# Classification of Electronic Data for Criminal Law Purposes

**Claudia Warken**

eucrim
European Law Forum: Prevention • Investigation • Prosecution

## ABSTRACT

Although the significance of electronic evidence for criminal investigations of any type of criminal offence has been steadily growing for years, respective legal frameworks in all EU Member States are only fragmented – if they exist at all. There is an urgent need for comprehensive legislation that takes into account the various grades of data sensitivity. For various reasons, the common distinction between subscriber data, traffic data, and content data is not suitable for this purpose. Instead, a new classification is necessary.
The article analyzes the relevant backgrounds and provides an overview of the current issues. More importantly, it proposes a new classification with five categories of electronic data. The key criterion for determining the sensitivity of a dataset – the data subject's reasonable expectation of confidentiality – allows a distinction as follows: (1) data of core significance for private life, (2) secret data, (3) shared confidential data, (4) data of limited accessibility, and (5) data of unlimited accessibility.
The article further shows that the newly proposed classification is comprehensive and technically neutral – thus, future-proof. In addition, it explains why the approach presented is solidly based and most suitable for legislative purposes, since it derives solely from the specifically affected fundamental rights.

## AUTHOR

**Claudia Warken**

Judge
Regional Court (Landgericht) Ulm, Germany

## CITE THIS ARTICLE

Warken, C. (2018). Classification of Electronic Data for Criminal Law Purposes. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2018-023

Published in eucrim 2018, Vol. 13(4) pp 226 – 234

https://eucrim.eu

ISSN:

# I. Theses[1]

Electronic data have become increasingly relevant as evidence in criminal investigations. Yet, there are – if any – only fragmented legal frameworks on European or national levels in the Member States of the European Union targeting the specific challenges posed by this unique type of evidence. Thus, there is a need for comprehensive and coherent legislative solutions on different levels.

The conditions and safeguards of different investigation measures depend on the intrusiveness of the respective measure. In the context of electronic data, the intrusiveness of a measure can vary widely. This has to be taken into account in the development of any legislative approach by means of an appropriate classification of the data. The common distinction of communication data, generally resulting in a classification of content data and non-content data or content data, traffic data and user data, does not meet the requirements of modern legistics.[2] The required classification has to reflect the sensitivity of specific types of electronic data. Thus, it should solely be based on the affected data subject's fundamental rights. The key criterion for determining the sensitivity of a dataset is the data subject's reasonable expectation of confidentiality.

It allows a classification as follows (in order of decreasing sensitivity): data of core significance for private life, secret data, shared confidential data, data of limited accessibility, and data of unlimited accessibility. The following sections further discuss this statement.

# II. Relevance of Electronic Data as Evidence – Specific Characteristics

Electronic data are increasingly relevant as evidence in criminal investigations. According to the common understanding, the term refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system.[3] These data play a significant role, e.g. where perpetrators communicate electronically or where the mere possession of an electronic device can provide location data for exact and specific times. In addition, it has been observed over the last few years that electronic data are not only relevant in the context of classical cybercrimes such as DDoS hits or ransomware attacks but also in the context of traditional offenses, such as fraud or child sexual abuse, which are more and more frequently committed through the internet.

Furthermore, the rapidly expanding use of electronic devices, e.g. for work-related and private purposes, for mobile communication, or in the Internet of Things, where devices exchange information through the internet directly, has led to the phenomena of Big Data – large amounts of information stored in electronic form and potentially relevant as evidence.

Electronic data for use as evidence in a criminal investigation can be obtained from the victim, the suspect, or any third party who, in most cases, is a service provider whose service refers to the creation, transmission, and/or storage of the data. Law enforcement can obtain the data through open or covert measures: A house search, including the seizure of electronic devices, such as a mobile phone or a laptop, is an example of an open investigation measure, while the interception of a mobile communication, for instance, is usually conducted in a covert way.

