The informational disorder and Artificial Intelligence; between major insidies and possible contrasting tools*

Andrea Ruffo [1,*]

[1] *University of Milan, Milan, Italy*

Abstract

The relentless development of digital technologies has brought about profound social changes over the past decade. In addition to improvements in the means, capabilities, and content of information and communication, the multifaceted pervasiveness of new hi-tech tools has amplified existing problems in the world of news, including disinformation and, more generally, all forms of informational disorder. Misinformation is among the forms of disorder where the use of new digital technologies, supported by Artificial Intelligence (AI), can amplify the harmful effects or, conversely, counter them.

Keywords

informational disorder, disinformation, Artificial Intelligence, European regulation, deep fakes

1. The evolution of the European fight against disinformation phenomena

Since the annexation of Crimea (2014) by the Russian Federation [2], the institutions of the European Union began to question the extent of the disinformation phenomena - which had disoriented public opinion on that occasion - and what regulatory and sanctioning tools were available to prevent and counteract their effects. In the year following the annexation, exactly on 20 March 2015, the European Council initiated, through the High Representative for the Common Foreign and Security Policy, the preparation of an action plan to counter Russian disinformation campaigns [3]. Subsequently, therefore, in 2016 the following were established: the European Centre of Excellence in Countering Hybrid Threats [4] and the Hybrid Threat Analysis Cell, which were added to the East Strat Task Force (ESCTF) [5]. The European Parliament resolution 2016/2276(INI) of 15 June 2017 'on online platforms and the digital single market' represents a milestone in the European strategy against disinformation, as in addition to condemning the spread of fake news in the digital world, it urged both online platforms to provide users with tools to report it and the European Commission to take regulatory action to reduce disinformation [6].

The fight against false news (media termed fake news) [7], spread online, thus became an element of the framework programme outlined by the European Commission, which envisaged both publishing in a special list, 'unmasking' them, the sources of disinformation and setting up a group of experts to create a paradigm to balance the citizens' right to access quality information with the freedoms deriving from Article 21 of the Constitution (freedom of thought). The report [8], produced the following year (2018) by the aforementioned group of experts, aimed to map out a more reliable and transparent digital info-sphere in which the first control would be entrusted to the users themselves, i.e. civil society and private companies (especially online service platforms and social-networks/media). In this way, a greater knowledge of digital media tools was promoted (so-called media literacy), the creation of tools (including algorithmic tools) that would allow the identification and removal of misinforming content (in parallel with an independent commission of verifiers), and the elaboration of some embryonic forms of internal regulation (list of principles), to

* *Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT*

[1,*] Corresponding author.

andrea.ruffo@unimi.it (A. Ruffo)

which all economic operators in the Internet world would have to adapt [9]. In parallel, the EU Commission set up an independent system of verifiers.
This initiative launched in May 2018 can be seen as the political and organisational incipit for the subsequent drafting, in the form of self-regulation, of the 'Code of Good Practice on Disinformation' (Code of Conduct), published at the very end of September 2018 [10].
Between 2019 and 2020, the persistence of disinformation campaigns and the conditioning of electoral events by parties outside the European Union [11] prompted the institutions in Brussels to plan new regulation and countermeasures. In this regard, the Rapid Alert System (R.A.S.), wanted in compliance with the Action Plan against disinformation [12], to improve information sharing (through micro-targeting [13]) between the EU and member states and the fight against disinformation phenomena.
The Sars-Covid-19 pandemic, with the consequent measures of prolonged home isolation (so-called lockdown), the mass vaccination campaign, and the increased use of digital platforms and social networks to communicate and work, at the same time as the spread of mystifying and destabilising news, represented a moment of very strong impetus for the strengthening of the EU's measures to prevent and combat disinformation [14].

