FONDATION ROBERT SCHUMAN

POLICY PAPER

European issues
n°578
1st December 2020

European Democracy, a fundamental system to be protected

Eric MAURICE

Democracy is the political and moral foundation of the European Union and its Member States. Its smooth functioning endeavours to pacify political alternation, reduce social tensions and eliminate judicial arbitrariness, thus guaranteeing civil peace and the prosperity of European societies. Moreover, in a world where the markers of liberal democracy resulting from the European Enlightenment are receding, the value of democracy is a tool of the Union's power and influence. In the absence of a functioning democracy the Union and its Member States would lose their capacity to act and defend their interests, either via the upkeep of rules-based multilateralism or the projection of their values and standards that are emulated by others.

Philosopher Marcel Gauchet notes that in today's world, politics have become "*the true functional and symbolic infrastructure of our societies*". Disinformation and manipulation campaigns aim to undermine this infrastructure by weakening the authority, legitimacy and effectiveness of politics in democratic societies. From this point of view, the European democratic system can be seen as a critical infrastructure that needs to be protected jointly, in the same way as the traditional material and technical infrastructures.

The U.S. presidential election of 2020, after that of 2016, is a reminder of the challenges facing the most established democracies, as well as a demonstration of the importance of the effective functioning and respect for institutions. The situation in the United States is partly the result of traditions and conditions specific to that country. But the mechanisms and symptoms are common to most democracies, particularly in Europe, where the manoeuvres to turn people against the action taken by the Union and its Member States to counter Covid-19 pandemic have taken advantage of social discontent.

Threats to democratic systems are both physical and, increasingly, virtual in nature, including cyber-attacks, hacking, disinformation and manipulation, mainly via the Internet. However, the answers are not only technical. The Internet is only the means by which policies to weaken open democratic societies can be pursued, and whose real scope of action affects both individual and collective minds and opinions.

The multiplication of the ways and means of undermining our democratic societies and systems is reflected in the concept of hybrid threats, defined by the Union as "*the mixture of coercive and subversive activities, conventional and unconventional methods (i.e. diplomatic, military, economic, technological) which can be used in a coordinated manner by state and non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*".

The response adopted over the past few years has therefore relied on a variety of means but also, in the European context, on coordination between the national level, which remains sovereign in many areas, and the European level.

On 2 December, the European Commission is due to present its Action Plan for European Democracy, the result of several consultations and the experience of recent years. The plan will be structured along three lines that cover more than just hybrid threats: the integrity of elections and political advertising; the fight against misinformation; and the strengthening of media freedom and pluralism.

The dual objective of this plan, according to the Commission, is to "*ensure that citizens are able to participate in the democratic system through informed* *decision-making free from unlawful interference and manipulation", as well as to "improve the resilience of our democracies*". This is different from and complementary to the actions taken by the institutions to protect the rule of law when it is challenged by some Member States.

These actions, implemented using the procedure of Article 7 of the Treaty on European Union, the authority of the Court of Justice, the new European mechanism for protecting the rule of law and, soon, the mechanism of conditionality included in the Union budget, constitute the internal pillar of the defence of the democratic infrastructure that underpins the European model. This study focuses on the external pillar - the fight against hybrid threats and electoral interference - and the intermediate pillar - the fight against disinformation and support for the media

1. TACKLING THE HYBRID THREAT

Hybrid threats are emerging from the constant development of new technologies and their use in information warfare theorised by Russia and applied by other States such as China or Iran. They are driven by non-military methods but serve strategic objectives traditionally pursued by military means: the weakening and vulnerability of the adversary with the aim of neutralising him and advancing one's own interests.

In the case of the European Union, vulnerability stems from the "imperfect" nature of European integration, in which the cohesion of the Member States is both a goal and a condition for decision-making. Dividing European countries to better prevent them from acting is a tactic used by the Union's economic adversaries, such as China or the United States. Dividing European citizens via hybrid threats to undermine the cohesion of the Union is the strategy pursued by its political adversaries such as Russia and China. This is how these two States tried to spread confusion in the spring of 2020 about the nature and origin of Covid-19 and the means to address it, while at the same time intervening to make it look as if they were helping Europeans in place of an "inactive EU".

