The (Future) European Electronic Evidence Delivery Order

Olga Fuentes Soriano
Miguel Hernández University

The Electronic Evidence Delivery Order is a legislative initiative of the European Union, currently in progress, which aims to create a specific procedural instrument to facilitate and speed up criminal investigations between the different Member States, in those cases - practically unavoidable today - in which digital information relevant to the clarification of the criminal commission comes into play.

Keywords: electronic evidence, criminal proceedings, criminal procedure, mutual recognition, judicial cooperation

INTRODUCTION

In recent times, encouraged by the transnational nature of criminal activity as well as by the need to consolidate the Area of Freedom, Security and Justice on which the European Union is built, we are witnessing a proliferation of procedural instruments that seek to establish certain channels of legal cooperation in order to promote and speed up the processing of cases and criminal investigations.

Common institutional mechanisms that have come into being in recent decades include, for *example, the European* arrest[1] warrant, the European evidence warrant and, finally, the European investigation order.

It is undoubtedly the latter that focuses the greatest hopes for success in the investigation (and evidence) of transnational crime; but the aforementioned European Investigation Order does not contain any reference to the specific practice of electronic investigative procedures that has become a key part of almost all criminal proceedings.

In view of the seriousness of many of the facts that can be accessed by means of electronic information - electronic evidence, therefore - their growing and exponential use and the specific characteristics of these, which require - or at least advise - individualised treatment, the European legislator is faced with the task of either reforming the 2014 Directive that regulates the European Research Order, to make room for them, or creating *ex novo* a regulatory instrument that takes into account these specific characteristics. His option, finally, has led him to opt for the latter possibility and, consequently, in 2018 the European Commission approved two important legislative initiatives aimed at tackling the always difficult cross-border gathering of evidence, especially significant when it is of a digital nature: The proposal for a Regulation on European orders for the surrender and preservation of electronic evidence for the purposes of criminal proceedings (COM (2018) 225 final, 2018/0108 (COD) and the Directive establishing harmonised rules for the appointment of legal representatives for the purposes of obtaining evidence in criminal proceedings (COM (2018) 226 final, 2018/2017 (COD).

The following pages will be dedicated to the study of some fundamental aspects that delimit the purpose and structure of the projected Order for the handing over of electronic evidence in criminal proceedings, leaving for another time, for reasons of space derived from participation in a collective work, the study of the Order for the conservation of evidence, also electronic, regulated in this same legislative project[2].

CONCEPT AND SCOPE

Article 2(1) of the Proposal for a Regulation governing the proposed European Evidence Warrant conceives it as a "binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence".

From the above definition, many aspects can be extracted which should be studied in depth in order to correctly define its concept and extension.

Firstly, the Delivery Order is conceived as a binding decision of a unilateral nature, which means that, effectively, once the Regulation has been adopted, any Member State may make use of it, thus obliging the recipient (service provider in another Member State) to comply with it. However, the proposal for a Regulation regulates the reasons for the recipient not complying with it; but, in principle and except for these exceptional situations, if the Order complies with the legal requirements established, its issuance directly binds the service provider to comply with it.

Secondly, the Electronic Evidence Delivery Order is a procedural instrument specific to the Union and its use is therefore restricted to Member States and, specifically, within them, to the issuing authorities or authorities recognised as having the capacity to issue such evidence - which will be analysed in the following section. The issue is by no means trivial because, precisely, the fact that the order for the handing over of electronic evidence is an exclusively European procedural resource will oblige us to seek new formulae for cooperation between the European Union and third States with regard to the taking of cross-border evidence. It is precisely in this context that the Recommendation for a Council Decision authorising the opening of negotiations for an Agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters of 5 February 2019 is[3] framed.

At present, the cooperation of the European Union States with the United States of America focuses on data without content. Content-free data' refers to data that provides information on, for example, subscribers or traffic to an online account, while 'content data' refers to, *e.g.,* e-mails, text messages, photos, videos, etc. Currently, the authorities of a Member State of the Union can address a request for non-content data to service providers located in the USA and, under US law, they are allowed to cooperate, always on a voluntary basis, by providing the requested data. This possible voluntary action creates a certain margin of legal uncertainty for the requesting European states and 'furthermore, in the words of the Explanatory Memorandum to the Recommendation for a Decision, it may be unreliable, may not respect the relevant procedural guarantees, is only feasible with a limited number of service providers all applying different policies, is not transparent, and lacks an accountability mechanism. The resulting fragmentation may lead to legal uncertainty, doubts about the legality of the process and concerns about the protection of fundamental rights and procedural safeguards of persons related to such applications[4]. The need, therefore, to establish channels of communication and action that favour the collection of electronic evidence between Europe and the USA -and that complement, in the corresponding area, the mechanisms for the collection of European cross-border evidence- is obvious, especially if we take into account that it is precisely there where the largest service providers in the world are based.

