FORENSIC DATA GOVERNANCE IN EU: A CERTIFICATION FRAMEWORK FOR IOT DEVICES

Fausto Galvan / Federico Costantini

Fausto Galvan, Digital Forensics Expert, galvanfausto14@gmail.com

Federico Costantini, Researcher in Legal Informatics, University of Udine, Department of Law, Via Treppo 18, 33100 Udine, IT federico.costantini@uniud.it

Keywords: ***Data governance, Certification, Key escrow, Digital Forensics, Internet of Things, forensics as a service***

Abstract: *Addressing IoT (Internet of Things) technologies is becoming a crucial challenge in Digital Forensics, showing the limits of traditional approaches and data collection techniques. Our contribution envisages a "data governance" model based on third-party certification of forensic copies extracted from IoT devices. Within this framework, on the one hand, the certification establishes the technical standards to which manufacturers, distributors and service providers have to abide by in order to enter the EU market; on the other hand, it is eliminated the threefold conflict between the duties of investigating authorities, the interests of device manufacturers and the fundamental rights of the suspects. In conclusion are discussed benefits and disadvantages of our proposal, drawing a path for future research.*

1. Introduction: data governance, Digital Forensics and IoT

The term "governance" means a complex system of social regulation which applies in many sectors[1]. We can argue that such complexity also afflicts the concept of "public governance" which can be tackled under at least four different aspects. Indeed, it can be considered by the institutional level of involved authorities (international, national, local), it can be analysed by the mixed composition of public powers as defined by the traditional political science (legislative, executive, judicial), it can be also structured as an effort to coordinate beneficially the impartiality of public authorities with the interests of private entities (stakeholders) and, finally, it can be integrated by the intertwin of legal regulation and technological procedures. Concerning this last aspect. In this contribution we address these last two aspects, the latter having become nowadays very tightly connected[2].

It might be said that nowadays an effective "public governance" cannot be achieved unless including a thorough technological assessment and, in particular, developing a strategic approach towards information technologies. On this regard, it is noteworthy that this topic has been conceptualized as "data governance" and has been recently defined as "*power relations between all the actors affected by, or having an effect on, the way data is accessed, controlled, shared and used, the various socio-technical arrangements set in place to generate value from data, and how such value is redistributed between actors*"[3]. About that there is a lively

1 Governance, n.: Oxford English Dictionary. 3, Oxford, Oxford University Press, (2015).

2 Floridi (Ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer International Publishing, Cham, 2015.

3 Micheli/Ponti/Craglia/Berti Suman, Emerging models of data governance in the age of datafication, Big Data & Society, volume 7, issue 2, 2020, p. 2053951720948087.

discussion among experts on many aspects, as guiding principles[4], scope[5], components[6], challenges[7], economic impact[8]. Data governance, to sum up, defines the policies to adopt in the deployment of technological infrastructures in order to improve the quality of data.

The European Union is shaping its own "data governance". The year 2020 perhaps will be remembered not only for the pandemic disease, but also for having been a turning point in European history for the extraordinary improved effort put by the institutions in pushing towards innovation, as emerges in COM (2020)66[9]. The strategy outlined in this document has been recently made a first significant step further with the proposal of the "Data Governance Act"[10], which will create a new legal framework in which new actors will intermediate the exchange of data, increasing the reliability of the entire ecosystem. Among the many provisions included in the proposal, it is noteworthy the fact that data can be shared not only for profit, but also for general interest, which is defined as "data altruism" (Art. 2(10)) when processing can be delegated to special entities, namely "data altruism organisations" (Art. 15). Therefore, we can argue that this EU Regulation, if it will come into force, will not only guarantee the availability of public-owned data, allowing for example its re-use, but also widen their employment, increasing their added value for customers and companies.

The need of a more structured governance, as a crucial component in the process of digitalization, has emerged even in the judicial sector, especially with regard to electronic evidence. Indeed, among the many initiatives included in the "E-Justice" Strategy which have been implemented in last years[11], recently it has been pointed out the benefit deriving from a comprehensive harmonization[12] of existing services and platforms. Specifically, the most recent initiatives aim at integrating the exchange of data concerning evidence into the E-Codex platform[13], creating specific standards and ontologies[14]. Thanks to this approach, many improvements have been made after 20 years since the "Budapest Convention" of the Council of Europe[15], which symbolically constitutes the certificate of birth of international cooperation in this field.

