II.3

Digital evidence for the criminal trial: limitless cloud and state boundaries

SUMMARY: 1. A baffled king. – 2. Mutual Legal Assistance and its shortcomings. – 3. The Empire strikes back: national remedies. – 4. Finding effectiveness: an EU regulation proposal. – 5. Conclusions.

1. It is hard to find a stronger manifestation of state sovereignty than the power to investigate a crime, try the suspect for it, and punish him once he is found guilty. The whole process is a show of public force: it brings reluctant witnesses to the stand, forcing them to tell the truth; it can violate the privacy of an apartment or listen to a phone call. In the last decade, another tool has been gaining importance on the criminal trial's stage: the sheer amount of data we produce daily can tell a lot about what we are up to, and it is no wonder that it can come handy during the investigation of almost any crime. There is no need for a cybercrime, or for the misuse of a device: digital information can always be relevant. The list of the last locations of the victim, the name of the person s/he was texting with, the record of a phone call or an email; all this data could play a role in any investigation.

This type of evidence, however, differs substantially from something as mundane as a knife: we share a significant amount of information with the company that provides the service to us[377]. They gather almost everything we produce and store it on a server[378]: we can access the information whenever we like, but it is physically preserved in a data center at the other corner of the world, displaced from time to time to ensure the efficient use of the infrastructure[379].

377 A couple of examples: the Onion – a satire U.S. website – described Facebook a C.I.A. program, and the most effective one. Since then, the company has gained access to more information developing a facial recognition algorithm, sharing the information among devices, so that it can keep track of phone calls and text messages sent outside the platform. However, Facebook is not the only one: Tinder – the dating app – keeps scrupulous records of all the users to improve the matching algorithm. A journalist asked for her entire record and received a staggering amount of data regarding her preferences: see J. Duportail, *I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets*, in *theguardian.com*, September 26, 2017.

For a strong critique of the *status quo* and technological ways forward see: S. Rasmussen, *The BINC Manifesto: Technology driven societal change, science policy &stakeholder engagement*, in C. Gershenson, T. Forese, J. M. Siqueiros, W. Aguilar, E. J. Izquierdo, H. Sayama (eds.), *Proceedings of the Artificial Life Conference 2016,* at *turing.iimas.unam.mx*; M. Monti, S. Rasmussen, *RAIN. A Bio-Inspired Communication and Data Storage infrastructure*, in *Artificial Life,* 2017, p. 552-557.

378 Sometimes it is a service; some others it is a business model: acquiring and selling data has become a business of its own, and according to the documentary *Terms and conditions may apply* (2013), it began with the Patriot Acts, that required the big tech companies to store information for surveillance purposes. Then they realized they could make money off of the incredible haystack they were building and started to do so.

For other industries, gathering data is vital to maintain the product working: artificial intelligence, for instance, needs to learn from past examples. Without memory, it cannot function, so it needs to keep a considerable amount of information to calculate the next answer.

379 See J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, August, 31, 2010, *rm.coe.int*; for a technical explanation, see Y. Sahu, R. K. Pateriya, R. K Gupta, *Cloud Server Optimisation with Load Balancing and Green Computing Techniques Using Dynamic Compare and Balance Algorithm*,

Long story short, those data have an owner: often a big, powerful one that operates on an international level day in and day out. The company does not need to be located or even represented in a country to provide services within its boundaries, and it is free to set up branches of their organization wherever they want, according to the most convenient business strategy.

This scenario is enough for traditional categories to lose their focus: citizenship and sovereignty can be set aside with ease, whereas the private policies of a single company can have a transnational impact[380].

On the one hand, being a citizen means enjoying a certain set of rights, which does not necessarily apply to one's data once they transit over a foreign server[381].

On the other hand, the authority of the state is not enough to gain access to the information produced on its own soil, relating to a crime entirely carried out on its territory. It is somewhere else, out of its reach. Law enforcement authorities have to ask for the help of the competent state through the available Mutual Legal Assistance (MLA) tools, and not because of the transnational nature of the crime: as we already mentioned, that could be entirely carried out within a nation's territory. Digital evidence, however, follows the fragmented, international territoriality of providers; not the political boundaries set to national states.

Given this framework, we will rapidly point out the main flaws of the traditional system and how some European states have been developing a different approach to secure the evidence anyway. Then, we will focus on a proposal for a European regulation that faces the issue, aiming to introduce new possibilities of direct interaction between states and service providers.

