A Case Study for an “Accountable” IoT Forensics

A CASE STUDY FOR AN «ACCOUNTABLE» IOT FORENSICS

Fausto Galvan / Federico Costantini / Sebastiano Battiato

Law Enforcement agent at the Public Prosecutor office at the Court of Udine and Digital Forensics Expert, galvanfausto14@gmail.com
Researcher, Department of Law – University of Udine, Via Treppo 18, 33100 Udine IT, federico.costantini@uniud.it,

Full Professor of Computer Science, Department of Mathematics and Computer Science, University of Catania, viale Andrea Doria 6, 95125 Catania IT, battiato@dmi.unict.it

Keywords: ***IoT, Internet of Things, Digital Forensics, Accountability, Information Quality***

Abstract: *IoT (Internet of Things) promise great potentials but pose many concerns. Billions of devices connected in global networks exchanging enormous amounts of data, indeed, can be highly vulnerable. Accountability is a crucial feature to foster awareness and reduce risks at all levels, yet it is difficult to put in practice when it comes to evaluate digital evidences in an IoT environment. In this paper we propose a formula for assessing Quality of Information in IoT devices for forensics purposes. After a short theoretical overview, we describe our tool and provide an example in order to show how its adoption can increase the transparency in the discussion of digital evidences*

1. Introduction

We are currently witnessing the advent of many concurring innovations, most of which involve ICTs: Artificial Intelligence, Cloud Computing, Distributed Ledger Technologies, Internet of Things, Big Data, 5G, just to name the most widely known. Their impact is said to be «disruptive» since it produces changes of great magnitude which are also mainly irreversible and unpredictable.[1] One of the main risks is that, while business companies are rushing for their introduction into market, concerns by public opinion are often afflicted by ideological and cultural biases and, based on that, policy makers sometimes make regrettable short-termed choices. In order to allow a «co-evolution» of technology and society[2] it is required the development of an ethical framework of «responsible digitalization» capable to provide guidance for a sustainable future.

In this scenario, it is crucial to guarantee the highest transparency in all processes in which technologies are involved sharing in an inclusive way the many advantages they can bring. This aim, in general, places in a special position especially those who are involved in designing new technologies and those who put them in use, since they are, as a matter of fact, «accountable» of their actions. Accountability is crucial in fiduciary positions held on behalf of third parties, which are not directly involved in decisions that an agent has to make.[3] The third party has the power to set a certain policy under which decisions have to be made by the agent, who

---

1 Christensen/Bower, Disruptive technologies: Catching the wave, The Journal of Product Innovation Management, volume 1, issue 13, 1996, p. 75–76, Christensen, The innovator's dilemma : the revolutionary book that will change the way you do business, 2011, Christensen/Raynor/McDonald, What is disruptive innovation?, Harvard Business Review, volume 93, issue 12, 2015, p. 44–53, Yu/Hang, A Reflective Review of Disruptive Innovation Theory, International Journal of Management Reviews, volume 12, issue 4, 2010, p. 435–452.

2 Book Symposium on Homo Sapiens Technologicus: Philosophie de la Technologie Contemporaine, Philosophie de la Sagesse Contemporaine By Michel Puech Editions Le Pommier, 2008, Pagallo/Casanovas/Madelin, The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data, The Theory and Practice of Legislation, 2019, p. 1–25, Ronzhyn/Wimmer, Literature Review of Ethical Concerns in the Use of Disruptive Technologies in Government 3.0. ICDS 2019: The Thirteenth International Conference on Digital Society and eGovernments, 2019.

3 Küsters/Truderung/Vogt, Accountability: definition and relationship to verifiability. Proceedings of the 17th ACM conference on Computer and communications security, 2010, p. 526–535.

is required not only to act according to said policy but also to explain the reasons for her/his choices. Accountability is fundamental also in judicial proceedings, when experts are summoned to provide explanations on assumptions, methods and results of their analysis, contributing to the discussion on the evidences admitted in trial. Due to that, legal arguments can be upheld by parties and decisions can be taken by the judge without specific forensic competences and skills, yet based on the knowledge of the circumstances in the case debated.

In digital forensics, accountability is one of the challenges which has become harder with «disruptive technologies». Indeed, such discipline, aimed to improve a methodology to access, capture and crystallize data to be brought in court,[4] has to keep the pace with several issues, such as cryptography (decentralized ledger systems), virtualization of resources (in cloud computing), «black box» outcomes (in artificial intelligence). Provided that, it can be argued that IoT technologies raise three main concerns: (1) the selection of information to be acquired since, on one hand, a great amount of data cannot be analyzed efficiently and, on the other, their relevance has to be justified; (2) the degree of uncertainty has to be assessed in order to allow an evaluation of the overall confidence of the analysis; (3) the choice of the tools has to be explained, especially if the acquisition cannot be repeated again under the same conditions. In a nutshell, it can be said that, in digital forensics, accountability pertains to the information quality (henceforth, also IQ) delivered into the judicial proceeding.

