Weise seiner Nutzung Einfluss auf seine Identifizierung nehmen kann.

genen Daten.[1801] Dieser Streit hat sich auch mit Inkrafttreten der DSGVO nicht geklärt.[1802]

Bei Daten in Blockchain-Systemen geht mittlerweile die überwiegende Auffassung davon aus, dass personenbezogenen Daten wohl häufig vorliegen.[1803] Dies kann allerdings von einer Einzelfallbetrachtung hinsichtlich der verarbeitenden Stelle und der verarbeiteten Informationen abhängig sein.[1804]

Insoweit besteht eine Parallelität zwischen der Reichweite des Personenbezugs im Rahmen der DSGVO und des RiS.[1805]

Zu beachten ist jedoch ein wesentlicher Unterschied zwischen der Einordnung im Rahmen des RiS und im Rahmen der DSGVO: im Rahmen des RiS wurde die Einordnung maßgeblich damit begründet, dass die Strafverfolgungsbehörden gegenüber den zur Identifizierung verpflichteten Stellen nach § 161 Abs. 1 StPO i.V.m. §§ 32 Abs. 3 i.V.m. 30 Abs. 3 GwG Auskunft über die Identitätsdaten von bestimmten *Bitcoin-Adressen* verlangen konnten.[1806] Diese Befugnisse stehen privaten Stellen grundsätzlich nicht zu. Allerdings bestehen auch für private Stellen grundsätzlich Möglichkeiten, einen Personenbezug herzustellen.[1807]

Insoweit liegen bei Blockchain-Daten auch im Rahmen der DSGVO in der Regel personenbezogene Daten vor.

1801 Siehe hierzu ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 75ff. Dieser Meinungsstreit wurde bereits im Rahmen des RiS dargestellt, siehe hierzu ausführlich unter Kap. 4, B.II.1.b)(2) m.w.N.

1802 Vgl. *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 85.

1803 *Bechtolf/Vogt*, ZD 2018, 66 (69); *Böhme/Pesch,* DuD 2017, 473 (481); *Finck*, Blockchain and the GDPR, S. 14ff; *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 121ff; BeckOK-DSR/*Schild,* DSGVO Art. 4 Rn. 20a.

1804 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 122f., der nachfolgend Fallgruppen bildet und diese hinsichtlich eines möglichen Personenbezugs einordnet.

1805 Ein Grund hierfür dürfte allerdings maßgeblich auch darin liegen, dass zur Frage, ob im Rahmen des RiS personenbezogene Daten vorliegen hinsichtlich der Identifizierbarkeit insbesondere auch auf die Maßstäbe des Datenschutzrechts der DSGVO und des früheren BDSG abgestellt wird, vgl. hierzu bereits ausführlich oben unter Kap. 4, B.II.1.b).

1806 Siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.1.c).

1807 Zu diesen Möglichkeiten insbesondere *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 138 m.w.N.

Dieses Ergebnis unterstreicht dementsprechend das bereits im Rahmen des RiS erörterte Ergebnis, dass bei den hier gegenständlichen Auswertungsmethoden grundsätzlich personenbezogene Daten verarbeitet werden.

2. Verarbeitung

Außerdem müssen für den Anwendungsbereich der DSGVO diese personenbezogenen Daten auch verarbeitet werden.[1808] Art. 4 Nr. 2 DSGVO definiert den Begriff der Verarbeitung als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“[1809]. Dementsprechend liegt grundsätzlich bei jedem Vorgang im Zusammenhang mit personenbezogenen Daten ein datenschutzrechtlich relevanter Verarbeitungsvorgang vor.[1810]

Insoweit liegt bereits durch das Herunterladen der jeweiligen Blockchain und durch die Teilnahme am *Peer-to-Peer*-Netzwerk der jeweiligen Blockchain ein datenschutzrechtlich relevanter Verarbeitungsvorgang vor, für den insbesondere ein Erlaubnistatbestand einschlägig sein muss.

Hieraus ergibt sich insoweit ein Unterschied zu der im Rahmen des RiS definierten Eingriffs-Grenze: Nach der Rechtsprechung des BVerfG ist diese bei öffentlich verfügbaren Daten erst erreicht, wenn allgemein zugängliche Informationen gezielt zusammengetragen, gespeichert oder unter Hinzuziehung weitere Daten ausgewertet werden und sich hieraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt.[1811] Ein derart rechtfertigungsbedürftiger Eingriff in das RiS liegt daher bei den

1808 Vgl. Art. 2 Abs. 1 DSGVO.
1809 So der Wortlaut des Art. 4 Nr. 2 DSGVO.
1810 BeckOK-DSR/*Schild*, Art. 4 Rn. 29; Simitis-Hornung-Spiecker/*Roßnagel*, DSGVO Art. 4 Nr. 2 Rn. 11; Ehmann-Selmayr/*Klabunde*, DSGVO Art. 4 Rn. 23.
1811 BVerfGE 120, 274 (345); siehe hierzu bereits ausführlich oben unter Kap. 4, B.II.2.b).

unmittelbaren Blockchain-Daten erst vor, wenn über ihr bloßes Herunterladen hinaus weitergehende Rückschlüsse gezogen werden.[1812]

Insoweit besteht ein Unterschied zwischen dem verfassungsrechtlichen Datenschutz und dem Datenschutz der DSGVO: während beim Datenschutz der DSGVO für jeden einzelnen Verarbeitungsvorgang personenbezogener Daten ein Erlaubnistatbestand erfüllt sein muss, ist eine verfassungsrechtliche Rechtfertigung im Rahmen des RiS nur erforderlich, wenn öffentlich verfügbare Informationen gezielt zusammengetragen und gespeichert werden.