2. When the state cannot secure the necessary information on its own, it can ask for help: every nation has its arsenal of tools and procedures to obtain the assistance of the competent state, generally based upon a patchwork of bilateral or multilateral treaties. The procedures that they provide for, however, are often cumbersome and slow, which is especially problematic for a kind of evidence that can be quickly erased, modified, encrypted or displaced[382].

Within the European Union, the cooperation should be simplified by the brand new European Investigation Order (EIO), in an attempt of standardizing and expediting the procedure; nonetheless, it does not contain any specific provision on digital evidence, focusing only on spot operations like the identification of the person "holding a subscription of a specified […] IP address"[383].

in *2013 5th International Conference and Computational Intelligence and Communication Networks, IEE Xplore*, 11 November 2013.

380 For a vivid example, see R. Budish, H. Burkert, U. Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects*, May 2, 2018, in cyber.harvard.edu.

381 See *Terms and conditions may apply* (2013) on the Total Information Awareness program; see *Citizen four* (2014) on the NSA domestic surveillance programs, based upon the documents leaked by Edward Snowden and subsequently made available by the N.S.A. itself, on the web page of the Domestic Surveillance Directorate: nsa.gov1.info.

382 For further considerations on the topic, see A. K. Woods, *Against Data Exceptionalism*, in *Stanford Law Rev.*, 2016, p.749.

383 Art. 10, lett. *e* of the directive; the Italian transposition added to this list also the identification of the person behind an email address: art. 9 lett. *e* D.Lgs. June 21, 2017, n. 108.

Moreover, Ireland is not a party to the directive, so it has not transposed it nor can be bound by its provisions, and this could be a major problem: most of the big tech corporations have their the European headquarters there. As a result, the ordinary MLA procedure is to be adopted, which means at least that the competent central authority has to be involved in the transmission of the request. The same applies to requests directed to non-EU countries such as U.S. and Canada.

Another problematic step is the phrasing of the request, that should be as specific as possible, so that the competent authority can decide what to do with it. It is tricky for all kind of requests, but the dialogue about digital evidence can be further complicated: there is no shared legal definition about the type of data that can be demanded, and no shared understanding of the conditions under which a certain kind of information can be released. The lack of common grounds can hurt the communication and a request – complete under the law of the issuing country – can be discarded as unbearably generic by the recipient[384].

Once the application is ready, one must decide to whom it shall be addressed, and it is no easy step. Which is the competent state to deal with it? The country where the company is based? The country where a local branch is based? The country where the data are stored? Each law can locate the provider according to different criteria, and as a result, there is little or no clarity as to who can obtain the information[385]. Providers as well hold their views as to which country has the authority to compel the production of their records, agreeing spontaneously to some requests and fighting others[386]

The best shot of the issuing authority is to forward the request to every state that is potentially connected to the information, hoping for at least one positive answer; of course, this method is not the most efficient for both the issuing and the receiving authorities[387].

But let us assume that at least one of these requests has landed in front of a receiving authority that can actually help. The investigators should find the required data, and the best way to do that is asking the provider, but not many European countries have a transparent procedure in place to cooperate with them.

Finally, MLA requests are suddenly going from "boutique" to "fast food"[388]: the number has been increasing, and many states do not have the resources to respond to all the asks adequately. It is time and energy consuming, and there is no interest of the receiving authority at stake, which can

384 For more on the topic, see the *Commission staff working document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, April 17, 2018, SWD(2018) 118, p.* 30 and following.

According to a survey on cross-border access to electronic evidence conducted by the European Commission, another common experience is the refusal to comply with the request due to the difficulty in establishing probable cause, which is also a sign of lack of specificity; see *Questionnaire on improving criminal justice in cyberspace. Summary of Responses*, 2017, p. 5, ec.europa.eu.

385 See K. Westmoreland, G. Kent, *International Law Enforcement Access to User Data: A Survival Guide and Call for Action*, in *Canadian Journ. of Law and Technology*, 2015, p. 232.

386 A. K. Woods, *Against Data Exceptionalism*, p. 735-736 and p. 745-747.

387 See *Questionnaire on improving criminal justice in cyberspace,* p. 7.

388 A. K. Woods, *Data Beyond Borders. Mutual Legal Assistance in the Internet Age*, 2015, uknowledge.uky.edu, p. 3.

result in a time-conservative work schedule. Those requests will be answered but with low priority, which could defeat the purpose of cooperation or make it impossible: data cannot be stored forever; they could be erased or encrypted while the ask lingers on someone's desk[389].