The health, economic and social crisis caused by Covid-19 has further exposed European societies to the hybrid risk. As stressed by the Commission, it has "*underlined how social divisions and uncertainties create a security vulnerability*". Despite this awareness, Europe remains highly exposed to hostile action.

Progressive increase in awareness

The first cyber-attack organised with the aim of destabilising a European state dates back to 2007, in Estonia, when Russia targeted ministries, parliament and banks in retaliation for the removal of a Soviet statue. But it was with the Ukrainian crisis in 2014 and the deployment of paramilitary, cyber and information activities by Russia that the Union came to understand the hybrid threat, the consequences of which on democratic systems became apparent with the American presidential election of 2016 and, to a lesser extent, with the referendum on Brexit in June 2016.

The U.S. presidential election of 2020 was not marked by such dramatic interference as the hacking of the Democratic campaign team in 2016, with the revelations intended to harm Hillary Clinton. But several bids to attack Joe Biden were noted. The authorities also warned against piracy and disinformation. Facebook and Twitter have suspended the accounts of fake media and journalists created by the Russian Internet Research Agency, the main source of online manipulation. Moreover, the FBI and the Cybersecurity and Infrastructure Security Agencies observed incursions by pirates identified as Russians in the authorities' networks at various levels, likewise the civil aviation networks.

In view of the European elections in 2024, and especially of important events such as the federal elections in Germany in the autumn of 2021 and the presidential and legislative elections in France in the spring of 2022, the American experience shows that the threat is still present and multifaceted. It also shows the role of federal structures, which can monitor the situation over a large territory at different levels, and the importance of the involvement of major digital platforms in coordination with the public authorities.

The Union's response since Russia's actions during the war in Ukraine has been continuous, with the aim of gaining an overview and supporting Member States in preventing and responding to threats. In 2016, it developed a Joint Framework on countering Hybrid Threats, comprising 22 operational measures, which was completed in 2018 with a plan "*to increase the resilience and bolster capabilities to address hybrid threats*."

At European level, risk analysis work is carried out by INTCEN, the Union's intelligence and situation centre, which is part of the European External Action Service (EEAS) and is responsible for exploiting "open" sources and analyses provided by the Member States' intelligence services.

The "fusion cell" was created within INTCEN in 2016, the former being defined as the "single central point for the analysis of hybrid threats", in liaison with the institutions and Member States to centralise alerts and risk analysis. The fusion cell works closely with the European Centre of Excellence for Hybrid Threat Assessment (Hybrid CoE), a Helsinki-based body created in 2017, which oversees a network of some 1,200 civilian and military experts, both governmental and private, from 28 countries (EU and NATO). The Centre conducts research as well as seminars and simulation exercises to strengthen the capabilities of participating States, in particular in the area of civil-military cooperation.

In early 2020, the Centre of Excellence and the Commission presented Member States with a "conceptual model" for the analysis of hybrid threats, which was tested during the Covid-19 crisis. Discussions are taking place within the framework of another recent structure, the "Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats". Set up within the Council in the summer of 2019 and made up of national experts, it is responsible, among other things, for defining common strategies and modes of action against all types of action that remain below the threshold of military action and, in particular, disinformation. Its work primarily involves an effort to continue to identify vulnerabilities, through questionnaires submitted to the Member States.

A report on the implementation of the strategy adopted since 2016, published in July 2020 notes that the Union has adapted to the development of hybrid threats and that "joined up work has become the norm" within European institutions and agencies. It stresses however that despite progress made in the Member States an established government level coordination and sufficient societal awareness within societies is still lacking. This is partly because not all governments share the same appreciation of the threat, nor the same willingness to expose their vulnerabilities.

Awareness of hybrid issues led to the establishment in the summer of 2020 of a special committee in the European Parliament on "foreign interference in all democratic processes in the European Union, including disinformation", which will issue its report in the autumn of 2021.

Cyberattacks and hacking

The dependence of all human activities on computer technologies and systems, which has been further accentuated by the health crisis, makes public and private infrastructures vulnerable to cyber-attacks and hacking. In the context of the protection of democracy, cyberthreats concern both the electoral process (the integrity of the ballot) and the environment in which it can take place (the security of the infrastructures necessary for the proper functioning of society).

