§ 13: Allgemeine Eigentums- und Vermögenskriminalität – Fokus: Cybercrime

I. Begriff

Die Zusammenfassung der „Eigentums- und Vermögensdelikte“ umfasst sehr heterogene Verhaltensweisen, die im Strafgesetzbuch u.a. mit „Diebstahl“, „Unterschlagung“, aber auch „Sachbeschädigung“ sowie „Betrug“ und „Untreue“ umschrieben werden.

Für kriminologische Zwecke wird zwischen alltagstypischer (= allgemeiner) eigentums- und vermögensbezogener Delinquenz und spezieller eigentums- und vermögensbezogener Delinquenz unterschieden. Letztere weist keinen Alltagsbezug auf, sondern ist gekennzeichnet durch die Einbindung in einen geschäftlichen Handlungskontext (zur Unterscheidung *Eisenberg/Kölbel* Kriminologie, § 45 Rn. 73).

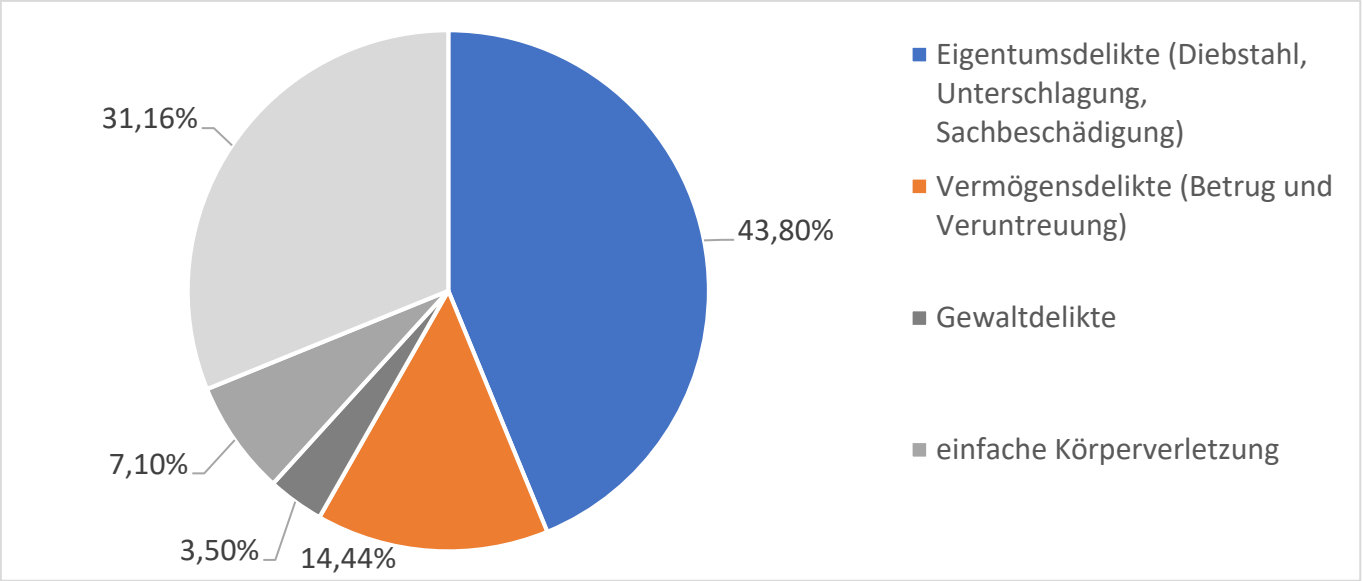
Spezielle Eigentums- und Vermögensdelikte werden in § 6 (Wirtschaftskriminalität) und § 14 (organisierte Kriminalität) der Vorlesung gesondert behandelt.

Bei der folgenden Darstellung der *Befunde* sind Überschneidungen von allgemeinen und speziellen Eigentums- und Vermögensdelikten nicht immer vermeidbar, da die Daten eine klare Abgrenzung nicht ermöglichen. Die PKS differenziert nicht danach, ob es sich um Eigentums- und Vermögensdelikte mit „Alltagsbezug“ (also Massendelinquenz) oder Delikte im Rahmen eines „geschäftlichen Handlungskontexts“ handelt (spezielle Eigentums- und Vermögensdelikte).

II. Überblick

1. Umfang der allgemeinen Eigentums- und Vermögenskriminalität

Die „alltagstypische eigentumsbezogene Delinquenz“ ist ubiquitär. Sie ist durch ein massenhaftes Auftreten und eine Verbreitung in allen gesellschaftlichen Bevölkerungsgruppen gekennzeichnet (*Eisenberg/Kölbel* Kriminologie, § 45 Rn. 73). Sie macht mit einem Anteil von knapp 60 % (PKS 2022) die größte Deliktsgruppe im Rahmen der registrierten Kriminalität aus. Eigentumsdelikte sind mit einem Anteil von ca. 44 % (inklusive Sachbeschädigung) an allen registrierten Delikten dominierend.

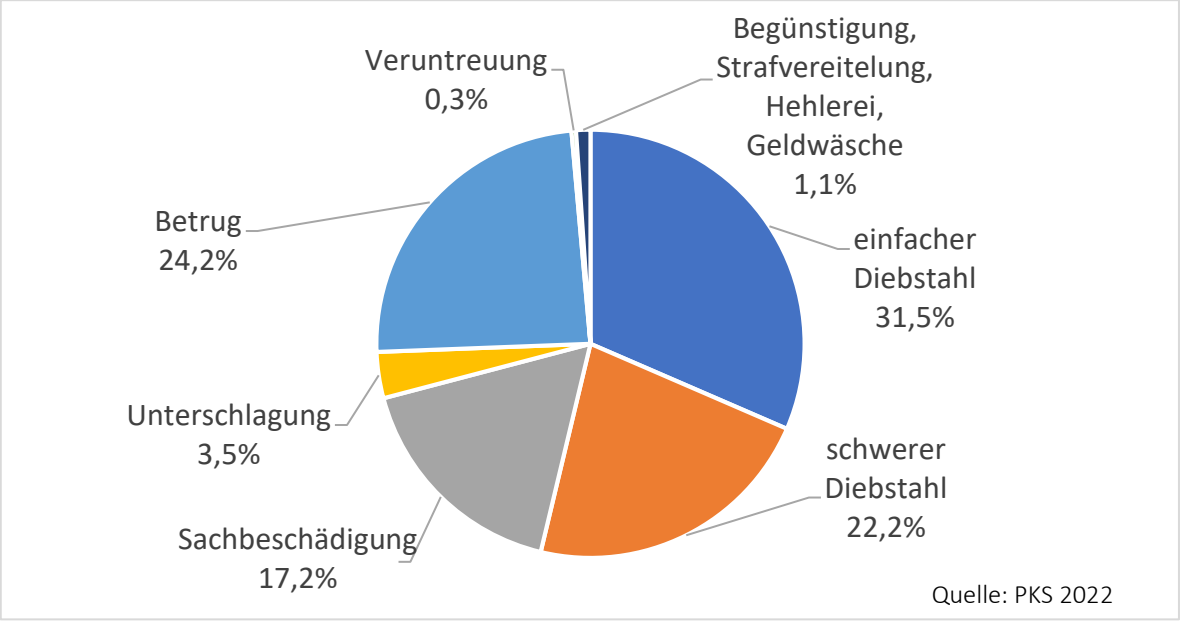


Quelle: PKS 2022

Aber nicht lediglich für das Hellfeld gilt dieser Befund. Auch in Dunkelfeldstudien machen die Eigentums- und Vermögensdelikte ganz regelmäßig den größten Anteil an den erfassten Delikten aus. Selbst unter Seniorinnen und Senioren dominieren neben Fahren unter Alkoholeinfluss Betrugs- und Eigentumsdelikte das Dunkelfeld (vgl. etwa *Kunz* Selbstberichtete Kriminalität älterer Menschen, in: Kunz/Gertz [Hrsg.], Straffälligkeit älterer Menschen, 2015, S. 25 [33]).

2. Struktur von Eigentums- und Vermögenskriminalität

Der einfache Diebstahl ist mit 31,5 % aller registrierten Eigentums- und Vermögensdelikte die größte Deliktsgruppe, gefolgt vom Betrug (24,2 %), schweren Diebstahl (22,2 %) und der Sachbeschädigung (17,2 %).

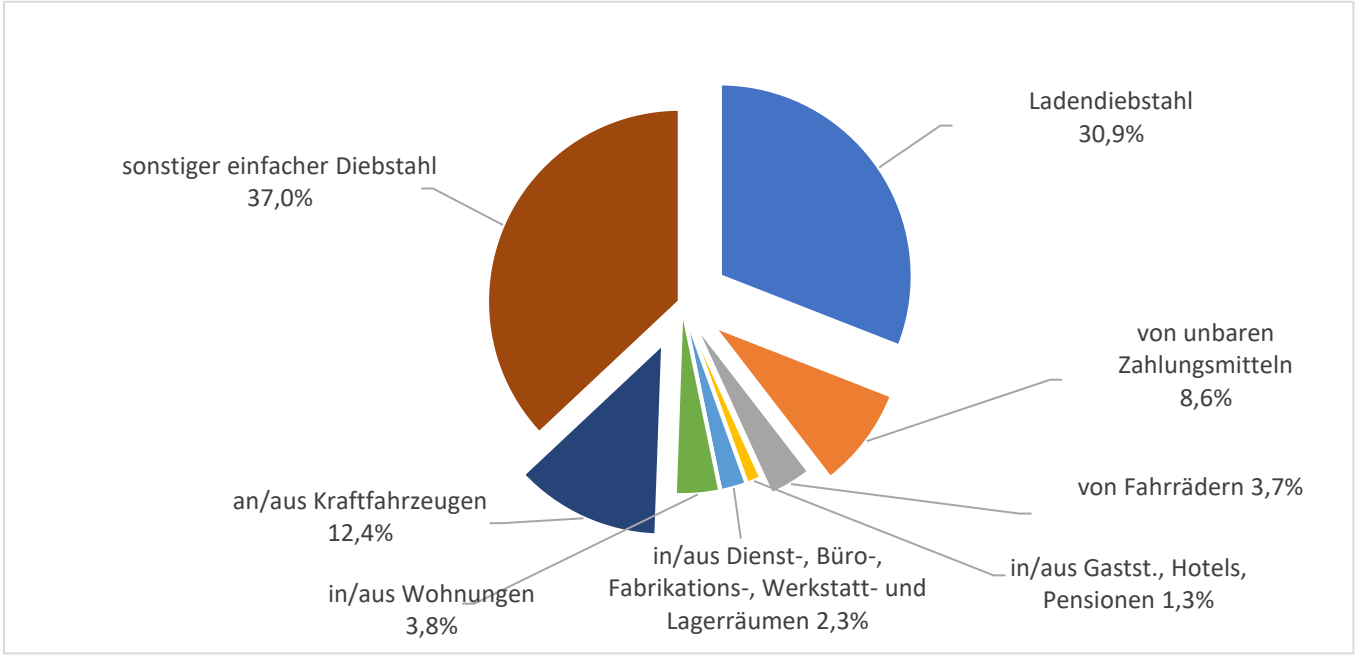


Sowohl zwischen den einzelnen registrierten Deliktsbereichen als auch innerhalb der Gruppen bestehen große strukturelle Unterschiede, die im Folgenden behandelt werden.