This delay in the response is the most urgent problem to solve: a good timing has always been critical to the success of the operations but, with electronic evidence, the whole process needs to be further expedited.

Confronted with this reality, many scholars have come up with proposals to adjust and modernize the framework.

One calls for a better response from private companies, which could be victims of cyber-attacks at any time: that they should invest more in digital security and digital forensics so that they can provide data to whoever can prosecute the crime they suffered[390]. It seems to be a form of self-help though, and not a solution that could benefit the entire system: the cooperation could be smoother for attacks on some victims, leaving everyone else out.

Other proposals touch directly upon a deeper problem: is the cloud manageable at all through the territoriality principle, or is it too hard to maintain this expression of sovereignty? According to some scholars, it is time to break down the borders, since territoriality is "the main obstacle for investigating actions within the clouds"[391]. Many theories stemmed from this premise: according to one of those[392], territoriality should be adapted to the challenges of a globalized world, or, at least, it should apply just to the jurisdiction, but not to the investigation. The cross-border access to digital evidence would then been ensured. This idea, however, could be hard to sell to the states themselves: they should allow a foreign authority to carry out an inquiry on their soil[393], which does not seem a realistic expectation. Moreover, the proposal would be of some use while following a live communication, but not as much in asking a private company for stored data, which seems to be the main issue[394].

Others have been trying to make territoriality more manageable, for instance by searching for a more tangible connecting factor: the location of the data can bring to inconsistent results, and it is difficult to establish. It should be replaced by something easier to ascertain as the formal power of disposal of the information[395]

Finally, it has been argued that digital information is not so special after all: it is stored on a physical layer that permits – among other criteria – to establish jurisdiction according to the

389 According to *Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies*, December 12, 2013, in obamawhitehouse.archives.gov, p. 227, "requests appear to average approximately 10 months to fulfill". Since the report, the number of MLA request directed to the U.S. has more than doubled: see A. K. Woods, *Against Data Exceptionalism*, p. 750.

390 J. I. James, *How Business Can Speed Up International Cybercrime Investigation*, in IEEE, 2017, p. 105.

391 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 8:

392 D. J. B. Svantesson, *Law Enforcement Cross-border Access to Data*, 2016, in researchgate.net.

393 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 10.

394 J. P. Mifsud Bonnici, M. Tudorica, J. A. Cannataci, *La regolamentazione delle prove elettroniche nei processi penali in "situazioni transnazionali": problemi in attesa di soluzioni*, in M. A. Biasiotti, M. Epifani, F. Turchi (a cura di), *Trattamento e scambio della prova digitale in Europa*, Napoli, 2015, p. 213.

395 J. Spoenle, *Cloud Computing and cybercrime investigations*, p. 10-11.

territoriality principle, allowing the whole structure to function[396]. The MLA system, nonetheless, would need a serious restyling to improve the response time and improve efficiency[397].

3. Given the intricacies of the MLA, States have come up with different approaches based on unilateral action, to obtain access and avoid the pains of cooperation with foreign authorities altogether. The individual strategies can be more effective, but that can also imply a big price to pay for the companies or the rights of the user.

The most infamous shortcut is mass surveillance, which impacts disproportionately on the individual's right to privacy. Other methods can protect the people and the national interest to access evidence, but strongly affect the liberties of the service providers: some states ask (or have considered asking) to locate all relevant information within the borders, so that it can be accessible at all time.

We will not delve into these attempts; instead, we will analyze the different strategies put in place by France, Germany and Italy. All those countries share the same need, but do not adopt the same approach in dealing with it.

France, for instance, is one of the few countries in the European Union to have explicit legislation in place that allows for the direct cooperation between law enforcement and service providers, and it has been there for quite some time. In 2004, art. 60-2 was introduced in the Code of Criminal Procedure, offering a legal base for direct cooperation with service providers[398]. Although it is limited to a particular kind of inquiry (*enquête de flagrance*), it serves as a model to the other provisions enabling such joint effort also in the other types of investigation that the Code describes: it is the case of art. 77-1-2 for the *enquête préliminaire* and art. 99-4 for the *instruction.*

This system contains two main possibilities: first, the providers have to disclose all the "information that is useful to the manifestation of the truth", unless they can oppose a privilege recognized by the law. The provider has to respond within the shortest delay possible; if it fails or refuses to answer without a legitimate motive, it will receive a 3.750 euro fine. Second, the law enforcement authorities can also require a specific class of service provides – those hosting communications over the internet – to preserve content information for up until one year; to do that, a judge has to review the application.

