Verdeckter Datenzugriff: Polizei soll schon bei Bagatellen E-Mails und Cloud-Daten einsehen dürfen

blank

Juni 2021

Eigenständigkeitserklärung

Hiermit erkläre ich, Markus Dietz, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Sämtliche Ausführungen, die anderen Schriften wörtlich oder sinngemäß entnommen wurden, habe ich als solche kenntlich gemacht.

Hiermit stimme ich zu, dass die vorliegende Arbeit in elektronischer Form mit entsprechender Software überprüft wird.

.....	.....
Markus Dietz	Ort und Datum

Abkürzungsverzeichnis

Da sich diese Ausarbeitung intensiv mit Gesetzestexten auseinandersetzt, gibt es im Voraus ein Symbol- und Abkürzungsverzeichnis:

Abkürzung	Bedeutung
§	Paragraf
§§	Paragrafen
StPO	Strafprozessordnung
StPO-E	Entwurf der Strafprozessordnung
Abs.	Absatz
ff.	die folgenden (Paragrafen)
TKÜ	Telekommunikationsüberwachung
GG	Grundgesetz

Abstract

Das Ziel der vorliegenden Ausarbeitung war die kritische Auseinandersetzung mit der Einführung des neuen Passus § 95a der Strafprozessordnung (von nun an StPO). Dazu wurden die Probleme der Strafverfolgungsbehörden im digitalen Zeitalter dargestellt und die Maßnahmen dieser bewertet. Auf dieser Grundlage basierend stellte sich heraus, dass § 95a als anfällig für eine Ausnutzung seitens der Strafverfolgungsbehörden ist. Deshalb ist dieser definitiv kritisch anzusehen und sollte von Begutachtern der Gesetzgebung detailliert bewertet und nach Möglichkeit verändert werden.

Inhaltsverzeichnis

1 Einleitung

Das Einschreiten in das digitale Zeitalter hat viele technologische Neuerungen mit sich gebracht. Das Internet ist eine davon. Mit dem Erfolg des Internets kamen, neben den positiven Entwicklungen, auch viele neue Probleme hinzu. Ein großes Problem ist die Verbreitung von digitalen, kriminellen Aktivitäten - die sogenannte *Cyberkriminalität*. Diese floriert durch die mögliche Anonymität und die direkte sowie kostenlose Kommunikation, die das Internet bieten kann.
Strafverfolgungsbehörden auf der ganzen Welt stehen nun vor der Aufgabe, Cyberkriminalität souverän aufzuklären. Diese Herausforderung wurde durch die vermehrte Einführung von Verschlüsselung und den größeren Sicherheitskonsens im Internet, vor allem in den letzten Jahren, außerordentlich erschwert. Beispiele hierfür sind die Standardisierung von Ende-zu-Ende Verschlüsselung bei Messenger-Diensten, wie WhatsApp, oder die seit 2018 gesetzliche vorgeschriebene SSL-Verschlüsselung von Websites. [7] Das macht es Strafverfolgern nahezu unmöglich, die Kommunikation während der Übertragung abzuhören. Der ehemalige FBI Direktor James Comey bezeichnet diesen Herausforderung als „The Challenge of Going Dark“ und gibt seine Bedenken in einer Rede zur Kenntnis:

> „Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.“ - James B. Comey [8]

Um nicht im „Dunkeln“ zu bleiben, hat auch die deutsche Gesetzgebung reagiert und den Strafverfolgungsbehörden effektive Mittel gegeben, welche in der Undurchsichtigkeit des Internets Erfolg versprechen. Diese Ausarbeitung beschäftigt sich hauptsächlich mit der StPO und dem, im März veröffentlichten und im Juni 2021, verabschiedeten Entwurf der StPO sowie dem darin enthaltenen Paragrafen 95a: Zurückstellung der Benachrichtigung des Beschuldigten. Trotz dieses harmlosen Titels muss dieser Entwurf kritisch betrachtet und bewertet werden, da er den Behörden es erlaubt, verdeckt, also ohne Benachrichtigung des Betroffenen, auf dessen Daten zuzugreifen. Dazu gehören auch E-Mails und Cloud Daten. Dies wird von Experten als ein Paradigmenwechsel angesehen. [11]

Zunächst wird der aktuelle Zustand der StPO dargestellt und die Maßnahmen erläutert, die den Strafverfolgungsbehörden bei der digitalen Strafverfolgung zur Verfügung stehen. Auf dieser Grundlage wird der Gesetzesentwurf des neuen § 95a StPO-E kritisch beleuchtet und es werden Probleme aufgezeigt, die bisher von der Gesetzgebung ungeachtet blieben. Abschließend wird in einem Fazit die Bewertung des § 95a zusammengefasst.