III. Der einfache Diebstahl

1. Allgemeines

Der Ladendiebstahl ist mit 30,9 % die größte homogene Gruppe. Im Vergleich zu 2021 ist ein Anstieg der Ladendiebstähle um 34,3 % (+ 87.975 Fälle) zu verzeichnen. Dies lässt sich mit dem Wegfall der durch die Coronapandemie verbundenen Einschränkungen in den Jahren 2020 und 2021 erklären.



Das Niveau des Vor-Corona-Jahres 2019 wurde jedoch nicht ganz erreicht. Die Fälle des Diebstahls im aktuellen Berichtsjahr liegen noch 2,3 % darunter (2019: 1.822.212 Fälle). Lediglich beim Ladendiebstahl (+ 5,8 %; 2019: 325.786 Fälle), Diebstahl an/aus Kraftfahrzeugen (+ 6,1 %; 2019: 222.129 Fälle) sowie beim Taschendiebstahl (+4,7 %; 2019: 94.106 Fälle) wurde das Niveau von 2019 überschritten.

Die Aufklärungsquote liegt durchschnittlich bei 29,8 % (Aufklärungsquote Straftaten insgesamt: 57,3 % [PKS 2022]), divergiert aber erheblich (einfacher Fahrraddiebstahl: 9,3 %; einfacher Ladendiebstahl: 89,3 %, hier wird mit Aufdeckung der Tat die tatverdächtige Person gleich „mitgeliefert“).

Ladendiebstahl ist Individualkriminalität (76,0 % der registrierten Tatverdächtigen handeln allein). Das gilt auch für den einfachen Fahrraddiebstahl (71,8 %) und den einfachen Diebstahl unbarer Zahlungsmittel (74,7 %).

Bei Ladendiebstahl sind 39,1 % der Tatverdächtigen Frauen (Durchschnitt bei Straftaten insgesamt: 25,2 %).

40,0 % der Tatverdächtigen beim Ladendiebstahl sind unter 21 Jahre alt, beim einfachen Fahrraddiebstahl sind es 38,9 %.

2. Zum Dunkelfeld

Die Dunkelziffer ist im Bereich des Ladendiebstahls vermutlich sehr hoch. Mitunter wird davon ausgegangen, dass 90 % bis 95 % der Delikte im Dunkelfeld verbleiben (*Eisenberg/Kölbel* Kriminologie, § 45 Rn. 82 unter Verweis auf *Köllisch* in: FS Kreuzer, 2008, S. 353 ff.).

3. Schadenssumme

Schon im Hellfeld fällt beim einfachen Ladendiebstahl der hohe Anteil entwendeter Gegenstände von geringem Wert ins Auge. 65,3 % aller Tatverdachtsfälle weisen einen Schaden von unter 50 Euro auf. Wird dagegen erst im Rahmen einer Inventur ein entsprechender Verlust festgestellt, dürfte es in den wenigsten Fällen zu einer Anzeige kommen, so dass der Anteil der Diebstahlsdelikte an Gegenständen unter 50 Euro im Dunkelfeld noch deutlich höher liegen dürfte.

Angaben über den Gesamtschaden durch Ladendiebstahl, der laut einer Studie des Handelsforschungsinstituts EHI 2022 rund 3,73 Mrd. Euro betragen haben soll, sind mit Vorsicht zu genießen. Die Zahlen spiegeln den sog. Inventurverlust wieder, der sich aus Ladendiebstahl, Personaldiebstahl und Diebstahl durch Servicekräfte und Liefernde ergibt. Deren jeweiliger Anteil am Gesamtschaden beruht auf Schätzungen von 88 befragten Unternehmen.

Weil auf entwendete Gegenstände keine Mehrwertsteuer gezahlt wurde, errechnet das EHI für 2022 einen gesamtgesellschaftlichen Schaden durch Ladendiebstahl von ca. 510 Mio. Euro, eher eine rein theoretische Größe.

Zum Vergleich: Der Rechercheverbund Correctiv schätzt den gesamten Steuerschaden im Zusammenhang mit Cum-Ex und Cum-Cum weltweit auf 150 Milliarden Euro, wovon 36 Milliarden auf Deutschland entfallen (vgl. Die Zeit v. 21.10.2021 mit kurzem Erklärvideo; zu den Schadenssummen im Bereich der Wirtschaftskriminalität § 6 der KK).

IV. Der Diebstahl unter erschwerenden Umständen

1. Allgemeines

Von einem Diebstahl unter erschwerenden Umständen ist die Rede, wenn die Voraussetzungen des § 243 StGB (Besonders schwerer Fall des Diebstahls) oder § 244 StGB (u.a. Wohnungseinbruchdiebstahl) vorliegen. Größte Gruppen innerhalb des Diebstahls unter erschwerenden Umständen sind der Diebstahl von Fahrrädern (30,3 %) und der Diebstahl an/aus Kraftfahrzeugen (14,4 %). Der hohe Anteil des Diebstahls von Fahrrädern am Diebstahl unter erschwerenden Umständen liegt daran, dass Fahrräder häufig durch eine Schutzvorrichtung (Fahrradschlösser) gegen Wegnahme besonders gesichert sind, vgl. § 243 Abs. 1 S. 2 Nr. 2 StGB.

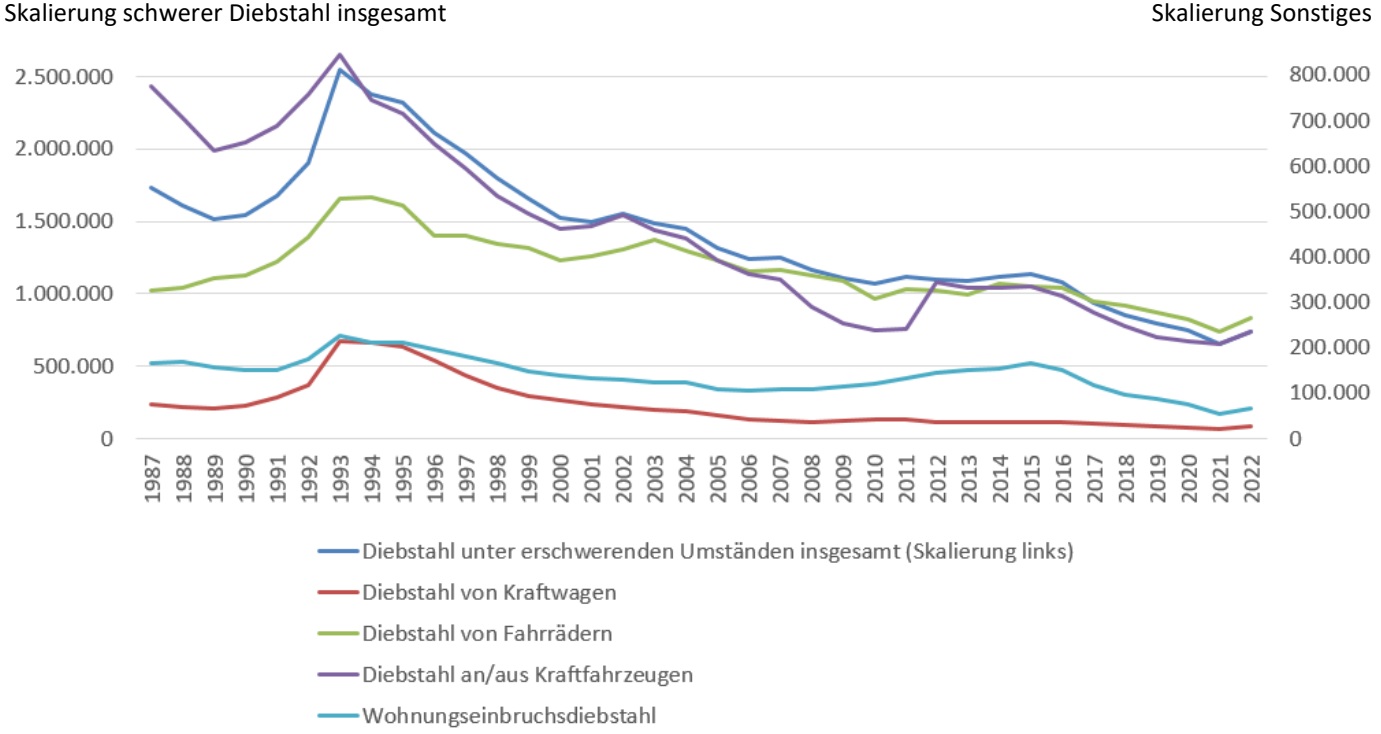
Die Aufklärungsquote ist mit 14,5 % (PKS 2022) deutlich geringer als bei einfachem Diebstahl (siehe bereits oben KK 402).

Der Frauenanteil bei schwerem Diebstahl ist mit 13,2 % unterdurchschnittlich. Der Anteil junger Personen unter 21 Jahren ist mit 28,8 % überdurchschnittlich (21,2 % bei Straftaten insgesamt [PKS 2022]).

Die Dunkelziffer dürfte wegen höherer Schäden (nur 9,6 % unter 50 Euro; 75,1 % über 250 Euro [PKS 2022]) und der höheren Sichtbarkeit geringer sein als beim einfachen Diebstahl.

Die Anzahl der registrierten Delikte des schweren Diebstahls ist stark rückläufig. Dies gilt für fast alle relevanten Untergruppen. Lediglich beim Wohnungseinbruchdiebstahl war zwischen 2008 und 2015 ein Anstieg zu beobachten; die Entwicklung des Fahrraddiebstahls nimmt wiederum einen etwas weniger gradlinigen Verlauf (vgl. Grafik auf der folgenden KK).

Entwicklung ausgewählter registrierter Delikte des schweren Diebstahls



Quelle: PKS Zeitreihen

2. Der „organisierte" Wohnungseinbruchdiebstahl

Im Jahr 2022 machte der Wohnungseinbruchdiebstahl 8,9 % aller Diebstähle unter erschwerten Umständen aus.

