11 January 2022 - Seul le prononcé fait foi

Report from the Bronner Commission

PRESENTATION OF THE COMMISSION OF EXPERTS

Launched by the President of the French Republic Emmanuel Macron on 29 September 2021, the Commission on Enlightenment in the Digital Age was chaired by sociologist Gérald Bronner. The commission was made up of 13 experts from different fields – historians, political analysts, legal experts, journalists, teachers, sociologists, and academic and civil society players – working together to gauge and understand the dangers to which the digital world exposes national cohesion and our democracy to improve how we respond to them.

Commission members

Gérald Bronner (Chair), specialist in cognitive sociology, is a Professor of Sociology at the University of Paris, member of the National Academy of Medicine, the Academy of Technologies, the University Institute of France and the l'Année Sociologique editorial committee. His books l'Empire des Croyances (2003), La Démocratie des Crédules (2013) and Apocalypse Cognitive (2021) focus on the formation and disappearance of collective beliefs, rumour, ideology, religion and magic, and on human cognition. These publications have played an important role in calling sociological attention to the dangers facing democracy in an age when the internet is paving the way for relativism.

Roland Cayrol is a political analyst whose work focuses on the media and its political influence, the structures and evolution of public opinion, and comparative political and electoral behaviour in France and in Europe. Founder-Director of the Institut Harris France (1977-1986), he helped found Consumer Science & Analytics, of which he was Director from 1986 to 2008. He collaborates regularly with France 5, RTL, RTBF and France 24 commenting on the news. He is Honorary Research Fellow at the Fondation Nationale des Sciences Politiques, Director and Adviser for Régions Magazine, and Director of his business consultancy firm, the Centre d'Études et d'Analyse.

Laurent Cordonier, Senior Researcher at the Fondation Descartes in Paris, studies information, disinformation and public debate in the age of the internet and social media. In 2016, he earned a PhD in Social Sciences from the University of Lausanne with which he continues to work as an external scientific collaborator. His work on conspiracy theories, the determinants of trust and the socio-cognitive mechanisms of social affiliation includes La Nature du Social – L'Apport Ignoré des Sciences Cognitives (2018).

Frédérick Douzet is a specialist in the geopolitics of cyberspace and a professor at the University of Paris 8. Director of her research laboratory (IFG Lab) and the GEODE Project – Geopolitics of the Datasphere (geode.science), she has been a member of the Defence Ethics Committee since January 2020 and sat on the Editorial Committee of the Revue Stratégique de Défense et de Sécurité Nationale in 2017. She was a member of the Global Commission on the Stability of Cyberspace (2017-2020) and chaired the Castex Chair of Cyberstrategy at the Institute for Higher National Defence Studies (IHEDN) from 2013 to 2018. She has received a number of national and international scientific awards for her research.

Rose-Marie Farinella, journalist-turned-teacher, holds workshops on media and information literacy. She developed a pedagogical scenario entitled, "News or fake news: how to tell the difference online from primary school age", which she has been teaching to ten year olds since 2014. Her work has been awarded five times, including at international level by UNESCO and the European Commission. She has co-authored a book, Des Têtes Bien Faites published by PUF, and has co-written Stop à la Manipulation with a journalist from Okapi, published in October.

Aude Favre, web journalist, launched a YouTube channel, WTFake, in 2017, specialized in exposing fake news to combat disinformation and open up the world of journalism to the public at large. She takes on major online disinformers, succeeding in having much conspiracy theory content taken down. With ten years' experience in writing documentaries and investigative journalism, she works for Zebra Production and founded the FAKE OFF association to counter fake news by training young people to view the media with a critical eye.

Jean Garrigues is a historian specialized in the political history of contemporary France. Professor Emeritus at the University of Orléans and Chairman of the Committee for Parliamentary and Political History, he has published some 30 books primarily on the institutions, actors, values, rituals and mythologies of the French Republic. Recent published work includes: Les Scandales de la République. De Panama à Benalla, 2019; La République Incarnée. De Gambetta à Macron, 2019; Les Perdants Magnifiques. De 1958 à Nos Jours, 2020; and Charles de Gaulle, l'Homme Providentiel, 2020.

Rahaf Harfoush is a Canadian digital anthropologist whose study focuses are the harmonious use of emerging technologies in business, the ethics of artificial intelligence, the digital development of our rural areas and improving cybersecurity in France. Member of the French Digital Council (CNN), she founded a digital consultancy firm called the Red Thread Institute of Digital Culture and teaches at Sciences Po Paris. Formerly, Rahaf was the Associate Director of the Technology Pioneer Program at the World Economic Forum.

