Dissemination of fake news - Reflections on the practices and limits of prevention of online disinformation

Dr. Fotios Spyropoulos et al.

Abstract

This paper outlines measures and practices in order to prevent disinformation and dissemination of false news. Despite the fact that this delinquent behavior is not at all new, the reasons mentioned make this approach contemporarily necessary. Due to this reason, the nature of modern "digital" information societies, the specific characteristics of information systems (development field and asymmetric dispersion of fake news) as well as the limits/obstacles related to interventions of preventions in general, are taken into consideration (protection of fundamental rights, displacement of crime, difficulty in keeping the legislators constantly aware of the progressive developments and so on). The analysis includes forms of prevention at a penal, general preventive level and also, according to the criminology sight, social and occasional prevention. Finally, a critical approach to prevention policies is carried out in the paper.

1. The general outline - concerns regarding the prevention of disinformation on the internet

1.1 The phenomenon of disinformation, also known as "fake news"[1] or "hoax"[2], has taken on new dimensions in the digital age[3], although it is not new[4] and the majority

This study is being developed in the context of postdoctoral research on "Hoaxes and spread of fake news - survey on the (in)security of fake news through the Internet and on the economic and technical dimension of the phenomenon - Legal treatment and de lege ferenda", funded by the General Secretariat for Research and Technology (GSRT) and the Hellenic Foundation for Research and Innovation (HFRI) in the framework of the first HFRI call for proposals for research projects to support postgraduate researchers. University of Western Attica is the host institution.

of researchers who have dealt with the issue state that disinformation has always existed as a social/communicative phenomenon[5]. As a consequence, there is a growing need to intensify the debate on the prevention of the phenomenon and on the relevant attitudes and practices [6].

The research team consists of: Fotios Spiropoulos (Lawyer - Economist, Doctor of Criminal Justice Studies of the department of Law School of National and Kapodistrian University of Athens, M.A. in penology, M.A. in criminology, scientist responsible for the project), Vassileios Karagiannopoulos [Senior Lecturer & Head of Ethics, Institute for Criminal Justice Studies, University of Portsmouth (UK)], Evangelia Androulaki (Lawyer, M.A. In criminology, member of the Crime Study Center's Management Board), Nikolaos Karagiannis (Lawyer, M.A. in criminology), Aristotelis Kompothrekas (Phd candidate at University of Patras, mathematician, M.A. in information technology) and professor at the University of Western Attica Dr. Lazaros Vryzidis.

This article is a publication of the relevant participation in the Proceedings of the Scientific Conference of the Hellenic Society of Criminology held on January 10 and 11, 2019 on the topic: "Greek Criminologists from Greece and abroad are talking about the Prevention of Crime".

[1] For the definition of "fake news" see indicatevely: *Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, Huan Liu,* Fake News Detection on Social Media: A Data Mining Perspective*,* url: https://arxiv.org/pdf/1708.01967.pdf on 07/19/2018 and *S. Zaryan*, Truth and Trust: How Audiences are Making Sense of Fake News, Lund University, 2017, pp. 6 f. & 61, url: https://lup.lub.lu.se/student-papers/search/publication/8906886 (accessed 07.08.2018), *Lion Gu, Vladimir Kropotov, Fyodor Yarochkin,* How Propagandists Abuse the Internet and Manipulate the Public, Forward Looking Threat Reasearch (FTR), url: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf (accessed 19.07.2018).

[2] See the definition of «hoax» (url: https://en.wikipedia.org/wiki/Hoax, accessed 10.08.2018): the term hoax is used in English to describe something fake, and it seems to come from the "magic" words "Hocus Pocus" (a phrase that resembles the phrase "abra cadabra" most used in our country). Urban Legend seems to be more accurate, however, as a hoax is actually a reputation, a legend that is "wandering" and spreading through the network.

[3] Typical is the case of "pizzagate" (for a short description of the scandal based on fake news see url: http://ellinikahoaxes.gr/2016/12/08/pizzagate/, accessed 13.09.2018), due to the fact that went "viral" in social media by influencing the US political scene.

[4] A typical "fake news" case with a financial motive that has historically been recorded relates to the defeat of Napoleon in Waterloo on Sunday June 18, 1815. Banker Nathan Rothschild in London was of direct economic interest. So, he spread the news that Napoleon had defeated Waterloo. Because of this, the stock market collapsed and then Rothschild started buying. Until the truth was revealed in London, two days later, he had multiplied his fortune (according to a statement by journalist Makis Provatas in the article of *Giannis Pantazopoulos*, What is news today? Five Greek journalists respond, Lifo, 21.01.2016 – url: https://www.lifo.gr/print/print_feature/87218, accessed 10.08.2018).

[5] See for example *Robert Darnton,* The True History of Fake News, The New York Review of Books, 2017 (url: https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/, accessed 22.12.2018) and *A. Panagopoulos* Fake News and Data Analysis Part A', 2018 (url: https://bit.ly/2rRn1cJ, accessed 22.12.2018).

[6] The choice of prevention does not mean disregarding the applicability or even the existence of repressive methods, but it is the realization of Cesare Beccaria's statement: "it is more useful to prevent crimes than to punish them" (See. *St. Alexiadis*, Criminology, Sakkoulas, Athens – Thessaloniki, 2004, p. 280).

1.2.1 It is therefore crucial to document the existing preventive[7] ways of dealing with disinformation and spreading fake news as well as to evaluate them critically. In order, however, to achieve as much efficiency as possible in our working hypothesis, it is important to clarify the specific problems and their parameters in which preventive practices are called upon to respond, in the present socio-historical context ("digital age", "information society" and so on).

1.2.2 The phenomenon of disinformation becomes crucial in the wake of the 'digital revolution' that began in 1980 and continues to this day[8]. Ulrich Sieber refers to the world-wide changes that take place at the dawn of the above revolution, underlining that information has been considered since then as an autonomous good, as an autonomous value[9]. In any case, in addition to the criminologists who approach the phenomenon, mainly interested in the correlations of new technological achievements with the modifications-changes occurring in the field of deviant / criminal behaviors[10], the analysis by communication specialists places disinformation in the wider context of so-called **information disorder[11]**.

---

[7] According to *Jacob Farsedakis*, "crime prevention" means all the strategies, programs and measures that we can design and apply in order to prevent the commission of crimes. Always in the context of an enlightened anti-crime policy. See *Jacob Farsedakis,* Crime prevention as anti-crime policy expedient (url: https://bit.ly/2rRWBYu, accessed 22.12.2018). The Council of Europe defines anti-crime policy as "all measures aimed at protecting society from crime, paying attention to the future development of the criminal and safeguarding the rights of the victim". See Conseil de l'Europe, La participation du public a la politique criminelle. Strasbourg, 1984, as mentioned in *A. Tsitoura*, Relations between anti- crime policy and criminological research at *N. Kourakis* (Ed.) Anti-Crime Policy. Twenty-six studies on its theoretical issues and failures in its implementation, Penal 42, Sakkoulas, Athens-Komotini, 1994, p. 63.

[8] The term "digital revolution" (in line with the terms "industrial revolution" and "rural revolution") means the transition from analog-mechanical electrical technology in digital technology as well as the upgrades brought about by information technology and technology of communications during the second half of the 20th century. The Digital Revolution also marked the beginning of the Information Age.

[9] See *Ulrich Sieber*, Legal Aspects of Computer-Related Crime in the Information Society, European Comission, 1998, p. 192. For this transition to the information society, to which Ulrich Sieber refers, Jean-François Lyotard, a major French philosopher of the twentieth century, states (in the late 1960s) that *"It is conceivable that the nation-states will one day fight for control information, just as they battled in the past for control over territory, and afterwards for control of access to and exploitation of raw materials and cheap labor. A new field is opened for industrial and commercial strategies on the one hand, and political and military strategies on the other".* See *Jean-François Lyotard*, The Postmodern Condition: A Report on Knowledge, Manchester University Press, 1984, p. 5

[10] See, for example, the relation between culture and crime techniques, which was criticized and analyzed by Dario Melossi [Dario Melossi, "The Social Theory and Changing Representations of the Criminal "by A. Koukoutsaki (ed.), Images of Crime, Pletron, 2000, p. 21].