Wohnungseinbruch wird in fast der Hälfte der Fälle von mehr als einer Person begangen. Während beim Fahrraddiebstahl unter erschwerenden Umständen 62,0 % der Tatverdächtigen allein handeln, sind es beim Wohnungseinbruchdiebstahl nur 54,6 % (PKS 2022). Die dadurch erforderlichen Absprachen zwischen den Beteiligten lassen aber nicht den Schluss zu, hierbei würde es sich regelmäßig um „organisierte Kriminalität" handeln. *Wollinger/Querbach/Röhrig/König* weisen darauf hin, dass es, anders als in anderen Deliktsbereichen, im Falle des Wohnungseinbruchs gerade keiner größeren Organisation bedarf, um sich zu bereichern. Die Begehung von Wohnungseinbrüchen verlangt weder ein umfangreiches Wissen zur Begehungsweise noch eine professionelle Hehlerstruktur zur Veräußerung des Diebesguts (*Wollinger/Querbach/Röhrig/König* Täterstrukturen und Strafermittlungen im Bereich des organisierten Wohnungseinbruchdiebstahls, 2018, S. 113, hier abrufbar).

a) Ermittlungserfolge

Wohnungseinbrüche beschäftigen die Ermittlungsbehörden und die Strafjustiz in besonderem Maße. Hierbei sind jedenfalls in Baden-Württemberg durchaus Erfolge zu vermelden: Die Aufklärungsquote liegt 2022 bundesweit bei 16,1 % (2014: 15,2 %), in Baden-Württemberg bei 17,5 % (2014: 14 %). Als Erfolgsindikator polizeilich-präventiver Arbeit wird dabei der Anteil der im Versuchsstadium „steckengebliebenen" Wohnungseinbrüche gewertet (2013: 41 %, 2022: 45,4 % [PKS 2022]).

2018 vermeldete das Innenministerium Baden-Württemberg die „Trendwende beim Wohnungseinbruch". Ob dieser Befund retrospektiv noch zu halten ist, ist fraglich.

Auch wegen den mitunter schweren psychischen Folgen für die Opfer eines Wohnungseinbruchsdiebstahls, wozu auch eine starke Beeinträchtigung des Sicherheitsempfindens gehört, wurde in den vergangenen Jahren die Präventions- und Ermittlungstätigkeit in diesem Feld intensiviert. Die Behandlung von Taten erfolgt dabei häufig in speziellen Ermittlungsgruppen; auch bei den Staatsanwaltschaften werden Wohnungseinbrüche gebündelt bearbeitet (*Wollinger/Querbach/Röhrig/König* a.a.O., S. 113 ff.).

b) Predictive Policing

Dabei wird in mittlerweile sieben Bundesländern, u.a. Baden-Württemberg, zudem auf sog. Predictive Policing zurückgegriffen (dazu u.a. *Singelnstein* NStZ 2018, 1 ff. und *Knobloch* Vor die Lage kommen: Predictive Policing in Deutschland, 2018, hier abrufbar). Hierbei handelt es sich um algorithmische Systeme, die zur Berechnung von Wahrscheinlichkeiten für das Auftreten von Verbrechen an bestimmten Orten zu bestimmten Zeiten genutzt werden, um mit entsprechenden polizeilichen Maßnahmen darauf zu reagieren (*Knobloch* a.a.O., S. 8). Im Zusammenhang mit der Prävention von Wohnungseinbrüchen wird ausschließlich ortsbezogenes Predictive Policing verwendet, d.h. es werden ausschließlich räumlich-zeitliche Variablen *ohne Personenbezug* berücksichtigt (anders bei personenbezogenen Systemen, die zu sog. *Heatlists* führen).

Die Systeme sind häufig theoriegeleitet, d.h. Kriminalitätstheorien bilden die Grundlage für die Datenauswahl für das algorithmische System. Populär ist dabei die *Near-Repeat-Hypothese*: In der Nähe von Einbruchstatorten werden in zeitlicher Nähe weitere Einbrüche begangen werden. Aus der Perspektive der

Täter:innen lässt sich so – ganz im Sinne der Rational Choice Theory – bei minimalem Aufwand der maximale Ertrag erzielen (*Knobloch* a.a.O., S. 18). Damit werden aber ein weiteres Mal diejenigen Kriminalitätstheorien herangezogen, die auf vordergründige Rationalität abstellen und insbesondere den Prozessen der Kriminalisierung keine Beachtung schenken. Mehr als eine kurzfristig zu realisierende Gefahrenabwehr kann auf diesem Weg nicht erreicht werden.

Kritik wird außerdem daran geäußert, dass auch die Daten von ausschließlich ortsbezogenen Predictive-Policing-Systemen eine stark erhöhte Kriminalität in solchen Vierteln indizieren würden, die einkommensschwach oder vorrangig von Minderheiten bewohnt sind. Und das, obwohl die Kriminalität in Wirklichkeit in der gesamten Stadt recht gleichmäßig verteilt sei (Studie „To predict and serve?“ im Zusammenhang mit Drogenkriminalität in den USA; hier abrufbar). Eine solche Verzerrung kann auf eine bereits in der Vergangenheit verstärkte Kontrolle dieser Gebiete zurückzuführen sein, sodass dort mehr Kriminalität und eine damit einhergehende statistische Überrepräsentation registriert wurde. Die Verzerrung birgt dann die Gefahr, dass die Software für eine weiterhin verstärkte Kontrolle besagter Viertel sorgt und es durch die dort vorfindbare Kriminalität zu einer selbsterfüllenden Prophezeiung kommt (s. vertiefend das Positionspapier des Bundes Deutscher Kriminalbeamter e.V.).

Eine noch zu verabschiedende EU-Verordnung soll Predictive Policing mit Einschränkungen versehen, sodass diese Methode nur nach Erlaubnis unabhängiger Behörden eingesetzt werden darf.

V. Die Sachbeschädigung

1. Allgemeines

Im Gegensatz zur sonstigen Entwicklung bei Eigentumsdelikten steigt die Zahl der registrierten Sachbeschädigungsdelikte (§§ 303-305a StGB) seit den 90er Jahren bis 2008 in der Tendenz an, wobei es zwischen 2001 und 2005 eine Stagnation gab. Nach einem massiven Anstieg bis 2007 (2005: 175.894 Tatverdächtige, 2007: 187.676 Tatverdächtige) waren die Zahlen zwischen 2009 und 2022 wieder rückläufig (2009: 177.728 Tatverdächtige; 2022: 124.132 Tatverdächtige [PKS Zeitenreihen]).

2. Graffiti(-Kunst)

Der 2006 zu verzeichnende Anstieg ist womöglich damit zu erklären, dass sich seit September 2005 strafbar macht, wer „unbefugt das Erscheinungsbild einer fremden Sache nicht nur unerheblich und nicht nur vorübergehend verändert." (§ 303 Abs. 2 StGB). Graffiti-Kunst wurde damit zur Straftat. Dabei bestanden damals wie heute selbst in der „Mitte der Gesellschaft" unterschiedliche Auffassungen über den richtigen Umgang mit Graffiti. Hierfür stehen Beispiele aus Stuttgart und Freiburg:

Das Stuttgarter Regierungspräsidium stellt Strafanzeigen gegen Unbekannt bei Graffiti, beispielsweise an Lärmschutzwänden entlang der Autobahnen. Entfernt wird jedoch, zum Missfallen der Polizei, wenig. Eine „Zensur" erfolgt nur bei „obszönen, politischen und anstößigen Inhalten" (Stuttgarter Zeitung vom 3.12.2020, S. 17 „Autobahn-Sprayer werden kaum mehr ausgebremst", hier abrufbar).

Konträr hierzu war das Vorgehen in Freiburg. Hier wurde viel dafür getan, solche „Kunstwerke“ schnellstmöglich wieder verschwinden zu lassen (in der Tradition von „Broken Windows“, vgl. dazu die KK 262 ff. aus der Kriminologie-I Vorlesung). Im Rahmen der sog. „Nachstreichgarantie bei Beseitigung von illegalen Graffiti bei privatem Eigentum“ konnte seit 2018 ein Antrag auf Kostenübernahme beim Verein Sicheres Freiburg e.V. gestellt werden. Voraussetzung für die Bewilligung war insbesondere das Stellen einer Strafanzeige. 2021 wurde vom Freiburger Gemeinderat beschlossen, die hierzu notwendige Förderung einzustellen.

3. Aufklärungsquote und Tatverdächtige

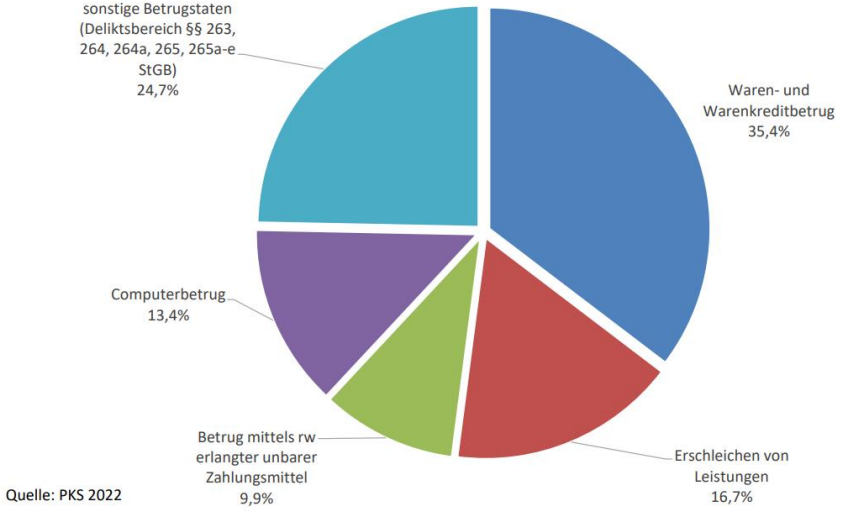
Die Aufklärungsquote bei den Sachbeschädigungsdelikten insgesamt ist mit 25,3 % unterdurchschnittlich im Vergleich zu Straftaten insgesamt. Noch geringer fällt die Aufklärungsquote bei Sachbeschädigung durch Graffiti aus (13,3 %).

68,8 % der Tatverdächtigen sind Alleintäter, nur 15,9 % sind Frauen und 34,7 % unter 21 Jahren (PKS 2022).

