THE FEATURES OF THE "AUTOMATED" DISINFORMATION ACTION OF THE MODERN ERA

Victor MORARU¹, Theofilos MAROUSIS²

¹PhD habil, Moldova State University, Chişinau, Republic of Moldova ²PhD student, Moldova State University, Chişinau, Republic of Moldova Corresponding author: Theofilos Marousis; e-mail: theofilos.ma@outlook.com

Abstract

Informational warfare has become an important part of any conflict on many levels, especially if these are military, political or economic. Propaganda has adapted to the new technological environment and has evolved into what we meet as computational propaganda (as one of its forms). In this paper, we focus on the role of digitized influence operations in the disinformation spreading process. We discuss how digital space can be influenced by bots, i.e. automation-human mimicking robots in social media, and how it contributes to the function of companies through advertising. We also discuss how platforms possibly without their intention, could potentially use cookies (as well as the algorithms) and through disinformation, increase the user's attention and engagement in order to harvest advertising profits. Finally, a very important issue is how these data from users could be used for behavioural targeting in political campaigns and voting events. Automation used for manipulative tactics urges the need to strengthen the measures against information falseness, in order to protect free decision-making and democratic values.

Keywords: disinformation, computational propaganda, opinion influence, bots.

1. INTRODUCTION

As we talk about fake news and propaganda (in its negative sense) we couldn't ignore a modern phenomenon of the Internet age. It is, that is, the circumstances in which propaganda and fake news, facilitated by the Internet, become attributes of a confrontation - information war. As C. Von Clausewitz said (we are referring to one of his most popular statements), war is thus "an act of force to compel our enemy to do our will" (Howard, & Paret, 1976). Information warfare is an important aspect of any conflict on many levels, especially if these are military, political or economic. Experts explain: "The war, after the second world conflict, evolved, turning into a total war, we could say in a type of war which, supported by the armed forces, systematically engages the civilian populations, urban territories, production areas and, in general, the entire economic process, propaganda, the psychic and moral energies of people who do not participates in armed confrontations, thus bringing with it an intensification of hostilities" (Fisichella, 2007). In the opinion of Prof. D. Stupples, today instead of military forces, states are increasingly launching non-lethal attacks against an enemy's information systems, thus we have Information Warfare (Stupples, 2015). The representatives of the military sphere believe that Information Warfare represents the use of political, diplomatic, economic and other nonmilitary measures in combination with the use of military forces (Gerasimov, 2016). The concept is known as "Gerasimov's Doctrine" (Bartles, 2016) and underlines the important role of nonmilitary means used to achieve political and strategic goals. Cyber warfare is nowadays part of informational warfare. NATO states that cyberwarfare may also involve so-called social cyber-attacks, by creating in people's minds a specific image of the world, consistent with the goals of the information warfare conducted by a given country (NATO, n.d.). As we understand, we may sometimes refer to information warfare in terms of military operations; however, it does not mean that we are talking only about military targets. G. Stein writes that information warfare, in its essence, is about ideas and epistemology, meaning that information warfare is about the way humans think and, more important, the way humans make decisions (Stein, 1995). We realize that one

cannot plan military operations without knowing what the adversary is planning. Military tactics were transferred to the political arena. The political opponent is treated as an enemy. They try to learn what the opponent is doing, and then it is up to the staff to plan their offense and wear them down. Conflict and information warfare can be at the level of states, but it can also be at the level of political parties within the same state. Each adversary may try to direct the flow of information to his advantage. We are essentially talking about influence operations.