The technological innovation which, according to some inspiring perspectives, is continuously accelerating[16], afflicts many aspects of our society. This trend has a significant impact on criminal investigations, since it can be claimed that digital forensics have inevitably become crucial in most of them[17].

---

4 Abraham/Schneider/vom Brocke, Data governance: A conceptual framework, structured review, and research agenda, International Journal of Information Management, volume 49, 2019, p. 424–438.

5 Alhassan/Sammon/Daly, Data governance activities: an analysis of the literature, Journal of Decision Systems, volume 25, issue sup1, 2016, p. 64–75.

6 Al-Ruithe/Benkhelifa/Hameed, Data Governance Taxonomy: Cloud versus Non-Cloud, Sustainability, volume 10, issue 1, 2018, p. 95.

7 Attard/Brennan, Challenges in Value-Driven Data Governance. In: Panetto, H./Debruyne, C./Proper, H.A./Ardagna, C.A./Roman, D. and Meersman, R. (Eds.), On the Move to Meaningful Internet Systems. OTM 2018 Conferences, Lecture Notes in Computer Science Springer International Publishing, Cham, 2018, p. 546–554.

8 Engels, Data Governance as the Enabler of the Data Economy, Intereconomics, volume 54, issue 4, 2019, p. 216–222.

9 A European strategy for data, COM/2020/66 final.

10 Proposal for a Regulation on European data governance (Data Governance Act), COM/2020/767 final.

11 E-Justice Action Plan 2009-2013, in OJ C 75, 31.3.2009, p. 1; E-Justice Action Plan 2014-2018, in OJ C 182, 14.6.2014, p. 2; Draft strategy on European e-Justice 2014–2018, in OJ C 376, 21.12.2013, p. 7. Velicogna, E-Justice in Europe: From National Experiences to EU Cross-Border Service Provision | SpringerLink. In: Alcaide Muñoz, L. and Rodríguez Bolívar, M. (Eds.), International E-Government Development Palgrave Macmillan, Cham, 2020, p. 39–72.

12 2019–2023 Action Plan European e-Justice, in OJ C 96, 13.3.2019, p. 9–32.

13 Council Conclusions 'Access to justice – seizing the opportunities of digitalisation' 2020/C 342 I/01, in OJ C 342I, 14.10.2020, p. 1–7.

14 For example: e-Evidence Digital Exchange System (eEDES). Biasiotti, A proposed electronic evidence exchange across the European Union | Digital Evidence and Electronic Signature Law Review, Digital Evidence and Electronic Signature Law Review, volume 14, 2020. See also www.evidence2e-codex.eu.

15 Convention on Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

16 Kurzweil, The singularity is near. When humans transcend biology, Gerald Duckworth, London, 2005.

17 A statistical analysis of the workload processed by an average forensic laboratory could demonstrate that in recent years forensic analysis performed on handheld devices has far exceeded that of traditional computers. In the laboratory of the Prosecutor's Office

In the near future, forensic experts will face many new challenges, especially with the massive adoption of IoT (Internet of Things) technologies. Indeed, in such a digital ecosystem the number of potentially interconnected devices, their vulnerability, the volatility of the storage units and the continuous exchange of information on open networks represent the major factors that greatly reduce the quality of the information available and which therefore limits the acquisition of genuine and reliable evidence. We argue that viable solutions, in this scenario, are made possible not only by enhancing the coordination among investigating authorities, by strengthening the cooperation among enforcement agencies and by the creation of interoperable systems and common standards – as designed by EU strategy – but also extending the actors involved in the process in order to include manufacturers, developers and distributors, on the one hand, and integrating automated processes of collection of relevant data, on the other. Therefore, we claim that an effective "data governance" has become vital in IoT forensics.

