TACKLING DISINFORMATION IN THE EU: THE CASE OF "TRUTHSTER"

Federico Costantini / Francesco Crisci / Silvia Venier / Stefano Bistarelli / Ivan Mercanti

Federico Costantini, University of Udine, Department of Law, Via Treppo 18, 33100 Udine (IT), federico.costantini@uniud.it

Francesco Crisci, University of Udine, Department of Economics, Via Tomadini 30/A, 33100 Udine (IT), francesco.crisci@uniud.it

Silvia Venier, Institute of Law, Politics, Development (DIRPOLIS), Scuola Superiore Sant'Anna, silvia.venier@santannapisa.it

Stefano Bistarelli, Department of Computer Science, University of Perugia, stefano.bistarelli@unipg.it

Ivan Mercanti, Department of Computer Science, University of Perugia, ivan.mercanti@unipg.it

Keywords: ***Blockchain, TruBlo, Fake news, Trust, Freedom of Expression, Journalism***

Abstract: *Tackling disinformation is crucial for the development of the Information Society. To do so it is necessary to empower journalists in the production of trustworthy information, and to nurture an economic ecosystem centred on a secure circulation of contents. In this contribution we present an interdisciplinary approach that aims at (1) finding a balance between freedom of expression and other fundamental rights (i.e., privacy and data protection), (2) developing business models driven by the production of genuine content, (3) exploiting the potentials of distributed ledger systems to provide media certification.*

1. Introduction[1]

1.1. An overview: from "truth" and "authority" to "trustworthiness" and "governance"

Truth is a human basic need from a threefold perspective: (1) individually, as a matter of personal spiritual quest, (2) socially, as a base for personal and economic trusted relations, and (3) politically, as an inevitable requirement for consent in a fair exercise of public power. Conversely, disinformation is as old as human *consortia*. In this sense, as regards interpersonal relations, it might be recalled that in ancient Greek culture – the cradle of Western civilization – popular rumour (*Pheme*) was already distinguished from slander (*Sychophantia*) and malice (*Diabolé*, which was embodied by goddess). As for the institutional aspect, the exploitation of misleading information has always been valued as an asset both in critical times – from the Chinese classic "Art. of War" we can quote the imperishable statement «*all warfare is based on deception*»[2] – and as a privileged tool for the ordinary exercise of power by the Sovereign.[3]

As we know, with Information Society,[4] transmission of messages and broadcasting of news achieved unprecedent speed and magnitude[5]. The uptake of mass-media (press, radio, television) caused the creation

[1] This contribution is the result of joint research of the co-authors. Individual contributions can be attributed as follows: Federico Costantini, par. 1 and 5, Silvia Venier, par. 2, Francesco Crisci, par. 3, Stefano Bistarelli and Ivan Mercanti, par. 4.

[2] Tzu, The art of war, VI-V b.C., Chapter One.

[3] Machiavelli, De Principatibus, 1514.

[4] Beniger, The Control Revolution: Technological and Economic Origins of the Information Society, Harvard University Press, Cambridge, Mass., 1986.

[5] Gleick, The Information: a History, a Theory, a Flood, Pantheon Books, New York, 2011.

of new enterprises (mass-media companies), new marketplaces (advertising) and new professional figures (journalists), while allowing an unparalleled concentration in the control of public opinion. As well as worldwide dictators learnt to master the art of media censorship and manipulation,[6] democratic regimes cherished freedom of expression as a mean to protect trust in social relations, fair competition among enterprises and fundamental rights of citizens. On the latter aspect, it is noteworthy that a continuous effort is being pursued by jurisprudence and scholars to update legal concepts and to balance appropriately freedom of expression and others fundamental rights (reputation, privacy, authorship and so on).[7]