[11] This category includes various phenomena such as mis-, dis and malinformation, but everything else adds to the dissatisfaction and distrust of the public towards the traditional media or online

1.2.3 Therefore, the critical importance of disinformation and the need for an effective inhibition derive directly from the immense importance that societies have given to information (in one word from the "computerization" of societies, according to Lyotard[12]).

1.3 True, over the years, the critical infrastructures of societies –societies that have been running since the 1950s and 1960s with the basic aim of optimizing the acquisition, storage, processing, valuation, transfer and dissemination of information– have become increasingly more complicated and interconnected, thanks to the advent of the digital age (internet[13], new forms of energy[14] and other digital media), which constitutes as a sweeping technological restructuring. The government, the military, the police, the health system, the educational institutions, the banks, the stock market, the various non-governmental organizations and private individuals depend on the digital technology they use, in order not only to function better than the their competitors, but generally to operate. In the criminological literature, this situation has been portrayed with the term digital infrastructures of modern societies[15].

1.4 *David S. Wall*, also refers to the term "digital convergence", in other words to the capacity of different technological devices (such as the telephone, television and personal computers), to offer similar types of services[16]. The above mentioned point of view should not escape our attention, as it is a crucial observation for the issue

information platforms such as propaganda, hate speech, sloppy journalism etc. See. *David Goldberg*, Responding to "Fake News": Is there an alternative to law and regulation?, p. 417, (url: https://www.swlaw.edu/sites/default/files/2018-05/417%20Goldberg.pdf, accessed 15.12.2018). See also the report of the Council of Europe which has the title ''Information Disorder'' (url: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c, accessed 27.12.2018).

[12] See *Jean-François Lyotard,* The Postmodern Condition: A Report on Knowledge, Manchester University Press, 1984, p. 7.

[13] The most fundamental element of the internet is undoubtedly the radical relativisation of space-time distances. See *A. Afuah & C.L. Tucci*, Internet business models and strategies (2nd ed.). New York, NY: McGraw-Hill, 2003, where the universality of the Internet and how it simultaneously leads to the spatiotemporal magnification and shrinkage of the world, are discussed.

[14] See also the concept of the Third Industrial Revolution at url: https://goo.gl/J5HMJ4, accessed 22.12.2018

[15] See *Bart Simon*, The Return of Panopticism: Supervision, Subjection and the New Surveillance, 2005, p. 1.

[16] See. *David S. Wall*, Hunting, Shooting and Phising: New Cybercrime Challenges for CyberCanadians In The 21st Century, The British Library, 2008, p. 6.

which we are concerned with: the capacity of the Internet to be an equally available information provider (which even prevails in immediacy and usability) leads to a partial break with established / traditional ways of information. First and foremost, new generations (though not only them) prefer to be informed from online sources, relying exclusively on mobile devices (and notifications they receive there), social media, etc..[17], while traditional journalism in mass media or scientific articles are gradually abandoned. Beyond the age variable, it has been empirically observed that "top-down" information is preferred mostly in developed and developing countries of Africa, Middle East and Latin America – moreover, this preference is manifested more intensely in periods of (mainly) economic-political crisis[18].

1.4 Nevertheless, digital technology has also been an appropriate instrument and an enabling environment for committing crimes (criminologists are familiar with the term "dual-use problem"[19]). Indeed, many scholars state that the use of information systems by criminals is perhaps the most important challenge faced by information societies[20]. Grabosky argues that there is a lasting struggle between official structures and perpetrators for the technological innovations[21].

1.5.1 Thus, the prevention procedures must take into account the parameters that arise from the criminal / deviating use of new technologies and the internet, in

[17] See *Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, Huan Liu*, Fake News Detection on Social Media: A Data Mining Perspective, url: https://arxiv.org/pdf/1708.01967.pdf (accessed 19.07.2018).

[18] See *Darrell M. West*, How to combat fake news and disinformation, 2017 (url: https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/, accessed στις 16.12.2018).

[19] It would be unrealistic to think that we can only reap the "good" fruits of technology, bypassing what some scholars like Neal Katyal call the dual-use problem, that is, as far an achievement, a technological development , an innovation, etc. is concerned both "positive" and "negative" uses are unavoidable (see *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center, 2000, p. 5).

[20] See *M. Kaiafa-Gbandi*, Penal Law and Abuses of Informatics, Armenopoulos Publishing, 2007, p. 1059 et seq. *Michael Tsagkatakis* notes that global economic forum included cybercrime among the 10 major threats to our planet and that the UN, the European Union, the Council of Europe, the G8 and the G20, NATO and its counterparts in Asia and Africa, undertook institutional initiatives (Treaty of Budapest, etc.), have make use of preventive and repressive mechanisms (Interpol, Eurojust, EUROPOL, Certs, IC3, EGC), have encourage private initiatives, centres of excellence (EC3, CCDCOE κλπ), research bodies, have promote synergies, education and training (See *Michael Tsagkatakis*, Computer Crime, Hellenic Center for Excellence in Combating Cybercrime, version 0.95, 2015, p. 2).

[21] See *P.N. Grabosky,* Crime and Technology in The Global Village, Paper presented at the conference: Internet Crime held in Melbourne, 1998, p. 6.

general. More specifically, regarding disinformation, it is also necessary to investigate whether its transfer to a digital environment is merely a qualitative change / change of framework or accompanied by quantitative variations / intensive differences, so that we can say that the growing demand for "fake news" may be a by-product of the fastest news cycles and short-cut posts (features of social media, along with dealing with news production as if it were a business matter and not a public function). Additionally, the use of Bots in spreading fake news makes unclear whether the behavior should be classified into a genuine Internet crime or a traditional crime [22], for which only possibilities for new and most convenient means of accomplishment were opened.

1.5.2 When digital technology started, particularly computer technology, the perpetrators were easier to identify for the simple reason that the high cost of acquiring this technology allowed a very narrow circle of people and specific companies to use it. However, today access to technology is much easier for everyone, which leads to the plurality of potential perpetrators (perpetrators who even enjoy the advantage of anonymity[23]) and therefore the work of any social control is hampered[24]. Also, the effects of these acts are simultaneously affect many targets irrespective of territorial limitation - in addition, such crimes are theorized as "crimes without homeland", due to their cross-border nature which

[22] *Ioannis Aggelis* distinguishes computer crimes as follows:
(a) crimes committed both in a common environment and on the Internet, e.g. slanderous defamation, the copying of a spiritual work, e.g. musical song (Article 66 of Law 2121/1993) or a computer program, pornography of minors, etc. When this crime is committed on the Internet, then is a crime related to cyberspace, or facilitated by the cyberspace (internet related crime).
(b) crimes committed only in a computer environment (that is without the use of the internet), e.g. the crimes referred to in Article 370c (1) PC, such as copying a program from a floppy disc or CD-ROM or from a computer, without the right to do so.
c) Genuine cybercrime or network crimes in the sense of criminalizing cyber-related behavior, e.g. illegal access to a computer (hacking).
(Ioannis Aggelis, The Council of Europe' s Convention on Cybercrime to be Adopted: Its Relationship with the Greek Legal Order, Legal Review, Issue 30).
See *F. Spiropoulos,* Without right access to electronic information systems, Penal no. 86. Sakkoulas, 2016, footnote 3.

