Francesco Biondo / Gevisa La Rocca /
Viviana Trapani (eds.)

Information Disorder

Learning to Recognize Fake News

PETER LANG

Francesco Biondo / Gevisa La Rocca / Viviana Trapani (eds.)

Information Disorder

The Fake News project was developed as a social project to suggest an idea of a plural, open, and dialectical society. One product of social action is public opinion, which directly and indirectly influences policy decisions, including those concerning the control and prospects of social innovation, thus exerting pressure on any kind of democratic regime. Disinformation hinders the free process of public opinion building by using various means to negatively influence public opinion with the effect of widening the chasm between decision-making power and active citizenry, who in turn needs to be properly informed to usefully contribute to achieving publicly shared goals in a transparent manner.

The Editors
Francesco Biondo is an associate professor of Legal Philosophy at the Department of Law, University of Palermo.

Gevisa La Rocca is an associate professor of Sociology of Communication at the Kore University of Enna.

Viviana Trapani is an associate professor of Industrial Design at the University of Palermo and coordinator of the Master's Degree Course in *Design and culture of the territory*.

www.peterlang.com

Information Disorder

Francesco Biondo / Gevisa La Rocca /
Viviana Trapani (eds.)

Information Disorder

Learning to Recognize Fake News

PETER LANG

Bibliographic Information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.d-nb.de.

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress

This volume has been made possible by the co-funding of ERDF to the "FAKE NEWS" project, through Regione Siciliana (Italy) - Assessorato delle Attività Produttive - CUP G79J18000630007 under the call entitled: "Programma Operativo FESR 2014-2020 della Regione Siciliana, Avviso pubblico per l'attuazione dell'Azione 1.1.5 Sostegno all'avanzamento tecnologico delle imprese attraverso il finanziamento di linee pilota e azioni di validazione precoce dei prodotti e di dimostrazione su larga scala".

Partnership:

- IT HUB S.R.L Milan | *leader of project – ICT know how*
- University of Palermo | *partner*
  Dipartimento di Architettura | *coordination of social and scientific activities*
  Dipartimento di Giurisprudenza | *scientific support in law disciplines*

With collaboration of:

- University of Salerno | *research support*
  Dipartimento di Informatica | *scientific support in informatics*

Cover illustration: © Cinzia Ferrara

ISSN 2511-9753
ISBN 978-3-631-88556-7 (Print) · E-ISBN 978-3-631-88557-4 (E-PDF)
E-ISBN 978-3-631-88558-1 (EPUB) · DOI 10.3726/b19996

Peter Lang – Berlin · Bruxelles · Lausanne · New York · Oxford
This publication has been peer reviewed.

www.peterlang.com

Contents

Part III Justice and Misinformation

Part IV Information and Misinformation Design

Stefano Pietropaoli

Extra computationem nulla salus? Considerations on democracy, fake news and blockchain

Abstract The possibility for individuals to interact without geographical constraints was hailed at the beginning of the 1990s as the start of an unstoppable process of democratisation. However, the increased complexity of the digital society and the scarcity of IT skills are leading to the progressive inability of social actors to control and critically select their cognitive sources, to the point of paralysing their ability to analyse them. Among the main focal points is the spread of fake news, which, mainly as a result of phenomena such as disintermediation and tools such as algorithms, filter bubbles and echo chambers, are able to pollute information. However, the very technologies behind the problem can also provide solutions. An interesting proposal to try to curb the problem of the massive spread of fake news is the use of blockchain technology to certify the origin of news. However, it is one thing to claim that blockchain represents a technology that can offer advantages, it is quite another to go so far as to contend that the use of solutions that leverage blockchain are capable of solving the problem at its root.

Keywords: Bubble democracy, fake news, freedom of thought, digital swarm, blockchain

Democracy and the digital revolution

It is a matter of fact that the spread of mass media – and television in particular – has played a decisive role in the transformation of twentieth-century democracy (Zolo, 1992). What we call the "digital revolution" has become an integral part of this process, having consequences of extraordinary significance (Lévy, 1990). Many have seen in it an event capable of breathing new life into democracy. Yet there seem to be many reasons that call for caution and invite to consider more carefully the actual democratic potential of the digital revolution (Gilder, 2018).