Cyber- attacks against infrastructure (electricity, communications) or public services (hospitals, transport) seek to instil a sense of vulnerability and possibly also to create chaos that prevents the proper conduct of an election or, more generally, engender distrust of the State and the political system. Operated by groups of hackers sometimes working for governments, they often comprise so-called Distributed Denial of Service Attacks (DDOS), or malicious software sent in an innocuous form - backdoors to block or control a system from the outside, or "ransomware" blocking a system and demanding a sum of money.

In addition to businesses, hospitals are regularly targeted, for example in the UK in 2017, France in 2019 and the Czech Republic in 2020. Attacks are often attributed to Russian hackers, but in June 2020, the President of the Commission pointed to China, warning that cyber-attacks on hospitals, in the midst of a coronavirus crisis, "cannot be tolerated".

This risk is not exclusively related to democratic processes. It concerns all States in the world, regardless of their political regime. It has long been the subject of strategies at national level and within the framework of alliances such as NATO. In 2013 the Union adopted a cybersecurity strategy, and in 2016 the directive on networks and IT systems security (NIS), which aims to increase the Member States' capabilities in terms of cybersecurity and to strengthen their cooperation in terms of information and response to incidents.

More specific are election-related cyber-threats, which, by definition, are of primary concern to all democracies. The integrity of an election can be jeopardised by hacking into voter lists or results collection systems, but also by "hack and leak", the hacking of a candidate's or party's internal systems, followed by the publication of real or faked documents in order to weaken or discredit the candidate.

The two main examples, attributed to Russia, are the hacking of US Democratic Party emails and their publication by Wikileaks prior to the 2016 presidential election, and the "Macron Leaks" resulting from the hacking of the candidate's "En Marche" political movement during the 2017 presidential campaign. A hacking of the Bundestag in 2015, also attributed to Russia by German Chancellor Angela Merkel, did not result in any particular revelation or destabilisation. The German Ministries of Defence and Foreign Affairs were also attacked in 2018.

Prior to the 2019 European elections, denial of service attacks were reported on websites providing information on the European elections in several states including Finland and the Czech Republic. In 2017, even before the MacronLeaks, France had given up on the e-vote, allowed only for voters living abroad during the general elections, due to the "*high level of risk of cyberattacks*."

More recently, computer attacks against local authority networks have been observed. This was the case in Marseille and its surrounding area, two days before the first round of local elections in March 2020. "*The impacted networks are used, for example, to edit the registration lists, to manage proxies, to manage everything related to the election*", explained Guillaume Poupard, Director General of the French Agency for IT systems security (ANSSI), to the Parliament's special committee on interference. It points to the risk of hacking into polling institutes on election days to distort initial estimates and cause confusion.

The EU relies on the European Network and Information Security Agency (ENISA), set up in 2004, to help Member States establish and coordinate national cybersecurity strategies and responses to risks or attacks. In the spring of 2019 ENISA published a series of recommandations for the Member States and undertook a simulation exercise with Parliament and the Commission to test the capabilities already in place. The agency works with the Member States from a technical point of view within the CSIRT[1] Network, the European Warning and Response Centre and since September 2020n within the Cyber Crisis Liaison Organisation Network (CyCLONe), whose goal it is to foster exchange of information regarding national strategies and to develop a coordinated incident impact analysis.

Under the directive on the security of networks and information systems (NIS), the EU set up a cooperation group in 2018 to map the national measures taken to ensure the security of networks and IT systems used in the context of elections, and to identify shortcomings that could affect European elections. The group set out a "compendium on cybersecurity of electoral technologies", whose recommendations have been adopted by at least 16 Member States in terms of making safe the European elections.

The European Security Union Strategy, presented by the Commission in July 2020, plans to develop the Union's "situational awareness" and its resilience, notably via an improved integration of information flows and the revision of the EU operational protocol for countering hybrid threats. In December the Commission will present an update of the cybersecurity strategy, which will include a revision of the NIS directive. One of the elements of this could be the classification of equipment

[1] Computer Security Incident Response Team, who exist both in the public and private spheres.

used for elections as critical infrastructure, so that the NIS Directive covers it and the obligations it sets out for States – as requested by the European Parliament.