The advent of Internet disrupted the paradigm which lasted since the end of Eighteenth century. In this sense, the decision by the U.S.A. Supreme Court in the case "ACLU / RENO" – in which Internet has been qualified «*a wholly new medium of worldwide human communication*»[8] – represents the symbolical act of foundation of the "cyberlaw",[9] the law or the Internet.[10] In fact, being available an indefinite set of heterogeneous resources (e.g. data, services, applications) flowing continuously throughout the world and instantaneously accessible, neither a "centralized" nor a "distributed" approach are feasible for regulating the newly discovered digital continent. As for the first, the obvious main risk is censorship, which can be perpetrated by private (services providers) as well as public actors (governmental agencies or bodies). Concerning the second, the threat is represented by a global Babel which leads inevitably to echo chambering, social instability, and institutional uncertainty. Conversely, a "decentralized" approach seems suitable, despite its difficult implementation,[11] due to its flexibility and resilience. It is not a coincidence that the same approach was chosen by the Internet pioneers for the network architecture which became today's Internet.[12]

Currently, after almost thirty years from the decision in the case ACLU / RENO, and a further wave of innovation in ICTs (e.g. social media), we can argue that not only the concept of truth has to be revisited according to new epistemical perspectives, but also that the legal provisions alone are inadequate to enforce, or even to safeguard it. On the one hand, the concept of "trustworthiness" seems to be more theoretically grounded,[13] flexible[14] and future-proof[15] than that of "truth". On the other, concerns for trustworthiness in communication are increased by the exploitation of the potentials of new technologies (e.g. artificial intelligence and "deep fakes").[16] In tackling such issues, legislators at every level have started adopting a softer approach to regulation, introducing complex governance systems which include three basic components: (1) traditional legal provisions, which offer a uniform framework of general and abstract rules;[17] (2) business models allowing economic sustainability (costs of maintenance and transactions); (3) technological infrastructure, combining the general rules of law with the design of an ecosystem meant to virtualize resources and automate processes.[18]

---

6 Arendt, The Origins of Totalitarianism, Harcourt, New York, 1951.

7 Warren/Brandeis, The Right to Privacy, Harvard Law Review, volume 4, issue 5, 1890, S. 193–220.

8 Supreme Court of the United States No. 96–511, 19 March 1997 -26 June 1997.

9 Lessig, Code and Other Laws of Cyberspace, Basic Books, New York, 1999.

10 Kettemann, The Normative Order of the Internet. A Theory of Rule and Regulation Online, Oxford University Press, London, 2020.

11 Buterin, The Meaning of Decentralization. Medium, 2017.

12 Baran, On Distributed Communications Networks, RAND Corporation papers, P-2626, RAND, Santa Monica (California), 1962.

13 Gettier, Is Justified True Belief Knowledge?, Analysis, volume 23, issue 6, 1963, S. 121–123.

14 Luhmann, Vertrauen: ein Mechanismus der Reduktion sozialer Komplexitaet, Soziologische Gegenwartsfragen, N. F., 28, F. Enke, Stuttgart, 1968.

15 Funtowicz/Ravetz, Uncertainty and Quality in Science for Policy, Theory and decision library. Series A. Philosophy and methodology of the social sciences, 15, Kluwer Academic Publishers, Dordrecht, 1990.

16 Coeckelbergh, Democracy, Epistemic Agency, and AI: Political Epistemology in Times of Artificial Intelligence, AI Ethics, 2022, S. 1–10.

17 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, volume 7, issue 1, 2019, S. 1–25.

18 Craglia/Scholten/Micheli/Hradec/Calzada/Luitjens/Boter/Ponti, Digitranscope. The governance of digitally-transformed society, Luxembourg, Publication Office of the EU, 2021, DOI: 10.2760/503546 (online), Theodorou/Dignum, Towards ethical and socio-legal governance in AI, Nature Machine Intelligence, volume 2, issue 1, 2020, S. 10–12.

From a theoretical perspective, today it seems that such model of governance – with the combination of the abovementioned three components – is the most suitable method to regulate a decentralized set of interdependent human communities which rely on a likewise decentralized worldwide network to survive and flourish as peacefully as possible. This approach is adopted even at the EU level, as confirmed by many provisions recently adopted (e.g. Digital Markets Act[19] and Digital Service Act[20]), or soon to be enacted (e.g. "AI Act"[21] and "Cyber Resilience Act"[22]).