In a debate often dominated by the polarization between "doomsters and initiates" – neo-luddites and techno-fanatics, those nostalgic for paper and pixel addicts – one of the most frequent arguments is that of the unstoppable emancipatory force inherent in digital technologies (Formenti, 2008). The web, in this perspective, is seen both as a very powerful tool for implementing knowledge in general (and political competence in particular) (Mathew, 2016) and as a means

capable of offering new forms of democratic participation, from electronic voting to the instant referendum.

In this regard, it is unquestionable that new technologies can provide tools with a high democratisation capacity (Rodotà, 1997 [2004], Rodotà, 2013; Fioriglio, 2017; Gometz, 2017). However, these tools must be employed in the political, economic and legal context in which this drive for democratisation is capable of achieving coherent, non-distorting effects. One excellent example is electronic voting (Mancarella, 2013). Just to refer to the Italian legal system, the use of a digital voting system – which allows one to express one's preference via a terminal (instead of pen and paper), and ensures therefore error-free electronic counting, as well as the immediate communication of the results – is clearly compatible with the principles established by Article 48 of the Italian Constitution (personality, equality, freedom and secrecy), only if used in a polling station operated by human beings. A vote expressed with a click from the computer in one's own home, even with the use of sophisticated authentication systems, would obviously have nothing "democratic" about it.

This latter consideration, I believe, calls for a more general reflection on digital technologies and on how the web has undergone an evolution that has distanced it increasingly from the media that preceded it. At its inception, the "web" was a sophisticated communication tool that could be managed by few who, thanks to their computer skills, were able to communicate via machines. The incredible increase in computing power of processors has rapidly made it possible to develop increasingly user-friendly operating systems, thus making it possible for pre-school children (as well as primates, as the odd story of the macaque Naruto teaches) to create digital content.

The web has thus become "demedialised": anyone who owns a device and has access to the web is able to produce and disseminate information.

The possibility of interaction between individuals without geographical constraints – now offered by technologies accessible to users without computer skills – was hailed at the beginning of the 1990s as the start of an unstoppable process of democratisation (Castells, 1996). But how naive that view was has been demonstrated by the recent history of the web: from the original idea of a "distributed" network (Baran, 1964) it has become "decentralised" but polycentric (Dorogovtsev & Mendes, 2013). In other words, the evolution of the web has led to new forms of concentration of power, resulting increasingly dominated by private oligopolies.

Web users, from mere consumers, have become producers of information. Here is the core issue: the exponential increase in data and information cannot in any way match the increase in the users' ability to select information, thus

developing their knowledge (and even less the "tacit knowledge" Polanyi talked about), their critical sense, and their political competence. In the days of big data, the variety and complexity of information is so great that it discourages us from embarking on critical paths and invites us to become completely self-referential.

Algorithms are now an integral part of all decision-making processes, from defining the probable recidivism rate of a convicted felon to buying the next book to read, from buying and selling shares on the stock exchange to choosing the partner most akin to our needs (Lettieri, 2020). This scenario is dominated by an absolute sense of impotence of the majority of citizens, by the rhetoric of the algorithmic black box, and by the hypostatisation of Technics. But behind every choice in the technological field there are nonetheless human beings, whose actions escape democratic control. As Bernard Stiegler noted, after all, Marx and Engels had already argued that "man is a technical being. As such, he is lured to his technics. There is a dominant class that seizes this luring power of technics to dominate those who are lured by it. And that is that way it is" (Rouvroy & Stiegler, 2015).

The increased complexity of the digital society and the scarcity of IT skills are leading to the progressive inability of social actors to control and critically select their cognitive sources, to the point of paralysing their ability to analyse them. The latter would consist precisely in the possibility of excluding what is not essential: an operation that today is suffocated by the flow of information that overwhelms us (Stiegler, 2012).

Increased knowability is not equivalent to increased knowledge. More information does not mean better decisions. Conversely, too much information creates an electronic cloud that blurs vision. As Han has argued: information now de-forms, and communication is now cumulation.