Our contribution envisages a model of data governance of electronic evidence suitable to be implemented in the EU framework and applied to IoT devices, whereby the creation of a public-private partnership based on a certification scheme combined with a third-party key escrow model. Indeed, we believe that the quality of the information carried by each single IoT device and exchanged in its environment can be standardized similarly to what happens in other technological sectors (e.g., certification of energy consumption by electric devices, cybersecurity clearance for 5G infrastructures[18]). Moreover, we deem that an independent agency would be optimal for issuing certifications and for monitoring the compliance with the said standards (as recently proposed in the field of artificial intelligence and robotics by the European Parliament[19]), acting as an impartial agent towards investigative authorities, judicial administration, public prosecutors and defendants.

The reminder of this contribution is as follows. In Section 2 we analyse our first tenet, namely the cooperation between public authorities and the private sector focusing on the field of ICTs, in order to remark the fact that this model is not entirely unknown and could be reliable also in Digital Forensics. In Section 3 we deepen the second assumption, regarding the intertwin between legal regulation and technological processes, showing how the acquisition of electronic evidence from IoT devices could be simplified and automated implementing a third-party escrow schema based on the extraction of data coupled with a HASH function. In the conclusion we balance drawbacks and benefits and offer some final evaluations.

2. Data governance and IoT Forensics: a certification agency to compose conflicts between public authorities, manufacturers and users

Twenty years after the aforementioned Budapest Convention on Cybercrime, many things have changed. Legislators worldwide have adopted new approaches to regulation, increasingly implementing "soft law" techniques. Such a trend, which can be claimed as parallel to the spreading of "governance" methods, originated as an instrument of self-regulation of international commercial relations and is characterized by the fact that rules are spontaneously respected by the interested parties, creating trust towards the environment in which

of the Udine (Italy), for example, it has been observed an exponential surge (almost 2000%) of mobile devices forensic analysis and it is foreseeable a further increase in the future.

18 See for Italy, Decreto del Presidente del Consiglio Dei Ministri 30 luglio 2020, n. 131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, in GU n.261 del 21-10-2020. https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg.

19 European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

they operate, thus reinforcing their strength. In other words, the effectiveness of the regulation is based on the accountability of the stakeholders[20].

The so-called "soft law" has been used by the European Union since its awakening in order to harmonize the legal systems of the Member States and, increasingly, as a tool for regulating the internal market. In this second case, and especially in the technological sector, this regulatory approach has shown remarkable results due to the integration of legal rules and industrial standards. Indeed, the duty of assuring certain levels of quality in products and services has been delegated to specific agencies, vested with the authority of issuing certifications to manufacturers in order to enable them to compete with each other in the EU market. Through this model, market regulation has been able to achieve a flexibility and a proactivity that would have been impossible with legal provisions based on the binominal obligation / penalty brought by traditional general theory of law[21].

It is remarkable to point out some cases in which such a model has already been deployed. Indeed, the certification model is contained in several recent pieces of legislation, as the "Cybersecurity Act" of 2019[22] whose article 48 contains a request to ENISA propose a European cybersecurity certification scheme (ECCG), or the GDPR, which allows the creation of codes of conduct for operators in a given economic sector (article 40 GDPR) and the use of product and service certification mechanisms (article 42 GDPR)[23]. Moreover, a recent proposal of Regulation[24] describes a procedure for requesting an ethical certification for "high risk" technological artifacts deploying artificial intelligence, robotics and related technologies. We can argue that the European Union has shown to be keen to a broader adoption of the certification model because it allows a proactive approach to "future-proof solutions".

As mentioned in the introduction, the exponential surge in the number and variety of electronic devices makes it necessary and urgent to change the traditional approach to Digital Forensics. Indeed, it is not foreseeable that the procedures provided by current Computer Forensics will still be adopted in the field of IoT, however agreed by the community of experts they might be. Moreover, it is unacceptable that any new approach could end up reducing fundamental rights and individual freedoms and allowing an arbitrary exercise of power by police authorities. One of the first objectives of "data governance" in this field should be to raise awareness in public opinion and stakeholders that the quality of forensic data is a value to be pursued in all circumstances, not depending on the possibility of a trial, and that it concerns everyone, not just those who may per involved in it.