1.2. Tacking online disinformation in the EU: a holistic approach

The fact that our democratic societies highly depend on the ability of producing, sharing and consuming trustworthy information from a wide variety of sources is noticeably acknowledged by the European Commission, which – in the Communication on *Tackling online disinformation: a European Approach* – has defined disinformation as «*verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security*».[23] While on the one hand democracy in Europe rests on the existence of free and independent media, on the other ICTs are profoundly changing the way traditional and new media produce and distribute information and the ways in which users are engaged in the fruition of information. Not only governments and digital platforms, but each media creator, in other terms, is put on the forefront of the battle against disinformation, and every user can be held hostage by propaganda.

In order to address this issue, EU institutions released a *Code of Practice on Disinformation* in 2018,[24] which was revisited in 2022 with the *EU Strengthened Code of Practice on Disinformation*.[25] This initiative aims at encouraging stakeholders to adopt a set of measures to empower content creators and users by ensuring the safe design of the architecture of their systems, and by providing them «*with tools to assess the provenance and edit history or authenticity or accuracy of digital content*». We can argue that this document confirms that an approach resulting from the combination of legal provisions, economic balances and technological tools is valued as a viable strategy even in this specific field. However, designing an abstract model, despite the positive reception and even a wide adoption by stakeholders, is not sufficient to eradicate disinformation, due to the different causes, the many modes, the heterogeneous actors, and the impact of such phenomenon. For such reason, the EU is committed to foster the development of new methods and tools to contain the spreading of disinformation, financing research and innovation projects.[26]

[19] Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022, S. 1–66, ELI: http://data.europa.eu/eli/reg/2022/1925/oj.

[20] Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, S. 1–102, ELI: http://data.europa.eu/eli/reg/2022/2065/oj

[21] Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM/2021/206 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

[22] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454.

[23] COM(2018) 236 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

[24] https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

[25] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[26] Joint Communication, Action Plan against Disinformation, JOIN/2018/36 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52018JC0036 .

1.3. Outline of the contribution: presenting project "TRUTHSTER"

In this contribution we present the background research of project "TRUTHSTER" which, in our view, can be considered not only as an example of the actions put in place by the EU aimed at tackling disinformation, but also paradigmatic of the approach adopted by the EU institutions.[27] Indeed, as we will explain below, we envision an ecosystem composed by three pillars: (1) a set of legal rules – including both legal provisions and private agreements – (2) a sustainable business model – based on "open innovation" paradigm – and (3) a digital platform – based on distributed ledger technologies – which is meant to avoid *by design* both centralized monopoly over media production and lack of control on its circulation. Furthermore, our leading concept is that trustworthiness in the information can be better pursued empowering individual media creators in their effort to build trust towards their own professionality. Hence, the practical outcome of TRUTHSTER is a tool – a mobile application – which is meant to integrate a "proof of validity" on digital media generated with journalist's device, focusing on those whose creation process requires an interaction with another human actor (mainly, video interviews, audio recordings, and photos) before being shared. In the process, a customized disclosure notice is automatically sent to the interviewee, containing the terms and conditions regulating the media release, thus acknowledging her/his fundamental rights (primarily, privacy).

In the following paragraphs we address each pillar separately. In section 2 we draw an outline of the legal framework focusing on the specific concerns that media creators – primarily journalists, but also influencers, and digital entrepreneurs in general – need to address in balancing freedom of entrepreneurship and of expression with the rights to privacy and data protection. In section 3 we briefly describe the envisaged business model and in section 4 we provide an overview of the technologies deployed. At the end we offer a few final remarks.