Ein Grund für diesen Unterschied könnte darin liegen, dass die verfassungsrechtliche Rechtfertigung von Grundrechtseingriffen höhere Anforderungen voraussetzt als das Vorliegen eines Erlaubnistatbestandes der DSGVO. So ist etwa für eine verfassungsrechtliche Rechtfertigung von Eingriffen in das RiS eine gesetzliche Grundlage erforderlich, die das Zitiergebot beachtet, hinreichend bestimmt die Möglichkeiten und Grenzen des Eingriffs festlegt und ein angemessenes Verhältnis zwischen Zweck und Mittel des Eingriffs aufweist.[1813] Dagegen ist für die Rechtmäßigkeit von Datenverarbeitungen nach der DSGVO neben der Beachtung der Datenschutzgrundsätze des Art. 5 maßgeblich erforderlich, dass ein Erlaubnistatbestand des Art. 6 Abs. 1 DSGVO einschlägig ist. Unter diese Erlaubnistatbestände fallen etwa auch das Vorliegen einer Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO), die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e) oder die Wahrnehmung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DSGVO). Für die Datenverarbeitung durch öffentliche Stellen hat der Gesetzgeber in Ausübung seiner Befugnis nach Art. 6 Abs. 3 lit. b) DSGVO eine allgemeine „Auffangnorm zur Rechtfertigung der Datenverarbeitung im öffentlichen Raum"[1814] geschaffen, die umfassend für alle Verarbeitungen innerhalb des Anwendungsbereichs des BDSG gilt.

Insoweit ließe sich annehmen, dass die Anforderungen für die Rechtfertigung von Eingriffen in das RiS höher sind als für die Rechtfertigung von Datenverarbeitungen nach der DSGVO, sodass die bereits benannten unterschiedlichen Grenzen hierin ihren Grund finden.

1812 Sieh zur Eingriffsgrenze bei den hier gegenständlichen Auswertungsmethoden insgesamt Kap. 4, B.II.2.c).

1813 Siehe zu den verfassungsrechtlichen Anforderungen von Eingriffen in das RiS im Einzelnen oben unter Kap. 5, C.

1814 BeckOK-DSR/*Wolff*, BDSG § 3 Rn. 1.

Grundsätzlich bleibt jedenfalls festzuhalten, dass bereits mit dem Herunterladen der Blockchain-Daten, ebenso wie mit allen weiteren Vorgängen der hier gegenständlichen Auswertungsmethoden eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO vorliegt.

II. Kein Ausnahmetatbestand des Art. 2 Abs. 2 DSGVO

Ausgenommen vom Anwendungsbereich der DSGVO sind jedoch Verarbeitungen personenbezogener Daten, die einen der vier genannten Ausnahmetatbestände erfüllen. Dies sind Verarbeitungen:

- „im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts [fallen],
- Durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
- Durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
- Durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit."[1815]

Insoweit sind vom Anwendungsbereich der DSGVO insbesondere Datenverarbeitungen im Rahmen der gemeinsamen Sicherheits- und Außenpolitik, sowie die Datenverarbeitung im Zusammenhang mit Straftaten ausgenommen.[1816]

1815 So der Wortlaut des Art. 2 Abs. 2 lit. a) – d) DSGVO.

1816 Darüber hinaus ist die Reichweite des Ausnahmetatbestandes Art. 2 Abs. 2 lit. a) DSGVO schwierig zu bestimmen. Wegen der weitreichenden Zuständigkeiten und Rechtssetzungskompetenzen der EU ist sowohl im privaten Bereich als auch bei Datenverarbeitungen durch öffentliche Stellen davon auszugehen, dass der Ausnahmetatbestand keine praktischen Auswirkungen hat, vgl. BeckOK-DSR/*Bäcker,* DSGVO Art. 2 Rn. 7ff. Ferner betrifft Art. 2 Abs. 2 lit. c) die sehr restriktiv auszulegende sog. Haushaltsausnahme, die Datenverarbeitungen vom Anwendungsbereich der DSGVO ausnimmt, wenn diese *ausschließlich* zu privaten oder familiären Zwecken erfolgt, vgl. BeckOK-DSR/*Bäcker,* DSGVO Art. 2 Rn. 12ff. Siehe zur umfassenden Reichweite des Ausnahmetatbestandes Art. 2 Abs. 2 lit. d) DSGVO bezüglich aller Datenverarbeitungen im Zusammenhang mit Straftaten, Specht/Mantz-HdB DSR/*Rogenkamp,* § 21 Rn. 5.

Für die hier gegenständlichen Auswertungsmethoden könnte insbesondere der Ausnahmetatbestand des Art. 2 Abs. 2 lit. d) DSGVO relevant sein, der Datenverarbeitungen von zuständigen Stellen im Zusammenhang mit Straftaten vom Anwendungsbereich der DSGVO ausnimmt.[1817] Dieser Ausnahmetatbestand verläuft insoweit parallel zum Anwendungsbereich der JI-RL.[1818] Denn neben der DSGVO hat die EU außerdem die JI-RL erlassen, die für die „Verarbeitung personenbezogener Daten durch die zuständigen Behörden"[1819] zum Zweck „der Verhütung, Ermittlung, Aufdeckung, oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit"[1820] gilt.[1821]

Der bereits diskutierte Einsatz der Auswertungsmethoden durch die Strafverfolgungsbehörden zum Zweck der Strafverfolgung[1822] kann insoweit nicht in den Anwendungsbereich der DSGVO fallen.

Fraglich ist, ob dies auch gelten kann, wenn Privatpersonen die Auswertungsmethoden einsetzen. Maßgeblich dürfte insoweit sein, dass der Ausnahmetatbestand des Art. 2 Abs. 2 lit. d) DSGVO nur einschlägig ist, wenn die „zuständigen Behörden"[1823] die Datenverarbeitung vornehmen.[1824] Zwar kann dies einerseits bedeuten, dass der Ausnahmetatbestand nicht einschlägig ist, wenn Behörden entgegen den Zuständigkeitsvorschriften agieren und insoweit die DSGVO anwendbar ist.[1825] Andererseits bedeutet dies aber auch, dass der Ausnahmetatbestand jedenfalls nicht bei der Datenverarbeitung durch Privatpersonen einschlägig ist.

Insoweit ist der sachliche Anwendungsbereich der DSGVO für den Einsatz der hier gegenständlichen Auswertungsmethoden durch Privatpersonen eröffnet.