Since IoT technologies allow an extensive and permanent flow of information, the problem of IQ is crucial, especially if the interaction is not filtered by human supervision.[5] Indeed, data are spread across an undetermined set of connected devices (e.g. in their type, number, and location);[6] machines are afflicted by different kinds of security vulnerabilities, therefore being exposed to attacks, communications can be unprotected (even unencrypted) – allowing third-party manipulation – and storage units could not grant secure access credentials. Furthermore, due to the high interdependence among devices, any anomaly can spread rapidly in an IoT ecosystem and flood outwards, thus criminal activities, even serious or destructive, can remain untraced. Moreover, IoT can produce anomalies which are unperceivable by human users, thus frustrating countermeasures or remedies.

Forensic analysis of digital evidence in IoT environment poses several challenges.[7] As a matter of fact, methods tested as valid for isolating devices in «chain of custody», as in «classical» digital forensics, are not effective, due to the continuous and deep interaction among devices. Indeed, IoT forensic analysis requires both cutting-edge technological solutions and new methodological approaches in order to grant integrity, authentication, and non-repudiation of digital evidence.

In this paper we present a tool for assessing Information Quality in IoT forensics, thus fostering the accountability of forensic expertise. Indeed, in our research[8] we have established a method that allows to perform a comparative estimation of the trustworthiness of digital evidences under different aspects and criteria. We claim that such method is particularly effective in the forensics analysis of a set of IoT devices, where a thor-

4 Palmer, A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS), New York, 2001.

5 Karkouch/Mousannif/Al Moatassime/Noel, Data Quality in Internet of Things: A state-of-the-art survey, Journal of Network and Computer Applications, volume 73, 2016, p. 57–81.

6 Zareen/Waqar/Aslam, Digital Forensics: Latest Challenges and Response. 2013 2nd National Conference on Information Assurance (NCIA) IEEE, Piscataway, NJ, 2013, p. 21–29.

7 Hegarty/Lamb/Attwood, Digital Evidence Challenges in the Internet of Things. Proceedings of the Tenth International Network Conference (INC) 2014 School of Computing & Mathematics Plymouth University, Plymouth, 2014, p. 163–172, Hossain/Karim/Hasan, FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 2018 IEEE International Congress on Internet of Things (ICIOT) IEEE, 2018, p. 33–40, Zawoad/Hasan, FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. 2015 IEEE International Conference on Services Computing IEEE, 2015, p. 279–284, Meffert/Clark/Baggili/Breitinger, Forensic State Acquisition from Internet of Things (FSAIoT): A General Framework and Practical approach for IoT Forensics through IoT Device State Acquisition. Proceedings of the 12th International Conference on Availability, Reliability and Security ACM, Reggio Calabria, Italy, 2017, p. 1–11.

8 Costantini/De Stefani/Galvan, The «Quality of Information» Challenges in IoT Forensics: An Introduction, Jusletter IT, issue 21 February 2019, 2019.

ough transparency of tenets, methods and outcomes is very difficult to achieve and moreover to communicate efficiently to others. After a short theoretical premise, we describe the method explaining the formula which formalizes it and then we offer an example in order to show how it could work on some of the most common devices. At the end, we provide some final observations and draw paths for future investigations.

2. Theoretical background: information, «quality of information» and IoT Forensics

In last twenty years a new approach has been spreading worldwide, the «Philosophy of Information» of Luciano Floridi.[9] According to this vision, «information» has three ontological statuses: (1) «information *as* reality», for example the electrical signal, which is transmitted regardless of the message contained; (2) «information *about* reality», such as information about natural phenomena, which can be true or false (hence in philosophical terms can be said to be «alethic») and (3) «information *for* reality», which conveys instructions or algorithms to one or many recipients.[10] In the original exposition of the theory of communication, similar concepts were expressed as different «levels», respectively as «technical», «semantic», and «influential»,[11] while cybernetics, previously defined three different kind of information: «technological», «natural», and «cultural».[12] This view has not only nurtured among scholars, but also influenced public opinion and gained credit at an institutional level,[13] being taken into consideration in many EU ethical guidelines[14] which aim at informing decision-makers, assisting stakeholders and raising awareness in public opinion on challenges to be faced in the near future. What is at stake is, at the end, the concept of humanity in itself.[15] In this paper we adopt this perspective as theoretical model since it is suitable to address in a more wider perspective the problem we are tackling.

It is noteworthy that the ontology provided by «Philosophy of Information» has been specified to the issues of IQ. Indeed, scholars have proposed different criteria of classification – distribution, heterogeneity, and autonomy – which allow one to establish six different types of information systems (monolithic, distributed, data warehouses, cooperative, cloud, and peer to peer).[16] One of the most interesting features of IQ is that it can be directly connected to the quality of the decisions that are based upon it. In this sense, an agent – either human or artificial – is influenced not only by shortage or by overload of information, but also by its quality. IQ, in short, is crucial for the outcome of the process, that is the utility of the decision in itself. Therefore, IQ can be studied under the same three perspectives shown before:[17] (1) «quality in information *as* reality» measures the affordability of the means implemented to transfer information and emerges for example in the

9 Floridi, The Philosophy of Information, Oxford University Press, Oxford, 2013, Floridi, The 4th Revolution. How the Infosphere is reshaping Human Reality, Oxford University Press, Oxford, 2014, Floridi, The Ethics of Information, Oxford University Press, Oxford, 2013, Durante, Ethics, Law and the Politics of Information. A Guide to the Philosophy of Luciano Floridi, Gordijn, B. and Roeser, S., The International Library of Ethics, Law and Technology, 18, Springer, Dordrecht, 2017.