Thirdly, it is absolutely clear from the above definition that the European Delivery Order must be sent by - and from - one Member State to a service provider in another Member State. That is to say, that the Electronic Evidence Delivery Order must be sent exclusively for evidence of a cross-border nature, understood in this sense.

Fourthly and finally, the European Evidence Warrant applies exclusively to what we generically know as electronic evidence, understood as that which provides information on data stored, disseminated or processed electronically, whether or not it has content[5]. Article 2(6[6]) of the Proposal for a Regulation itself defines "electronic evidence" for the purposes of European Delivery and Storage Orders as "evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a European Delivery Order or European Storage Order certificate, consisting of subscriber data, access data, transaction data and stored content data"[7].

The fact that the processing of information relating to personal data is in any event carried out makes it possible to meet all the requirements of due respect for fundamental rights, over and above the[8] necessary compliance with all the Community rules on the protection of those[9] rights.

Finally, it should be noted, although it does not derive from the definition of a European order for the surrender of electronic evidence offered in Article 2 of the Proposal for a Regulation under analysis, that this order may only be used within criminal proceedings that have already begun. That is to say, those cross-border electronic evidences that could be relevant for the processing of civil, labour or contentious-administrative proceedings may not be requested directly by the interested State from the service provider established in another State by means of the referral of this legal instrument.

With the criminal field thus established, as well as the one in which the Order can develop, attention will be focused, from this moment on, on deepening other important aspects that contribute to the delimitation of its scope of application.

Firstly, it should be remembered that the fact that the European Evidence Warrant is a cross-border one means that the Warrant will only be applicable - and only addressable - to service providers that provide services in States other than the one that issues the Warrant. It can therefore never be used in national environments, no matter how much it is intended to collect data on subjects or communications across borders. The transnational nature of the evidence is marked by the place of establishment or connection of the service provider to whom the Order is addressed, who is, in short, the one who must comply with the Order and provide the required data. The different location of the service provider with respect to the State issuing the Order is what marks the transnational or cross-border nature of the evidence to be obtained.

Although the character of the service providers will be dealt with in greater depth in the following section, when dealing with the subjective requirements for the issue of a European Delivery Order, it is now appropriate to refer, in order to delimit the scope of the Order, to the different types of data that can be collected through it.

The Proposal for a Regulation recognises four types of data for whose delivery procedures it will establish relevant differential nuances, since the effect on fundamental rights will vary considerably depending on those to which the Order refers. The Proposal distinguishes between: 1) subscriber data; 2) access data; 3) transactional data; and finally 4) content data.

In view of the definitions in Article 2 of the proposed Regulation, 'subscriber data' shall mean any data pertaining to the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email; as well as any data concerning the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user.

“Access data" are data concerning the start and end of a user's access session to a service, and which are strictly necessary to identify the user of the service (*e.g.* the date and time of access, or connection and disconnection to the service, together with the IP address assigned to the user by the Internet access service provider, data identifying the interface used and the identification of the user). This area also includes electronic communications metadata[10]. The express reference to this type of data - access data - is striking as it is collected *ex novo* in the Proposal, thus separating this legislative instrument from the usual references in the legislation of the various European States which normally recognise the existence of only subscriber, transaction and content data. In any case and as will be seen below, data relating to

access have common characteristics with subscribers' data and this will allow, in many cases, to process them jointly.

The "transaction data" refers - as its name indicates to the concept that art. 2 of Proposal for Regulation provides - transaction data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. As foreseen for access data, this also includes electronic communications metadata as defined in the Proposal for a Regulation on privacy and protection of personal data in the electronic communications sector, referred to above. However, unlike access data (and subscribers' data) which do not provide any information about the subjects interacting with the user, transaction data allow obtaining information about the contacts and the whereabouts of the user, and can serve to establish the profile of an individual.

The data listed so far constitute what is known as "data without content" and which service providers may voluntarily hand over to the judicial or police authorities, always with due regard for the legal requirements arising from the necessary data protection.

These data without content are finally referred to as "content data" and refer to any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.