1817 Kühling-Buchner/*Kühling/Raab,* DSGVO Art. 2 Rn. 29.
1818 Kühling-Buchner/*Kühling/Raab,* DSGVO Art. 2 Rn. 29.
1819 So der Wortlaut aus Art. 2 Abs. 1 JI-RL.
1820 So der Wortlaut aus Art. 1 Abs. 1 JI-RL.
1821 Simitis-Hornung-Spiecker/*Roßnagel,* DSGVO Art. 2 Rn. 38. Die Vorgaben der JI-RL wurden mittlerweile durch den deutschen Gesetzgeber in Teil 3 des BDSG umgesetzt, vgl. Simitis-Hornung-Spiecker/*Roßnagel,* DSGVO Art. 2 Rn. 42.
1822 Siehe hierzu ausführlich oben unter Kap. 4, 5.
1823 So der Wortlaut des Art. 2 Abs. 2 lit. d) DSGVO.
1824 Sydow-DSGVO/*Enöckl,* Art. 2 Rn. 15.
1825 Sydow-DSGVO/*Enöckl,* Art. 2 Rn. 15.

III. Exkurs – Private Ermittlungen im Zusammenhang mit Straftaten und Kooperationen zwischen Strafverfolgungsbehörden und Privaten

Grundsätzlich stellen sich in diesem Zusammenhang aber auch zwei weitere Fragen: denn einerseits müssen private Ermittlungen auch grundsätzlich (strafprozess-)rechtlich zulässig sein. Andererseits kommt in der Praxis insbesondere in Betracht, dass derartige Ermittlungen von den Strafverfolgungsbehörden an Private ausgelagert werden. Daher stellt sich die weitere Frage, inwieweit eine derartige Auslagerung zulässig ist.

Weitgehende Einigkeit besteht zunächst dahingehend, dass auch Private befugt sind, Ermittlungen vorzunehmen und diesen Ermittlungen insbesondere kein staatliches Ermittlungsmonopol entgegensteht.[1826] Dies zeige sich bereits an der Zulässigkeit von Privat- und Nebenklage.[1827] Unterschiedlich werden allerdings die Grenzen privater Ermittlungen bewertet. So nimmt etwa *Bockemühl* an, dass verdeckte, technikgestützte Ermittlungen durch Private nicht zulässig seien, da die Vorschriften der §§ 100a, 100c, 100f StPO eine Sperrwirkung entfalten würden.[1828] Dem gegenüber nimmt die wohl überwiegende Auffassung in der Literatur an, dass die Grenze der Zulässigkeit privater Ermittlungen die allgemeinen Gesetze und insbesondere die Strafvorschriften darstellen.[1829] Dies könne im Einzelfall zwar zum gleichen Ergebnis führen, eine allgemeine Sperrwirkung der Befugnisse der Strafverfolgungsbehörden aus der StPO bestehe jedoch nicht.[1830]

1826 Löwe-Rosenberg/*Erb,* § 160, Rn. 9f.; MüKo-StPO/*Kölbel,* § 160 Rn. 25; Gercke/Julius/Temming/Zöller/*Zöller,* § 160, Rn. 8; *Hellmann,* Strafprozessrecht, Rn. 527ff.; SK-StPO/*Wohlers/Deiters,* § 160 Rn. 2; jeweils m.w.N. A.A. *Brunhöber* GA 2010, 571ff., die davon ausgeht, dass wegen des staatlichen Ermittlungsmonopols, die Zulässigkeit privater Ermittlungen positiv begründet werden müsse. Dies sei etwa bei privaten Ermittlungen durch den Beschuldigten und seine Vertreter der Fall, da der Beschuldigte nicht Objekt des Strafverfahrens werden dürfe. Dies gelte dem entgegen jedoch nicht für Verletzten einer Straftat. Siehe zur Zulässigkeit und Reichweite privater Ermittlungen ausführlich *Bockemühl,* Private Ermittlungen; *Stoffer,* Wie viel Privatisierung „verträgt" das strafprozessuale Ermittlungsverfahren.

1827 Löwe-Rosenberg/*Gössel,* Einleitung L , Rn. 183 m.w.N.

1828 *Bockemühl,* Private Ermittlungen, S. 86.

1829 *Hellmann,* Strafprozessrecht, Rn. 529; Löwe-Rosenberg/*Erb,* § 160 Rn. 10; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8.

1830 Zu beachten ist jedoch, dass den privaten Ermittlern die strafprozessualen Zwangsbefugnisse der StPO nicht zustehen, vgl. hierzu *Hellmann,* Strafprozessrecht, Rn. 529; Löwe-Rosenberg/*Erb,* § 160 Rn. 10; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8.

Ähnlich ist auch die Rechtsprechung des BGH zur Beweisverwertung von privaten Zeugenaussagen zu verstehen.[1831] Der BGH stellte etwa fest, dass es dem Verteidiger nicht verwehrt sei, „eigene Ermittlungen zu führen, inbes. Zeugen oder Mitbesch. vor und außerhalb der Hauptverhandlung zu befragen"[1832]. Hieraus leitet etwa *Jahn* ab, dass private Ermittlungen auch parallel zu laufenden staatlichen Strafverfahren grundsätzlich zulässig seien.[1833]

Festzuhalten bleibt, dass Ermittlungen durch Private grundsätzlich zulässig sind und die Grenze der Zulässigkeit in den allgemeinen Gesetzen – insbesondere den Strafvorschriften – liegt. Dementsprechend können auch die hier gegenständlichen Auswertungsmethoden grundsätzlich zu privaten Ermittlungen eingesetzt werden. Darüber hinaus können Beweise, die rechtmäßig von Privaten ermittelt wurden, grundsätzlich auch verwendet und verwertet werden.[1834]