2. COMPUTATIONAL PROPAGANDA. A STYLE OF OUR AGE

The phenomenon of computational propaganda has recently attracted the attention of several authors, involved in identifying its defining features. D. Arnaudo et al. (Arnaudo et al., 2021) write that Information Manipulation is a set of tactics involving the collection and dissemination of information in order to influence or disrupt democratic decision-making. Propaganda has adapted to the new digital environment, uses new technologies and has evolved into what we meet as computational propaganda. S. Woolley & Ph. Howard (Woolley & Howard, 2017) define that computational propaganda involves the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks. R. DiResta (Diresta, 2018) says that computational propaganda is a suite of tools or tactics used in modern disinformation campaigns that take place online and these include automated social media accounts that spread the message and the algorithmic gaming of social media platforms to disseminate it. Those automated social media accounts are known as "bots." Those bots serve exactly the purpose of mimicking human behaviour and spreading misinformation across real-human social media interactions. S. Woolley & P. Howard say that political bots "are also used for more malicious activities" (Woolley, & Howard, 2017), like political manipulation. They are effective tools for strengthening online propaganda and hate campaigns and are associated with spamming and harassment. The penetration of bots, i.e. automation-human mimicking robots in social media is so great that it has an influence on public opinion and forces technological giants (Facebook, Twitter) to take measures in order to limit them. According to European Parliament (Europarliament, 2018), responding to growing concern about the impact of disinformation bots, Twitter suspended up to 70 million accounts between May and June 2018 and Facebook removed 583 million fake accounts in the first quarter of 2018 in an attempt to combat false news. The existence of bots in social media is so massive, they now make up a respectable part of the percentage of posts. A typical example is the fact that in the 2016 presidential election in the United States, 20% of all political tweets originated from accounts that were likely to be bots, according to A. Bessi & E. Ferrara (Bessi & Ferrara, 2016). According to C. Shao, G. Ciampaglia et al. (Shao et al., 2018) bots are characterized as "super spreaders" of misinformation, because they act in different ways. According to their research, bots may play a critical role in driving the viral spread of content from low-credibility sources, they can mention influential users in tweets that link to low-credibility content, they can retweet articles within seconds and if anything of that is reposted from other verified users, then it increases its credibility and seems real news. Bessi & Ferrara (Bessi & Ferrara, 2016) report that social bots in online political discussion can create three tangible issues: a) influence can be redistributed across suspicious accounts that may be operated with malicious purposes, b) the political conversation can become further polarized, c) the spreading of misinformation and unverified information can be enhanced. The main role of bots is to reproduce specific news or words that serve their own ideological side. They try to "trend" these news or keywords so that more people will see them through their social media feed and thus increase the chances of influencing public opinion. F. Schafer writes that the aim of computational propaganda strategy is to manipulate public opinion by creating trending topics through pushing certain hashtags or highjacking existing ones (Schafer, 2022). Of course, computational propaganda is not done only by bots and the algorithms they use. It is also done by real people who use either their own or

fake profiles on social media, in order to publish memes against their ideological opponents, use hate speech, threaten, accuse or do character assassination. These are the so-called Internet trolls. Marwick & Lewis state that the concept of troll described those who deliberately baited people to elicit an emotional response, but in recent years the term is characterized by the use of deliberately offensive speech, antipathy toward sensationalism in the mainstream media, the desire to create emotional impact in targets and the preservation of ambiguity (Marwick & Lewis, 2017). European Parliament (Europarliament, 2018) refers trolls as human online agents, sometimes sponsored by state actors to harass other users or post divisive content to spark controversies. Bradshaw & Howard (Bradshaw & Howard, 2017) also refer to them as "cyber troops" because they function like an online party army whose goal is to destroy the opponent through negative propaganda. They also report that government-based cyber troops are public servants tasked with influencing public opinion (Bradshaw & Howard, 2017). In other cases, they may also operate as private contractors or volunteers. N. Monaco & C. Nyst say that statesponsored trolling attacks represent "an innovative manipulation of new technologies" and they try to seed distrust in mainstream media and turn public opinion against journalists and activists (Monaco, 2018). In any case, trolls along with bots use social media posts, likes, retweets, reports, comments, memes etc., and create Internet trends with the aim of influencing public opinion. To what extent they succeed in this we cannot say with precision. However, the intensity with which they "shoot" social media certainly plays more or less a role in their success rate.

3. THE ROLE OF TECHNOLOGY AND ARTIFICIAL INTELLIGENCE AS A "PLAYMAKER" OF DISINFORMATION DISSEMINATION TODAY

Technology and automation play an important role today in supporting and operating the Internet and social media. But if used in a suitable way, it can also work beneficially for misinformation to spread. As we saw earlier, bots are a useful link in the computational propaganda process. The company Norton (Norton, 2018), which deals with cyber security and the creation of antivirus systems, provides some useful information about bots (or web crawlers) and explains that there are two kinds: the good bots, that gather information or make automatic interactions and secondly, the bad bots, that contain malware and infect its host, sending information back to a central server (gather passwords, log keystrokes, launch DoS attacks etc). But there is a differentiation here. In social media it is possible to meet a good bot (gathers info and interacts with others) but with bad intentions (spread propaganda). So, in terms of political communication we could say that we have a bad bot. It depends on the intentions of the administrator of bots and the purposes he wants to use them for. Accordingly, Roth (Head of Safety and Integrity of Twitter) and Pickles (Director, Global Public Policy & Development of Twitter) talk about manipulative tactics and describe what they try to prevent in their platform:

- Malicious use of automation to undermine and disrupt the public conversation, like trying to get something to trend
- Artificial amplification of conversations on Twitter, including through creating multiple or overlapping accounts
- Generating, soliciting, or purchasing fake engagements
- Engaging in bulk or aggressive tweeting, engaging, or following
- Using hashtags in a spammy way (Roth & Pickles, 2020)

Boshmaf et al. (Boshmaf et al., 2013) calls them "social bots" because they mimic human behaviour in social platforms by interacting with other users (through comments, likes etc.), using Artificial Intelligence (AI). Their aim is to disguise as real people and to reach "influencial position" in the platforms, thus have an effect on public opinion. Salge & Berente (Salge & Berente, 2017) characterize social bots in terms of deceitfulness and unethicality, because they violate the prima facie duty of fidelity, spread fake news, spamming and limit free speech. Experts have established certain strategies that bots use to spread fake news (Shao et al., 2018). They say that firstly, bots promote fake news in the early stage, before it goes viral, secondly, they aim to direct them to influencers, using replies and mentions and thirdly, they try to conceal their geographic location. Suarez-Serrato et al. in their research about online protests (Suarez-Serrato et al., 2016), talk about "cyborg" accounts that combine automation and human intervention and may play a role in suppression of communication. M. Stella et al. report that the presence of robots in a social system impacts human perception of social reality. In their research about the Catalonia Referendum of 2017, they found that bots (on twitter) targeted human influencers, mainly Independentists and provoked negative and inflammatory sentiments to some users (violence, shame against government and police) and inflamed social conflict online (Stella, Cristoforetti & De Domenico, 2019). Another interesting fact is that S. Gonzalez-Bailon & M. De Domenico in their research examined two events, the Yellow Vests movement in 2018 in France and the Catalonia Referendum of 2017. They found that unverified bots, by being more numerous, generated more content, interacted with more humans and gathered more attention that human accounts (Gonzalez-Bailonn & De Domenico, 2021). Stella et al., similarly with the term "cyborgs," talk about "augmented humans" during elections, meaning the exploitation of bots by humans, in order to gain impact online (Stella, Ferrara & De Domenico, 2018). From this we understand that today, even a single person has the ability to create a fake "cloud" of followers (bots), who will be able to spread their opinions or any information they want, they will press like, they will interact with others users, always according to the administrator's intentions and for his benefit. Therefore, we can imagine what possibilities are offered for an organization, company, political party or country that wants to use this digital "army" to propagate their positions. Bots are also a tool for financial fraud. The emergence of blockchain technology was accompanied by the emergence of cryptocurrencies. Mirtaheri et al. describe how bots are used by scammers in social media campaigns, in order to manipulate cryptocurrency prices. They create hype for certain brands. They are the so-called "pump" (when prices rise

artificially) and "dump" (when prices fall) operations (Mirtaheri et al., 2021).

Another technological element that plays a crucial role on the disinformation spreading process is algorithms. When a person searches for something by typing in a search engine, then some search results related to the topic appear, which will have been gathered through an algorithm. In essence, algorithms act as navigators for users on their journey through the digital world, so that they don't get bogged down in a jungle of information. L. Rainie & J. Anderson say that algorithms are instructions for solving a problem, artificial intelligence is literally algorithms and that in the future we may have self-learning and self-programming algorithms (Rainie & Anderson, 2017). Social media platforms also use algorithms. O'Brien (O'brien, 2023) says that social media algorithms make classification, assist in ranking search results, advertisements and sort content in a user's feed. The problem that arises is that users can sometimes see in their feed what the algorithm decides to show them, even if it is disinformation, misleading content, hate speech etc. The same can be done with the recommended videos or advertising messages. M. Vestager, the European Commissioner for Competition and Executive Vice President of the European Commission for A Europe Fit for the Digital Age stated that: "When recommender systems choose which information to promote, and what to hide, they profoundly affect what we know about the world...; those results might be manipulated by so-called "bot farms," to make content look more popular than it really is. Or the things that we see might not really be the most useful news stories, but the ones that are likely to get a response - and earn more advertising...; they affect the ideas and arguments we hear - and the political choices we believe we can make" (Vestager, 2020).