In the field of cybersecurity, threats have therefore been identified, and the priority is above all to pool information, methodologies and means of action in an area where the sovereignty of States remains clearly established and risk analysis is unequally shared.

1. ENSURING THE INTEGRITY OF ELECTIONS

Democratic systems are characterised above all by free, undistorted elections in which citizens express their views on the basis of open and fair debate. In contrast to dictatorships and authoritarian regimes, democratic countries establish clear rules in advance to ensure the fairness of the elections and the legitimacy of the resulting powers. Circumventing these rules, distorting debates and electoral processes are the means by which third groups or States can influence the outcome of elections and/or weaken the legitimacy of elected leaders, and thus their ability to act.

In this area, the EU can only intervene directly in the European elections, but it can also encourage national actors to follow common rules or best practice. Prior to the last European elections, in September 2018, the Commission proposed a series of measures and recommendations, which has served as a base to date for joint action to ensure the security of the electoral processes in Europe. The Commission placed the accent on cybersecurity, transparency and data protection.

One of the main measures in this "election package" was the creation of the European Cooperation Network on Elections, in which Member States exchange views on their electoral legislation, risk assessment and awareness campaigns, as well as on data protection rules or cybersecurity. The Network has been a point of contact between Member States, the Parliament and various bodies such as the Authority for European Political Parties and European Political Foundations, Europol or audio-visual media regulators. The process has enabled, among other things, the identification of differences in approach between States and has made to start remedying inadequacies. In the future, the Cooperation Network is due to continue to promote the alignment of rules and develop cooperation with media and platforms.

In September 2020 France, Latvia and Lithuania suggested taking things further and they created a joint election protection mechanism, which can rely on a panel of national experts who are prepared to help any Member State to protect its electoral system against attacks. This mechanism will be based on a preventive aspect at the Member State’s request to identify attempts to destabilise electoral processes and also on feedback.

Party Financing

Within the European Cooperation Network on Elections, the Member States have drawn up a table of the rules in force in each of their countries concerning party financing and expenditure, as well as rules applicable to audio-visual and social network campaigns and advertising.

It emerged that some States had no rules on the transparency of political donations or did not prohibit anonymous donations. Party funding from abroad was not prohibited in all countries, although some limited the amount or required it to be declared. Only about half of the Member States imposed transparency on political advertising. A minority of States imposed specific rules for social networks.

Since the organisation of political life is a national competence, the Union can only legislate on the organisation and financing of European political parties and related foundations. However, the rules that have been introduced apply in the context of European elections to national parties federated within European parties and can therefore be incorporated into national electoral rules. A regulation of 2014, which gave legal personality to the European parties, was amended in 2018 and 2019, in particular to strengthen the parties' responsibility in the use of funds and to allow sanctions to be made in the event of infringements of the rules governing the use of personal data. Latvia, for example, has introduced an application to monitor party funding and to report potential abuses to the Anti-Corruption Bureau.

As part of the "election package", the Commission has asked Member States to improve the transparency of political financing, spending and advertising. The work was partly carried out by the European Cooperation Network on Elections, which is to take stock of the situation and identify the remaining legal gaps. The Commission has already announced that, as part of the Action Plan on European Democracy, it will present a legislative proposal to increase transparency requirements by the end of 2021.

At present, Europeans lack information on the extent and mechanisms of foreign funding of political parties. Several press investigations have highlighted the links between Russia and extreme right-wing parties such as the Austrian FPÖ, the Lega in Italy and the Rassemblement National in France. Documenting circumventions of the law is one of the objectives of the European Parliament's special committee on foreign interference, which is looking, in particular, into allegations of political financing, legal or otherwise, through intermediary companies or donors using a third-country nominee. Its work could lead to more targeted means of action.

Online advertising

Away from posters and leaflets, political communication takes place via the internet and social networks, most often in a legal vacuum that allows for all kinds of abuse. Online, even more than on walls and in the street, messages come from established parties but also from multiple, more or less identified groups that can influence and manipulate the democratic debate.

The major challenge in this area is to prevent the targeting of voters through algorithms and the analysis of their personal data, in order to reach them with messages of a political nature whose origin and beneficiary are often opaque.

