

## Hybrid CoE Strategic Analysis 16

# **Combating the manipulation of information – a French case**

MARINE GUILLAUME





Hybrid CoE Strategic Analysis 16

## Combating the manipulation of information – a French case

What if these campaigns, which seem to be increasingly integrated into strategies of interference and power waged by external actors, were actually able to distort the election results and therefore violate the sovereignty of states? – asks Marine Guillaume, Digital Ambassador Deputy at the French Ministry of Europe and Foreign Affairs and Lecturer at the École Polytechnique.

## Fighting against information manipulation – legal means

In March 2018, Richard Ferrand, who was then En Marche! Member of the National Assembly (now President of the National Assembly), and several of his colleagues from the same political party, tabled a motion entitled the 'Law to combat false information'. Colloquially referred to by the press and a part of the opposition as the 'Anti-fake news law', this motion denounced the multiplication of 'massive campaigns of false information aimed at using online communication services in order to modify the normal course of the electoral process'. Its goal was to overcome the weaknesses of the existing French legal framework, notably by creating new legal tools that would adapt the old legal principles framing the diffusion of false information (dating back to Article 27 of the 29 July 1881 law on the freedom of the press) to the era of digital media, and which would be

empowered to rapidly withdraw problematic online content. As the objective of the motion was to directly tackle the electoral process modalities, two motions actually had to be tabled in two different Commissions.<sup>1</sup>

#### The need to update the legal framework

There are three reasons why the motion for the 'Law to combat false information' came about. First, the numerous information manipulation campaigns of recent years, defined as a coordinated campaign designed to diffuse false information or information that is consciously distorted with a political intention to hurt, started to raise concerns: Were democracies able to resist and overcome these types of threats in the digital era? What if these campaigns, which seem to be increasingly integrated into strategies of interference and power waged by external actors, were actually able to distort the election results and therefore violate

1 'Commission des lois' and 'Commission des affaires culturelles et de l'éducation'.

the sovereignty of states? These questions started to intensify in France after the 2016 US presidential elections, and the debate on the impact of the DNC hacking and leaks on the eventual election of Donald Trump. They were reinforced by suspicions of Russian interference in the Brexit referendum and subsequently by the so-called Macron leaks episode, namely the release two days before the second and final round of the rench presidential election of 9 gigabytes of data hacked from Emmanuel Macron's campaign team. Democracies started to realize that a new existential danger, inherent in the social media era, was posing a threat that they had to tackle.

Second, the Russian media RT and Sputnik started to gain a larger audience in France and to become increasingly visible. Their editorial line, which involves a combination of distorted, biased and entirely fabricated information, was heavily criticized, notably by French President Emmanuel Macron, who did not hesitate to dub them 'propaganda outlets' in front of President Putin (during the Versailles Summit of May 2017). Yet the existing regulation framing media activity in France did not really provide tools for framing broadcast online content. Put differently, the 'CSA' (an independent institution that regulates the media) had no power to limit the activity of RT and Sputnik on the internet, which was all the more problematic as most of their content is actually created for online distribution. This incapacity to regulate the main 'fuel' of information campaigns (i.e. false information online) rapidly emerged as a major shortcoming that needed to be addressed, without limiting the freedom of speech principle.

Third, growing discontent towards digital platforms, accused of standing by while facilitating crime, terrorism, violence and disinformation, started to be shared by a wider number of governments and actors. The strongly worded speech delivered by Theresa May at the Davos Forum (January 2018) on the subject of digital platforms encapsulated this discontent: 'These companies have some of the best brains in the world. They must focus their brightest and best on meeting these fundamental social responsibilities'. In this regard, the law banning online hate speech that came into force in Germany at the start of 2018, which requires social platforms to remove offensive posts within 24 hours, was perceived as an important step that could pave the way for a more general constraining and regulative approach towards digital platforms, when information is used not as an expression of opinions or for broadcasting news, but as a manipulative tool to harm the targeted society.

#### The French case

The motion was the subject of many discussions and of an ongoing disagreement between the two Houses of the National Assembly. The Senate rejected the text twice. During the whole discussion process, some amendments were made and the title of the motion changed from the 'Law to combat false information' to the 'Law against the manipulation of information'. The motion was finally appr ved by the National Assembly on 20 November 2018. The French Prime Minister and more than 60 Senators then decided to submit an appeal to the Constitutional Council so that the latter would examine the legality of the motion. The Constitutional Council released its decision on 20 December 2018 and stated that the motion was indeed legal, but expressed concerns about some of the interpretations.