10 Lundgren, Does semantic information need to be truthful?, Synthese, 2017, Dretske, Knowledge & the flow of information, MIT Press, Cambridge, Mass., 1981.

11 Weaver, The Mathematics of Communication, Scientific American, volume 181, issue 1, 1949, p. 11–15.

12 Borgmann, Holding on to reality. The Nature of Information at the turn of the Millennium, University of Chicago Press, Chicago, 1999.

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

14 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI. European Union, 2019, High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendations for Trustworthy AI. European Union,2019, Floridi/Cowls/Beltrametti/Chatila/Chazerand/Dignum/Luetge/Madelin/Pagallo/Rossi/Schafer/Valcke/Vayena, AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines, volume 28, issue 4, 2018, p. 689–707.

15 Harari, 21 Lessons for the 21st Century, Jonathan Cape, London, 2018.

16 Batini/Scannapieco, Data and Information Quality: Dimensions, Principles and Techniques, Springer Publishing Company, Incorporated, 2016.

17 Floridi/Illari, The Philosophy of Information Quality, Synthese library, 358, Springer, Berlin-Heidelberg, 2014.

traditional problem of reducing noise, distortion, or losses in signal transmission; (2) «quality in information *about* reality» measures the reliability of the information provided in representing the related events and is concerned with the dissimilarity of information to the facts to which it refers; (3) «quality in information *for* reality» measures the trustworthiness of the agent who receives information or, generally, of those involved in further processes, and has to be addressed when processes present inconsistencies, loopholes, or conflicts.

We can implement the model provided by the «Philosophy of Information» to digital forensics, drawing the following tripartite classification: (1) Digital forensics quality in «information *as* reality» is relevant in order to preserve the integrity of the collected information, and it is epitomized in the concept of «chain of custody»[18]; (2) Digital forensics quality in «information *about* reality» is concerned about the trustworthiness of the representation of events, which has to be verified with other sources of evidence; (3) Digital forensics quality in «information *for* reality» is involved in the discussion of evidence among parties (inquiring authorities, defendants, judges, forensics experts). As we know, judicial trials have to proceed according to precise rules which establish specific requirements for admissibility and the burden of proof. Here also external variables can make a difference, such as personal competences of the agents involved, «soft skills» (argumentation abilities, trial strategies), cost of analytical tools, and available time.

Consequently, we can classify the issues raising in IoT forensics according to the same pattern, as follows: (1) IoT forensics quality in «information *as* reality» addresses the fact that it is difficult to isolate a single device or crystalize a specific piece of information, since the boundaries of relevance are blurred[19]; (2) IoT forensics quality in «information *about* reality» pertains the fact that it is problematic to detect a specific source, to trace the chain of interactions, or to measure the influence of a single item in shaping the representation of an event, since «correlation is not causation»; however, the IoT is, above all, a matter of correlation; (2) IoT forensics quality «in information *for* reality», where the challenge is to demonstrate the compliance to legal and technical procedures. Under this perspective, the human factor plays a part along with technological variables, as shown in digital forensics and the role of accountability is crucial.

Ontological status of Information	**Quality of Information; level of analysis**	**Quality of Information in Digital Forensics**	**Quality of Information in IoT Forensics**
Information *as* reality	Traditional theory of communication	Chain of custody	Relevance[20]
Information *about* reality	Consistency with other represented facts	External validation with other sources of evidence	Uncertainty[21]
Information *for* reality	Logical coherence	Adjective rules (admission & burden of proof)	Accountability[22]

Table 1: IQ tripartite analysis and IoT issues

[18] The «chain of custody» entails the measures to ensure «the collection of evidence in electronic form of a criminal offence» (article 14 §.2 lett. b) as enforced pursuant art. 14 of the CoE Convention n. 185 on Cybercrime signed in Budapest in 2001. This procedure is described by several technical standards, see ISO 27001:2017, ISO/IEC 25012:2008, ISO/IEC 27037:2012, ISO/IEC 27041:2015, ISO/IEC 27042:2015, ISO/IEC 27050-1:2016.

[19] Wills/Alenezi/Zulkipli/Huda, IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security Scitepress, 2017, p. 315–324, Conti/Dehghantanha/Franke/Watson, Internet of Things Security and Forensics: Challenges and opportunities, Future Generation Computer Systems, volume 78, 2018, p. 544–546.

[20] The purpose of the «chain of custody» is to restrain the scope of the admissible evidences in court, so excluding those which cannot be considered relevant to the decision of the case.

