House Searches and Seizures in Criminal Proceedings:

The Perspective of an Effective Protection of Fundamental Rights with a Focus on Mobile Devices and Data

Günther Schaunig*

Contents

* Postdoctoral researcher (University of Liechtenstein, Liechtenstein Business Law School, Professorship of Economic Criminal Law, Compliance and Digitalization) and tax associate (KPMG Austria). Contact: guenther.schaunig@uni.li, gschaunig@kpmg.at.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

I. Introduction

Criminal procedural law aims to clarify criminal offences in the sense of investigating the material truth. Law enforcement authorities need evidence for this purpose. This evidence increasingly comes from the digital world, in particular from mobile devices. The main way for authorities to obtain this evidence is through house searches. Thus, this article focuses firstly on house searches and secondly on seizures and confiscations of mobile devices under Austrian law.[1]

Major criminal proceedings and in particular white-collar criminal proceedings are hardly conceivable without utilising evidence from the world of big data. Consider two examples from a national and an international perspective:

From a national perspective, a first example is the "raid" at the Austrian Federal Office for the Protection of the Constitution and Counterterrorism in 2018, which attracted attention internationally.[2] The discussion triggered by the search measures in this office about the permissibility of searches and seizures in the public sector and the associated access to sensitive documents even led to an amendment of the Austrian Code of Criminal Procedure (*Strafprozeßordnung 1975* in the current version, subsequently StPO).[3] At the Austrian Federal Office for the Protection of

[1] In general Höcher, 'Gedanken zur Sicherstellung von Mobiltelefonen', in Dietrich/Glaser/Kert/Tipold (eds.), *Festschrift Wolfgang Brandstetter* (Vienna, 2022) 419; cf. on criminal tax law e.g. Köck, 'Die Sicherstellung von Krypto-Assets im Finanzstrafverfahren' (2023) *ZWF* 84; Hribernigg/Weber, 'Steuerfahndung und Hausdurchsuchung', in Gröhs/Kotschnigg (eds.), *Finanzstrafrecht in der Praxis – Band 2* (Vienna, 2008) 65.

[2] Report of the Committee of Inquiry into Political Influence on the Federal Office for the Protection of the Constitution and Counterterrorism (*Bericht des Untersuchungsausschusses betreffend die politische Einflussnahme auf das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, 2019) 167. The Federal Office for the Protection of the Constitution and Counterterrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*) was replaced by the Directorate for State Protection and Intelligence (*Direktion Staatsschutz und Nachrichtendienst*).

[3] Ifsits, 'Zum strafprozessualen Schutz klassifizierter Informationen nach § 112a StPO' (2023) *ÖJZ* 220; see also Tipold, 'Hausdurchsuchung oder Amtshilfe – Das ist hier die Frage!' (2021) *JSt* 225; Tipold,

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

the Constitution and Counterterrorism extensive seizures were made; the Higher Regional Court (*Oberlandesgericht*, subsequently OLG) ultimately ruled that most of the searches were unlawful.[4] The Austrian Central Public Prosecutor's Office for Combating Economic Crime and Corruption (*Zentrale Staatsanwaltschaft zur Verfolgung von Wirtschaftsstrafsachen und Korruption*) brought charges against the defendants. During the trial, the defence accused the public prosecutor's office of bringing charges against the former head of espionage not based on "incidental findings" made during the search at the time. The defence alleged that the prosecution had deliberately searched for evidence (fishing expeditions, *Beweisausforschung*). All of the defendants were acquitted.[5] They were subjected to years of psychological and financial strain as a result of the criminal proceedings.[6] Similar problems exist in connection with the so-called "Casinos Case" (*Casinos-Akt*), which consolidated multiple corruption proceedings in the Republic of Austria (keyword: "chats" by politicians).[7]

From an international perspective, a second example is the notable EncroChat case. This investigation into 32,477 mobile phones has led to a debate over whether data intercepted in France can be used as evidence in German criminal proceedings; in

'Hausdurchsuchung oder Amtshilfe – was für eine Frage? Hausdurchsuchung!' (2021) *JSt* 461.

[4] Report of the Committee of Inquiry into Political Influence on the Federal Office for the Protection of the Constitution and Counterterrorism (2019) 91 ff, 179 ff.

[5] Cf. unknown author, 'Freisprüche im Prozess gegen Ex-BVT-Spionagechef' (*Der Standard*, 3 March 2022) https://www.derstandard.at/story/2000133817835/freisprueche-im-prozess-gegen-ex-bvt-spionagechef, accessed 18 February 2025; on the difficult concept of accidental findings Bauer, *Verwertungsverbote zur Gewährleistung von Waffengleichheit* (Vienna, 2015) 116 ff; Tomaš, 'Strafprozessuale Beweisverwertung nach rechtswidriger Durchsuchung' (2024) *ÖJZ* 928; see also point IV.

[6] Cf. on this problem Rohregger, 'Kollateralschäden im Strafverfahren – Was darf der Staat dem Beschuldigten zumuten?' (2017) *JBl* 219.

[7] Cf. on the Casinos Act e.g. Graber/Schmid, 'WKStA will neue "hochrelevante Beweise" für blauen Casinos-Deal gefunden haben' (*Der Standard*, 29 April 2023) https://www.derstandard.at/story/2000145978761/wksta-will-neue-hochrelevante-beweise-fuer-blauen-casinos-deal-gefunden, accessed 18 February 2025; cf. on chats e.g. Hagen/Marchart/Schmid, 'Welche Chats die heimische Politik erschüttern' (*Der Standard*, 2 March 2022) https://www.derstandard.at/story/2000133753280/welche-chats-die-heimische-politik-erschuettern, accessed 18 February 2025; cf. Kert/Schroll, 'Die Kronzeugenregelung und ihre Grenzen' (2022) *ZWF* 166. The authors of the last mentioned article expressly mention the name of the accused. This is remarkable from the perspective of the personal rights of the accused. In addition, the investigation proceedings are not public (Section 12 (1) StPO). This should not be done in future. Too many aspects – including those from the private lives of the accused – are already public anyway; cf. the convincing problem statement by Brandstetter/Zöchbauer, 'Grundrechtsverwirrung oder Grundrechtserosion?' (2022) *MR* 3.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

addition to questions of European mutual legal assistance, fundamental questions of criminal procedure, data protection and constitutional law arise.[8]

Recently, the Austrian Bar Association (chamber of attorneys, *Österreichischer Rechtsanwaltskammertag*) called for a reform of criminal procedural standards regarding the seizure and analysis of data and data carriers on the basis of an expert opinion.[9] This expert opinion saw an "imbalance at the expense of the defence, which is not granted a legal hearing in the evaluation process of sometimes enormous amounts of data."[10]

In its ruling of 14 December 2023, G 352/2021, the Austrian Constitutional Court (*Verfassungsgerichtshof*, subsequently VfGH) repealed key provisions on seizure in the StPO, including the central legal basis (Section 110 (1) no. 1 StPO). The VfGH concluded that the seizure of mobile phones and mobile data carriers in criminal proceedings without prior judicial authorisation is unconstitutional.[11] The provisions repealed by the VfGH were Section 110 (1) no. 1 , Section 110 (4) and Section 111 (2) StPO. The legislator recently passed a comprehensive reform of the StPO

[8] Schmidt, 'Zur strafprozessualen Verwertbarkeit der Daten aus der Überwachung verschlüsselter Mobiltelefone durch einen anderen Mitgliedstaat der EU' (2022) *ZStW* 982 (982 f); see also Papathanasiou, 'EncroChat – das "WhatsApp der Kriminellen" und seine strafverfahrensrechtliche Relevanz' (2022) *ZJS* 259; CJEU Case C-670/22 *Staatsanwaltschaft Berlin/M.N.*, 30 April 2024, ECLI:EU:C:2024:372. Decisions of the CJEU can be accessed via https://curia.europa.eu/juris with their ECLI, case number or party names; for a similar case in Austria see Austrian OGH 24 May 2023, 15 Os 13/23k; Schmoller, 'Ergebnisse einer von einer ausländischen Behörde durchgeführten Überwachungsmaßnahme – Verwendungsverbot?' (2023) *JBl* 739; Caspar-Bures, 'Ein rechtsstaatliches Strafverfahren verlangt eindeutig rechtskonforme Beweismittel' (2024) *JSt* 445.

[9] Cf. Dworzak/Hruschka, 'ÖRAK fordert tiefgreifende Reformen bei der Sicherstellung und Auswertung von Daten und Datenträgern' (2023) *AnwBl* 61; see also Brandstetter/Zöchbauer, (2022) *MR* 3.

[10] Zerbes/Ghazanfari, 'Stellungnahme im Auftrag des Instituts für Anwaltsrecht der Universität Wien zur Sicherstellung und Auswertung von Daten und Datenträgern' (2022) *AnwBl* 640 (640, in the original with emphasis in bold); see also Zerbes/Ghazanfari, 'Sicherstellung und Verwertung von Handy-Daten – Reformperspektiven' (2023) *AnwBl* 559.

[11] Cf. from the most recent literature Rohregger, 'VfGH: Handysicherstellung verfassungswidrig' (2024) *ZWF* 2; Reindl-Krauskopf, 'Verfassungswidrigkeit von Bestimmungen der StPO über die Sicherstellung von Gegenständen (wie Datenträgern) aus Beweisgründen' (2024) *JBl* 166; Schumann, 'Datenschutz im Informationszeitalter – Verfassungswidrigkeit der StPO in Betreff der Sicherstellung von Mobiltelefonen' (2024) *ÖJZ* 471; Schumann, '"Sicherstellung von Daten neu" – Reparatur oder (R)evolution?' (2024) *ÖJZ* 675; Soyer/Marsch, 'VfGH zur Handysicherstellung. Eigentlich: VfGH zur Sicherstellung von Daten(-trägern) und IT-Endgeräten. Parallel: VfGH zum doppelten Rechtsschutz im Ermittlungsverfahren' (2024) *JSt* 118; Soyer/Marsch, 'VfGH und Handysicherstellung – technische und rechtliche Fragen aus dem Verfahren' (2024) *AnwBl* 164; Schönborn/Thiel, 'Verhältnismäßigkeit und Datenschutz bei der Sicherstellung von Daten(trägern)' (2024) *ZWF* 139; all decisions of the Austrian Constitutional Court can be accessed via http://ris.bka.gv.at/Judikatur/ with their case number.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

(*Strafprozessrechtsänderungsgesetz 2024*).[12] In this way, the legislature aims to enact provisions that meet the constitutional requirements.