From citizen to user

Digital technologies hold enormous democratic potential. But they can also turn out to be a very effective tool for strengthening ideologies that are anything but democratic. In other words, I consider unfounded both the visions of a necessarily salvific technology and the arguments of those who demonise the digital era as the insidious and incurable fruit of the capitalistic logic.

What I would like to stress is that these technologies can and should be governed politically. There is no destiny in the drift we are witnessing: but we need awareness, knowledge, open-mindedness and imagination to get out of the phase of denial of politics that we are experiencing (Preterossi, 2011).

It was not "Technics" – a hypostatised fetish that would like to justify impossible nostalgia – but the neoliberal and depoliticising post-ideology that made the oligopolies that control the web possible. We are living what we can call, without any rhetoric, a "revolution": but even if it is a revolution in our way of living, thinking and being, it is not a democratic revolution. In the absolute majority of cases, if we do a search on the internet, we use the Google search engine; if we buy goods online, we use the services offered by Amazon; if we want to interact with other individuals at a distance, we use Facebook/Instagram/WhatsApp (the trinity of the empire founded by Mark Zuckerberg); if we use a mobile phone, we exploit the potential of the Android (Google again) or Apple operating systems. "Distribution" has become "concentration," but I insist: this outcome was the result of a series of deliberate and entirely "political" choices (Foroohar, 2019; Taplin, 2017; Wu, 2013).

The ability of capitalism to merge with the control of technological development and its applications is revealed in its most recent expressions: the "capitalism of platforms," or – to use Shoshana Zuboff's expression – "surveillance capitalism" (Zuboff, 2019). Regardless of the different perspectives to address the problem, the criticisms levelled against this outcome share an analysis of the crisis of democratic institutions and the deterioration of citizenship. The parable in which modern citizenship was inscribed, in which individuals moved within political communities to which they felt responsible, has come to an end. Citizens have become consumers, mere passive users of variously offered services, who express their decisions in the same way they express their purchasing preferences. And in the same way, therefore, their electoral inclinations can be scrutinised, through data mining processes.

If the life of users is by now increasingly projected into the internet, also the individual political and legal dimension suffers the same fate. We are thus witnessing an integral datafication of the personality, with remarkable consequences in terms of the effective protection of freedoms and the concrete exercise of fundamental rights. Reduced to holograms floating on screens, users incessantly exchange data and information about what they do, think, and experience. Existence is totally "protocolled" and made controllable this way, continuously monitored by a digital panoptic: this is not a futuristic dystopia, but a factual reality, linked to the unwritten law by which the control of users is the more pervasive the easier it is to use the devices they use.

As Damiano Palano has effectively argued (Palano, 2020), the critique of party rule and the push towards the personalisation of politics – elements that already characterised the "democracy of the public" – have combined in a new dynamic of the relationship between citizens and information and communication

technologies: while voters had previously been radio listeners and television viewers, but still an "audience", an audience watching a common show, now they are turning into self-referential, fragmented "bubbles", unable to express a political unity.

Public space is thus reduced to a "social network". Democratic discourse is no longer possible because the user is structurally aphasic. There is no discourse but only opinions: a continuous regurgitation of "likes" that bubble up in a fragmented and polarised cyberspace, where one's own convictions are made to resonate without being open to any dialogue and, often, with a hybrid violence – suspended between virtual and real – but no less terrible.

Fake news between disinformation and misinformation

In the scenario I have tried to outline in the pages above, the new structure of information opens up new issues that call into question fundamental rights such as freedom of expression.

The current structure of the internet allows anyone with a device and access to the web to disseminate information and news. While, on the one hand, this can represent an opportunity for the development of public discourse and the guarantee of plurality of information, on the other hand, it is necessary to reckon with the possible negative consequences of this dynamic.

The way information is produced, disseminated and used has changed at a dizzying pace since the advent of the web. A system in which the individual plays an active and completely new role has now been established: just having a PC, a smartphone or a tablet transforms users from simple users of the news to producers. The web has broken the monopoly of mainstream media. Today everyone can create information, comment on information already on the web or on social networks, share content entered by others and propose new content. This fracture has contributed to the start of the so-called disintermediation process, i.e., the elimination of intermediation structures – "filters" or "intermediate bodies" – between two or more users in the process of communication and service provision.