Although it is observed and as advanced, the first two types of data analysed (subscriber data and access data) tend to have the same objective; the common and basic objective of identifying the user. In this respect they differ significantly from the other two groups of data (transaction and content data) whose purpose is to add some additional information to that initial identification. Given the difference in information provided by the two groups, it is true that the interference they produce in fundamental rights and, therefore, the safeguards and requirements to be taken into account, will be very different in either case[11]. And this is always based on the consideration that, insofar as they affect - to a greater or lesser extent - the right to data protection, the whole of the Community legislative acquis aimed at that protection will be applicable to them.

The collection, delivery and processing of subscriber and access data is subject to less strict requirements than those applicable to transaction and content data, no doubt because of their greater sensitivity in the latter cases. In that sense, while for the issuance or validation of a European order for the delivery of subscriber data or access data it is foreseen to accept as sufficient the intervention of the competent prosecutor, the intervention of the judicial authority will always be required to obtain transaction and content data.

In parallel and for the same reasons, while the European order for the surrender of subscriber or access data may be issued for any kind of criminal offence, the order for the surrender of transaction or content data will be limited to a much more restricted objective scope.

Thus, the Proposal for a Regulation has sought formulas to limit the objective scope of electronic evidence delivery orders when they refer to data on transactions or content; and from among the classic option of attending to a criterion of quantitative penal limitation or a selection of cases of a qualitative nature (that is, attending to the *quantum of the* penalty or the punishable conduct) it opts, in sum, for a combination of both criteria.

It thus establishes, on the one hand - art. 5 4 (a)-, that an Electronic Evidence Delivery Order affecting transaction or content data will only be feasible when issued for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years.

And, together with this, on the other hand -art. 5 4 (b)-, it is admitted the valid issuance of these Orders of delivery of data when it is a question of the investigation and prosecution of the criminal conducts that it specifically determines, independently of the penalty with which they are sanctioned, provided that they have been committed through an information system[12]. Specifically, this concerns the commission of certain offences relating to fraud and counterfeiting of means of payment, sexual offences against minors, offences against information systems and terrorist offences[13].

THE AUTHORITY ISSUING THE ORDER

The legal reference to the issuing authority[14] (and not to the issuing State) involves determining, as a starting point, which institution or institutions are in a position to issue an Electronic Evidence Delivery Order. And at this point, the disparate regulation of the Member States -the different procedural systems in force in the Union-[15] will oblige us to formulate rules with a lax and premeditated vocation of generality from which to cover this diverse procedural reality.

Thus, and based on the distinction mentioned above between the lower requirements for obtaining subscriber data and access data, on the one hand, and the higher requirements for transaction and content data, on the other, the Proposal for a Regulation differentiates between the authorities to which it recognises competence to issue the Order in[16] one case or another.

Where data relating to access or subscribers are concerned, the issuing of the surrender order will be considerably less formal and may come from a variety of authorities which, however, are not covered when the other data are concerned. Thus, it may be issued - in the first case - not only by any judicial or prosecutorial authority but also by any other authority which in the State has been recognised as having competence in criminal investigations provided that, in the latter case, the order is validated after examination of compliance with the conditions for issue by a judge or prosecutor in the issuing State itself. The intervention of a judge or public prosecutor, either for the issuing or for the validation of a surrender order affecting access or subscriber data, will be necessary in all cases; but it should be noted that the intervention - the issuing or validation of the order - may come from the judge or public prosecutor.

However, in view of its greater impact on the fundamental rights at stake, a surrender order which relates to transaction or content data must be issued by a judicial authority[17]. There is no doubt that we are dealing with a clear express manifestation of the jurisdictionality required as a requirement for the limitation of fundamental rights.

In the light of the above proposal for a regulation, two points of view raised for improvement could be taken into consideration. On the one hand, that the absence of an express regulation allowing defendants to request a surrender order under the same conditions as those granted to the Public Prosecutor's Office has been seen by the European Lawyers as a clear attack on the principle of equality of arms between the prosecution and the defence, which places the defendant at a disadvantage[18]. And on the other hand, the possibility that the Public Prosecutor's Office may issue these orders, even when they refer to access or subscriber data, has been seen by the European Economic and Social Committee as a violation of European data protection legislation, thus making it appropriate that, in any case, they should be issued by a judicial authority[19].

THE ADDRESSEE OF THE ORDER

The recipient of the projected Electronic Evidence Delivery Order will be - with the nuances that will be seen below - the service provider from whom the requested data are required.

