Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings

Ingeborg Zerbes*

This paper discusses three topics in the area of procuring electronic data by means of coercion: In a first step it raises the question whether traditional seizure exceeds to data stored in the seized object as such (e.g. a pc). It goes to explore legal issues related to data stored in external databases. Finally, it focuses on transnational situations when mutual legal assistance is needed. It argues that the concept of forum regit actum may be superior to the to the traditional locus regit actum approach.

A. Key issues of criminal procedural law

When we talk about *transnational* exchange of evidence we talk about mutual legal assistance, and when we talk about mutual legal assistance in *criminal investigations,* we have first to deal with procedural law issues as such: every act of cooperation between states in investigation matters is ultimately based on criminal procedural law – even if different national legal systems converge.

Before switching over to the *real* cross-border subjects, I will briefly give an overview of the key questions of procedural law, according to which the collection of electronic evidence is to be executed.

I. Access to electronic data based on seizure

1. Seizure of physical IT-devices

The most important investigation measure to obtain access to electronic data is a very traditional one: the seizure of physical objects, namely the seizure of the data storage devices as such – the computers, notebooks, hard-disks, mobile phones, i-pads etc. found in the possession of the affected person. This measure – seizure of objects of evidence – is part of the traditional set of coercive measures in every national criminal procedural law. Within the traditional rules, the law enforcement authorities are firstly able to *seize* objects of evidence; furthermore they have the competence to *examine* the seized objects; and the examination of a seized object is not restricted to looking at it from the outside: the authorities are allowed to open it and to examine its contents. Translated into the world of IT, this means that the authorities are allowed to start up a seized IT-device, and to gain access to all data stored on it, albeit, they are restricted to the subject of their investigation.[1]

* Prof. Dr. iur. Ingeborg Zerbes, Professor of Criminal Law and Head of Department at the University of Bremen (Germany).

[1] *Zerbes/El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, Neue Zeitschrift für Strafrecht (NStZ)2015, p. 425 (p. 427).

2. Access to the external database using the seized devices: online investigation 'light'

These days, the particular quality of electronic data, which we store on a computer and to which we gain access to by a computer, is that it is no longer bound to a specific personal device. The modern technique of data storage is to use external storage-space on a server run by host providers. Special usernames and passwords enable us to upload, to download and to work with our data whenever we have connection to the internet.

In doing so, we benefit from a larger volume of data storage and are no longer bound to our personal storage device but have flexibility, gaining access to cyber-space wherever internet-access is available. The issue is however, whether authorities are allowed, when having seized a device, to use it to gain access to the external database of the entitled user. This technique is called 'online investigation light'. Though a legal basis for it is usually found in the national procedural laws, the authorities typically lack the login data – the virtual keys – to gain access to the external storage-space. Are they therefore allowed to use spyware or cracking-tools to obtain them?

The answer to this question depends on the particular applicable national law. Key issues in this context are the principles of subsidiarity and proportionality of such invasive measures. Both principles are uncontroversial elements of every liberal legal constitution, insofar as they have gained international significance. Accordingly, they are found in every legal order – even when they are implemented in different ways. But what do they mean in the context of the lawfulness of the application of cracking-tools? They require questioning the affected person for disclosure of the login data before running such programs on a seized computer because an interrogation guarantees transparency: due to the hearing it is obvious for her or him that the authorities are going to enter her or his external database. If the requested person *then* keeps silent, the authorities may apply their spyware.

In contrast, *without* any prior interrogation, the investigation – cracking the login data and gaining access to the external data-storage – is executed undercover. This is, like any undercover measure, more invasive than open proceedings. In terms of subsidiarity and proportionality, therefore, the *open* investigation takes preference. As such, applying cracking-tools or any other spyware *without* informing the affected person through prior interrogation will be only allowed if the authorities have reason to expect that otherwise relevant data will be lost.

II. Access to the external database without using the seized devices: 'genuine' online investigation

Occasionally, the law enforcement authorities know the personal codes for the external database, but they have obtained them independently from a particular device, by a witness, for example, or by the application of specific spyware. Using this login data, they are able to pose virtually as the authorized person, entering his

storage-spaces and social media platforms. These investigation measures are discussed as classical online investigation.