2. The legal pillar: balancing rights and protecting their core

Fundamental rights represent the overall architecture that underpins information sharing in our democratic societies. In particular, the right of freedom of expression represents the cornerstone of the activity of journalists.[28] Indeed, according to the European Convention on Human Rights (ECHR), journalists as well as NGOs, bloggers and scholars represent "watchdogs" of the public opinion, thus benefiting of a special protection (Art. 10 ECHR). Consequently, public authorities aren't allowed to restrict freedom to investigate, report and comment on all matters of public interest.[29] In order to obtain such increased protection, journalists are expected to comply with the duties and responsibilities connected with their role. For instance, while the ECHR states that journalists are not required to verify official sources in reporting news released by them, professional responsibility of journalists entails that it is mandatory to validate information before releasing it publicly to a reasonable extent. In the case of an interview published in newspapers, however, some differences have been drawn between the transcription of the interviewee's statement and the journalist's own declarations.[30]

As observed above, freedom of expression requires to be balanced with other fundamental rights. Such balance becomes more difficult in the digital realm, since on the Internet not only, as stated by the ECtHR, risks are generally considered more consistent than those related with traditional press,[31] but also new kinds

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

[28] As recognised by the Universal Declaration of Human Rights (Art. 19), the European Convention on Human Rights (Art. 10) and the Charter of Fundamental Rights of the European Union (Art. 11).

[29] On the role of the press, see e.g. ECtHR in Affaire Campos Dâmaso C. Portugal, § 30; on academic researchers see Başkaya and Okçuoğlu v. Turkey [GC], §§ 61–67; on the role of bloggers and popular users of social media as watchdogs, see e.g. ECtHR *Magyar Helsinki Bizottság v. Hungary* [GC], § 168.

[30] See Case of Kącki v. Poland § 52.

[31] See ECtHR, Guide on data protection (2022), par. 369 et seq., available at https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0.

of threats emerge, thus requiring new remedies, as confirmed by the "right to be forgotten", which can be claimed only against online search engines and media web archives[32], not towards newspapers and traditional media in general. Furthermore, the fact that fundamental rights are embodied not only in International Treaties and in legislation, but also in secondary sources of law, creates interpretative nuances and exceptions, thus increasing uncertainty for professionals and *de facto* hindering their freedom. As we know, Regulation (EU) 679/2016 (henceforth "GDPR")[33] establishes specific rights for data subjects and obligations for data processors and controllers. Interestingly, pursuant to Art. 85 GDPR and recital 153, Member States are entitled to provide for derogations or exemptions – which must be notified to the EU Commission – to adapt the application of data protection in the field of media production. Pursuant this clause, in Italy, for example, the Data Protection Supervisor has enacted a "Professional Code" for journalists[34], according to which a reporter is required to disclose her or his qualification while collecting news in order to benefit of the exemption from Art.s 13 and 14 of the GDPR (duty to provide information to the data subjects). The perverse consequence of this measure, aimed at simplifying practical duties, is that the figure of journalists is weakened since, once released the media – and shared once for all the personal data collected – they are exposed to legal claims concerning media authorship, consent, personal image and so on, and deprived of any proof in their defence.

In general, when media directly involve persons of interest (e.g., an interviewed), their consent for using their personal data or their personal image (e.g., protected materials) represents a critical requirement. In fact, especially field reporters tend to avoid the practical inconveniency of collecting a documented expression of will (mostly, if it is expected to be on paper). In general, professional media creators currently lack an effective protection to ensure (1) the genuinity of information sources, (2) the integrity of the content produced and (3) the compliance with legal requirements (laws, bylaws, professional codes of practices) throughout the process of collecting and publishing media. On their part, those who are directly involved in the media content (e.g., interviews' respondents), are unable to control their own data once the news is spread, or unaware of their own rights, or incapable to exercise them, or often incapacitated to claim damage compensation.

The design concepts of the TRUTHSTER application are aimed at addressing such legal issues, and specifically: (1) the interview should not be released without the consent of the interviewee; (2) the consent of the interviewee should be easy to collect by the interviewer; (3) the certification of the media content and the expression of consent of the interviewee should be activated by the same simple gesture; (4) the certification of the media content should include any relevant data (embedded as metadata), and it should be performed by a decentralized platform to avoid censorship or manipulation; (5) the documentation of the interaction and of the certification should be available for both the interviewer and the interviewee.