Rachel Khan, legal expert, actress and author, was a high-level athlete in her childhood before studying public and international human rights law. She was Cultural Adviser to Jean-Paul Huchon, President of the Regional Council of Île-de-France from 2009 to 2015, Director of the 1000 Visages association working for access to cinema professions for young people, and is currently Co-Director of La Place, Paris's cultural centre for hip hop. In 2013, she embarked on an acting career. She has published a number of books, including an autobiographical novel published in 2016 and a 2021 essay entitled Racée, which distances itself from decolonial thinking.

Anne Muxel is a sociologist and political analyst specialized in the study of the forms of link between individuals and politics, and the democratic system in general, by analysing attitudes and behaviour (new forms of political expression, electoral behaviour, and forms of socialization and construction of political identity). She has conducted many studies on the transmission of values in intergenerational dynamics and is a renowned expert in youth studies. Senior Research Fellow in Sociology and Political Science at the National Centre for Scientific Research (CEVIPOF/Sciences Po), she is also Head of the Defence and Society domain at the French Defence Ministry's Institute for Strategic Research of the École Militaire (IRSEM).

Rudy Reichstadt is founder and CEO of Conspiracy Watch, an online press service for critical analysis of conspiracy theories, and Associate Expert at the Fondation Jean-Jaurès where he has coordinated a number of opinion polls on conspiracy beliefs in French society. He is co-author of the documentary Complotisme: les Alibis de la Terreur and author of an essay on conspiracy thinking published by Grasset. He co-presents the Complorama podcast on France Info and is also a member of the French Audiovisual Board's Online Hate Speech Observatory.

Iannis Roder is a historian specialized in the Shoah and teaches lower secondary school in Saint-Denis. He is also head of education and training at the Shoah Memorial, Director of the Fondation Jean-Jaurès Education Observatory and member of the Council of Experts on Secularism. He collaborates regularly with Le Monde's Education supplement and has written a number of books on teaching in social relegation environments and teaching the history of the Shoah, including Allons z'enfants... la République Vous Appelle in 2018 and Sortir de l'Ère Victimaire, Pour une Nouvelle Approche de la Shoah et des Crimes de Masse in 2020.

Bertrand Warusfel is Professor of Law at the University of Paris 8, lawyer at the Paris Bar and Vice-President of the French Association of Security and Defence Law (AFDSD). Combining academic research with his experience of practising law, his work is situated mainly at the cusp of public law and private law, focusing on issues of information and intangible law. With his specific expertise in public defence and security law, he also works in the areas of industrial property and new technologies and digital law.

Annette Wieviorka is a historian who has specialized in the Shoah and the history of the Jewish people in the 20th century since the 1992 publication of her thesis, Déportation et Génocide: Entre la Mémoire et l'Oubli. Professor of History, long-time teacher in China and Senior Research Fellow at the National Centre for Scientific Research (CNRS), she was a member of the Working Party on the Spoliation of Jews in France, also known as the Mattéoli Mission. Her essay L'Heure d'Exactitude: Histoire, Mémoire, Témoignage, published in 2011, reviews the memory of the Shoah and its key developments, showing the extent to which the "era of the witness" forms a memorial and historiographic turning point.

Contents

Executive Summary

The digital revolution is radically changing our lifestyles, our economies and our social practices. It is also transforming how we relate to information. Today, we are confronted with an unprecedented mass of available information and a profusion of competing points of view, which are expressed unfiltered by a process that is hard for internet and social media users to understand. This saturation and deregulation of the online information market is putting a severe strain on our epistemic vigilance capabilities, making us more vulnerable to false information.

Disinformation, misinformation, fake news, conspiracy theories… Any number of terms are being used to refer to the false news that circulates online with the potential to influence our attitudes and our behaviour, but also our world view, at the risk of the emergence of endless parallel realities and the disappearance of the common epistemic space required for exchanges of opinions, ideas and values, in short, for democracy. Some of this disinformation, as we shall see, is the product of real foreign cyber-interference by players seeking to manipulate our opinions, incite violence and hatred, or destabilize our society for strategic ends.

Our commission was tasked first with presenting an overview of the state of knowledge on information disorders in the digital age and the democratic disruption they cause, and second with making recommendations to address them. Any endeavour to counter disinformation runs the risk of undermining essential values of our democracy such as freedom of expression, opinion and information. Our commission has worked with a view to preserving these freedoms. Consequently, our recommendations do not aim to eradicate information disorders – which would clearly be neither possible nor desirable – but to limit the propagation of content detrimental to democracy, deter malicious behaviour, punish illicit practices, enhance risk prevention and increase user vigilance.

