universität wien

Exposé

Arbeitstitel der Dissertation

Überwachung von IT-Verhalten

Der Computer als Ermittlungswerkzeug Mobiltelefon & Co als Beweismittel

Verfasserin

Mag.ª Shirin Ghazanfari

Angestrebter akademischer Grad

Doktorin der Rechtswissenschaften (Dr.in iuris)

Betreuerin

Univ. Prof.in Mag.ª Dr.in Ingeborg Zerbes

Wien, Juli 2020

Studienkennzahl laut Studienblatt: A 783 101

Studienrichtung laut Studienblatt: Rechtswissenschaften

Fachbereich: Strafrecht und Kriminologie

Inhaltsverzeichnis

Einführung in das Thema

Das Internet of Things (IOT) ist im heutigen Alltag kaum noch wegzudenken. IOT ist die Gesamtheit aller smarten Systeme, die durch Kommunikation und Datenübertragung funktionieren. Mehr Daten bedeuten in diesem Zusammenhang mehr Informationen. Zur Erleichterung von Kommunikation werden – freiwillig – durch den Endnutzer Daten freigegeben. Der User verwendet ein Smartphone, auf dem er E-Mails, Fotos, Videos, präferierte Musik, usw gespeichert hat. Um dem Fitness-Ziel näher zu kommen, verwendet er eine Smart Watch, auf der seine Meta- und Gesundheitsdaten gespeichert sind. Um die optimale Route beim Laufen oder am Weg in den Urlaub zu finden, verwendet er Routenplaner und Tracking Systeme wie *Google Maps* und *Runtastic*. Die privaten Urlaubsbilder und andere höchstpersönliche Momente hält er auf Social Media fest und schaltet im Urlaub über ein Smart Home den Strom aus – wenn er vergessen hat, seinem *Alexa*-Gerät die Anweisung zu geben, sich darum zu kümmern.

Man darf wohl ohne den Vorwurf zu übertreiben das Mobiltelefon das „moderne Tagebuch" des Menschen nennen, das – wenn es in die Hände der Ermittlungsbehörden fällt – einen tiefgreifenden, präzisen Einblick in das Leben betroffener Personen ermöglicht. Miteinbezogen sind nicht nur der Inhaber selbst, sondern auch diejenigen, die mit ihm in Kontakt waren. Zu dieser modernen „Selbstüberwachung" entscheidet sich der Nutzer letzten Endes freiwillig. Er gibt die Freigabebestätigung ab, er selbst gibt seine Daten preis. Genutzt wird IOT nicht nur durch Private, sondern auch durch öffentliche Institutionen und Berufsgeheimnisträger, was zur Folge hat, dass öffentliche wie nicht öffentliche (geheime) Informationen digital zugriffbereit bleiben. Diese Masse an frei zugänglichen sowie leicht zu beschaffenden Daten bietet nicht nur Raum für kriminelle Handlungen, sie bietet den Ermittlungsbehörden auch Vorteile: Schnellere und effizientere Ermittlungen werden durch den Zugriff auf große Datenmengen ermöglicht, was zur Folge haben kann, dass kriminelle Netzwerke digital leichter aufzuspüren sind. Eine genauere Ortung Verdächtiger ist durch dessen digitalen „Fußabdruck" ebenfalls ungleich einfacher möglich als früher. Eines steht fest: Verdeckte und offene Ermittlungsmaßnahmen mit Hilfe von oder an IOT ermöglichen intensive (Überwachungs-) Eingriffe im höchstpersönlichen Bereich. Schwierig ist, hierbei abzugrenzen, unter welchen Voraussetzungen Ermittlungsbehörden auf die auf diesen Smartphones etc selbst, aber auch auf externen Computern gespeicherte Daten – Stichwort: Cloudcomputing – zugreifen dürfen.