2 Digitale Strafverfolgung in Deutschland

Bevor wir uns mit dem neuen Passus der StPO auseinandersetzen können, muss erst geklärt werden, was der aktuelle Stand dieser ist und wie die digitale Strafverfolgung aussieht.

Die Strafverfolgung in Deutschland wird von den Strafverfolgungsbehörden durchgeführt. Dazu gehören:

- die Staatsanwaltschaft
- die Polizei (die Landespolizei, die Bundespolizei und das Bundeskriminalamt)
- die Zollabteilung und die Finanzverwaltung im Bereich Steuerrecht und sein Steuerermittlungsbüro

Diese Behörden wenden das Strafprozessrecht an, bei dem es sich insbesondere um die deutsche Strafprozessordnung (StPO) handelt. Nach § 152 Abs. 2 der StPO sind sie an das Legalitätsprinzip gebunden, das vorsieht, dass jede mutmaßliche Straftat grundsätzlich von Amts wegen untersucht werden *muss*. [15]
Die StPO ist demnach ein besonders wichtiger Teil der Gesetzgebung und benötigt intensive Überprüfung, da viele der dort beschriebenen Maßnahmen in die Grundrechte der Verdachtspersonen eingreifen. Insbesondere im Zusammenhang mit digitaler Überwachung wird das Post- und Fernmeldegeheimnis verletzt, welches in Art. 10 GG festgeschrieben ist.

Die StPO ist ein alter Gesetzestext, welcher...

> „mitunter Normen enthält, die sich seit ihrer ursprünglichen Fassung von 1877 kaum verändert haben und daher mangels Berücksichtigung technischer Neuerungen den aktuellen Erfordernissen kaum gewachsen sind.“
> - Hilgendorf/Valerius [14]

Damit sich die Strafverfolgungsbehörden den neuen kriminellen Möglichkeiten, welche sich auf informationstechnischen Geräten oder im Internet zutragen, stellen können, sind in den letzten Jahren einige Paragrafen ergänzt und neu interpretiert worden. Insbesondere diejenigen, die dazu dienen digitale Beweismittel zu sichern und so Straftaten aufzudecken. Die Gesetzgebung steht immer wieder vor dem Problem, durch Ermächtigungsgrundlagen den Strafverfolgern einerseits wirkungsreiche Maßnahmen zu geben,

andererseits aber den Bürger vor Eingriffen in seine Grundrechte zu schützen. [12] Dies ist ein Grund, warum die Terminologien und Einsatzanforderungen der Methoden in Deutschland besonders zielorientiert formuliert sind, wie z.B. Online-Durchsuchungen, wobei die Gesetzgebungen in anderen Ländern eher Oberbegriffe verwenden, wie z.B. in den Niederlanden: *onderzoek in een geautomatiseerd werk* - Untersuchung in einem Computer). [13]

Als Maßnahmen der Strafverfolgung gibt es zum einen die Möglichkeit zur Sicherstellung und Beschlagnahme (§§ 94 ff.), welche es den Behörden in diesem Kontext erlaubt, Datenträger und Daten zu beschlagnahmen. Zum anderem dürfen die Behörden Telekommunikationsüberwachung (TKÜ) (§ 100 StPO) einsetzen. Dazu gehören die Quellen-TKÜ und die Online-Durchsuchung, beide benötigen einen unbemerkten Zugriff auf das Endgerät (z.B. PC, Laptop, Smartphone) des Betroffenen. [1]
Die dazugehörigen Paragrafen der StPO werden im Folgenden behandelt.