The requests are subject to the procedure that the regulatory part of the Code lays out. They ask the police to write a detailed report on the ask, specifying which company has been asked and what kind of information are to be handed over. As to the practical details of the interaction, they are established by a protocol approved by the ministry of justice and every organization with which the law enforcement needs to cooperate.

396 It is the main argument of A. K. Woods, *Against Data Exceptionalism*, to which responded D. J. B. Svantesson, *Against 'Against Data Exceptionalism'*, in *Masaryk University Jour. of Law and Tech*. 2016, p. 200; as well as Z. D. Clopton, *Data Institutionalism: A Reply to Andrew Woods*, *Stanford Law Rev. (online),* 2016.

397 For a multi-dimensional approach, see A. K. Woods, *Data Beyond Borders*, p. 8-14. The same view has been held by DigitalEurope, *DIGITALEUROPE views on Law Enforcement Access to Digital Evidence*, October 17, 2016, p. 4: the document encourages a more efficient MLA remedies instead of unilateral actions to access cross-border evidence.

398 Art. R15-33-68 contains the list of what enterprises are to be considered service providers for the purposes of this statute.

So, when the state asks for information, the request is regarded by the state as binding: not answering is punished with the fine but also with a class II misdemeanor, for disobeying the orders of a court of law[399]; both the punishments, however, can be easily factored in the decision not to answer: the criminal misdemeanor is punishable with another fine whose maximum amount is 150 euros. Moreover, those rules do not seem to apply to a service provider that is not established in France, or, in any case, it is not clear how they could be enforced without the cooperation of another country[400], which leads us back to square 1.

The system, however, seems adequate to interact at least with domestic providers, even if the deterrence of the sanctions is quite low. This mechanism relies heavily on the voluntary cooperation of the service providers but does not solve the main issue: the state does not have means to coerce compliance, if necessary.

The approach has not been shared by Germany, that has recently passed a new law addressing the issue of illegal content spreading through social networks (*Netzwerkdurchsetzungsgesetz – NetzDG*)[401]. This piece of legislation, among other things, asks all social networks to choose a representative that operates within the territory of the state: he or she will be in charge of dealing with the (criminal) law enforcement authorities' demands; the company is required to disclose the information within 48 hours upon receipt[402]. The style here is radically different. What Germany has done is forcing the providers to establish a direct, visible connection between the country and the platform, so that the state can have an easy access point and start the procedure quickly and officially. Unlike the French regulation, it gives a precise deadline to the companies, under the penalty of 500.000 euros for the failure to respond[403]. The law clearly states that the infractions shall be punished even if they are committed abroad. The aim is clear: it is about getting back territoriality (so, sovereignty) as to what happens within German borders, and the jokes are on the service provider. It is its responsibility to delete illegal content, to battle hate speech and to help to prosecute potential crimes in a short delay from the request.

399 Art. R642-1 of the French Criminal Code.

400 The survey of the European Commission showed that France is among the states that have concluded formal or informal agreements with foreign service providers and that consider the cooperation mandatory, although it is not clear what to do in case of the company's failure or refusal to respond.

401 This new statute is highly controversial. On the one hand, it has been criticized by the U.N. and the E.U. as a law allowing for censorship; on the other hand, the application of its provisions to their full extent would lead to an extra esteemed cost of 530 million euros per year: M. Etzold, *Facebook attackiert Heiko Maas*, May 28, 2017, wiwo.de.

The new law imposes to all the major social networks operating within German boundaries to delete illegal contents after 24 hours from a complaint. It is now in force since a few months and the German press already reported a general failure to respond to the illicit content. According to the reports that have been released, the compliance rate varies highly from company to company. While YouTube and Twitter try to be as efficient as they can, Facebook reportedly fall way behind the schedule, and has been criticized for how the report mechanism has been structured: F. Rütten, *Wie Facebook und Twitter das neue Löschgesetz umsetzen*, January 4, 2018, stern.de; *Facebook löschte bisher nur 362 Beiträge*, July 27, 2018, t-online.de; *Fast 500.000 Beschwerden, nur wenuge Löschungen*, July 27, 2018, manager-magazin.de; F. Steiner, *Wie viel Facebook & Co. mithilfe des NetzDG löschen*, July 27, 2018, deutschlandfunk.de.

402 § 5 (2) *NetzDG*.

403 § 4 (1) n. 8, § 4 (2) *NetzDG*.