Understanding the psychosocial mechanisms (Chapter I) that make us vulnerable to false information sheds light on the levers that can be used to limit its effects. False information forms a minority of the information content circulating on the internet and social media and we are generally capable of telling it apart from reliable information. However, some of it manages to make an impression and is therefore potentially harmful to both the individuals concerned and society. The social media set-up whereby information is lost in a mass of entertainment content in no way encourages cognitive vigilance, a key shield against gullibility. Hence our recommendation to develop the teaching of critical thinking (R27 & R29). Academic research shows that an analytical mind capable of resisting some of our immediate intuitions is a key faculty to distinguish truth from falsehood, especially on the internet and social media. We also recommend investing in scientific research (R1) and pressing the digital platforms to open up their data to researchers (R20), since there are still gaps in our knowledge of the prevalence of online disinformation (particularly in France), of its effects and the mechanisms by which it affects individuals. Lastly, we would like to draw attention to the fact that countering disinformation in our country can only be effective if media and institutions, as epistemic authorities, work to reforge a bond of trust with all citizens.

Some algorithmic dynamics (Chapter II), without being responsible for our beliefs and behaviour, do influence them. We focused on three of these phenomena in particular: algorithmic curation, which refers to how algorithms organize the rank and frequency of appearance of information based on its attention-drawing capacity; social calibration, or how social media alters the perception of the representativeness and popularity of certain points of view; and asymmetric influence, enabling the prevalence of certain extreme minority views. We therefore propose a series of measures to improve the design of user interfaces (R2) and counter popularity bias (R3) in order to move away from an algorithmic logic based on a strictly commercial model; introduce accountability for influencers (R4) with high online visibility; promote expertise (R5) and encourage dialogue between platforms and scientists (R6) to better reflect the true state of knowledge; and, lastly, guard against the risk of over-moderation (R7) by means of closer analysis of user reports.

One of the main drivers of disinformation is profit. A study of the fake news economy (Chapter III) shows that programmatic advertising represents a substantial source of income for disinformation makers, often without the knowledge of the companies using agencies to broadcast their campaigns and whose advertisements are found on websites propagating hateful content, conspiracy theories or content liable to disturb the public peace. We therefore propose making programmatic advertising players accountable (R8). Crowdfunding platforms and monetized YouTube channels can also be used to collect funds. Hence the proposal to encourage good practices

by platforms to prevent indirect participation in the funding of projects involving incitement to hatred or the propagation of disinformation (R9). Lastly, general press websites frequently use sponsored links to clickbait websites often peddling false information, especially regarding health issues.

The other major driver of disinformation is strategic competition. The hardening of the global geopolitical climate has given rise to an ongoing confrontational dynamic that is a feature of conflict in the digital age. This dynamic is associated with foreign cyber-interference operations (Chapter IV). It is behind the emergence of increasingly hybrid threats that have disrupted the presidential campaigns in the United States since 2016 and have also affected France. Hence the importance of analysing past disinformation campaigns in order to protect the integrity of future electoral processes (R10). These information manoeuvres have internationalized with the health crisis in the last two years, calling for the creation of a European-level crisis management mechanism (R14). These threats cover a wide range of players and modi operandi, complicating the ability to understand, detect and prevent them. Their analysis calls for researchers to have access to platform data (R20) and structured data sharing by players studying these phenomena (R11). International law can do little in this area. This is why we recommend stringent cooperation with the platforms (R15) and the creation of a working group at the OECD in a spirit of co-regulation. Lastly, the militarization of cyberspace has brought with it a proliferation of information operations. In the ultra-dynamic universe of cyberspace shared by all players, substantial interactions between the civilian, economic and military worlds blur the notions of domestic/foreign theatre and produce effects that in turn fuel the threat. For these reasons, the commission recommends consulting the Defence Ethics Committee regarding the French doctrine for countering cyber influence operations (R13) and creating an interministerial digital governance mechanism that covers the many interactions specific to this shared space (R12).

Turning to law and cyberspace (Chapter V), a study of the legal provisions that might be useful to prevent and punish the different forms of disinformation (in the sense of the malicious dissemination of false news) supports refraining from amending or replacing the current Article 27 of the 1881 Press Law (R16 & R17). However, the penal sanction could be rounded out by a mechanism to engage the civil liability of persons maliciously disseminating false news potentially harmful to others. Such civil liability could be proportionate to the level of virality of dissemination and the online popularity of its perpetrator (R18). Court case lead-times, in particular to obtain a final decision on the merits of a case, remain largely inadequate for the required rapid response to the viral circulation of certain false news stories. The French Audiovisual Board (CSA), becoming the Audiovisual and Digital Communications Regulatory Authority (ARCOM) on 1 January 2022, will be tasked with oversight of compliance by the platforms with their obligations to rapidly remove certain serious illegal content and already has a more general responsibility to combat the dissemination of false news. A minimum requirement in our opinion is a formal ARCOM reporting procedure open to all citizens (R19) to inform ARCOM of difficulties encountered with obtaining a platform's action in response to a complaint and cases of unilateral removal of content that did not justify such a radical measure so that the platform can take appropriate action. Lastly, with respect to the European Digital Services Act (DSA), the commission proposes making platforms accountable by explicitly including in the DSA a provision recognising that any false news capable of disturbing public order constitutes reprehensible content (R21), establishing an external expert body to cooperate with the platforms (R22), and creating a co-regulation regime among platforms, regulators and civil society (R23).