2. Modifications The European legal framework for combating online disinformation

Wanting to outline the current European regulatory perimeter for countering online disinformation, it should be pointed out that following the approval of the 'European Digital Package' under the first Von der Leyen Presidency [15], there has been, in the post-pandemic period and in conjunction with the Russian invasion of Ukraine, a further strengthening of the measures already adopted in 2018.
Indeed, on 16 June 2022, the previous 'Code of Good Practice against Disinformation' was updated and amended, with the publication of the 'Enhanced Code of Good Practice on Disinformation'.
It is precisely this latter document, commonly referred to as the Strengthened Code (strengthened) [16], to which 34 signatory companies [17] have adhered, that aims to achieve the goals set out by the Commission in May 2021, by establishing a broader range of commitments and measures to combat online disinformation. The signatories committed themselves, in fact, to: demonetising the spread of disinformation; guaranteeing the transparency of political advertising; empowering users for a conscious use of the Internet; increasing cooperation with fact-checkers; and providing greater access to platform data.
The strengthened code, moreover, precisely to increase the transparency of the digital reality of platforms (often characterised by information asymmetry), introduces: an ad hoc centre to provide all information on the policies of intermediary service providers connected to the main site, as well as a permanent task force (chaired by the EU Commission and formed by a number of stakeholders and other European bodies) to continue to update the implementation of the regulatory measures in progress to the incessant technological progress, which also affects the techniques and tools of disinformation.
This enhanced monitoring is amplified by the Code by means of a reporting system whereby very large online platforms (big players [18]), under the Digital Service Act (DSA), will have to report on their operations to combat and prevent disinformation every six months, unlike smaller players who will do so annually. In this system, assessment mechanisms are introduced by the Enhanced Code that will judge, by means of numerical performance indicators (Key Performance Indicators - KPIs), the platforms on the basis of the adequacy, effectiveness and number of anti-disinformation measures implemented.
The provisions introduced in 2022 by the Strengthened Code mean that the nature of the document has substantially changed compared to the self-regulatory nature of its predecessor (code of good practice) [19], voluntarily subscribed to in 2018 by many digital technology and advertising

companies, and is therefore to be considered a co-regulatory instrument, in which the European Commission exercises apex control in accordance with Article 45 of the Digital Service Act [20].
The strengthened code also contains a clear commitment to work towards the definition of structural indicators, making it possible to measure the overall impact of the code on disinformation.
The Digital Service Act (DSA) [21], an EU regulation on services provided by large web companies, which addresses the issue of effective and efficient moderation and online content, and also introduces forms of liability for digital platforms, is - in fact - the most up-to-date source of regulation in the European regulatory perimeter for combating online disinformation.
In this regard, explicit references to the issue of information disorder are contained in the recitals and articles, which are reproduced below for completeness.
Recitals no:
- 69 and 83 (for the generic risk of disinformation campaigns)
- 84 (for risk assessment by service providers, expressly referred to in Art. 34)
- 88 (in respect of awareness-raising actions against disinformation)
- 95 (on the prevention in advertisements of manipulation and disinformation techniques. See also Art. 39 on the subject of transparency in online advertising)
- 104 (on platforms' codes of conduct on disinformation)
- 106 (refers to the strengthening of the 'code of good practice on disinformation)
- 108 (indicates that the Article 36 Crisis Response Mechanism also applies in the case of disinformation)

Through the application of Article 74 (concerning the financial penalties that the Commission may impose on providers of online platforms), moreover, the DSA aims to disincentivise disinformation from an economic point of view; given that after determining the falsity of a content, in addition to the financial penalty for non-compliance with the rules of the regulation, advertising revenues for platforms and search engines would also be reduced to zero or drastically reduced.
According to Art. 10(a), web companies will have to carry out checks on the 'effectiveness' (i.e. the real existence) of accounts in order to discourage the use of fake profiles, thus limiting potential misinformative conduct.
However, in addition to the previous references, it is precisely Article 45 of the DSA that introduces the novelty of the use of indicators (specifically performance indicators) as part of the assessment under the platforms' codes of conduct [22].

3. Informational Disorder and the Risks for the State

The importance of countering the phenomena of information disorder (of which 'pure' disinformation is only one of the most recognisable forms of conduct) is to prevent such actions, which form part of the instrumentarium of hybrid wars [23], from jeopardising both the rights of individual citizens and the very integrity of states [24].
The phenomenon of information disorder can subsume within it various conducts, sometimes not necessarily voluntary and malicious, which can be subsumed under the four macro categories of:
- disinformation,
- misinformation,
- malicious information,
- misrepresentation.

In the case of the first type, i.e. 'pure' or 'classic' disinformation, this is conduct that involves the intentional creation and/or malicious dissemination of false information, with the aim of causing damage to a State or a system of countries, with integrated or jointly easily influential information/media channels (in the latter case, it can be considered that the result of a successful disinformation campaign against, for example, France may give rise to misinformation in Italy or vice versa). Until the first half of the 20th century, disinformation operations were the almost exclusive prerogative of national intelligence and security apparatuses, which adopted them to influence

satellite states pro domo loro or to "prepare the ground" for eventual war actions in hostile countries. With the evolution of mass media (the diffusion, for civilian purposes, of the Internet channel) and the emergence of non-national and asymmetrical global actors, cross-cutting and non-national disinformation actions have also developed, which may pursue criminal ends that are "third" and contrary to the policies of states or act in support of them but without depending on them directly, so as to disguise their objectives and to camouflage themselves among investigative and/or philanthropic forms of information.