This article is based on the framework of criminal procedural law and constitutional law.[13] In accordance with the case law of the European Court of Human Rights (subsequently the Court and in footnotes ECtHR) and the VfGH, it examines the golden mean of the rule of law between the poles of effective prosecution of crimes on the one hand and the rights of the accused on the other. In contrast to the pre-digital era (copies of paper records, small amounts of data), the accused themselves often do not know what is contained in the seized chat messages. This is problematic from the point of view of equality of arms and proportionality (Art 6, Art 8 European Convention on Human Rights, subsequently ECHR).

House searches are one of the most practically significant and effective measures for prosecuting and investigating criminal offences, they are part of the core set of criminal investigation instruments and are intended to ensure the effective administration of criminal justice in accordance with the rule of law; they are not a secret but rather an open investigative measure.[14] The latter also applies to seizures (*Sicherstellung*, Section 109 no. 1 StPO), confiscations (*Beschlagnahme*, Section 109 no. 2 StPO) and confiscation of data carriers and data (*Beschlagnahme von Datenträgern und Daten*, Section 109 no. 2a StPO). The following analysis of the problem therefore deals with the legal basis for accessing existing and "static" data, data carriers and data storage devices and does not address secret investigative

[12] Federal Law Gazette I 2024/157.

[13] Union law is not included in this article; see current Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the enforcement of custodial sentences following criminal proceedings; see Böse, 'Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel' (2022) *ZWF* 9; Herrnfeld, 'Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel' (2022) *ZWF* 2; Kynast, 'Verordnung zu elektronischen Beweismitteln in Strafsachen' (2023) *AnwBl* 479; recently CJEU Case C-548/21 *Bezirkshauptmannschaft Landeck/C.G.*, 4 October 2024, ECLI:EU:C:2024:830; see also Menhofer, 'EuGH steckt rechtlichen Rahmen für Zugriff auf Handy-Daten ab' (2024) *SWK* 1242; Glaser/Kert, 'EuGH: Anforderungen an die Sicherstellung von Mobiltelefonen' (2024) *ZWF* 288. In terms of content, the CJEU clarifies the fundamental rights parameters set by the VfGH in its ruling of 14 December 2023, G 352/2021.

[14] Applicable to Austria from the German literature Kroll, *Kernbereichsschutz bei Durchsuchungen* (Tübingen, 2021) 1 with further references. According to Kroll's convincing conclusion (ibid 163 with further references), a functioning criminal justice system does not require truth-seeking at any price, but rather a criminal procedure law that is orientated towards human dignity and civil liberties.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

measures (e.g. surveillance of telecommunications, online searches or data in online clouds).[15]

Firstly, the article outlines the problems it will consider (point II). The article then examines the fundamental rights framework regarding house searches (Art 8 ECHR, point III) and seizures (Art 6 ECHR, point IV). It subsequently examines how the Austrian legal situation, which is also characterised by the jurisprudence of the criminal justice system (Austrian Supreme Court, *Oberster Gerichtshof*, subsequently OGH; also OLG), is to be assessed in relation to the requirements of the jurisprudence of the Court and VfGH.

This article is neither a legal analysis nor an expression of opinion on the lex lata or the lex ferenda. Rather, it is a preparation of the framework of fundamental rights, supported by an analysis of case law, which is intended to support further work in connection with – current or future – legal provisions of all stakeholders. The main part of the article provides a benchmark for the assessment of the legal situation applicable prior to 1 January 2025 (points III to VII). The standards developed in this main part also apply – mutatis mutandis – as an aid to interpretation in light of the new legal situation as of 1 January 2025 (*Strafprozessrechtsänderungsgesetz 2024*). Consequently, in the last point, the article examines the innovative legislative cornerstones as well as the fundamental rights safeguards of this new legal situation (point VIII).

While the VfGH based its reasoning in its decision of 14 December 2023, G 352/2021, regarding seizure (point IV) on Art 8 ECHR and the fundamental right to data protection pursuant to Section 1 (1) Data Protection Act (*Datenschutzgesetz*, subsequently DSG), this article focuses on Art 6 ECHR and thus expands the spectrum of legal assessment. As the VfGH also deemed the current legal situation unconstitutional due to a lack of legal protection,[16] the article proposes specific

[15] Jahn/Brodowski, 'Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision', in Hoven/Kudlich (eds.), *Digitalisierung und Strafverfahren* (Baden-Baden, 2020) 67 (72 ff.), also takes this approach from the German literature. Online searches "light", which involve using a notebook found at the search location to access data via the internet that the defendant has stored on a cloud storage space, are also not dealt with; see Kroll, *Kernbereichschutz bei Durchsuchungen* 2, 66 ff with further references; see also Ghazanfari, 'Zu den Anforderungen an die Überwachung von (moderner) interpersoneller Kommunikation' (2024) *JSt* 459.

[16] Para. 83: "The contested provisions also violate § 1 (2) DSG in conjunction with Art. 8 (2) ECHR for another reason. The StPO of 1975 does not guarantee that those affected by the seizure of data carriers have adequate legal protection during the investigation proceedings and in the subsequent (main) proceedings."

requests that defendants can make in the context of criminal proceedings to safeguard their rights under criminal procedure and fundamental rights (points VI and VII).

II. Subject of the Study

A. General Information

Imagine the police and the public prosecutor are at your door and want to conduct a house search. In practice, the house is being searched – whether it is legally compliant is of secondary importance.[17]

Imagine the police and the public prosecutor want to seize your mobile phone and all the data stored on it. In practice, they usually simply take everything.[18] Even if a house search in, for example, criminal tax proceedings is not legally compliant, the evidence obtained is typically still utilised in tax proceedings.

Deciding which documents are relevant (see point VI.A for more details) is much more difficult when seizing data carriers than when seizing paper documents for reasons of quantity; this also results in the practice of seizing data carriers in their entirety and then filtering out the relevant data.[19]

Quite simply, the accused has the short end of the stick. Subsequent remediation of unlawful investigative measures – in particular a house search – is not possible. From a fundamental rights perspective, at most a determination of the violation would be possible, either by the Court or the OGH.[20]

Pursuant to Section 117 (2) StPO, the search of places and objects is the search of a property, room, vehicle or container that is not generally accessible (lit a) or of a

[17] On the problem from the perspective of the author's own practical experience Premissl, *Strafrechtsschutz und Grundrechte* (Vienna, 2008) passim; on the problem of the gap between theory and practice Miklau/Szymanski, 'Strafverfahrensreform und Sicherheitsbehörden – eine Nahtstelle zwischen Justiz- und Verwaltungsrecht', in Melnizky/Müller (eds.), *Strafrecht, Strafprozeßrecht und Kriminologie – Festschrift Franz Pallin* (Vienna, 1989) 249 (253 ff); Tipold, 'Gilt die StPO im strafrechtlichen Ermittlungsverfahren?' in Dietrich/Glaser/Kert/Tipold (eds.), *Festschrift Wolfgang Brandstetter* (Vienna, 2022) 389.

[18] Information from a former employee of a criminal investigation authority who wishes to remain anonymous.

[19] Schönbauer, 'Technisch-organisatorische Aspekte bei der Sicherstellung von Daten und Datenträgern' (2023) *AnwBl* 42 (43).

[20] Cf. on the extended application for renewal of the criminal proceedings by the OGH (Section 363a StPO per analogiam) Flora, 'Section 363a', in Bertel/Venier (eds.), *StPO – Strafprozessordnung, Band II* (Vienna, 2020) para. 8.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

dwelling or another place protected by domestic authority and objects located therein (lit b).

Roughly summarised, the provisions on seizure encompass the authority to seize data carriers in order to subsequently examine data and information.[21] The central legal basis is usually seizure for reasons of evidence (Section 110 (1) no. 1 StPO). The necessity for evidentiary purposes and relevance as evidence is sufficient for a seizure.[22]

Seizure is the temporary establishment of the power of disposal over objects (*Sicherstellung*, Section 109 no. 1 lit a StPO). Seizure is admissible if it appears necessary for reasons of evidence. With regard to data, however, this only applies to the extent that it concerns selective data or data recorded by means of recording devices in public or publicly accessible places (Section 110 (1) no. 1 StPO). Confiscation is a court decision to establish or continue a seizure (*Beschlagnahme*, Section 109 no. 2 StPO). Confiscation of data carriers and data is a court decision to establish a seizure order concerning data carriers and data as well as various other categories (*Beschlagnahme von Datenträgern und Daten*, Section 109 no. 2a StPO). This article uses the term seizure as an umbrella term to describe a justification of the power of disposal over objects, data and data carriers.[23]

Searches of places are permissible if there is a factual basis to assume that objects or evidence are located there that are to be seized or analysed (Section 119 (1) StPO). Searches of places and objects must be ordered by the public prosecutor's office with court approval; in the event of imminent danger, investigators are entitled to carry out these searches provisionally without an order or authorisation (Section 120 (1) StPO).

B. House Search

If a house search is legally compliant, the rest of the proceedings are also unencumbered per se if no other legal violations or violations of fundamental rights occur during the proceedings. The situation is different if a house search is unlawful: the violation of law can then no longer be remedied. The entire procedure is infected.

---

[21] Ghazanfari, 'Bekanntgabe des PUK-Codes und Duplizierung einer SIM-Karte – Sicherstellung?' (2021) *JBl* 740 (744).

[22] Tipold/Zerbes, 'Section 110', in Fuchs/Ratz (eds.), *Wiener Kommentar StPO* (Vienna, 2021) para. 5.

[23] To the extent that the legal distinction between seizure, confiscation and confiscation of data carriers and data is addressed in the specific sense, reference is made to it in the respective context.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

On the basis of a single instance of unlawful and excessive behaviour, criminal proceedings are initiated with all the accompanying consequences.

