Issue 37
March 2019

CREOGN Research Note

French Gendarmerie Officers Academy Research Centre

SOCIAL NETWORKS: PARADOXES AND TECHNOLOGICAL CONVERGENCE

By M. Philippe AUBERT-COUTURIER, in 2nd year of Master's degree internship at CREOGN

Summary of a publication by Mr Daniel GUINIER[1], Doctor of Science, expert in cybercrime and financial crimes at the International Criminal Court in The Hague

In 2018, there were some 4.2 billion Internet users (i.e. 55% of the world's population), 3.4 billion of whom were users of social networks (*Facebook, Twitter, LinkedIn, Whatsapp, etc.*). In addition to their growing importance, social networks have multiple facets: a space for sharing and exchanging information, they are also proving to be places of influence and even manipulation. New forms of threats and vulnerabilities have emerged, particularly in relation to the manipulation of public opinion. The use of bots[2] and trolls[3] has also made it possible to industrialise the sharing of false information.

1. The multiple challenges of social networks

A medium of exchange subject to numerous abuses

Social networks have gradually become a place for exchanging knowledge and information. On the borderline between private and public life, the law is enforced in respect of everyone's rights, despite the feeling of impunity that can sometimes prevail.

However, caution is needed on social networks, which are regularly used for manipulation or discrediting purposes. Any information disseminated can thus be instantly seen, used and retransmitted, including by people who were not necessarily the original recipients. This instantaneousness explains the growing phenomenon of the spread of rumours or false information (fake news). It is therefore more necessary than ever to measure the risk inherent in social networks in order to use them better.

A space of construction and vulnerabilities for users

Social networks have helped democratize access to public expression for populations that previously had no access to it. Today, people use them to reveal a lot of information about themselves, but also about other people. Each Internet user builds his own image on social networks, in the form of a digital portrait that he tends to enhance as he wishes.

This propensity of users to reveal themselves on social networks is sometimes out of step with the proximity they have with other users and is not always controlled. Many users do not care about the confidentiality of the

1 GUINIER, Daniel. Réseaux sociaux, paradoxes et convergence technologique. *Expertises*, n° 444, march 2019. ("Social networks, paradoxes and technological convergence.")

2 A "bot" is a computer program that operates autonomously and whose main mission is to perform tasks repeatedly. Automated subscriptions, conversational and interactive robots (chatbot), etc., the bot relies on databases to respond to surfers' requests.

3 "Trolls" are accounts of surfers who voluntarily start controversies on social networking sites, discussion forums or blogs, with the aim of provoking or generating reactions in return, through excessive, insulting or advertising contributions.

information they publish and the access settings to their accounts and publications. Also, information is regularly treated too lightly and is perceived and retransmitted without any real control of its validity. In addition, a lot of information is passed from one social network to another, for example from *Facebook* to *Twitter*, which amplifies its reach.

Digital challenges for companies

Social networks are a recent sphere of communication and influence for companies. The forms of exchange that they induce have gradually led to the emergence of the issue of digital influence. The need to actively engage in social media is nowadays the guarantee for companies to play on equal terms with their competitors. Conversely, disregarding the digital sphere is in some ways equivalent to ceding a significant amount of notoriety and reputation to adversaries.

This is all the more important because the immediacy of the dissemination of information makes it more necessary than ever to monitor the situation in order to ensure that the company can react quickly and appropriately in an increasing context of damage to its reputation. In fact, the latter is now perceived as a major risk[4], given the wide audience possibilities provided by the Internet. A good - or bad - reputation can thus spread to hundreds of millions of people in a very short time.

Companies are therefore trying to control their digital identity through their representation on social networks, without however being able to guarantee total control of their e-reputation, which can be undermined by certain major influencers. In fact, social networks have seen the emergence of new forms of vulnerabilities and threats for the various actors who evolve on them.

2. New threats and vulnerabilities

The online influence ecosystem

The online influence ecosystem is composed of several overlapping spheres, shared between human and robotic Internet users. Within this ecosystem, some great influencers stand out: renowned experts, media personalities, activist groups, etc. These modern "gurus" are followed by a host of "adepts" who echo back their messages.

The moderation system of social networks, based on algorithms, offers new possibilities to these influencers, whether they are human or robotic.

A complex algorithmic system

The moderation of social networks is essentially the responsibility of algorithms whose action on the reputation and therefore the influence of content is decisive, as in the case of *Twitter*, which gives priority to the *tweets* deemed most relevant. This algorithmic selection has immediately visible consequences: increase in the number of views, *likes*, *retweets*, etc.

Several questions arise as to how these algorithms work: firstly, on what criteria should the selection be made between what is relevant and what is not? Similarly, on what basis should the deletion of content or the suspension of an account be decided? A first issue thus lies in the legal qualification of the content. A second difficulty concerns the capacity to react and process the enormous flow of data. In this respect, nearly 10 million tweets are published every minute throughout the world. Finally, another major challenge lies in the vulnerability of the algorithms to possible attacks, whether bypassing or malicious modifications. Moreover, this threat is accentuated by the possibility of errors due to the complexity of the algorithms[5].