[23] See *Sara M. Smyth*, Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada, 2007, p. 61

[24] Βλ. *Rob D 'Ovidio*, The Evolution of Computers and Crime: Complicating Security Practice, Security Journal, 2007, σελ. 46

is not limited to geographical boundaries[25]. Also, as the cost of participation in the crime, the cost of committing it and the risk of getting caught [26] [27] (taking into account the difficulty in collecting 'electronic evidence' [28]) of the perpetrator is small, cybercrime can deliver large profits [at a cost-benefit analysis level (rational choice [29])] - therefore the digital environment is much more attractive[30]. In addition, the recording of cybercriminality does not correspond to reality, as very few cases are reported internationally[31], with immediate consequence that is much less visible than

[25] *K. Vishnu Konoorayar*, Regulating Cyberspace: The Emerging Problems and Challenges, Cochin University Law Review, 2003, p. 414

[26] The identification of a digital criminal, as a rule, is very difficult (though not impossible), just like his (actual) place of execution, and that is because the perpetrator can be traced to a specific place, the evidence, however, are located in a different and remote country or are located at the same time in many different countries. Even more difficult is the case of the disinformation we are concerned with, the wide spread of which the so-called "bots" are responsible, namely information systems affected by malicious software that can be used for mass attacks or in this case for reproduction and dispersal of (false) information from the person who handles the specific system's capabilities (See this analysis at url: https://privacy.ellak.gr/2017/04/11/botnets-i-strati-ipologiston-zompi-pou-apoferoun-ekatommiria/, accessed 01.01.2019). See *Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini,* "The Rise of Social Bots," Communications of the ACM, July, 2016 and *Chengcheng Shao, Giovanni Luca Ciampaglia, Onur Varol,*
Alessandro Flammini, and Filippo Menczer, The spread of fake news by social bots (url: https://andyblackassociates.co.uk/wp-content/uploads/2015/06/fakenewsbots.pdf, accessed 9.12.2018).

[27] Encryption appears to be so effective that it is used on the Internet even to commit illegal acts, which must be kept secret both by the common view and by the authorities. See, for example, the detailed article-report by *K. Deligiannis*, The World of Dark Internet, KATHIMERINI newspaper, May 4, 2014, p. 29, which explains and analyzes the concept of "Darknet". In particular, darknet is a network of servers that are based on encryption technologies to exchange data by camouflaging and hiding electronic traces and is accessible only to users who have installed a similar mechanism on their device (recently the " darknet "acquired its own search engine called "Grams"). Darknet is mainly used for illegal activities and transactions.

[28] There is a difficulty in collecting the so-called "electronic evidence", that is, the appropriate evidence found in computer systems and are necessary for detecting electronic crimes, as these elements can be hidden, encrypted, loaded with viruses and possibly scattered anywhere in the world. See. *Marc. M. Goodman*, "Why The Police Don't Care About Computer Crime", Harvard Journal of law and Technology, 1997, p. 483, *Marie-Helen Maras Jones*, Computer Forensics: Cybercriminals, Laws, and Evidence 2nd Edition, Bartlett Learning, 2014 and *Eoghan Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Academic Press; 3rd edition, 2011, pp. 7-14

[29] For an analysis of theory of rational choice see *M. Galanou*, On the Economic Analysis of the Criminal Justice System, Criminal Justice 1/2008, pp. 81-82. and *K.D. Spinelli*, Criminology - Contemporary and Older Directions, Sakkoulas, Athens - Komotini, 2005, 2nd ed., pp. 177-178.

[30] *Neal Kumar Katyal*, Criminal Law in Cyberspace, Georgetown University Law Center, 2000, p. 4

[31] It is estimated that only 15% is reported to the Authorities, see Iak. *Farsidakis*, Cybercrime and its treatment (url: https://criminology.panteion.gr/attachments/article/386/j%20farsedakis%20%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CF%87%CF%8E%CF%81%CE%BFs.pdf, accessed 24.12.2018).

the crime in the natural world. In addition, the number of victims - but also the extent of victimization - compared to traditional ways of committing crimes is much larger[32].

1.5.3 With regard to jurisdiction issues, there are problems of either positive jurisdiction, a case claimed by more than one State, or of negative jurisdiction in the sense that no State claims jurisdiction over the case in question[33]. Bearing in mind that for the most part, investigation of online crime, demands cooperation[34] of at least two states (the state where the crime is externalized and the state where the evidence is stored), things are even more complicated because state co-operation is a difficult task, since we are always struggling with the contradiction between the absence of international consensus[35] about what constitutes criminal behavior and the simultaneous presence of a multitude of different definitions. We are, therefore, facing a dichotomy between the globalization of electronic crime - which may impose not only the gradual homogeneity of law at international level (universal law, jus commune, etc.) but also modification of the way we perceive the legal order, as *Mireille Delmas-Marty* stresses[36]- and the territoriality of domestic legislation[37].

1.6 Finally, the idea of an effective, once and for all "victorious" as well as unimpeded prevention is, in our opinion, illusory because any solution is burdened with new problems[38]. More specifically, when we are talking about policies and practices of dealing with criminality, it is advisable to take into account the criminals' adaptation to new circumstances. Russell G. Smith, Nicholas Wolanin and Glenn

[32] Digital crimes differ from traditional as follows: a) They are usually commited from a remote location, b) The identification of the digital criminal is technologically complex, c) They are very profitable and at the same time the risk of getting caught is minimized, d) the number of the victims compared to that of traditional crimes is larger, e) the financial losses of 'digital' victims are much higher than those of the victims of traditional crimes and f) for the most part they are not recorded by any official body, ie. their "dark number" is of great importance – See *Xristos Tsouramanis*, Digital Criminality. The (in)secure aspect of the Internet, Katsaros, Athens, 2005, pp. 7-8.

[33] See *Susan W. Brenner & Bert-Jaap Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, 2004, p. 3

[34] See *N. Parisi & D. Rinoldi*, Recent Evolutions in the Fight against Corruption in the International Trade Law, Le droit des affaires internationales, 2004, p.1

[35] See *Andra Terbea*, The Internal Market for Gambling Services and The Need for A Cleaner Proportionality Test, Master Programme In European Business Law, Spring 2010, p. 43.

[36] See *M. Delmas – Marty*, Modèles et mouvements de politique criminelle, FeniXX réédition numérique (Economica), 1982

[37] See for example *Fausto Pocar*, New Challenges for International Rule Against Cyber-Crime, Kluwer Academic Publishers, Netherland, 2004, p. 28.

[38] See. *Helmut Wilke*, Introduction to System's Theory, Kritiki, 1997, pp. 111, 119 and 130.

Worthington notice that there are six cases of crime displacement, that is criminal activities are shifting as a consequence of the application of crime prevention efforts[39] (spatio-temporal displacements, displacement referring to the modus operandi, displacement of the perpetrators of the offenses, displacement at the types of crimes, displacement of the targets)[40]. At the same time, the scope of the anti-crime policy and the methods-techniques of scientific research that the first is employing, as well as the practices of prevention, is also determined externally by the principles of democracy and human rights[41], as well as by the sphere of economy and by the further uninterrupted development of technology[42]. Regarding the anticipated interaction between science and anti-crime policy, we argue that scientific discourse is a source of anti-crime policy[43]. Indeed, includes proposals for the role and objectives of criminal justice system[44] as far as tackling crime is concerned. However, it should also maintains a safety distance from the system (avoiding adopting, without questioning, its rationale), supporting the system's self-reflection. As a result, a further impediment worth mentioning is also the partial incompatibility that arises between criminological research and its implementation by the state[45].

[39] *Soumyo D. Moitra* proposed a model of an anti-crime policy simulator which allows us to observe how criminality will be affected if it is subject to certain anti-crime and security measures (See *Soumyo D. Moitra,* Developing Policies for Cybercrime, European Journal of Crime, Criminal Law and Criminal Justice, Netherlands, 2005, pp. 458-459.) It is also worth mentioning that there is a direction in criminology called *digital or computational criminology,* which uses computer science and applied mathematics' methods and expertise in order to help to the understanding of complex criminal phenomena and to suggest solutions to related problems (for example production of software for cybercrime prevention, identifying and detecting hackers etc.). See *Richard Berk*, Algorithmic Criminology, Department of Statistics Department of Criminology University of Pennsylvania, 2012, pp. 1-3.