Another technique of disinformation is misinformation propaganda, which more than tends not only to publicize sweetened news to influence domestic public opinion but has in the latter the channel (and not the goal) of spreading the fake news, according to the principle "if our citizens believe it, the enemy will believe it too."

Misinformation, on the other hand, consists of conduct that involves the unwitting creation and/or dissemination of false information. In this case the one who spreads or generates the news (perhaps, for example, after viewing an audio-visual source or translating the foreign press) is in good faith and thinks he or she is rendering a service to the community, without realizing that, instead, he or she is contributing to propagating disinformation. It is, therefore, an action that does not involve malicious intent on the part of the main actors (journalists, members of the institutions or informants in various capacities) but integrates, depending on the case, the possible culpable responsibilities for inexperience, culpa in vigilando and lack of professionalism. In addition to "classic" tools for inducing misinformation (e.g. artfully spread rumors, false news sources made to be found by improvised officials or journalists or media influential figures) and misinformation induced "reflexively" by misinformation of others, thanks to the refinement of digital techniques of "special effects" there has arisen -in the last decade- the tool of deep-fake, which consists of the alteration, by artificial computer reworking, of an audiovisual content, with such a degree of verisimilitude that it is difficult to distinguish from the true for the human eye. Misinformation increases its effectiveness in proportion to the degree of fame and reliability of the source who unwittingly creates it (the better known and popular the author of the news will be, the more reliable the content of the news will be; according to the principle that "if he/she says it, it will be true").

Malicious information, from malicious information ("harmful information" or "malicious i."), in turn, consists of the willful and malicious dissemination of news that is true but covered by a confidentiality regime (in Italy, four levels can be distinguished: confidential "R," confidential "RR," secret "S," and top secret "SS"), for the purpose of creating adverse consequences and/or discredit in the Institutions (mainly governments) that have secreted it. Very often such conduct is perpetrated as a result of other acts of hybrid warfare such as hacker attacks on government servers and/or confidential databases, material misappropriation of strategically important documents, or bribery of officials in charge.

Finally, improvised or recentism-influenced information is a fourth category that contributes to increasing information disorder, which I personally believe to be quite distinct from the previous ones, is represented by the reckless dissemination of news (so-called improvised or recentism-influenced information) that is true but partial or not yet fully defined, with respect to complex and very recent events. With the rise of social platforms and, in general, of the Web among the channels for disseminating news and audiovisual content, the world of information has been progressively affected, both in the method of source research and in narrative timing, tending to increasingly favor media and emotional narration of facts over their in-depth critical content. The "race for exclusivity" (i.e., to be the first to provide information in order to overcome media competition) originates, in complex and changing contexts (as in the case of the pandemic emergency or the war events in Ukraine), information that is partial or contradictory with subsequent developments of facts or with the same thematic insights, generating confusion and disorientation in public opinion, as well as a sense of distrust towards institutions and accredited information channels, thus leaving room for the possible creep of possible disinformation or misinformation-induced actions.

Although technically dissimilar actions, given the multifaceted nature of media channel technologies and the interconnectedness of cause-and-effect relationships, the four misinforming conducts can often be found simultaneously, directly concatenated with each other [25].
Given the extreme versatility of the information-disrupting conducts (described above) and the subtlety with which they can be combined with each other - to conceal themselves, go undetected and thus hit the target - it seems clear that all disinforming phenomena are considered a risk to states, at the center of international agendas of prevention and countering [26].
The risks to the state can be of a different nature, ranging from marginal aspects and related only to the mere information of individual citizens (in any case enshrined in the constitutional right to be informed, ex art. 21 Const.) to the political and social destabilization of the entire country affected.
The restriction of the right to general information, the manipulation of public opinion by hostile countries, the systematic discrediting of institutions, the infiltration of the circuit of information and public security, the socio-political destabilization, the compromise, theft and damage of data carried in the carrier information circuits and of the storage and dissemination systems themselves, are only the main risks - placed on an evidently increasing scale - that the State can run if it does not effectively counter the disinformation campaigns [27].