Nothing of the kind has been happening in Italy: there is no legislation regulating interaction with any service provider, that fall under the general regulation of searches and seizures. They can voluntarily cooperate and give out the information or be searched. There has been little or no attention to specific issues, apart from some vague provisions regarding the chain of custody and the seizure by copy, which is an option available only for service providers[404]. Playing in this scenario, the investigators have two main ways to get the information they want: the first one is targeting the device[405]. It is an easy remedy, but it has two main flaws: first, the device could not be an easy access point to all the information stored in the cloud; it could be the opposite: the cloud could be an effective way to peek into an encrypted cell phone[406]. Second, the information displayed on the device is often a copy of the original, which is stored safely somewhere else: some records could be altered or canceled, undermining the reliability of the evidence. The issue here is not the admissibility in court – the rules on authentication are quite relaxed – but it is still important that the evidence collected and presented at trial has a strong probative value, which could be achieved through the transparent cooperation with service providers. Law enforcement has to rely then on the spontaneous cooperation of the providers, that can decide to answer to disclosure requests or to refuse it without fear of consequences[407].

4. The current legal framework needs to be reshaped, as it does not seem to be efficient for any of the stakeholders involved. The states cannot rely upon sure means of cooperation, and the MLA procedure does not seem to be an option (at least, not for all cases that potentially require access to digitally stored evidence). The providers are in an awkward position: they have to keep good relationships with the states they are doing business in, but they also cannot afford to disclose costumers' data without due process: the enhanced protection of privacy has been a selling point since Snowden's revelations[408]. In between, the users cannot do much more than wait and see: they agreed to terms and conditions that normally allow for any kind of appropriate action to help to

404 This is another issue that legislations struggle with: does the copy of a bunch of information amount to a seizure? In Italy yes, but just for one kind of duplicate (bit stream image): see Cass., S.U., July 20, 2017, *Andreucci*, n. 40963, in *C.e.d.*, n. 270497, for a note, see L. Bartoli, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. (web)*, 2018, f. 1. In the U.S. it is still unclear whether or not the Fourth amendment is to be applied to the digital duplication: according to a well-known perspective, yes, but only if it is not possible to examine the data before copying it: O. Kerr, *Fourth amendment seizures of computer data*, *Yale L. Journ.,* 2010, p. 700; for an overview on the issue, see *Digital Duplication and the Fourth Amendment*, *Harv. L. Rev.*, 2016, p. 1046.

405 On the low level of protection that the device enjoys in the Italian system see G. Lasagni, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *NJECL*, 2018, p. 386.

406 Quite the contrary: it could be encrypted and the cooperation with the provider could be the shortest way to get ahold of the contents, as the S. Bernardino case has clearly demonstrated.

407 Facebook, for instance, has been heard on how it cooperates with law enforcement authorities to prevent hate speech and violence against women: for an example, see the Italian Senate commission on Femicide and gender related violent crimes, transcript of the hearin held on July 25, 2017, *senato.it*, p. 30 and following.

408 Amazon, for instance, has made very clear that it will challenge all the requests that deems insufficient and that it is lobbying for the introduction of adequate standards for this kind of cooperation: see S. Schmidt, *Privacy and Data Security*, June 12, 2015, *aws.amazon.com*. After all, Amazon had the largest share in the cloud services' market: see C. Coles, *AWS vs Azure vs Google Cloud. Market Share 2018*, May 1, 2018, *skyhighnetworks.com*.

investigate a crime. The decision is ultimately in the companies' hands: if they tend to be indulgent towards the requests, the information will be handed over, and often the procedure will not guarantee the basic safeguards as to the necessity and the proportionality of the investigative action.

The overall picture is nothing short of chaotic. The burden of extra-territoriality has been passed on to providers, which directly receive the requests, phrased according to different national frameworks instead of having them channeled through a single "competent authority". Together with the burden, however, comes the power to decide on a case-to-case basis: the single company can make its own policy as to the cooperation, and since it is voluntary, 'No' is always an option[409].

Thanks to a thorough consultation with States, national judiciaries, law enforcement authorities and the association of the service providers, the European Commission identified the core issues: the complete obscurity in the procedure, the lack of reliability and the troubles in holding both companies and law authority agencies accountable for their actions. To face these deficiencies, the European Commission has drafted a proposal for a regulation which – if approved – would govern and enhance direct cooperation between individual states and service providers by introducing two new tools, the European Production Order and the European Preservation Order[410].