This is precisely one of the important new features of this regulation. The fact that the request for delivery is addressed directly to the person who has the data requested (without the need to resort to any intervening authority that would act as an intermediary in its processing) and the recognition of its binding nature and, therefore, obligatory for the service provider, will undoubtedly speed up the process of obtaining it, taking into account, furthermore, the valued reasons for non-compliance -of non-execution- of the Order and the short response times granted.

However, this greater agility in obtaining the evidence may clash with certain fundamental rights of the person under investigation, such as the right to a defence, since it is not necessary for the authorities of the State receiving the order to supervise it, and because the person under investigation cannot make prior allegations either in the State that issued the order or in the State that received it[20]. This is, once again, a reflection of the eternal tension between the greater agility of the proceedings and the need to do so while safeguarding the fundamental rights at stake. But in fact, the system proposed by the Regulation

converts judicial control over the obtaining of evidence which fully affects fundamental rights into a purely incidental control, which will only take place when the service provider - a private body - refuses to execute the Order. It has been argued that if successful, this proposal would involve the "privatisation" of mutual recognition[21].

In this context, one of the main concerns of the regulations is to delimit precisely who will be considered as service providers for this purpose; and, in accordance with the provisions of Article 2 (3),[22] those who, regardless of whether they are natural or legal persons and whether or not they have an establishment in the State of the Union in which they are required, provide one or more of the services specified in the provision and which relate to: (B[23]) information society services, where[24] data storage is an essential component of the service provided to the user, in particular social networks, online markets facilitating transactions between users, and other data hosting services; and (C) Internet domain name and IP address allocation services, such as providers of IP addresses and registrars of domain names, and related privacy and representation services.

In order to send these service providers a Delivery Order, it has been held that it is not necessary for them to have a fixed establishment in the State of the Union in which they are required; what the regulations require is that there be only a "close link" between the service provider and the State in which it provides the service. And while it is true that the best example of such close ties could be the existence of an establishment of the service provider in the State,[25] other indicators can also be assessed, such as the fact of having a significant number of users, the use of the State's language to advertise the services, or the currency used to carry out commercial transactions, or even the availability of a mobile application in the national applications store[26]. In this respect, the Regulation itself specifies that the mere accessibility of an online interface (such as the accessibility of the service provider's or intermediary's website, or of an e-mail address and other contact details) in one or more Member States, taken in isolation, would not constitute a sufficient condition for the application of the Regulation[27].

Aware from Europe of the importance that the effective reception of the Order has for its compliance and for the success of its forecasts, in parallel with the processing of this proposal for a Regulation, the procedures for approving a Community Directive establishing the obligation for service providers to appoint a legal representative in the country in which they provide their services were initiated[28]. The legal representative designated will be the person with whom the issuing authority understands the delivery order; however, in the absence of such designation, the order may be sent to any establishment of the provider in any other country of the Union (Article 7.2 of the proposal for a Regulation). It should be noted, in any case, that the referral of the Order to a specific service provider must be made in relation to services that the latter has offered within the scope of the Union; thus, an Order for the delivery of electronic evidence cannot be addressed to a service provider established in the Union, but in relation to services offered and provided outside the scope of the Union[29].

In any case, the European Bar has not accepted with pleasure the option of choosing the service provider as the recipient of the Order. Its fundamental concern is that in the case of sensitive data or data protected by a recognised privilege, such as the secrecy of lawyer-client relations, the procedure provided for by the proposed Regulation whereby the issuing State must consult the competent authority of the State in which the data will be collected may not be entirely satisfactory. In this respect, the European Bar Association considers that, whenever possible, the surrender orders should be sent directly to the data controller who would be better able to ensure that specially protected data are safeguarded[30].

OBJECTIVE REQUIREMENTS OF THE ORDER: PROPORTIONALITY AND NECESSITY

The valid issuance of a European Evidence Warrant is conditional upon compliance with the requirements of proportionality and necessity of the measure, as well as the requirement that a similar measure exists in the issuing State for the same criminal offence in a comparable national situation. All of these circumstances[31] must be duly accredited in the Order, although it should be noted that, especially with regard to the need and proportionality of the measure - and in order not to prejudice the course of the

investigation - its justification must not be included in the presentation of the EPOC certificate that[32] will be used as a formal instrument for transmitting the Order.