First, the authorities can gain access to the external dataset *statically*[2] by looking only once into the i-cloud, the dropbox, the storage-space given by a host-provider, the mailbox, the bank accounts etc of the affected person. In doing so, they obtain all data stored at the time of their scanning, all *previous* e-mails, text-files, money transfers of the entitled user included.

Secondly, by applying the login data of the affected person, the authorities have the possibility to investigate *dynamically.*[3] According to this approach they could gain access repeatedly, observing any change of the databases: the incoming and outgoing e-mails, the current bank account activities, additional documents which the user stores into his i-cloud, his server-space etc.

This kind of investigation – using login codes without previous seizure of any IT-device – is considered as an even more invasive measure: without the act of seizure, the affected person has no reason to expect any disclosure of his data by the law enforcement authorities – her or his data are scanned undercover. Therefore, the legitimacy of all these kinds of online investigation is discussed controversially. In short, according to the German criminal procedural law neither the static nor the dynamic way of online investigation is allowed.[4] Hence, entering an electronic database is still bound to the particular seized device of the entitled user. In some other states, however, we might find rules allowing online investigation. To sum up, we have to consider crucial differences between national legal orders. Differences between national legal orders lead us to the sequence of problems which are related to transnational investigations.

B. Transnational Access to Electronic Data

I. Transnational access to data beyond mutual legal assistance?

So far, we have discussed the situation that electronic data is stored in external storage-spaces. If this external storage-space is physically located in the state which runs the investigation we have only to apply its national legal order. But this is rare – often the server where the data are stored is abroad. When under these circumstances the law enforcement authorities gain access to the external data-base, they need to make sure they respect the sovereign powers of the state where the server is domiciled.

Let us consider what the cybercrime convention of the Council of Europe offers as a solution. This convention starts off quite conventionally: it binds the *transnational* access to data to mutual legal assistance. As such, the state which seeks

[2] *Buermeyer*, Die Online-Durchsuchung. Technischer Hintergrund des versteckten hoheitlichen Zugriffs auf Computersysteme, 4 HRRS 2007, p. 154, (p. 160).

[3] Ibid.

[4] Ibid., pp. 165-166, *Zimmermann*, Die europäische Ermittlungsanordnung- Schreckgespenst oder Zukunftsmodell für grenzüberschreitende Strafverfahren?, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2015, p. 143 (p. 143).

particular electronic evidence located in another state has formally to request mutual legal assistance from this particular state. Only in two special situations the convention provides for a competence for a direct transnational access: One exception is applied to data which are public anyway.[5] This is ruled in Art. 32 paragraph a. of the Convention, stating that each Member State 'may, without the authorisation of another Party … access publicly available (open source) stored computer data, regardless of where the data is located geographically'. In most cases, however, openly available data are not the really interesting ones – evidence for a criminal law investigation usually is stored secretly.

A second dispensation from mutual legal assistance is found in Art. 32 paragraph b. of the convention. It allows each Member State to 'access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.' In such cases it is obviously assumed that no coercive measure is executed so that the key characteristic of a sovereign acting is no longer given.[6]

But when the legally authorised person, who is affected by the investigation, does *not* agree to the disclosure of her or his data, not even the cybercrime convention dispenses from a formal request for mutual legal assistance nor does it provide for any urgent procedure. The outcome of this is that the accused person or any involved person can delete any evidence within a couple of minutes from any internet access. Even a request for mutual legal assistance for the purpose of just provisional *freezing* of the particular data, which is provided by Art. 29 of the cybercrime convention, would usually be too late.[7]

Of course, it is worth considering, whether transnational access to a database is really an intrusion into sovereign powers.[8] After all, the invasion into the external database is executed solely from the state where the executing authority is domiciled and therefore without entering the foreign state physically. The affected user is in general authorised to disclose her or his (external) data to any third person. So the individual rights of the *provider,* who runs the server in the foreign state, are not affected by the access of the authorities; he has no legal interest in the data as such. Therefore, the authorities of the state where the disclosure of the external database is executed have not affected any individual right in the foreign state where the server is located.[9] On the other hand, the cybercrime convention is not based on

[5] LR/Tsambikakis, 26. Vol. 2014, § 110 Rn. 9.