The European Production Order is intended to oblige service providers to hand over information to the member state that requires it, without the necessary involvement of the law enforcement authorities of another member state. The European Preservation Order aims at freezing useful information, allowing the law enforcement authorities to follow through with a request to secure the evidence, neutralizing the risk of losing relevant material.

They would enlarge the spectrum of possibilities when it comes to cross-border access to digital evidence: they would not replace any MLA solution; they would just provide for an alternative. Moreover, they would not abolish per se any national solution already in place, meaning that any law enforcement authority will be able to choose how to ask for the information it needs. On the one hand, this strategy could play well, allowing a certain degree of flexibility: the investigators could be free to choose the tool that better fits into their strategies, being just able to count on two new cards in the game. On the other hand, this could bring to a residual application of the regulation: it is a compelling mechanism, but it also comes with some conditions attached. It could be easy to circumvent its limitations by simply resorting to an informal ask to the service provider: it has worked so far and could work again in the future. It looks like it is up to the private companies to uphold a single standard when it comes to this matter: they are the ones having to respond to the information requests in the first place, and they have an interest in reducing the

409 As a result, some states normally get what they want whereas some others are left behind: See European Commission, *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, December 2, 2016, 15072/16, in data.consilium.europa.eu (hereafter: *Non-paper 1*), p. 9-10.

K. Ligeti, G. Robinson, *Cross-border access to electronic evidence: Policy and legislative challenges*, in S. Carrera, V. Mitsilegas, *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, Brussels, p. 103. The authors remarked that the compliance rate highly varies form country to country, at least in Google's response pattern. They positively respond to the 75% of requests from Finland, but they do not respond to Hungarian authorities.

410 See European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, SWD(2018) 118, April 17, 2018, eur-lex.europa.eu.

variables. Then, they would probably use the procedure as a shield: they would hand over data under a binding order, instead of passing information "under the desk", according to non-transparent policies or a case-by-case rationale.

Coming down to the details: the regulation provides for a common set of definitions as to what qualifies as a service provider and what kind of records can be secured.

Let's start with the first classification: the draft regulation mentions communication services, internet domain and IP numbering services and information society services as defined by Art. 1(1) point (b) of Directive (EU)2015/1535. This last reference is designed to include «any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services», which can apply to a broad set of situations: for instance, all the marketplace and social networks are included. The companies that provide such a service can be reached by the authorities of any member state as long as they offer their services in the European Union. In other words, they are subject to those orders if they enable physical or legal persons within the union to use the services they provide or if they have a substantial connection to the European Union; therefore, the regulation does not apply to companies that do not fall in those categories and to services that are rendered outside the European Union.

As for the type of data that can be obtained, the regulation lays down four categories: subscriber data, access data, transactional data and content data.

The first two categories are the least problematic with respect to the interference that the disclosure would realize, and they should normally be interesting at the early stages of an investigation to identify the suspect; they consist in information such as the name and address of the user; the IP address and the logs of access to the service[411].

Transactional and content data, on the contrary, are suitable to be presented as evidence as to what happened: they can be defined as metadata and the actual text message, email, photo, video, recording and so on. The treatment of these last two is much more problematic: even if the metadata does not seem as decisive, they can be interconnected with other information and help painting a pretty accurate picture of what the specific content was; however, the most intrusive measure is for sure the order to disclose content data.

For this reason, and to ensure a minimum level of proportionality, the regulation provides for two safeguards: the order to produce transactional and content data shall be approved by a judge or a court, and can be only issued if the alleged infraction is punished with a custodial sentence of not less than three years in its maximum amount.

A production order for subscriber and access data can be issued for all criminal offenses, and the authority of the prosecutor will suffice as there is no need for the validation of the judge.

The difference in treatment seems reasonable: it takes into account the different intensity of the public authority's interference in the subject's private life[412], but this order of things also shows

411 It is also the object of the vast majority of the requests.

412 During the discussion on the Proposal, the EESC has pointed out that also subscriber and access data are personal information: therefore, a judge should be involved in issuing the order as well: *Opinion of the European Economic and Social Committee*, n. 11533/18, July 12, 2018, *eur-lex.europa.eu*, point 1.7. The opinion, however, does not square with the fact that the prosecutor normally has access to personal data of the defendant or a person of interest in an investigation, without the judge being necessarily involved. Moreover, these types of data do not necessarily involve a third party, which can also justify a more relaxed standard.