VI. Der Betrug

1. Allgemeines

Im Rahmen der Deliktszusammenfassung der Betrugsdelikte (§§ 263, 263a, 264, 264a, 265, 265a-265e StGB) nehmen der Waren- und Warenkreditbetrug mit 35,4 % größten Anteil ein. Bei dieser Betrugsform bietet die Täterin entweder Waren (v.a. im Internet) an, die diese nicht besitzt oder nicht versenden will, oder kauft Waren, die diese nicht bezahlen will. Gefolgt wird diese Betrugsform zahlenmäßig vom Erschleichen von Leistungen mit 16,7 %, worunter insbesondere die Beförderungserschleichung (also das Fahren ohne Fahrschein fällt, vgl. hierzu die KK 82 ff.).



Quelle: PKS 2022

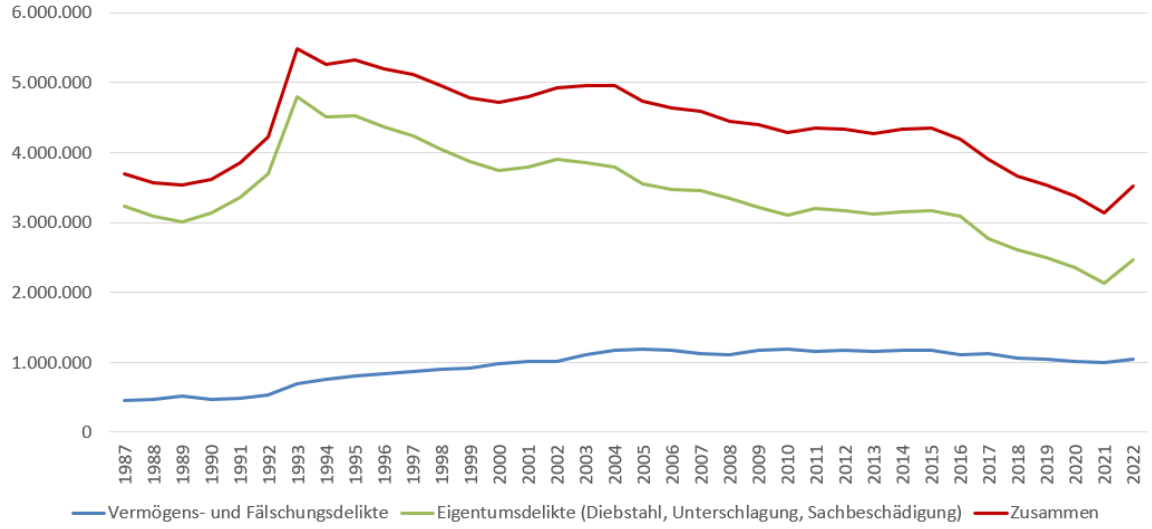
Die Aufklärungsquote ist mit 58,0 % hoch, da Anzeige oft nur erfolgt, wenn einem die tatverdächtige Person bekannt ist. Der Anteil weiblicher Tatverdächtiger ist mit 29,7 % überdurchschnittlich.

Altersstrukturell ergeben sich große Unterschiede zwischen einzelnen Betrugsdelikten. 2022 waren 22,5 % der Tatverdächtigen der Leistungserschleichung unter 21 Jahre alt, aber nur 11,2 % der Tatverdächtigen bei Waren- und Warenkreditbetrug.

VII. Entwicklung der allgemeinen Eigentums- und Vermögenskriminalität

Während Eigentumsdelikte insgesamt mit lediglich geringfügigen Unterbrechungen in den letzten Jahren stark zurückgehen, steigen Vermögensdelikte tendenziell an, wobei in den letzten Jahren eine Stagnation festzustellen ist:

Entwicklung registrierter Eigentums- und Vermögenskriminalität

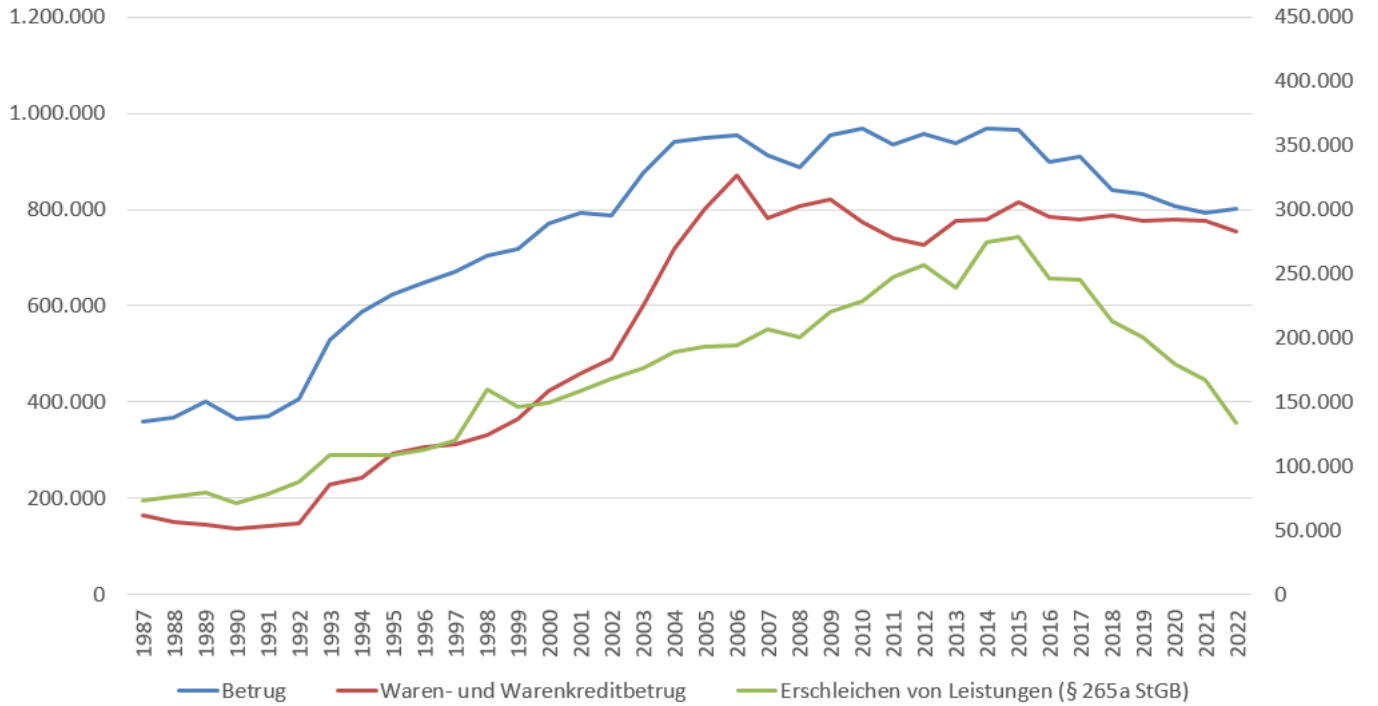


Quelle: PKS Zeitreihen

Ein besonders großer Anstieg wurde bei Waren- und Warenkreditbetrug verzeichnet (von 2000 bis 2006 Zunahme um 105,9 % in diesem Bereich; 2006: 327.052 Fälle). Seit 2006 sind die Betrugsfälle in der Tendenz wieder rückläufig (2022: 801.412 Fälle, Abnahme um 16,0 % seit 2006). Auch der Waren- und Warenkreditbetrug ist mittlerweile auf 283.320 Fälle im Jahr 2022 gesunken (Abnahme um 10,7 % seit 2006).

Entwicklung registrierter Betrugsdelikte

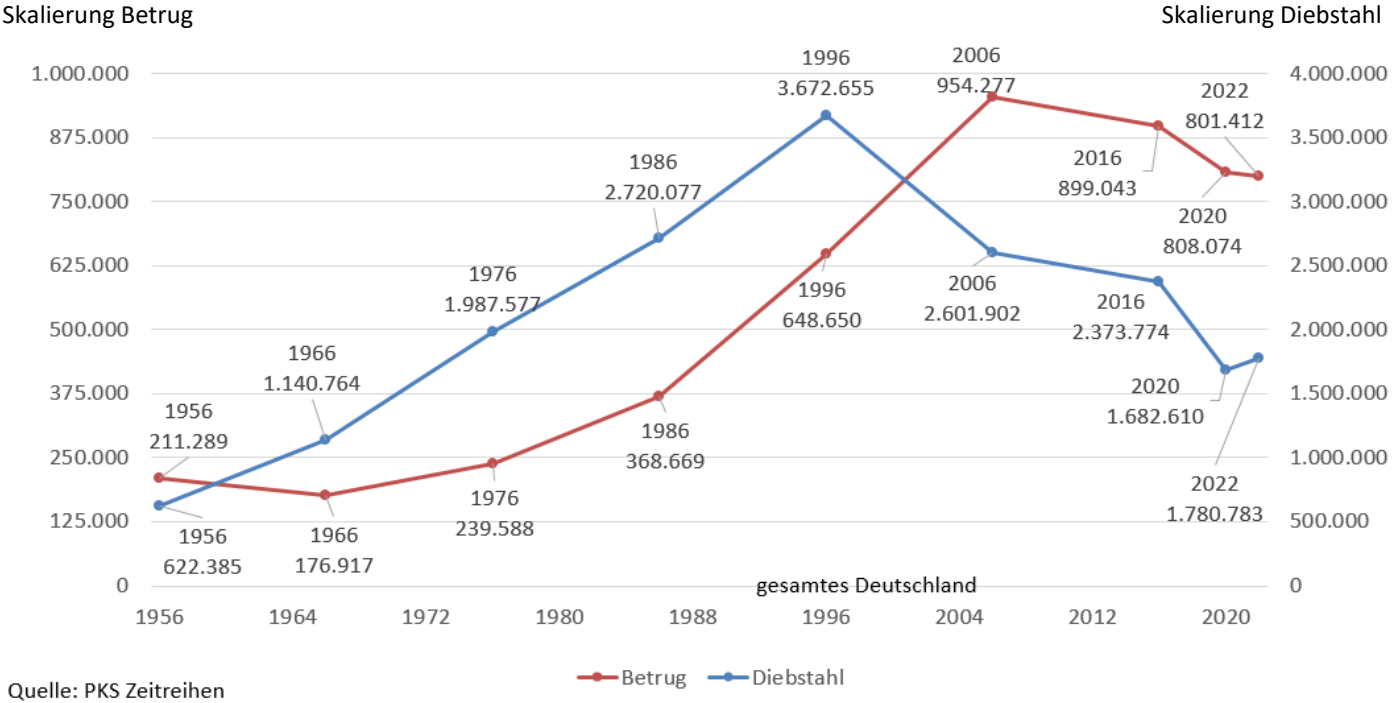
Skalierung Betrug insgesamt



Quelle: PKS Zeitreihen

Bei Betrachtung der gesamten Entwicklung der Nachkriegszeit sind sowohl registrierte Diebstähle als auch Betrug (erst seit den 1970ern) Jahre drastisch angestiegen (Diebstahl bis Mitte der 1990er):

Langzeitentwicklung der Registrierung von Betrug und Diebstahl



Quelle: PKS Zeitreihen

VIII. Tatmittel Internet als Erklärung?

Eine Erklärung für die über viele Jahre gegenläufige Entwicklung von Eigentums- und Vermögensdelikten liegt möglicherweise im Tatmittel Internet.