[6] *Brodowski/Eisenmenger*, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden – Sachliche und zeitliche Reichweite der „kleinen Online-Durchsuchung" nach § 110 Abs. 3 StPO, Zeitschrift für Datenschutz (ZD) 2014, p. 119 (p. 123).

[7] *Zerbes/El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, Neue Zeitschrift für Strafrecht (NStZ) 2015,p. 425 (pp. 430-431), *Gaede*, Der grundrechtliche Schutz gespeicherter E-Mails beim Provider und ihre weltweite strafprozessuale Bewachung, Strafverteidiger (StV) 2009, p. 96 (p. 101).

[8] See for example, *Soiné*, Fahndung via Internet – 1 Teil, Neue Zeitschrift für Strafrecht (NStZ) 1997, p. 166, (p.167).

[9] *Zerbes/El-Ghazi*, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, Neue Zeitschrift für Strafrecht (NStZ) 2015,p. 425 (p. 431).

this idea; otherwise, the two exceptional cases in which no mutual legal assistance is necessary would hardly be necessary.

II. Traditional mutual legal assistance: 'locus regit actum' as a leading principle

We are still, therefore, bound to mutual legal assistance. This means that the state which runs the investigation has formally to transmit a request for data-seizure and data-transfer to the state where the data are located physically. The traditional law[10] of this process – the mutual legal assistance process – is bound to a principle which is closely connected with national sovereignty: it is the principle of *locus regit actum,* according to which the *requested* state performs the requested investigative measure pursuant to *its* law. In other words, the state in which the evidence is collected and whose national authorities execute the corresponding investigative measure thereby determines the rules applicable to this investigation: the limits of proportionality, the right to be present and to participate, the right to refuse cooperation such as, for example, the right to refuse to testify, all formal requirements such as, in particular, the requirement of judicial authorisation.[11]

Applied to transnational access to electronic evidence this means that all measures of disclosure are executed by the national legal order of the state where the data are physically stored. Therefore, the affected person has all individual rights according to the national legal order of the requested state: she or he is to inform about the access to the database by the authorities if the legal order of the requested state provides for such a transparent proceeding; she or he can refuse the disclosure of the data if she or he has such a right in the requested state, for example, based on professional secrets which are particularly protected.

Considering each *individual prosecutorial action* in isolation, this principle – the locus regit actum principle – always protects the particular local law of criminal procedure of the *requested* state: its authorities apply *their* domestic law alone. As such, the coherence of the *entire* prosecution is affected, sometimes to the detriment of individual rights, since the main trial will take place later in the *requesting* state – it is *its* investigation for which it has posed the request. There, evidence will be presented that was collected according to foreign law (the law of the requested state); there will occasionally be evidence that – although it would have been admissible where collected – would be illegal from the perspective of the law of the trial court.[12]

[10] E.g. CoE-European Convention on Mutual Assistance in Criminal Matters from 20 April 1959, Art. 3 I: The requested party shall execute in the manner provided for by its law.

[11] *Zerbes*, Collecting and Using Evidence: a Patchwork of Legal Orders, in: European Criminal Policy Initiative (ed. by Petter Asp), The European Public Prosecutor's Office- Legal and Criminal Policy Perspectives, p. 210 (p. 216), *Heger*, Perspektiven des Europäischen Strafrechts nach dem Vertrag von Lissabon, 8 ZIS2009,p. 547, (pp. 552-553).

[12] *Zerbes*, Collecting and Using Evidence: a Patchwork of Legal Orders, in: European Criminal Policy Initiative (ed. by Petter Asp), The European Public Prosecutor's Office- Legal and Criminal Policy Perspectives, p. 210, (p. 217), *Gless*, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung, pp. 114-115, *Mangiaracina*, A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order, Vol. 10 Utrecht Law Review2013, p. 113 (p. 115).