[21] The accuracy in the analysis of IoT devices can be measured evaluating the exchange of data in its environment.

[22] Choices concerning technical or legal procedure adopted are really transparent when they can be understood by third parties, regardless specific skills or abilities.

3. Description of the IQA formula for IoT forensics

As observed above, the pipeline that leads to the assessment of IQ in a set of data hangs on different factors, many of whom cannot be precisely quantified but only estimated[23]. Since the very beginning of this research, in the various steps devoted to clarify this procedure, beside the theoretical approach, we developed a set of formulas with the goal to give a more pragmatic comprehension of the issue.

In our analysis[24], we assumed that, under the hypothesis of an investigative scenario where the digital evidences are collected from a set of n IoT devices, is possible to model the IQ of the information extracted from them introducing a percentage coefficient, that we named IQA (Information Quality Assessment), defined as follows:

$$\mathrm{IQA} = \frac{\sum_{i=1}^{n} (DTC_i + DST_i + CS_i + CM_i + SR_i + PC_i + TDA_i + OT_i + OS_i)}{9n} \times 100 \quad (1)$$

where:

- i = i-th device;
- DTC = device technical status;
- DST = device security status (confidentiality, integrity, availability, …);
- CS = cloud service security status;
- CM = cloud service manipulation of raw data;
- SR = source reliability;
- PC = privacy (GDPR) compliance;
- TDA = technical data accessibility;
- OT = observer technological advancement;
- OS = observer skills;

Allowed values are all decimal between 0 = «bad» and 1 = «good».

The above terms can be aggregate according to the theoretical background, and in particular with the general model proposed in Section 2, producing the classification shown in Table 2. Subsequent considerations, mainly connected to the need to discuss about the concepts of information «as», «about», or «for» reality, together with the definition of layers involved in this model, lead to a refinement of (1), and to define (2), (3) and (4) as follows:

$$\mathrm{IQA_I} = \frac{\sum_{i=1}^{n} (DTC_i + DST_i + CS_i)}{3n} \times 100 \quad (2)$$

$$\mathrm{IQA_{II}} = \frac{\sum_{i=1}^{n} (CM_i + SR_i)}{2n} \times 100 \quad (3)$$

$$\mathrm{IQA_{III}} = \frac{\sum_{i=1}^{n} (PC_i + TDA_i + OT_i + OS_i)}{4n} \times 100 \quad (4)$$

where:

- $\mathrm{IQA_I}$= information *as* reality
- $\mathrm{IQA_{II}}$ = information *about* reality
- $\mathrm{IQA_{III}}$ = information *for* reality

[23] We cannot forget the noise coming with the data flow, which must be carefully identified and removed. Of course, such a process has to be performed very cautiously since it may cause the definitive loss of precious data.

[24] Costantini/De Stefani/Galvan, The «Quality of Information» Challenges in IoT Forensics: An Introduction, cit.

Categories in Quality of Information	Philosophy of information	Requirements
Intrinsic	Information *as* reality (relevance)	DTC
Contextual		DST
		CS
Representational	Information *about* reality (uncertainty)	CM
		SR
Accessibility	Information *for* reality (accountability)	PC
		TDA
		OT
		OS

Table 2: Synopsis of IQ requirements and information categories

4. Forensic analysis of electronic evidences using IQA formulas

After having considered the topic of this paper from a theoretical point of view and defining the set of formulas devoted to quantify its various components, in this section we aim to test these findings by simulating an investigative scenario. In our case-study, we assume that a set of IoT digital devices are seized on a crime scene. Specifically, we stipulate that are sent to a Digital Forensics expert to be analized the following devices: 1) a smartphone; 2) the SIMCard inside of 1; 3) a drone; 4) a smartwatch; 5) a laptop pc; 6) a smart TV. Since information inside each device is organized and stored in different ways, depending on the policies of the respective brand, it is difficult to compare IQ among devices and evaluate the overall IQ. For this reason, we adopt the above explained theoretical and mathematical model, according to which is required, for each device, taking under consideration all the term that compose (1). This could be a very difficult challenge, for a couple of reasons: a) the device manufacturers may not (or not yet) have made public the requested technical information, and b) these data could be either not available or not as detailed as necessary. The level of these evaluations should be similar to what exposed in (CLARKet al. 2017)[25], (BOZTAS et al. 2015)[26] and (ODOM et al. 2019)[27], where the file system, the shape and the format of the log files and other useful forensic clues are exposed in case of a drone, a smart TV and a smartwatch. After this kind of deep analysis, we could fill a table as Table 3 below, implement (1), (2), (3) and (4), and generate a set of charts that allows to better insight the IQ of the examined evidences. An example of the outcome of an evaluation table in case of the six devices of our case study. The numbers inserted in this example were calculated after an evaluation made by the authors. For the test we considered the following devices:

1. Smartphone Huawei model ALE-L21 (P8 Light), with Android 6.0, 2 Gb RAM, CPU Octa-core 1.2 GHz, kernek version 3.10.86-g33ff982;
2. Nano SIMCard 4G Telecom Italia year 2017;
3. As discussed in (CLARKet al. 2017);
4. As discussed in (BOZTAS et al. 2015);

[25] Clark/Meffert/Baggili/Breitinger, DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III, Digital Investigation, volume 22, 2017, p. S3–S14.