The speed of access, the possibility to connect anywhere thanks to mobile devices, the almost zero cost, and the immediacy make the internet – and social media – the individual's favourite place to get information. The primacy previously held by traditional media is thus undermined and we are heading towards the twilight of the media established in the twentieth century.

This phenomenon of disintermediation overrides the classic structure of professional associations, including that of journalists. In doing so, it also eliminates

the controls and standards required to perform certain roles in society, creating a particularly significant vulnerability to the status of the information professional. And in this perspective, we cannot fail to perceive as alarming the increasing diffusion of phenomena such as filter bubbles and echo chambers, which represent a complex device of information pollution.

The "filter bubble" is the result of algorithms that analyse the behaviour of individual users online, show them the news, content and posts most akin to their opinions and in line with their ideas. The consequence is that users are offered content that is always close to and consistent with their own opinions and are seldom offered news and information that embraces other lines of thought or alternative beliefs. Often users are unaware of this mechanism also because of the illusion of total freedom that the web conveys to us and that lets users believe that they are completely independent in their choices and in the way they inform themselves on the internet.

The phenomenon of filter bubbles is accompanied by that of echo chambers. Whoever is inside an echo chamber will hear repeated endlessly what is being said by others who are with him or her, in an increasingly confused and distorted version-but nevertheless destined to remain the only source of information for the reference group. People who get their information from a social network and have only people who embrace the same ideas as they do in their circle of friends find themselves at the centre of an echo chamber where every thought will be returned and amplified without anyone questioning it. This triggers the further dynamics of the "confirmation bias", which pushes individuals to select in a biased way the ideas and information that surround them, instinctively going to seek and prefer those in line with their ideals and personal beliefs. This mechanism is crucial for the effectiveness of fake news: if the false or manipulated news that is proposed to us is oriented in the same direction of the ideals of those subject at the centre of the echo chamber, they will surrender any critical defence and will tend to accept that news as true without checking it in any way.

The current prominence of social media means, therefore, that information is increasingly produced by the flow of content generated by users, who are inclined to divide into groups that are similar from an ideological point of view. This is a "friendship paradox" that causes the creation of illusory majorities that use social media as a sounding board for invented, misleading, and distorted information. It is important to note that fake news can be either false or misleading and can be spread either with the deliberate intention to deceive or out of actual ignorance of the truth, i.e., even without being aware of the incorrectness of the news spread. Fake news can in fact be a source of disinformation but also of misinformation: in the first case, a piece of news is intentionally created and

spread with the awareness that it is false; while in the second case, a content, an article or a post is shared ignoring its falsity. In other words, fake news not only alters a subject's or social group's perception of reality but causes them to share it in a spontaneous and participatory manner.

It is also important to highlight that not everything that is called fake news is completely false news: on the contrary, the most dangerous and effective fake news is precisely that mix of verified and invented news. There are several varieties of misinformation, each with unique characteristics. First, there is satire or parody, which lacks the will to create fake news but risks obtaining the same result as the latter if the satirical news is taken as true. On other occasions, however, misinformation is achieved through the manipulation of facts and data that are carefully selected to convey a negative image of the person or event being reported. Other manifestations of incorrect information are identified in false connections and false context. In the first case, the title of the article or the images it contains evoke something different from what turns out to be real content.

In summary, fake news are completely false news or partially true but manipulated, passed off as correct information and circulated via the web. Their creation or spreading can be voluntary, that is, accompanied by the user's awareness that the news is false (in this case we speak of disinformation), or it can be involuntary, when the user ignores the falsity of the news and, believing in its truthfulness, spreads it (in this case we speak of misinformation).

This is an ancient phenomenon, but one that has taken on unprecedented importance with the advent of the Web 3.0. Through social networks, fake news can circulate with a much greater speed and capacity than in the past. Circulation is facilitated by the fact that they are articulated through a decentralised communication system in which barriers to entry, control mechanisms, and clear accountability provisions are lacking. It is in this thicket of information that more or more frequently we come across fake news, deep fakes, hate speech: phenomena that pollute information and make it difficult to distinguish reliable news from false or low quality news.