Fraglich ist allerdings, ob und inwieweit eine Kooperation der Strafverfolgungsbehörden mit privaten Ermittlern zulässig ist. Hier besteht ebenfalls weitgehende Einigkeit darüber, dass Kooperationen der Strafverfolgungsbehörden mit Privaten grundsätzlich zulässig sind.[1835] So stellt etwa das BVerfG fest, dass auf Grund des Legalitätsprinzips hohe Anforderungen an die Unparteilichkeit der Personen zu stellen sind, derer sich die Strafverfolgungsbehörden bedienen, grundsätzlich könnten die Strafverfolgungsbehörden aber private Personen etwa als Sachverständige einbeziehen.[1836] Die Grenze dieser zulässigen Kooperation liegt allerdings darin, dass die Vorschriften des Prozessrechts hierdurch nicht umgangen werden dürfen

1831 Vgl. BGH StV 2003, 602f.
1832 BGH StV 2003, 602.
1833 *Jahn,* StV 2009, 41 (43).
1834 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 28; Vgl. *Hellmann,* Strafprozessrecht, Rn. 530. Umstritten ist allerdings, „inwieweit unzulässig erlangte Erkenntnisse ein Verwertungsverbot auslösen" können. Siehe hierzu ausführlich m.w.N. Löwe-Rosenberg/*Gössel,* Einleitung L., Rn. 183 ff.; vgl. *Hellmann,* Strafprozessrecht, Rn. 530, der feststellt, dass rechtswidrig erlangte Beweismittel nicht generell zu einem Verwertungsverbot führen, sondern „im Einzelfall unter Berücksichtigung aller maßgeblichen Umstände eine Abwägung des öffentlichen Interesses an einer möglichst vollständigen Wahrheitsermittlung und der schutzwürdigen Interessen des Betroffenen" vorzunehmen ist.
1835 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 27; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8; *Brunhöber,* GA 2010, 571 (576).
1836 BVerfG BeckRS 2007, 26565.

und die Staatsanwaltschaft die faktische Ermittlungsleitung nicht aus der Hand geben dürfen.[1837]

Insoweit dürfte bei einer Kooperation der Strafverfolgungsbehörden mit privaten Ermittlern, die die hier gegenständlichen Auswertungsmethoden einsetzen, nicht dazu führen, dass prozessrechtliche Vorschriften umgangen werden oder die faktische Leitung der Ermittlungshandlungen umgangen werden. Dementsprechend dürfen im Fall einer Kooperation die bereits dargestellten Grenzen des § 161 StPO[1838] für die hier gegenständlichen Auswertungsmethoden nicht umgangen werden.

IV. Zwischenergebnis

Der sachliche Anwendungsbereich der DSGVO setzt die Verarbeitung personenbezogener Daten durch eine private Stelle voraus. Da auch für private Stellen Möglichkeiten bestehen, die in der Blockchain enthaltenen Informationen einer Person zuzuordnen liegen hier personenbezogene Daten vor. Darüber hinaus liegt eine datenschutzrechtlich relevante Verarbeitung durch die bloße Teilnahme am *Peer-to-Peer*-Netzwerk der Blockchain und im Herunterladen der Blockchain-Daten vor. Darüber hinaus ist bei der hier betrachteten Anwendung der Auswertungsmethoden keiner der in Art. 2 Abs. 2 DSGVO enthaltenen Ausnahmetatbestände einschlägig. Schließlich sind auch private Ermittlungen und Kooperationen der Strafverfolgungsbehörden mit privaten Ermittlern grundsätzlich (strafprozess-)rechtlich zulässig, soweit nicht die Grenzen der allgemeinen Gesetze – insbesondere der Strafvorschriften – überschritten werden, die Vorschriften des Prozessrechtes hierdurch nicht umgangen werden und die faktische Ermittlungsleitung der Staatsanwaltschaft nicht abgegeben wird.

B. Rechtmäßigkeit der Datenverarbeitung

Wie bereits erwähnt, ist eine Datenverarbeitung nach der DSGVO nur rechtmäßig, wenn einer der insgesamt sechs in Art. 6 Abs. 1 DSGVO ab-

1837 Löwe-Rosenberg/*Erb,* § 160 Rn. 10; MüKo-StPO/*Kölbel,* § 160 Rn. 27; Gercke/Julius/Temming/Zöller/*Zöller,* § 160 Rn. 8; *Brunhöber,* GA 2010, 571 (576ff.).

1838 Siehe hierzu bereits ausführlich oben unter Kap. 5, D.

schließend aufgezählten Erlaubnistatbestände erfüllt ist.[1839] Dies sind die Einwilligung des Betroffenen (Art. 6 Abs. 1 lit. a) DSGVO), die Erfüllung eines Vertrages oder Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 lit. b) DSGVO), die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c) DSGVO), der Schutz lebenswichtiger Interessen ((Art. 6 Abs. 1 lit. d) DSGVO), die Erfüllung öffentlicher Aufgaben ((Art. 6 Abs. 1 lit. e) DSGVO) und die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f) DSGVO).[1840]

Im Rahmen der Datenverarbeitung bei Blockchains werden bisher insbesondere der Erlaubnistatbestand der Einwilligung des Betroffenen (hierzu unter I.) und die Wahrnehmung berechtigter Interessen (hierzu unter II.) diskutiert.[1841]

I. Art. 6 Abs. 1 lit. a) – Einwilligung des Betroffenen

Nach Art. 6 Abs. 1 lit. a) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die betroffene Person „ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke“[1842] erteilt hat. Dies wird grundsätzlich auch im Zusammenhang mit der Datenverarbeitung bei Blockchains in Betracht gezogen.[1843]

Für eine wirksame Einwilligung ist grundsätzlich erforderlich, dass sie in „informierter Weise“[1844] erfolgt.[1845] Dabei ist es auch möglich, dass eine

1839 Simitis-Hornung-Spiecker/*Roßnagel,* Einführung zu Art. 6 Rn. 1.

1840 Vgl. zur Aufzählung dieser Erlaubnistatbestände insbesondere *Peitz,* Datenschutzrechtliche Verantwortlichkeit in Blockchain-Systemen, S. 147.