Die registrierten Straftaten, die mittels des Internets begangen werden, waren 2022 in 61,4 % der Fälle Betrugstaten, mit großem Abstand gefolgt von Delikten gegen die sexuelle Selbstbestimmung (13,5 %) und der Beleidigung (4,4 %). § 242 StGB scheint mit dem vergegenständlichten Tatobjekt „Sache“ im Bereich der virtuellen Welt an Bedeutung zu verlieren. § 303a StGB („Datenveränderung“) ist insofern ein erster Ansatz des Gesetzgebers, der in der Wissenschaft aber auf erhebliche Bedenken stößt (vgl. *Kudlich* Diebstahl und Unterschlagung, in: Hilgendorf/Kudlich/Valerius [Hrsg.], Handbuch des Strafrechts, Band 5, 2020, § 29 Rn. 172: „bedenklich weit gefasst“, „zu unbestimmt“).

Aber auch die klassischen Vermögensstraftatbestände werden nicht lediglich auf neuere Entwicklungen angewendet, sondern stets auch hinsichtlich neuer Tatbegehungsformen mittels des Internets oder Computersystemen angepasst und erweitert. Exemplarisch lässt sich der Computerbetrug gem. § 263a StGB benennen, der 1986 eingeführt wurde, um Betrugsfälle strafrechtlich zu erfassen, bei denen kein Mensch getäuscht wird. Auch das gesetzgeberische Tätigwerden in diesem Bereich mag insoweit zum Anstieg der Fallzahlen beigetragen haben.

1. Erfassung von Straftaten im Internet in der PKS und dem Bundeslagebild Cybercrime

Insbesondere im Bereich der Internetkriminalität ist die kriminalstatistische Aufbereitung des Phänomens auch als ein Versuch der Ermittlungsbehörden zu bewerten, eine breitere Öffentlichkeit auf ausgemachte Gefährdungslagen aufmerksam zu machen (so *Plank* Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? in: Rüdiger/Bayerl [Hrsg.] Cyberkriminologie - Kriminologie für das digitale Zeitalter, 2020, S. 13 [18]).

Die **Polizeiliche Kriminalstatistik** kennt zum einen die Deliktszusammenfassung der **Computerkriminalität** (= Computerkriminalität im engeren Sinne). Hierunter fallen die § 263a, §§ 269, 270 StGB, §§ 303a, 303b StGB, §§ 202a, 202b, 202c StGB sowie die Softwarepiraterie.

Zum anderen werden die **„Straftaten mit dem Tatmittel Internet“** (= Computerkriminalität im weiteren Sinne) in einer Deliktskategorie zusammengeführt. Hierunter werden alle Straftaten erfasst, die auf dem Internet basieren oder mit den Techniken des Internets geschehen. Zur Computerkriminalität im engeren Sinn ergeben sich dabei etwa im Bereich des Computerbetruges Schnittmengen. Erfasst werden aber auch „reguläre“ Straftaten, bei deren Begehung zwar Informationstechnologie genutzt wurde, der Schwerpunkt strafrechtlichen Unrechts jedoch nicht in der Manipulation von Computersystemen liegt. Von Bedeutung sind insoweit insbesondere Betrugsfälle nach § 263 StGB im Bereich des E-Commerce (dazu auch die KK 411), die Verbreitung pornographischer Erzeugnisse sowie Straftaten im Zusammenhang mit Verletzungen des Urheberrechts (§§ 106 ff. UrhG).

Darüber hinaus wird seit 2010 jährlich vom BKA das **Bundeslagebild Cybercrime** veröffentlicht (Ausgabe 2022 hier online abrufbar). Abgebildet werden hier die sog. Cybercrime-Delikte im engeren Sinne (CCieS). Hierzu zählen

- Computerbetrug als Cybercrime im engeren Sinne (§ 263a StGB), hierunter fallen etwa der Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten oder das betrügerische Erlangen von Kfz.
- Missbräuchliche Nutzung von Telekommunikationsdiensten (§ 263a StGB). Das BKA erfasst hierzu Fälle, in denen Sicherheitslücken oder schwache Zugangssicherungen den unberechtigten Zugriff auf Router ermöglicht haben und so gezielt etwa Auslandstelefonieverbindungen angewählt wurden.
- Sonstiger Computerbetrug (§ 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB)
- Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Daten-Hehlerei (§§ 202a, 202b, 202c, 202d StGB), erfasst sind damit die Vorstufen zum betrügerischen Einsatz der Daten.
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB), worunter etwa die Vortäuschung einer Legende zwecks Erlangung einer Vorkasse-Überweisung auf eBay fällt.
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB): „digitale Sachbeschädigung. Hierunter fällt etwa die Verbreitung von Trojaner, Viren, Würmer usw.).

2. Merkmale der Internetkriminalität

- **Verfügbarkeit von Tatwerkzeugen:** Die zur Begehung von Internetstraftaten notwendigen Tatwerkzeuge sind zumeist frei erhältlich. Der Austausch kinderpornographischer Erzeugnisse bzw. das Herunterladen urheberrechtlich geschützter Werke erfordert nur einen Internetanschluss sowie die geeignete Hard- und Software. Aber auch Softwareprodukte, deren vorrangiger Zweck die Begehung von Straftaten ist (z.B. Programme zur Überwindung von Passwort- oder Kopierschutzmaßnahmen), sind verfügbar. Hier lässt sich in den letzten Jahren eine zunehmende Professionalisierung und Spezialisierung der Anbieterinnen und Anbieter auf online-Marktplätzen im Darknet beobachten (sog. cybercrime as a service).

- **Anonymität:** Vielfältige Möglichkeiten der Anonymisierung (Verwendung öffentlicher Internetterminals, Nutzung von Anonymisierungstechniken [etwa das sogenannte „Tor-Netzwerk"]) erschweren die Rückverfolgung von Straftäter:innen im Internet.

- **Automatisierung:** Der Zahl der über das Internet ausgeführten Angriffe steht vermutlich eine relativ kleine Anzahl von Täterinnen und Täter gegenüber, was auf eine zunehmende Automatisierung von Angriffsprozessen schließen lässt. Dies gilt insbesondere für den Versand von Spam-E-Mails und Hackingangriffen gegenüber öffentlichen Einrichtungen oder Unternehmen. Allein die beiden deutschen Mailanbieter WEB.DE und GMX registrierten 2018 im Durchschnitt 150 Millionen Spam-Mails am Tag (vgl. die Statistik auf statista.com hierzu). Allein die Deutsche Telekom registrierte im April 2019 bis zu 46 Millionen Cyber-Angriffe pro Tag (vgl. die entsprechende Meldung der Telekom; s. hier den tagesaktuellen Stand). Solche Zahlen wären durch eine manuelle Ausführung nicht erreichbar und sind nur

durch den Einsatz von Softwaretools zur Automatisierung von Prozessen möglich. Entsprechende Dienstleistungen können ebenfalls auf online-Marktplätzen erworben werden.

- **Transnationalität/Unabhängigkeit von Tat- und Handlungsort:** Der Zugriff auf Inhalte ist infolge der Netzwerkarchitektur weltweit möglich. Die Begehung einer Internetstraftat setzt nicht voraus, dass der Täter oder die Täterin an dem Ort, an dem der Erfolg der Tat eintritt, anwesend ist. Zahlreiche Dienstanbieterinnen und Dienstanbieter (cybercime as a service, s.o.), deren Dienste bei der Begehung von Straftaten genutzt werden, bieten ihre Dienste aus dem Ausland an.

3. Hellfeldbefunde

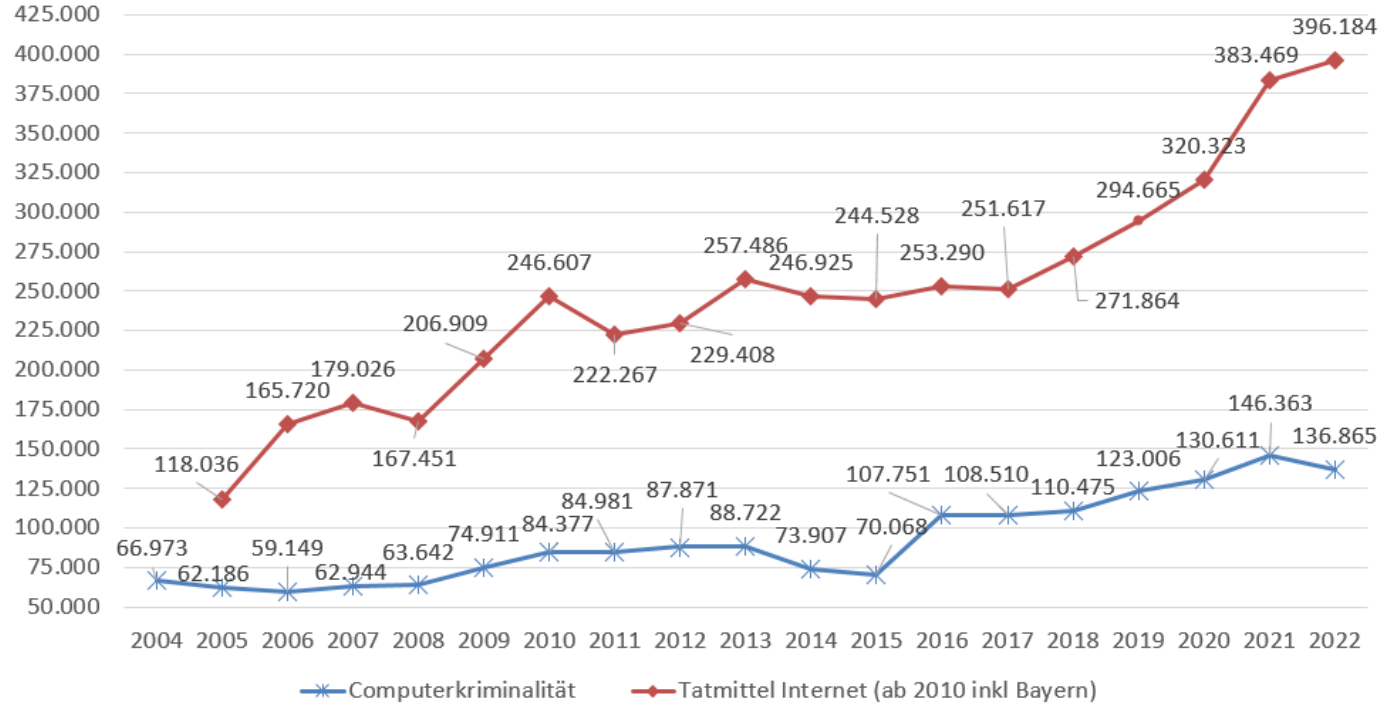
a) PKS

Die Entwicklung der Straftaten im Bereich der Computerkriminalität verlief in den Jahren 2004-2022 mit Schwankungen, wobei tendenziell ein Anstieg zu verzeichnen ist. Nachdem 2021 mit 146.363 Fällen ein neuer Höchstwert für diesen Deliktsbereich registriert wurde, ging die Anzahl 2022 wieder leicht zurück auf 136.865 Fälle, was einer Abnahme von 6,5 % entspricht.