Die bisherigen Instrumente in der Strafprozessordnung (StPO), die in diesem Zusammenhang einen Zugriff auf Endgeräte und auf Online-sowie Offline-Inhalte ermöglichen, sind die Sicherstellung und Beschlagnahme (§ 109 ff), die Hausdurchsuchung § 117, 119 ff) sowie die Befugnisse zum Zugriff auf Daten und Inhalte von Nachrichten (§§ 134, 135, 137 ff).[1] Die Abgrenzung zwischen diesen Ermittlungsmethoden ist formell und technisch nicht immer einfach. Während die Sicherstellung und Beschlagnahme sowie die Hausdurchsuchung offene

[1] Dies stellt lediglich einen Überblick über die wichtigsten Methoden dar. Die Abgrenzung zu anderen offenen sowie verdeckten Ermittlungsmethoden und weitere Befugnisse aus Sicherheitspolizeigesetz (SPG) und Polizeilichem Staatsschutzgesetz (PStSG) werden im Zuge der Erarbeitung der Dissertation mitbehandelt werden.

und gegenstandsbezogene Maßnahmen sind, von denen der Betroffene Kenntnis erlangen muss, steht eine solche Offenheit dem Zweck der (Nachrichten-)Überwachung entgegen. Die Überwachung verschlüsselter Nachrichten – genauer: die Entschlüsselung von Nachrichten, damit sie überhaupt überwacht werden können – ist nach der StPO derzeit nicht zulässig: Der VfGH[2] hat die gesetzlichen Grundlagen einer sog „Quellen-TKÜ" (auch „Bundestrojaner") wieder aufgehoben. Diese sind aber nur vorerst Geschichte – dem Versuch einer Neuregelung steht nichts im Wege. Die Diskussion um eine verpflichtende Überwachungs-App im Zusammenhang mit dem Corona Virus zur Prävention von sogenannten Clustern[3] hat jüngst noch einmal gezeigt, dass ein solcher Grundrechtseingriff wohl überlegt und an eine hohe Eingriffsschwelle gebunden sein muss. Das Interesse der Ermittlungsbehörden am Zugriff auf End-to-End-verschlüsselte[4] Kommunikation muss, so der kern der VfGH-Entscheidung, in Relation zur Schwere des Eingriffs stehen, er muss von einer online-Überwachung im weiteren Sinn – die Beobachtung sämtlichen Verhaltens an einem Rechner – abgrenzbar sein und er darf nicht mehr mit heimlicher Durschsung verbunden werden.

Die Frage, die sich in diesem Zusammenhang stellt, ist: Dürfen die Ermittlungsbehörden all das, was sie theoretisch könnten? Sind Eingriffe in Grundrechte immer gerechtfertigt? Sind in der StPO ausreichend Rechtsschutzmöglichkeiten vorgesehen?

Weitere Probleme stellen sich in Zusammenhang mit dem Datentypus, auf den zugegriffen werden darf, der aber nicht abschließend definiert ist. Die Sensibilität der Daten variiert, manche sind vor den Strafverfolgungsbehörden sogar abgeschirmt, man denke etwa an Anwaltsunterlage. Die bestehenden Eingriffsschwellen – vor allem die der Sicherstellung[5], aber auch der Nachrichtenüberwachung – müssen im Hinblick auf sensible Daten neu überdacht werden. Denn die enorme und geradezu unabsehbare Reichweite der (beobachtenden) Einsicht in Daten, die das IOT generiert, bietet Raum für Missbrauch, für den Zugriff auf geheime (zB berufsgeheime) Daten und tendiert zur Unverhältnismäßigkeit. Unbescholtene Bürgerinnen und Bürger könnten in das „Visier des Staates geraten"[6], weil Verdächtige mit ihnen zuvor kommuniziert oder Fotos von ihnen gespeichert haben. Ermittlungsbehörden erlangen Zugriff auf jegliche Kommunikationspartner des Inhabers des Mobiltelefons. Und wenn es so weit ist, ist nicht abschließend geregelt, wer worauf zugreifen darf und wie mit Zufallsfunden und neuen Verbindungen umzugehen ist – und wenn es doch

[2] VfGH 11. 12. 2019, G 72-74/2018-48, G 181-182/2019-18.

[3] https://www.derstandard.at/story/2000118645764/stopp-corona-app-was-hat-das-rote-kreuz-bloss-falsch.

[4] End-to-End ist ein Mechanismus, der vor Absenden einer in der App verfassten Nachricht diese verschlüsselt und somit für andere unlesbar macht. Fängt man eine solche Nachricht nach Verschlüsselung ab, ist es nicht mehr möglich, sie zu entschlüsseln.