We believe that the simplest way to obtain this result is to establish that IoT devices – those fulfilling binding requirements – entering the European market should comply with certain standards, including the possibility to create a forensic copy of their storage units in the most complete way. It goes without saying that it is very unlikely even to enter such a negotiation with global players at national level. Therefore, we can hypothesize the institution of an agency of sort by the EU, which in this contribution we will call EECA (Electronic Evidence Certification Authority), or the empowerment of existing authorities already operating as a EU organism (e.g., ENISA). This entity would essentially be responsible for verifying that the devices introduced in the EU market comply with the required technological standards. In a nutshell, it would attribute to market operators a kind of accountability that otherwise they would not have.

---

20 Guzman/Meyer, International Soft Law, Journal of Legal Analysis, volume 2, issue 1, 2010, p. 171-224, Di Robilant, Genealogies of Soft Law, The American Journal of Comparative Law, volume 54, issue 3, 2006, p. 499-554, Sheldon, Soft Law. In: Armstrong, J.D. (Ed.), Routledge handbook of international law Routledge, London; New York, 2014, p. 68–80.

21 In the ICT sector, for example, a crucial role has been played by the ISO / IEC 27000 on information security, while for digital forensics it is also relevant the quality of information, provided by ISO / IEC 25000.

22 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in OJ L 151, 7.6.2019, p. 15–69.

23 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in OJ L 119, 4.5.2016, p. 1–88.

24 Framework of ethical aspects of artificial intelligence, robotics and related technologies, adopted by the European Parliament on 20 October 2020, P9_TA(2020)0275).

The essential purpose of EECA is to neutralize a twofold conflict: between investigative authorities and manufacturers, on one side, and between prosecutors and defendants, on the other. The first pertains to the direct access to devices, which is claimed by officers, especially in criminal investigations, on one hand, and it is refused by manufacturers to avoid intrusions on industrial secrets and strategic know-how, on the other. As examples in this sense, we can mention the "Clipper Chip"[25] dispute of the Nineties and the more recent one between F.B.I. and Apple in the aftermath of the San Bernardino attack of 2015[26]. The second regards the risks of contamination and manipulation of the source of evidence, since EECA would be vested with the maximum impartiality towards each actor involved in a trial. We believe that the trustworthiness of the agency, under these two aspects, would be based on the fact that its role is merely technical, so less prone to be strumentalized or manipulated. In our proposal the balance of the conflicting interest is obtained by the fact that detectives do not access the device but the forensic copy extracted which is owned by them. The same copy remains available for disclosure according to the defendant's rights granted by the criminal procedure system of the Member State where the trial is based.

3. A double-layered IoT forensic data governance model

In order to explain the technical details of our proposal, we offer a preliminary outlook on the most common issues emerging in an ordinary workflow in which a physical device is analysed for forensic purposes, then we describe a valid solution that has been actually deployed in the Netherlands. After that, we outline our proposal briefly describing its technical details and the resulting procedure of collection of electronic evidence. Our proposal can be represented as composed by a two-layered model, the first being a "security mark" that manufacturers should be required to obtain for their IoT devices in order to market them within the EU, while the second is qualified by the implementation of a HASH function to the data extracted from the target device.

3.1. The first layer of certification: a decentralized forensic data governance

Let's assume that a device is legitimely seized during an investigation. To begin with, after having acquired the device law enforcement agents should have to carry them to a laboratory which should be available in a reasonable time, ready to operate, supplied with cutting-edge – and so, expensive – technologies, geographically near to the prosecutors' offices where investigations are being conducted or to the courts where trials will be held. Needless to say, sometimes in real life these preliminary conditions aren't always concurring at the optimum combination. Secondly, after the analysis, the laboratory should return the device to requesting officers together with a report listing the performed technical operations and describing the results obtained. About that, concerns can arise from the reliability of tools employed, especially due to the fact that manufacturers or distributors usually introduce built-in security measures to protect information contained in their products or services. In other terms, every forensic data extraction is done bypassing such hurdles, mostly without the cooperation of the producers of the devices[27], and overcoming many other difficulties, such as exploiting "0-day" vulnerabilities, or adapting to different models which, although bearing the same name, are constantly

[25] https://en.wikipedia.org/wiki/Clipper_chip.