Paulitsch summarises the situation as follows: an official house search is a coercive measure that interferes with fundamental rights and must therefore fulfil strict legal requirements. So much for the theory. In practice, searches can usually neither be prevented nor stopped by those affected. The authorities refer them to legal remedies. It is true that courts often rule in retrospect that searches were unlawful. However, those affected who expect compensation for unlawful actions are usually disappointed. Official liability claims are extremely difficult to enforce and are associated with a high litigation risk. The affected party's fundamental rights are violated, but their damage usually remains unredressed. What remains are feelings of powerlessness and the impression of being at the mercy of the arbitrary behaviour of the authorities.[24]

However, this outline of the problem does not even point out that unlawful house searches do not entail any prohibitions on the utilisation of evidence, not even for incidental findings; apart from the possibility of a lighter sentence on a subsequently convicted defendant affected by an unlawful house search, few remedies can be expected on appeal.[25]

In connection with the seizure of mobile devices, there were no effective prohibitions on the utilisation of evidence prior to 2025.[26] If data carriers are searched for evidence of the commission of a criminal offence other than the one that gave rise to the seizure of the data carrier, this is a violation of Section 5 (1) first sentence StPO (principle of legality),[27] which addresses the problem of fishing expeditions (see also point IV). However, it is hardly possible in practice for the person concerned to prove the

[24] Paulitsch, 'Einleitung', in Paulitsch (ed.), *Praxishandbuch Hausdurchsuchung,* 2nd edn. (Vienna, 2023) 1.

[25] Vogl, 'Review of Paulitsch (ed.): Praxishandbuch Hausdurchsuchung' (2018) *JSt* 441 (442).

[26] Austrian OGH 2 July 1992, 15 Os 3/92; all decisions of the Austrian OGH can be accessed via http://ris.bka.gv.at/Judikatur/ with their case number; Ruhri, 'Grenzen der Verwendung und Verwertung von Verfahrensergebnissen in Strafverfahren und Urteil in Österreich' (2020) *AnwBl* 23 (25 f); see also Bauer, *Verwertungsverbote zur Gewährleistung von Waffengleichheit* 159 ff; Murschetz, *Verwertungsverbote bei Zwangsmaßnahmen gegen den Beschuldigten* (Vienna, 1999) 141 ff; from the German literature Warnking, *Strafprozessuale Beweisverbote in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und ihre Auswirkungen auf das deutsche Recht* (Frankfurt am Main, 2009) 279 ff; on the problem already Schmoller, 'Heimliche Tonbandaufnahmen als Beweismittel im Strafprozeß?' (1994) *JBl* 153.

[27] Ratz, 'Beweiswürdigung im Ermittlungsakt und Sicherstellung ohne Kriminalpolizei und durch Sachverständige' (2022) *ÖJZ* 58 (65).

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

violation of the law. The *Strafprozessrechtsänderungsgesetz 2024* has established new rules. Results of an evaluation may only be used as evidence if the investigative measure was lawfully ordered and authorised; otherwise the measure is null and void. If the evaluation of data reveals evidence of a criminal offence other than the one that gave rise to the seizure of data carriers and data, a separate file must be created, insofar as its use as evidence is admissible (Section 115j StPO). The order that a separate file is to be created follows the already existing basic system of the StPO (Section 122 (2), Section 140 (2) StPO). This means that the same technical procedure applies to data as to objects.

C. Seizure

Höcher summarises the pre-2025 legal situation as follows: as a rule, the seizure of a mobile phone takes place as a provisional justification of the power of disposal over objects for reasons of evidence. In this case, the seizure is generally ordered by the public prosecutor's office without court authorisation and carried out by the criminal investigation department. However, the reason why seizures of mobile phones are very often associated with court authorisations is that such seizures often take place as part of house searches, which in turn require court approval (Section 120 (1) StPO). A mobile phone is generally reduced to its function as a data carrier because it is not the mobile phone itself but the data it contains that is of interest to the law enforcement authorities. Electronic data are regarded as immaterial objects and require material embodiment for their existence; this material embodiment is the mobile phone as a data carrier. In this respect, a mobile phone is equivalent to a hard drive, a USB stick, a CD, etc. In *theory,* mobile devices will be seized in accordance with the following procedure: a person's mobile phone is taken from them and a copy of the information/data required for the criminal proceedings is made. The person then receives the mobile phone back together with a confirmation of the seizure showing which data was copied. An objection (Section 106 StPO) can be lodged against the seizure of this data on the grounds of an infringement of the law, and legal protection is guaranteed. However, this theoretical procedure is rarely invoked for various reasons.[28]

According to the OGH, "investigation files are not factual, but legally determined".[29] What this means in practice is not immediately apparent to the average practitioner (see points VI and VII). The cited case law of the OGH concerns data material that has been seized for evidentiary purposes and has not yet been analysed; only the

[28] Höcher, 'Gedanken zur Sicherstellung', 419 (420 f).

[29] Austrian OGH 1 June 2021, 14 Os 35/21k.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

assessment as information relevant to evidence concerning substantial facts also leads to, according to this position, accessibility by way of inspection of the file in accordance with Section 53 (1) StPO.[30] In other words, not everything that comes to the attention of the public prosecutor's office or the financial criminal authority may be included in the file; according to parts of the case law, documents and data that have been seized but not yet analysed, not yet recognised as significant or relevant to the proceedings and therefore not included in the file in written or electronic form are not subject to file inspection.[31] The expert opinion cited at the beginning of point I recently called for "transparency towards the accused", in particular because an enormous surplus of data is seized from a smartphone or other communication device. The law enforcement authorities – according to the proposal for an amendment to the law – should, for example, create a separate file for incidental findings.[32]

The *Strafprozessrechtsänderungsgesetz 2024* has established new rules: a judicial authorisation is now required for the confiscation of data carriers and data. This authorisation specifies which categories of data and data content may be seized and for what period of time (Section 115f (3) StPO).

III. Fundamental Rights Framework for House Searches (Art 8 ECHR)

Art 8 (1) and (2) ECHR states: "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[30] Ainedter/Poppenwimmer, 'Persönlichkeitsschutz und Akteneinsicht von (Mit-)Beschuldigten' (2023) *ZWF* 61 (66).

[31] See Köck, 'Verbandsverantwortlichkeit und Akteneinsicht im gerichtlichen und verwaltungsbehördlichen Finanzstrafverfahren', in Achatz/Brandl/Kert (eds.), *Festschrift Roman Leitner – Steuerrecht – Finanzstrafrecht – Wirtschaftsstrafrecht* (Vienna, 2022) 317 (321 f with reference to OGH 1 June 2021, 14 Os 35/21k). However, the author does not mention any alternative opinions that take a different position; cf. point VII.A.

[32] Zerbes/Ghazanfari, (2022) *AnwBl* 640 (649).

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

The following principles, which also represent a review structure, can be derived from the case law of the Court for house searches:[33]

First step: Interference with Art 8 ECHR

It must be examined whether an individual's rights to respect for their private life, home and correspondence have been violated both by (i) the search order (and usually combined with seizure) as such and by (ii) the manner in which it was carried out. In the case of house searches, the Court generally first establishes an interference.[34] It takes into account all the circumstances of the individual case.[35]

Second step: Compliance with legal and foreseeable standards and legitimate aim of the interference

In particularly serious cases, a violation of Art 8 ECHR already occurs at this level. Art 8 ECHR requires the law in question to be compatible with the rule of law. In the context of searches and seizures, domestic law must provide some protection to the individual against arbitrary interference. Thus, domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such measures. Search represents a serious interference with private life, home and correspondence and accordingly must be based on precise legal provisions. It is essential to have clear, detailed rules on the subject.[36] In this context, it must be examined whether, due to the ineffectiveness and unpredictability of legal protection by the courts, there was ultimately no legal basis for the interference.[37]

---

[33] Summarising the catalogue of criteria, see also Ranzoni, 'Aktuelle Fragen in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte' (2018) *LJZ* 114 (117 f). In addition to Art 8 ECHR, there are other relevant provisions in Austria, see Austrian VfGH 11 December 2019, G 72/2019 ua, VfSlg 20.356/2019: According to Article 9 of the Law on the General Rights of Citizens (*Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger*), the right of domicile is inviolable. In addition, the Law for the protection of domiciliary rights (*Gesetz vom 27. October 1862, zum Schutze des Hausrechtes*) is part of the Law on the General Rights of Citizens and has constitutional status.

[34] From the numerous cases, e.g. *Posevini v Bulgaria* App no 63638/14 (ECtHR, 19 January 2017), para. 65; all decisions of the ECtHR can be accessed via https://hudoc.echr.coe.int/eng with their case number or party names.

[35] *Vinks and Others v Latvia* App no 28926/10 (ECtHR, 30 January 2020), para. 118.

[36] *Sallinen and Others v Finland* App no 50882/99 (ECtHR, 27 September 2005), paras. 82, 90.

[37] *Prezhdarovi v Bulgaria* App no 8429/05 (ECtHR, 30 September 2014), paras. 50 f; *Sallinen and Others v Finland* App no 50882/99 (ECtHR, 27 September 2005), para. 92; *Heino v Finland* App no 56720/09 (ECtHR, 15 February 2011), para. 46.

It is furthermore required to examine whether the measure pursued legitimate aims (Art 8 (2) ECHR). A search is not necessary in a democratic society if carried out without relevant and sufficient grounds and in the absence of safeguards that would confine the impact of the measure within reasonable bounds.[38]

In the vast majority of cases, there is a legal basis for the intervention. According to Austrian law, this would formally be the StPO. However, the Court understands this criterion not only formally, but also includes the case law of national courts.[39]

Third step: Necessity in a democratic society and proportionality

Assuming that the Court concludes that there is a legal basis and a legitimate aim, the proportionality of the aim with regard to the means would have to be analysed.[40] It must be examined whether (i) the search and seizure order as such and (ii) the manner in which it was carried out were proportionate. The Court examines this on two levels.[41]

Firstly, the proportionality of the search as such: the Court considers whether national law and enforcement practice provide adequate and effective safeguards against abuse or arbitrariness. Central to the analysis is whether the search warrant (i) was issued by a judge, (ii) was based on reasonable suspicion and (iii) was reasonably limited in scope.[42]

Judicial authorisation and effective procedural safeguards: the mere fact of judicial review is not in itself sufficient protection against abuse and arbitrariness.[43] In principle, the Court weights judicial review ex post positively. However, even this subsequent review is not a compelling justification for coercive measures that are intrusive in the sense of a self-serving purpose.[44]

[38] *Misan v Russia* App no 4261/04 (ECtHR, 2 October 2014), para. 63.