[26] Boztas/Riethoven/Roeloffs, Smart TV forensics: Digital Traces on Televisions, Ibid., volume 12, 2015, p. S72–S80.

[27] Odom/Lindmar/Hirt/Brunty, Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices, Journal of Forensic Sciences, 2019.

5. IBM Thinkpad Edge E30, o.s. Windows 10, 8 Gb RAM, Intel i5 processor;
6. As discussed in (ODOM et al. 2019);

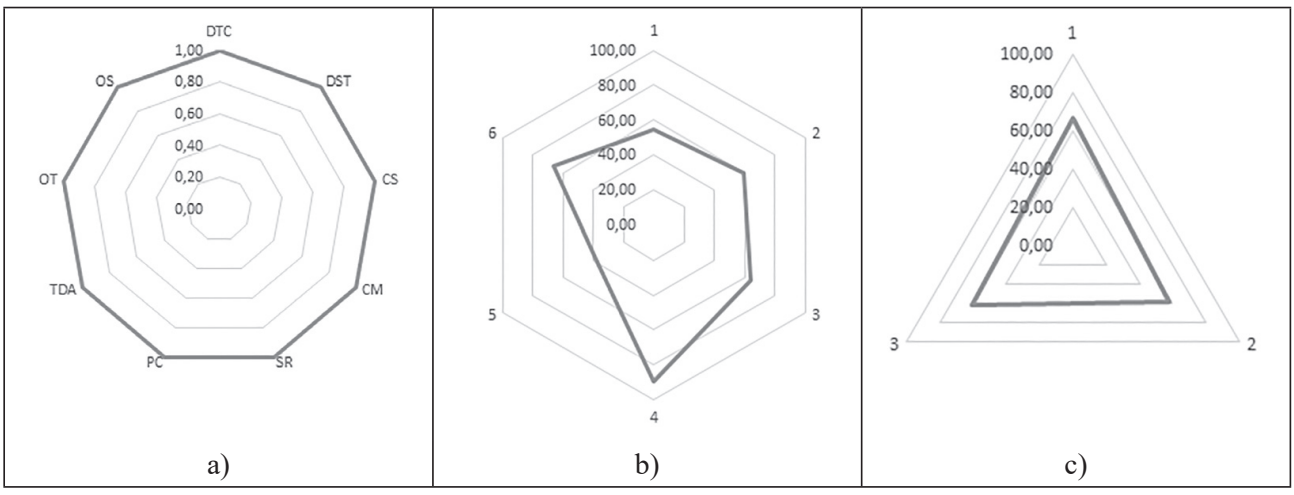
device 1 smartphone		**device 2 SIMCard**		**device 3 drone**		**device 4 smartTV**		**device 5 pc laptop**		**device 6 smartwatch**	
DTC	*0,56*	DTC	*0,93*	DTC	*0,97*	DTC	*0,91*	DTC	*0,39*	DTC	*0,89*
DST	*0,62*	DST	*0,12*	DST	*0,48*	DST	*0,16*	DST	*0,30*	DST	*0,82*
CS	*0,47*	CS	*1,00*	CS	*0,69*	CS	*0,91*	CS	*0,48*	CS	*0,44*
CM	*0,34*	CM	*0,17*	CM	*0,76*	CM	*0,80*	CM	*0,58*	CM	*0,85*
SR	*0,48*	SR	*0,76*	SR	*0,50*	SR	*0,98*	SR	*0,56*	SR	*0,18*
PC	*0,77*	PC	*0,82*	PC	*0,77*	PC	*0,80*	PC	*0,00*	PC	*0,98*
TDA	*0,55*	TDA	*0,60*	TDA	*0,21*	TDA	*0,99*	TDA	*0,26*	TDA	*0,65*
OT	*0,84*	OT	*0,07*	OT	*0,89*	OT	*0,80*	OT	*0,07*	OT	*0,89*
OS	*0,26*	OS	*0,88*	OS	*0,45*	OS	*0,95*	OS	*0,79*	OS	*0,31*

Table 3: terms of (1), (2), (3) and (4) evaluated by the authors for devices 1 – 6

By applying (1), (2), (3) and (4) to all devices, with the data exposed in Tab.3 as input, we obtain the following results, revealing that the IQA of the set of all seizured devices is about 62%, device nr.4 is the one achieving the best result in terms of Information Quality, whereas device nr.5 bears the worst performance:

$IQA_{I} = 61,96\ \%$	$IQA_{III} = 54,74\ \%$	$IQA_{device2} = 59,49\ \%$	$IQA_{device4} = 89,79\ \%$	$IQA_{device6} = 66,68\ \%$
$IQA_{II} = 56,30\ \%$	$IQA_{device1} = 54,37\ \%$	$IQA_{device3} = 63,73\ \%$	$IQA_{device5} = 38,19\ \%$	$IQA_{tot} = 62,04\ \%$

The «Quality» of information can be shown also by a set of *radar* chart, which offers a more immediate representation. In Figure 1 a set of evaluations is showed, considering both the total of the acquired staff and the single device. Subfigure a) represents a model of the best result that can be achieved: all the elements that compose the evaluation are at the maximum level, so the polygon is completely surrounded by the blue line. Subfigure b) shows at the same time the IQA of all the examined devices, and allows to appreciate immediately the best result of devices nr.4 already highlighted. Subfigure c) shows together the IQA calculate with (2), (3) and (4), whereas in every subfigures from d) to i) the performances of every single device are represented. Also from the comparison between these latter set of images, it is easily identified the peaking values of device nr.4 among the others.