Die Kategorie der Straftaten mit Tatmittel Internet wird in der PKS seit 2005 gesondert dargestellt. Für das Jahr 2022 wurde ein Anstieg der Taten um 3,3 % auf 396.184 Fälle bekanntgegeben. Insgesamt sind bei dieser Deliktskategorie seit ihrer Einführung erhebliche Anstiege zu verzeichnen, allein in den letzten drei Jahren ist ein Anstieg von knapp 35 % zu beobachten. Im Vergleich zum Jahr 2005 sind die Straftaten mit dem Tatmittel Internet um 236 % angestiegen. Etwas relativiert wird die Deliktsentwicklung allerdings dadurch, dass in einzelnen Jahren ganze Bundesländer, die zuvor keine gesonderte Erfassung durchführten,

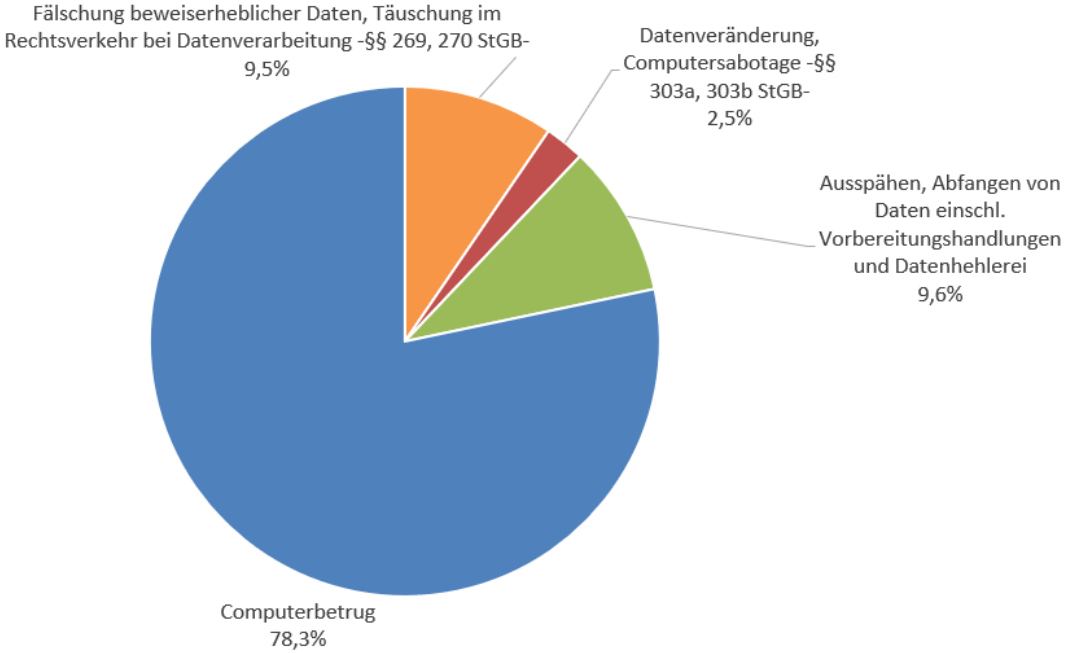
in die Statistik erstmalig miteinbezogen worden sind (2010 etwa durch das Land Bayern). So würde sich der 2010 vermerkte Anstieg um 19 % bei einer Nichtbeachtung Bayerns auf ein Plus von 8 % reduzieren.

Entwicklung Fallzahlen Computerkriminalität und Internet als Tatmittel



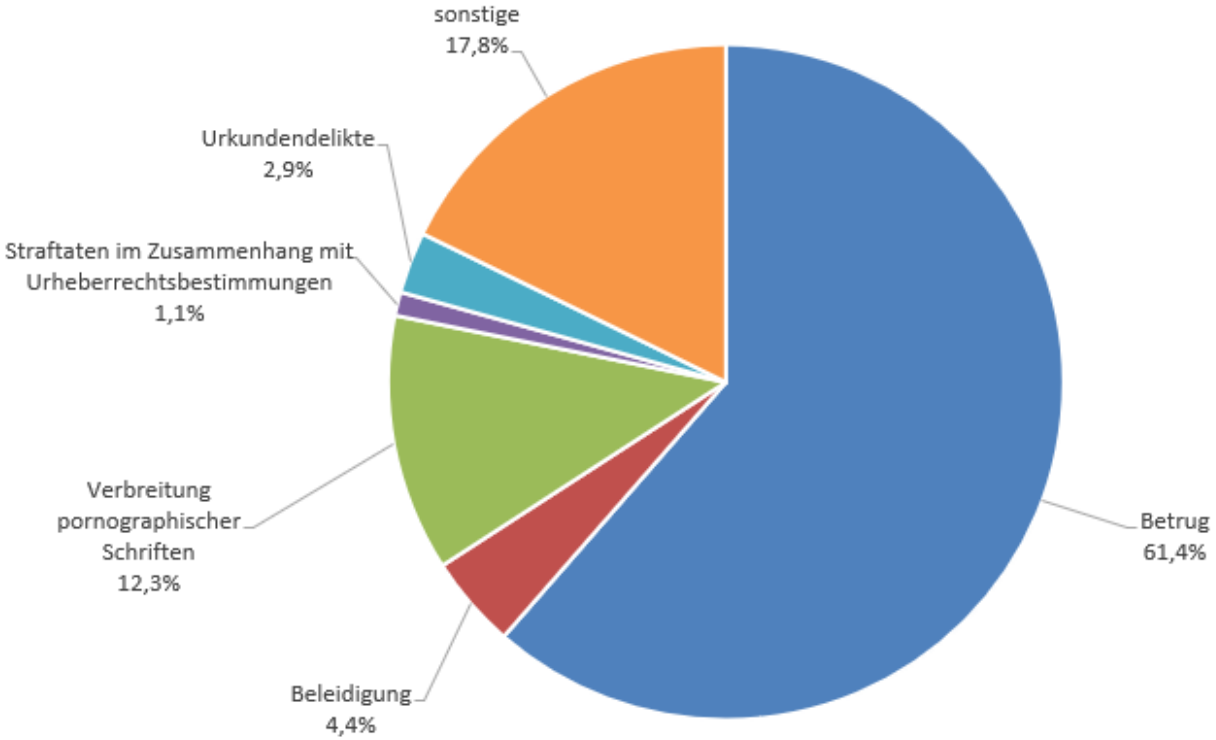
Quelle: PKS 2022

Im Bereich der Computerkriminalität entfallen die größten Anteile registrierter Taten auf den Computerbetrug (78,3 %). Das Ausspähen und Abfangen von Daten einschließlich Vorbereitungshandlungen sowie die Datenhehlerei machen 9,6 % aus.



Quelle: PKS 2022

Bei den Straftaten mit Tatmittel Internet dominieren eindeutig Betrugsdelikte (61,4 %).

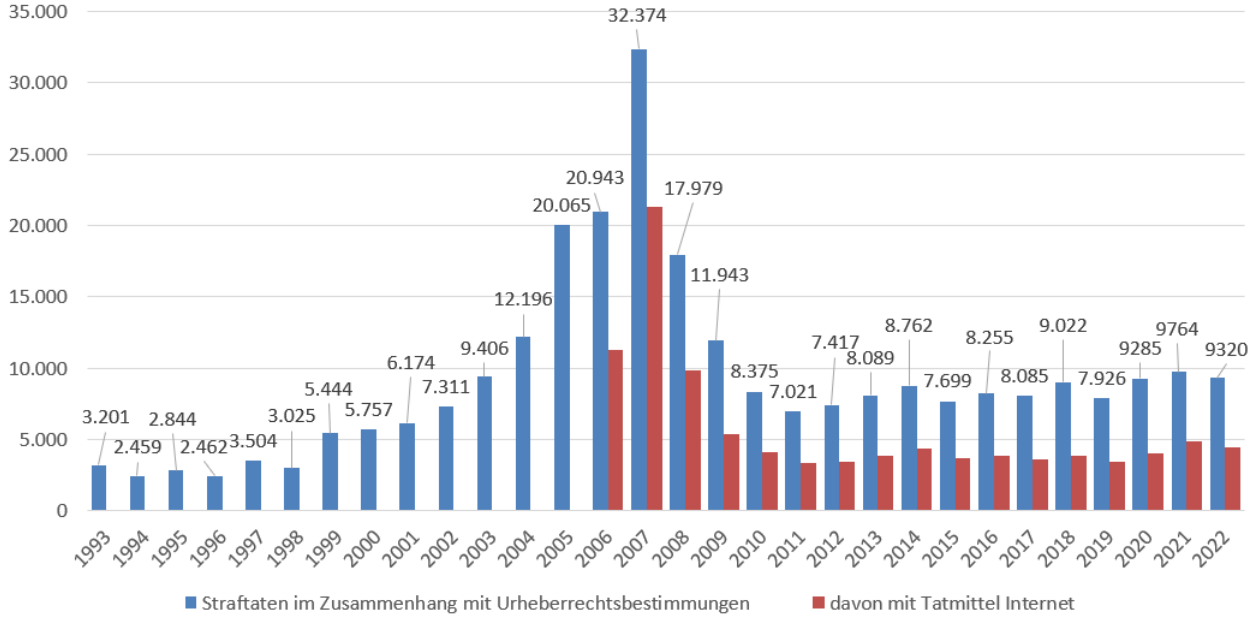


Quelle: PKS 2022

Innerhalb der Betrugsdelikte kommt der größte Anteil dem Waren- und Warenkreditbetrug mit 60,5 % zu.