Because electronic data are intangible – they are nothing more than a processable sequence of zeros and ones –, they show characteristics that are not comparable to those of other, tangible evidence.[4] In contrast

https://doi.org/10.30709/eucrim-2018-023

to physical things, the handover of electronic data usually does not imply a loss of control; on the contrary, the data possessor usually keeps the original dataset and only transfers a copy of it – either electronically, on a data storage device, or as a printout on paper. From a technical point of view, electronic data can generally be accessed (and thus be obtained) from anywhere in the world as long as they are accessible through the internet; the necessary act for their seizure does not have to take place at the concrete data location. Concerning the acquisition of electronic data, time is a crucial factor, not only because this evidence can be transmitted with literally nearly speed of light, but also because such transmission can be carried out irrespective of any national borders. Last but not least, compared to physical things, it is much easier to create and process electronic data anonymously; traces in the virtual cyberspace can be hidden much better.[5] Once law enforcement has obtained electronic data that are potential evidence, they usually have to be converted into a compatible, readable format for further processing. This implies the risk of intentional, unintentional, and even unnoticed manipulation of the original information.

# III. Existing Legal Frameworks (Criminal Law)

Even though electronic data show unique characteristics that have a significant impact on their availability and admissibility as evidence, only a few legal frameworks exist and they take only some of the specifics into account. Even where specific legal provisions of criminal procedure exist, the legal landscape on European level as much as on national levels in the European Union, the USA, and other "Western" countries is fragmented. There is no comprehensive set of rules addressing these specific issues. Like in other EU countries, the German Code of Criminal Procedure,[6] lacks explicit regulations, e.g. on the acquisition of electronic data from any third party who is not a telecommunication service provider,[7] on the acquisition of machine-to-machine information, on preliminary measures for data preservation ("quick freeze"), on the handling of large amounts of Big Data, and on procedures to guarantee and confirm the integrity and authenticity of a dataset. As in other jurisdictions, existing provisions referring to tangible pieces of evidence are applied in order to fill gaps – a questionable approach in the sensitive area of criminal law.

Although there is a cross-border aspect in many cases referring to electronic evidence, it is often unclear how a provider who offers service in a country without having any physical assets there should be dealt with.[8] It is also unclear whether a request for data disclosure should be served in the country where the service provider has its headquarters or, if different, rather in the country where the data are stored.[9] Unsolved issues of jurisdiction arise, e.g. if a multi-national botnet is used to commit a DDoS attack in one country, if several perpetrators who are located in different jurisdictions act together, or if a number of victims in different countries are affected through one offense.[10] In addition, the problem of "loss of location" – electronic data stored abroad and, at the same time, accessible from home – is being discussed controversially.

The current general opinion seems to favor prohibiting the domestic investigator from processing such data, due to the assumed violation of the other state's sovereignty that such an act would cause. The same seems to apply to the situation involving "loss of knowledge of location," where it is not even clear where the data are located. Thus, they could well be stored domestically so that there would be no cross-border situation at all; still, the potential risk of violation of another country's sovereignty would prevent the investigator from using these data.[11] Preliminary cross-border data retention is regulated only between EU Member States,[12] and there are no comparable instruments concerning other countries. Last but not least, open questions remain when service providers who operate internationally find themselves in situations of conflicting law, e.g. when the disclosure of certain data is requested by one country and a compliant disclosure would violate another country's data protection laws.

https://doi.org/10.30709/eucrim-2018-023

In a nutshell, there is a lack of legislation – both quantitatively and qualitatively. Only recently, legislators have begun to tackle the issues, leading, for example, to the European Commission's proposal on access to electronic evidence in criminal investigations of April 2018[13] or to the Council of Europe's current discussion on an additional protocol to the Convention on Cybercrime. On the national level, provisions allowing remote evidence gathering through the internet have been introduced lately e.g. in Belgium, Germany and Austria while the US CLOUD Act of March 2018 specifically aims at data "in the cloud". Still, these approaches cover only some of the problems. The lack of clear and reliable normative concepts in criminal investigations endanger legal certainty and jeopardize the fundamental rights of affected persons.