2.1 Sicherstellung und Beschlagnahme nach §§ 94 ff. StPO

Der § 94 dient grundsätzlich der Sicherstellung von Gegenständen als Beweismittel. Wenn ein Gegenstand als Beweismittel von Bedeutung für einen Strafprozess sein kann, muss dieser nach Abs. 1 in Verwahrung genommen werden. Wenn der Besitzer dieses Gegenstandes diesen nicht freiwillig herausgeben will, so muss nach Abs. 2 eine Beschlagnahme angeordnet werden. Für eine Beschlagnahme ist es lediglich ausreichend, wenn der betroffene Gegenstand potenziell wichtig für die Ermittlung sein kann. [1] Daher besteht ein dringender Bedarf an einem vorhergegangenem Verdacht, wie z.B wenn die Verdachtsperson sich an einem Tatort aufgehalten hat.
Ein weiterer Punkt ist die Benachrichtigung des Betroffenen. Nach Art. 103 Abs. 1 GG haben Bürger ein verfassungsrechtlich garantiertes Recht auf rechtliches Gehör, weshalb der Betroffene einer Beschlagnahme nach der Durchführung zu benachrichtigen ist. Diese Benachrichtung ist auch in den §§ 33 Abs. 1 und 35 Abs. 2 der StPO festgelegt, damit der Beschuldigte sich vor der Entscheidung eines Gerichts verteidigen kann. [2] Gerade dieses grundlegende Recht auf Benachrichtigung kann mit dem neuen Entwurf der StPO zurückgestellt werden (siehe Kapitel 3).
Letztendlich ist es wichtig, den Ausmaß der Beschlagnahme mit der Schwere der Straftat in ein vernünftiges Verhältnis zu setzen. Somit wird verhindert, dass Grundrechte von Personen mit Verdacht auf eine leichte Straftat bewahrt werden und die Beschlagnahme trotzdem effektiv bei schweren Straftaten genutzt werden kann. [12]

Eine Möglichkeit digitale Beweise zu sammeln, ist die Beschlagnahme von Datenträgern. Diese ist nach § 94 gut zu realisieren, da ein Datenträger ein *Gegenstand* ist, was dem Wortlaut des Paragrafen entspricht. Der Datenträger kann für die Ermittlung eventuell wichtige Daten enthalten, weshalb das schon z.B. die Beschlagnahme des Smartphones

oder PCs gerechtfertigt. Hier ist es wichtig anzugeben, welche Daten des Datenträgers zu verwerten sind, um die Privatsphäre des Betroffenen nicht auszureizen. So kann auch angeordnet werden, dass nur tatrelevante Dateien zur Auswertung kopiert werden und nicht der gesamte Datenträger beschlagnahmt werden soll. [12]
Bei der direkten Anordnung zur Beschlagnahme von *Daten* ergibt sich das Problem der Körperlichkeit, da § 94 StPO den Wortlaut „Gegenstand“ benutzt und Daten genau genommen keine Gegenstände sind. Laut Ruppert...

> „verlangen weder der allgemeine Sprachgebrauch, noch das juristische Gesamtverständnis des Begriffs zwingend nach dem Kriterium der Körperlichkeit. Insbesondere angesichts des Telos der Norm, Beweismittel zu sichern, scheint daher ein fortschrittliches Verständnis der Formulierung dergestalt, dass auch Daten per se erfasst sind, geboten.“ - Ruppert [12]

Demnach ist die Beschlagnahme von Daten möglich und sogar der Beschlagnahme von gesamten Datenträgern vorzuziehen. Diese Vorgehensweise schützt einerseits die Privatsphäre des Betroffenen und auch die von unbeteiligten Dritten[1], andererseits bedeutet dies auch, dass Cloud-Daten und E-Mail Accounts beschlagnahmt werden dürfen, obwohl diese keine Gegenstände sind.[2]