[40] See *Russell Smith, Nicolas Wolanin & Glenn Worthington,* e-crime solutions and crime displacement, (url: https://aic.gov.au/publications/tandi/tandi243, accessed 24.12.2018). For example, using credit cards as a measure to avoid cash theft has led to new criminal opportunities by theft of electronic credit card data. Therefore, it is preferable to think of the anti-crime policy as a process of feedback rather than as the rapporteur of definitive solutions-responses.

[41] See for example *Jacob Farsedakis,* Criminology and Human Rights, in Penal Sciences: theory and practice. Tribute to Anna Benaki-Psarouda, Sakkoulas, Athens-Komotin*i,*2008, pp. 1441-1448

[42] See *Mathieu Deflem*, Technology and the Internationalization of Policing: A Comparative Historical Perspective, Justice Quarterly 19(3), 2002, p. 454

[43] See an extensive analysis at *St. Alexiadis*, Criminology, p. 277 et seq.

[44] Regarding the analysis of the criminal justice system, see *K.D. Spinelli*, Study on Criminal Justice System, Sakkoulas, Athens - Komotini, 2007.

[45] See A. Tsitoura, "Relations between Anti-crime Policy and Criminological Research" at N. Kourakis (ed.) Anti-crime Policy. Twenty-one studies on its theoretical issues and failures in its implementation, Sakkoulas, Athens-Komotini, 1994, pp. 65-66.

Efforts to categorize all preventive measures have resulted in different typologies, depending on the classification criteria, in particular based either on the geographical distribution of the measures or on their short or long-term effect, or on whether the measures concern a particular issue to be settled or can be widely extended[46], as well as on accountable parties, on who would be the agent that takes the necessary preventive action, depending on whether the measures are focused solely on disinformation or are directed towards the general public's mistrust towards the media, on whether the solutions are legislative or not, on whether the arrangements are externally imposed or result from self-regulation and so on. Taking this into consideration, from the point of view of criminology and jurisprudence, we examine the issue of (primary)[47] prevention in its general penal, situational and social form (in order to render the logic behind their application more visible).

2. Preventing online disinformation with penal provisions

2.1 According to the basic rationale of general penal prevention, its objectives are achieved when citizens refrain from committing crimes due to the fact that they are afraid of the punishment prescribed by the law but also given the pedagogical function that this law exercises on citizens[48], serving as a compass that shows them the right way to comply with the approved social rule[49]. Spreading fake news is treated as a criminal offense in several domestic laws[50].

[46] See *David Goldberg*, Responding to "Fake News": Is there an alternative to law and regulation?, p. 417, (url: https://www.swlaw.edu/sites/default/files/2018-05/417%20Goldberg.pdf, accessed 15.12.2018), *Daniel Funke*, A guide to anti-misinformation actions around the world (url: https://www.poynter.org/ifcn/anti-misinformation-actions/, accessed 14.12.2018) and *Gulizar Haciyakupoglu, Jennifer Yang Hui, V. S. Suguna, Dymples Leong, and Muhammad Faizal Bin Abdul Rahman*, Countering Fake News. A Survey of Recent Global Initiatives, S. Rajaratnam School of International Studies, 2018, σελ. 7 (url: https://www.rsis.edu.sg/wpcontent/uploads/2018/03/PR180307_Countering-Fake-News.pdf, accessed 01.01.2019).

[47] Primary prevention has as ultimate goal (direct or indirect) to weaken criminogenic factors and to prevent the occurrence of social situations and behaviors that are considered criminal. See, *G. Nikolopoulos*, The European Union as an Anti-crime Policy agent: The Hague Program and its Implementation, Athens, 2008, pp. 9-33

[48] For the dissuasive operation and the restrictive effects of (penal) law, see the in-depth analysis of *L. Kotsalis*, in Penal Dogma and Anti-crime Policy: Friction between them? to: Ant. Manganas (Ed..), Honorary volume for Aliki Giatopoulou - Marangopoulou, Law Library, Athens, 2003, vol. I, p. 645 et seq.

[49] Penal prevention, that is, that we are trying to implement using the law as a means, is distinguished in general and specific. The specific penal prevention (for which the research data on the issue of disinformation is not sufficient, so we decided to avoid including it in this document) is addressed to

2.2.1 We will proceed to an indicative (and not exhaustive) reference to countries that have criminalized disinformation and we will discuss the weaknesses[51] of prevention through penal provisions via a variety of objections that have been expressed.

2.2.2 Countries where it was found that there is a legislative provision for the publication and spreading of fake news and disinformation [52], are the following: Greece[53], Cyprus[54], China[55], Uganda and Zimbabwe [56], Germany[57], Canada[58], Italy[59], France[60], Belarus[61], Egypt[62] and Kenya[63].

---

those who have already violated the law and its objectives are achieved or deemed to be achieved by the imposition and execution of a penalty in order for the perpetrators to improve themselves or to be neutralized, as well as not to re-offend. See *Jacob Farsedakis*, Crime prevention as anti-crime policy expedient (url: https://bit.ly/2rRWBYu, accessed 22.12.2018). For the concept of general penal prevention see indicatively *N. Androulaki,* Penal Law - General Part - Theory of Crime, Sakkoulas, Athens 2000, pp. 41 et seq. and *N. Kourakis*, Introduction to Penal Theory, Sakkoulas, Athens, 2000, p. 29 et seq. Furthermore, as far as general prevention and its relation to the effectiveness of penal laws is concerned see *Efi Lambropoulou*, Sociology of Penal Law and the Institutions of Criminal Justice, Sideris, Athens, 2012, p. 185 et seq.

[50] For the effectiveness of punishment in the prevention of crimes, see also the results of the research conducted by *A. Manganas, M. Zannis, St. Papamichail and G. Lazos*, Crimes, Punishment and Greek Public Opinion, Criminal Justice 8-9, 2002, p. 943 et seq.

[51] On the other hand, an interpretation of the possible ineffectiveness of penal laws can be found at *Efi Lambropoulou*, Sociology of Penal Law and the Institutions of Criminal Justice, Sideris, Athens, 2012, p. 179 et seq.

[52] The various terminological issues regarding the appropriateness of the use of the concepts of "fake news" and "disinformation or misinformaton" (some countries refer to the first term and others to the second) are important. The all-ecompassing capability of the second term is obvious as it can incorporate practices that go beyond anything that looks like "news" [e.g. rumors, forms of automated accounts used for Astroturfing (the deceptive practice of presenting an orchestrated marketing or public relations campaign in the guise of unsolicited comments from members of the public.), networks of false followers, constructed information mixed with events, targeted advertisements, videos, memes, practices that have to do with the dissemination not the production of the news, that is, with commenting, sharing, tweeting and re-tweeting, etc.]. So, a penal prevention policy that seeks to gradually harmonize domestic laws may need to go for the term misinformation/disinformation [which version of it will of course be preferred by the 2 (misinformation or disinformation) depends on the subjective substance that prevails, namely, the second version focuses exclusively on the behaviors that are intentional but the former is also susceptible to negligence). See also the High Level Expert Group's report, where the terms "disinformation" and "misinformation" are suggested (url: https://ec.europa.eu/digital-single-market/en/news/final-report-high-levelexpert-group-fake-news-and-online-disinformation, accessed 06.09.2018)].

[53] Article 191, Greece's Penal Code

[54] See Cyprus' Penal Code, Chapter. 154, article 50, titled: "Publication of fake news, etc". (url: http://www.cylaw.org/nomoi/enop/non-ind/0_154/full.html, accessed 26.12.2018).

[55] Βλ. https://www.poynter.org/news/guide-anti-misinformation-actions-around-world?fbclid=IwAR0nUeJaooXX3C2OjzDrBOFy5lbvU3Hqp57rJPoqx133Cs7xy1W4IezwANg, accessed 14.12.2018

[56] See *David Goldberg*, Responding to "Fake News": Is there an alternative to law and regulation?, p. 425 (url: https://www.swlaw.edu/sites/default/files/2018-05/417%20Goldberg.pdf, accessed 15.12.2018).