[39] *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), paras. 40 f.

[40] *Cacuci and Others v Romania* App no 27153/07 (ECtHR, 17 January 2017), para. 91.

[41] *Cacuci and Others v Romania* App no 27153/07 (ECtHR, 17 January 2017), paras. 92, 95, 104.

[42] *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), para. 44.

[43] *Stefanov v Bulgaria* App no 65755/01 (ECtHR, 22 May 2008), para. 39; *Cacuci and Others v Romania* App no 27153/07 (ECtHR, 17 January 2017), para. 92.

[44] *Prezhdarovi v Bulgaria* App no 8429/05 (ECtHR, 30 September 2014), para. 49; *Vinks and Others v Latvia* App no 28926/10 (ECtHR, 30 January 2020), para. 115.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

Reasonable suspicion: reasonable suspicion must be examined ex ante at the time the search warrant is issued.[45] The grounds must be substantial and sufficient.[46] A prosecutor's order drafted in broad terms was not sufficient in the Court's view. In this particular case, the search order did not give any consideration to why the suspect could have been regarded to be in possession of the material in question and why there had been a need to search for it. There was no reference to any material evidence except for information allegedly received by the police.[47]

Reasonable limitation of scope: the scope of the search must be reasonably limited.[48] If the search warrant is formulated in very general terms and allows practically unlimited searches and seizures of objects and data, the Court denies a reasonable limitation.[49] Such a scope would only be permitted in cases of suspected serious criminality (terrorism).[50] The Court weights the unnecessary seizure of private data negatively.[51] In case of electronic devices, there is a higher standard of protection against overreach.[52] The scope of the order must not be overreaching and must be limited to what is necessary in view of the circumstances.[53]

If there is no reasonable limitation on the scope of the search warrant, the Court examines whether these deficiencies could be covered by sufficient procedural safeguards and whether these safeguards were suitable to protect the person concerned from abuse and arbitrariness. The Court weights the inadequate issuing of a report negatively.[54] The Court attaches particular importance to the manner in which judicial review bodies conduct their review. It is disproportionate if the reviewing court only gives very brief and general reasons for authorising the use of all electronic data, does not go into the scope and does not give reasons why the search

[45] *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), para. 46.

[46] *Smirnov v Russia* App no 71362/01 (ECtHR, 7 June 2007), para. 47; *Misan v Russia* App no 4261/04 (ECtHR, 2 October 2014), paras. 56 ff.

[47] *Dorož v Poland* App no 71205/11 (ECtHR, 29 October 2020), para. 27.

[48] *Stefanov v Bulgaria* App no 65755/01 (ECtHR, 22 May 2008), para. 41.

[49] *Roemen and Others v Luxembourg* App no 51772/99 (ECtHR, 25 February 2003), para. 70; *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), para. 47; *Stefanov v Bulgaria* App no 65755/01 (ECtHR, 22 May 2008), paras. 41 f.

[50] *Sher and Others v United Kingdom* App no 5201/11 (ECtHR, 20 October 2015), para. 174.

[51] *Prezhdarovi v Bulgaria* App no 8429/05 (ECtHR, 30 September 2014), para. 49.

[52] *Sher and Others v United Kingdom* App no 5201/11 (ECtHR, 20 October 2015), para. 174.

[53] *Buck v Germany* App no 41604/98 (ECtHR, 28 April 2005), para. 50.

[54] *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), paras. 47 ff.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

of all documents was necessary.[55] If the judge does not even superficially examine the search order, this in fact approaches the absence of a judicial review ex ante, which the Court weights particularly negatively.[56] If, in addition, the economic and social existence of the person concerned is destroyed by the measures due to the loss of employment and reputation, the Court weights this negatively.[57]

Secondly, the method of execution: the Court also examines the method of execution of the search.[58] Failure to provide confirmation of the search in the home and its results within 24 hours would be a violation of the right under Section 122 (3) StPO. The Court weights such violations negatively.[59]

IV. Fundamental Rights Framework for Seizure, Access to Files and Evaluation of Data Carriers (Art 6 ECHR)

The case law on seizures and access to files is nowhere near as differentiated and clearly definable as that on house searches.[60] Therefore, it is not possible to present a concrete examination structure as for house searches (point III). This is also due to the different structure of the fundamental rights contained in Art 8 ECHR on the one hand, which is primarily relevant for house searches, and in Art 6 ECHR on the other, which is primarily relevant for the inspection of files in connection with seizures. With this in mind, this article attempts to derive specific principles from the general case law that are relevant to questions of criminal procedure in connection with seizures. Art 6 ECHR, with its integral right to a fair trial, defines a right to concrete and effective participation; the right to participation under Art 6 ECHR grants the accused the right to participate fully in the decision-making process in open-ended proceedings and thus to participate in the process of judgement.[61]

---

[55] *Robathin v Austria* App no 30457/06 (ECtHR, 3 July 2012), para. 51.

[56] *Vinks and Others v Latvia* App no 28926/10 (ECtHR, 30 January 2020), para. 104. Critical of Austrian practice and case law Tipold, 'Gilt die StPO?' 389 (394 ff).

[57] *Stefanov v Bulgaria* App no 65755/01 (ECtHR, 22 May 2008), para. 38.

[58] *Stefanov v Bulgaria* App no 65755/01 (ECtHR, 22 May 2008), para. 38.

[59] *Wieser und Bicos Beteiligungen GmbH v Austria* App no 74336/01 (ECtHR, 16 October 2007), para. 63.

[60] Cf. also from the German literature Gaede, *Fairness als Teilhabe – Das Recht auf konkrete und wirksame Teilhabe durch Verteidigung gemäß Art. 6 EMRK* (Berlin, 2007) 243 ff, 828 ff; Meglalu, *Das Akteneinsichtsrecht der Verteidigung* (Tübingen, 2023) 45 ff.

[61] From the German literature Gaede, *Fairness als Teilhabe* 920.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

In its decision of 14 December 2023, G 352/2021, the VfGH considered an appropriate balancing of interests to be central and stated the following: "The legislator must ensure that those affected by the seizure of a data carrier and the evaluation of the data stored on it (locally or externally) (can) receive the information necessary to safeguard their rights in the (investigation and possibly subsequent main) proceedings in an appropriate manner."[62] Although the VfGH formally based its decision on Art 8 ECHR and the fundamental right to data protection pursuant to Section 1 (1) DSG, the quoted statement is more accurately located within the scope of protection of Art 6 ECHR. This article therefore considers other important court decisions that can determine and concretise the balancing of interests deemed necessary by the VfGH.

The following principles can be derived from the case law of the Court and the VfGH in connection with the seizure of mobile devices:

The Court considers fishing expeditions to be a violation of the fair trial principle under Art 6 ECHR. If large amounts of data are available to the investigating authorities and these data are analysed by the authorities, the Court requires that the accused be at least involved in the definition of the search criteria and the relevant material in order to ensure equality of arms and protection against abuse.[63]

The Court interprets the right to access to the case file, which is a partial guarantee of the fair trial principle under Art 6 ECHR, very broadly. Specifically, the Court demands "unrestricted access to the case file and unrestricted use of any notes". According to the Court, this applies "a fortiori" if the good reputation of the accused is at stake and the legal basis for the denial of access to the case file is questionable.[64] The defence must therefore be entitled to unrestricted access to the files in order to guarantee fair criminal proceedings in accordance with fundamental rights.

According to the principles derived by the Court from Art 6 ECHR, equality of arms in criminal proceedings means that both the public prosecutor and the defence must have the same opportunity to gain knowledge of the investigative act and to comment on it. According to the Court, it is crucial to "have a real opportunity to comment on them".[65]

---

[62] Para. 101.

[63] *Sigurður Einarsson and Others v Iceland* App no 39757/15 (ECtHR, 4 June 2019), para. 90; similarly *Regner v Czech Republic* App no 35289/11 (ECtHR, 19 September 2017), para. 160.

[64] *Moiseyev v Russia* App no 62936/00 (ECtHR, 9 October 2008), para. 217.

[65] *Huseyn and Others v Azerbaijan* App no 35485/05 (ECtHR, 26 July 2011), para. 175.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

In particular, the prosecuting authorities must make both incriminating and exculpatory material available to the accused. This right is not absolute. In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. However, only such measures restricting the rights of the defence as are strictly necessary are permissible under Art 6 ECHR. Moreover, the investigating authorities may not carry out the assessment of this balancing of interests themselves without violating Art 6 ECHR.[66] In cases in which evidence is withheld from the accused – for reasons of the public interest, for example – the Court states that the decision-making procedure must be reviewed to ensure that there is equality of arms and adequate legal protection.[67]

According to the VfGH, the right to a fair trial requires, in the sense of the principle of equality of arms, full access to the contents of the file, which includes not only the inspection of the file itself, but also the possibility of making copies of the relevant documents. A violation of the principle of equality of arms may also be indicated if the public prosecutor, in contrast to the accused, is not subject to any restrictions.[68]

According to the VfGH, unrestricted access to the case files and the use of all records – including the possibility of obtaining copies of the relevant documents if necessary – ensures the principle of equality of arms. It is contrary to this principle to exclude the accused from accessing large amounts of material in the possession of the prosecution that may have relevance as evidence. This can be assumed in particular if the public prosecutor's office bases its indictment heavily on the extensive and (at least in the public prosecutor's opinion) meaningful material that is available to it – in contrast to the accused – at any time. The decisive factor for the violation of fundamental rights recognised by the VfGH in this case was "the order unilaterally incriminating the accused".[69]

---

[66] *Rowe and Davis v United Kingdom* App no 28901/95 (ECtHR, 16 February 2000), paras. 59 ff.