Obwohl die Straftaten mit dem Tatmittel Internet anstiegen, ist seit einigen Jahren ein erheblicher Rückgang der Straftaten gegen das Urheberrecht (inkl. illegale Downloads) zu verzeichnen. Bis 2007 stieg die Fallzahl bei diesen Delikten noch massiv an, was auf technische Entwicklungen zurückzuführen ist: Zum einen gab es in dieser Zeit immer mehr neu geschützte Tatobjekte (z.B. Softwareprodukte), zum anderen sind die Tatbegehungsmöglichkeiten mit der Verbreitung des Internets enorm gestiegen (*Eisenberg/Kölbel* Kriminologie, § 45 Rn. 76).

Seit 2008 sind bei den Straftaten gegen das Urheberrecht wieder enorme Rückgänge zu verzeichnen. Hier liegt die Vermutung nahe, dass es mit der zunehmenden Verbreitung von legalen Streamingdiensten (für Musik [z.B. Spotify], Filme [z.B. Netflix], Hörbücher [z.B. Audible] etc.) sowie illegalen Streaming-Anbietern (bekannt wurde u.a. die Seite „kinox.to“) unattraktiver geworden ist, Dateien über Filesharing-Plattformen illegal zu downloaden.



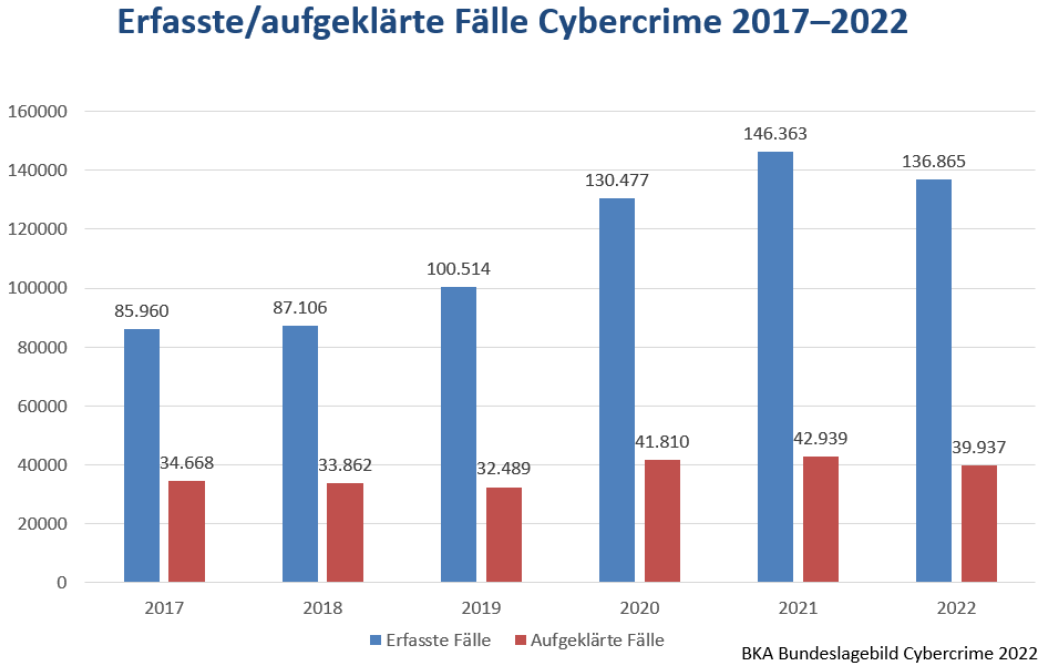
Quelle: PKS Zeitreihen

Quelle: PKS Zeitreihen

Dennoch werden nach wie vor 48,1 % der Straftaten gegen das Urheberrecht über das Internet begangen. Die hohen Aufklärungsquoten (77,4 % bei Urheberrechtsstraftaten insgesamt, 74,7 % bei Tatbegehung über das Internet) sind auf die Musikindustrie zurückzuführen, die speziell nach Verstößen sucht und diese ausnahmslos zur Anzeige bringt.

b) Bundeslagebild Cybercrime

Interessant sind hier unter anderem die Befunde zur Aufklärungsquote bei Cybercrime-Delikten. Während die Zahl der registrierten Fälle Jahr für Jahr ansteigt, stagniert die Anzahl der aufgeklärten Fälle. Dementsprechend sank die Aufklärungsquote von 40,3 % im Jahr 2017 auf 29,2 % im Jahr 2022.



4. Ursachen

Gegenwärtig dominieren auf der **Rational-Choice-Theory** aufbauende Erklärungsansätze für die Entwicklungen im Bereich der Computerkriminalität (vgl. zu den ökonomischen Kriminalitätstheorien die KK 61 ff. der Kriminologie I-Vorlesung, hier abrufbar).

Der Anstieg der mit dem Tatmittel Internet verübten Straftaten lässt sich überwiegend mit dem rasanten Bedeutungsgewinn des E-Commerce erklären, infolgedessen große Teile des Geschäftsverkehrs bargeldlos ablaufen. Im Internet abgeschlossene Geschäfte begünstigen dabei die Entstehung betrugsrelevanter Sachverhalte, wobei auf Aspekte der **Routine-Activity-Theory** Bezug genommen werden kann: Tatbereite Personen finden über Online-Kaufportale wie eBay oder Amazon etc. eine Vielzahl lohnender Tatobjekte sowie unerfahrene, mit den Gefahren online abgewickelter Kaufverträge nicht vertraute und somit nicht hinreichend geschützte Opfer.

Auch die technische Fortentwicklung von Internet und Computersystemen lässt sich im Sinne **erweiterter Möglichkeiten (Tatgelegenheiten) für Rechtsgutsverletzungen** als Erklärung steigender Fallzahlen heranziehen: So ermöglichen etwa verbesserte Datenübertragungsgeschwindigkeiten den massenhaften Austausch urheberrechtlich geschützter Daten über das Internet.

Der Aussicht, mittels des Ausspähens von Zugangsdaten oder internetbasierenden Betrugsdelikten hohe finanzielle Gewinne einstreichen zu können, steht ein vermeintlich geringer Kostenfaktor entgegen. Zum einen erfordert die Tatbegehung angesichts der generellen Verfügbarkeit von Tatwerkzeugen keinen größeren Aufwand, zum anderen verspricht die Anonymität des Internets Sicherheit vor Identifizierung und strafrechtlicher Verfolgung. Auch die sog. moralischen Kosten (Stichwort: **Neutralisierungstechniken**, dazu

die KK 46 ff. der Kriminologie I-Vorlesung, hier abrufbar) fallen vergleichsweise gering aus, da das Tatopfer zumeist gesichtslos bleibt und der verursachte rein finanzielle Schaden eine abstrakte Komponente.

In diesem Zusammenhang wird auch auf die **Broken-Windows-Theorie** Bezug genommen (zu dieser „Theorie" die KK 262 ff. der Kriminologie I-Vorlesung, hier abrufbar), um die Forderung nach einer stärkeren (polizeilichen) Kontrolle im Netz theoretisch zu unterfüttern. So wie in der realen Welt sichtbare Normverstöße, die nicht zeitnah behoben werden, zu weiteren Normverstößen führen sollen, wird derselbe Effekt bei nicht geahndeten Normverstößen im Internet angenommen (*Rüdiger* Das Broken Web: Herausforderungen für die Polizeipräsens im digitalen Raum, in: Rüdiger/Bayerl [Hrsg.], Digitale Polizeiarbeit, 2018, S. 259 [267]). Verschärft werde diese Gefährdungslage im digitalen Raum durch die hier anzutreffende „fixierte Kriminalitätstransparenz": Internetnutzerinnen und -nutzer werden demnach permanent mit scheinbar folgenlosen kriminellen Inhalten und Handlungen konfrontiert, was zu einer Erosion ihrer eigenen Normtreue führen könnte. Während Tatorte in der realen Welt kurz nach der dort begangenen Straftat als solche nicht mehr erkennbar sind, bleiben beispielsweise betrügerische Angebote oder Websites über einen längeren Zeitraum weiterhin einsehbar (*Rüdiger/Bayerl* Cyberkriminologie – Braucht die Kriminologie ein digitales Upgrade, in: Rüdiger/Bayerl [Hrsg.], Cyberkriminologie – Kriminologie für das digitale Zeitalter, 2020, S. 3 [5 f.]).

5. Gesetzgeberische Reaktion und Strafverfolgung

Die Abhängigkeit heutiger Informationsgesellschaften von der Funktionsfähigkeit ihrer Kommunikationsinfrastruktur (insbesondere IT-Systemen) und die Verletzbarkeit dieser technischen Infrastruktur haben zu einer zunehmenden Einflussnahme des Gesetzgebers auf dieses Gefüge geführt.

Ansätze zur Bekämpfung der Computer- und Internetkriminalität liegen dabei unter anderem in der Verhinderung des Zugangs zu Tatwerkzeugen, etwa zu geeigneter Software. So stellen die Tatbestände der § 263a Abs. 3 StGB bzw. § 202c StGB bereits die Entwicklung einer Software zur Begehung eines Computerbetrugs bzw. die Vorbereitung bestimmter Computerdelikte durch die Erstellung von Programmen unter Strafe. Folge ist eine bedenkliche Überkriminalisierung von Vorbereitungshandlungen im Bereich bestimmter Computer- und Internetdelikte, während die Begehung vergleichbarer Vorbereitungshandlungen außerhalb des digitalen Raumes (noch) keine strafrechtliche Sanktionierung erfährt. Generell lassen sich im Strafrecht aber Vorverlagerungstendenzen in vielen Deliktsfeldern ausfindig machen (vgl. etwa *Puschke* in: Hefendehl [Hrsg.], Grenzenlose Vorverlagerung des Strafrechts, 2010, S. 9-40).

Abseits des materiellen Strafrechts führte das Bemühen zur Bekämpfung der Computer- und Internetkriminalität zu einer Erweiterung strafverfahrensrechtlicher Ermittlungsbefugnisse (§ 100a StPO [Telekommunikationsüberwachung], § 100b StPO [Online-Durchsuchung], § 100g StPO [Verkehrsdatenerhebung], § 100f StPO [Akustische Überwachung außerhalb von Wohnraum] StPO).

Dennoch stellen die speziellen Wesensmerkmale der Computer- und Internetkriminalität sowie deren stetiger technischer Wandel den Strafverfolgungsbehörden nach wie vor besondere Herausforderungen (zur Aufklärungsquote bereits die KK 426). Als Grundproblem stellt sich dabei die dezentrale Netzwerkarchitek-

tur des Internets dar, die äußerst resistent gegenüber jeglichen autoritären Eingriffen und Kontrollversuchen von außen ist. Zur Bewältigung weiterer Probleme der Strafverfolgung werden laufend neu entwickelte, passgenaue Konzepte verfolgt:

Der Transnationalität vieler Computer- und Internetdelikte und der damit einhergehenden Beschränkung der Strafverfolgungsmöglichkeiten durch das Souveränitätsprinzip soll durch eine enge Verzahnung und Koordinierung der nationalen Behörden sowie einer Harmonisierung nationaler strafrechtlicher Vorschriften begegnet werden.