The mechanism of the filter bubble immediately reveals how the strategy that drives the spread of fake news has been developed in a commercial context: the algorithm profiles users, captures their tastes and attitudes to spending, and provides news capable of attracting their attention and influencing their behaviour. The user "shares" the content multiple times, triggering an amplifying effect that conveys, along with the fake news, advertising.

If this mechanism was born as a marketing strategy, however, it is on the political level that it unlocks its disruptive potential. Fake news does not only serve to convey incentives to purchase, but it also produces politically

relevant effects, conditioning the opinions of users and creating pockets of consensus on specific issues, to the point of undermining a country's political stability.

The disintermediation that characterises the Web 3.0 enables new political uses of communication. Just think, for example, of an election campaign. Today, a candidate can have direct contact with voters effectively, quickly, and at negligible cost compared to traditional strategies. A speech given during an election campaign can be delivered in a certain place and be shared immediately, reaching the electorate in every corner of the country. Perhaps there is, however, another more relevant aspect: the ability to tailor the message to the audience. Thanks to the traces that users leave more or less voluntarily on social networks, the organisers of an electoral campaign can draw on a whole series of information and data regarding possible voters. This way, thanks to an accurate analysis of elements such as gender, age, likes, place of residence, habits and so on, it is possible to tailor an electoral message that suits the audience to which it is addressed. At the same time, social platforms make it possible to analyse public opinion at all times, rendering the mood of the electorate on a given topic intelligible moment by moment, and thus enabling real-time updates of electoral strategy.

In this perspective, it is clear that if the use of social networks is accompanied by the use of fake news, the process of building political consensus is radically disrupted. For empirical confirmation, suffice it to think of the results of the Brexit referendum or the election of the 45th President of the United States (Allcott & Gentzkow, 2017), events in which fake news played a significant role in overturning forecasts, favouring respectively the exit of the United Kingdom from the EU and the victory of Donald Trump over Hilary Clinton (Special Counsel R.S. Mueller III, 2019).

Blockchain: Does technology take, does technology give?

We have seen how the use of social networks has facilitated access to a colossal mass of information without mediation and control. If we are living today in the age of integral knowability, we are not, however, living in the age of integral knowledge. On the contrary, we have to face phenomena that make access to reliable information more complex, thus altering or even preventing access to knowledge, the forming of political opinion, and public debate.

Law (along with rights) is being challenged by technologies. However, the very technologies behind the problem can also provide solutions. For some time now, research centres and software solution developers around the world have

been developing strategies that make it possible to detect early and then break down the viral potential of fake news (Sharma et al., 2018).

Combating the spread of fake news on social media, which is ontologically predisposed to the creation of "noise" (Zubiaga et al., 2018), in particular, requires a critical approach in the perspective of data mining (Shu et al., 2017), which allows identifying solutions that are data-oriented (and therefore aimed at the analysis of datasets), but also feature-oriented (content analysis), model-oriented (supervised or completely entrusted AI tools) and application-oriented (aimed at the detection or removal of fake news).

There are many tools that digital technologies can offer to ensure the trustworthiness of news disseminated online (Zhang & Gupta, 2018). I am thinking, in particular, of the ever-widening array of artificial intelligence strategies built on applications of machine learning and deep learning (Ahmed, Traore, & Saad, 2017), such as genetic algorithms (Sahoo & Gupta, 2020) and Graph Neural Networks (Mahmud et al., 2022).

But the most promising solution is probably the use of blockchain technology. The idea behind blockchain technology dates back to the 1990s, when Stuart Haber and Walter Scott Stornetta (Haber & Stornetta, 1991) developed a technique capable of marking digital documents in order to prevent the possibility of backdating them. However, it is only twenty years later, with Satoshi Nakamoto and the invention of Bitcoin, that the blockchain has established itself as a tool for exchanging information in a secure way, without the intervention of third parties responsible for ensuring its certainty. Bitcoin does nothing more than allow a participant to carry out digital transactions directly with another party without the need to resort to and rely on a centralised intermediary to validate payments.