Lastly, the best response to information disorders that are so complicated to stop is probably individual moderation, since everyone is now an operator on the online information market. Media and information literacy (MIL) and the teaching of critical thinking (Chapter VI) pave the way to help us assess this cacophony of information with a new-found independence of judgement. The national education system has a key role to play in this, yet initiatives in this area are disparate. Hence the need to create an interministerial unit focused on the development of critical thinking and MIL for all (R24). A better understanding of the cognitive difficulties experienced by students would also improve the design of educational content (R25). Awareness of the importance of these areas could be raised by making the development of critical thinking and MIL an Issue of National Interest (R26), systematically teaching critical thinking and MIL in schools (R27), and outreach with education authorities in educational establishments and local education authorities as well as with local elected officials, local authorities and chief librarians (R28). Lastly, it is important to create a continuum between time spent at school, university, the world of culture, the world of work and civil society (R29). Training in intellectual vigilance should ultimately be a shared goal for any society that values the life blood of the legacy of the Age of Enlightenment and the hopes it kindled.

To conclude, forward-looking thinking provides insights into new issues that will arise in the future. The metaverse concept, for example, points in the direction of a universe in which we will be immersed in an increasing conflation of real and virtual worlds. This calls for ethical thinking (R30).

The singular purpose of our report was to urgently consider solutions to curb a problem exacerbated, if not transformed by the digital age. This work in no way excuses us from the collective thinking required in tandem to consider the type of society and democracy we wish to build in this evolving digital world.

Glossary

False information (or misinformation): False or inaccurate information content, whether or not deliberately created and disseminated to deceive.

In this report, the term 'false information' is also used as a generic term to refer to all misinformation

In this report, the term "false information" is also used as a generic term to refer to all misinformation, disinformation, fake news, hyperpartisan news, conspiracy theories and clickbait.

Disinformation: False or inaccurate information content or set of information content created with the deliberate intention to deceive.

Fake news: Fabricated or highly inaccurate information content published on the internet and presented in such a way that it can pass as legitimate news for the general public.

Hyperpartisan news: Information content covering events that really happened, but with a very strong partisan bias making it potentially misleading.

Clickbait: Sensationalized, often false, inaccurate or misleading information content designed solely to attract the attention of internet users in order to generate traffic on the page hosting the content.

Conspiracy theory: A narrative that tends to erroneously explain an event or phenomenon, when other explanations are more plausible, as the result of covert action by a generally small group of individuals in pursuit of a legally or morally reprehensible goal. In addition to displaying a preference for intentionalist explanations, a conspiracy theory generally disputes, without any real evidence, the mainstream explanation for a given set of circumstances and accuses those in whose interest it would actually or supposedly be.

Foreign cyber-interference: Digital intervention by a state or agents acting on behalf of a state in the politics of another state.
This definition varies across platforms and institutions. The definition given by Viginum is: "Structured, coordinated operations by foreign actors designed to propagate patently misleading and hostile content via the digital platforms for the purpose of undermining the fundamental interests of the Nation."

Foreign cyber influence: Information operation conducted in cyberspace (internet and social media) by a foreign actor or group of foreign actors for the purpose of influence.

Introduction

In his essay "What Is Enlightenment?" (1784), the philosopher Immanuel Kant rallied his contemporaries with a famous phrase, "Dare to know! Have the courage to use your own understanding! That is the motto of enlightenment." This motto bore the hope of a century: the coming advent, driven by progress with education and the availability of information, of an enlightened society founded on reason and knowledge.
The early 21st century does not appear to have entirely fulfilled this hope, and this "motto of enlightenment" warrants re-examination in the age of the digital revolution. The game changer it represents is radically changing our lifestyles, our economies and our social practices. It is also raising profound questions regarding the notions of power and democracy. It has come about against the backdrop of a rise in populism, the exacerbation of religious conflicts and geopolitical tensions between leading powers, popular mistrust of elites and institutions, and tremendous challenges for the future of humanity such as climate change and pandemics.
The digital revolution offers an unprecedented opportunity to rethink the frames of representative democracy by capitalizing on the complex dynamic systems with the capacity, among others, for the massive spread of knowledge, an unprecedented level of social interaction and greater citizen participation. It also offers new forms of governance and collective intelligence, albeit mostly as yet to be invented.
We are still at the dawn of this revolution, the scale of which we are only just starting to gauge. It requires us to define our ambitions for a changing world in which we are still struggling to project ourselves collectively. Yet we already need to rise to the many challenges that this revolution presents.