1841 Darüber hinaus diskutiert *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 155ff. für den Vollzug von Transaktionen, ob der Erlaubnistatbestand der Erfüllung einer vertraglichen Pflicht oder Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 lit. b) DSGVO) bei einer privaten Blockchain einschlägig sein kann. Ausgeschlossen ist dies nach *Peitz* aber beim Betrieb der hier gegenständlichen öffentlichen Blockchains (siehe zur Begrenzung des Untersuchungsgegenstandes oben unter Kap. 2, B.IV.).

1842 So der Wortlaut des Art. 6 Abs. 1 lit. a) DSGVO.

1843 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149; vgl. zum BDSG etwa *Hofert,* ZD 2017, 161 (164); *Böhme/Pesch,* DuD 2017, 473 (479);

1844 So der Wortlaut des Art. 4 Nr. 11 DSGVO.

1845 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149; Auernhammer/*Kramer,* DSGVO Art. 6 Rn. 21.

Einwilligung konkludent erfolgt.[1846] Eine Willigung setzt nach Erwägungsgrund Nr. 42 S. 4 DSGVO voraus, „dass die betroffene Person mindestens weiß, ‚wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen'"[1847].

Insoweit käme grundsätzlich das Vorliegen einer konkludenten Einwilligung in die Datenverarbeitung zum Fortschreiben der Transaktionshistorie[1848] in Betracht. Dies wird aber aus mehreren Gründen abgelehnt[1849]:

So ist für das Vorliegen einer konkludenten Einwilligung erforderlich, dass eine eindeutig bestätigende Handlung vorliegt.[1850] Hierzu genügt es nicht, wenn lediglich eine Transaktionsnachricht an das Blockchain-Netzwerk versendet wird.[1851] Darüber hinaus dürfte es in der Regel an der nach Art. 4 Nr. 11 DSGVO erforderlichen Informiertheit bezüglich der Datenverarbeitung beim Versenden einer Transaktionsnachricht fehlen.[1852] Ferner bestehen grundsätzlich Zweifel am Vorliegen der erforderlichen Freiwilligkeit.[1853] Schließlich ist es auf Grund der technischen Funktionsweise von Blockchains[1854] in der Regel nicht möglich, die Einwilligung später zu widerrufen, da die einmal in die Datenblöcke aufgenommenen Transaktionen faktisch nachträglich nicht mehr verändert werden können.[1855]

Insoweit kann der in Art. 6 Abs. 1 lit. a) DSGVO enthaltene Erlaubnistatbestand der Einwilligung schon nicht für die Datenverarbeitung, die lediglich für das Fortschreiben der Transaktionshistorie erforderlich ist, herangezogen werden. Die hier gegenständlichen Datenverarbeitungen durch die Auswertungsmethoden können dementsprechend keinesfalls einer Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO unterfallen – zumal selbst beim

1846 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 150 m.w.N.

1847 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 149.

1848 Sieh zur technischen Funktionsweise bereits ausführlich oben unter Kap. 2, A.III.1.c).

1849 Siehe hierzu ausführlich *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 150ff.

1850 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151.

1851 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151.

1852 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 151f.

1853 Diese setzt nämlich auch voraus, dass die „Einwilligung ohne jeglichen Druck oder Zwang abgegeben […] [und] ohne Nachteile wieder zurückgenommen werden kann", *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 152 mit Verweis auf Erwägungsgrund Nr. 42 S. 5 DSGVO.

1854 Siehe hierzu ausführlich oben unter Kap. 2, A., B.

1855 Siehe zur technischen Funktionsweise oben unter Kap. 2, A.III.2.; *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 154.

Vorliegen einer Einwilligung in die Datenverarbeitung zum Fortschreiben der Blockchain sich diese nicht auf die hier gegenständlichen Auswertungsmethoden beziehen würde.[1856]

II. Art. 6 Abs. 1 lit. f) DSGVO – Wahrnehmung berechtigter Interessen

Ein weiterer Erlaubnistatbestand ist in Art. 6 Abs. 1 lit. f) DSGVO enthalten und berechtigt zur Verarbeitung personenbezogener Daten, wenn dies zur „Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist"[1857], „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen"[1858].

Die berechtigten Interessen des Art. 6 Abs. 1 lit. f) DSGVO sind grundsätzlich weit zu verstehen, so dass sowohl wirtschaftliche als auch ideelle und rechtliche Interessen hiervon erfasst sind.[1859] Dementsprechend sind jedenfalls die grundrechtlich geschützten Interessen des Verantwortlichen erfasst.[1860]

Kern dieses Erlaubnistatbestandes ist eine Abwägung der widerstreitenden Interessen – also der Interessen des für die Datenverarbeitung Verantwortlichen und des von der Datenverarbeitung Betroffenen.[1861] Maßgeblich für diese Interessenabwägung ist insoweit, zu welchem Zweck der Verantwortliche die jeweiligen Daten verarbeitet. So dürfte jedenfalls ein deutlicher Unterschied zwischen dem Fortschreiben der jeweiligen Blockchain-Transaktionen[1862] und den hier gegenständlichen Auswertungsmethoden bestehen.

So spricht etwa bei der Verarbeitung zum Zwecke des Fortschreibens der Blockchain grundsätzlich für ein überwiegendes Interesse des Verantwortli-

1856 Vgl. *Hofert,* ZD 2017, 161 (165).
1857 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 158.
1858 So der Wortlaut des Art. 6 Abs. 1 lit. f) DSGVO.
1859 Simitis-Hornung-Spiecker/*Schantz*, DSGVO Art. 6 Abs. 1 Rn. 98; BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 68; Auernhammer/*Kramer,* DSGVO Art. 6 Rn. 72; Rücker-Kugler/*Dienst,* Rn. 399.
1860 Simitis-Hornung-Spiecker/*Schantz*, DSGVO Art. 6 Abs. 1 Rn. 99; m.w.N; Paal-Pauly/*Frenzel,* DSGVO Art. 6 Rn. 28; vgl. Ehmann-Selmayr/*Heberlein,* DSGVO Art. 6 Rn. 25f.
1861 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 158.
1862 Siehe zur technischen Funktionsweise bereits ausführlich oben unter Kap. 2, A.III.