[5] Die Sicherstellung eines Mobiltelefons, auf dem sich auch offline sensible Daten befinden, ist derzeit zulässig, sobald sie aus Beweisgründen (Z 1), Sicherung privatrechtlicher Ansprüche (Z 2) oder zur Sicherung der Konfiskation, des Verfalls, des erweiterten Verfalls, der Einziehung oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung erforderlich erscheint.

[6] *Fink*, Der "Bundestrojaner" ist (hoffentlich) endlich Geschichte, AnwBl 2020/32.

geregelt ist, ist die Eingriffsschwelle, zumindest was die Sicherstellung anbelangt, sehr gering. Klaffen Praxis und Theorie auseinander?

Forschungsfrage

Inwieweit ermöglicht die StPO in ihrer derzeitigen Form die Durchführung von Ermittlungsmaßnahmen an und durch Informationstechnologie und welcher rechtlicher Erweiterungen oder Modifikationen bedarf es, um auf neue Technologien und Datenmengen angemessen zu reagieren?

Erforschung von Informationstechnologie – das Mobiltelefon im Besonderen – als Ermittlungswerkzeug unter Verwendung von durch die Arbeit führende Fragen:

Was kann und darf man?
Bestandsaufnahme derzeitiger Ermittlungsmethoden
Was kann, darf man aber nicht?
Ermittlungsmethoden, die rechtlich nicht gedeckt, technisch aber möglich sind
Was darf, kann man aber nicht?
Ermittlungsmaßnahmen mit Rechtsgrundlage, die technisch nicht durchführbar sind
Was kann und darf man nicht?
Lücken in der Rechtsordnung, die auch neue technische Lösungen verlangen
Wie wird man es können und dürfen?
Lückenschließung ua durch Rechtsvergleich unter Einbringung eigener Lösungsvorschläge

Aufbau der Dissertation

I. Teil Bestandsaufnahme
II. Teil Ansätze, Perspektiven, Lösungsvorschläge

Der Erste Teil wird etwa zwei Drittel der Arbeit umfassen und dient der **Bestandsaufnahme.** Der Einstieg soll anhand einer **Handysicherstellung** durch die KriPo erfolgen: Eine solche ermöglicht nahezu sämtliche Formen des Datenzugriffs. Auf welche Daten, die über dieses Handy sichtbar gemacht werden können, dürfen die Strafverfolgungsbehörden zugreifen? Welche Ermittlungsbefugnisse stehen ihnen dafür zur Verfügung und an welche Grenzen sind sie gebunden?

In gebotener Kürze werden in dieser Bestandsaufnahme auch **technische Grundlagen** skizziert: die faktischen Möglichkeiten, die in der Folge rechtlich analysiert werden.

Eine grundlegende Unterscheidung wird zwischen dem Zugriff auf **Online-** und dem Zugriff auf **Offline-Medien** gezogen. Hierzu ist eine **Kategorisierung** der betroffenen Datentypen unter Heranziehung des TKG und eine Analyse der **Eingriffsschwellen** für die jeweiligen Ermittlungsmaßnahmen notwendig. Auch wenn das Telekommunikationsgesetz bereits viele Daten[7] unterscheidet, ist keine abschließende Regelung zu finden: zB fehlen spezielle Hinweise auf Gesundheitsdaten, die in Apps vorzufinden sind. Ohne Anspruch auf

[7] Siehe § 92 Abs 3 Telekommunikationsgesetz (TKG).

Vollständigkeit sollen besondere Problembereiche hervorgehoben und genauer behandelt werden. Eines der Kernthemen wird die Abgrenzung zwischen einer (offenen) Sicherstellung und einer (geheimen) Überwachung sein.

Daten **verschiedener Sensibilität** verlangen zudem ein dieser Sensibilität entsprechendes Schutzniveau. Dass über die Sicherstellung eines Mobiltelefons der Zugriff auf sämtliche Offline- und Online-Daten möglich wäre, bedeutet nicht, dass er auch im Hinblick auf das in Verdacht stehende Delikt angemessen oder erlaubt ist (siehe unten).