Blockchain, as it is known, is only one of the available Distributed Ledger Technologies (DLT). This particular category of technologies is characterised by a peer-to-peer distributed ledger system in which the entries in the database are replicated across a sequence of nodes. Moreover, the system is regulated through shared and distributed consensus mechanisms among all nodes.

Distributed ledger technologies differ both from technologies based on a centralised ledger as well as those that are characterised by a structure based on a decentralised ledger. The centralised ledger, which is the most common, is characterised by a strictly centralised one-to-many relationship. In this type of technology everything must be managed in relation to a centralised structure: trust comes from the authoritativeness of the person at the head of the organisation. The decentralised ledger, instead, introduces a centralised set-up at local level, so that there will be several central cores characterised by a one-to-many

relationship, which, in turn, have relations with all the other central cores always through a one-to-many relationship. This will give multiple central entities. In the decentralised ledger, governance and trust are still entrusted to a centralised entity.

The distributed ledger differs from these two models in that there is no central entity: there is no head, and a fully distributed logic is adopted. Trust and governance are distributed among all parties, as is consensus.

The blockchain is, therefore, a structure of shared and immutable data: a sort of digital ledger in which information is contained in blocks accompanied by fingerprint hashing and temporal validation. Each transaction is signed and validated, and then stored in blocks and associated with a timestamp. Each block is uniquely associated with a hash, generated by a non-invertible algorithmic function. Each block, besides its own hash, also contains that of the previous block (with the only exception of the first block, called "genesis"). This way the hash acts as a link between the various blocks and guarantees the non-alteration of the block and the data it also contains thanks to strategies such as "proof-of-work" (PoW), a consensus algorithm that avoids the risk of tampering even by attackers with very high computing power. The set of blocks concatenated by means of a cryptographic function and hashes constitutes the ledger, that is, the public register in which all transactions are recorded in a definitive, transparent and sequential way.

The key actors in this mechanism are the miners who compete, through computers or computer systems, to solve the mathematical problem (the proof-of-work) that allows adding a new block to the chain and to obtain a reward. Whenever a new block is added, it is sent to all nodes in the network, which can then verify the block and ensure that it has not been altered. If this check is successful, each node adds the block to its blockchain.

Unlike centralised structures, where control, data management, and authorisations are entrusted to a central authority and the system is based on the trust placed in it by all participants, the management of data updates in distributed registries is done with the cooperation of the participants that make it possible to access, distribute, and share data. Thanks to the use of one of the many existing consensus mechanisms (which can be distinguished into permissionless or public, permissioned or private, and hybrid chains), these technologies allow intermediation by third parties to be eliminated: all users participating in the chain can verify and control the correctness of transactions.

The decentralisation that characterises the blockchain makes it difficult to manipulate and particularly reliable. If one of the nodes belonging to the chain is compromised, the other nodes retain their operability and preserve the chain.

And so here we come to the core of the matter: is it possible to imagine the use of blockchain technology, as it is able to guarantee the immutability, traceability and authenticity of the data it contains, in the fight against disinformation and misinformation online?

Thanks to its characteristics (consensus-based decentralisation, transparency, security, immutability and efficiency), blockchain has proven to be an extremely versatile tool, suitable for use in a very wide variety of sectors. Often associated with the phenomenon of cryptocurrencies, this technology represents a platform for the exchange of information and data that can potentially be used in the most diverse fields: from supply chain management to the management of a patient's medical record, from the remuneration of the authors of a piece of music for each listening session to the automatic refund of a flight ticket that has been cancelled.

The blockchain can therefore also offer the possibility to trace the process of a news item, to keep track of its author, to ensure that it has not been modified during distribution and sharing on online platforms, and to determine with certainty the date on which an article was written. In other words, it could fulfil two important functions to counter the spread of fake news: certify the author making it possible to assess his or her reliability and trace the path of the news item allowing for a reconstruction of its "history".