[26] Costantini/De Stefani, Collecting evidence in the «Information Society»: theoretical background, current issues and future perspectives in «Cloud Forensics». In: Schweighofer, E./Kummer, F./Hötzendorfer, W. and Sorge, C. (Eds.), Trends un Communities des Rechtinformatik. Tagungsband des 20. Internationalen Rechstinformatik Symposion / Trends and Communities if Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium, 326, Österreichische Computer Gesellschaft, Wien, 2017, p. 461–468.

[27] Galvan/Costantini/Battiato, A Case Study for an "Accountable" IoT Forensics. In: Schweighofer, E./Hötzendorfer, W./Kummer, F. and Saarenpää, A. (Eds.), Verantwortungsbewusste Digitalisierung / Responsible Digitalization. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020 / Proceedings of the 23rd International Legal Informatics Symposium IRIS 2020, Colloquium, II.28, Weblaw, Bern, 2020, p. 533–542, Costantini/De Stefani/Galvan, The «Quality of Information» Challenges in IoT Forensics: An Introduction, Jusletter IT, issue 21 February 2019.

improved and released into the market[28], or even to different operating systems, which are monthly, even if slightly, upgraded. Lastly, since normally the detectives and the technicians of the forensic laboratory cover different roles and develop different expertise, the firsts being the only one aware of the context of the investigation, and the seconds dealing only with the task to extract data, it might be that some information obtained could be useless to the investigators, or, conversely, that analysts could have overlooked essential information.

There have been many initiatives aimed at simplifying the workflow while strengthening the "chain of custody" of electronic evidence. Among them, remarkable in our view is the solution elaborated by a group of scholars in 2006 and implemented in the Netherlands since 2012[29]. In this model, detectives are enabled to upload any sort of data – so called "traces" – into a cloud archive owned by central laboratory, where they can be remotely analysed by experts, thus the concept of "forensics as a service", thus allowing law enforcers to obtain timely intelligence suitable to be exploited in the early phases of investigations. Namely, when they can be more effective in solving them.

Among the many advantages of the model just mentioned, there is a feature that can be improved, which pertains to the topic of this year's IRIS conference: the "data governance" of electronic evidence. Such centralized model, indeed, could be optimal in most cases, but – at least – it lacks flexibility and adaptability to specific conditions. Furthermore, it does not define a proactive and comprehensive strategy which could provide a concrete and enduring benefit for the whole system. In other words, we believe that when it comes to IoT forensics, decentralization and scalability should be prioritized as leading organizing principles, as well as design specifications should be adopted by manufacturers in order to automate extraction of data featured by high quality.

These further conditions can be obtained introducing the "security mark" as anticipated in the introduction of this section. We propose that manufacturers could be requested to submit their products to the approval of the EECA as a prerequisite to introduce them into the EU market. In order to obtain such certification, the design of IoT devices should include a cloud service which should be available for the extraction of a "forensic copy" by law enforcers. It is remarkable, in this model, that detectives do not access the devices directly, neither opening them physically nor manipulating their content, being their activity limited to connect the device to a certified pc and extract the certified copy of archived data. To sum up, the access granted to investigative authorities should have no "write" authorization (only the extraction of data), should be allowed only under specific conditions (mainly an authorization issued by a judge) and should be limited to a defined outcome (the forensic copy of the archive). Defendants, of course, should have the same privileges.

3.2. The second layer of certification: HASH function and third-party escrow

The second layer of certification is granted by applying a HASH function to the data extracted in order to guarantee the genuinity of the forensic copy. In this paper we can define a hash function as an efficiently computable[30], collision free[31] and not invertible[32] mathematical function which takes any string as input, and produces a fixed-size (i.e., 256 bit) string as output. Such a definition allows to stipulate that:

1. Any file of any length (a single image, a text file, or an entire bitstream copy of a hard disk) can be mapped in a fixed-length string[33]. The time needed for this "transformation" depends on the size of the original data stream, and goes from a few seconds to some minutes;

[28] As an example of this huge number of models, see https://it.wikipedia.org/wiki/Samsung_Galaxy which only includes the list of "Samsung Galaxy" models from June 2009 to April 2019.