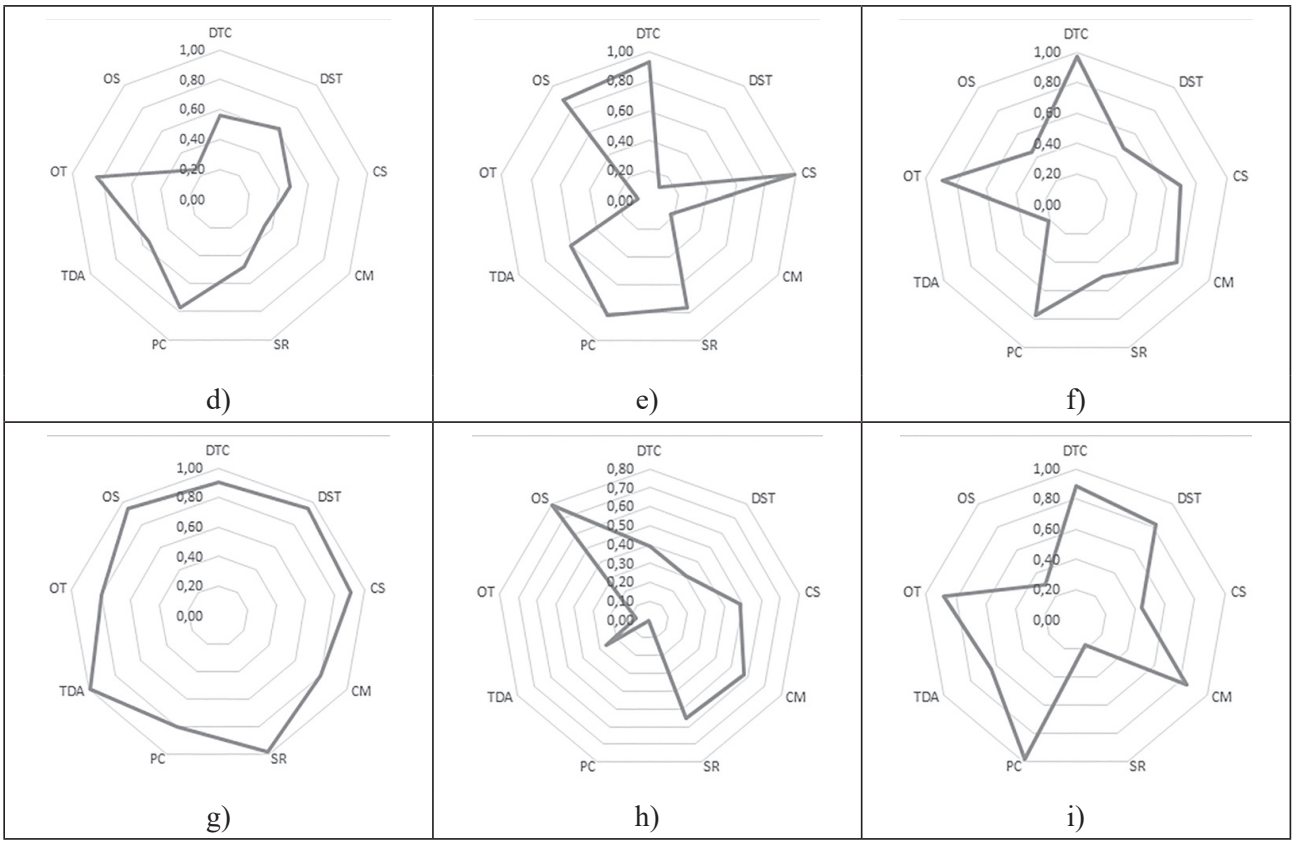


Figure 1: Graphic visualization of the outcomes[28]

5. Evaluation of results

In this contribution we present an improved approach which was introduced in a previous paper (Costantini et al., 2019). Our model is aimed to join together and evaluate the forensic features of a set of heterogeneous digital devices, so addressing the main challenge of IoT forensics within a sound theoretical framework such as the Philosophy of Information and with a rigorous methodology. Using the proposed formulas, it is possible to obtain an immediate overview of the quality of analysed evidences, allowing to assess its impact upon investigation and in court[29].