[67] *Regner v Czech Republic* App no 35289/11 (ECtHR, 19 September 2017), para. 149.

[68] Derived from the review decision of the Austrian VfGH 13 December 2011, G 85/11 ua, VfSlg 19.590/2011 with reference to the case law of the ECtHR.

[69] Austrian VfGH 13 December 2012, G 137/11, VfSlg 19.730/2012; according to the OGH's case law on Art 6 ECHR, unilaterally restricting access to files for the accused is also problematic if the accused is denied access to potentially exculpatory documents while the investigating authorities have access to the documents. According to the OGH a detrimental influence on the decision and an impossibility of a meaningful defence must be proven, Austrian OGH 22 September 2020, 11 Os 66/20w.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

The fundamental rights standards for this detrimental influence are demonstrated by relevant VfGH case law, which sets the threshold for a violation of fundamental rights very low: for example, in its decision VfSlg 15.840/2000 the VfGH recognised a violation of the principle of equality of arms by failing to inform a complaining lawyer in a timely manner of the statement made by the chamber lawyer in the proceedings before the Supreme Appeals and Disciplinary Commission for Lawyers. The arguments developed in this VfGH decision can be generalised: the VfGH initially referred to the Court in the case of *Brandstetter v Austria*.[70] In this case, the Court considered the principle of equality of arms to have been violated because the senior public prosecutor's opinion ("croquis") on the appeal of the complainant had not been brought to the complainant's attention. Although the croquis was included in the court file, neither the fact of its submission nor the document itself was brought to the attention of the defence. As the right of the defence to inspect the file also includes the croquis, the Court did not consider this procedure to be sufficient to ensure that the defence was made aware of this document for the purpose of submitting a possible counterstatement. In a similar ruling, the Court went – in the opinion of the VfGH – one step further in its reasoning by taking the view that it was not important for the assumption of a violation of the right to a fair trial whether a submission by the other side required a reaction from the defence. Against the background of the protective purpose of Art 6 ECHR, the Court stated: "It is a matter for the defence to assess whether a submission deserves a reaction."[71] The Court found that it was therefore unfair for the prosecution to make a submission to the court of which the defence was unaware.

As a result, the VfGH found that even the complainant's statutory right to inspect court files in the cited case was not sufficient to fulfil the guarantees of Art 6 ECHR; the VfGH supported this reasoning by referring to the Court's judgement in *Brandstetter v Austria*. The complainant had suffered an informational disadvantage before the Supreme Appeals and Disciplinary Commission "compared to the 'prosecution side', which violated his right guaranteed under Art 6 ECHR with regard to the 'principle of equality of arms'."[72]

[70] *Brandstetter v Austria* App no 11170/84 (ECtHR, 28 August 1991).

[71] *Bulut v Austria* App no 17358/90 (59/1994/506/588) (ECtHR, 22 February 1996), para. 49.

[72] Austrian VfGH 21 June 2000, B 412/98, VfSlg 15.840/2000.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

V. Interim Findings

A house search is a brief investigative measure and practically finished in one act. This article has noted the limits here; it is hardly possible to make any further deductions or instructions for practical cases. The seizure and evaluation of data have a different and more permanent quality of intervention. The direct relevance for the outcome of the proceedings is open-ended and – in contrast to house searches – there are options for action and the right to have a say. This applies in particular to the issue of access to files. The following remarks are based on this framework and focus on the seizure and inspection of files. Seizures relate to individual items and can also be carried out independently of house searches; prior to 2025, only extremely low-threshold conditions existed for this procedure, as the powers of seizure available to the investigating authorities dated back to a time before "big data", smartphones and modern information technology.[73]

A key legal premise of the following discussion is technological neutrality: the provisions of the StPO must be interpreted in a technologically neutral manner.[74] In general, data must not be treated less favourably than physical objects. The fact that the issue of technological neutrality has an important fundamental rights dimension is shown by the case law of the VfGH, which has dealt with the issue of paper files versus electronic files in data protection law.[75] It is easy to deduce from the VfGH's case law that mere knowledge of (i) the data sources and (ii) the nature of the data processing basis is necessary in order to be able to assert certain rights.[76] Again, if the accused does not know (i) which data the investigating authorities have and (ii) in which form they process data, they cannot effectively assert their rights.

[73] Dworzak/Hruschka, (2023) *AnwBl* 61 (61 with reference to Fink).

[74] Austrian OGH 1 August 2023, 14 Os 57/23y on Section 52 (1) first sentence of the StPO (inspection of files for the defence counsel): "Accordingly, copies are 'copies' or 'other reproductions of the contents of the file', whereby these terms are to be understood in a media- and technology-neutral manner"; see also the legislative materials on the Criminal Procedure Reform Act ErläutRV 25 BlgNR 22. GP 156, 186; Höcher, 'Gedanken zur Sicherstellung', 419 (421).

[75] Austrian VfGH 10 December 2014, B 1187/2013, VfSlg 19.937/2014; Austrian VfGH 12 December 2017, E 3249/2016, VfSlg 20.227/2017; see also Austrian OGH 15 February 2014, 6 Ob 6/14x.

[76] See references point IV.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

VI. Seizure and Information Rights: Legal Situation Prior to 1 January 2025

A. Criminal Procedural Framework

The following thesis of a public prosecutor from the Austrian Central Public Prosecutor's Office for Combating Economic Crime and Corruption sounds sobering: in the course of executing a seizure, it is not possible to decide and sort out (select) on site which data is specifically relevant to the proceedings due to the extensive amount of data. On site, it is essentially only possible to check whether the seizure of data is covered by the scope of the order (rough screening). As a result, the case law of the OLG Vienna means that law enforcement authorities are allowed to seize more and more data, including data that is not relevant to the proceedings. The case law of the OLG Vienna shows that the options of the accused are limited when it comes to the seizure of electronic data.[77]

As a result, the accused is generally not in possession of the data on the mobile phone. It is therefore logical that the authorities are often in a far more comfortable position than the accused.

A statement by Weratschnig is therefore quite surprising: he writes that "the accused can ensure that exculpatory circumstances are also included in the file by submitting corresponding requests for evidence (or presenting corresponding documents from their own data material). In view of his own database [...] the accused has a knowledge advantage over the prosecuting authorities."[78]

This statement seems cynical. If the legal and factual situation is clear, the accused may have a knowledge advantage with regard to the offence committed, because only he knows whether he actually committed the offence.[79] Under no circumstances, however, does this apply to data. The accused's right to be heard (Art 6 ECHR) is decisively curtailed, at least in connection with large data carriers: he does not have the same information as the authorities and therefore has only a limited opportunity

[77] Weratschnig, 'Waffengleichheit und Digitalisierung', in Lehmkuhl/Meyer (eds.), *Das Unternehmen im Brennpunkt nationaler und internationaler Strafverfahren* (Baden-Baden, 2020) 203 (207 ff).

[78] Weratschnig, 'Waffengleichheit und Digitalisierung', 203 (218).

[79] Cf e.g. Liechtenstein OGH 20 February 1995, 4 U 11/94-22 (1995) *LES* 91 (92): "In the preliminary proceedings, the accused has a knowledge advantage over the prosecuting authorities, because the accused knows from the outset whether or not he has committed the offence with which he is charged. The prosecuting authorities, on the other hand, must first familiarise themselves with the facts of the case." In more complex white-collar criminal cases (e.g. breach of trust), however, the question of the offence may also be unclear or at least a grey area, so that the accused would not have a knowledge advantage in this respect either.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

to request that data which he considers exculpatory should also be included in the file.[80]

This article rebuts the quoted statement in two respects. Firstly, it aims to raise awareness of the restrictions on fundamental rights that form the framework for legally compliant investigative actions by the authorities. Secondly, it proposes concrete requests as to how accused persons can defend themselves against violations of the law.[81]

In this respect, for Ruhri it is crucial to answer the question of why data that the police and public prosecutor's office consider to be unrelated to the suspicion examined in the proceedings is seized in the first place; this cannot be done for reasons of proof. Since the law enforcement authorities cannot be assumed to seize data excessively or in the hope of an incidental finding, the mere fact that documents are in the custody of the police or judiciary as a result of an ordered measure justifies the presumption of relevance to the proceedings. The ordered seizure brings the data into a direct relationship with the proceedings and the subject matter of the proceedings. It is based on the fact that the data is covered by a seizure order formulated by the public prosecutor's office and therefore at least prima facie relevant to the subject matter of the proceedings.[82]

The central practical problem focuses on the question of which processes should be used to separate relevant information from non-relevant information in criminal proceedings.[83] The investigating authorities can fall back on the fact that the assessment of necessity and relevance is a process (the "relevance test", *Relevanzprüfung*). This usually results in a state of limbo in major white-collar criminal proceedings, in which the accused's rights of defence are severely restricted (see point VII.A for more details). After all, the investigating authorities themselves carry out the relevance check precisely in order to find out what is relevant. And without this structured search, they would not have this particular knowledge.

From the perspective of information rights, there is now a crucial problem: how can I request something that I do not know? The relevance check is therefore ultimately

[80] Zerbes/Ghazanfari, (2022) *AnwBl* 640 (648).

[81] Divjak, 'Die Durchsetzung von Datenschutzrechten im Ermittlungsverfahren' (2022) *JBl* 489, is also convincing with this approach of proposing concrete applications.

[82] Ruhri, 'Rechtliche Bewertung determiniert Ermittlungsergebnisse' (2022) *JBl* 58 (60).

[83] Weratschnig, 'Waffengleichheit und Digitalisierung', 203 (204).

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

also the decisive link between seizure (here point VI) and inspection of files (the following point VII).

This connection in the sense of communicating vessels is also shown by the case law of the Court. According to the Court, there is a certain obligation to label the requested data and documents and, in addition, a certain obligation to concretise specific requests; at the same time, law enforcement authorities must provide protocols or inventory lists of seized data.[84] The less a defendant knows about the content of the seized data, the more difficult it is for him to fulfil his duty to cooperate.