As the Cambridge Analytica scandal in the United Kingdom and the United States has shown, platform users’ personal data can be used for online campaigns. The content, sometimes funded by foreign, third parties, can be considered as voter manipulation, especially when it favours polarising subjects or creates the illusion that a radical subject or opinion is more widespread than it actually is.

The need for transparency concerns two types of actor: political parties and related movements and organisations that may publish online political advertising; and the digital platforms on which advertisements are broadcast.

In 2018, the Commission recommended that Member States, political parties and campaign organisations should encourage the "active disclosure" of the identity of those behind political advertising and messages, as well as the publication by parties of the spending related to the dissemination of political content. Before the European election in 2019, the Commissioner for Justice wrote to the leaders of the national parties in all Member States to encourage them to follow these recommendations. According to the Commission, parties took little action to list their advertising or disclose their spending in this area beyond the information already available on the platforms. Some explained that they depended in part on the terms of use established by the platforms, such as Facebook in 2019.

Within the framework of the Code of Good Practice against Disinformation, platforms have introduced the obligation to clearly indicate the names of parties, movements or candidates behind political content. The system was then applied in the Member States. They have also created databases of political advertisements, in which users can consult the names of the parties that have used these publications, the amounts spent and the audience reached, as well as the criteria according to which the content was posted on users' profiles.

In a report published in September 2020, the Commission highlighted the shortcomings of these measures: the collection and publication of data is not automatic and varies between platforms, with databases allowing partial searches only. In addition, the procedures for authorising political content remain incomplete, and the display of the statement indicating who is at the origin of the message disappears when the message is shared - which greatly reduces the information available to the user-voter.

The Commission, the Parliament and the Member States are calling the platforms to make the criteria for the display of political advertisements more transparent and, in particular, to open up their algorithms to researchers. The Commission's action plan will include a legislative initiative, planned for 2021, to increase transparency on paid political advertising. The ideas mentioned include the ban on sending messages that are not clearly and officially paid for or approved by the candidates, the pre-validation of messages by platforms in cooperation with electoral authorities and national media regulators, the prohibition of micro-targeting, mandatory fact-checking of political advertisements, as well as the creation of online portals, managed by electoral authorities, where information about sponsors and funding of advertisements can be found.

2. COUNTERING DISINFORMATION

In 2018, 45% of those interviewed for a Eurobarometer Survey quoted the internet as their main source of information regarding national political affairs, far behind the television (77%), but ahead of radio (39%) and newspapers (35%). The percentages were almost identical regarding European affairs.

In the information warfare waged against democracies, disinformation is the most widespread weapon, the simplest to use and the most complex to counter. Its very concept is difficult to define because it covers several realities, which need to be distinguished in order to combat them more effectively.

In 2018, in the light of the activity of the Russian media and their relays in the Member States, the Commission defined disinformation as "*information which verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm includes threats to democratic processes as well as to public goods such as Union citizens' health, environment or security.*".

But in 2020, given the development of the "infodemic"[2] making it more difficult for the public to adhere to health policies in the face of the Covid-19 pandemic, the Commission now distinguishes between disinformation and misinformation. The first is typified by "*an intention to deceive or cause public harm or to make economic gain*", whilst the second is incorrect information shared by citizens "*unknowingly with friends and family in good faith*." This distinction will help improve the development of a better response: "*well-targeted rebuttals and myth busting and media literacy initiatives*" to remedy misinformation; more direct action by public authorities, including through legislation, to combat misinformation.

Some experts, notably in France, reject this distinction, which they consider to be too simplistic, and emphasise "the manipulation of information", defined as the "*intentional, massive dissemination of false or biased news for hostile political purposes*." In their opinion the answer must especially come from civil society, which public authorities would simply support.

Since the Commission presented its first strategy against disinformation in 2018, the question regarding the role played by each of the actors - public authorities, political parties, media, citizens and civil society organisations - has been central to thought into the measures to be taken, at national or European level. But none of these measures will be effective without fully involving another actor: internet platforms.

Regulation of the platforms

Because of its open, transnational, mainly free and lightly regulated nature, the internet is the field of all battles for influence and opinion. To defend themselves, democracies must impose rules without infringing freedoms, control content without submitting to censorship, and make accountable for their actions companies that are sometimes surpassed by their omnipotence.