2.2.3 In spite of the essential differentiations in almost all points [regarding the objective and subjective substance, the time by which the crime is considered completed, the capability of the news to cause fear or concern to the public, the severity of the penalties, the fact that some provisions are up-to-date to apply to the Internet and information systems[64] and others are not, the accountable parties[65], etc.], the provisions converge on their purpose, that is to prevent the deterioration of public order or the public's confidence in the State and its organs. In short, it is commonly accepted that the perpetrator's actions affect (questiones) the regulatory capacity and authority of the state [66] in a specific area of social life [67]. However, it has been

[57] See Joe Miller, Germany Votes for 50m Euro Social Media Fines, BBC, 2017 (url: http://www.bbc.co.uk/news/technology-40444354, accessed 26.12.2018)

[58] Βλ. https://laws-lois.justice.gc.ca/eng/acts/c-46/section-181.html, προσπελάστηκε στις 26.12.2018

[59] See http://www.altalex.com/documents/news/2014/08/25/delle-contravvenzioni-di-polizia, accessed 26.12.2018

[60] Article 27 of the French law about press prohibits the dissemination of fake or falsified news [Ciara Nugent, France Is Voting on a Law Banning Fake News. Here's How it could Work, Time, Ιούνιος 2018 (url: http://time.com/5304611/france-fake-news-law-macron, accessed 10.08.2018)]. On 22 of December 2018 the President of the Republic of France adopted Law No. 2018-1202 and organic law no. 2018-1201 on the fight against information manipulation - the text in its original form can be found here url: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id&fbclid=IwAR1bXQ7K6gnVGUJN4SkTsfMFTX8BCyG-P123bLVmfWz8KXRShGEGmMttluw, (accessed στις 12.03.2019).

[61] See https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html, accessed 26.12.2018

[62] See https://www.wsj.com/articles/egypt-passes-law-to-regulate-media-as-president-sisi-consolidates-power-1531769232, accessed 26.12.2018

[63] See https://web.archive.org/web/20180720094920/http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/ComputerandCybercrimesBill_2017.pdf, accessed 26.12.2018

[64] The big challenge, as we have noted above, is to address the modern "epidemy" of disinformation, mainly through social networks. Spreading is facilitated by information systems and social media, since automated notification functions (and therefore extensive and rapid dispersal) of publications occur. For the problem of bots and botnets see *Stefan Wojcik, Solomon Messing, Aaron Smith, Lee Rainie & Paul Hitlin*, Bots in the Twittersphere An estimated two-thirds of tweeted links to popular websites are posted by automated accounts – not human beings, Pew Research Center Internet and Technology, 09.04.2018 (url: http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/, accessed 13.09.2018) and *Alexandra Samuel,* How bots took over twitter, Harvard Business Review, 19.06.2015, (url: https://hbr.org/2015/06/how-bots-took-over-twitter, accessed 13.09.2018).

[65] For example, individuals, technology companies, webmasters, administrators of social media groups, internet service providers, online advertisers, mass media, etc.

[66] In the United Kingdom, the data protection and security provisions of 2003, and in particular Article 127 (2), have a strong role to play in penalizing the dissemination of fake news, stating that: "A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he: (a) sends by means of a public electronic communications network, a message that he knows to be false, (b) causes such a message to be sent". The difficulty of grouping this provision along with the previous ones is obvious, since its deviation from the rest is of paramount importance, that is there is no explicit reference to public order.

adequately pointed out that they are similar in terms of the generality of their formulation (abstract risk)[68] and that is why the guarantee functioning of the law is at stake (however, very narrowly determined concept of risk, is not without problems – for example it will very soon become obsolete due to the leaps of technological change).

2.3 It is true that the provisions that are related to the prevention of disinformation are not standardized solely in criminal law. Typically, we can refer to journalists' codes of ethics[69] as well as consultation documents ("Green Papers"), which serve as a more general guide to navigation safety, such as the one published by the UK Government[70].

2.4 Moreover, within the framework of the Council of Europe, the right to freedom of expression – apart from the national laws of the members states and their constitutions – is vigorously protected by the Convention for the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights

[67] Perhaps this common assumption (which is not itself completely free of problems) can be a springboard for further equalizations (or at least could facilitate a global dialogue with interlocutors, states, transnational or supra-governmental structures, etc.).

[68] The prominence / suitability of the news to cause concern is dealt with in general and in abstract terms, whereas these provisions may have to define the act of disinformation based on a result of a particular risk, which would also justify the act's penalization.

[69] As far as prevention is concerned by law, this chapter could include (due to their regulatory texture but also given their pedagogical aspect) and "codes of journalistic ethics", although independent and beyond from legal obligations, as they include a set of principles and rules to guide the practice of journalism, adopted and implemented by professional organizations of journalists, possibly in cooperation with other subjects in the context of self-regulation of information media. The content of these texts refers to journalistic tasks whose ratio is to secure and promote, within limits, an objective journalistic practice that confirms the journal's "social role", contributing to the fulfillment of the right of citizens to valid information. Of course, firstly, they do not constitute penal provisions. Secondly, we have already seen that the internet user himself is capable of reproducing and disseminating fake news, mainly through social networks. See *Tiina Laitila*, Codes of Ethics in Europe, at Kaarle Nordensteng (edit), Reports on Media ethics in Europe, Tampere – University of Tampere, 1995, p. 23 επ., and *Pauli Juusela*, Journalistic codes of ethics in the CSCE countries, Tampere – University of Tampere, 1991.

[70] By linking the phenomenon of spreading fake news to the Internet and social media, the UK government has published the "Internet Safety Strategy" Green Paper which provides informative advice covering a wide range of issues and questions about safe web browsing. See Department for Digital, Culture, Media and Sport, Internet Safety Strategy – Green paper, UK, 2017 (url: https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper, accessed 31.12.2018)

(ECHR))[71]. According to article 10§2 conditions, restrictions or penalties for the exercise of this right are justified only when there is an urgent social need. The above suggestion and, more generally, respect for freedom of speech, does not seem to have been followed if one analyzes the current legislation of many states or the various bills proposed by several governments on the issue of disinformation. The main weakness of this form of prevention is eventually its susceptibility to possible abuses - there have often been governmental tactics that actually seek to control information flows and the censorship of dissidents and are much less aimed at ensuring social order[72]. Therefore, once again, the question arises of the factors that ultimately affect the legislator. As these factors vary (which is quite reasonable), the arising difficulty is the achievement of the homogeneity of terms to be used as elements of criminal provisions.

2.5.1 Disinformation impedes the right of the public to knowledge as well as the right of individuals to seek, receive and influence information and ideas of all kinds [73] while the experts, official institutions and the notion of objective facts are despised and de-legitimized - this undermines the ability of society to engage in rational dialogue. However, the (near) mechanical response of states to the problem with criminalization or further stricter penalties is not and should not be the only way to tackle disinformation. For this reason, the High Level Expert Group (HLEG) explicitly advises the European Commission to avoid simplistic solutions and underlines that all forms of censorship will be ineffective, while there is absolutely no incentive to enforce regulations[74].

[71] See the full text here: url: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer, accessed 23/07/2018.

[72] See for example *Mong Palatino*, "Philippine Senator Moves to Criminalize 'Fake News' – Could This Lead to Censorship?", Global Voices, 2017. Although penal provisions are tempting and seem very effective, the risk for investigative journalism, political confrontation, and scientific activity is enormous as the possibility of critical positions being silenced is left open. For example, in Egypt, a producer of Al-Jazeera was arrested for allegedly undermining state institutions and reporting fake news in order to spread chaos. This happened after the release of a documentary criticizing the Egyptian army (see Committee to Protect Journalists, "Egypt Arrests Al-Jazeera Producer on Fake News Charge," 2016).