The content which provokes powerful emotions and sentimental response, has increased probabilities to get viral. The researchers consider that platforms encourage the propagation of popular content, in order to increase user engagement (Susarla, Oh & Tan, 2016). J. Paschen writes that fake news titles provoke strong and more negative emotions than real news (e.g. anger) (Paschen, 2020). Liu et al. in their research about medical information on social media, found that misleading content might inflame more engagement than high degree information (Liu et al., 2019). From this we understand that platforms may promote popular content, even if it is of low credibility or even if it belongs to the zone of falseness. P. Borges & R. Gambarato say that "the logic of algorithms to personalize content on search engines, news aggregators, and social networks therefore potentially creates filter bubbles and echo chambers that can lead to ideological segregation, perpetuation of misinformation, and confirmation biases" (Borges & Gambarato, 2019). A 2021 research conducted by Mozilla Foundation reports that the AI-driven algorithm of an examined famous platform, in many cases, recommended videos of political misinformation, Covid misinformation, inappropriate content and hate speech. They also add that this algorithm supports an estimated 700 million hours of watch time every day (YouTube Regrets, 2021). From these we understand the penetration dynamic that a platform can have in public opinion and that it can be "contaminated" with misinformation. Essentially, in some cases, social media can possibly be a "Trojan Horse" of misinformation for public life. Given the importance of the problem, A. Tutt proposes the creation of an "FDA for algorithms", i.e. a government organization (corresponding to the Food and Drug Administration) that will aim to regulate algorithms in terms of safety and effectiveness (Tutt, 2017).

Cookies are also an interesting aspect of the digital world and of how it contributes to the function of companies through advertising. According to Google Company, cookies are small pieces of text sent to your browser by a website you visit and they help both the user and the websites because:

- They are used for functionality, by maintaining your preferences in a website
- for security, by user authentication (for example prevention of scam)
- for analytics, by collecting data and using statistics to understand how a user interacts with a specific service
- for advertising, by personalizing ads

• for personalization (relevant results, recommendations, ads etc.) (Google, n.d.)

According to Kaspersky company, which provides Internet Security services, cookies are personalized, as their data are labelled with a unique ID of the user and his computer and most of them are safe, but some can be used to track you without your consent (Kaspersky, n.d.). The tracking cookies are used to store preferences and marketing data (activity on websites, browsing and purchase history, location etc.). Tracking cookies are used by marketers to target the users with advertisements that may interest them based on their browsing history (Strycharz et al., 2021). Essentially, through cookies, the platforms and sites outline the user's online behaviour and create an advertising profile for each one, so that they can direct advertisements to them, related to their preferences, with greater accuracy and effectiveness. The problem is that there is a possibility that the platforms will use cookies (as well as the algorithms we saw earlier) and through disinformation, increase the user's attention and engagement in order to harvest advertising profits. Something similar happens in the case of television, where the increase in viewership also provides advertising revenue, even if it is so-called trash TV. S. Paudel et al. (Paudel et al., 2020) write that false information can be a profitable business, producing large sums of advertising revenue from viral content, while social media are a fantastic environment for this. As reported by CBS (Bidar, 2021), in 2021, lawmakers in US demand stricter regulations for social media platforms regarding the problem of misinformation, with both Democrats and Republicans expressing similar sentiments and Congressman Pallone Jr. saying that "your business model itself has become the problem and the time for selfregulation is over." Nancy Pelosi, Speaker of the United States House of Representatives, in a message of social media executives, said: "You will be held accountable for your misconduct," (Turvill & Nancy, 2020) like the other time he expressed himself "again and again, social media platforms have sold out the public interest to pad their corporate profits. Their business model is to make money at the expense of the truth." (Pelosi, 2020) Also, a very important issue is how these data from users could be used for behavioural

targeting in political campaigns and voting events. Information Commissioner's Office launched an investigation about the use of data-analytics. In their report to Parliament (Ico.org.uk, 2018), they talk about companies and organizations that used data analytics and demographics to create psychographic profiles, to micro-target voters, in order to conduct persuasive data-driven campaigns. Based on the above, we could say that concepts such as advertising/marketing, political ideology, privacy, democratic transparency and fair competition are beginning to be questioned, as they try to coexist together in a situation that is not fully regulated and one affects the other, to a small or large extent. S. Zuboff (Zuboff, 2015) talks about surveillance capitalism and describes it as a phenomenon that produces the possibility of modifying people's behaviours and the things for profit and control. We believe, based on the above, that data is a key element in all of this, being the raw material of the whole process.