> **Beispiel Wall Street Market:**
> Wall Street Market gehörte zu den größten Dark-Net Marktplätzen seiner Zeit. Ein Darknet-Markt ist ein, virtueller Marktplatz abseits des Internets, der im Tor-Netzwerk betrieben wird. Das Tor-Netzwerk bietet eine Verschleierung der IP-Adressen der Nutzer, was es Strafverfolgern besonders schwer macht, Ermittlungen durchzuführen. Aufgrunddessen wurde Wall Street Market hauptsächlich für Drogenhandel und den Verkauf von fremden Daten (wie z.B. Kreditkarten und Nutzerdaten) und Malware verwendet.
> Am 23. und 24. April 2019 wurden die drei mutmaßlichen Websitebetreiber festgenommen und es kam zu einer Hausdurchsuchung. Hierbei wurden Computer und Datenträger nach § 94 beschlagnahmt. Am 2. Mai 2019 wurden die in Deuschland gehosteten Server der Website vom Europol und dem Bundeskriminalamt beschlagnahmt und abgeschaltet. Durch den Zugriff auf die Datenträger konnten bis Ende Juni 2019 Kryptowährungen im Wert von 16 Millionen Euro beschlagnahmt werden. Durch die strafrechtlichen Maßnahmen und die damit gesammelten Beweise konnten die Behörden eine erfolgreiche Ermittlung und Festnahme der Cyberkriminellen durchführen. [16]

[1] Auf Geräten von Verdachtspersonen können auch Daten von unbeteiligten Personen vorhanden sein, z.B. Fotos oder Nachrichten. Es wichtig diese nicht tatrelevanten Daten zu schützen.
[2] Diese Erkenntnis ist wichtig für die Bewertung des neuen Gesetzentwurfes in Kapitel 3.

Abbildung 2.1: Banner der beschlagnahmten Website von Wall Street Market. [3]

Trotz des angesprochenen Alters der StPO beweist sich § 94, im Rahmen des digitalen Zeitalters, als durchaus vernünftiges und zukunftsorientiertes Mittel der Strafverfolgung. [12]

2.2 Telekommunikationsüberwachung (TKÜ) nach § 100 a StPO

Eine weitere beliebte Methode der Strafverfolgung ist die TKÜ. Der § 100 a beschreibt die Überwachung und Aufzeichnung jeglicher Art von Telekommunikation. [1] Dabei ist der Begriff der Telekommunikation absichtlich interpretationsoffen gehalten, um auch zukünftige Arten der Nachrichtenübertragung zu erfassen. [12] Dementsprechend fallen unter den Begriff der Telekommunikation alle gängigen Kommunikationsmittel, wie z.B Messenger-Dienste (WhatsApp etc.), E-Mails und Telefonie.
Die TKÜ ist ein tiefgreifenderer Eingriff als die Beschlagnahme, weshalb die Anforderungen, um diese anzuordnen, auch höher gesetzt sind. Das wird damit begründet, dass eine TKÜ das Fernmedegeheimnis des Art. 10 Abs. 1 GG verletzt und zudem heimlich durchgeführt wird, *also ohne den Betroffenen zu benachrichtigen.* Dementsprechend darf die TKÜ nur eingesetzt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass eine schwere Straftat begangen wurde oder geplant ist (nach Abs. 1 Satz 1 Nr. 1). Außerdem muss begründet werden, dass die Ermittlung auf anderen Wege, wesentlich

erschwert oder aussichtslos wäre und deshalb auf die TKÜ zurückgegriffen werden muss (nach Abs. 1 Satz 1 Nr. 3). [1] Eine Begründung hierfür wäre die Strafverfolgung von Cyberkriminellen, die nur über das Internet kommunizieren und sich nicht persönlich treffen. Dies trifft oft bei den Administratoren von Dark-Net Marktplätzen, wie auch Wall Street Market, zu.
Der Einsatzrahmen der TKÜ ist im Abs. 2 aufgelistet und reicht von Straftaten des Hochverrats über Mord und Totschlag bis hin zu Straftaten des Betäubungsmittelgesetzes. Aber auch bei Straftaten gegen den wirtschaftlichen Wettbewerb, Steuerhinterziehung und Straftaten des Raubes und der Erpressung kann die TKÜ eingesetzt werden.