[73] See Organization for Security and Co-operation in Europe, "Joint declaration on freedom of expression and "fake news", disinformation and propaganda" (url: https://www.osce.org/fom/302796, accessed 24/07/2018).

[74] See High Level Expert Group (HLEG) https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation. The adoption of the critical stance is accompanied by the re-testing of all self-evident truths. Therefore, we should not a priori

2.5.2 Yet another possible (and mostly unexpected) negative impact of penal prevention is said to be the "Streisand effect", according to which prohibited / censored content attracts more than usual the attention of the public[75]. In China[76] for example, a more aggressive censorship policy on social networking media that disputes the dominant narrative has reinforced some people's belief that the truth lies in alternative sources of information, while traditional media (newspapers, television, etc.) broadcast propaganda. Moreover, the legislation that renders social networking companies or website administrators and so on accountable parties, often results in the limitation of uninterruptible communication, interaction and navigation of individuals. Accountable parties stepping up their scrutiny action are willing to "over-censor"[77] - are constantly alerted so they can delete in time [78] any posts, in order to evade sanctions.

3. Criminological Reflections on Preventing Online Disinformation

In addition to penal prevention, prevention at the crimonological level can be divided into two types: situational and social prevention. Situational is the prevention applied

approve or reject any proposed measure, nor we can assume that any measure, even if it is necessary, is also sufficient by itself. In short, more time and more detailed research is needed before the States conclude.

[75] For Streisand effect see an article at "The economist" published in 16.04.2013 with the title "What is the Streisand effect?", url: https://www.economist.com/the-economist-explains/2013/04/15/what-is-the-streisand-effect (accessed 05.04.2019).

[76] See *Jing Zeng, Chung-Hong Chan, King-Wah Fu and David Sutcliffe*, "Censorship or rumour management? How Weibo constructs "truth" around crisis events," The Policy and Internet blog, October 03, 2017

[77] See *Courtney C. Radsch*, "Proposed German Legislation Threatens Broad Internet Censorship," Committee to Protect Journalists, 2017

[78] See for example the Netzwerkdurchsetzungsgesetz (Social Network Enforcement Law) in Germany at *Joe Miller*, Germany Votes for 50m Euro Social Media Fines, BBC, 2017 (url: http://www.bbc.co.uk/news/technology-40444354, accessed 28.12.2018), where we read that: "From October, Facebook, YouTube, and other sites with more than two million users in Germany must take down posts containing hate speech or other criminal material within 24 hours. Content that is not obviously unlawful must be assessed within seven days. The new law is one of the toughest of its kind in the world. Failure to comply will result in a 5m euro penalty, which could rise to 50m euros depending on the severity of the offence". It has been noted that other countries, less democratic, rely on this law but also on similar perilous perceptions, in order to legitimize the suppression of the free press [see *Emma Lux*, Efforts to Curb Fraudulent News Have Repercussions Around the Globe, REPORTERS COMMITTEE, 2017 (url: https://www.rcfp.org/browse-media-lawresources/news/efforts-curb-fraudulent-news-have-repercussions-around-globe, accessed 28.12.2018)]. Instead, a well-time warning is not by default 'censorship' as the final decision is taken by the users. For example, many platforms paste the "disputed news" label into posts with unreliable / inaccurate content without deleting it.

by taking a series of technical and organizational measures[79], which attempt to block the achievement of the goals of those who are preparing to commit crimes[80]. Despite their temporary nature, these measures deal with the problem faster as they override the time-consuming bureaucratic procedures, present at other forms of prevention [81]. The role of social prevention, of course, is, as we shall see below, rather decisive [82], as its measures are primarily targeted [83] in reducing criminogenic factors that lead to criminal behavior and facilitate it. In any case, at this level and contrary to penal provisions, the perception of state exclusivity in the domain of prevention is affected and procedures of social control are diffused into a variety of regulatory fields. Besides, the primary element of social control is the variety of its modes[84].

3.1 Situational Prevention

3.1.1 The theoretical justification of this form of prevention is provided by the criminological theory of "routine activity theory", which was first introduced by

[79] Generally, in the context of information security, industries have developed several programs and sophisticated techniques such as antivirus and antispam, firewalls, updates of the operating system, automated intrusion detection systems, biometric applications, cryptography etc. (see. *D. Denning*, Information Warfare and Security, Boston: Addison Wesley, 1999). In any case, security measures do not by themselves ensure a drastic reduction in the risk of victimization, so they must be accompanied by the proper use and operation of the devices and the internet. Therefore, the other criminological prevention strategy (social) is also crucial at this point.

[80] See. *R. Clarke*, Situational Crime Prevention: Successful Case Studies, Harrow and Heston, Albany, NY, 1992.

[81] The managerial tone of situational prevention of course directs criminology to evidence-based policy and initiative evaluation, in terms of their effectiveness in rapidly reducing crime, that is to say the minimization of the recorded incidents is primary, while the substantial impairment of the probability of the crime occurring is neglected (see *J. Shapland*, Reducing Crime: Implications for Criminology Present and Criminology's Futures, British Crimonology Conference: Selected Proceedings. Vol. 3, 2000, pp. 2-3). Hence, it is rightly argued that occasionally prevention is crypto-suppressive (see *A. Sykiotou*, "Preventive use of the Internet in the name of security and violations of privacy, and protection of personal data", at Symmeikta in honor of professor Petros Parras, titled Ongoing Public Law, Sakkoulas, 2012, pp. 987-1005).

[82] It is also worth mentioning Enrico Ferri's phrase: "the need for criminal justice will weaken to the point where social justice is implemented" [see *Enrico Ferri,* Causes of Criminal Behaviour, at *J. Muncie, E. McLaughlin and M. Langan* (ed.), Criminological Perspectives, London: Sage Publications, 1999, pp. 34-39].

[83] There are, however, the factors capable of holding a person out of committing the crime. The "game" of these two categories of factors, as Iacobos Farsedakis notes, determines the outcome. A properly oriented anti-crime policy must weaken the former and strengthen the latter (see I. Farsedakis, "The Alphabet of Criminology", at Honorary Volume of K. D. Spinelli, Sakkoulas, Athens-Komotini, 2010, pp. 401-413).

[84] See *A. V. Horwitz*, The logic of social control, Plenum Press, New York – London, 1990.

Lawrence E. Cohen and Marcus Felson, and claims that crime occurs when three elements converge: (1) a motivated offender, (2) a suitable target, and (3) the absence or the inadequacy of a capable guardian[85]. Of these three preconditions, it is argued that the one that needs to be emphasized the most is the third one, in order to create the appropriate guardians that make the efforts of the perpetrators difficult. Direct preventative control seems to be more complicated in the case of potential perpetrators, since we have to do with the subjective intake of the relation between man and the social environment, with the attitudes and personal views of individuals. As far as the second presupposition is concerned, which refers to the suitable target (for example an electronic computing system), it would be inconceivable that our protection should focus on the abolition of the use of technology in order to guard against possible violations and criminal behaviors – thus, it is preferable to weaken the third factor.

3.1.2 Therefore, an indicative presentation of preventive measures concerning disinformation is attempted below.

3.1.2.1 First of all, it is worth referring to the checking of facts, traditionally conducted by experts and analysts. The fact-checking is the act of checking the data of a non-imaginary text in order to determine the accuracy and correctness of the actual statements in this text. This can be done either before (ante hoc) or after (post hoc) publishing or spreading the text. Verification before spreading aims at removing errors and inaccuracies and then safely spreading or refusing publication if all criteria are not confirmed. Verification post-dissemination is usually followed by written reports of inaccuracies and sometimes visual metrics provided by the fact-checking organization[86]. Additionally, one can also find computational methods for automated[87] verification of the validity of a statement.