4. CONCLUSIONS

As we observe, in the modern era, propaganda for political, economic or even military reasons represents an existing phenomenon that has raised concerns and has evolved into what we meet as computational propaganda. Disinformation tactics in the digital world use automation such as bots, cookies and algorithms as tools for creating a suitable environment to influence opinions. Social media platforms, respectively without their intent, are the arena in which such operations conduct, because they are the point of human communication and argument exchange in the digital space. Thus, the battle against disinformation should be enhanced, especially in the digital world in order to protect democratic values, preserve a healthy dialogue in the public sphere and avoid scenarios of surveillance capitalism where the data could be possibly used for social manipulation and disrupting free opinion-making.

References

Arnaudo, D., Bradshaw, S, Ooi, H., Schwalbe, K., et al. (2021) *Combating Information Manipulation: A Playbook for Elections and Beyond* / The International Republican Institute, The National Democratic Institute & The Stanford Internet Observatory. Washington: IRI.

Bartles, C.K. (2016) Getting Gerasimov Right. *Military Review* (The Professional Journal of the U.S. Army), pp. 30-38.

Bessi, A. & Ferrara, E. (2016) Social bots distort the 2016 U.S. Presidential election online discussion. *First Monday*, 21(11).

Bidar, M. (2021) Lawmakers vow stricter regulations on social media platforms to combat misinformation. *CBS News*. Availabl from: https://www.cbsnews.com/ news/misinformation-extremism-hearing-googlefacebook-twitter-watch-live-stream-today-2021-03-25/ [June 22, 2024]

Borges, P.M. & Gambarato, R.R. (2019) The Role of Beliefs and Behaviour on Facebook: A Semiotic Approach to Algorithms, Fake News, and Transmedia Journalism. *International Journal of Communication*, 13, pp. 603-618.

Boshmaf, Y., Muslukhov, I., Beznosov, K. & Ripeanu, M. (2013) Design and analysis of a social botnet. In: *Computer Networks*. 57(2), pp. 556-578.

Bradshaw, S. & Howard, P. (2017) *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.* University of Oxford: Computational Propaganda Research Project.

Europarliament (2018) Computational propaganda techniques / European Parliamentary Research Service. Available from: https://www.europarl.europa.eu/ RegData/etudes/ATAG/2018/628284/EPRS_ ATA(2018)628284_EN.pdf [June 22, 2024]

Diresta, R. (2018) Computational Propaganda. Public relations in a high-tech age. *The Yale Review*, 106 (4), pp. 12-29.

Fisichella, D. (2007) Political science: issues, concepts, theories/ Translation from Italian and afterword by Victor Moraru. Iaşi: Polirom.

Gerasimov, V. (2016) The Value of Science Is in the Foresight. *Military Review* (The Professional Journal of the U.S. Army), pp. 23-29.

Gonzalez-Bailon, S. & De Domenico, M. (2021) Bots are less central than verified accounts during contentious political events. *Proceedings of the National Academy of Sciences of the United States of America* (PNAS), 118(11), pp. 1-8.

Howard, M. & Paret, P. (1976) Clausewitz Carl von. *On War*. New Jersey: Princeton University Press.

Google (n.d.) How Google uses cookies. Available from: https://policies.google.com/technologies/ cookies?hl=en-US [June 22, 2024]

NATO (n.d.) Information Warfare / Defence Education Enhancement Programme Available from: https://www. nato.int/nato_static_fl2014/assets/pdf/2020/5/ pdf/2005-deepportal4-information-warfare.pdf [June 22, 2024]

Ico.org.uk (2018) Investigation into data analytics for political purposes / *Information Commissioner's Office*. Available from: https://ico.org.uk/action-weve-taken/ investigation-into-data-analytics-for-political-purposes/ [June 22, 2024]

Liu, X., Zhang, B., Susarla, A., Padman, R. (2019) Go to YouTube and Call Me in the Morning: Use of Social Media for Chronic Conditions. *MIS Quarterly* (Management Information Systems), 44(1b), pp. 257-283. Marwick, A. & Lewis, R. (2017) *Media manipulation and Disinformation online* / Report. New York: Data and Society Research Institute.

Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Ver Steeg, G. & Galstyan, A. (2021) Identifying and Analysing Cryptocurrency Manipulations in Social Media. *IEEE Transactions on Computational Social Systems*, 8(3), pp. 607-617.

Monaco, N. (2018) Nyst, C. State-sponsored trolling. How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns. Palo Alto: Institute for the Future.