It notably specified that the judge could halt the diffusion of a piece of 'information content' only if the latter was evidently false or misleading, and if the risk of altering the sincerity of the vote was also evident. The motion was finally enacted two days later, on 22 December 2018.

The 'Law against the manipulation of information', **information manipulation being defined as the 'inexact or misleading** *allegation of a fact that could alter the sincerity of an upcoming vote and that is spread deliberately, artificially or automatically and massively to the online public through a communication service*', is based upon fi e pillars.

#### First, the law mentions that the operators of a digital platform have the duty to cooperate to combat disinformation.

They are notably encouraged to make efforts and to improve their actions in a number of domains: the transparency of their algorithms (I); the promotion of content created by companies, press agencies and TV communication services (II); the fight against accounts that diffuse false information (III); informing users about the identity of the physical or social entity, social head office and social object of mo al persons that pay them in exchange for the promotion of information content tied to a debate of general interest (IV); informing users about the nature, origin, and modalities of content diffusion (V); and promoting media literacy (VI). Digital platforms also have a duty to designate a legal representative to be the respective point of contact on French territory.

#### Second, the operators of digital platforms also have the duty during the electoral period (i.e. defined as three months before the first d y of the general election until the vote) to strengthen their transparency obligation towards

#### the sponsored information content.

The law requests digital platform operators to provide loyal, clear and transparent information on the identity of those who pay for information content tied to a debate of general interest, and on the total amount paid for diffusing this content. The law likewise requests digital platform operators to be transparent in the way personal data are used in order to promote content tied to a debate of general interest.

Third, the law creates a new legal procedure: the possibility to take the case to a 'juge des référés' to fight against disinformation during the electoral **period** in order to halt the diffusion of an inaccurate or misleading allegation or imputation of a fact (I) that can deliberately alter the sincerity of the upcoming vote (II) in an artificial or massi e way through a communication service for the online public (III). Once the case has been put before the judge, 48 hours are allowed for the pronouncement of a decision and to take the proportionate and necessary measures to halt the diffusion should the content meet all the three previously described criteria.

Fourth, the law reinforces the power of the CSA (Conseil Supérieur de l'Audiovisuel, namely the independent authority of TV media and radio regulation) **to fight** against any attempted destabilization or disinformation campaign by a media television service controlled or influenced by a foreign state; if, during the electoral period (defined below), the CSA observes that a service which is under the influence of a foreign state is delibe ately diffusing false information in order to alter the sincerity of the vote, the CSA can, in order to prevent or put a stop to the disruption, request the suspension of the service diffusion by any procedure of

electronic communication until the end of the voting operations.

Fifth, **the law underlines the necessity to support and reinforce media literacy** (especially for content disseminated over the internet) in schools.

## The legal framework against information manipulation also has it challenges

Combating information manipulation is difficult. Balancing between countering hostile foreign state-generated activity and allowing domestically generated critical activity is a challenge. From its elaboration to its enactment, the French law has been criticized, either for being perceived as **offering too minor and non-enforceable measures** (I) or **for adding ambiguous obligations that might seriously threaten the freedom of expression** (II). These criticisms can be classified within three different arguments.

In the first argument, the new legal proc dure created by the law (with the 'juge des référés') was criticized by some observers as being doomed to be inefficient because of two main difficulties. Firstl, assessing that certain content is inaccurate or misleading requires an important margin of interpretation which is difficult to reconcile with the necessity for the judge to decide rapidly and firmly whether the content should be taken **down**. This assessment is all the more complex in an electoral context where, by nature, many people express opinions and contradictory arguments that can be perceived as erroneous or insincere. Secondly, assessing that certain content can hurt the sincerity of the vote before the vote has even taken place is problematic with regard to the French law

**tradition**. Indeed, the latter tended to favour a retrospective assessment: it is only after the vote occurs that one can measure whether the vote has or has not been influenced y the diffusion of certain content. By inverting this principle, this new legal procedure contradicts the French tradition and makes the judge's decisions more complex.

The second critical argument points to the fact that the law mentions several new duties for digital platform operators be they to cooperate in combating disinformation or to strengthen their transparency obligations. Yet, in both cases, these duties are not constraining: States can only name and shame them. From this perspective, this aspect of the law does not really confer anything new with regard to what has already been accomplished in the European Commission vis-à-vis digital platforms to combat disinformation (notably with the Code of Conduct for digital platforms put in place by the Commission). In the worst case, naming and shaming can play into the hands of hostile information manipulators.