In fact, the materialization of an Order is carried out through the completion and delivery of the standardized forms (called EPOC -for delivery orders- and EPOC-PR -for conservation orders-) that have been included in Annexes I and II to the Proposal of Regulations and that are foreseen to speed up and facilitate the processing of the requests. Only when the recipient of the order fails to comply with it, will the issuing authority send the COPE certificate to the competent judicial authority of that State, accompanied, in this case, by justification of the proportionality and necessity of the measure in order to initiate the procedures for its execution as provided for in the Regulation itself[33].

The requirement of proportionality can be analysed from two different perspectives: from the proportionality, in general, of the regulatory provisions - that is to say, analysing whether, in general, the regulation of these research measures is justified for the achievement of the established purposes - and from the perspective of the specific case and the data requested in relation to it. Insofar as the first option has been explained above by limiting it to only certain criminal cases depending on the type of data requested, reference will be made below to the requirement of proportionality in the specific case, which must be duly substantiated - in the terms seen - in the application. The purpose is to ensure respect for fundamental rights and the principles recognised by the Charter of Fundamental Rights of the European Union[34]. In this context, these rights may be affected when certain data are requested from persons who are the accused party in ongoing criminal proceedings; but also when the rights of third parties who are not even parties to the proceedings are affected. The existence, precisely, of this justification of proportionality in the specific case will allow the articulation of the resources and challenges foreseen to fight against the effectiveness of an evidence that could have been obtained with a violation of Fundamental Rights. While for those who are part of a process, the internal mechanisms of the State in which the process is being carried out will be the ones that mark the existing procedural options to oppose this evidence, those who see their rights affected without being part of any process will be able to challenge this information, illegally obtained, through the mechanisms that have been foreseen, in the State of emission of the Order[35].

It should be noted, however, that Article 11(2) of the proposal for a Regulation has laid down the obligation to inform the person whose data are requested without delay. However, the possibility to suspend the disclosure of this fact for "such time as may be necessary and proportionate to avoid the obstruction of criminal proceedings" may open a way to conflict with the right to a fair trial. That is why the European Advocacy has considered that "the imposition of confidentiality restrictions on EPOs must be subject to the approval of an independent judicial authority and, in each case, be duly motivated and justified by the issuing authority on the basis of meaningful and documented assessments"[36].

Following the consolidated doctrine of the Spanish Constitutional Court, the weighting of the proportionality of a measure that limits fundamental rights requires the assessment of three fundamental aspects that constitute what has been called the constitutional "triple filter": the "suitability of the measure" or its specific adaptation to achieve the proposed objective; the "necessity" of the measure, in the sense that there is no other less harmful measure for achieving the same purpose; and, finally, the "proportionality in the strict sense" or balance between the greater advantages that the measure must represent with respect to the general interest, as opposed to possible specific damages to certain goods or values[37]. The justification for the proportionality of the measure in a European order for the delivery of electronic evidence must make reference to each and every one of the extremes - or filters - referred to, understanding proportionality in a broad sense, which also includes the assessment of its "necessity".

However, when defining the objective requirements to be taken into account for the valid issuance of a surrender order, it is also required that the issuing State has provided for a similar measure for the investigation of the offence. The justification for this requires that, in addition to the above, the applicable criminal law provisions of the issuing State be stated in the order (Article 5(5)(f)).

However, as the European Advocate General has rightly pointed out in relation to the proportionality of the measure, it is true that the conditions for issuing a European Surrender or Conservation Order do not include any threshold of sufficient degree of suspicion (*see* Article 5). Therefore, in its view and in

order to avoid possible abuses, the final legal text should expressly reflect that surrender orders can only be validated by the competent authorities if there are compelling reasons which give rise to a sufficient degree of suspicion to justify the cross-border confiscation of data[38].

ACKNOWLEDGEMENT

This work was financially supported by the Research Project R+D+I called "Investigation and evidence of money laundering. The 4th Guideline" (Reference DER2016-80685-P).