chen, dass der Nutzer einer Blockchain in der Regel mit der Datenverarbeitung rechnen muss.[1863]

Fraglich ist, ob dies auch für die hier gegenständlichen Auswertungsmethoden gelten kann. So nimmt etwa *Peitz* an, dass ein Nutzer von Blockchains nicht mit der systematischen Auswertung der Blockchain-Daten rechnen muss und dies nicht erkennbar sei und insoweit eine derartige Verarbeitung nicht nach Art. 6 Abs. 1 lit. f) DSGVO zulässig sei.[1864] Zu beachten ist allerdings, dass einerseits eine Verarbeitung nicht unmittelbar dadurch unzulässig wird, dass sie für den Betroffenen nicht erkennbar ist.[1865] Andererseits muss beachtet werden, dass mit den hier gegenständlichen Auswertungsmethoden zwar auch Profilbildung möglich ist, dies aber im Zusammenhang mit Straftaten vorgenommen werden soll und insoweit wohl kein kommerzieller Werbezweck mit der Datenverarbeitung verfolgt wird.[1866]

Dementsprechend stellt sich zunächst die Frage, zu welchem Zweck die hier gegenständlichen Auswertungsmethoden eingesetzt werden sollen.

Der bisher betrachtete Zweck lag in der Strafverfolgung, nachdem der Verdacht einer Straftat bestand.[1867] Zu beachten ist jedoch, dass von Art. 6 Abs. 1 lit. f) DSGVO in Abgrenzung zu Art. 6 Abs. 1 lit. e) DSGVO nicht die Wahrnehmung öffentlicher Interessen, die keinen Bezug zur einzelnen Person haben, erfasst sind.[1868] Öffentliche Interessen (wie etwa die Terro-

1863 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159; vgl. insoweit insbesondere das Bitcoin zugrundeliegende White-Paper *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, S. 6, worin bereits auf die datenschutzrechtliche Relevanz hingewiesen wird; siehe insoweit etwa auch https://bitcoin.org/de/ (letzter Abruf: 20. Dezember 2021), wo etwa die technische Funktionsweise der Bitcoin-Blockchain erklärt wird. Siehe insoweit vergleichbar auch die hier bestimmte Grenze des Grundrechtseingriffs im Rahmen des RiS bei öffentlich verfügbaren Daten oben unter Kap. 4, B.II.2.b)(3).

1864 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159.

1865 So *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159; vgl. insoweit insbesondere Art. 14 Abs. 5 lit. b) DSGVO, nach dem die Informationspflichten gegenüber dem Betroffenen u.a. auch entfallen, wenn hierdurch die Ziele der Verarbeitung unmöglich gemacht werden oder ernsthaft beeinträchtigt werden.

1866 *Peitz,* Datenschutzrechtliche Verantwortlichkeit bei Blockchain-Systemen, S. 159f, stellt abweichend maßgeblich auf die systematische Analyse von Blockchain-Daten zu Werbezwecken ab.

1867 Siehe hierzu insbesondere bereits oben unter Kap. 5, A; siehe zum Erfordernis des Anfangsverdachts bereits oben unter Kap. 5, D.I.

1868 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99.

rismusabwehr oder Volksgesundheit) können den berechtigten Interessen des Verantwortlichen zwar ein „stärkeres Gewicht verleihen oder sich mit den berechtigten Interessen des Verantwortlichen oder Dritten decken“[1869], „[a]usgeschlossen ist jedoch, dass private Stellen eine Verarbeitung mit der Wahrnehmung von Allgemeininteressen […] rechtfertigen“[1870].

Als berechtigtes Interesse ist jedoch die Eigentums- und Beweissicherung zulässig. So kann etwa ein präventiver Zweck zur Sicherung des Eigentums verfolgt werden sowie auch ein repressiver Zweck zur Sicherung von Beweismaterial zur Aufklärung und Verfolgung von Straftaten sowie zur gerichtlichen Geltendmachung.[1871] Insoweit sind auch die „Aufklärung und Verfolgung von Straftaten und die Sicherung von Beweismaterial zur gerichtlichen Durchsetzung zivilrechtlicher Schadensersatzansprüche als berechtigte Interessen grundsätzlich anzuerkennen.“[1872] Explizit nennt Erwägungsgrund Nr. 47 DSGVO etwa „die Verhinderung von Betrug“ als berechtigtes Interesse. Anerkannt ist neben diesem vorrangig präventiven Zweck aber auch, die Verfolgung von Straftaten. So nimmt etwa das OVG Lüneburg an, dass die Videoüberwachung in Fahrzeugen um etwa „‘Vandalismusschäden und/oder Straftaten in den Fahrzeugen unter Beibringung von Beweismitteln zur Anzeige bringen zu können“[1873] ein berechtigtes Interesse darstellt.[1874] So käme bei den hier gegenständlichen Auswertungsmethoden etwa ein berechtigtes Interesse in Betracht, wenn der Betroffene von Ransomware[1875] die Auswertungsmethoden einsetzt, um den Täter zu ermitteln oder Anhaltspunkte zur Täteridentifizierung zu erhalten.

1869 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99; so auch *Art. 29 Datenschutzgruppe*, WP 217, S. 45.

1870 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 99.

1871 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 75ff.

1872 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78 m.w.N. Ähnlich auch Sydow-DSGVO/*Reimer,* Art. 6 Rn. 57, der darauf abstellt, dass nach Erwägungsgrund Nr. 50 Abs. 2 S. 3 DSGVO die Übermittlung personenbezogener Daten zur Aufklärung von Straftaten ein berechtigtes Interesse ist, selbst, wenn die Straftat den Übermittler selbst nicht betrifft.

1873 OVG Lüneburg, BeckRS 2017, 123619 Rn. 29.

1874 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78, der unter Verweis auf die zuvor genannte Entscheidung des OVG Lüneburg feststellt, dass auch die Verfolgung und Aufklärung von Straftaten ein berechtigtes darstellt.