Today's information chaos
One of the most striking phenomena of today's world is the massive deregulation of the information market, sped by the development of the internet and illustrated by at least two significant phenomena: first, the extraordinary mass of available information unprecedented in the history of humanity, and second, the fact that everyone can add their own world view to what has become a burgeoning market.
This has all sorts of implications, but the most obvious is the emergence of widespread competition among all the intellectual models that purport to describe the world, from the crudest to the most sophisticated. Today, anyone with a social media account can directly contradict a professor from the National Academy of Medicine on the issue of vaccines, for example. The former may even attract a larger audience than the latter. Can this profusion of competing points of view, unranked by the expertise and knowledge of those who voice them, bring to pass this world of knowledge to which our ancestors aspired in the Age of Enlightenment? Can we hope that the most well-argued and soundly demonstrated statements will prevail thanks to this free competition over products of gullibility in the form of superstitions, urban legends and other conspiracy theories?
Even a cursory glance at the current situation shows that to be doubtful. Although the internet and social media provide access to an unparalleled volume of reliable knowledge and information, they have also opened the door to the sharing of a large amount of false information with repercussions that rarely remain confined to social

media. The storming of the Capitol in the United States in 2021 is a prime example of just how conspiracy theories, such as those freely circulating on social media among Donald Trump's supporters, can trigger political violence. Online disinformation during the pandemic has exacerbated fears about vaccines, leading sometimes, in France, to the vandalization of vaccination centres. A certain number of criminal acts have been fomented, again in France, and sometimes even acted upon in the name of conspiracy theories disseminated on the internet. For example, there was the kidnapping of young Mia by individuals taking their cue from Rémy Daillet's conspiracy theories. And then there were the violent acts planned by members of an extreme right-wing conspiracy movement against the health minister, a Masonic lodge and vaccination centres, which were thwarted by the General Directorate for Internal Security (DGSI).

It would obviously be naive to think that such events are purely the product of the workings of the internet and social media. Firstly, manipulation of facts and information was around well before the internet. Secondly, online disinformation is not the root of the problem, but a symptom of and catalyst for our societies' ills, albeit often exacerbating them. As such, conspiracy theories are characteristic of those make-believe narratives that have always accompanied the history of human societies, feeding on mistrust of authorities, institutions and media or on the feeling of anomie. In France, as elsewhere, imaginations have been fired by tales of conspiracy throughout our contemporary history, and well before the appearance of the internet. Theories of Jewish, Jesuit and Free Mason conspiracies polluted the public debate in the 19th century and through a good part of the 20th century. Their common trait was to propose a simplistic reading of society at the time, supposedly threatened by a powerful secret organization aspiring to rule the world. Raul Girardet sees this "golden age of the plot" as the expression of a profound social malaise, of collective angst in the face of a fast-changing world striding towards democracy, industrial revolution and capitalism. This analysis, placed in the current context, would apply in terms of the appeal of these oversimplistic, vindictive tales of conspiracy in an era of globalization with the feeling of dispossession it implies, the feeling of being cut off from political decisions and the feeling of a loss of control over our environment.

It is therefore important to note that conspiracy theories also thrive on (un)favourable social conditions. Studies find a higher average level of conspiracy thinking in countries where people feel socially threatened (high unemployment rate, for example) and where the institutions and authorities are perceived as untrustworthy. If we add that some governments are not always above suspicion of endeavours to manipulate public opinion by disseminating false information, it becomes clear that many factors are in place to ensure conspiracy theories meet with a certain amount of success.

These make-believe tales offer to make political sense of the world. That is why they can paradoxically be socializers and mobilizers for some people to find new social coalitions, new social integrations and even a new way of doing politics. These new socialization frameworks influence attitudes and behaviour in terms of personal and social life, but also world views. For example, it has been shown that exposure to conspiracy theories discourages democratic participation by voting in elections, fuels prejudice, if not violence against certain population groups, and can lead to the rejection of scientific consensus on numerous issues such as climate change and the efficacy of vaccines.

The success of these narratives is therefore deeply rooted in certain social realities largely independent of the digital world. However, conspiracy beliefs aside, some internet properties increase the harmful potential of false information. In particular, the ubiquitous, instant nature of social media is such that harmful content can be posted and disseminated at one and the same time as the event to which it relates. For example, all sorts of conspiracy theories about the Notre-Dame de Paris Cathedral fire proliferated over social media as the fire was still raging. Some of these theories, highly shared and commented on, quickly acquired such visibility that they had to be debunked in the media, obliged to root out disinformation.

Lastly, digital tools greatly increase the strength of players, especially state actors, seeking to interfere in an electoral process, manipulate public opinion, mislead the adversary, discredit political dissidents, cheat victims or harass vulnerable persons. Government agents, criminals and even private individuals can cheaply make content go artificially viral, cover their tracks and their identity, and put together fake images and fake videos that are virtually impossible to tell apart from real images and videos in order to harm, make a profit, advance their interests or destabilize democratic societies.