New vulnerabilities : *bots* and *trolls*

4 Aon report 2017 and Deloitte study.

5 GUINIER, David. *Sur la place des algorithmes et les exigences face à la complexité*. *Revue Experts,* n° 139, july 2018, p. 40-44. (*"On the place of algorithms and the requirements of complexity")

The development of social networks thus has its dark side. Their growth has allowed new forms of manipulation, particularly through the worldwide propagation of false or misleading information, which has been amplified by the use of *trolls* and *bots*. *Trolls*, social network accounts created by humans, are indeed a major vector for the propagation of biased content. Their use today is essentially aimed at creating controversy around targeted topics. Similarly, social *bots* are programmes designed to deceive Internet users by simulating human behaviour through automated interactions on social networks. By posing as real people, they are able to infiltrate social networks and gain the trust of users, sometimes for malicious purposes. They are also supported by classic *bots*, which are linked to a machine and make it possible to amplify the virality of targeted information. *Bots* and *trolls* are major distribution relays for certain influencers, acting as real sounding boards for social network users. The impacted profiles can be counted in the millions.

The case of the 2017 French presidential campaign

These disinformation operations were illustrated on a large scale during the 2017 French presidential campaign. E. Ferrara thus brought to light a vast operation to manipulate public opinion[6], by analysing 17 million *tweets* relating to the election period, posted between 27 April and 7 May 2017. In total, some 18,324 social *bots* are said to have participated in this disinformation campaign targeting, in particular, candidate Emmanuel Macron, with a peak of *tweets* attributed to *bots* on 7 May 2017, the date of the elections. However, it has been shown that these disinformation cascades are first attributed to human *tweets*, which are then amplified by a resonance phenomenon.

This new threat posed by *bots* and *trolls* is now taking on a particular dimension, boosted by the new opportunities offered by technological convergence.

3. The possibilities brought about by technological convergence

Further improvement of information tools

Technological convergence, initially limited to computer technologies, now refers more broadly to the integration of several devices, services and networks within a single system or device. It is a ubiquitous phenomenon and involves combining technologies from several fields such as multimedia or telecommunications.

In the field of computer science, progress made in artificial intelligence has allowed for the advanced development of bots, enabling them to simulate real Internet users more than ever before, making them undetectable. This manipulation is accentuated by mixing false information with accurate and verifiable content. These influence strategies take the form of real destabilisation operations, targeting the very foundations of democracy[7].

The limits of technological convergence

However, this progress must be put into perspective, as demonstrated by the *Tay* experiment conducted by Microsoft in March 2018. A chatbot with artificial intelligence, *Tay* took on the profile of a teenage girl to chat on social networks, basing its words on pre-written answers or public databases. The experiment quickly gained momentum, with *Tay* attracting 23,000 followers in less than a day, sending out some 100,000 tweets. However, limits to the chatbot's learning and exchange capabilities soon became apparent after the robot made inappropriate or racist comments, and *Tay* was soon the target of insults and sexist remarks. Microsoft

6 FERRARA, Emilio. *Disinformation and social bot operations in the run up to the 2017 French presidential election*, University of Southern California, Information Sciences Institute, Vol. 22, n° 8.

7 JEANGÈNE-VILMER, Jean-Baptiste, ESCORCIA, Alexandre, GUILLAUME, Marine, HERRERA, Janaina. *Les manipulations de l'information : un défi pour nos démocraties. ("Information manipulation: a challenge for our democracies.")* Report of the *Centre d'analyse, de prévision et de stratégie* (CAPS) from the Ministry of Europe and Foreign Affairs and the *Institut de recherche stratégique de l'École militaire* (IRSEM), august 2018, p. 210.

therefore finally put an end to the experiment.

What is the response of the digital players?

In contrast to the primary vocation of social networks as a place for sharing knowledge, technological convergence, by combining the Internet, social networks, bots, artificial intelligence and big data, is likely to represent a growing asset for operations to destabilise or manipulate public opinion. The challenge for social networking platforms will be to maintain rigorous ethics to guarantee the proper use of social networks, under the control of states and institutions. The latter have been able to measure the extent of the risks of manipulation, leading them to strengthen consultation between the various stakeholders concerned: public authorities, operators, social network users, etc. A change in legislation also merits in-depth examination, in order to settle the question of the balance between freedom of expression and control of the authenticity and truthfulness of comments posted online on social networks. The aim is to provide a definitive response to the recurrent accusations that public freedoms on the Internet are being undermined, particularly in terms of freedom of expression. In this respect, particular attention should be paid to Law 2018-1202 of 22 December 2018 on the fight against the manipulation of information[8], particularly during the European electoral process.

Conclusion

Social networks constitute a single reality, but perceived from several different angles, depending on the nature of the actors involved: Internet users, companies, social network operators, etc. In fact, the ecosystem of online influence reveals divergent interests between these different actors, made up of human beings but also of "algorithmic entities", with increasing capacities for action and to which technological convergence has conferred new possibilities. Social networks therefore have a paradoxical nature that must be taken into account in order to avoid certain abuses, one of the manifestations of which is the manipulation of public opinion. Fake news and provocative messages are indeed a serious threat for all web actors, which should be addressed and regulated, either through legal tools or through a global cooperation process.

Translated by SLT Clément DE SAVIGNY and the French Gendarmerie Officers Academy Language Department

8 General WATIN-AUGOUARD, Marc. Law n° 2018-1202 of 22 December 2018 on the fight against information manipulation. *Note du CREOGN* [online], n° 36, january 2019. Available on : https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/La-loi-n-2018-1202-du-22-decembre-2018-relative-a-la-lutte-contre-la-manipulation-de-l-information