# IV. General Legistic Requirements

The right of equal treatment is a fundamental right generally accepted in all modern "Western" legal frameworks. In the simplified words of the German Constitutional Court, it calls on the legislator and law enforcement to treat equal cases equally and unequal cases unequally unless there are reasonable grounds to deviate from this rule. Accordingly, deriving from the fundamental right of equal treatment and depending on the object of a concrete investigation measure, there is a general understanding that different conditions and safeguards may apply. Thus, the search of a home follows different rules than one for a bag on the street, even though both objects are physical things that belong to an individual. Obviously, the search of a home and that of a bag on the street are considered unequal cases because the intrusiveness, e.g. regarding the fundamental right of privacy, is higher in the first scenario than in the second one. This example indicates that the level of interference with the respective fundamental right(s) is an appropriate criterion by which to group and to distinguish cases or, in other words, to determine whether cases are equal or unequal.

That is nicely said, yet it provokes the next question of how the level of interference with fundamental rights is determined or, in other words, what the appropriate criteria for the differentiation are. Why exactly is a home considered more private than a bag on the street? What is the concrete reason for this legal distinction? Many national constitutions even ban certain aspects as distinguishing features at all.[14] Outside this banned scope, there are many possible options at the discretion of the legislator.

# V. Classifying Electronic Data – Traditional Approach

Consensus exists that there is a wide range of potential interference with fundamental rights through the acquisition and the use of electronic data in a criminal investigation. It is further commonly agreed that this broad range of potential intrusiveness calls for a set of possible measures with different conditions and safeguards. As referred to above, for instance, acquiring the content of the mobile communication of a lawyer and his/her client is legally not equal to acquiring the content of a communication in an open internet chat; the first example is considered much more sensitive than the second one. There are many more examples which reflect the general assumption that the sensitivity of one dataset is not always identical to the one of another dataset – even if both could be grouped, for example, as personal communication content information. Cases differ; they may be unequal.

In addition, there are apparently no reasonable grounds for treating the unequal cases equally. The general sense of justice requires communication with a lawyer and communication in an open chat to be treated differently. Thus, for constitutional reasons and based on the fundamental right of equal treatment, a differentiation of electronic data is an indispensable requirement for any comprehensive legal framework tackling the issue. There is currently no structural approach of how to differentiate electronic data comprehensively. Only regarding communication data different levels of sensitivity are assumed, leading to a

https://doi.org/10.30709/eucrim-2018-023

distinction between content data and non-content data (or metadata), while non-content data are sometimes further broken down into user data (or subscriber data) and traffic data.[15]

This differentiation is widely acknowledged. It derives from the transition of classical telecommunication providers from analogue to digital networks in the early 1990s. For billing purposes, the companies had to rely on the data provided in the service contract, such as the name of the subscriber and his/her address, and the monthly bill was invoiced in paper form. In addition, the details of the concrete service, such as the destination and duration of a call (today's traffic data), had to be documented in order to provide proof in case of disagreement about the billing. Lastly, and different than today, the content of a communication was of no relevance for the involved service provider. Having its origin in the practical needs of service providers, the traditional differentiation subsequently found its way into legal frameworks concerning data protection and criminal procedural law.

Irrespective of whether it was compliant with legal requirements in the past, the traditional differentiation used today is no longer suitable anymore with regard to modern communications. Especially in the context of social media and open chat fora, the content of a communication can no longer automatically be assumed more sensitive than non-content data that the user does not want to share publicly. In addition, the needs of the service providers involved have changed significantly. They no longer need to possess the traditional user data, e.g. when pre-paid services are offered, and often, parameters like the duration of a call via an internet application, such as Skype or WhatsApp, are of no relevance for billing. In fact, the user increasingly does not have to pay for a service with an amount of money based on the amount of service delivered. Instead, the user agrees (with more or less awareness) that his/her personal data will be given in exchange for the service. These data might include the content of a communication which is of high economic value because it can be sold, analyzed, and ultimately used e.g. for tailored advertising.

To add to the complexity of the problem, the common distinction of communication data refers to the same wording internationally; yet, due to the technical expansion of communication means, the terms are often used with slightly different but relevant different meanings.[16] Apart from concerns emerging from the traditional distinction of communication data, major classification gaps remain regarding all non-communication data. This affects not only the machine-to-machine exchange of information, which is increasing significantly with the growth of the Internet of Things and which covers everything from most sensitive to most trivial data and also any data that are not shared but only stored on the user's device or "in the cloud."