[29] van Baar/van Beek/van Eijk, Digital Forensics as a Service: A game changer, Digital Investigation, volume 11, 2014, p. S54-S62, van Beek/van Eijk/van Baar/Ugen/Bodde/Siemelink, Digital forensics as a service: Game on, Ibid., volume 15, 2015, p. 20–38, van Beek/van den Bos/Boztas/van Eijk/Schramp/Ugen, Digital forensics as a service: Stepping up the game, Forensic Science International: Digital Investigation, volume 35, 2020, p. 301021.

[30] For every input, in a reasonable amount of time, it is possible to find the output.

[31] Nobody can find values x and y, such that x and y are different, and H(x)=H(y).

[32] Given the output H(x), there's no feasible way to figure out what the input x was.

[33] Usually, the output of a hash function is a string of 128, 256 or 512 bits.

2. Even if surely different strings of bits can collide to the same HASH, since the number of possible *n*-bits strings are limited to 2^n whereas the number of possible inputs of the hash function is virtually infinite, there are no known algorithms suitable to find 2 different strings with the same HASH. The consequence is that, starting from a data stream, nobody can (that is, there aren't computers able to) find a different data stream with the same HASH. Applied to our certification framework, this property ensures us that we can't "duplicate" our extracted data with another set of data having the same HASH.
3. It's impossible, from a given hash, to obtain the data stream which has that hash as output. This means that, starting by the hash of data extracted from a device, nobody can reconstruct the content of the device itself.

A mathematical function with the three properties just described can be used also to mark a digital content of whatever length, since once done this, it would be impossible for someone both to understand which is the original starting set of data, and to produce (in acceptable time) another set of data with the same HASH.

This last feature is the main reason why the HASH function is well-known by scholars and practitioners, especially in information security and moreover forensic analysis. Indeed, it is applied to the data collected in order to assure the genuinity and integrity of evidence[34]. We suggest that a HASH string should be automatically generated by the process of extraction from the cloud of the IoT device inspected, and at the same time made available to detectives and directly sent – or uploaded – to a database owned by the EECA.

The result of the process would be threefold. First, investigative authorities do not need direct access with the device – in fact, they do not need even physical contact with it – since the acquisition of data does not require its apprehension, thus manufacturers are not required to share trade secrets or technical details with governments or companies. Second, since the generation of the HASH string is automated, it cannot be influenced by any human intervention, so tampering evidence becomes very improbable. Third, the EECA operates as third-party escrow of the HASH function, namely the only piece of information the genuinity of the evidence depends on. Each interested party – defendants, *in primis* – should be allowed to access the EECA archive – even remotely, of course – in order to verify the concordance between the HASH string associated with the forensic copy of the IoT device storage and the HASH string registered in the EECA database. A match between the HASH strong enclosed in the prosecutor's office casefile and the HASH string recorded in the EECA database should warrant the integrity of the electronic evidence.

4. Conclusions

Despite how far and improbable might be the moment in which our proposal becomes effective – we are fully aware that introducing a technological standard or a certification scheme is a very complex matter – the fact is that the EU is moving towards a wider adoption of both "governance" and "soft law" approaches as a way to implement the principle of "proportionality" (Article 5(4) TEU) while it is increasing the integration between traditional legislation and technological standards in order to maintain a flexible and adaptable approach to complexity. In our model, the challenges presented by IoT forensics can be addressed as a matter of "data governance" within the same institutional framework described.