Lastly, the reinforcement of CSA power also remains limited: it only applies to TV and radio content. From this perspective, it does not encompass online media (i.e. media produced for social networks), which are precisely the type of media most produced and used by those who are behind information manipulation campaigns.

The French law was designed to **propose a new approach to combat information manipulation campaigns** mostly by reinforcing the **power of trustworthy third parties** (Conseil Supérieur de l'Audiovisuel), and by calling on platforms to be more **transparent**. It also aimed to uphold the **freedom of speech and**  expression that is paramount in democracies, especially in times of electoral processes, when ideas and debates are often polarized. The upcoming European elections will be a major test. Some commentators are already underlining the risk of malicious actors launching information campaigns that would purposely and not precisely meet the criteria defined y the law (and hence would not fall under the law), and using this as a tool to 'guarantee' their legitimacy. Others underline the necessity for platforms, which have already developed an ambiguous relationship with the law (i.e. Twitter has recently censored an advertisement by the

Ministry of Interior raising awareness of the European elections in the name of the law), to be more accountable and to work in a more transparent and collaborative way with civil society in order to fight against disinformation. Finally, **a strong** civil society aware of the risks and equipped with strong critical reasoning skills can provide better protection against the resources and resourcefulness of malicious external actors intent upon destabilizing electoral processes with information manipulation campaigns. While useful to some extent, regulation is not the only tool to achieve these objectives.

#### Author

**Marine Guillaume** is Digital Ambassador Deputy at the French Ministry of Europe and Foreign Affairs, and a Lecturer at the École Polytechnique. She previously served for two and a half years as Policy Officer on Cybersecurity and Digital Affairs' at the Policy Planning Staff of the Ministry for Europe and Foreign Affairs. She was also an Associate Consultant for Bain & Company (May 2015–August 2016). Holding a doctorate in Political Science from Columbia University and Sciences Po Paris, she has previously worked as both a Lecturer at the School of International Public Affairs (SIPA), and as a Lecturer at Sciences Po Paris.

#### Literature:

Beswick, E. 'Twitter blocks French government ad campaign using France's own fake news law', *Reuters*, 3 April 2019, <u>https://www.euronews.com/2019/04/03/</u> twitter-blocks-french-government-ad-campaign-using-france-s-own-fake-news-law.

CAPS-IRSEM Report, Information Manipulation: a Challenge for Our Democracies, August 2018, <u>https://www.diplomatie.gouv.fr/IMG/pdf/informa-tion\_manipulation\_rvb\_cle838736.pdf</u>.

Discours de la Conférence de presse conjointe de MM. Emmanuel Macron, Président de la République, et Vladimir Poutine, Président de la Fédération de Russie, sur les relations franco-russes et sur les conflits en Syrie et en Uk aine, à Versailles le 29 mai 2017, <u>http://discours.vie-publique.fr/notices/177001526.html</u>.

France Diplomatie, Combating the manipulation of information, <u>https://www.gouvernement.fr/en/combating-the-manipulation-of-information.</u>

Le Drian, J.-Y. (Minister of Europe and Foreign Affairs), discourse for the Conference 'Sociétés civiles, médias et pouvoirs publics: les démocraties face aux manipulations de l'information', <u>https://www.diplomatie.gouv.fr/fr/les-ministres/jean-yves-le-drian/discours/article/conference-internationale-societes-civiles-medias-et-pouvoirs-publics-les.</u>

Toucas, B. 'The Macron Leaks: The Defeat of Informational Warfare', *CSIS Commentary*, May 30, 2017, <u>https://www.csis.org/analysis/macron-leaks-defeat-in-formational-warfare</u>.

Untersinger, M. *Le Monde*, 'Loi sur les "fake news": les députés sur la corde raide', 7 June 2018, <u>https://www.lemonde.fr/politique/article/2018/06/07/loi-sur-la-manipulation-de-l-information-les-deputes-sur-la-corde-raide\_5310839\_823448.</u> <u>html.</u>

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.

ISBN 978-952-7282-45-8 ISSN 2670-2282

Second version of the publication. Previously published as "Strategic Analysis 2/2019: Combating the manipulation of information – a French case"

May 2019

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

The responsibility for the views expressed ultimately rests with the authors.