Thus, the traditional model of classifying electronic data has served its time. A new approach must be taken.

# VI. Classifying Electronic Data – Current Discussion

The required re-classification of electronic data for criminal purposes should ideally fulfil several conditions in order to allow "good" legislation: Firstly, it should aim at covering all potential electronic evidence. The classification should be comprehensive in order to avoid legislative gaps. Secondly, the classification should be technically neutral. Only then can the solution be future-proof. That is especially true in the rapidly developing cyber area, where specific technical issues may have become irrelevant by the time a referring legislation is finally adopted and implemented. Ultimately, the classification should follow an abstract structure and avoid any catalogue listing. Even if a list of detailed types of data seems to facilitate their handling at first glance, such a list would be likely to miss one or the other type – if not from the outset, then possibly after a short time, as no legal amendment procedure can keep up with the rapid technical developments in IT. In addition, a catalogue listing would likely blur the actual differentiator – if there is an appropriate one, it should simply be named.

Taking these premises into account, it needs to be determined what exactly constitutes the sensitivity of electronic data. Aspects which, generally have an impact on the intrusiveness of any investigation action – namely whether the measure is open or covert, its duration, or the number of people affected – should be considered when it comes to the proportionality test of the measure. However, they do not play a role for the classification as such.

Various approaches are currently discussed about how to determine the sensitivity of electronic data best. The main problem is the identification of the criteria which determine their sensitivity. In short, the following criteria are under discussion, both separately and in combination with one another:

## 1. The content of the data

This criterion is reflected in the traditional distinction of communication data, where the content of a set of data refers either to the content of the communication itself or to metadata that is created through the processing of the data. The flaws of this approach are described above. In particular, it can no longer be assumed that the content of a publicly shared communication is more sensitive *per se* than, for example, location data that the user wishes to hide. It depends on the individual circumstances – therefore, referring to the content of a set of data is not a suitable criterion for a general classification. In addition, referral to the content of a set of data would cause practical problems at the very least when intercepted or retrieved stored data are concerned: determining the content would first require obtaining and inspecting the data, which might only be allowed for certain types of content.

## 2. The amount of data collected

This aspect raises not only technical issues: What amount of data is considered appropriate for differentiation? How to deal with situations where the data to be obtained are unknown in advance? It also rules out the premise of technical neutrality that the classification should follow. In addition, it cannot be assumed that a small amount of data is generally less sensitive than a larger amount. Thus, the amount of data is not an appropriate criterion for classification purposes. Nevertheless, it is of significant relevance for the proportionality test of any concrete measure that is applied.

## 3. The technical origin of the data

In order to determine the sensitivity of a set of data, one could refer to its technical origin (e.g. an electronic document or a digital picture) or the underlying service (e.g. a mobile call, a video stream, or a mere storage in the cloud). Besides the fact that such an approach would not respect the condition of technical neutrality, there is no comprehensible reason why, for instance, a document should legally be treated differently than a picture. Thus, the technical origin of the data can be discarded as a criterion.

## 4. The processing state of the data

It is generally assumed that data in rest are more sensitive than data in transit. Although this assumption is not based on obvious legal reasons (there are strong arguments in favor of the opposite conclusion), there are legal provisions which are based on this differentiation and, accordingly, establish different investigation measures like real-time communication interception, on the one hand, and the seizure of a data storage device, on the other. Like the data volume criterion, the state of the data is not technically neutral. Current problems in this context occur concretely regarding cloud storage: from the user's point of view, his/her data are stored and "laid to rest" in the cloud while, in fact, the data are frequently processed (split, re-merged, duplicated, transferred from one server to another one, etc.) for security reasons. In practice, this makes it

https://doi.org/10.30709/eucrim-2018-023

almost impossible to determine the state of a set of data at the exact time when an investigation measure is to be applied. Furthermore, the applied differentiation is very broad because it provides only two groups. That is not sufficient for legal purposes, since there is no doubt that the sensitivity of stored data, e.g. on an USB-stick, can vary widely. Thus, referring to the state of the data is of little help for the required data classification.