4. The negative contribution of Artificial Intelligence to information disorder

Given the pervasiveness of the disinformative conducts of that make up the defining spectrum of informational disorder, it seems clear that the Internet and related digital technologies can only exponentially increase the risks to states and, more broadly, to the individuals who populate them.
As technological development relentlessly outpaces the proceeding of the world of law and, therefore, of any form of ex ante regulation, the new technologies of the Internet world (whether digital, algorithmic or machine learning-based) are simultaneously a challenge and an aid to lawmakers.
This is also the case with Artificial Intelligence (AI), a technology based on both supervised and unsupervised machine learning, which since the second decade of the 2000s has been experiencing a steady rise in functional applications and scientific debate.
The European legal world has tried to find an unambiguous definition of AI, referring to the term as all "\[\...\] those systems that exhibit intelligent behavior by analyzing their environment and performing actions, with some degree of autonomy, to achieve specific goals" [28]. This is obviously a very generic definition, dating back to 2021, which only vaguely outlines the potential and risks of Artificial Intelligence.
In this specific case, wanting to trace the negative contribution (as further amplifying harmful conduct already taking place online) that AI will be able to make to information disorder, it is first necessary to present the vast array of digital products that such technology creates or will be able to further enhance.
Among the best known of these, directly considered a product of artificial intelligence, are deep fakes, defined in 2020 by the Italian Data Protection Authority as those audio-visual products that "\[\...\] are photos, videos, and audios created thanks to artificial intelligence (AI) software that, starting from real content (images and audios), manage to modify or recreate, in an extremely realistic way, the characteristics and movements of a face or body and to faithfully imitate a given voice" [29].
These are therefore falsifications of photos, audio or videos that are so faithful and in-depth (as the apposition "deep" directly refers to) that only a meticulous AI system can succeed in creating [30].
Compared to previous forms of artificial modification (think of the old photomontages or the distortions of sound or the cuts or blackening or blurring of videos) these are products that are much more faithful to reality and, for this reason, much more difficult to distinguish by the human eye in the absence of further contextual information.

To deep fakes, which can be considered in all respects a direct product of AI, we must add, due to the dizzying increase in the negative potential that this technology can unleash from them, computer trolls, sock-puppets and sealioners.
Proceeding in order, cyber trolls, who can be considered the conceptual basis of the other two categories (more refined and specialized), are technically Internet users who interact with others with an annoying and provocative attitude to disturb the normal coexistence of communities and social networks, in order to cause interpersonal conflicts and online controversies. Behind every troll, through a false public identity, there is generally a real user who, protected by a pseudo anonymity, operated undisturbed. With the advent and implementation of AI, now, even computer trolls, codified their behavior through machine learning, could be managed by an artificial system, with further problems for the damaged user and for any coercive prevention or inhibition measures (because artificial intelligence can replicate the same behaviors countless times and quickly with new and different ID profiles).
Following the same pattern as trolls, AI can also generate sock-puppets (literally translating from the English "straw men"), which in computer language indicate those fake computer profiles created by users of social networks or other virtual communities to obtain, through the opposition to their fake and illogical or weak arguments (often wrong and bad), greater consensus and approval. By applying artificial intelligence, such "virtual straw men" could be even more difficult to recognize and much more effective both in carrying out plausible behaviors and in self-duplication and relating, with a further distortion of reality.
Sealioners, on the other hand, are those fake computer profiles that feign ignorance or kindness while incessantly asking for answers and evidence (often ignoring or evading the evidence already presented) to a victim user, with the excuse of "just trying to have a debate" in order to provoke him to respond with anger, so as to act as an injured party by presenting the target as, for example, a closed and unreasonable person. The application of AI, even in this case, can only enhance both the mimetic capabilities of such attempts and their debate capabilities, making the provocative approach even more scientific and, collaterally acquiring with computer archiving precision all the data provided in the debate by the target user. Information, in this case yes real and sensitive, which can be processed by the same sealioner artificial intelligence system for other malicious purposes or in any case not permitted by the Law.
For all this and for the further implementations that, with technological progress and unsupervised learning, AI systems can develop, it is clear how such technologies can exponentially incentivize information disorder. If on the one hand, in fact, deep fakes, as they are deeply (and accurately false) can be a direct source of disinformation or misinformation, on the other hand trolls, sock puppets and sealioners compete as more or less reliable channels to spread false or partial information and to steal other information, even confidential, potentially also productive of misinformation (or malicious information) conduct.
Considering, therefore, the relevance of the positive and negative impact of Artificial Intelligence in society, it is not surprising that the European institutions (Parliament and Council) have outlined in the new AI Regulation (or AI Act) a specific attention to the contribution of AI towards disinformation and therefore the measures necessary to reduce it.