Curbing the propagation of disinformation

Given the potential harms of disinformation, it seems advisable to take steps to check its propagation on the internet. However, any move to actively intervene in this information market, especially if it is political in origin, raises the question of the preservation of freedoms, especially the freedom of opinion that is a pillar of the Declaration of the Rights of Man and of the Citizen. Yet the current information cacophony in no way guarantees the full expression of this freedom. Information on the internet is actually pre-curated by algorithms that sometimes appear to escape their very creators and that have become our masters when they were supposed to be our servants. For example, 120,000 years of videos are watched every day on YouTube, with 70% of viewings prompted by the recommendation made by the platform's artificial intelligence. This is just one of many examples of the editorial curating power of the leading web operators. Information is hence organized in a deregulated digital world: it is managed by algorithms behind the scenes, consequently capable of influencing our opinions without our knowledge.

Furthermore, this type of curation does not always give precedence to the sincerest or most well-argued information. For example, a 2019 study found that the majority of searches (54%) on the term 'climate' on

YouTube directed internet users to climate change denial videos. Although social media is becoming an increasingly important source of news, especially for the younger generations, all the surveys show that it is also perceived as the least reliable source of news. This paradox is somewhat reminiscent of Ovid: "Video meliora proboque, deteriora sequor" (I see the right and approve it, and yet the wrong pursue).
Neither is social media conducive to dispassionate democratic debate. An analysis of Twitter, for example, showed that adding a single word of indignation to a given tweet increased its expected retweet rate by 17%. The observation for Facebook is no brighter, since the famous social network was found to be algorithmically favouring posts prompting angry reactions over those expressing temperance and approval. This does much to make social media platforms places of conflictual expression rather than spaces for sharing and reasoned discussion of points of view. There is also evidence that social media's recommendation algorithms can play a role in radicalization. An internal Facebook report, for example, stated that two-thirds of individuals who had joined an extremist group on the social network did so following a recommendation from the algorithm.
Algorithms hence shape how we relate to information in a way that often remains too opaque for both users and legislators. Yet one of the first pillars of resilience for our societies is understanding how information is produced and disseminated, but also how users take it on board and share it.

Strengthening society's resilience

We know, when it comes to disinformation and conspiracy theories, that prevention is more effective than correction. A study has shown that the first impression given by false information often endures, even when the individual given that information learns that it is incorrect. Debunking that information is therefore not enough to erase the impression made, which subsequently leads the individual to have an erroneous interpretation of any new information on the same subject. Understandably, the instant nature of social media gives a certain competitive advantage to false information, quickly generated and disseminated, over reliable information that takes time to be checked and cross-checked.
Another aspect of the way the internet works can cultivate credulity. Psychologists have long since shown that, in many situations, we tend to prefer new information that adheres to our established beliefs over that which might contradict them (especially when the beliefs in question tie in with our values). This is the famous 'confirmation bias', also called a 'congeniality bias' by researchers. This confirmation bias hence produces a tendency to search essentially for information that will reinforce our points of view. The internet facilitates the expression of this bias insofar as the quantity of available information is such that finding personally satisfactory information is just a few clicks away, irrespective of whether it equates with reality.
This does not mean that we are less exposed to divergent points of view on the internet than in offline life, but that we can easily find any number of elements on the internet to support our beliefs, including when those beliefs run counter to the state of knowledge on a given subject. Research has shown that such a belief reinforcement mechanism is definitely at work on the internet when it comes to conspiracy theories, and that it can even prompt certain individuals concerned to surround themselves on social media with people who share their conspiracy beliefs, thereby forming 'echo chambers' within which positions gradually radicalize.
The saturated state of the online information market places a severe strain on our epistemic vigilance capabilities. We are exposed to so much content that we can spend very little time considering the credibility of each piece of content, making us more susceptible to false information. Online repetition of erroneous information can moreover strengthen its power of persuasion, since the more we encounter the same argument, the same post or the same tweet, the greater the impression that it is true.
Consequently, there is a risk of individuals finding themselves in parallel realities where consensus on facts empirically documented by information experts and theories supported by experiments and scientific literature is no longer possible.

The need for a common epistemic space

With the availability of false information on the internet and the polarization of social media, the very possibility of a common epistemic and debating space is under threat, i.e. a world in which it is possible to discuss, contradict and revise a judgement, a world where points of view can differ, but are always commensurable. Donald Trump, with his 89 million followers on Twitter before he was barred from the social network, epitomises this threat. There are American citizens who live in the same society in the United States, but not necessarily in the same world. This is precisely how the statements of former Trump campaign manager, Kellyanne Conway, can be interpreted. She championed the idea that more people had attended Trump's inauguration ceremony than for any president before him, even though the facts clearly proved her wrong. She might have admitted that she was mistaken, but chose instead to refer to "alternative facts", as if the same reality could be given two contradictory interpretations of equal value.
This statement made official the breakdown of a common debating space in the United States. Disagreement is normal in a democracy, but debate presupposes that the arguments exchanged are commensurable, and it is this fundamental principle that is under threat today. Although France is not the United States, a recent Stanford University study nevertheless shows that the level of 'affective polarization' in our country – that is the extent to which citizens feel hostile to other political parties than toward their own – has risen steadily over the last 40 years to stand today at one of the highest levels of the twelve OECD countries studied.
The existence of a common epistemic space is a cornerstone of social life, and democracy in particular. Without such a space, no collective problem can find acceptable solutions despite the differences of opinion. The problems we face are considerable – such as climate change – but a prerequisite is needed to solve them: the