O'brien, C. (2023) How Do Social Media Algorithms Work? Available from: https:// digitalmarketinginstitute.com/blog/how-do-socialmedia-algorithms-work [May 22, 2024]

Paschen, J. (2020) Investigating the emotional appeal of fake news using artificial intelligence and human contributions. *Journal of Product & Brand Management*, 29(2), pp. 223-233.

Paudel, S., Kamde, R., Borkar, S. & Kokuntur, P. (2020) A Research study on Relationship between Fake News and Advertising. *International Journal for Research in Engineering Application & Management*, 6(1), pp. 256-261.

Pelosi, N. (2020) Disinformation Must Stop. Available from: https://pelosi.house.gov/media-center/pelosiupdates/disinformation-must-stop [May 29, 2024]

Rainie, L. & Anderson, J. (2017) Code-Dependent: Pros and Cons of the Algorithm Age? Available from: h t t p s : / / w w w . p e w r e s e a r c h . o r g / internet/2017/02/08/code-dependent-pros-and-consof-the-algorithm-age/ [May 29, 2024]

Roth, Y. & Pickles, N. Bot or not? The facts about platform manipulation on Twitter. Available from: https://blog.twitter.com/en_us/topics/ company/2020/bot-or-not_[May 29, 2024]

Salge, C. & Berente, N. (2017) Is that social bot behaving unethically? *Communications of the ACM*, 60(9). pp. 29-31.

Schafer, F. (2022) Japan's Shift to the Right: Computational Propaganda, Abe Shinzō's LDP, and Internet Right-Wingers. *The Asia-Pacific Journal*, 20(2), pp. 1-18.

Shao, C., Ciampaglia, G.L. et al. (2018) The spread of low-credibility content by social bots. *Nature Communications*, 9(1), p. 4787.

Stein, G.J. (1995) Information Warfare. *Airpower Journal*, 9(1), pp. 30-38.

Stella, M., Cristoforetti, M. & De Domenico, M. (2019) Influence of augmented humans in online interactions during voting events. *Plos One*, 14(5), pp. 1-16.

Stella, M., Ferrara, E. & De Domenico M. Bots increase exposure to negative and inflammatory content in online social systems. *Proceedings of the National Academy of Sciences of the United States of America* (PNAS), 115(49), pp. 12435-12440.

Strycharz, J., Smit, E., Helberger, N. & Van Noort, G. (2021) No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. In: *Computers in Human Behaviour*, **120**, **pp. 1-11**.

Stupples, D. (2015) What is information warfare? Available from: https://www.weforum.org/ agenda/2015/12/what-is-information-warfare/ [May 29, 2024]

Suarez-Serrato, P., Roberts, M.E., Davis, C. & Menczer, F. (2016) On the Influence of Social Bots in Online Protests - Preliminary Findings of a Mexican Case Study / Lecture Notes in Computer Science. *Social Informatics* (SocInfo), pp. 269-278.

Susarla, A., Oh, J.H., Tan, Y. (2016) Influentials, Imitables, or Susceptibles? Virality and Word-of-Mouth Conversations in Online Social Networks. *Journal of Management Information Systems*, 33(1), pp. 139-170.

Turvill, W. & Nancy, P. (2020) Social media bosses have 'utterly failed' to combat Covid-19 disinformation. *Press Gazette*, June 17, 2020.

Tutt, A. (2017) An FDA for Algorithms. *Administrative Law Review*, 69(1), pp. 83-122.

Vestager, M. (2020) Algorithms and democracy – Algorithm Watch Online Policy Dialogue. Available from: https://ec.europa.eu/commission/commissioners/ 2019-2024/vestager/announcements/algorithms-anddemocracy-algorithmwatch-online-policy-dialogue-30october-2020_en [June 29, 2024]

Norton (2018) What are Bots? / NortonLifeLock. Available from: https://us.norton.com/blog/malware/what-arebots# [June 29, 2024]

Kaspersky (n.d.) What are Cookies? Available from: https://www.kaspersky.com/resource-center/ definitions/cookies [June 25, 2024]

Woolley, S.C. & Howard, P.N. (2017) Computational Propaganda Worldwide: Executive summary. In: Samuel C. Woolley and Philip N. Howard (Eds.). *Computational Propaganda Worldwide*. University of Oxford: Computational Propaganda Research Project, p. 14.

YouTube Regrets (2021) A crowdsourced investigation into YouTube's recommendation algorithm / Report. Available from: https://assets.mofoprod.net/network/ documents/Mozilla_YouTube_Regrets_Report.pdf [July 25, 2024]

Zuboff, S. (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30, pp. 75-89.