3. The economic pillar: entrepreneurial innovation

The project proposes a formula for entrepreneurial innovation that seeks overcome the traditional distinctions of the innovation process, underpinning innovation on a dimension of cultural entrepreneurship (the evolution of the digital media creation culture).[35] The proposed business model feeds an alternative socio-cultural dimension to the dominant professional and work models in the traditional news media sector. Potentially, it

[32] See in particular the ground-breaking judgment of the Court of Justice of the EU (CJEU) in Google Spain (2014), Case 131/12 Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez v AEPD. See also ECtHR, Guide on data protection (2022), par. 280–282.

[33] Regulation (EU) 2016/679 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, in OJ L 119, 4.5.2016, S. 1–88, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[34] Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica" (G.U. del 4 gennaio 2019, n. 3), https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9067692

[35] Goyanes/Rodriguez-Castro/Campos-Freire, Value and Intelligence of Business Models in Journalism, Journalistic Metamorphosis: Media Transformation in the Digital Age, Springer, Cham, 2020, S. 171–184.

is possible to trigger or at least nurture processes of institutional and organisational change in the traditional formulas of work organisation (in the information chain and in the functioning of newsrooms) and in the management of the journalistic profession.

The characteristic aspects of the TRUTHSTER project's business solution are the concept of entrepreneurial innovation (new organisational forms and innovative business models designed in a coherent manner) and the use of platforms as „relational infrastructures" based on the „participatory culture" of data journalism as a social and cultural phenomenon, likewise it happens with the movement of digital markers (e.g. "Arduino"), which is at the same time (1) a digital prototyping board (a „digital artefact"), (2) an entrepreneurial model focused on entrepreneurial learning and entrepreneurial innovation practices, and (3) a collective platform for creatives and innovators focused on the community and culture of digital makers.

In short, the solution envisaged by the Truthster project in terms of business model and organizational design is economically sustainable only if the „participatory" dimension of the project and the „membership" mechanism simultaneously feed the three components of the ecosystem: (1) the continuous production of open source applications and tools (especially by professional developers and from the world of academic entrepreneurship); (2) the adoption of such tools to feed the cultural dimension of the data journalism movement; (3) the development of the platform as an online community of creatives and innovators around the convergence of technologies such as blockchain and artificial intelligence in news media.

4. The technological pillar: the need for a decentralized platform

The implications of blockchain technologies in the field of human rights have drawn attention by scholars. On the one side, blockchain promises to facilitate freedom of expression and balance it with the protection of the rights to privacy and data protection.[36] Yet, for its own decentralized and immutable structure, blockchain may also hamper accountability of data controllers and the exercise of right to access, modify and delete personal data. Some recommendations to governments, private actors in the digital sectors and stakeholders have been provided by EU national Data Supervisors[37] and by NGOs.[38]

The opportunity offered of blockchain to provide a decentralised system for the validation of content and a clear chain of custody can be relevant in the field of journalism, and several models have been proposed so far.[39] According to Harrison and Leopold, "[*b*]*y providing greater transparency into the lifecycle of content, blockchain could offer a mechanism to restore trust in our digital ecosystem*".[40] Indeed, blockchain can track and verify the origin of news and visual content, as demonstrated by the New York Times and IBM "News Provenance Project".[41] Some media corporations and news agencies have started to develop blockchain-based

[36] Zyskind/Nathan/Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops, 2015, S. 180–184. DOI: 10.1109/SPW.2015.27.

[37] Commission Nationale Informatique et libertés (CNIL), Blockchain. Solutions for a responsible use of the blockchain in the context of personal data (2018), https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf. For a discussion, see Daoui/Fleinert-Jensen/Lempérière, GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions, Stanford Journal of Blockchain Law & Policy, 2019. https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france .