To date, the European approach has been to favour the self, albeit supervised, regulation of the platforms. This was reflected in the introduction in October 2018 of a Code of Practice on Disinformation, for which the signatories have to give account on a regular basis. The Code currently has sixteen signatories: nine professional associations, one communications group

[2] *The definition of the World Health Organisation, taken up by the Commission is: an excessive amount of information about a problem, which makes it difficult to identify a solution, particularly in the context of the health situation.*

and six platforms (Facebook, Twitter, Google, owner of YouTube, Mozilla, TikTok and Microsoft, owner of the LinkedIn professional network and the Bing search engine). In an assessment published in September 2020, the Commission estimates that the Code has provided a framework for a structured dialogue between businesses and public authorities, and has led to greater platform transparency, as well as real action on their part. But it stresses that, in order to be more effective, the Code should develop common definitions, clear procedures and precise commitments that are applicable to all signatories and in all Member States. It notes that researchers, the authorities and the public at large are still very much reliant on the willingness of platforms to share information and data and that it is therefore difficult to precisely assess the timeliness and impact of the platforms' actions.

Hundreds of thousands of fake accounts, managed by humans or bots, have been deleted by Facebook, YouTube and Twitter, but the data is not accessible for tracing and attribution. In addition, the limited number of signatories limits the Code's scope. Messenger and WhatsApp, which are owned by Facebook and through which false information is increasingly circulated, have not been engaged, nor has Snapchat.

The Commission's approach is therefore expected to be more offensive and committed to a logic of co-regulation, with more concrete obligations imposed on the platforms, when it presents its "Digital Services Act" on 9 December, which will complete the Action Plan on European Democracy in this area. The aim, in the words of commissioner Jourova, is both to "digitise democracy and democratise the digital world".

Economic Model

The economic model of the platforms and certain sites favours the dissemination of sensationalist and polemical content that generates traffic and commitment ("likes", comments, sharing), and therefore profit. One response is to control the placement of advertising, to reduce the promotion of content that supports disinformation and the polarisation of democratic life.

As part of the Code of Conduct, platforms have begun to limit "clickbaits" and related advertising revenues. Advertising on "impostor" sites, which masquerade as news sites to promote a political agenda, has been blocked. But the platforms have continued to allow advertising on disinformation sites, and above all, they have continued to accept so-called "advocacy" advertising on their own online services.

A research by the American research centre the Global Disinformation Index deems that yearly Google generates around 60% of the advertising revenues of sites that spread disinformation in Europe, to a total of 48 million $.

In addition to increased monitoring of the way advertisements are distributed on the web, the Commission stresses the need to improve the identification of disinformation sites, including through increased cooperation with researchers and fact checkers. This responsibility should be shared by the platforms as well as by advertisers and their operators.

At present, platforms do not provide researchers with the data that would allow them to track and analyse how content is published, promoted and shared. The European Digital Media Observatory (EDMO) was set up in June 2020 to provide researchers with the means to develop the tools and exchange networks necessary for this task. The action plan for European democracy will probably provide stronger incentives for the platforms to open up their data.

Fact Checking

In 2015, the EU set up its own team of fact-checkers, EastStratCom, devoted to countering Russian disinformation, to which two teams focusing on the Mediterranean region and the Western Balkans were added in 2017. But this "task-force", whose site EUvsDisinfo is one of the Union's main strategic communication tools, remains limited in terms of both human and budgetary means. And its methodology, with no clear criteria to qualify a publication as disinformation, and its action, which is more akin to anti-Russian counter-propaganda, are sometimes criticised and highlight the limits of the exercise.

The Rapid Alert System, a platform on which Member States and institutions can report cases of misinformation, exchange analyses and best practices and also coordinate their response is more effective. Set up in March 2019 prior to the European elections, it provided, in collaboration with the European Cooperation Network on Elections, "*a comprehensive picture of disinformation activities during the election period*". It is now mainly used to deal with disinformation about the Covid-19 and has proven its usefulness, even if a Parliament study points to a lack of standardisation of the information collated and of coordination at Member State level.

At a time when disinformation no longer comes solely from Russia, but also from China, Iran and Turkey, the fight must be waged more widely, and by all the players in the media ecosystem.