ENDNOTES

1. The European Arrest Warrant has been considered the trigger for a whole series of subsequently agreed normative instruments aimed at establishing common minimum guarantees for defendants and victims in criminal proceedings, at European level. LARO GONZÁLEZ, M.E., "Derechos y garantías del menor en el proceso penal. Harmonización legislativa y necesidades procesales", La Ley Unión Europea, Nº 73, 30 September 2019, Wolters Kluwer (p.1). The author points out, however, that this necessary procedural harmonization, of which she seems to have become aware as far as adult proceedings are concerned, is absent from any reference in juvenile criminal proceedings except for Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for juvenile suspects and defendants in criminal proceedings.
2. I have addressed the issue more extensively in "Europe's Digital Evidence Challenge. El establecimiento de instrumentos probatorios comunes: las Órdenes europeas de entrega y conservación de pruebas electrónicas", *Era Digital, Sociedad y Derecho* (Dir. FUENTES SORIANO O.), Tirant lo Blanch, Valencia, 2020, pp. 281 to 343.
3. COM (2019) 70 final. For the objectives and negotiating guidelines contained in the Recommendation for a Decision, see GÓMEZ AMIGO, L., "Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que aproxima", Revista Española de Derecho Europeo, nº 71, July-September 2019, pp. 23 to 56 (on the subject, specifically, pp. 50 to 53).
4. Explanatory memorandum. Recommendation for a COUNCIL DECISION authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters COM/2019/70 final. 1. Context
5. Many qualifiers have been added to the concept of evidence to denote the idea of information extracted from computer data: that is, data obtained, stored, disseminated... by means of computerized and therefore electronic procedures. We have thus spoken of electronic, telematic, digital, cybernetic, technological evidence, proof of the digital fact, etc. Of all of these, technological evidence has been the most used in recent procedural reforms; however, it is perfectly interchangeable with electronic evidence in this Proposal for a European Regulation. On this subject, *in extenso,* see ARRABAL PLATERO, P., *La prueba tecnológica. Aportación, práctica y valoración,* Tirant lo Blanch, Valencia, 2019, pp. 29 to 39, for whom "technological evidence refers, on the one hand, to those computer data, that is, electronic impulses susceptible to being "stored in any part of the planet, sent to the other end of the globe in a matter of seconds, quickly altered or cloned, stored in hidden folders, distant servers, encrypted, etc.On the one hand, it is important to be able to access the information that is "stored in any part of the world in a matter of seconds, to be quickly altered or cloned, to be stored in hidden folders, on distant servers, encrypted, etc." with a transcendence in a process -see a pen drive or a hard disk- and, on the other hand, to those elements obtained through technological means -such as, for example, a computer expert's report, communications intercepted by means of technological mechanisms, ...- (Op, cit., p. 33)
6. It should be noted, at this point, that while in the proposed Regulations in English the definition of electronic evidence in Article 2 is found at number 6, in the document drawn up in Spanish by the committee, this proposal occupies number 5 of the same legal precept.
7. In cases where the data - the proof - is stored by a third party on behalf of a given service provider, it is this third party that will be in charge of processing the data of the service provider. In this sense MONTORO SÁNCHEZ, J.A., "Breve análisis acerca del futuro Reglamento Comunitario "E-Evidence" sobre las órdenes europeas de conservación y entrega de pruebas y evidencias electrónicas a efectos de enjuiciamiento penal", in *Orden europea de investigación y prueba transfronteriza en la unión europea,* GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019, p. 176.