[38] Art. 19, Blockchain and Freedom of Expression (2019), S. 37–38, available at https://www.Art.19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf

[39] Kim/Yoon, Journalism Model Based on Blockchain with Sharing Space, Symmetry, volume 11, issue 1, 2019. https://www.mdpi.com/386868, Jurado/Delgado/Ortigosa, Tracking News Stories Using Blockchain to Guarantee their Traceability and Information Analysis, International Journal of Interactive Multimedia and Artificial Intelligence, volume 6, issue 3, 2020, S. 39–46, Sintes-Olivella/Xicoy-Comas/Yeste-Piquer, Blockchain at the service of quality journalism: the Civil case, Profesional De La Informacion, volume 29, issue 5, 2020. https://doi.org/10.3145/epi.2020.sep.22, Teixeira/Amorim/Silva/Lopes/Filipe, A New Approach to Crowd Journalism Using a Blockchain-Based Infrastructure, Momm 2020: The 18th International Conference on Advances in Mobile Computing & Multimedia, 2020, S. 170–178.

[40] Harrison/Leopold, How Blockchain Can Help Combat Disinformation, Harward Business Review, 2021. https://hbr.org/2021/07/how-blockchain-can-help-combat-disinformation.

[41] https://www.newsprovenanceproject.com/.

solutions to address specific concerns such as copyright infringements (WordProof[42]), to certify press releases (ANSA check[43]), or even to certify online content for forensic purposes (LegalEye[44]).

We believe that blockchain technology promises to serve as one of these technical solutions, as it offers a mechanism to enhance trust in the information shared. It can ensure that providers of information are verified, and users' rights exercised, as it can and securely store the timestamps of a publication, certify the provenance of news stories, thus increasing the reputation of verified content producers. Furthermore, smart contracts offer a new, simplified, and automatized tool to boost the value-chain of trusted information, since they can regulate how it can be created, shared, and consumed (e.g., managing copyright validation and micropayments).

Our solution is based on three main components: (1) a mobile and web interface for the interviewer, (2) a cloud-ready backend server, and (3) a web app for the interviewed. The user experience will be the following: the interviewer logs through her/his mobile device into the TRUTHSTER application, which identifies her/him and the device itself, after a preliminary KYC procedure. The user is allowed to insert the personal data (e.g. name, surname, address, contact details) of the interviewee, and to configure the legal framework regulating the digital content before its generation (including privacy and media release options chosen by the interviewee). Once the media is recorded, the interviewee is requested to interact with the interviewer (e.g. sending an SMS to her/him or generating a QR code to scan).

Such interaction triggers four processes: (1) the calculation of the hash of the file (together with metadata included by the user, such as the identity of the interviewee, and recorded automatically, such as GPS position of the device), (2) the transmission of such data (in a human comprehensible format) to the interviewee for future reference (e.g. GDPR notice), (3) the upload of the file into a cloud server,[45] (4) the storage of hash and metadata in decentralized platform, which is provided by Alastria,[46] an open-source and permissioned blockchain platform.[47] The interface is enriched by other functionalities, such as a navigable history of the interviews stored in the DB, and other practical tools.

5. Conclusion

While the impact of blockchain has been not only a technological innovation, but undoubtedly also a social phenomenon, their practical benefits and disadvantages are still under discussion, with "pros" and "cons" which depend on the context of their application (which are very wide, from cryptocurrencies to supply-chain certification). In our project the use of such a platform offers the supreme advantage that it allows to align theoretical background (the need of a decentralized governance for supporting trustworthiness of media) with legal requirements (the challenge of protecting fundamental rights in the digital realm) and with sustainability concerns (the interest of the single media creator as a design requirement). In the next months we are planning to release a White Paper both to showcase the outcome of our research and to demonstrate the validity of our tenets.

6. Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 957228 (see https://www.trublo.eu/ for details).

42 https://wordproof.com .
43 https://www.ansa.it/sito/static/ansa_check.html.
44 https://www.legaleye.it.
45 MongoDB, https://www.mongodb.com.
46 https://alastria.io/.
47 The interviewer is notified of the completion of the process by a Node.js server.

7. Reference

Arendt, Hannah, The origins of Totalitarianism, Harcourt, New York, 1951.