Der Vorgang einer Standard-TKÜ ist so vorgesehen, dass man die Kommunikation auf dem *Übertragungsweg* überwacht und aufnimmt. Im Kontext der Telekommunikation kann diese z.B. beim Internet-Service-Provider (z.B. Telekom oder Vodafone) oder bei den E-Mail-Providern mitgeschnitten werden. Diese Telekommunikationsdienstleister sind laut § 100a Abs. 4 dazu verpflichtet, den Strafverfolgungsbehörden Auskunft zu geben oder Maßnahmen zur TKÜ zu ermöglichen. Jedoch bewährt sich diese Methode der TKÜ nur dann, wenn die Kommunikation unverschlüsselt stattfindet. Wenn diese verschlüsselt ist, dann sind die Daten, ohne den dazugehörigen Schlüssel, nicht verwertbar.[3] Ein Abhören der laufenden Übertragung bei den Telekommunikationsdienstleistern hat hier also wenig Sinn.
Um auch bei verschlüsselter Kommunikation Ermittlungen durchführen zu können, wurde zum 24. August 2017, mit dem Gesetz zur Neuregelung der effektiveren und praxistauglicheren Gestaltung des Strafverfahrens, die **Quellen-TKÜ** und die **Online-Durchsuchung** eingeführt. [4] Beide Methoden stellen eine erhebliche Erweiterung der Befugnisse von Strafverfolgungsbehörden dar, da in beiden Fällen das Endgerät des Betroffenen heimlich infiltriert werden muss. Dies geschieht durch die Einschleusung einer Spionagesoftware, auch **Staatstrojaner** genannt. Diese Software gehört zu den Remote Access Tools (RATs) und ermöglicht den Behörden einen uneingeschränkten Fernzugriff auf das Gerät. In den Folgenden Kapiteln werden die neuen Methoden erläutert.

2.2.1 Quellen-TKÜ nach § 100 a Abs. 1 Satz 2, 3 StPO

Die Quellen-TKÜ löst das Problem der Ende-zu-Ende Verschlüsselung, da hier die Kommunikation nicht bei der Übertragung mitgeschnitten wird, sondern direkt auf dem Endgerät des Absenders oder des Empfängers, also sinnbildlich an der Quelle der Kommunikation. Durch das Infiltrieren des Gerätes mit einem RAT (Staatstrojaner) können die Nachrichten vor oder nach der Verschlüsselung angesehen werden.
Die Quellen-TKÜ ist als Ergänzung des § 100a konzipiert, welcher die TKÜ einer *laufenden* Übertragung beschreibt. Ein Eingriff auf das Gerät geht jedoch weit über eine laufende Übertragung hinaus, weshalb hier nicht nur das Fernmeldegeheimnis nach § 10 GG verletzt wird, sondern auch das Grundrecht auf Vertraulichkeit und Integrität

[3] Nur durch das Aufbringen von extrem hoher Rechenleistung kann eine moderne Verschlüsselung geknackt werden.

informationstechnischer Systeme. [12] Um eine Quellen-TKÜ anzuordnen genügt nach Abs. 1 Satz 2, 3 schon der Verdacht, dass die abzuhörende Kommunikation verschlüsselt abläuft. Jedoch dürfen nur die Daten auf dem Endgerät überwacht und aufgezeichnet werden, die ab dem Zeitpunkt der gerichtlichen Anordnung

> „auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können." - § 100a Abs. 1 Satz 3 [1]

Diese zeitliche Begrenzung ist äußerst wichtig, da so nicht auf alle Nachrichten und Daten einer Kommunikation zugegriffen werden kann, was einer Online-Durchsuchung entsprechen würde.