ability to draw on collective intelligence.
It is clear that the internet is a tremendous advance whereby information and knowledge can circulate at an unprecedented speed and on an unprecedented scale, just as it makes public debate among citizens possible by transcending geographical distances. Yet the downside is that this technology also facilitates the dissemination of false and misleading information, with sometimes very real consequences, and could drive forward the polarization of our society rather than a well-argued exchange of points of view. It is on this question of such digital disruption of democracy that the President of the French Republic asked our commission to reflect.

The commission's objectives and working methods
This commission was tasked with taking stock of the research and knowledge built up on the subject by consulting scientific literature and existing reports and consulting in person or in writing researchers and public and private players connected with the digital world. It had a very short timeframe in which to do so (100 days) and, in these circumstances, immediately ruled out any aspiration to comprehensiveness.
The question is obviously not new to us, since institutions such as the WHO, UN, Council of Europe and many others have published analyses of the phenomenon. Discussions are also underway at the Council of the European Union and the European Parliament regarding the new European Digital Services Act (DSA) intended to guarantee a safe and responsible online environment.
The members of our commission felt that the subject of the digital disruption of democracy could be analytically broken down into seven sub-topics, which structure this report.
The first sub-topic concerns the psychosocial mechanisms that can make us vulnerable to false information and diminish our ability to identify it as inaccurate or misleading. What does science have to say about the variables involved in these phenomena?
The second sub-topic looks into the possibilities of altering the online information market's algorithmic models. Is it possible to change certain visibility and virality rules governing this market to mitigate its negative effects?
The third sub-topic explores the economic drivers of the dissemination of false information and hatred on line. The ecosystem of information on the internet is driven by an attention economy dependent on the leading digital companies (social media, search engines, online video platforms, etc.). These companies are not always opposed to making the efforts required to regulate this market's negative externalities, but some of their economic interests (mainly based on user engagement) do not necessarily coincide with a concern for the quality of the information disseminated in the digital world.
The other major threat to the stability of democracy comes from foreign cyber-interference, by state or private players, which serves their interests in the digital world. These manoeuvres are documented and discussed by this report's fourth sub-topic.
The fifth sub-topic answers some of the previous questions by looking into the question of the regulation of this market by law. This question is both sensitive and key. It is on the agenda of all thinking on the digital disruption of democracy – and, in particular, when this report was written, addressed by the preparatory work for the European Digital Services Act (DSA).
The best response to information disorder driven by the digital world is probably individual moderation, since everyone is now an operator on the online information market. It is therefore the focus of the sixth sub-topic to present the state of knowledge on MIL (media and information literacy) and the teaching of critical thinking. How can we assess information, suspend judgement and counter specious reasoning? The skills needed for good practices in this area can be proposed to all levels and at all moments of our intellectual education. The national education system is a key institution in this respect to give all our fellow citizens the tools they need to recover their independence of judgement in this cacophony of information. Training in intellectual vigilance should also be a shared goal for any society cherishing the legacy and hopes of the Age of Enlightenment. The traditional media channels (press, radio and television) have a key role to play in assisting with this effort since they remain the main source of content production. However, they are not spared the negative externalities of this deregulation of the market. The way in which a certain digital model contaminates journalists' work and restricts their editorial freedom warrants analysis.
The seventh sub-topic, by way of a conclusion to this report, raises the question of a new form of digital citizenship. The informed involvement of each and every one of our fellow citizens is one of the avenues considered to offset the prevalence of the most radical and conflictual assertions on social media. If certain ideas are gaining online visibility disproportionate to their representativeness, it is because they are championed (especially in the case of the anti-vaccine movements) by communities more motivated than others to voice their point of view. This asymmetry should naturally not be met with censorship, but with thinking on everyone's involvement in this new citizen space that the digital worlds have become.
These worlds also offer the ideal technical conditions to create spaces for new democratic debate. It remains for us to consider the forms these spaces could take to avert certain observed pitfalls and ensure that they voice the wisdom of the crowd rather than the wisdom of the loud.