Als **Zwischenbilanz** soll herausgearbeitet sein: „**Was können und dürfen die Ermittlungsbehörden derzeit"?**

Anschließend werden die neuen technischen Hilfsmittel untersucht, für deren Einsatz derzeitige **(noch) keine rechtliche Grundlage** existiert, kurzum soll es um die Frage gehen: **„Was können, dürfen die Ermittlungsbehörden aber nicht?"** Insbesondere das nach einer Hausdurchsuchung weitergehende Mitlesen von Daten auf Computern, die im Rahmen einer Hausdurchsuchung aufgefunden worden sind, ist als Überwachungsmaßnahme nicht mehr vom Instrument mitumfasst.[8] Auch strafprozessuale Ermittlungen im Internet, die nicht über ein Endgerät des Verdächtigen erfolgen, sollen mitbehandelt werden. Liegt immer eine verdeckte Ermittlung durch die Polizei vor, wenn sie sich auf Sozial Media und im Dark Net bewegt und offene Informationen inspiziert? Verdeckte Ermittlungen liegen jedenfalls vor, wenn die Polizei anonym oder unter Pseudonym aktiv Kontakt zu Verdächtigen aufnimmt.[9]

Weiters sollen Ermittlungsmaßnahmen und Zugriffe auf Daten betrachtet werden, die rechtlich zwar eine Grundlage finden, technisch aber (noch) nicht umsetzbar sind. Unter diesen Punkt wäre vor Aufhebung der österreichischen Quellen-TKÜ das Problem der Revidierbarkeit des Infiltrierens eines Computersystems gefallen. Auch die Gefahren für Behörden wie der „Hack zurück", also das Hacken behördlicher Systeme durch den Betroffenen, müssen hier mitbehandelt werden, um zu eruieren **„Was dürfen, können die Ermittlungsbehörden aber nicht?"**

In einem letzten Schritt des ersten Teils soll eruiert werden, welche Ermittlungsmaßnahmen weder rechtlich gedeckt noch derzeit technisch möglich sind. Die Bilanz dieses Teiles lautet **„Was dürfen und können die Ermittlungsbehörden nicht?"** Ein großes Thema wird hier die durch den VfGH aufgehobene **Quellentelekommunikationsüberwachung** sein.[10] Eine solche Quellen-TKÜ bringt zwar Möglichkeiten, vor allem aber komplexe Fragestellungen mit sich. Zum einen ist zu klären, an welcher Eingriffsschwelle man für die Maßnahmen ansetzt. Im

[8] *Zerbes/El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, 432.

[9] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht Rz 5.35.

[10] Telekommunikationsüberwachung ist die Bezeichnung für die Überwachung von allen Telekommunikationsvorgängen und Telekommunikationsinhalten: Wann also wer mit wem wie oft von wo aus wohin und worüber kommuniziert.

aufgehobenen § 135a StPO[11] musste es sich um eine aktuelle Entführung oder, bei Zustimmung des Inhabers, auch die mit mehr als sechs Monaten Freiheitsstrafe bedrohten Vorsatztaten handeln. Die übrigen Anlasstaten waren: Eine mit mehr als 10 Jahren Freiheitsstrafe bedrohte Vorsatztat oder eine Straftat nach §§ 278a-278e StGB (Kriminelle Organisation, Terroristische Vereinigung, terroristische Straftaten und bestimmte terrorismusfördernde Straftaten) oder eine Straftat im Rahmen einer kriminellen Gruppierung (§§ 278-278b StGB) oder mit mehr als 5 Jahren FS bedrohte Vorsatztat gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung. All dies aber nur, wenn die Aufklärung ansonsten wesentlich erschwert wäre, bei dringendem Tatverdacht oder wenn der Beschuldigte Inhaber oder erwarteter Benützer des überwachten Computersystems wäre oder erwartet wurde, dass er dorthin Nachrichten adressieren werde. Zum anderen hätten all diese Punkte unter der Prämisse stattfinden sollen, dass die Spyware nachträglich unschädlich gemacht wird und revidierbar ist und, dass andere Computersysteme schadlos gehalten werden können, was nicht der Fall war.