2.2.2 Online-Durchsuchung nach § 100 b StPO

Neben der Quellen-TKÜ wurde mit der Gesetzeseinführung vom August 2018 auch die Online-Durchsuchung hinzugefügt. Zur Durchführung wird wieder das Endgerät des Betroffenen heimlich infiltriert. Bei dieser Methode ist es den Behörden erlaubt, sämtliche Daten des Betroffenen einzusehen und zu verwerten. Im 3. Absatz wird explizit erwähnt, dass sich die Maßnahme nur gegen das Gerät des Beschuldigten richten darf und nicht gegen Geräte von unbeteiligten Personen. Jedoch darf die Maßnahme auch dann durchgeführt werden, wenn andere Personen davon unvermeidbar betroffen werden, z.B. weil Daten dieser Personen auf dem Gerät des Beschuldigten gespeichert sind.
Die Online-Durchsuchung darf nur dann angeordnet werden, wenn die potenzielle Tat der Verdachtsperson einer besonders schweren Straftat aus dem Straftatenkatalog in Abs. 2 entspricht und die Ermittlung über andere Methoden erschwert oder aussichtslos wäre. Dieser Katalog ist enger gefasst als der der TKÜ. Straftaten, wie z.B. gegen den wirtschaftlichen Wettbewerb wurden gänzlich weggelassen und Straftaten, wie z.B. die des Raubes wurden zu schwerer Raub und Raub mit Todesfolge abgeändert. Aufgrund dessen gilt die Maßnahme der Online-Durchsuchung als eine der schwerwiegendsten Maßnahmen der StPO. [1]

3 Einführung von § 95a StPO-E: Heimliche Beschlagnahme

Im März 2021 wurde ein Entwurf eines „Gesetzes zur Fortentwicklung der StPO und anderer Vorschriften“ veröffentlicht. Kurz vor Verabschiedung, und somit ohne Möglichkeit der Bewertung von Begutachtern, wurde § 95a zur *heimlichen* Beschlagnahme hinzugefügt. Die Strafverfolgungsbehörden sollen damit leichter auf E-Mails und Cloud-Inhalte zugreifen können, ohne den Betroffenen benachrichtigen zu müssen. [11]

Dieser Entwurf wurde wenige Tage vor Fertigstellung dieser Ausarbeitung, am 10.06.2021, vom Bundestag unverändert angenommen. Die folgenden Kritikpunkte wurden von der Gesetzgebung ***nicht*** *beachtet.* [6]

Die Überschrift des Paragrafen: „Zurückstellung der Benachrichtigung des Beschuldigten“, ist unscheinbar und kann deshalb fehlleiten. Die Beschlagnahme von Daten nach §§ 94 ff. gehörte bisher zu den offenen Standardmaßnahmen einer Strafverfolgung. Im Gegensatz zur TKÜ oder Online-Durchsuchung musste der Beschuldigte nach der Durchführung benachrichtigt werden, damit dieser sich im Strafverfahren verteidigen konnte. Der neue Paragraf bietet den Behörden die Möglichkeit, eine heimliche Beschlagnahme durchzuführen, welche auch in Form von Daten möglich ist (festgestellt in 2.1). [9]
Besonders die heimliche Beschlagnahme von E-Mails und Clouddaten lässt sich mit einer Quellen-TKÜ und Online-Durchsuchung vergleichen. Ein langjährig geführter E-Mail Account könnte wesentlich für die Erstellung eines detaillierten Persönlichkeitsprofils sein. Eine Cloud als externer Datenträger könnte genauso viele Daten enthalten, wie das Endgerät des Betroffenen. Heutzutage setzen immer mehr Anwendungen auf die automatische Speicherung von Inhalten in der Cloud. [9] Der Foto-Messenger Snapchat ist ein hierfür ein Beispiel, da alle in der App gespeicherten Bilder in eine Cloud geladen werden, ohne dies dem Nutzer direkt mitzuteilen.

Dr. Mayeul Hiéramente, ein Rechtsanwalt und Fachanwalt für Strafrecht, sieht in dem Paragrafen einen Paradigmenwechsel. Laut ihm liegt das größte Problem in der strukturellen Natur der Regelung:

> „Der Gesetzesentwurf schafft keine gesonderte Rechtsgrundlage für die „heimliche Beschlagnahme“. Diese soll nach Vorstellung der Bundesregierung vielmehr nach den gewohnten Regeln (§§ 94 ff. StPO) erfolgen. Für eine Beschlagnahme ist bereits ein Anfangsverdacht ausreichend, diese Hürde ist in der Praxis äußerst schnell überwunden.“ - Dr. Hiéramente [9]