## 5. Data protection law approach

Data protection law concerns personal data as opposed to non-personal data and differentiates further within the first category between sensitive and less sensitive data. The top-level differentiation between personal and non-personal data obviously applies to criminal investigation measures as well, as there is no need to legislate measures that do not affect a person (or even a large number of persons). However, this broad differentiation does not really help. The additional distinction division of personal data into sensitive and less sensitive data only targets data *about* a person and does not provide a classification of data *from* a person. Furthermore, the relevant criterion derives from the societal mainstream and is therefore not necessarily compatible with criminal law aspects.[17] Last but not least, such a distinction assumes that the content of a set of data is known before a measure is taken, which is not the case in many investigation measures. For these reasons, the approach of data protection law does not support a data classification for criminal law purposes.

## 6. Significance of the data for the investigation

Focusing on the significance of the data for the concrete investigation causes an unsolvable problem: in order to determine the significance of data, one can refer to the individual case or to comparable cases in general. Under the first option, the significance could only be determined once the investigation has progressed, thus, once the data have been obtained and used. At this point in time, the classification would not matter anymore. Under the second option, the statistical analysis would itself rely on a classification (or else the analysis would not make any sense), so the question of the appropriate criterion would remain unsolved. In addition to the practical issues, the data's significance for an investigation does not reflect the somehow person-related link to the sensitivity of a set of data; most useful data can be of marginal sensitivity and vice versa. Thus, this criterion should only be considered for the test of proportionality and, specifically, of the necessity of a concrete measure.

## 7. Offense concerned/applicable investigation measure

One could apply a scheme by which the seriousness of the offense concerned or the applicable investigation measure would determine the type of data that would be accessible. Thus, the more serious the offense or the less intrusive the applicable investigation measure (in general terms, i.e. an open measure, e.g., would have to be considered less intrusive than a covert one), the less strict the conditions and safeguards. However, that would not allow an originary classification of data and instead turn the legistic approach upside down: the classification is a pre-condition to determining conditions and safeguards and not the other way around.

Taking into account the flaws of each of the discussed approaches, there does not seem to be a feasible solution based on a combination of several of the criteria; all of them exhibit major problems. Thus, the current discussions do not provide a solid solution.

# VII. Classifying Electronic Data – A New Approach

What is instead needed in order to determine the criteria for a dataset's sensitivity, is a new line of thinking that takes into account the premises mentioned above – being comprehensive, technically neutral, and abstract as opposed to detail-listing – and focuses on legal aspects, namely on the fundamental rights of the data subject.

Looking at other provisions that deal with evidence in criminal procedural law, the focus on legal aspects is very common, e.g. information that can be obtained through physical interference or contact with a person. Here, the fundamental right of physical integrity is affected and, depending on how much it is affected, different investigation measures with different safeguards and conditions apply. The extent of physical interference is the key criterion for classifying the body-related evidence. It can range from minor (e.g. taking a person's picture or fingerprint) to more severe (e.g. taking a blood sample). Even beyond that, the grade of intrusiveness provides different categories of body-related information such as appearance, fingerprint, and blood count. The same applies to documents for which legal provisions have established the assumption of different levels of sensitivity that are derived from the affected fundamental rights.

In the context of electronic evidence, it is therefore necessary in a first step to determine the fundamental rights that are specifically affected, then to extract their key content, and thirdly to filter out the aspect that allows for a differentiation between minor and more serious interferences. Once that aspect has been carved out, it can be applied.

## 1. Relevant fundamental rights

There is a general understanding that the specific fundamental rights which concern electronic data encompass the right of respect for private life, the right of self-determination, and the right of secrecy of correspondence. Although the concrete interpretations may slightly differ (especially when they refer to very similar, yet not identical legal frameworks like the European Convention on Human Rights, the European Charter of Fundamental Rights, or national constitutions), there is still an overall agreement that the principles of the above-mentioned fundamental rights are the relevant ones.