one main critical aspect. Setting a threshold at three years of maximum custodial sentence is hardly a limit at all: in the Italian legal system, there is basically no petty crime that would not allow law enforcement authorities to ask for the disclosure of the most sensitive information on the scale[413]. To be fair, it is very hard to set a reasonable scope with this kind of legal instrument: regulations work immediately throughout the entire Union, regardless of how the criminal codes punish crimes within one state's borders. There is no harmonized criminal code; the harshness of punishment is for the single nation to decide and the European Union has little to do with that. However, three years of maximum custodial sentence seems to be too generous, and the proposal itself tries to justify the choice, aimed at not undermining «the effectiveness of the instrument and its use by practitioners»[414]. Yet, this explanation does not seem to be fully satisfactory. If effectiveness had to be a concern in this phase, it would have been better served by setting no general limit. On the contrary: effectiveness should be properly balanced with the proportionality of state's action, or the outcome could be an odd, efficient tool that systematically harms more individual rights than it is necessary and reasonable to do.

Now, let's have a closer look at the procedure. The issuing authority – a court, a judge, a prosecutor – can resort to those Orders during the investigation or the trial and has to comply with a series of instruction provided by the draft regulation. The document shall specify the issuing and (if necessary) the validating authority; the provider that the measure addresses; the person whose data are to be disclosed; the requested data categories; the criminal statute whose alleged violation is being investigated; a couple of other technical details and, most importantly, the ground for the necessity and proportionality of the measure[415].

This last requirement is particularly relevant when the issuing authority is asking for the disclosure of content and transactional information: in this case, a judge or a court shall validate the order, which would be a hard thing to do without a reasoned explanation on why this measure has to be taken and why it is proportionate.

In all other cases (production order for less sensitive data; preservation order) the prosecutor can do everything on his own; nonetheless, the grounds on which the action is taken should be specified: the person whose data have been sought could later challenge the legality of the Order, especially on those grounds. In the first part of the procedure, however, these explanations will remain between the issuing authority and itself.

The Proposal also states that an Order can be issued if a similar action is allowed under the issuing state's law, which is a difficult condition to verify: one of the points of departure for this drafted regulation is exactly the absence of national provisions on direct cooperation with service providers, and it is not clear how to establish an analogy. If the order demands the disclosure of stored communication, the closest proxy could be the national 'interception of communications,' that is only allowed under different standards. It is as if the regulation would like to impose uniform standards across the countries, but also wanted these two Orders to blend in the national system: it seems hard to have it both ways. At the end of the day, it is plausible for this clause to be disregarded: the Proposal sets its own limits, which are way easier to control and verify.

413 See also Meijer Commitee, 'CM1809 Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters', *statewatch.org*, 18 July 2018, p. 1.
414 *Proposal*, p. 16.
415 The complete list of requirements is contained by articles 5 and 6 of the Proposal.

Another circumstance that should prevent the adoption of a Production Order is the fact that the disclosure of those data would harm fundamental interests of the addressee's state, such as its national security and defense; or that the information would be privileged under the addressee's state law. The first condition deals with the protection of the other county's most delicate balance, and it is bizarre that such an evaluation is left to a single judicial authority of a foreign country. Probably it will have no means to assess the impact that such a request should have on another State's national security, and it is why those requests were managed through MLA to begin with. This trait has also been noticed by a member state that, during the discussion of the proposal, has underlined that it is important to involve also the addressee's state in the early stage of the procedure, to avoid an erosion of the state's sovereignty[416]. The same goes for the second possible issue: the assessment is not as difficult, but the single authority is supposed to know the precise extent of another country's laws establishing privilege, which does not seem realistic. Moreover, if the Italian law authority asked Facebook for the content data – including the messaging history – of the person A, it could stumble upon privileged communications that they did not expect to find there in the first place. It is not possible to know in advance the full extent of what does a service provider have, and it could be complicated to establish in advance whether the information is protected by the other state's law.

Let us assume that the Order has been issued. It is not still enough to address the company: the issuing authority needs to complete a Certificate[417] that can be sent directly to the provider, without any communication with the state where the provider is established. The certificate contains all the information that the Order had to provide, except for the necessity and proportionality justification: that content shall remain confidential, not to put the investigation at risk.

The addressee has then 10 days upon the receipt to send the relevant data to the issuing authority; it the EPOC is incomplete or contains error, the company has 5 days to ask for clarifications through the form provided for by the Annex III of the proposal.