Baran, Paul, On Distributed Communications Networks, RAND Corporation papers, P-2626, RAND, Santa Monica (California), 1962.

Beniger, James R., The Control Revolution: Technological and Economic Origins of the Information Society, Harvard University Press, Cambridge, Mass., 1986.

Buterin, Vitalik, The Meaning of Decentralization. Medium, 2017.

Coeckelbergh, Mark, Democracy, epistemic agency, and AI: political epistemology in times of artificial intelligence, AI Ethics, 2022, S. 1–10.

Craglia, Massimo/Scholten, Henk/Micheli, Marina/Hradec, Jiri/Calzada, Igor/Luitjens, Stevens/Boter, Jaap/Ponti, Marisa, Digitranscope. The governance of digitally-transformed society, Luxembourg, Publication Office of the EU, 2021, DOI: 10.2760/503546 (online)

Daoui, Sonia/Fleinert-Jensen, Thomas/Lempérière, Marc, GDPR, Blockchain and the French Data Protection Authority: Many Answers but Some Remaining Questions, Stanford Journal of Blockchain Law & Policy, 2019.

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

Funtowicz, Silvio O./ Ravetz, Jerome R., Uncertainty and quality in science for policy, Theory and decision library. Series A. Philosophy and methodology of the social sciences, 15, Kluwer Academic Publishers, Dordrecht, 1990.

Gettier, Edmund, Is Justified True Belief Knowledge?, Analysis, volume 23, issue 6, 1963, S. 121–123.

Gleick, James, The information : a history, a theory, a flood, Pantheon Books, New York, 2011.

Goyanes, M./Rodriguez-Castro, M./Campos-Freire, F., Value and Intelligence of Business Models in Journalism, Journalistic Metamorphosis: Media Transformation in the Digital Age, Springer, Cham, 2020, S. 171–184.

Harrison, Kathryn/ Leopold, Amelia, How Blockchain Can Help Combat Disinformation, Harward Business Review, 2021.

Jurado, F./Delgado, O./Ortigosa, A., Tracking News Stories Using Blockchain to Guarantee their Traceability and Information Analysis, International Journal of Interactive Multimedia and Artificial Intelligence, volume 6, issue 3, 2020, S. 39–46.

Kettemann, Matthias C., The Normative Order of the Internet. A Theory of Rule and Regulation Online, Oxford University Press, London, 2020.

Kim, B./Yoon, Y., Journalism Model Based on Blockchain with Sharing Space, Symmetry, volume 11, issue 1, 2019.

Lessig, Lawrence, Code and other Laws of Cyberspace, Basic Books, New York, 1999.

Luhmann, Niklas, Vertrauen: ein Mechanismus der Reduktion sozialer Komplexitaet, Soziologische Gegenwartsfragen, N. F., 28, F. Enke, Stuttgart, 1968.

Machiavelli, Niccolò, De Principatibus, 1514.

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, volume 7, issue 1, 2019, S. 1–25.

Sintes-Olivella, M./Xicoy-Comas, E./Yeste-Piquer, E., Blockchain at the service of quality journalism: the Civil case, Profesional De La Informacion, volume 29, issue 5, 2020.

Teixeira, L./Amorim, I./Silva, A. U./Lopes, J. C./Filipe, V., A New Approach to Crowd Journalism Using a Blockchain-Based Infrastructure, Momm 2020: The 18th International Conference on Advances in Mobile Computing & Multimedia, 2020, S. 170–178.

Theodorou, Andreas/Dignum, Virginia, Towards ethical and socio-legal governance in AI, Nature Machine Intelligence, volume 2, issue 1, 2020, S. 10–12.

Tzu, Sun, The art of war, VI-V b.C.

Warren, Samuel D./ Brandeis, Louis D., The Right to Privacy, Harvard Law Review, volume 4, issue 5, 1890, S. 193–220.

Zyskind, G./Nathan, O./Pentland, A., Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops, 2015, S. 180–184. DOI: 10.1109/SPW.2015.27.