[85] For an in-depth analysis of these three elements see *Majid Yar*, The Novelty of "Cybercrime" - An Assessment in Light of Routine Activity Theory, European Journal of Criminology, Volume 2 (4): 407–427: 1477-3708, European Society of Criminology and SAGE Publications, London, Thousand Oaks CA, and New Delhi 2005.

[86] See https://en.wikipedia.org/wiki/Fact-checking#Organizations_and_individuals and https://en.wikipedia.org/wiki/Category:Fact-checking_websites, accessed 29.12.2018

[87] See *William Yang Wang*, Liar, Liar Pants on Fire. A New Benchmark Dataset for Fake News Detection, Computation and Language, 2017 and *Eugenio Tacchini, Gabriele Ballarin, Marco Della Vedova, Stefano Moret, and Luca de Alfaro,* Some Like It Hoax: Automated Fake News Detection in Social Networks, Human-Computer Interaction, 2017.

3.1.2.2 Furthermore, social media, for example Facebook [88], give instructions to their users in order to be aware of fake news.

3.1.2.3 Natural language processing tools have also been suggested[89], tools that analyze the content of the news and could inform the user about its content and quality before he takes any further actions to share it[90].

3.1.3 In these ways, efforts are being made to limit to a certain extent the fraudulent or non-fraudulent dispersion due to users' activities. However, as we have repeatedly pointed out, Bots-users are also responsible for the rapid news (whether true or fake) dispersion. An established way of tracking-detecting bots and botnets[91] is the analysis of the profile of users of social media and the messages they send through natural language processing algorithms and artificial intelligence algorithms. Similarly, analyzing the characteristics of a network[92] is the key ingredient for detecting a botnet, but also for tracking the dispersion of a viral news story, as well as determining who is responsible for it. For example, if we identify a set of users who send messages to each other and at the same time have similar profile and message attributes, then it is very likely that these users form a Bot network. For the analysis of network features, new database technologies are also applied, such as Graph Data Base, and have the advantage of processing a large amount of data more efficiently than other traditional relational databases[93] [94].

3.1.4 In order to tackle disinformation, other suggested measures aim at removing the anonymity that individuals enjoy while navigating the internet. Companies can do this via real-name registration, by requiring Internet users to provide their hosting platform with their real identity. So, users become accountable for what they publish or disseminate on the internet and are not covered behind fake names and accounts

[88] See. https://www.facebook.com/help/188118808357379, accessed στις 29.12.2018.
[89] See for example ClaimBuster, at https://idir-server2.uta.edu/claimbuster/, accessed 30.12.2018.
[90] See https://dl.acm.org/citation.cfm?id=2857153, accessed 29.12.2018.
[91] Botnet is the set of virtual-fake users who can send messages to each other. (see also the botnet definition above).
[92] See https://arxiv.org/abs/1804.10233 accessed 29.12.2018.
[93] See https://cambridge-intelligence.com/detecting-fake-news/, accessed 29.12.2018
[94] Two free-access tools that make good use of many of the technologies mentioned above are Hoaxy and Botometer. See https://hoaxy.iuni.iu.edu/ and https://botometer.iuni.iu.edu/#!/ respectively, accessed 29.12.2018.

when they make aggressive comments or engage in prohibited activities[95]. Something similar can also apply to managers - for example, a bill submitted to the Italian Senate in February 2017 required those wishing to open an online platform that would publish or disseminate information to the public to provide the name of the platform, its URL, the name and surname of the manager and its tax number[96].

3.1.5 Measures, which are based on the cooperation of public, organizations and governments, are the following:

3.1.5.1 At first, there is the practice of reporting, that is, through a smartphone application, the public can report fake news that they encounter or complain about misleading information[97].

3.1.5.2 Then, it is argued that it would be particularly helpful to integrate the practice of crowdsourcing, which is to use the skills and training of readers-listeners to detect potential flaws in news coverage.

3.1.5.3 Moreover, some approaches refer to the profitability of fake news due to advertising [98], as one of the most important causes of their rapid proliferation, so they suggest concentrating on thoroughly controlling ad placements as the most appropriate - immediate - response to the problem (already some social networking platforms like Facebook have made it difficult for users to try to render fake news profitable). Autoregulation in the field of digital advertising is imperative (among others) and the fact that the ad industry has a personal interest (brand-safety) to monitor its advertising networks, detecting and removing the advertisers that support fake news sites.[99].

---

[95] See *Zhixiong Liao*, An Economic Analysis on Internet Regulation in China and Proposals to Policy and Law Makers, International Journal of Technology Policy and Law, 2016.

[96] See *Francesca Fanucci*, "How Italy wants to slam fake news: Use fines and prisons," Media Power Monitor, 2017

[97] See *Shawn Lim*, Thailand Launches "Media Watch" App to Combat Fake News, The Drum, 2017. Reports in this case go straight to the Ministry of Public Health.

[98] In the digital age, the status of advertising is changing. The modern model is often based on the number of clicks related to impressive and extremely popular (viral) content. This model is based on ad networks that manage offices which ensure concurrent placement of advertisements based on algorithmic decision-making. This makes it easier to place ads on websites that publish appealing content (invocation of emotions, disinformation, and so on).

[99] This (rather ambitious) argument is set out here: *David Goldberg*, Responding to "Fake News": Is there an alternative to law and regulation?, p. 434-435 , (url: https://www.swlaw.edu/sites/default/files/2018-05/417%20Goldberg.pdf, accessed 12.2018).

3.1.6 Finally, situational prevention includes what is called an issue-focused approach[100], e.g. aims to tackle disinformation during the election period. In particular, the Communication from the Commission to the European Parliament and the Council entitled " Tackling online disinformation: a European Approach" states that "The spread of disinformation also affects political decision-making processes through distortion of public opinion"[101]. An example of the issue focused approach is the Ukrainian journalist organization StopFake, which is dedicated exclusively to the uncovering Kremlin's disinformation and propaganda. It also explores how other countries around the world are affected by these distortions[102]. These approaches are believed to facilitate the conceptualization of fake news due to their specific context and thus accelerate the identification of relevant fictitious information. Therefore, issue-focused approaches show better results than partial-isolated abstract efforts that have not been focused.

3.2. Social prevention

[100] For example, Facebook supported governments during the recent French and German elections (see *Josh Constine*, 11 ways Facebook tried to thwart election interference in Germany, TechCrunch, September 27, 2017 and *Eric Auchard and Joseph Menn*, Facebook cracks down on 30,000 fake accounts in France, Reuters, April 14, 2017). See also the task force practice at *Will Ziebell*, Australia forms task force to guard elections from cyber attacks, Reuters, 2018 (url: https://www.reuters.com/article/us-australia-security-elections/australia-forms-task-force-to-guard-elections-from-cyber-attacks-idUSKCN1J506D, accessed 30.12.2018).

[101] Page 2, url: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0236&from=EN, accessed 30.12.2018).

[102] See. https://www.stopfake.org/en/about-us/, accessed 30.12.2018.

3.2.1 The other prevention mode at the criminological level has a more social character and consists of proper education[103] and informing of citizens. Citizens, given that the human factor is crucial, being aware of the extent of the problem, i.e. the forms and dangers of disinformation, will first and foremost be better protected and more likely to report incidents of victimization (helping to minimize the dark number). In other words, they can participate in tackling the phenomenon[104] in a variety of ways, such as by helping to identify problematic and suspicious websites[105]. The desirable result, thanks in particular to active citizenship and the feedback given to the system, is the continuous monitoring of the problem and the constant re-evaluation / updating of the existing responses to it.

3.2.2.1 First of all, a renewed focus has been proposed on "media literacy" in schools[106], based on the joint action of educational institutions with journalists, entrepreneurs, non-profit organizations and other institutions and aims to foster the emotional self-management of students. Emphasis should be given to the ability to emotionally distance ourselves from the content we encounter in a variety of publications. Simple and understandable lessons related to the moves that need to be done before we express our liking or before we decide to share news, avoiding filter bubbles, understanding of the risks posed by exposure to information, are now necessary to be taken from an early age. Also, "media literacy" must provide (especially) children and young people[107] with the criteria for assessing the validity

[103] Many non-profit organizations such as Politifact, Factcheck org., StopFake, etc., in addition to their occasional operation regarding the verdict on validity of a story, also have a pedagogical mission. For example, StopFake provides guidance to its readers on how to verify whether a story is fake. It also features videos where experts debunk fake news, which are being shown on both the internet and on television. See https://www.stopfake.org/en/about-us/, accessed 30.12.2018.