8. On the construction and scope of the right to data protection as a fundamental right, see ARRABAL PLATERO, P., "La videovigilancia laboral como prueba en el proceso", Revista General de Derecho procesal. Iustel, nº 37, 2015, pp. 11 and following. On the demands of speciality, suitability, exceptionality and need for the measure and, finally, proportionality as requirements for its limitation, I have had the opportunity to pronounce in "Comunicaciones telemáticas: práctica y valoración de la prueba", in *El proceso penal. Cuestiones fundamentales* (Coord. FUENTES SORIANO), Tirant Lo Blanch, Valencia, 2017. In this respect also BUENO DE MATA, F., *Las diligencias de investigación penal (...), cit.* pp. 30-38; on the obligation of collaboration of servers located outside Spain, pp. 71-76.
9. This is stated in Recital 2 of the proposal for a Regulation "Effective mechanisms for obtaining electronic evidence [with reference to European Arrest Warrants] are essential in the fight against crime, subject to conditions that guarantee full compliance with the fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union and enshrined in the Treaties, in particular the principles of necessity and proportionality, procedural safeguards, data protection, confidentiality of correspondence and privacy". This insistence on the necessary respect of the acquis communautaire on data protection is clearly expressed in the detail of the precautions to be taken by the different subjects involved by a surrender order; thus, Recital 57 states that 'personal data obtained under this Regulation should be processed only if necessary and proportionate for the purpose of prevention, investigation, detection and prosecution of criminal offences, the application of criminal penalties and the exercise of the rights of the defence. In particular, Member States shall ensure that relevant data protection policies and measures are applied to the transmission of personal data from competent authorities to service providers for the purposes of this Regulation, as well as measures to ensure data security. Service providers shall ensure the same for the transmission of personal data to the relevant authorities. Only authorised persons shall have access to information containing personal data that can be obtained through authentication processes. Consideration should be given to the use of mechanisms to ensure authentication, such as notified national electronic identification systems or trusted services as provided for in Regulation (EU) No 910/2014 of the European Parliament.
10. According to article 4(3)(C) - which does not g, as the proposal for a Regulation states - of the Proposal for a Regulation on privacy and protection of personal data in the electronic communications sector 'electronic communications metadata' shall mean any 'data processed in an electronic communications network for the purpose of transmitting, distributing or exchanging electronic communications content'; This includes data used to track and identify the source and destination of a communication, device location data generated in the context of the provision of electronic communications services, as well as the date, time, duration and type of communication
11. This is clearly expressed in Recital 23 of the Proposal by recognising that 'while subscriber data and access data are useful to obtain first indications in an investigation into the identity of a suspect, transaction data and content data are more relevant as evidential material'.
12. As defined in Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8. 'information system' means 'any device or group of devices which are interconnected or linked, one or more of which carries out, by means of a program, automatic processing of computer data and computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its operation, use, protection and maintenance' (Article 2(a))
13. The specific criminal acts listed in the provision are (Article 5.4.b): those defined in Articles 3, 4 and 5 of Council Framework Decision 2001/413/JHA; those defined in Articles 3 to 7 of Directive 2011/93/EU of the European Parliament and of the Council; those defined in Articles 3 to 8 of Directive 2013/40/EU of the European Parliament and of the Council; and in point c) the criminal offences defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541 of the European Parliament and of the Council
14. See Article 4 of the Proposal for a Regulation for its definition.
15. On the need to establish a common normative substratum of evidence for the different countries of the EU, see ORMAZÁBAL SÁNCHEZ, G., "El tortuoso camino hacia la construcción del espacio judicial europeo en materia penal. Algunas consideraciones en torno al reconocimiento mutuo de pruebas, la euroorden y la Fiscalía Europea" in *Derecho y proceso. Liber Amicorum by Professor Francisco Ramos Méndez* (CACHÓN CADENAS and FRANCO ARIAS, Coords.), Barcelona 2018, pp. 1805 and following
16. Cf. Article 4(1) and (2)
17. It should be borne in mind that the authority that validates the order in the cases analysed is now considered the issuing authority for the purposes of transmitting the COPD and COPD-CR certificate referred to in the

annexes to the regulations, which is the formal channel for transmitting the reference orders. Art. 4.4 of the Proposal for a Regulation

18. Cfr https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf (p. 6)
19. Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and of the Council on European orders for the surrender and preservation of electronic evidence for purposes of criminal proceedings (COM(2018) 225 final - 2018/0108 (COD)) - Proposal for a Directive of the European Parliament and of the Council establishing harmonised rules for the appointment of legal representatives for the purposes of obtaining evidence in criminal proceedings (COM(2018) 226 final - 2018/0107 (COD)) 2018/C 367/17. In its Conclusion 1.7. it can be read that 'the EESC welcomes the fact that both Orders must be issued or confirmed by a judicial authority of a Member State. However, the EESC considers it problematic that, for the collection of subscriber data and access data, public prosecutors can also issue warrants and supports the fact that the collection of personal data is subject to the authorisation of a judge'.
20. In this sense MONTORO SÁNCHEZ, J.A., "Breve análisis (...), cit.
21. GÓMEZ AMIGO, L., "Las Órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima", Revista Española de Derecho Europeo, nº 71, July-September 2019, pp. 23-56 (specifically, p. 54.
22. Note that in the Spanish text of the Proposed Regulations, this reference is found in Article 2 (2) and not 2 (3) as it appears in the English text of the proposal.
23. Information society services, as defined in Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, means "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". In order to clarify the wording of this provision, it is stated that "the following shall be understood (ii) "by electronic means" means that the service is sent from the source and received by the recipient by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means
24. An electronic communications service, as defined in Article 2(4) of the Directive on the European Electronic Communications Code, means a service provided "normally for remuneration over electronic communications networks, which includes, with the exception of services providing or exercising editorial control over content transmitted using electronic communications networks and services, the following types of services: (a) 'Internet access service' as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120; (b) 'interpersonal communications service'; and (c) services consisting wholly or mainly of the conveyance of signals, such as transmission services used for the provision of machine-to-machine services and for broadcasting
25. Establishment" is understood in the proposed Regulation as the "effective exercise of an economic activity for an indefinite period through a stable infrastructure from which the activity of providing services is carried out or a stable infrastructure from which the activity is managed" (art. 2 (5); note that in the Spanish text this definition is found in art. 2 (4))
26. Cf. Recital 28.
27. Cf. Recital 27.
28. Currently under discussion: Proposal for a Directive of the European Parliament and of the Council establishing harmonised rules for the appointment of legal representatives for the purposes of obtaining evidence in criminal proceedings. COM (2018) 216 Final; 2018/0107 (COD)
29. Cf. Recital 26.
30. In the previous comments issued by the European Lawyers' Office at the request of the Commission, for the processing of the legal text under consideration, it can be read (p. 3) that requests for access to digital evidence should, where possible, always be addressed to the data controllers, rather than to the data providers who, especially when the data are managed by a law firm, would provide better guarantees against any illicit exchange of privileged information