However, it should be stressed that, while on the one hand the mechanisms highlighted above can prove to be a valuable aid in assessing the reliability of news, ascertaining its origin and originality, on the other hand blockchain is not able to guarantee that the news is "true": if the news originally recorded is false, it will remain so, and the chain will limit itself to guaranteeing its traceability, originality and origin.

Many research centres around the world are working in this direction. One of the most promising systems (Qayyum, Qadir, Janjua, & Sher, 2019) is based on a structure with three key elements: a publishers management protocol manages the authors of the publications, checking the reliability and authoritativeness of the sources; a smart contract for news publishes the news on the network, accompanying it with relevant information such as the name of the publisher, the timestamp, the public cryptographic key; finally, building the news blockchain, composed of "honest miner nodes", maintains the integrity of the system.

However, it is also important to account for more basic experiments that have already been translated into reality. Some journalists, for example, use the platform Lirax.org to affix, next to their signature at the bottom of an article, a QR code that allows access to the original document certified in blockchain, accompanied by the date and time when the article was recorded, place of signing and

certification of the author, and proof of his or her actual membership in a professional association.

In addition, more and more news agencies are using blockchain technologies to make the news they disseminate easily identifiable. Each publication is accompanied by a digital stamp that ensures its originality. For each news item published by the agency it is possible to know with certainty the correspondence with the original content, the date and time of registration, the author and so on. Such a solution allows readers to check the origin of the news consulted and any updates made to it, thus facilitating what readers need to do to verify the reliability of the news.

Having a mechanism that allows you to verify the origin of the news from an authoritative source and its originality is an unquestionable advantage for readers who need to choose who to trust in the vast ocean of information available online. However, in my opinion, to claim that this is the ultimate solution to an extremely varied and ever-expanding phenomenon seems naive.

While digital technologies are both capable of generating problems and offering solutions to these very problems, the "human factor" must always be considered fundamental. As tools, digital platforms always remain "neutral": it is not the social medium itself that generates good or bad information, but it is always the use that people make of that tool that allows evaluating its reliability, lawfulness, correctness, and justice.

This, of course, does not mean adopting a drastically critical perspective towards the undeniable opportunities offered by digital technologies. Rather, it means taking on the burden of knowing how these tools work: without this effort, it is not possible to build the awareness that must necessarily guide the relationship between human beings and technological tools.

In conclusion: we welcome all efforts made to develop strategies to counter the phenomenon of fake news using algorithms, blockchain and neural networks. However, we cannot expect that the answer to the problem can be delegated to machines, because just as the human factor is part of the problem, the human factor must also be part of the solution. Therefore, a "hybrid" approach based on awareness and the wise use of "intelligent" tools, always under the supervision of humans (Shabani & Sokhn, 2018) seems to me the only viable way on the road to defend free information and democracy.

References

Ahmed, Hadeer / Traore, Issa / Saad, Sherif. Detection of online fake news using n-gram analysis and machine learning techniques. *International conference*

on intelligent, secure, and dependable systems in distributed and cloud environments. Springer: Dordrecht, 2017, pp. 127–138.

Allcott, Hunt / Gentzkow, Matthew. Social media and fake news in the 2016 election. *Journal of economic perspectives, 31*(2), 2017, pp. 211–236.

Baran, Paul. On distributed communications networks. *IEEE Transactions on Communications Systems, 12*, 1964, pp. 1–9.

Castells, Manuel. *The Rise of the Network Society. The Information Age: Economy, Society and Culture.* Blackwell: Cambridge, MA-Oxford, 1996.

Dorogovtsev, Sergey N. / Mendes, José F. *Evolution of Networks: From Biological Networks to the Internet and WWW*. Oxford University Press: Oxford, 2013.

Fioriglio, Gianluigi. *Democrazia elettronica. Presupposti e strumenti.* Cedam-Wolters Kluwer: Padova, 2017.

Formenti, Carlo. *Cybersoviet. Utopie postdemocratiche e nuovi media.* Raffaello Cortina: Milano, 2008.

Foroohar, Rana. *Don't Be Evil. How Big Tech Betrayed Its Founding Principles.* Currency: New York, 2019.

Gilder, George. *Life After Google.* Washington D.C.: Regner Gateway, 2018.