Für eine „normale“ Beschlagnahme gibt es keinen Straftatenkatalog, was bedeutet das Bagatelldelikte, wie ein Diebstahl im Supermarkt, als Einsatzgrund ausreichen würden. Das Bundesverfassungsgericht hat diese niedrige gesetzliche Hürde akzeptiert, da die ausführende Behörde den Beschuldigten nach der Durchführung der Beschlagnahme benachrichtigen muss und dieser dann seine Rechte im Verfahren geltend machen kann. [9] Mit dem neuen § 95a können die Behörden die Beschlagnahme durchführen und *danach* eine Zurückstellung der nachträglichen Benachrichtigung beantragen, was erst dann erhöhte Anforderungen und einen richterlichen Beschluss mit sich bringen würde. [11] Demnach darf die Benachrichtigung nur dann zurückgestellt werden, wenn die mutmaßliche Straftat dem Straftatenkatalog aus § 100a Abs. 2 entspricht. Damit wird die heimliche Beschlagnahme mit der TKÜ nach § 100a gleichgesetzt. Die Zurückstellung soll ausschließlich dann in Betracht gezogen werden, wenn die Benachrichtigung den Untersuchungszweck gefährden würde. [5]
Gerade, weil die heimliche Beschlagnahme erst im Nachhinein beantragt werden kann, erkennt Dr. Hiéramente hier ein Schlupfloch für die Strafverfolgungsbehörden. Zu dem Zeitpunkt der Beantragung befinden sich die Daten bereits in den Händen der Strafverfolgern (LKA, Steuerfahndung etc.). Dies kann ausgenutzt werden: Nach der Begutachtung der Daten kann auf Grundlage dieser die heimliche Beschlagnahme begründet und somit eine Zurückstellung der Benachrichtigung beantragt werden. Erst dann gelten die erhöhten Anforderungen. [9]
Außerdem sieht der Gesetzesentwurf keine Konsequenzen vor, wenn nach der Beschlagnahme die erforderliche Mitteilung nicht erfolgt. Dr. Hiéramente geht davon aus, dass Strafgerichte keine Verwertungsverbote für beschlagnahmte Daten aussprechen dürfen, wie es z.B. bei der Quellen-TKÜ oder der Online-Durchsuchung üblich ist. Von Löschungspflichten wird im Entwurf ebenso wenig erwähnt. [9]

Alexander Ignor, Vorsitzender des Strafrechtsausschusses der Bundesrechtsanwaltskammer und Professor an der Berliner Humboldt-Universität sowie der bereits erwähnte Dr. Hiéramente geben ähnliche Sorgen zum Gesetzgebungsverfahren zur Kenntnis. Beide erkennen, dass in den letzten Monaten mehrere Sicherheitsgesetze ungewöhnlich schnell durch den Bundestag „gejagt“ wurden, was eine kritische Auseinandersetzung mit den Themen erschwert hatte. Sogar die gehörten Sachverständigen sollen auf die kurzen Fristen hingewiesen haben [11]
Ein Beispiel hierfür wäre ein, am 09.10.2021 verabschiedeteter neuer Gesetzesentwurf zur „Anpassung des Verfassungsschutzrechts“. Mit diesem Entwurf gibt der Bundestag Staatstrojaner für Geheimdienste und Bundespolizei frei. [10]

> „Diese gesetzgeberische Hektik droht handwerkliche Fehler zu produzieren und führt zu einer Gesetzgebung *in dubio pro Sicherheit*.“
> - Dr. Hiéramente [9]

Demnach würde ein Grundsatz „im Zweifel für die **Sicherheit**“ gelten, anstatt wie bisher *pro reo*, also „im Zweifel für den **Angeklagten**“.