## 2. Key content of the relevant fundamental rights

Concisely, the key content of the relevant fundamental rights regarding electronic data is the data subject's possibility to freely and independently decide what happens to his/her data – who should have access to them, with whom they are shared, etc. Electronic data might, for example, not be shared at all, be shared only with most trusted persons, or be shared publicly with an uncontrolled number of persons. Thus, the core issue of data-related fundamental rights relates to the confidentiality of the data.

## 3. Key criterion for differentiating the grade of interference

The grade of interference with the confidentiality of data depends on how much the free will of the data subject is respected: the more it is respected, the less interference. In other words, the more the data subject can reasonably expect that a set of data will remain confident, the more sensitive the data are. It needs to be stressed that, because of its derivation from individual fundamental rights, the sensitivity of electronic data depends only on the data subject; there is no room for allowing e.g. the legislator or society to decide what is sensitive for a specific individual.

https://doi.org/10.30709/eucrim-2018-023

These findings allow the following conclusions: First, whether a set of data is sensitive or not does not depend on the *status* of the data subject in the investigation; it is the same for the suspect, the victim, and the witness alike. Thus, the role of the data subject in the investigation is irrelevant for the classification of electronic data; it only requires consideration when it comes to the proportionality test of a concrete investigation measure.

- Second, the coincidental *processing state* of the data (whether it is currently being processed or not) does not matter for the classification of electronic data. The sensitivity, e.g. of the content of an electronic diary, does not depend on whether it is still on the laptop at home, in the process of being transmitted to the storage place in the cloud, or already stored there.
- Third, the level of *confidentiality* that can be reasonably expected depends on the circumstances of the specific case. There are two crucial aspects for its determination: the data subject's behavior (i.e. to what extent he/she shares the respective data) and his/her bond of trust with the person who receives the data. This bond of trust can be based on both actual and/or legal grounds, e.g. on the personal relationship between close friends or on a contractual agreement with a service provider. On the contrary, the content of the information does not play a key role for the confidentiality assessment; it may be an indicator, but nothing more.

# VIII. Applying the New Criterion of Reasonable Expectation of Confidentiality

The finding that the classification of electronic data has to rely only on the criterion of the data subject's reasonable expectation of confidentiality allows classifications of different granularities. In order to find a workable balance between the wide range of potential data sensitivity and the number of data categories, a classification with five categories is proposed. These are, in order of decreasing sensitivity: (1) data of core significance for private life, (2) secret data, (3) shared confidential data, (4) data of limited accessibility, and (5) data of unlimited accessibility.

## 1. Data of core significance for private life

The first category – the data of core significance for private life – refers to the *most private, inviolable data*; the reasonable expectation of confidentiality extends to the level of knowledge that the information will not be used as evidence in a criminal investigation.

## 2. Secret data

The category of secret data refers to additional electronic information that the data subject has not shared with anyone else or, alternatively, to data that have been transferred to a reliable, usually non-natural third party with the only intention that this party stores the data without gaining knowledge of its actual content, e.g. where a provider offers the automated service of cloud storage without any additional services. In both cases, the reasonable *expectation of confidentiality is very high*.

## 3. Shared confidential data

Shared confidential data has been shared with specifically trusted persons under the data subject's reasonable expectation that the information will not be distributed any further, e.g. with a spouse, a very close

friend, a lawyer or a doctor. Compared to secret data, however, there is an *increased risk that the information will be leaked*.

## 4. Data of limited accessibility

Data of limited accessibility is data that have been shared with one or a limited number of individuals who are not specifically trusted. This category takes into account that a controlled distribution of the data still indicates a certain will to maintain at least some confidentiality, while at the same time acknowledging that *the reasonable expectation that the data will not be shared further is rather limited*. It covers all communication metadata in the sense of the traditional classification, because the use of electronic means for communication inevitably depends on information like the recipient's contact data or the radio cell used. This information is available to the involved service provider(s) who generally cannot claim specific personal trustworthiness.