Of course, there are some disadvantages: to begin with, cloud storage would be sustainable only for some kind of devices (e.g., TV, video surveillance) or some sort of data (e.g., images, geotagging) or purposes (e.g., public tenders, high risk infrastructures), not for every kind of device introduced in the EU market, thus the range of data collection is significantly limited. Secondly, the HASH signature could become obsolete with the introduction of new technologies, such as quantum computation, therefore another technology should be adopted. Finally,

[34] Roussev, Vassil, Hashing and Data Fingerprinting in Digital Forensics, IEEE Security & Privacy Magazine, 7.2 (2009), 49–55, https://doi.org/10.1109/MSP.2009.40, Lakshmi, K. Aishwarya/Honnavali, Prasad B./Rajashree, S., Ensure the Validity of Forensic Evidence by Using a Hash Function, Inventive Communication and Computational Technologies, 2021, 341–46 https://doi.org/10.1007/978-981-15-7345-3_28.

the creation of EECA will increase the already significant number and variety of EU institutions, if not overlap or duplicate with existing competences (ENISA, at least). We believe that these drawbacks can be properly addressed and that our proposal could be integrated into the ongoing development of E-CODEX.

There are also possible further implementations or variants to be considered: the certification could be voluntary in some cases and obligatory in others, EECA could result by the coordination of country-based delegations or agencies in order to increase decentralization and avoid bottlenecks, the process of extraction could be limited to specific data instead of aiming at copying the whole archive in order to better comply with privacy requirements, the data extracted could be formatted in an XML schema in order to include them into current ontologies and increase the automation of the whole ecosystem.

In the future we intend to deepen the details of our proposal and improve its technical accuracy.

Acknowledgement

This chapter is the result of joint research of the co-authors. Specific individual contributions can be attributed as follows: Federico Costantini, paragraphs 1, 2; Fausto Galvan, paragraph 3 and 4. The authors express their gratitude to Marco De Stefani for his precious suggestions.

References

Governance, n.: Oxford English Dictionary. 3, Oxford, Oxford University Press, 2015.

Abraham, Rene/Schneider, Johannes/vom Brocke, Jan, Data governance: A conceptual framework, structured review, and research agenda, International Journal of Information Management, volume 49, 2019, p. 424–438.

Al-Ruithe, Majid/Benkhelifa, Elhadj/Hameed, Khawar, Data Governance Taxonomy: Cloud versus Non-Cloud, Sustainability, volume 10, issue 1, 2018, p. 95.

Alhassan, Ibrahim/Sammon, David/Daly, Mary, Data governance activities: an analysis of the literature, Journal of Decision Systems, volume 25, issue sup1, 2016, p. 64–75.

Attard, Judie/ Brennan, Rob, Challenges in Value-Driven Data Governance. In: Panetto Hervé, Debruyne Christophe, Proper Henderik A., Ardagna Claudio Agostino, Roman Dumitru, Meersman Robert (Eds.), On the Move to Meaningful Internet Systems. OTM 2018 Conferences, Lecture Notes in Computer Science Springer International Publishing, Cham, 2018, p. 546–554.

Biasiotti, Maria Angela, A proposed electronic evidence exchange across the European Union | Digital Evidence and Electronic Signature Law Review, Digital Evidence and Electronic Signature Law Review, volume 14, 2017.

Engels, Barbara, Data Governance as the Enabler of the Data Economy, Intereconomics, volume 54, issue 4, 2019, p. 216–222.

Floridi, Luciano (Ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer International Publishing, Cham 2015.

Kurzweil, Ray, The singularity is near. When humans transcend biology, Gerald Duckworth, London, 2005.

Lakshmi, K. Aishwarya/Honnavali, Prasad B./Rajashree, S., Ensure the Validity of Forensic Evidence by Using a Hash Function, Inventive Communication and Computational Technologies, 2021, 341–46 https://doi.org/10.1007/978-981-15-7345-3_28.

Micheli, Marina/Ponti, Marisa/Craglia, Max/Berti Suman, Anna, Emerging models of data governance in the age of datafication, Big Data & Society, volume 7, issue 2, 2020, p. 2053951720948087.

Roussev, Vassil, Hashing and Data Fingerprinting in Digital Forensics, IEEE Security & Privacy Magazine, 7.2 (2009), 49–55, https://doi.org/10.1109/MSP.2009.40.

Velicogna, Marco, E-Justice in Europe: From National Experiences to EU Cross-Border Service Provision | SpringerLink. In: Alcaide Muñoz L., Rodríguez Bolívar M. (Eds.), International E-Government Development Palgrave Macmillan, Cham, 2020, p. 39–72.