B. Rights of the Accused

The following requests by the accused are conceivable within the framework described in point VI.A:

- Request for designation of all seized or confiscated objects (data carriers, data) with simultaneous disclosure of the underlying seizure orders or confiscation warrants.
- Request for designation or specification of the seizure protocols or inventory lists.
- Request for designation of all produced duplicates of seized or confiscated items (data carriers, data).
- Request for a description of the scope and content of any data pool created on the basis of originals or duplicates.

VII. Content and Scope of the Act of Investigation and Access to Files: Legal Situation Prior to 1 January 2025

A. Criminal Procedural Framework

The public prosecutor quoted at the beginning of point VI.A puts forward the following further theses, citing two decisions of the OLG: on the one hand, the OLG Linz, according to which the accused must be granted access to files concerning seized data;[85] on the other, the OLG Vienna, according to which the accused must not be granted access to files concerning seized data.[86] The author comments as

[84] *Sigurður Einarsson and Others v Iceland* App no 39757/15 (ECtHR, 4 June 2019), paras. 90 ff.

[85] OLG Linz 11 June 2015, 8 Bs 171/14z; some decisions of the Austrian OLGs – including this one – can be accessed via http://ris.bka.gv.at/Judikatur/ with their case number. Some others are published in scientific journals and accessible via legal databases.

[86] OLG Vienna 10 March 2016, 17 Bs 42/16z.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

follows on the OLG Vienna: in this decision – which can certainly be described as fundamental – the court expressly stated that documents and data do not become part of the investigative file simply by the mere (provisional) seizure, which only constitutes the obtaining of custody. Therefore, only data that is categorised as relevant to the proceedings after examination (by the prosecution authorities) and included in the investigation file must be understood as the results of the investigation proceedings within the meaning of Section 51 (1) StPO. However, the law does not provide for the participation of the accused in this process (viewing process).[87]

Why the second decision is "fundamental" and why it should be given preference over the one issued by the OLG Linz is not supported by legal reasoning, but merely asserted. The author also fails to provide a legal basis for the seizure of data that is "not relevant to the proceedings". The seizure must already have a minimum degree of relevance to the proceedings; otherwise the seizure itself would be unlawful.[88] Furthermore, there are not only the two cited decisions of the OLG Vienna and the OLG Linz. There is, for example, another decision by the OLG Vienna issued in 2017, which represents a more liberal interpretation of the law than the one from 2016. The court concluded in 2017 that the public prosecutor's office can certainly be allowed to take a considerable amount of time to analyse a large quantity of material. That the prosecuting authority recognises the relevance of the documents and storage media in question as evidence on the one hand – be it through further seizure or through the production of duplicates – and on the other claims sole authority to assess the significance of this evidence-relevant material for the accused does not meet the requirements of Art 6 ECHR.[89]

The prosecutor does not even mention the examples given, other positions or even contrary case law of the Court (see point IV), although he refers intensively to Art 6 ECHR at the beginning of his contribution. To suggest that there is no alternative to the position he advocates is not a balanced contribution to the legal discourse.

Now that the prosecution's point of view is known, the defence's point of view should also be given space.

---

[87] Weratschnig, 'Waffengleichheit und Digitalisierung', 203 (213 f).

[88] Wess/Machan, 'Akteneinsicht in sichergestellte, aber noch nicht als verfahrensrelevant erkannte Unterlagen und elektronische Daten?', in Lewisch (ed.), *Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2016* (Vienna, 2016) 167 (173).

[89] OLG Vienna 14 June 2017, 23 Bs 240/16m; see also OLG Vienna 4 June 2014, 21 Bs 226/13s (2015) *JSt* 139; OLG Vienna 8 November 2019, 23 Bs 193/19d (2020) *JSt* 59.

Höcher summarises as follows: for the defence, the evaluation process resembles a black box: it is roughly known what information and data is available and the result of the process can be seen in the investigation file. What happens in between can hardly be reconstructed from the outside and is therefore virtually unverifiable and difficult to influence for various reasons. The OLG Vienna elegantly describes the evaluation process as a "state of limbo" (a term that is foreign to the StPO), in which it is not yet possible to say what will become the content of the file. In the opinion of the OLG Vienna, the foundation of a comprehensive defence is not impaired because the material related to the subject matter of the proceedings can be viewed anyway once the evaluation process has been completed. In other words, the defence should simply wait for the result of the evaluation because it cannot influence the evaluation anyway. The public prosecutor's office argues further that the purpose of the investigation would be jeopardised if the accused were to evaluate the data more quickly than the investigating authority. Legal protection is severely restricted because the "state of suspense" is largely beyond legal control. Therefore, the practice of the prosecution authorities in Austria leads to the worst possible outcome from the perspective of the accused: if the accused wants the information/data available to the prosecution authorities to be deleted, such deletion can be rejected with reference to the fact that the relevance check has not yet been fully completed. If, on the other hand, the accused wishes to analyse the information and data available to the law enforcement authorities in order to disprove an allegation, this will be rejected after the relevance check has been completed, with reference to the fact that the information and data not in the investigation file have been deleted. Yet only the information and data in the investigation file can be inspected in the first place.[90]

It is obvious that the practice outlined in the previous paragraph is not in line with the case law of the Court and VfGH and is therefore unconstitutional. This is also evident from the decision of the VfGH of 14 December 2023, G 352/2021 (see point IV).

B. Rights of the Accused

The following requests by the accused are conceivable within the framework described in point VII.A:

[90] Höcher, 'Gedanken zur Sicherstellung', 419 (424 ff with reference to OLG Vienna 24 September 2018, 20 Bs 93/18z); see also Pillichshammer/Wess, 'Zum Beginn eines (weiteren) strafrechtlichen Ermittlungsverfahrens bei der Sichtung sichergestellter Datensätze durch die Strafverfolgungsbehörden' (2024) *ZWF* 14.

The literature has proposed the right to the following requests (with a proposal to amend the law):

- Request for all parts of the investigative file to be made available on one (or more) data carriers (bit-identical copy, copy of the subsequently restored data and the preserved volatile data). In this way, the data available to him after a seizure would correspond completely with the data on which the investigating authorities are working, and he would be able to exercise his participation rights and make further requests on this basis.
- Request to add to the file material exculpatory for the accused that the authorities have sorted out as irrelevant.
- Request that data which the accused considers irrelevant in terms of suspicion is not included in the file.[91]

The following further requests are conceivable:

- Request for an electronic copy of the file.
- Request to view files via VPN access.
- Request for on-site inspection of files.
- Request for disclosure of which categories of data (data groups) the investigating authorities have created.[92]
- Request for disclosure of the legal basis on which data that is not yet part of the investigative act is stored and analysed or request for a description of the scope and content of the data that is also available to the investigating authorities but has not been included in the investigation file.[93]
- Request to supplement the file.[94]

---

[91] See Zerbes/Ghazanfari, (2022) *AnwBl* 640 (649).

[92] Cf. with four categories *Sigurður Einarsson and Others v Iceland* App no 39757/15 (ECtHR, 4 June 2019), para. 88: "[...] several collections of documents/data: the 'full collection of data' which encompassed all the material obtained by the prosecution; [...] a sub-category data 'tagged' as a result of the Clearwell searches using specified keywords but not subsequently included in the investigation file; the 'investigation documents', identified from that material by means of further searches and manual review as potentially relevant to the case; and the 'evidence in the case', that is the material selected from the 'investigation documents'".

[93] See OLG Vienna 14 June 2017, 23 Bs 240/16m; see also Austrian OGH 13 October 2020, 11 Os 56/20z: archiving of information by law enforcement agencies not in the service of the administration of criminal justice occurs without legal cover (Art 18 (1) B-VG) and violates Section 5 (1) StPO, thus a right under this act within the meaning of no. 1 of Section 106 (1) StPO.

[94] See Austrian OGH 1 June 2021, 14 Os 35/21k.

- Request for justification in the event of refusal. For example, a subjective right to justification of the restriction of access to the file can be argued.[95]

VIII. Legal Situation Since 1 January 2025 (*Strafprozessrechtsänderungsgesetz 2024*): Legislative Cornerstones and Fundamental Rights Safeguards

House searches and seizures are coercive measures taken by the authorities in criminal proceedings to clarify the suspicion of a criminal offence in order to establish the material truth.

While there were already measures in place to ensure guarantees of fundamental rights during house searches, significant restrictions on the confiscation of data carriers and data were only implemented by the *Strafprozessrechtsänderungsgesetz 2024*. A judicial authorisation must now exist prior to such a confiscation, in which the scope, the type of data category and the time period must be determined in advance. In addition, a distinction between the processing and analysis of data – also not previously made under the old legal situation – is standardised.

The legislator has thus fulfilled the minimum requirements set forth in the case law of the Court and the VfGH. In its ruling of 14 December 2023, G 352/2021, the VfGH focused on the fundamental rights of Art 8 ECHR and Section 1 DSG. In so doing, it placed the emphasis on the proportionality test and prioritised those aspects of a future legislative measure that play a key role in a proportionality assessment.[96]

However, the legislature recognised the breadth of the issue in terms of fundamental rights and, with its legislative measures of the *Strafprozessrechtsänderungsgesetz 2024*, created guarantees to ensure a fair trial within the meaning of Art 6 ECHR. As parties to the proceedings, the accused and other participants benefit from a protection mechanism that was previously lacking in this quality and breadth.

This broad-based approach by the legislature is convincing, as Art 6 ECHR forms the core of the protection mechanisms of constitutional criminal proceedings.

---

[95] OLG Vienna 3 February 2021, 18 Bs 192/20x (2021) *JSt* 301. The principle of subsidiarity and the principle of proportionality pursuant to 110 (4) StPO can also be helpful; see Tipold/Zerbes, 'Prev. Section 110-115', in Fuchs/Ratz (eds.), *Wiener Kommentar StPO* (Vienna, 2021) para. 8: seizure and confiscation are only constitutional if no less drastic measure with the same prospect of success is available. Instead of a seizure, an inspection must be carried out as far as possible. If copies are sufficient, the holder must be given the original; if an image is sufficient, the holder must be given the object; see also Keplinger/Prunner/Pühringer, 'Section 110', in Birklbauer/Haumer/Nimmervoll/Wess (eds.), *Linzer Kommentar zur Strafprozessordnung* (Vienna, 2020) para. 10.