[104] See *Anastasia Chalkia*, Viewpoints on participatory anti-crime policy in territories with criminality gradation, located in Athens, Criminology, 2004, p. 66.

[105] See *Louise I. Shelley*, Organized Crime, Terrorism and Cybercrime, in: Security Sector Reform: Institutions, Society and Good Governance, Alan Bryden/Philipp Fluri (eds.), Nomos Verlagsgesellschaft, 2003, Baden-Baden p. 310. The practice of reporting has been noted few pages above, as we included it into situational prevention. Here, of course, we focus on the educational background as a prerequisite for a more accurate implementation of the situational prevention proposals.

[106] Examples of countries where this measure has already entered into force are Canada, Italy and Taiwan (see *Gulizar Haciyakupoglu, Jennifer Yang Hui, V. S. Suguna, Dymples Leong, and Muhammad Faizal Bin Abdul Rahman*, Countering Fake News. A Survey of Recent Global Initiatives, S. Rajaratnam School of International Studies, 2018, p. 7 (url: https://www.rsis.edu.sg/wp-content/uploads/2018/03/PR180307_Countering-Fake-News.pdf, accessed 01.01.2019).

[107] It is estimated that world-wide, one in three internet users is under 18 years old and that young people from 12 to 15 years old spend more than twenty hours a week on the Internet. See

and the degree of bias of the sources, as well as the criteria for distinguishing the different types of journalism (for example investigative, propaganda, editorial etc.)[108]. In short, it provides guidelines for access to information but also for its analysis, evaluation and creation while enhancing the understanding of the role of the media in society as well as the basic research and self-expression skills necessary for citizens of a modern democracy[109].

3.2.2.2 It is a fact that there are enough educational methods to make this possible but a certain one deserves our attention: there are fake news board games, which facilitate the identification of fake news encountered by individuals on the Internet or in the mass media and lead to the significant reduction of their persuasiveness -something that seems scientifically valid[110]. Similar games are also available on initiatives that aim to counter fake news, such as stop fake bingo on the stop fake website[111].

3.2.3 Equally important (as an extension of the above) is the crystallization of social norms and mentalities-mindsets that contribute to avoiding the trap of disinformation. For example, it would be prudent and appropriate for individuals to gather (if possible) all (or several of) the opinions expressed on each issue that concerns them

---

https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf, accessed 15.12.2018.

[108] See *Darren G. Lilleker*, Evidence to the Culture, Media and Sport Committee 'Fake news' inquiry presented by members of the Centre for Politics & Media Research, Faculty for Media & Communication, Bournemouth University, UK (url: http://eprints.bournemouth.ac.uk/28610/3/Evidence%20Submission%20-%20Fake%20News%20FINAL.pdf, accessed 30.12.2018).

[109] See Center for Media Literacy, Media Literacy: A Definition and More (url: http://www.medialit.org/media-literacy-definition-and-more, accessed 01.01.2019), *Douglas Kellner*, Cultural Studies, Multiculturalism, and Media Culture (url: https://pages.gseis.ucla.edu/faculty/kellner/papers/SAGEcs.htm, accessed 01.01.2019) and National Literacy Trust, Commission on Fake News and the Teaching of Critical Literacy Skills in Schools (url: https://literacytrust.org.uk/policy-and-campaigns/all-party-parliamentary-group-literacy/fakenews/, accessed 01.01.2018).

[110] See *Jon Roozenbeek & Sander van der Linden,* The Fake News Game: Actively Inoculating Against the Risk of Misinformation, Manuscript accepted and in press at the Journal of Risk Research (url: https://www.cam.ac.uk/sites/www.cam.ac.uk/files/fakenews_latest_jrr_aaas.pdf, accessed 01.01.2019). Playing games of course, always had a socializing function according to many theorists (one of them is the highly influential American sociologist GH Mead), while a common misunderstanding is that game is opposed to seriousness, as the Dutch historian of culture Johan Huizinga is elaborately portrayed, in the first chapter of Homo Ludens, one of the most important studies ever written about games. See. *George Ritzer*, Theory of symbolic interactions at *Maria Petmezidou* (ed.) Contemporary Sociological Theory, volume 1, Crete University Press, pp. 245-246 and *Johan Huizinga*, Homo Ludens: Homo Ludens: A Study of the Play-Element in Culture, Angelico Press, 2016, respectively.

[111] See https://www.stopfake.org/content/uploads/2017/04/StopFake-Bingo.pdf, accessed 01.01.2019

instead of jumping to any rash conclusions, as well as to share information responsibly after first crossing - validating the authenticity of the source and the writer and after fully reading the news and not fragmentarily). This greatly increases the chances of formulating citizens capable of making mature and realistic estimations of who they ought to trust without running the risk of manipulation and deception at any time. Finally, it is a fundamental obligation of all bodies that characterize news as fake and censor them to provide evidence, arguments and justification – otherwise, there is no guarantee that this does not translate into obstructing the propagation of perceptions undermining their worldview - so that citizens too are getting used to think and evaluate in the same way.

3. Concluding Remarks

In summary, the questions arising from the preceding presentation of the diversity of responses to disinformation relate to country-by-country variations in both the application of the same preventive measure (for example, divergences in legislation) and the choice of the type of prevention (penal, situational, social) or even a combination of preventive measures. Although there is no consensus on which version of prevention responds to the problem more satisfactorily, the ultimate goal of all measures should undoubtedly be to mitigate the phenomenon without, however, violating any acquired freedoms or losing the privileges of the digital age. For this reason, it is advisable not to proceed to an exclusive choice of measure (e.g. laws, safety measures, educational campaigns or interdisciplinary researches, etc.) but to a combination of many measures[112].

[112] See, for example, the First Draft initiative, which sets up a non-profit coalition to combat disinformation (url: https://firstdraftnews.org/community-of-practice/, accessed 01.01.2019). The partners in the coalition are: technology companies (e.g. Google News Lab, Facebook and Twitter), academic and research institutes (e.g. University of Southern California Annenberg School of Communication and Journalism, Tufts Fletcher School and Public Data Lab), news agencies (e.g. The Washington Post, Reuters and The Guardian) and other similar organizations (e.g. FactCheck Initiative Japan and Now This). This initiative is dedicated to supporting journalists, academics and technicians working to address challenges related to trust, reliability and truth in the digital age. It includes a global verification and collaborative research network, it collaborates with its increasingly growing community to conduct innovative and experimental research projects, and it continually provides training (online and offline) oriented to the expansion and integration of best practices into news agencies and schools of journalism around the world. Focused on addressing the information disorder, First Draft is based on its pioneering work around elections in the US, France, the UK, Germany, Brazil and Nigeria. Finally, in 2019, it will support the development of sustainable,

In order to maintain an open, democratic system, the coordination of the actions of governments, technology companies, consumers and so on, is very crucial. Governments must promote media literacy and strengthen professional journalism in their countries. The news industry must provide high-quality journalism to regain public confidence. Technological enterprises need to invest in tools that detect fake news and help reduce the economic incentives of those who profit from disinformation. Educational institutions must incorporate media literacy into their curricula and give them high priority. Finally, individuals have to consult various sources in order to avoid unilateralism that lead to blind acceptance of falsehoods and above all to be (at least in the first instance) skeptic of things they hear or read.

collaborative efforts in Argentina, Australia, Canada, Indonesia, South Africa, Spain and Uruguay, as well as a cross-border plan to study on tactics and trends in disinformation in Europe.