6. Conclusions and future perspectives

In a society where information is valued – or better, it is the utmost value as it is for us – and an open mindset is cherished – sanctified by the many declaration of fundamental rights and basic individual freedom – every knowledge generates a kind of expectation in those who does not own it. Experts are not compelled to share their know-how, yet they cannot abuse of it and they should explain the reasons of their actions. Our future

[28] The results of the IQA calculated by (1), (2), (3) and (4) become more intelligible with the help of this kind of charts, where the bigger the part of the inner figure is surrounded, the best is the achievement. In the above representation, a) was given as a model, and represents an example of the best result that a certain evaluation could achieve, since all the evaluated terms are at the higher level; b) is the IQA of all the devices showed together, that allows to highlight how, in the considered case work, the device 4 is the one with the best performance; c) shows at the same time the IQAI, II,III; d) – i) are the charts referred to every term of the formulas of every devices, respectively 1 – 6. Also in this comparison confirms that devices nr.4 obtains the best result.

[29] In the proposed example, for reasons of space, we could not deepen in the explanation of the methods used to evaluated the single device to fill Table 3. One of the proposals for future work is indeed developing set of shared rules in order to clarify this phase of the process.

work in this field will be devoted to fine-tune the model, involving the community of Digital Forensics experts in the attempt to define in detail each term composing the formula and to promote it as a technical standard.

7. References

Book Symposium on Homo sapiens Technologicus: Philosophie de la Technologie Contemporaine, Philosophie de la Sagesse Contemporaine By Michel Puech Editions Le Pommier, 2008.

Batini, Carlo/Scannapieco, Monica, Data and Information Quality: Dimensions, Principles and Techniques, Springer Publishing Company, Incorporated, 2016.

Borgmann, Albert, Holding on to reality. The nature of information at the turn of the millennium, University of Chicago Press, Chicago, 1999.

Boztas, A./Riethoven, A. R. J./Roeloffs, M., Smart TV forensics: Digital traces on televisions, Digital Investigation, volume 12, 2015, p. S72–S80.

Christensen, Clayton M., The innovator's dilemma : the revolutionary book that will change the way you do business, 2011.

Christensen, Clayton M./Bower, Joseph L., Disruptive technologies: Catching the wave, The Journal of Product Innovation Management, volume 1, issue 13, 1996, p. 75–76.

Christensen, Clayton M./Raynor, Michael E./McDonald, Rory What is disruptive innovation?, Harvard Business Review, volume 93, issue 12, 2015, p. 44–53.

Clark, Devon R./Meffert, Christopher/Baggili, Ibrahim/Breitinger, Frank, DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III, Digital Investigation, volume 22, 2017, p. S3–S14.

Conti, Mauro/Dehghantanha, Ali/Franke, Katrin/Watson, Steve, Internet of Things security and forensics: Challenges and opportunities, Future Generation Computer Systems, volume 78, 2018, p. 544–546.

Costantini, Federico/De Stefani, Marco Alvise/Galvan, Fausto, The «Quality of Information» Challenges in IoT Forensics: An Introduction, Jusletter IT, issue 21 February 2019, 2019.

Dretske, Fred I., Knowledge & the flow of information, MIT Press, Cambridge, Mass., 1981.

Durante, Massimo, Ethics, Law and the Politics of Information. A Guide to the Philosophy of Luciano Floridi, Gordijn Bert, Roeser Sabine, The International Library of Ethics, Law and Technology, 18, Springer, Dordrecht, 2017.

Floridi, Luciano, The Ethics of Information, Oxford University Press, Oxford, 2013.

Floridi, Luciano, The Philosophy of Information, Oxford University Press, Oxford, 2013.

Floridi, Luciano, The 4th Revolution. How the infosphere is reshaping human reality, Oxford University Press, Oxford, 2014.

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

Floridi, Luciano/Cowls, Josh/Beltrametti, Monica/Chatila, Raja/Chazerand, Patrice/Dignum, Virginia/Luetge, Christoph/Madelin, Robert/Pagallo, Ugo/Rossi, Francesca/Schafer, Burkhard/Valcke, Peggy/Vayena, Effy, AI4People–An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines, volume 28, issue 4, 2018, p. 689–707.

Floridi, Luciano/Illari, Phyllis, The philosophy of Information quality, Synthese library, 358, Springer, Berlin-Heidelberg, 2014.

Harari, Yuval Noah, 21 Lessons for the 21st Century, Jonathan Cape, London, 2018.

Hegarty, Robert/Lamb, David J./Attwood, Andrew, Digital Evidence Challenges in the Internet of Things, Proceedings of the Tenth International Network Conference (INC) 2014 School of Computing & Mathematics Plymouth University, Plymouth, 2014, p. 163–172.

High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI. European Union, 2019.

High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendations for Trustworthy AI. European Union, 2019.

Hossain, M./Karim, Y./Hasan, R., FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger, 2018 IEEE International Congress on Internet of Things (ICIOT) IEEE, 2018, p. 33–40.

Karkouch, Aimad/Mousannif, Hajar/Al Moatassime, Hassan/Noel, Thomas, Data quality in internet of things: A state-of-the-art survey, Journal of Network and Computer Applications, volume 73, 2016, p. 57–81.