The provider informs the user of the disclosure, unless it is not asked to keep the request confidential; in this case, the issuing authority will have to inform the person without delay about the execution of an EPOC (but not of an EPOC-PR), or they can postpone such a notification until when it would not damage the investigation. According to the proposal, this provision has been shaped following the example of the EIO directive: its art. 19 provides for precautions to preserve confidentiality. This parallel, however, does not seem to hold too well: art. 19 of the Directive is addressed to a judicial authority of another member state, and not a private company. Only the last paragraph mentions banks, but it points out that the States should take the necessary measures to prevent them from disclosing their cooperation with an ongoing investigation. The approach seems radically different here: the general rule is that providers – a private corporation – can give notice to their clients unless they are explicitly prohibited to.

Assuming that the addressee is (or was) providing a service to the suspect and that the EPOC appears to be legitimate and complete, there is still a window of legitimate non-compliance

416 See the Note from the General Secretariat of the Council to the Delegations, Interinstitutional File n. 2018/0108(COD), June 26, 2018 (hereafter: Note), *eur-lex.europa.eu*, p. 6.

417 The Proposal also provides for the templates: the European Production Order Certificate (EPOC) template is referred to as Annex I; the European Preservation Order Certificate (EPOC-PR) as Annex II.

with the request, and the drafted regulation does envisage two main kinds of reasons for that: technical and legal.

As for the technical side, the data could have been canceled due to the ordinary data retention obligations, or upon request of the user. Those are listed under the 'de facto impossibility', that gives the provider a legitimate reason not to answer[418]. It could also avoid liability if it is not answering because of force majeure.

As for the legal reasons, the provider could take issue at the manifestly abusive EPOC or at the request that violates the Charter of Fundamental Rights of the European Union. If this is the case, the addressee can reject the EPOC and send a copy of the rejection form to its EU home-state, so that the competent authorities can ask for clarifications to the issuing authority.

Moreover, the EPOC could conflict with a third country's legislation on data disclosure, and at that point, the addressee would be put in a "damn you if you do, damn you if you don't" kind of situation. The conflict of obligation has to be notified to the issuing authority and argued in depth by the provider, that also must point out the rules that are relevant to the case and how they contradict the European obligation.

Both the evaluations require a deep knowledge of the law and the necessary skills to apply it, and they are quite extraordinary tasks to be assigned to the legal department of a private corporation. Besides, not all service providers are trillion-dollar-worth conglomerates with the necessary resources to hire the sharpest legal minds on the market: some of them are middle-sized companies and playing the judge would be quite demanding[419].

In case of non-compliance, however, the issuing authority can decide to ask the relevant member state to execute the measure: first, the Order has to be recognized. This approval should be given without formalities and would bring to a second round of cooperation with the original addressee, that can oppose the order again, for the same set of reasons. At that point, the executing state can impose sanctions.

The picture appears to be quite convoluted: the procedure is basically put in place since its inception, but carried out by the competent member state, which should act upon the Order written by a foreign authority. This step of the procedure is the only one to be directly linked to the principle of the mutual recognition (art. 82 TFEU), and yet it pointed to as the legal basis for the entire regulation.

5. The compact territoriality of the national state clashes with the diffused territoriality of the cloud and they are not easy to reconcile. Sure, unilateral action is a captivating method: it promises quick results, but it also unbalances the system. The providers are charged with a role for which that

418 To a certain extent, the *de facto* possibility depends on the policy of the provider: after the San Bernardino case, for instance, many messaging applications shifted to end-to-end encryption (before – among the mainstream apps – it was implemented by the secret conversations of Telegram): the message is stored in a server, but the company cannot open it; only the users (the two ends of that communication) have the key. For more on the topic, see: R. Budish, H. Burkert, U. Gasser, *Encryption Policy and Its International Impacts*.

419 Those expectations have already been defined as "unrealistic": see Note, p. 6-7. For another critical view on the point, see V. Mitsilegas, *The privatization of mutual trust in Europe's area of criminal justice. The case of e-evidence*, in *MJECL*, August 9, 2018.

they have no authority (or credibility)[420], the states go searching for information at the risk of harming even national security of another country.

This approach, however, does not seem consistent with the role of sovereignty as we know it. To implement a coherent solution, we should reconceptualize the concept to make it compatible with a liquid cloud. Besides, the other path forward is to give MLA a serious try, by investing in bilateral or multilateral treaties which could provide for easy and standardized procedures, secure portals for the presentation of the requests and a user-friendly system to check and answer them.

LAURA BARTOLI

420 It is just a step forward in a known direction; service providers have already been charged with institutional tasks: see E. Haber, *Privatisation of the Judiciary*, in Seattle University Law Rev., 2016, 115.