More and more media are offering fact-checking systems to try to counter the flow and influence of disinformation. The media alone, whose resources should, above all, be devoted to information according to professional and ethical criteria, rather than to the defensive and incomplete response to fake news, cannot undertake this huge task. It must also be addressed by civil society, on the basis of reliable criteria and comprehensive data. The action of both the States and the Union in this field can only be supportive, so that we do not get caught in the trap, which Vera Jourova, who grew up in communist Czechoslovakia, describes as the "Ministry of Truth".

The EDMO, with a budget of €2.5 million, brings together fact checkers, researchers and different actors to develop tools to better understand the mechanisms and effects of disinformation and its propagation, identify those responsible and organise the battle with actors in civil society. The centre has been operating since June 2020 under the aegis of the European University Institute in Florence. A second phase of the project is planned, with a budget of €9 million, which will set up a network of regional and national digital research centres. In this area, the platforms should be made more transparent to researchers and civil society.

Pluralism and the freedom of the media

The independence of the media, in compliance with the law and ethical rules, is one of the guarantees of free and undistorted debate, and also one of the bulwarks against abuse of power and arbitrariness. Economically weakened by the development of the Internet, traditional media find themselves in competition with all other types of often unprofessional, unverified and untruthful content. "*Quality information is usually behind a paywall, and propaganda is always free of charge,*" notes Christopher Wylie, who revealed the Cambridge Analytica scandal.

The fight against false information and manipulation financed by third countries or facilitated by the economic model of the Internet must therefore be balanced by providing support for rigorous information and the media that produce it. Including in the face of economic interests and moves to exercise control by the authorities, as is the case in Hungary and Poland. Media freedom and pluralism are also taken into account in the new Rule of Law Mechanism.

At present the Union is financing ten projects in support of the media and pluralism, to a total of 7 million €. Several of these projects aim to encourage investigative journalism, and another, under the aegis of Reporters Without Borders, is working on the development of a reference tool to promote transparency and reliability of the media. Two projects, led by the Centre for Pluralism and Media Freedom of the European University Institute in Florence, are dedicated to the development of a rapid response mechanism for violation of press freedom and a Media Pluralism Monitor based on predefined criteria,, which delivered its first report in July 2020.

A further €62 million is provided for in the Multi-annual Financial Framework for 2021-2027, to launch other projects in support of media and pluralism, including a database for transparency on media ownership (Media Ownership Monitor).

The Commission also plans to further support media literacy programmes for those categories of the population most exposed to manipulation, in particular young people. The aim will be to foster "critical thinking, the capacity to identify disinformation and digital skills and support empowerment of citizens as such".

Other initiatives exist outside of the Union's framework but in which Member States are involved. This is the case in particular of the Information and Democracy Partnership, initiated by the RSF whereby 38 countries, of which 20 EU Member States commit "to promoting national and international legal frameworks that are compliant and conducive to the right to freedom of opinion and expression" and ask the platforms to "*comply with the principles of transparency, accountability, and political, ideological and religious neutrality."*

The Commission will present a legislative proposal by the end of 2021 against abusive proceedings targeting journalists and rights defenders (often referred to as SLAPPs) often by individuals, companies or even governments under investigation to put pressure on the investigating parties. Maltese journalist Daphne Caruana Galizia was subject to 47 such cases at the time of her murder in 2017. In a resolution adopted in 25 November, the Parliament asks the Commission to present a legislative proposal to establish minimum standards across the EU. Many NGOs are also calling on the Commission to review the so-called Brussels 1 and Rome 2 regulations, which give complainants the possibility to choose the Member State in which they can lodge a complaint, thus allowing them to choose the strictest defamation laws and impose excessive procedural costs on the journalists concerned. The variety of proceedings, direct (defamation) or indirect (tax harassment) and of targeted people (journalists but also NGOs) nevertheless makes it difficult to address the issue by legislative means at EU level.

***

The action plan on European democracy, which extends and develops the strategy introduced since 2016-2018, is taking place in an ever-changing context. The underlying trend of mistrust towards governments and elites, compounded by events such as the Gilets Jaunes (Yellow Vest) movement in France and, even more so, the Covid-19 pandemic, has altered the origin and course of current disinformation attacks.