In light of this inconsistency between the investigation stage and the trial stage, both phases of the proceedings should be conducted according to one and the same system and thus an overall balanced proceeding could be achieved. To meet this challenge, a different principle has been established: the *lex fori* approach, according to which the place of the main trial proceeding determines not only the applicable rules for the *main trial* stage but also for the preceding *investigation* stage.[13] This approach is discussed as following.

III. Mutual legal assistance within the European Union´: 'forum regit actum' as a future principle

The principle of *forum regit actum* it finally prevailed in the Directive on the European Investigation Order (EIO[14]) – even if only as an optional provision[15] (Art. 9 para. 2 EIO) – and thus it will finally determine almost all actions of transfer of evidence between the EU Member States.[16] It is based on the principle mutual recognition of judgments and judicial decisions which at the Tampere-summit has been imposed as a 'cornerstone' of the future judicial cooperation within the Member States of the European Union. The core idea is – quite roughly explained – that in mutual legal assistance matters a judicial decision of one member state is to be executed in each other member state as such and in principle without any substantive review by the authorities of the executing state.[17]

In this context – the requested measures are to recognize and execute – the principle of 'forum regit actum' is obvious. According to this principle, the Member State in which the evidence will be used in court and will, therefore, have an influence on the judgement – the so-called *issuing* state of an European Investigation order – can (co-) determine the 'formalities and procedures' (Art. 9 para. 2 EIO) applicable to the investigation to be executed abroad through the *executing*

---

[13] *Zerbes*, Collecting and Using Evidence: a Patchwork of Legal Orders, in: European Criminal Initiative (ed. by Petter Asp), The European Public Prosecutor's Office- Legal and Criminal Policy Perspectives, p. 210, (p. 217), *Allegrezza*, Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility, 9 ZIS 2010, p. 569 (p. 578).

[14] Directive regarding the European Investigation Order in criminal matters, OJ 2014 L 130/1; the idea is not entirely new as it was already established in the EU Convention on Mutual Assistance in Criminal Matters between the Member States of the EU from 2000 (Art. 4), OJ 2000 C 197/1.

[15] In so far critics by ECPI, A Manifesto on European Criminal Procedure Law, 11ZIS 2013, p. 430 (p. 435).

[16] *Zerbes*, in: European Criminal Policy Initiative (ed. by Petter Asp), The European Public Prosecutor's Office-Legal and Criminal Policy Perspectives, p. 210, (p. 217), *Zimmermann*, Die Europäische Ermittlungsanordnung – Schreckgespenst oder Zukunftsmodell für grenzüberschreitende Strafverfahren?, (ZStW) 2015, p. 143 (p. 148), *Ahlbrecht*, Die Europäische Ermittlungsanordnung – oder EU-Durchsuchung leicht gemacht, Strafverteidiger (StV) 2013, p. 114 (p. 116), *Böse*, Die Europäische Ermittlungsanordnung – Beweistransfer nach neuen Regeln? 4 ZIS 2014 p. 152 (p. 152), *Bachmaier Winter*, European Investigation Order for Obtaining Evidence in the Criminal Proceedings – Study of the Proposal for a European Directive, 9 ZIS 2010, p. 580 (p. 583).

[17] *Zimmermann*, Die Europäische Ermittlungsanordnung – Schreckgespenst oder Zukunftsmodell für grenzüberschreitende Strafverfahren ? Zeitschrift für die gesamte Strafrechtswissenschaft(ZStW) 2015, p. 143 (pp. 146 ff.), *Schuster*, Die Europäische Ermittlungsanordnung – Möglichkeiten einer gesetzlichen Realisierung, 6 Strafverteidiger (StV) 2015, 393 (pp. 393-394), Bachmaier Winter, European Investigation Order for Obtaining Evidence in the Criminal Proceedings- Study of the Proposal for a European Directive, 9 ZIS 2010, p. 580 (pp. 581-582), *Mangiaracina*, A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order, Vol. 10 Utrecht Law Review (2013), p. 113 (p. 116).