1875 Ransomware bezeichnet eine Schadsoftware, mit der in der Regel der Zugang zu Daten oder technischen Geräten erschwert oder gänzlich verhindert wird, vgl. *Grzywotz/Köhler/Rückert,* StV 2016, 753 (756). In der Regel fordern die „Erpresser“ eine Art Lösegeld, um den Zugang wieder herzustellen. Das Lösegeld wird häufig mit Kryptowährungen bezahlt.

Zur Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 lit. f) DSGVO ist darüber hinaus erforderlich, dass die Datenverarbeitungen zu dem verfolgten Zweck erforderlich sind und die Interessen der Betroffenen nicht das berechtigte Interesse des Verantwortlichen überwiegen.[1876]

Erforderlich ist eine Datenverarbeitung, wenn die berechtigten Interessen nicht auf einem anderen, weniger intensiven Weg genauso effektiv verfolgt werden können.[1877] So nimmt etwa der BGH für den Einsatz von Dash-Cams ans, dass „jedenfalls die permanente anlassloses Aufzeichnung des gesamten Geschehens entlang der Fahrstrecke […] zur Wahrnehmung [der| Interessen […] nicht erforderlich"[1878] sei, da ihr Ziel etwa durch andere privacy-by-design Ansätze erreicht werden könne.[1879] Insoweit muss beim Einsatz der hier gegenständlichen Auswertungsmethoden darauf geachtet werden, welche der konkreten Auswertungsmethoden eine möglichst geringe Eingriffsintensität aufweisen.[1880]

Darüber hinaus muss eine Abwägung der widerstreitenden Interessen stattfinden, bei der die Interessen des Betroffenen nicht überwiegen dürfen. Hierbei müssen nicht nur die konkret eingetretenen Folgen, sondern auch die möglichen Risiken, die mit der Datenverarbeitung einhergehen, berücksichtigt werden.[1881] Zur Bewertung der Eingriffsintensität werden dabei folgende Faktoren herangezogen:

– Art und Umfang der verarbeiteten Daten[1882]: so kann es einerseits insbesondere intensitätserhöhend sein, wenn auf Grund des Umfangs der erhobenen Daten die Möglichkeit besteht, dass diese zusammengeführt und verknüpft werden und sich so umfangreiche Informationen ergeben, aus denen ein Profil des Betroffenen erstellt werden kann. Dies führt in der Regel zum Überwiegen der Interessen des Betroffenen.[1883] Andererseits kann auch die Art der verarbeiteten Daten besonders intensitätser-

1876 BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 69.
1877 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 100.
1878 BGH NJW 2018, 2883 (2885 Rn. 19).
1879 BGH NJW 2018, 2883 (2885 Rn. 25).
1880 Vgl. *Fröwis/Gottschalk/Haslhofer/Rückert/Pesch*, arXiv:1906.12221 [cs.CY] 2019, 1 (7).
1881 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 101.
1882 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 105.
1883 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 106, der allerdings darauf abstellt, dass nur dann in der Regel ein überwiegendes Interesse des Betroffenen vorliegt, wenn ein Profil des Betroffenen zu kommerziellen Zwecken erstellt wird.

höhend sein, etwa wenn der „Aussagegehalt über eine Person besonders hoch ist."[1884]

- Anlass und Umstände der Verarbeitung[1885]: so kann sich etwa die verdeckte[1886], die dauerhafte oder anlasslose Datenerhebung intensitätserhöhend auswirken.[1887]
- Mögliche Folgen der Datenverarbeitung: So werden Datenverarbeitungen, durch die negative Folgen für den Betroffenen drohen als besonders risikoreich eingestuft.[1888]
- Kontext der Datenverarbeitung: so erhöht sich die Intensität etwa, wenn der Betroffene nicht mit der Datenverarbeitung rechnen musste. Insoweit sind auch die Vertraulichkeitserwartungen des Betroffenen zu berücksichtigen.[1889] Andersherum ist es intensitätsverringernd zu berücksichtigen, wenn der Betroffene mit der Verarbeitung rechnen musste.[1890] So muss der Betroffene bei öffentlich verfügbaren Daten in „sehr viel stärkerem Maß"[1891] mit der Verarbeitung dieser Daten rechnen.

Auf der anderen Seite hängt die Interessenabwägung natürlich auch von der Gewichtung der Interessen, die der Verantwortliche mit der Datenverarbeitung verfolgt, ab.[1892] Zwar lassen sich der DSGVO keine unmittelbaren Kriterien für die Abwägung entnehmen[1893], aus der Systematik der DSGVO ergibt sich allerdings, dass etwa die Durchsetzung zivilrechtlicher Ansprüche wohl einen privilegierten Zweck darstellt, da die DSGVO Datenverarbeitungen zu diesem Zweck mehrfach privilegiert.[1894]

Die vorstehend dargestellten Kriterien zur Bewertung der Intensität der Datenverarbeitung sind dabei fast vollständig deckungsgleich mit den zur Bewertung der Grundrechtsintensität herangezogenen Kriterien.[1895] So

1884 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 105.
1885 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111.
1886 Bzw. die heimliche Datenerhebung, Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111.
1887 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 111; vgl. BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 72.
1888 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 107.
1889 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 109.
1890 BeckOK-DSR/*Albers/Veit,* DSGVO Art. 6 Rn. 72; Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 108.
1891 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 110.
1892 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103.
1893 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103.
1894 Simitis-Hornung-Spiecker/*Schantz,* DSGVO Art. 6 Rn. 103, 123.
1895 Siehe hierzu ausführlich oben unter Kap. 5, D.II.1., 2.

wurde auch im grundrechtsrelevanten Bereich die Art und der Umfang der erhobenen Daten für die Bewertung der Intensität berücksichtigt werden.[1896] Darüber hinaus wurden auch im grundrechtsrelevanten Bereich die Umstände der Datenerhebung relevant. So wurde etwa intensitätssteigernd berücksichtigt werden, wenn anlasslos Daten erhoben werden oder wenn hierbei Vertraulichkeitserwartungen verletzt werden.[1897]

Insoweit kann hinsichtlich der Intensität der hier gegenständlichen Auswertungsmethoden auf die bereits erfolgte Einordnung verwiesen werden.[1898]

Zu beachten ist jedoch, dass anders als im Rahmen von § 161 StPO nach Art. 6 Abs. 1 lit. f) DSGVO nicht nur geringfügige Grundrechtseingriffe rechtmäßig sind. Erforderlich ist im Rahmen der Interessenabwägung des Art. 6 Abs. 1 lit. f) DSGVO vielmehr, dass die Intensität der Beeinträchtigung nicht die Interessen der verantwortlichen Stelle überwiegen.[1899] Dementsprechend führt es nicht zwangsläufig zur Unrechtmäßigkeit der Auswertungsmethoden nach Art. 6 Abs. 1 lit. f) DSGVO, wenn bei diesen ein nicht mehr nur geringfügiger Grundrechtseingriff vorliegt.