## 5. Data of unlimited accessibility

For information distributed publicly – or data of unlimited accessibility (e.g. on an open social media platform) –, there is *no reasonable expectation of confidentiality*. The same applies to data voluntarily shared with law enforcement authorities with the knowledge that the information might serve as evidence in a criminal investigation. Furthermore, it covers data that voluntarily and legally disclosed to law enforcement by a third party, at least if the third party has obtained the data in a legal way. The reason for including the last-mentioned alternative is the consideration that the confidentiality was breached through the act of a third party without pro-active support from any authority, and the materialized risk of voluntary disclosure by the informed third party is fully on the data subject`s side.

# IX. Résumé

The newly introduced approach allows a comprehensive data classification for criminal law purposes, which is urgently needed. It avoids the problem of defining communication data and closes current gaps.[18] The comprehensive classification facilitates an all-encompassing regulation that embraces all criminal investigation measures related to electronic data.[19]

Since it is solely based on the affected fundamental rights of the data subject and not dependent on, e.g. billing purposes of telecommunication service providers in the past, it is solidly based for legal purposes. For the same reason, the new classification of electronic data is also coherent with the existing classifications of other types of criminal evidence, e.g. documents or body-related information, both of which are also categorized according to the level of interference with the affected fundamental rights.

In addition, because of its technical neutrality, the new model is decoupled from future technical developments; it is future-proof. Furthermore, the questionable legislative differentiation between telecommunication service providers and over-the-top service providers becomes obsolete; when offering services that are identical from the user's perspective, they have to be treated equally.

The referral to abstract terms for the different categories avoids the flaws inherent to a detail-listing catalogue. One can assume that, with the knowledge of its legistic derivation, the courts would substantiate the various categories – as it has happened in the context of other abstract terms in criminal law.

https://doi.org/10.30709/eucrim-2018-023

# X. Outlook

This article focuses on criminal law, yet its derivation from the affected fundamental rights might allow further potential applications, e.g. regarding data retention or civil law. In practice, the approach can be directly applied where existing legal provisions do not address the issue of the required level of proof concerning the integrity and authenticity of electronic data that are to serve as evidence. The lower the level of sensitivity, the more easily a court could, in general, assume the integrity and authenticity of the data. In other words, the more confidential the data, the higher the required level of proof of their integrity and authenticity. Furthermore, until a comprehensive legal framework enters into force, the new model can serve the test of proportionality for any investigative measure that refers to electronic data.

Due to the comparable protection of fundamental rights in the "Western" world and specifically the European Union, the model could subsequently be applied in these countries as well. This would significantly improve the more and more frequently required international cooperation regarding the acquisition and exchange of electronic data as well as their admissibility in court.

While the new classification provides solutions, new questions also emerge. As mentioned earlier, the courts would have to substantiate some abstract legal terms, such as the "reasonable expectation" of confidentiality. However, this would only be a matter of time and is no issue of principle concern. Within the context of determining the reasonable expectation of confidentiality, the use of encryption could be considered an additional indicator, possibly depending on whether it is applied intentionally or by default through the service provider. Further issues arise in cases in which the data subject's behavior does not correspond to his/her expectation of confidentiality, e.g. where data are shared unknowingly or where a third party distributes the information without being allowed to do so.

Finally, it has to be clarified who the data subject is, e.g. in cases of machine-to-machine communication (any non-public information exchange eventually refers to at least one person), or when the data relate to a group of natural persons or a legal person.

These questions are not exclusive. Finding appropriate solutions requires a rethinking of how to approach potential electronic evidence. This article is meant as a first impulse to start the discussion.