Manipulation and lies are no longer only spread from abroad, especially from Russia. The Member States and the Union are no longer facing just foreign interference, but also an endogenous phenomenon, even if though is still encouraged or financed from outside. The recourse to conspiracy theories and the rejection of pluralism that is apparent in the United States is also developing in Europe and cannot be tackled solely by a hybrid response or the regulation of platforms. The response is political and largely based on economic and social factors, especially in European societies that have been weakened by the pandemic.

There is a close, if not systematic, link between social dissatisfaction, mistrust of the authorities and protest voting, and susceptibility to misinformation and conspiracy theories. "*More than the gap between rich and poor regions, it is the long-term economic and industrial trajectory of places that makes a difference in the anti-system vote*", a Commission study of 2018 notes. This distrust of the system often results in a polarisation of opinions and a search for alternative information that challenges the established order. Another Commission report, dating back to 2019 and which proved correct during the Covid-19 crisis, noted that "*Relevant, synthesised, expert advice is increasingly needed but the authority of such experts is being challenged* ".

"*The principle of informing policy through evidence could be recognised as a key accompaniment to the principles of democracy and the rule of law. Similarly, the notion of independent scientific institutions as part of 'checks and balances' in democracy could be championed and defended*" advocated the report, stressing that the fight against disinformation must be strongly based on a sense of accountability on the part of the authorities in all fields - political or health, but also intellectual and media-related.

From this point of view, developments in the United States since 2016, which resulted in Donald Trump's higher than expected score on 3 November 2020 and the election to Congress of candidates who support QAnon conspiracy theories may shed some light on the situation in Europe.

On the one hand, if "fake news" is spreading through malicious sites and social networks,the extent of the mistrust thus created is strengthened by the attitude of certain media and political forces. Media such as Fox News and the attitude of the Republican Party has enabled the destabilisation of American democracy by Donald Trump. The ethical responsibility of the European media, in particular certain so-called news channels, therefore, appears essential as a complement to initiatives in favour of media independence and pluralism. Similarly, clear, strict rules regarding the way parties function and their transparency may prove to be a first bulwark in the defence of democracy.

On the other hand, Donald Trump broke a taboo - that of a democratic head of State challenging the conduct of the elections and refusing to recognise the result. When democracy is called into question by those who should be the guarantee of its proper functioning, strong institutional and civic counterbalances are still needed to prevent a major destabilisation of society. While two governments in the Union, in Hungary and Poland, already partly reject the foundations of the rule of law and have media at their disposal, the defence of checks and balances by the other Member States and the European institutions, in particular the Commission and the Court of Justice, is of additional importance.

The question of protecting the rule of law, which has long been theoretical, has emerged at a time when the Union is developing a panoply of tools, which it is preparing to strengthen, against hybrid risks and foreign interference. Given the limits of Article 7 TEU, the Commission, the Parliament and the Member States - with the exception of Hungary and Poland - are seeking to broaden their means of action.

The Rule of Law Mechanism, whose first annual report was debated for the first time by the Member States on 17 November is a first step towards systematic and preventive action. The conditionality mechanism applied to the EU budget, which is to be implemented with the new multiannual financial framework and the recovery plan, is also a tool for direct intervention in States that no longer want to follow the rules. Strategies against cyber threats, interference and disinformation, developed in parallel, provide Europe with a wide range of tools to defend its democracy. The challenge ahead is a more assertive and direct articulation of its multiple dimensions, both internal and external.

Eric Maurice
Head of the Robert Schuman Foundation's
Brussels office

Contributors to this study were:

Florian Da

Julian Parodi
Research assistants at the
Robert Schuman Foundation's Brussels office

You can read all of our publications on our site :
www.robert-schuman.eu

Publishing Director : Pascale JOANNIN

THE FONDATION ROBERT SCHUMAN, created in 1991 and acknowledged by State decree in 1992, is the main French research centre on Europe. It develops research on the European Union and its policies and promotes the content of these in France , Europe and abroad. It encourages, enriches and stimulates European debate thanks to its research, publications and the organisation of conferences. The Foundation is presided over by Mr. Jean-Dominique Giuliani.