Küsters, Ralf/Truderung, Tomasz/Vogt, Andreas, Accountability: definition and relationship to verifiability. Proc. Of The Proceedings of the 17th ACM conference on Computer and communications security, p. 526–535 (2010).

Lundgren, Björn, Does semantic information need to be truthful?, Synthese, 2017.

Meffert, Christopher/Clark, Devon/Baggili, Ibrahim/Breitinger, Frank, Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition, Proceedings of the 12th International Conference on Availability, Reliability and Security ACM, Reggio Calabria, Italy, 2017, p. 1–11.

Odom, Nicole R./Lindmar, Jesse M./Hirt, John/Brunty, Josh, Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices, Journal of Forensic Sciences, 2019.

Pagallo, Ugo/Casanovas, Pompeu/Madelin, Robert, The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data, The Theory and Practice of Legislation, 2019, p. 1–25.

Palmer, Gary, A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS), New York, 2001.

Ronzhyn, Alexander/Wimmer, Maria A., Literature Review of Ethical Concerns in the Use of Disruptive Technologies in Government 3.0, ICDS 2019: The Thirteenth International Conference on Digital Society and eGovernments, 2019.

Weaver, Warren, The Mathematics of Communication, Scientific American, volume 181, issue 1, 1949, p. 11–15.

Wills, Gary B./Alenezi, Ahmed/Zulkipli, Nik/Huda, Nurul, IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things, Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security Scitepress, 2017, p. 315–324.

Yu, Dan/Hang, Chang Chieh, A Reflective Review of Disruptive Innovation Theory, International Journal of Management Reviews, volume 12, issue 4, 2010, p. 435–452.

Zareen, Muhammad Sharjeel/Waqar, Adeela/Aslam, Baber, Digital Forensics: Latest Challenges and Response, 2013 2nd National Conference on Information Assurance (NCIA) IEEE, Piscataway, NJ, 2013, p. 21–29.

Zawoad, S./Hasan, R., FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things, 2015 IEEE International Conference on Services Computing IEEE, 2015, p. 279–284.

Colloquium

Erich Schweighofer / Walter Hötzendorfer /
Franz Kummer / Ahti Saarenpää (Hrsg. / Eds.)

Verantwortungsbewusste Digitalisierung

Responsible Digitalization

Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020

Proceedings of the 23rd International Legal Infomatics Symposium IRIS 2020

EDITIONS WEBLAW

Sämtliche in diesem Buch verwendeten personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen. Zwecks besserer Lesbarkeit wurde zum Teil auf eine unmittelbare geschlechtsneutrale Schreibweise verzichtet.

Trotz sorgfältigster Bearbeitung erfolgen alle Angaben ohne Gewähr. Eine Haftung des Verlags, der Herausgeber und der Autoren ist ausgeschlossen.

O Codex
I Commentatio
II Colloquium
III Dissertatio
IV Doctrina
V Liber amicorum
VI Magister
VII Monographia
VIII Thesis
IX Scriptum
X Anthologia

Editions Weblaw

Bestellung und Vertrieb Schweiz: Weblaw AG, Bern
Bestellung und Vertrieb international: Nova MD GmbH, Vachendorf
ISBN 978-3-96698-589-5

INHALTSVERZEICHNIS / TABLE OF CONTENTS

Das 23. Internationale Rechtsinformatik Symposion befasst sich mit Verantwortungsbewusster Digitalisierung. Die Respektierung rechtlicher und ethischer Prinzipien in der Wissens- und Netzwerkgesellschaft soll sicherstellen, dass Digitalisierung einen Mehrwert für alle bringt und die Menschenrechte beachtet werden. Digitale Ämter, E-Commerce, datengetriebene Industriefertigung, KI und Robotik, Internet of Things, Cloud Computing und Smartphones sind die Merkmale dieser Entwicklung. Die ethische und soziale Komponente dieses tiefgreifenden Wandels tritt immer mehr ins Zentrum der Diskussion.

Schwerpunkte:

- Generalthema: Verantwortungsbewusste Digitalisierung
- Autonomes Fahren
- Text- und Vertragsanalyse
- Rechtsinformation / Suchtechnologien
- Robolaw
- Theorie der Rechtsinformatik
- E-Government / E-Justiz / E-Democracy
- LegalTech
- Rechtstheorie
- Rechtsvisualisierung / Legal Design
- Sicherheit & Recht
- Datenschutz
- IP-Recht
- E-Commerce
- E-Procurement

Der Band umfasst neben neuen wissenschaftlichen Erkenntnissen auch Beiträge zu praktischen Problemstellungen und Anwendungen der Rechtsinformatik. In Zusammenarbeit mit dem Verlag Editions Weblaw werden alle gedruckten Tagungsbände (nunmehr ab 2000) sowie weitere exklusiv digital publizierte Beiträge in der Zeitschrift Jusletter IT unter www.jusletter-it.eu zugänglich gemacht.

ISBN: 978-3-96698-589-5