---

1. The content of this article was extensively elaborated in German in the doctoral thesis submitted by the author to the Law Faculty of the University of Heidelberg, Germany in May 2018 under the original title "Klassifikation elektronischer Beweismittel für strafprozessuale Zwecke". The dissertation will be published in 2019.↩
2. The term „legistics" refers to the sum of all aspects that have to be considered by any law maker in order to create „good" laws – such as the principles of necessity and proportionality. It seems that the seldomly used term has been introduced by U Karpen, *Gesetzgebungslehre – neu evaluiert – Legistics – freshly evaluated*, Baden-Baden 2008. Accordingly, references are made to „legistic requirements" in this article, meaning those that should ideally be considered in any law making process.↩
3. See, e.g., Art. 2(b) of the Directive 2013/40/EU on attacks against information systems (O.J. L 218, 14.8.2013, 8) and Art. 1(b) of the Council of Europe's Convention on Cybercrime (ETS 185).↩
4. Traditional evidence includes persons (witnesses and experts) and physical things (objects for legal inspection such as documents, pictures, or real estate).↩
5. E.g., the use of proxy servers can hide concrete data transfers while user names, e-mail addresses, and other identifiers do not have to reveal any information about the persons behind them. Another major challenge for law enforcement in this context is the simultaneous distribution of identical dynamic IP addresses to up to several thousand users at one time.↩
6. Strafprozessordnung, StPO.↩
7. In most countries, the term "telecommunication service provider" refers to the traditional provider who is usually legally obliged to cooperate with law enforcement, whereas the new over-the-top service providers generally do not have to disclose available electronic data. This distinction is made even where identical data is available (e.g., when it comes to the IP address used for a concrete communication) or where, from the user's point of view, identical services are delivered (e.g., a mobile phone call without an additional user's application or via WhatsApp for instance). In Germany, the differentiating definitions of the respective service providers are found in the Telekommunikationsgesetz (TKG) and the Telemediengesetz (TMG).↩
8. This was one of the main legal questions in the *YAHOO! Inc. v Belgium* case (Hof van Cassatie of Belgium, 1 December 2015, case P.13.2082.N).↩

https://doi.org/10.30709/eucrim-2018-023

9. That was the key question in the so-called *Microsoft Ireland case* (Supreme Court of the United States, No. 17-2, 584 U.S. (2018)) in the USA, which was rendered moot by the US Supreme Court after the Clarifying Lawful Overseas Use of Data Act (CLOUD Act; H.R. 4943) was enacted in March 2018.↩
10. E.g., in May 2017, the WannaCry ransomware attack hit more than 300,000 computers across more than 150 countries within hours.↩
11. For more detailed information about „loss of location" and „loss of knowledge of location" see, e.g., B-J. Koops and M. Goodwin, *Cyberspace, the Cloud, and Cross-border Criminal Investigation. The Limits and Possibilities of International Law*, 2014; A.-M. Osula, "Accessing Extraterritorially Located Data: Options for States", in: M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, U. Sieber, "Straftaten und Strafverfolgung im Internet", *Gutachten C zum 69. Deutschen Juristentag,* 2012, C 77 and C 143; C. Warken, "Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil I", (2017) *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, 289, 295; M. Zoetekouw, "Ignorantia Terrae Non Excusat", Discussion Paper for the Crossing Borders: Jusrisdiction in Cyberspace conference – March 2016.↩
12. Existing general instruments are the European Investigation Order (Directive 2014/41/EU regarding the European Investigation Order in criminal matters, O.J. L 130, 1.5.2014, 1) and the European Freezing Order (Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence, O.J. L 196, 2.8.2003, 45).↩
13. The European Commission's e-evidence proposal of April 2018 ("Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters", COM(2018) 225 final – 2018/0108 (COD)) includes, e.g., "quick freeze" provisions and data disclosure obligations specifically designed for electronic data that would apply to any provider offering services in the EU, irrespective of the location of its headquarters or of the location of data storage.↩
14. In modern "Western" constitutions, e.g., the gender of a person, his/her religion, or his/her origin are inapplicable differentiators.↩
15. The term „communication data" is not legally defined. Thus, it remains unclear what exactly is covered.↩
16. E.g., machine-to-machine data exchange is not always considered communication data; information about the user's bank account is only sometimes covered by subscriber data; an IP address might be subscriber data or traffic data.↩
17. Data protection law considers, e.g., genetic and biometric data to be equally sensitive. In criminal procedural law, however, the use of genetic data, such as information about a genetic disorder, is much more limited than the use of biometric data, such as a fingerprint.↩
18. The doctoral thesis includes a table comparing different datasets and their categorizations in the traditional system (if any) with the newly proposed one; it also shows the practical and structural advantages of the new classification.↩
19. The doctoral thesis includes a concrete, comprehensive, and commented draft of how electronic data could be dealt with in the German Code of Criminal Procedure.↩



ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union