Der **Zweite Teil** wird etwa ein Drittel der Arbeit umfassen und soll, auch mit Hilfe rechtsvergleichender Ansätze, **eigene Lösungsvorschläge** beinhalten. Die letzte Frage, die es zu beantworten gilt, ist: **„Unter welche Voraussetzungen sollen die Ermittlungsbehörden all' das, was möglich ist, dürfen?"** Entworfen werden sollen Formulierungen für die Ermittlungsmaßnahmen an sich, für Rechtsschutzmöglichkeiten, technische Ausstattung, für den Grundrechtsschutz und für die durch einzelne Befugnisgrenzen garantierte Verhältnismäßigkeit. Ein wichtiger Bereich ist die Anknüpfung der StPO an einzelne Tatbestände. Der in Strafrechtkreisen kritisierte Vorschlag, die Strafdrohung für gewisse Straftaten anzuheben, um dadurch eine Neuregelung die Quellen-TKÜ zu ermöglichen, steht der bestehenden deutschen Regelung gegenüber, die an zwar konkrete, aber insgesamt äußert umfassende Deliktskataloge anknüpft.[12] Die optimale Lösung scheint damit nicht erreicht, denn auch eine Überregulierung führt zu Rechtsunsicherheit. Eine sinnvolle, transparente Grenze soll hier gefunden werden. Das Schlusslicht bilden das Resümee und der Ausblick in die Zukunft.

Forschungsstand

Aktuell existiert keine Dissertation zum Thema „Ermittlungsmaßnahmen im Wandel und IOT". Die Materialien zu diesem Themenbereich sind überschaubar. In der österreichischen Rechtsliteratur wird diesem Thema in Form von Zeitschriftenbeiträgen Rechnung getragen. Entscheidungsbesprechungen zum Bundestrojaner sind ein Großteil der aktuellen Literatur. Bücher finden sich keine, allerdings widmet das Handbuch IT-Strafrecht dem Thema ein Kapitel. Wichtige Überlegungen zur Überwachung finden sich überdies in *Zerbes*, Spitzeln, Spähen, Spionieren. Kommentierungen zu StPO Bestimmungen finden sich hingegen bundesweit in anerkannten Kommentaren. In der Schweizer sowie in Deutscher Literatur

[11] Bundesgesetz, mit dem die Strafprozessordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018), BGBl 27/2018.

[12] Siehe §§ 100a und 100b dStPO.

wird das Thema allerdings intensiver behandelt – nicht zuletzt wegen der in Deutschland bereits bestehenden Online-Durchsuchung § 100b dStPO und der Telekommunikationsüberwachung § 100a dStPO. Viel Material widmet sich der in Österreich durch den VfGH aufgehobenen §§ 134 Z 3a und 135a StPO.

Forschungsmethode

Es handelt sich um eine rein dogmatische Arbeit. Erforscht wird anhand wissenschaftlicher Recherche rechtlicher und technischer Natur unter Zuhilfenahme von Print- und Online-Literatur und entsprechender nationaler und internationaler Rechtsdatenbanken. Außerdem sind Vorfeldgespräche mit Personen aus der Praxis geplant, die informell stattfinden sollen. Inhaltlich werden diese nicht in die Arbeit miteinbezogen, sie dienen lediglich der Erkennung bestehender praktischer Probleme, auf die ein besonderes Augenmerk zu richten sein wird. Zu diesem Zweck wird der Dialog mit Polizeiinspektionen der Landespolizeidirektionen Wien und Niederösterreich, dem Bundeskriminalamt – in concreto dem Cybercrime Competence Center C^4 – der Staatsanwaltschaft Wien und der Strafverteidigung angestrebt. Zum Zweck der Erforschung anderer strafprozessualer Ermittlungstatbestände soll der Rechtvergleich mit Deutschland und der Schweiz durchgeführt werden.

Vorläufiger Arbeitsplan

WiSe 2019/20	Recherche
	Erarbeitung Exposé
SoSe 2020	Teilnahme an Lehrveranstaltungen für DissertantInnen
	Fakultätsöffentliche Präsentation des Dissertationsvorhabens
	Einreichung Exposé
	Vorfeldgespräche Teil I
WiSe 2020/21	Vorfeldgespräche Teil II
	Verfassen des Ersten Teiles
SoSe 2021	Verfassen des Zweiten Teiles Erstellen der Rohfassung
Wise 2022/23	Überarbeitung
	Einreichung
SoSe 2023	Defensio

Vorläufiges Literaturverzeichnis

Bertel/Venier Strafprozessordnung Jan Sramek 2012.

Bertel/Venier/Tipold, Strafprozessrecht[13], Manz 2020.