[96] Reindl-Krauskopf, (2024) *JBl* 166 (174).

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

Judicial and procedural fundamental rights combine different legal positions, all of which have a point of reference in effective legal protection as an expression of a European constitutional principle of the rule of law.[97]

The legislature has established a reasonable reform and created the essential legal cornerstones for authorities to enforce the law. The future will show whether a reasonable middle way can be found in the actual enforcement of the law to reconcile the tension between establishing the material truth and protecting fundamental rights in accordance with the constitution.

IX. Summary

The ECHR is designed to guarantee not rights that are theoretical or illusory but rights that are practical and effective.[98] This article has focused on searches of premises (house searches) and seizures of mobile devices and data under Austrian criminal procedural law. In accordance with the case law of the European Court of Human Rights and the Austrian Constitutional Court it examined the question regarding the golden mean of the rule of law between the poles of effective crime fighting on the one hand and the rights of the accused on the other.

Strict requirements for house searches must be derived from Art 8 ECHR (in particular compliance with legal and foreseeable standards and legitimate aim of the interference, proportionality of the search, judicial authorisation, effective procedural safeguards and reasonable limitation of scope).

If large amounts of data are available to the investigating authorities and these data are analysed by the authorities, Art 6 ECHR requires that the accused at least be involved in the definition of the search criteria and the relevant material in order to ensure equality of arms and to be protected against abuse.

Unrestricted access to the case files and the use of all records – including the possibility of obtaining copies of the relevant documents if necessary – ensure the principle of equality of arms. If the accused does not know which data the investigating authorities have and in which form they process this data, they cannot effectively assert their rights.

The points summarised above regarding the specific guarantees of fundamental rights are reflected in the current amendment to the StPO. Through the

[97] Grabenwarter/Pabel, *Europäische Menschenrechtskonvention*, 7th edn. (Munich, Basel, Vienna, 2021) sec. 24 para. 1.

[98] *Sejdovic v Italy* App no 56581/00 (ECtHR, (GC) 1 March 2006), para. 94.

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

Strafprozessrechtsänderungsgesetz 2024, the legislator has established the necessary legislative measures to fulfill the promise of fundamental rights under constitutional law.

Hopefully this article will also provide a basis for further practical findings and academic research in the future. After all, given the momentum in the world of big data, the last word in this context is far from spoken.

X. Bibliography

A. Primary Sources

CJEU Case C-670/22 *Staatsanwaltschaft Berlin/M.N.*, 30 April 2024, ECLI:EU:C:2024:372

CJEU Case C-548/21 *Bezirkshauptmannschaft Landeck/C.G.*, 4 October 2024, ECLI:EU:C:2024:830

Brandstetter v Austria App no 11170/84 (ECtHR, 28 August 1991)

Bulut v Austria App no 17358/90 (59/1994/506/588) (ECtHR, 22 February 1996)

Rowe and Davis v United Kingdom App no 28901/95 (ECtHR, 16 February 2000)

Roemen and Others v Luxembourg App no 51772/99 (ECtHR, 25 February 2003)

Buck v Germany App no 41604/98 (ECtHR, 28 April 2005)

Sallinen and Others v Finland App no 50882/99 (ECtHR, 27 September 2005)

Sejdovic v Italy App no 56581/00 (ECtHR, (GC) 1 March 2006)

Smirnov v Russia App no 71362/01 (ECtHR, 7 June 2007)

Wieser und Bicos Beteiligungen GmbH v Austria App no 74336/01 (ECtHR, 16 October 2007)

Stefanov v Bulgaria App no 65755/01 (ECtHR, 22 May 2008)

Moiseyev v Russia App no 62936/00 (ECtHR, 9 October 2008)

Heino v Finland App no 56720/09 (ECtHR, 15 February 2011)

Huseyn and Others v Azerbaijan App no 35485/05 (ECtHR, 26 July 2011)

Robathin v Austria App no 30457/06 (ECtHR, 3 July 2012)

Prezhdarovi v Bulgaria App no 8429/05 (ECtHR, 30 September 2014)

Misan v Russia App no 4261/04 (ECtHR, 2 October 2014)

Sher and Others v United Kingdom App no 5201/11 (ECtHR, 20 October 2015)

Cacuci and Others v Romania App no 27153/07 (ECtHR, 17 January 2017)

Posevini v Bulgaria App no 63638/14 (ECtHR, 19 January 2017)

Regner v Czech Republic App no 35289/11 (ECtHR, 19 September 2017)

Sigurður Einarsson and Others v Iceland App no 39757/15 (ECtHR, 4 June 2019)

Vinks and Others v Latvia App no 28926/10 (ECtHR, 30 January 2020)

Dorož v Poland App no 71205/11 (ECtHR, 29 October 2020)

Austrian OGH 2 July 1992, 15 Os 3/92

Austrian OGH 15 February 2014, 6 Ob 6/14x

Austrian OGH 22 September 2020, 11 Os 66/20w

Austrian OGH 13 October 2020, 11 Os 56/20z

Austrian OGH 1 June 2021, 14 Os 35/21k

Austrian OGH 24 May 2023, 15 Os 13/23k

Austrian OGH 1 August 2023, 14 Os 57/23y

Liechtenstein OGH 20 February 1995, 4 U 11/94-22 (1995) *Liechtensteinische Entscheidungssammlung (LES)* 91

OLG Vienna 4 June 2014, 21 Bs 226/13s (2015) *Journal für Strafrecht (JSt)* 139

OLG Linz 11 June 2015, 8 Bs 171/14z

OLG Vienna 10 March 2016, 17 Bs 42/16z

OLG Vienna 14 June 2017, 23 Bs 240/16m

OLG Vienna 24 September 2018, 20 Bs 93/18z

OLG Vienna 8 November 2019, 23 Bs 193/19d (2020) *Journal für Strafrecht (JSt)* 59

OLG Vienna 3 February 2021, 18 Bs 192/20x (2021) *Journal für Strafrecht (JSt)* 301

Austrian VfGH 21 June 2000, B 412/98, VfSlg 15.840/2000

Austrian VfGH 13 December 2011, G 85/11 ua, VfSlg 19.590/2011

Austrian VfGH 13 December 2012, G 137/11, VfSlg 19.730/2012

Austrian VfGH 10 December 2014, B 1187/2013, VfSlg 19.937/2014

Austrian VfGH 12 December 2017, E 3249/2016, VfSlg 20.227/2017

University of Vienna Law Review, Vol. 9 No 1 (2025), pp. 20-54, https://doi.org/10.25365/vlr-2025-9-1-20.

Austrian VfGH 11 December 2019, G 72/2019 ua, VfSlg 20.356/2019

Austrian VfGH 14 December 2023, G 352/2021

Legislative materials on the Criminal Procedure Reform Act ErläutRV 25 BlgNR 22. GP

Report of the Committee of Inquiry into Political Influence on the Federal Office for the Protection of the Constitution and Counterterrorism (2019)

B. Secondary Sources

Ainedter, Klaus and Poppenwimmer, Linda, 'Persönlichkeitsschutz und Akteneinsicht von (Mit-)Beschuldigten' (2023) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 61

Bauer, Manuela, *Verwertungsverbote zur Gewährleistung von Waffengleichheit* (Vienna, 2015)

Böse, Martin, 'Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel' (2022) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 9

Brandstetter, Wolfgang and Zöchbauer, Peter, 'Grundrechtsverwirrung oder Grundrechtserosion?' (2022) *Medien und Recht (MR)* 3

Caspar-Bures, Bettina, 'Ein rechtsstaatliches Strafverfahren verlangt eindeutig rechtskonforme Beweismittel' (2024) *Journal für Strafrecht (JSt)* 445

Divjak, Jonas, 'Die Durchsetzung von Datenschutzrechten im Ermittlungsverfahren' (2022) *Juristische Blätter (JBl)* 489

Dworzak, Danijela and Hruschka, Bernhard, 'ÖRAK fordert tiefgreifende Reformen bei der Sicherstellung und Auswertung von Daten und Datenträgern' (2023) *Österreichisches Anwaltsblatt (AnwBl)* 61

Flora, Margarethe, 'Section 363a' in Christian Bertel, Andreas Venier (eds.), *StPO – Strafprozessordnung, Band II* (Vienna, 2020)

Gaede, Karsten, *Fairness als Teilhabe – Das Recht auf konkrete und wirksame Teilhabe durch Verteidigung gemäß Art. 6 EMRK* (Berlin, 2007)

Ghazanfari, Shirin, 'Bekanntgabe des PUK-Codes und Duplizierung einer SIM-Karte – Sicherstellung?' (2021) *Juristische Blätter (JBl)* 740

Ghazanfari, Shirin, 'Zu den Anforderungen an die Überwachung von (moderner) interpersoneller Kommunikation' (2024) *Journal für Strafrecht (JSt)* 459

Glaser, Severin and Kert, Robert, 'EuGH: Anforderungen an die Sicherstellung von Mobiltelefonen' (2024) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 288

Grabenwarter, Christoph and Pabel, Katharina, *Europäische Menschenrechtskonvention*, 7th edn. (Munich, Basel, Vienna, 2021)

Herrnfeld, Judith, 'Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel' (2022) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 2

Höcher, Markus, 'Gedanken zur Sicherstellung von Mobiltelefonen', in Otto Dietrich, Severin Glaser, Robert Kert, Alexander Tipold (eds.), *Festschrift Wolfgang Brandstetter* (Vienna, 2022) 419

Hribernigg, Michael and Weber, Josef, 'Steuerfahndung und Hausdurchsuchung', in Bernhard Gröhs, Michael Kotschnigg (eds.), *Finanzstrafrecht in der Praxis – Band 2* (Vienna, 2008) 65