5. Conclusions

The obligations of traceability, transparency, limitation of use, information to the user and possible human supervision and intervention, provided for by the AI Regulation, both for suppliers and for users of artificial intelligence systems, therefore represent a first form of suitable instrument to limit the harmful impact of this technology in the field of information disorder.
However, these are corollary principles that are still too nuanced and vague and do not directly affect all existing forms of disinformation through sources (e.g. deep fake) or channels of dissemination (trolls, sock puppets and sealioners) generated by AI but which, in some way, want to be a starting regulatory element. The very fact of having included in the regulatory scope of the regulation the

definition of deep fakes and the obligations for those responsible for AI systems, may constitute a favorable element for any case law to combat disinformation conduct (such as misinformation) originating from the incorrect or maliciously induced use of other technologies.
Of course, the timing with which all the measures provided for by the Regulation will come into force (especially the sanctioning ones) leave a wide limbo and time margin for maneuver for disinformation actors, who in the meantime will be able to use their own systems to escape the mesh of the regulation but, however, precisely because of the general abstractness of the provisions, they are forced to go beyond the fundamental elements of AI.
On the other hand, the correct interpretation of the principles outlined by the AI Act, may lead, in the research and development of new artificial intelligence systems, to the creation of AI products capable of recognizing the bad uses of the same technology, thus contributing -- with the same means and equal precision -- to limit its negative contributions to society.
I refer to the topic of contrasting disinformation, just as (according to the American approach) a true news item effectively refutes a false one, an artificial intelligence, used for the good of society, contrasts that used for illicit purposes.

Acknowledgements

This work was supported by the PNRR SERICS project (ACK: PE000014).

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[2] S. Lattanzi, “La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino”, in MediaLaws, n. 3, 2022, p. 163.
[3] See the European Council website at the following link: <https://www.consilium.europa.eu/it/press/press-releases/2015/03/20/conclusions-european-council/>.
[4] Joint Communication from the High Representative of the European Union to the European Parliament and the Council, Joint Framework to counter hybrid threats. The European Union's response, Brussels, 6.4.2016.
[5] See the article “EU to counter Russian propaganda by promoting 'European values'”, published by The Guardian on 25 June 2015.
[6] S. Sassi, “L'Unione Europea e la lotta alla disinformazione online”, in federalismi, n. 15, 2023, 189.
[7] COM(2017/650 “final”), del 24.10.2017 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, «Commission Work Program 2018. An agenda for more united, stronger and more democratic Europe», Strasburg, p. 4.
[8] See the EU site to the link: https://ec.europa/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-andonline-disinformation.
[9] See Report from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018/794 final) on the implementation of the Communication "Tackling online disinformation: a European approach", Brussels, 5.12.2018, p. 1.
[10] O. Pollicino, “I Codici di Condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della Strategia europea contro la disinformazione online”, in Rivista Trimestrale di Diritto Pubblico fasc. 4, 2022, 2 ss.
[11] Consider the Cambridge Analytica case or the various disinformation practices, attributable to actors directly or indirectly linked to the Russian Federation, in relation to some electoral appointments or public consultations of citizens (referendums) held in EU states.

[12] See Joint Communication from the European Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation, Brussels, 5.12.2018, p.7 ff. See the EU website at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0036.

[13] System that provides for the detailed sectoral subdivision of objectives and information elements, allowing communication oriented according to membership in one of the identified categories.

[14] See the press release by High Representative J. Borrell and Vice-President for Values and Transparency V. Jourová, 10 June 2020, Coronavirus: Strengthened EU action against disinformation -- Brussels). The First (Borrell) stated that «\[\...\]influence operations and targeted disinformation campaigns are a recognised weapon of state and non-state actors, the European Union is stepping up its activities and improving its capacities to fight this battle» while the Vice-President added that «To fight disinformation, we need to mobilise all relevant actors, from digital platforms to public authorities, and support fact-checkers and independent media. While digital platforms have taken positive steps during the pandemic, they need to step up their efforts. Our actions are deeply rooted in fundamental rights, in particular freedom of expression and information».

[15] F. Zorzi Giustiniani, "The European Union and digital regulation: the Digital Services Package and the Code of Good Practices on Disinformation", in Nomos, n. 2, 2022, 3 ff.

[16] M. Monti, "The EU Code of Practice on Disinformation: Efforts in Progress to Counter Fake News", and "The Strengthened Code of Practice on Disinformation: Another Stone of the New European Digital Fortress?", both in MediaLaws.eu, No. 1, 2019 and No. 2, 2022.