https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf

31. In addition to these circumstances, the Delivery Order must also refer to all the data that the logic of its proper functioning requires and which Art. 5 (5) is responsible for detailing: identification data of the issuing authority as well as the validating authority, where applicable; the data of the service provider to whom it is addressed and on its behalf, that of its legal representative (in which way I understand that the literal diction of Art. 5 (5) should be interpreted. b) when it states that it must indicate "the recipient of the European delivery order referred to in Article 7"); the persons whose data are requested (except where the sole purpose of the order is to identify a person); the category of data requested (subscriber data, access data, transaction data or content data); the period covered by the request for delivery; the reasons justifying the urgency with which delivery is requested within the special time limits laid down for these cases; and, finally, where the order concerns data stored or processed as part of an infrastructure provided by a service provider to an undertaking or other entity other than a natural person, the statement that the measures could not be directly addressed to the undertaking or entity, as provided for in the Regulation as a general rule, on the ground that this could jeopardise the investigation. In my opinion, however, a correct understanding of this requirement requires not only that this be stated in the application, but also that it be justified in the application the specific reasons why it is understood that the investigation would be jeopardised if it were to be requested directly from the undertaking or entity; I have dealt with this subject in detail in 'Europe facing the challenge
32. Vid. Art. 8.3 Proposal of Regulation.
33. Art. 14 Proposal for a Regulation.
34. The possibility of limiting the exercise of the rights and freedoms provided for in the Charter of the Union is contemplated in Article 52.1 of the same and subject to the principles of proportionality and necessity, but the lack of specific regulation on fundamental rights in the sphere of the European Union will mean -as ARMENTA rightly points out- "that a possible claim will have to overcome a certainly complex situation in which European regulations, the case law of the ECHR and the TJUE, as well as the internal regulations of the various Constitutional Courts, concur". ARMENTA DEU, T., "Orden Europea de Investigación y exclusión probatoria. Admissibility, challenge and refusal in the State of trial or execution when a violation of a fundamental right is found", in Orden europea de *investigación y prueba transfronteriza en la unión europea,* GONZÁLEZ CANO (Dir.), Tirant lo Blanch, Valencia, 2019, p. 781.
35. In this respect, Recital 54 of the Proposal for a Regulation clarifies that 'It is essential that all persons whose data are sought in criminal investigations or criminal proceedings have access to effective judicial protection in accordance with Article 47 of the Charter of Fundamental Rights of the European Union. For suspects and defendants, the right to an effective remedy must be exercised during criminal proceedings. This may affect the admissibility, or where appropriate the weight in the proceedings, of evidence obtained by these means. They also benefit from all the procedural guarantees applicable to them, such as the right to information. Persons who are not suspects or defendants should also have the right to effective judicial protection. Therefore, as a minimum, the possibility to challenge the legality of a European surrender order, in particular its necessity and proportionality, should be provided for. This Regulation should not limit the possible grounds for challenging the legality of the order. Such remedies should be exercised in the issuing State in accordance with its national law.
36. CCBE Preliminary comments on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Punto 6
https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf
37. By all, JTS 96/2012 of 7 May (JTS 2012, 96)
38. CCBE Preliminary comments on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. Punto 3
https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20180629_CCBE-Preliminary-comments-on-the-Commission-proposal-for-a-Regulation-on-European-Production-and-Preservation-Orders-for-electronic-evidence-in-criminal-matters.pdf