Auf die Anonymität des Kriminalitätsbereiches wird vermehrt mit der Blockade des Zugangs zu Anonymisierungsservern reagiert. Des Weiteren werden technische Maßnahmen zur Identifizierung des vom Täter tatsächlich genutzten Internetzugangs weiterentwickelt, etwa die Ermittlung der IP-Adresse des Nutzers durch den Einsatz von Cookies. Ebenfalls in diese Richtung geht die Debatte um eine Klarnamenpflicht in sozialen Netzwerken. Allerdings wurde das Erfordernis der Verwendung von Klarnamen in einer Entscheidung des BGH zu der Klarnamenpflicht in den Geschäftsbedingungen von Facebook als unwirksam erklärt (BGH NJW 2022, 1314). Begründet wird dies dadurch, dass das Erfordernis nicht mit § 13 Abs. 6 Satz 1 TMG a.F. (Telemediengesetz) vereinbar ist, nach welchem Anbieter die Nutzung ihrer Dienste „anonym oder unter Pseudonym zu ermöglichen haben [...]“. Eine interne Pflicht zur Klarnamenangabe bei der Registrierung, die nur für den Anbieter sichtbar ist, ist von der Entscheidung nicht betroffen. Präventive Maßnahmen zur Vorbeugung von Computer- und Internetkriminalität liegen in der Beobachtung einschlägiger Internetforen durch die Sicherheitsbehörden, der Verbesserung technischer Selbstschutzmaßnahmen durch Behörden und Unternehmen sowie der Schaffung spezialisierter Kooperationseinrichtungen zur Analyse des weltweiten Datenverkehrs.

Auch jenseits der konkreten Bekämpfung der Internet- und Computerkriminalität nutzen Behörden die Medien zu Zwecken der Aufklärung und Verfolgung von Straftaten in vielfältiger Weise:

- Zugriff auf neue Informationsquellen: Aus der Überprüfung von Computer- und Telekommunikationsdaten versprechen sich Sicherheitsbehörden Hinweise auf begangene oder geplante Straftaten. Wenngleich die Rechtsgrundlage mancher Eingriffsmaßnahmen (etwa beim Zugriff auf E-Mails) nach wie vor umstritten ist, stellt die Überprüfung von Telekommunikationsdaten eine zentrale Vorgehensweise der Behörden bei der Aufklärung von Straftaten dar. Für das Jahr 2022 wurden im Jahresbericht der Bundesnetzagentur 23 Millionen automatisierte Auskunftsersuchen der Sicherheitsbehörden (auf Grundlage des § 173 TKG) verzeichnet. 104 Telekommunikationsunternehmen sind verpflichtet, am Verfahren teilzunehmen. Die Sicherheitsbehörden können also innerhalb kürzester Zeit eine Anfrage bei der Bundesnetzagentur stellen, die Bundesnetzagentur kann automatisch die Daten aus den Kundendateien der Telekommunikationsanbieter abrufen.
- Auf sog. „Internet-Streifen“ überprüfen Ermittlungsbehörden anlassunabhängig Online-Inhalte auf strafrechtlich relevante Hinweise, etwa auch in Gestalt der verdeckten Teilnahme an Kommunikationseinrichtungen (Foren, Soziale Netzwerke etc.). Problematisch erscheinen solche Vorgehensweisen insofern, als die Objekte der staatlichen Ermittlungsbegehrlichkeiten stets besonders grundrechtssensibel sind. So können das heimliche Abrufen, Zusammentragen und Verknüpfen einer Vielzahl von Daten aus unterschiedlichen Lebensbereichen erhebliche Eingriffe in die Grundrechte des Fernmeldegeheimnisses und der informationellen Selbstbestimmung darstellen.

- Neue Ermittlungsmaßnahmen und Zugriffsmöglichkeiten: Der Ausweitung staatlicher Zugriffsmöglichkeiten dienen Instrumente wie die Online-Durchsuchung (seit 2017 geregelt in § 100b StPO [strafprozessual] und § 49 BKAG [zur Gefahrenabwehr]), die Quellen-Telekommunikationsüberwachung (geregelt in § 100a Abs. 1 S. 2 StPO [strafprozessual] und § 51 Abs. 2 BKAG [zur Gefahrenabwehr]) und die Vorratsdatenspeicherung (Neuregelung in § 176 TKG [bis 2021 § 113b TKG]). Gegen die strafprozessuale Online-Durchsuchung und die Quellen-TKÜ wurde im August 2018 Verfassungsbeschwerde erhoben, die das BVerfG jedoch im April 2023 als unzulässig zurückwies. Gegen die Vorratsdatenspeicherung wurde bereits 2015 Verfassungsbeschwerde erhoben, zudem legte das Bundesverwaltungsgericht im September 2019 die Frage der Vereinbarkeit der deutschen Vorratsdatenspeicherung mit der europäischen „Datenschutzrichtlinie für elektronische Kommunikation“ dem EuGH vor. Der EuGH urteilte im September 2022, dass eine anlasslose Speicherung von Kommunikationsdaten mit genannter Richtlinie nicht vereinbar sei. Dem folgend erklärte das BVerwG im August 2023 die Regelung des § 176 TKG für unanwendbar (BVerwG, Urteil vom 14.08.2023 - 6 C 6.22)
- Befugnis für staatliche Behörden, bestimmte Straftaten zu begehen, um damit Ermittlungsansätze zu erhalten. Seit 2020 ist den Ermittlungsbehörden die Herstellung und Verbreitung fiktiver Kinderpornographie gestattet, um damit Zugang zu entsprechenden Online-Foren zu erhalten (Tatbestandsausschlussfall in § 184b Abs. 6 StGB: Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte). Kritisch hierzu der Beitrag von Thomas Fischer auf Spiegel Online vom 2.1.2020).

- Verfolgungsaufrufe: Zur Herstellung einer umfangreichen Kontrolldichte wird durch den Einsatz von Fernsehen (Aktenzeichen XY) und Internet als Fahndungsmittel eine möglichst breite Öffentlichkeit in die konkrete Strafverfolgung einbezogen.
- Staatliche Reaktion auf private Ermittlungen: Im 2010 ausgestrahlten TV-Format „Tatort Internet“ (RTL II) wurden reale Straftaten von Privatpersonen provoziert und zum Zwecke der gezielten Diffamierung der Täter:innen ausgestrahlt. Knüpfen staatliche Strafverfahren daran an, besteht neben den ohnehin zu befürchtenden Stigmatisierungswirkungen die Gefahr, dass elementare Verfahrensgrundsätze – etwa die Beschuldigtenrechte im Ermittlungsverfahren – umgangen werden.

IX. Alternative Deutungsrahmen?

Insbesondere die sog. Underground Economy wird in offiziellen Berichten wie dem Bundeslagebild im Cybercrime (dort S. 8 ff.) oder auch in den Medien (vgl. nur die Netflix-Serie „How to sell drugs online (fast)“) wiederholt als eine wesentliche Ausprägung des Kriminalitätsfeldes Cybercrime aufgeführt.

Die hier auf Betrugsdelikte ausgelegten Dienstleistungen („cybercrime as a service“) reichen vom Anbieten digitaler Identitäten, dem Verkauf von gefälschten Inseraten etwa auf eBay oder Amazon, dem Aufsetzen von ganzen Fake-Shops bis hin zu gefälschten Paketversendungsnummern. Insbesondere bei beabsichtigten Betrugstaten gegenüber klassischen Verbraucher:innen spielen Kontodaten eine wichtige Rolle. Die Angabe eines Sparkassen- oder Volksbankkontos als Verkäuferkonto lässt ein Online-Angebot wesentlich seriöser erscheinen als etwa die Bezahlmethode PayPal.

Daneben existieren im Darknet auch diverse Angebote an Drogen, Waffen und – insb. als Reaktion auf die Coronapandemie – Impfstoffen (vgl. die Beispiele im Bundeslagebild Cybercrime S. 9 f.).

In diesem Zusammenhang macht die Studie von *Aldrige* und *Décary-Hétu* auf Aspekte aufmerksam, die in den phänomenologischen Schilderungen des BKA keine Beachtung finden (*Aldrige/Décary-Hétu* Not an „eBay for Drugs“: The Cryptomarket „Silk Road“ as a Paradigm Shifting Criminal Innovation, 2014, hier abrufbar).

Von der Kriminologin und dem Kriminologen wurden die auf der Darknet-Plattform Silk-Road eingestellten Drogen-Angebote nach Quantität und Preis ausgewertet. Die beiden Forschenden gelangten auf diese Weise zu der Annahme, die Plattform werde insbesondere von Drogendealenden („Handeltreibende“ im Sinne des deutschen BtMG) und nicht von Konsumentinnen und Konsumenten genutzt.

Die Drogenbeschaffung über Online-Marktplätze könnte, so der Ausblick der Studie, zu einer Reduzierung der sonst im Zusammenhang mit Drogengeschäften zu beobachtenden Kollateralschäden in Form von psychischer Gewalt, Erpressungen, Einschüchterungen usw. führen (a.a.O. S. 16).

Die Überlegungen wurden in der Studie von *Barrat/Ferris/Winstock* aufgegriffen (*Barrat/Ferris/Winstock* Safer scoring? Cryptomarkets, social supply and drug market violence, International Journal of Drug Policy 35 (2016), 24 ff., die Zusammenfassung ist hier abrufbar). Eine Befragung unter Cryptomarket-Nutzerinnen und -Nutzern (n = 3.794), die auf diese Weise in den letzten 12 Monaten vor der Befragung Drogen bezogen haben, ergaben tatsächlich ein geringeres Vorkommen von Bedrohungen für die eigene Sicherheit (3 % der Befragten) oder Erleben physischer Gewalt (1 % der Befragten) im Vergleich zum Drogenbezug über Freunde/Bekannte (14 % / 6 %), bekannte Dealer (24 % / 10 %) oder Fremde (35 % / 15 %).

Literaturhinweis:

Eisenberg/Kölbel Kriminologie, § 45 Rn. 73–107.

P.-A. Albrecht Kriminologie, §§ 31, 32 zur Entkriminalisierungsdebatte.

BKA (Hrsg.) Bundeslagebild Cybercrime 2022, 2023.

Zum Darknet etwa *Bachmann*/*Arslan* „Darknet“ Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber, NZWiSt 2019, 241.