[17] They are: Adobe, Alliance4Europe, Avaaz, Clubhouse, Crisp, Demagog, DoubleVerify, DOT Europe, Ebiquity, European Association of Communication Agencies (EACA), Faktograf, Globsec, Google, IAB Europe (Interactive Advertising Bureau Europe), Kinzen, Kreativitet & Kommunikation, Logically, Maldita.es, MediaMath, Meta, Microsoft, Neeva, Newsback, NewsGuard, PagellaPoltica, Reporters without Borders (RSF), Seznam, ScienceFeedback, The Bright App, The Global Disinformation Index, The GARM Initiative, TikTok, Twitch, Twitter, Vimeo, VOST Europe, WhoTargetsMe and World Federation of Advertisers (WFA).

[18] E. Kuczerawy, "Fighting on-line disinformation: did the EU Code of Practice forget about freedom of exepression?", in E. Kuzelewska, G. Terzis, D. Trottier, D. Kloza (a cura di), "Disinformation and Digital Media as a Challenge for Democracy", Intersentia, n. 8-9, 2019.

[19]: Sassi, "The European Union and the Fight against Online Disinformation", cit.

[20] For this reason, the strengthened code tends to become a mitigation measure and a recognized code of conduct within the co-regulatory framework of the DSA.

[21]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation).

[22] Point 3 of Article 45 DSA, in fact, establishes that: "\[\...\] the Commission and the Committee and, where appropriate, other bodies shall aim to ensure that codes of conduct clearly define their specific objectives, contain key performance indicators to measure the achievement of those objectives and take due account of the needs and interests of all stakeholders, in particular citizens, at Union level. The Commission and the Committee shall also aim to ensure that participants regularly report to the Commission and their Digital Service Coordinators at the place of establishment on all measures taken and their results, measured on the basis of the key performance indicators contained in the codes of conduct. The key performance indicators and reporting obligations shall take into account the differences between the different participants in terms of size and capacity"

[23] N. Bussolati, "The Rise of Non-State Actors in Cyberwarfare" in J. Ohlin, K. Govern, C. Finkelstein (a cura di), *CyberWar: Law and Ethics for Virtual Conflicts", University Press, Oxford, 2015, 102-126.

[24] S. Cymutta, M. Zwanenburg, P. Oling, “Military Data and Information Sharing -- A European Union Perspective*, in *Proceedings of the 14the Annual International Conference on Cyber Conflict”, 2022, 3 ss.

[25] The following "school case" can be an example. An unexpected event occurs, producing long-term developments, the media circle reacts by immediately providing partial news, rushing to compete for exclusives, but the same information is denied by subsequent events and by the mass media themselves; therefore, confusion is created in public opinion, which generates distrust in the institutions and traditional information channels. At this point, a hostile State, which has an interest in exploiting and worsening the situation, introduces other false or true classified news (therefore stolen and declassified) thus increasing the information disorder. Some sectors of free information (both national and foreign) take up this latest news, presenting it as truth and accrediting it with their reliability as a newspaper/author, spreading it further. As can be seen in the example, constructed ad hoc (but, however, attributable to specific cases that have occurred), all four forms of information disorder are intertwined and linked. From an initial situation of news affected by recency and not accurately verified, we move on to the possible disinformation and misinformation operated by a hostile Power, which if not appropriately detected and contrasted (in the world of the Internet it becomes more difficult because the news persists and, like in a Hydra, multiplies in various channels/forms) will spread further, cloaking itself in reliability thanks to the media that spread it.

[26] See on the subject, the report of January 10, 2024 of the World Economic Forum, which included them among the most relevant threats to the stability of countries and of the Western democratic-economic and value system itself. Attached below is the link to the website: https://www3.weforum.org/docs/WEF_GRR24_Press%20release_ITA.pdf

[27] S. Giusti, E. Piras, “Democracy and Fake News Information Manipulation and Post-Truth Politics”, London, 2020.

[28] According to the position paper Preparing a just future for Artificial Intelligence and Fundamental Rights, drafted by the European Union Agency for Fundamental Rights (FRA), 2021.

[29] Guarantor for the Protection of Personal Data, Deepfake. The fake that "steals" your face and privacy, December 28, 2020.

[30] M. Cazzaniga, “A new technique (also) for conveying disinformation: European responses to deepfakes”, in Medialaws, 2023, 172 ff.