Ob und in welchen Fallkonstellationen diese Interessenabwägung beim Einsatz der hier gegenständlichen Auswertungsmethoden im Einzelfall zu dem Ergebnis kommen kann, dass eine rechtmäßige Datenverarbeitung vorliegt, muss einer gesonderten, ausführlichen Prüfung vorbehalten bleiben. Dabei dürfte sich etwa die Frage stellen, ob und inwieweit die Schwere der Straftat zu deren Aufklärung die Auswertungsmethoden eingesetzt werden sollen, in die Interessenabwägung einbezogen werden kann und, ob sich ein Unterschied daraus ergibt, dass bereits bei der Erhebung von Blockchain-Daten ein rechtfertigungsbedürftiger Datenverarbeitungsvorgang vorliegt.[1900]

III. Zwischenergebnis

Festzuhalten bleibt, dass im Datenschutzrecht der DSGVO für die hier gegenständlichen Auswertungsmethoden nur der Rechtmäßigkeitstatbestand des Art. 6 Abs. 1 lit. f) DSGVO einschlägig sein kann. Erforderlich ist in die-

1896 Siehe hierzu etwa bereits Kap. 5, D.II.1.e), D.II.2.a).
1897 Siehe hierzu etwa bereits Kap. 5, D.II.1.e), D.II.2.b).
1898 Siehe hierzu ausführlich oben unter Kap. 5, D.II.3.
1899 Paal-Pauly/*Frenzel,* DSGVO Art. 6 Rn. 27.
1900 Siehe hierzu bereits oben unter Kap. 6, A.I.2.

sem Rahmen, dass der Verantwortliche der Datenverarbeitung ein berechtigtes Interesse mit der Datenverarbeitung verfolgt, die Datenverarbeitung hierzu erforderlich ist und die Interessen der Betroffenen nicht überwiegen. Dabei bleibt insbesondere festzuhalten, dass die Kriterien zur Abwägung der Interessen fast deckungsgleich mit den Kriterien sind, die zur Bewertung der Grundrechtsintensität herangezogen wurden. Unterschiedlich ist jedoch, dass im Rahmen von Art. 6 Abs. 1 lit. f) DSGVO jedoch auch eine nicht nur geringfügige Intensität der Beeinträchtigung rechtmäßig sein kann. Ob dies beim Einsatz der hier gegenständlichen Auswertungsmethoden der Fall sein kann, muss allerdings einer weitergehenden Untersuchung vorbehalten bleiben.

C. Zusammenfassung

Aus dem Vorstehenden ergibt sich, dass der Anwendungsbereich der DSGVO für die hier gegenständlichen Auswertungsmethoden eröffnet ist. Denn grundsätzlich ist bei den in der Blockchain enthaltenen Daten ebenfalls von personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO auszugehen und andererseits liegt bereits durch die bloße Teilnahme am Blockchain-Netzwerk und dem Herunterladen der in der Blockchain enthaltenen Daten grundsätzlich eine nach Art. 4 Nr. 2 DSGVO relevante Datenverarbeitung vor. Insoweit besteht hier ein Unterschied zwischen der Grenze eines verfassungsrechtlich rechtfertigungsbedürftigen Eingriffs in das RiS und eines datenschutzrechtlich erlaubnispflichtigen Datenverarbeitungsvorgangs.

Darüber hinaus ist nach Art. 6 Abs. 1 DSGVO für die Rechtmäßigkeit einer Datenverarbeitung erforderlich, dass einer der abschließenden Rechtmäßigkeitstatbestände erfüllt ist. Für die hier gegenständlichen Auswertungsmethoden kommt nur die Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 lit. f) DSGVO in Betracht. Ein hierzu erforderliches berechtigtes Interesse kann auch in der „Aufklärung und Verfolgung von Straftaten Strafverfolgung und [der] Sicherung von Beweismaterial zur gerichtlichen Durchsetzung zivilrechtlicher Schadensersatzansprüche“[1901] liegen. Allerdings muss die Datenverarbeitung hierzu erforderlich sein und

1901 Simitis-Hornung-Spiecker/*Scholz,* DSGVO Anhang 1 Art. 6 Rn. 78 m.w.N. Ähnlich auch Sydow-DSGVO/*Reimer,* Art. 6 Rn. 57, der darauf abstellt, dass nach Erwägungsgrund Nr. 50 Abs. 2 S. 3 DSGVO die Übermittlung personenbezogener Daten

es dürfen keine Interessen der Betroffenen überwiegen. Interessant ist dabei insbesondere, dass die Kriterien, die zur Bewertung der Interessen der Betroffenen herangezogen werden, fast deckungsgleich mit den Kriterien zur Bewertung der Grundrechtsintensität sind. Ein Unterschied besteht allerdings dahingehend, dass Art. 6 Abs. 1 lit. f) DSGVO – anders als § 161 StPO – nicht für die Rechtmäßigkeit der Datenverarbeitung voraussetzt, dass nur eine geringfügige Grundrechtsintensität vorliegt. Die für Art. 6 Abs. 1 lit. f) DSGVO erforderliche Interessenabwägung muss allerdings einer gesonderten Prüfung vorbehalten bleiben.

zur Aufklärung von Straftaten ein berechtigtes Interesse ist, selbst, wenn die Straftat den Übermittler selbst nicht betrifft.