Birklbauer in *Fuchs/Ratz*, WK StPO §§ 118ff (Stand 1.6.2010, rdb.at).

Birklbauer in *Fuchs/Ratz*, WK StPO Vor §§ 118–124 (Stand 1.6.2010, rdb.at).

Birklbauer/Haumer/Nimmervoll/Wess Linzer Kommentar zur Strafprozessordnung; Verlag Österreich 2020.

Birklbauer; Tipold/Zerbes in *Fuchs/Ratz*, WK StPO § 117 (Stand 1.6.2010, rdb.at).

Bruns, KK-StPO[8], StPO §§ 100aff, 2019.

Fabrizy, StPO[13] Kurzkommentar, Manz 2017.

Fink, Der "Bundestrojaner" ist (hoffentlich) endlich Geschichte, AnwBl 2020/32.

Flora in *Fuchs/Ratz,* WK StPO § 116 (Stand 1.10.2018, rdb.at).

Gorzala, Online-Identifikation von Bankkunden, ÖBA 2019, 120.

Hauck in *Löwe-Rosenberg*, StPO[26] 3 §§ 100aff De Gruyter 2013.

Hinterhofer/Oshidari, System des österreichischen Strafverfahrens (2017) (Stand 1.3.2017, rdb.at).

Hinterhofer/Oshidari, System des österreichischen Strafverfahrens Manz 2017.

Kroschl in *Schmölzer/Mühlbacher* StPO 1 §§ 110ff.

Menges in *Löwe-Rosenberg,* StPO[26] 3 §§ 94ff De Gruyter 2013.

Meyer-Goßner/Schmitt Strafprozessordnung[63], § 110, C. H. Beck 2017.

Ohrnhofer in *Schmölzer/Mühlbacher* StPO 2 §§ 134ff.

Proschofsky, „'Stopp Corona'-App: Was hast das Rote Kreuz bloß falsch gemacht" in Der Standard, 11.07.2020, https://www.derstandard.at/story/2000118645764/stopp-corona-app-was-hat-das-rote-kreuz-bloss-falsch (zugegriffen am 14.07.2020).

Reindl-Krauskopf in *Fuchs/Ratz,* §§ 144ff (Stand 1.11.2019).

Reindl-Krauskopf in *Fuchs/Ratz*, WK StPO § 136 (Stand 1.4.2016, rdb.at).

Reindl-Krauskopf in *Fuchs/Ratz*, WK StPO §§ 137ff (Stand 1.11.2019, rdb.at).

Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht Manz 2018.

Reindl-Krauskopf; Tipold/Zerbes in *Fuchs/Ratz* WK StPO §§ 134ff (Stand 1.4.2016).

Rohregger, Kollateralschäden im Strafverfahren - Was darf der Staat dem Beschuldigten zumuten?, JBl 2017, 219.

Seiler, Strafprozessrecht[18] 2020.

Tipold/*Zerbes* in *Fuchs*/*Ratz*, WK StPO §§ 119ff (Stand 1.4.2010, rdb.at).

Tipold/*Zerbes* in *Fuchs*/*Ratz*, WK StPO §§ 110ff (Stand 1.11.2015, rdb.at).

Tipold/*Zerbes* in *Fuchs*/*Ratz*, WK StPO Vor §§ 119–122 (Stand 1.4.2010, rdb.at).

Tipold/*Zerbes in Fuchs*/*Ratz*, WK StPO Vor §§ 110–115 (Stand 1.11.2015, rdb.at).

Tipold/*Zerbes; Flora* in *Fuchs*/*Ratz*, WK StPO § 109 (Stand 13.11.2017, rdb.at).

VfGH 11. 12. 2019, G 72-74/2018-48, G 181-182/2019-18.

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (Anhänge) - Allgemeine Ausrichtung (Ergänzung), Ratsdok. 9365/19 vom 17.05.2019, https://db.eurocrim.org/db/de/vorgang/380/ (Zugriff am 14.07.2020).

Wolter, Systematischer Kommentar zur Strafprozessordnung[5], Heymanns, Carl 2017.

Zerbes, Spitzeln, Spähen, Spionieren. Sprengung strafprozessualer Grenzen durch geheime Zugriffe auf Kommunikation, Springer Wien 2010.

Zerbes/*El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, 432.