state. Such a principle is convincing to the extent, that firstly the *collection* and secondly the later *admission* of evidence, result from one and the same code of criminal procedure. The legal detriment arising from a kind of 'patchwork proceeding'[18] – the combination of evidence collected according to the provisions of state A and then admitted in State B – could thus be avoided.[19] Evidence collected abroad pursuant to legal assistance would be gathered in such a way – particularly in guaranteeing the rights of the individual – that it could be used by the trial court without complication.[20]

The binding nature of the foreign law in the executing state of the EIO is not absolute: For its legitimisation it requires a clarification in favour of the binding nature of certain individual interests. In other words, despite of the application of the foreign legal order in principal, it is necessary to protect certain fundamental rights, upon the protection of which the individual in the executing state must be able to rely and which have priority over the principle of efficiency of (cross border) prosecution.[21] Hence, the Directive on the European Investigation Order limits its *lex fori* approach.[22] In particular, it respects the national *ordre public*: The executing state is not required to comply with standards of the issuing state that are 'contrary to the fundamental principles of law of the executing State' (Art. 9 para. 2 EIO).

As a second consideration, 'immunities' and 'privileges' (Art. 11. para. 1 lit. a) anchored in the national law of the executing state could stand in the way of executing an EIO. This relates primarily to the principle of confidentiality applying to certain professions (lawyers, doctors, journalists etc.), which lead to rights to refuse to testify and to prohibitions of confiscation. Practitioners of such professions must not, therefore, fear being forced to disclose professional secrets pursuant to a legal order other than that of the legal system in which they practise.[23]

Thirdly, certain limits on proportionality concretised in the executing state are protected from being disturbed by a divergent understanding in the issuing state. The executing state can refuse the execution of an EIO if the requested measure is only permissible in the executing state in case of an explicitly enumerated serious

[18] ECPI, A Manifesto on European Criminal Procedure Law, 11 ZIS 2013, p. 430 (p. 435).

[19] *Zerbes*, Collecting and using evidence in: European Criminal Initiative (ed. by Petter Asp), The European Public Prosecutor's Office- Legal and Criminal Policy Perspectives, p. 210, (p. 217).

[20] ECPI, A Manifesto on European Criminal Procedure Law, 11 ZIS 2013, p. 430 (p. 435); *Gless*, Grenzüberschreitende Beweissammlung, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2013, p.573, (pp. 590 ff.), *Zimmermann/Glaser/Motz*, Mutual Recognition and its Implication for Gathering of Evidence in Criminal Proceedings: A Critical Analysis of the Initiative for a European Investigation Order, EuCLR 2011, p. 56 (p. 72), *Heger*, Europäische Beweissicherung- Perspektiven der strafrechtlichen Zusammenarbeit in Europa, 14 ZIS 2007, p. 547 (p. 553).

[21] *Gless*, Grenzüberschreitende Beweissammlung, in: ZStW 2013, p. 573(603), Gless, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung,Baden-Baden 2006, p. 117, *Heger*, Europäische Beweissicherung-Perspektiven der strafrechtlichen Zusammenarbeit in Europa, 14 ZIS 2007, p. 547 (p. 553).

[22] In particular *Böse*, Die Europäische Ermittlungsanordnung – Beweistransfer nach neuen Regeln? ZIS 2014, pp. 156 f.

[23] See e. g. *Schuster*, Die Europäische Ermittlungsanordnung – Möglichkeiten einer gesetzlichen Realisierung, Strafverteidiger 2015, p. 393 (pp. 396 -397), *Zimmermann*, Die Europäische Ermittlungsanordnung – Schreckgespenst oder Zukunftsmodell für grenzüberschreitende Strafverfahren?, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2015, p. 143 (p. 153).

offense and the applicable investigation order is not based on such a suspicion (Art. 11 para. 1 lit. h).

Let us look at what this actually means for the exchange of electronic data based on the European Investigation Order. In the first place, this means that the freeze, seizure and transfer of the database is, in principal, executed according to the law of the issuing state which runs the investigation; as such, the executing state has to apply a foreign legal order. Secondly, the application of the foreign legal order is limited by fundamental rights provided for by the legal order of the executing state. Certain individual privileges, such as the protection of certain professional secrets, remain indispensable.

This is the current compromise between coherence of the entire procedure and the protection of essential rights. It remains to be seen if this will work.