Gometz, Gianmarco. *Democrazia elettronica. Teoria e tecniche.* EtS: Pisa, 2017.

Haber, Stuart / Stornetta, Wakefield S. How to time-stamp a digital document. *Journal of Cryptology*, *3*(2), 1991, pp. 99–111.

Lettieri, Nicola. *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico.* Mucchi: Modena, 2020.

Lévy, Pierre. *Les technologies de l'intelligence. L'Avenir de la pensée à l'ère informatique.* La Découverte: Paris, 1990.

Mahmud, Fahim M. / Rayhan, Mahi / Shuvo, Mahdi H. / Sadia, Islam / Morol, Kishor. A comparative analysis of Graph Neural Networks and commonly used machine learning algorithms on fake news detection. *7th International Conference on Data Science and Machine Learning Applications (CDMA)*, 2022, pp. 97–102.

Mancarella, Marco. *eVoting e nuove dimensioni della democrazia.* Tangram Edizioni Scientifiche: Trento, 2013.

Mathew, Ashwin J. The myth of the decentralised Internet. *Internet Policy Review*, *5*(3), 2016, retrieved 1.6.2022, from DOI 10.14763/2016.3.425.

Palano, Damiano. *Bubble Democracy. La fine del pubblico e la nuova polarizzazione.* Scholé: Milano, 2020.

Preterossi, Geminello. *La politica negata.* Roma-Bari: Laterza, 2011.

Qayyum, Adnan / Qadir, Junaid / Janjua, Muhammad U. / Sher, Falak. Using blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional, 21*(4), 2019, pp. 16–24.

Rodotà, Stefano. *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione.* Roma-Bari: Laterza, 1997 [ediz. accresciuta 2004].

Rodotà, Stefano. *Iperdemocrazia.* Roma-Bari: Laterza, 2013.

Rouvroy, Antoinette / Stiegler, Bernard. Le régime de vérité numérique. De la gouvernementalité algorithmique à un nouvel État de droit. *Socio, 4*, 2015, pp. 113–140.

Sahoo, Somya R. / Gupta, Brij B. Classification of spammer and nonspammer content in online social network using genetic algorithm-based feature selection. *Enterprise Information Systems*, *14*(5), 2020, pp. 710–736.

Shabani, Shaban / Sokhn, Maria. Hybrid machine-crowd approach for fake news detection. *IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, 2018, pp. 299–306.

Sharma, Karishma / Qian, Feng / Jiang, He / Ruchansky, Natali / Zhang, Ming / Liu., Yan. Combating fake news: A survey on identification and mitigation techniques. *ACM Trans Intell. Syst. Technol., 37*(4), (2018, August), 41.

Shu, Kai / Sliva, Amy / Wang, Suhang / Tang, Jiliang / Liu, Huan. Fake news detection on social media: A data mining perspective. *SIGKDD Explor. Newsletter*, *19*(1), 2017, June, pp. 22–36.

Special Counsel R.S. Mueller III. *Report on the Investigation into Russian Interference in the 2016 Presidential Election.* Washington D.C., 2019: https://www.justice.gov/storage/report.pdf.

Stiegler, Bernard. *Èta*t *de choc. Bêtise et savoir au XXI siècle.* Paris: Fayard/Mille et une nuits, 2012.

Taplin, Jonathan. *Move Fast and Break Things.* London: Macmillan, 2017.

Wu, Tim. *The Master Switch. The Rise and Fall of Information Empires.* London: Atlantic Books, 2013.

Zhang, Zhiyong / Gupta, Brij B. Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 2018, pp. 914–925.

Zolo, Danilo. *Il principato democratico. Per una teoria realistica della democrazia.* Milano: Feltrinelli, 1992.

Zubiaga, Arkaitz / Aker, Ahmet / Bontcheva, Kalina / Liakata, Maria / Procter, Rob. Detection and resolution of rumours in social media: A survey. *ACM Computing Surveys* (*CSUR*), *51*(2), 2018, pp. 1–36.

Zuboff, Shoshana. *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.* PublicAffairs, New York, 2019.