Ifsits, Clara, 'Zum strafprozessualen Schutz klassifizierter Informationen nach § 112a StPO' (2023) *Österreichische Juristinnenzeitung (ÖJZ)* 220

Jahn, Matthias and Brodowski, Dominik, 'Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverhandlung und Revision', in Elisa Hoven, Hans Kudlich (eds.), *Digitalisierung und Strafverfahren* (Baden-Baden, 2020) 67

Keplinger, Rudolf, Prunner, Marina and Pühringer, Lisa, 'Section 110' in Alois Birklbauer, René Haumer, Rainer Nimmervoll, Norbert Wess (eds.), *Linzer Kommentar zur Strafprozessordnung* (Vienna, 2020)

Kert, Robert and Schroll, Hans Valentin, 'Die Kronzeugenregelung und ihre Grenzen' (2022) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 166

Köck, Elisabeth, 'Verbandsverantwortlichkeit und Akteneinsicht im gerichtlichen und verwaltungsbehördlichen Finanzstrafverfahren', in Markus Achatz, Rainer Brandl, Robert Kert (eds.), *Festschrift Roman Leitner – Steuerrecht – Finanzstrafrecht – Wirtschaftsstrafrecht* (Vienna, 2022) 317

Köck, Elisabeth, 'Die Sicherstellung von Krypto-Assets im Finanzstrafverfahren' (2023) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 84

Kroll, Fritz, *Kernbereichsschutz bei Durchsuchungen* (Tübingen, 2021)

Kynast, Britta, 'Verordnung zu elektronischen Beweismitteln in Strafsachen' (2023) *Österreichisches Anwaltsblatt (AnwBl)* 479

Meglalu, Saber, *Das Akteneinsichtsrecht der Verteidigung* (Tübingen, 2023)

Menhofer, Stefan, 'EuGH steckt rechtlichen Rahmen für Zugriff auf Handy-Daten ab' (2024) *Steuer- und WirtschaftsKartei (SWK)* 1242

Miklau, Roland and Szymanski, Wolf, 'Strafverfahrensreform und Sicherheitsbehörden – eine Nahtstelle zwischen Justiz- und Verwaltungsrecht', in Walter Melnizky, Otto Müller (eds.), *Strafrecht, Strafprozeßrecht und Kriminologie – Festschrift Franz Pallin* (Vienna, 1989) 249

Murschetz, Verena, *Verwertungsverbote bei Zwangsmaßnahmen gegen den Beschuldigten* (Vienna, 1999)

Papathanasiou, Konstantina, 'EncroChat – das "WhatsApp der Kriminellen" und seine strafverfahrensrechtliche Relevanz' (2022) *Zeitschrift für das Juristische Studium (ZJS)* 259

Paulitsch, Heidemarie, 'Einleitung', in Heidemarie Paulitsch (ed.), *Praxishandbuch Hausdurchsuchung,* 2nd edn. (Vienna, 2023) 1

Pillichshammer, Thomas and Wess, Norbert, 'Zum Beginn eines (weiteren) strafrechtlichen Ermittlungsverfahrens bei der Sichtung sichergestellter Datensätze durch die Strafverfolgungsbehörden' (2024) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 14

Premissl, Karl, *Strafrechtsschutz und Grundrechte* (Vienna, 2008)

Ranzoni, Carlo, 'Aktuelle Fragen in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte' (2018) *Liechtensteinische Juristenzeitung (LJZ)* 114

Ratz, Eckart, 'Beweiswürdigung im Ermittlungsakt und Sicherstellung ohne Kriminalpolizei und durch Sachverständige' (2022) *Österreichische Jurist:innenzeitung (ÖJZ)* 58

Reindl-Krauskopf, Susanne, 'Verfassungswidrigkeit von Bestimmungen der StPO über die Sicherstellung von Gegenständen (wie Datenträgern) aus Beweisgründen' (2024) *Juristische Blätter (JBl)* 166

Rohregger, Michael, 'Kollateralschäden im Strafverfahren – Was darf der Staat dem Beschuldigten zumuten?' (2017) *Juristische Blätter (JBl)* 219

Rohregger, Michael, 'VfGH: Handysicherstellung verfassungswidrig' (2024) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 2

Ruhri, Gerald, 'Grenzen der Verwendung und Verwertung von Verfahrensergebnissen in Strafverfahren und Urteil in Österreich' (2020) *Österreichisches Anwaltsblatt (AnwBl)* 23

Ruhri, Gerald, 'Rechtliche Bewertung determiniert Ermittlungsergebnisse' (2022) *Juristische Blätter (JBl)* 58

Schmidt, Anja, 'Zur strafprozessualen Verwertbarkeit der Daten aus der Überwachung verschlüsselter Mobiltelefone durch einen anderen Mitgliedstaat der EU' (2022) *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)* 982

Schmoller, Kurt, 'Heimliche Tonbandaufnahmen als Beweismittel im Strafprozeß?' (1994) *Juristische Blätter (JBl)* 153

Schmoller, Kurt, 'Ergebnisse einer von einer ausländischen Behörde durchgeführten Überwachungsmaßnahme – Verwendungsverbot?' (2023) *Juristische Blätter (JBl)* 739

Schönbauer, Franz, 'Technisch-organisatorische Aspekte bei der Sicherstellung von Daten und Datenträgern' (2023) *Österreichisches Anwaltsblatt (AnwBl)* 42

Schönborn, Elias and Thiel, Jan Uwe, 'Verhältnismäßigkeit und Datenschutz bei der Sicherstellung von Daten(trägern)' (2024) *Zeitschrift für Wirtschafts- und Finanzstrafrecht (ZWF)* 139

Schumann, Stefan, 'Datenschutz im Informationszeitalter – Verfassungswidrigkeit der StPO in Betreff der Sicherstellung von Mobiltelefonen' (2024) *Österreichische Jurist:innenzeitung (ÖJZ)* 471

Schumann, Stefan, '"Sicherstellung von Daten neu" – Reparatur oder (R)evolution?' (2024) *Österreichische Jurist:innenzeitung (ÖJZ)* 675

Soyer, Richard and Marsch, Philip, 'VfGH und Handysicherstellung – technische und rechtliche Fragen aus dem Verfahren' (2024) *Österreichisches Anwaltsblatt (AnwBl) 164*

Soyer, Richard and Marsch, Philip, 'VfGH zur Handysicherstellung. Eigentlich: VfGH zur Sicherstellung von Daten(-trägern) und IT-Endgeräten. Parallel: VfGH zum doppelten Rechtsschutz im Ermittlungsverfahren' (2024) *Journal für Strafrecht (JSt)* 118

Tipold, Alexander, 'Hausdurchsuchung oder Amtshilfe – Das ist hier die Frage!' (2021) *Journal für Strafrecht (JSt)* 225

Tipold, Alexander, 'Hausdurchsuchung oder Amtshilfe – was für eine Frage? Hausdurchsuchung!' (2021) *Journal für Strafrecht (JSt)* 461

Tipold, Alexander, 'Gilt die StPO im strafrechtlichen Ermittlungsverfahren?' in Otto Dietrich, Severin Glaser, Robert Kert, Alexander Tipold (eds.), *Festschrift Wolfgang Brandstetter* (Vienna, 2022) 389

Tipold, Alexander and Zerbes, Ingeborg, 'Prev. Section 110-115', in Helmut Fuchs, Eckart Ratz (eds.), *Wiener Kommentar StPO* (Vienna, 2021)

Tipold, Alexander and Zerbes, Ingeborg, 'Section 110', in Helmut Fuchs, Eckart Ratz (eds.), *Wiener Kommentar StPO* (Vienna, 2021)

Tomaš, Dijana, 'Strafprozessuale Beweisverwertung nach rechtswidriger Durchsuchung' (2024) *Österreichische Jurist:innenzeitung (ÖJZ)* 928

Vogl, Felix Karl, 'Review of Paulitsch (ed.): Praxishandbuch Hausdurchsuchung' (2018) *Journal für Strafrecht (JSt)* 441

Warnking, Vera, *Strafprozessuale Beweisverbote in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und ihre Auswirkungen auf das deutsche Recht* (Frankfurt am Main, 2009)

Weratschnig, Bernhard, 'Waffengleichheit und Digitalisierung', in Marianne Johanna Lehmkuhl, Frank Meyer (eds.), *Das Unternehmen im Brennpunkt nationaler und internationaler Strafverfahren* (Baden-Baden, 2020) 203

Wess, Norbert and Machan, Markus, 'Akteneinsicht in sichergestellte, aber noch nicht als verfahrensrelevant erkannte Unterlagen und elektronische Daten?', in Peter Lewisch (ed.), *Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2016* (Vienna, 2016) 167

Zerbes, Ingeborg and Ghazanfari, Shirin, 'Stellungnahme im Auftrag des Instituts für Anwaltsrecht der Universität Wien zur Sicherstellung und Auswertung von Daten und Datenträgern' (2022) *Österreichisches Anwaltsblatt (AnwBl)* 640

Zerbes, Ingeborg and Ghazanfari, Shirin, 'Sicherstellung und Verwertung von Handy-Daten – Reformperspektiven' (2023) *Österreichisches Anwaltsblatt (AnwBl)* 559

C. Internet Sources

Hagen, Lara, Marchart, Jan Michael and Schmid, Fabian, 'Welche Chats die heimische Politik erschüttern' (*Der Standard*, 2 March 2022), https://www.derstandard.at/story/2000133753280/welche-chats-die-heimische-politik-erschuettern, accessed 18 February 2025

Graber, Renate and Schmid, Fabian, 'WKStA will neue "hochrelevante Beweise" für blauen Casinos-Deal gefunden haben' (*Der Standard*, 29 April 2023), https://www.derstandard.at/story/2000145978761/wksta-will-neue-hochrelevante-beweise-fuer-blauen-casinos-deal-gefunden, accessed 18 February 2025

unknown author, 'Freisprüche im Prozess gegen Ex-BVT-Spionagechef' (*Der Standard*, 3 March 2022), https://www.derstandard.at/story/2000133817835/freisprueche-im-prozess-gegen-ex-bvt-spionagechef, accessed 18 February 2025