4 Fazit

Im Laufe dieser Ausarbeitung wurden die Probleme des digitalen Zeitalters dargestellt und die aktuellen Maßnahmen der StPO, also die Beschlagnahme und die TKÜ mit der Quellen-TKÜ sowie der Online-Durchsuchung, untersucht. Die Schwere der Maßnahmen wurde im Verhältnis zum praktischen Einsatzrahmen bewertet und für angemessen befunden. Bei der Bewertung des neuen § 95a wurde klargestellt, dass dieser anfällig für Ausnutzung seitens der Strafverfolgungsbehörden ist. Diese, in Kapitel 3 genannten Kritikpunkte sind Grund genug, den Paragrafen zu überarbeiten und die Struktur der anderen Maßnahmen der Strafverfolgung anzupassen. Dies ist ist im Gesetzgebungsverfahren des Entwurfes nicht mehr möglich, da dieser im Juni 2021 unverändert verabschiedet wurde. Die Gesetzgebung hat folglich die Kritikpunkte mehrerer Experten nicht aufgenommen. Die Möglichkeit einer Änderung kann sich nur in zukünftigen Gesetzesentwürfen der StPo ergeben.
Eine abschließende, themenübergreifende Erkenntnis ist die ungewöhnliche Geschwindigkeit von Gesetzgebungsverfahren von Sicherheitsgesetzen. Experten warnen vor Nachlässigkeit und appellieren zu einer intensiveren Auseinandersetzung mit diesen Gesetzen.

Literaturverzeichnis

[1] Strafprozeßordnung (StPO), 2021. Besucht am 15.05.2021. URL: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html.

[2] Bundesgerichtshof. Beschluss in der Strafsache wegen Bandenhandels mit Betäubungsmitteln in nicht geringer Menge. 2015. Besucht am 18.06.2021. URL: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=72331&pos=0&anz=1.

[3] Bundeskriminalamt. Bildquelle: WALL STREET MARKET – Presseeinladung, 2019. Besucht am 16.06.2021. URL: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html.

[4] Bundesregierung. Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, 2018. Besucht am 16.05.2021. URL: http://dipbt.bundestag.de/extrakt/ba/WP18/788/78842.html.

[5] Bundesregierung. Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften. 2021. Besucht am 08.05.2021. URL: https://www.bundesrat.de/SharedDocs/drucksachen/2021/0001-0100/57-21.pdf?__blob=publicationFile&v=1.

[6] Deutscher Bundestag. Vorgang - Gesetzgebung - Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften, 2021. Besucht am 18.06.2021. URL: https://dip.bundestag.de/vorgang/.../272971.

[7] CCDM GmbH. SSL-Zertifikat wird ab dem 25. Mai Pflicht! - CCDM GmbH, 2018. Besucht am 16.05.2021. URL: https://ccdm.de/news/ssl-zertifikat-wird-ab-dem-25-mai-pflicht/.

[8] Federal Bureau of Investigation. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? | Federal Bureau of Investigation, 2014. Besucht am 17.06.2021. URL: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[9] Mayeul Hiéramente. Beschlagnahme von E-Mails: In aller Heimlichkeit, 2021. Besucht am 08.05.2021. URL: https://netzpolitik.org/2021/beschlagnahme-von-e-mails-in-aller-heimlichkeit/.

[10] Stefan Krempl. Bundestag gibt Staatstrojaner für Geheimdienste und Bundespolizei frei. *heise online*, 2021. Besucht am 18.06.2021. URL: `https://www.heise.de/news/Bundestag-gibt-Staatstrojaner-fuer-Geheimdienste-und-Bundespolizei-frei-6067818.html`.

[11] Dieter Petereit. Verdeckter Datenzugriff: Polizei soll schon bei Bagatellen E-Mails und Cloud-Daten einsehen dürfen. 05.03.2021. Besucht am 08.05.2021. URL: `https://t3n.de/news/verdeckter-datenzugriff-polizei-1363914/`.

[12] Felix Ruppert. Die moderne Klaviatur der Strafverfolgung im digitalen Zeitalter. 2018.

[13] Ivan Škorvánek, Bert-Jaap Koops, Bryce Clayton Newell, and Andrew Roberts. "My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking. *Brigham Young University Law Review*, 2019.

[14] Hilgendorf / Valerius. Computer- und Internetstrafrecht (2. Auflage), Springer Verlag. 2012.

[15] Wikipedia. Strafverfolgungsbehörde, 2020. Besucht am 15.05.2021. URL: `https://de.wikipedia.org/wiki/Strafverfolgungsbehörde`.

[16] Wikipedia. Wall Street Market, 2021. Besucht am 17.06.2021. URL: `https://de.wikipedia.org/Wall_Street_Market`.