I
The Psychosocial Mechanisms of Disinformation

A large part of what we know, or think we know, does not come from our own senses and experience, but from what we are told. Right from childhood, we are constantly exposed to information imparted by the people

around us – parents, friends, teachers, etc. – and the media brings us news on the state of the world that we could not obtain on our own. Human beings hence find themselves in a state of profound epistemic dependence on their fellow beings.

Although this situation gives us the wherewithal to significantly broaden our knowledge compared with the knowledge we could have on our own, it also exposes us to the risk of being inadvertently misled, if not deliberately deceived by others. The existence of such a risk does not prevent us from adopting a form of trust by default in the information conveyed. Research has shown that we tend on average to accept rather than reject incoming information. We are even capable of believing inaccurate information that should be recognized as such based on prior knowledge.

Our tendency to take as true incoming information is not in itself irrational. Under normal circumstances, most of the information conveyed by members of our entourage is true – this is generally ordinary everyday information without any major epistemic implications. Statistically, it is therefore rational to exhibit a bias to accept incoming information and to only reject what is highly unlikely or obviously false (which is precisely what we do most of the time). However, in a world where a great deal of information now comes to us from the internet and social media, does such baseline trust by default remain reasonable? Here again, it all depends on the relative proportion of true and false found online.

I.1. Representation of false information on the internet

To date, academic research has been unable to accurately estimate the percentage of disinformation on social media and the internet in general. Such an estimate would actually be extremely hard to produce, with findings fluctuating enormously over time and by the linguistic regions and countries considered. We know, for example, that election periods in democratic countries are particularly propitious moments for the online dissemination of false information.

A study of the 2016 American presidential election illustrates this well. Its authors searched for the main fake news articles circulating on the internet before the election. They identified 115 pro-Donald Trump (or anti-Hillary Clinton) articles and 41 pro-Clinton (or anti-Trump) articles. The researchers then measured their dissemination on Facebook in the three months before the election. They found that the pro-Trump fake news items were shared on the social media platform 30.3 million times over this period and the pro-Clinton articles were shared 7.6 million times.

Although these figures are impressive, fake news forms a minority of all the news content to which American internet users are exposed, including during election periods. This is shown by studies that have looked into the sources of information consulted by Americans: the websites known to publish dubious content make up a small proportion of people's online information diets. Data on internet users' actual media consumption is thin on the ground in France. However, a recent study by the Fondation Descartes shows that, on the whole, the majority of French people also get their information from reliable websites.

The authors of this study recorded for 30 consecutive days the internet news information activity of 2,372 adults residing in France, selected to make up a representative panel of the French population. It was found that 39% of these people had accessed an unreliable source of information at least once over the period. However, on average, they had spent just 11% of their daily online news information time on these sources (corresponding to 0.4% of their total connected time). This average obviously varied across individuals, with some of them having accessed unreliable sources more regularly and for longer periods of time than others.

It should be noted that, by the authors' own admission, this study based mainly on the frequentation of news information and disinformation websites underestimates the individuals' exposure to false news information circulating on social media. The same holds true for the studies conducted in the United States using a similar methodology. Therefore, although it can be said that the French access websites publishing fake news less on the whole than traditional media websites, we do not have the data to estimate our fellow citizens' average level of exposure to false information on social media.

Nevertheless, we do know that, in France, fake news regularly benefits from a certain virality on social media and that social media users are more likely than others to access unreliable information websites. It can be concluded from this fact, also observed in the United States, that social media constitutes a significant gateway to disinformation, even though fake news probably forms a minority of all the news content circulating on it.

I.2. Effects of disinformation

Mass disinformation is not necessary when it comes to negatively influencing people exposed to false information: a small number of false information stories can have measurable effects on individuals' beliefs and attitudes. This is illustrated by a study conducted in the United Kingdom and the United States to measure the impact of COVID-19 misinformation on vaccination intent.

In early September 2020, the authors of this study exposed 3,000 UK respondents and as many US respondents to five pieces of misinformation about COVID-19 vaccines. These were misleading messages circulating a great deal on social media at the time. At the same time, 1,000 participants in each of the two countries were exposed to five pieces of factual information about COVID-19 vaccines. The researchers measured participant intent to receive a vaccine before and after having been exposed to the five pieces of misinformation (treatment groups of 3,000 individuals in each country) and the five pieces of factual information (control groups of 1,000 individuals in each country).

Before treatment, 54.1% of UK respondents and 42.5% of US respondents reported that they would 'definitely' accept a COVID-19 vaccine. Following exposure to the five pieces of misinformation about COVID-

definitely" accept a COVID-19 vaccine. Following exposure to the five pieces of misinformation about COVID-19 vaccines, these proportions fell to 48.6% and 39.8% respectively in the treatment groups, representing a decrease of around 6 percentage points compared with the control groups after exposure to the five pieces of factual information. These findings clearly show that exposure to a small number of misleading social media posts is enough to negatively influence (at least in the short term) the way individuals feel about vaccination.
As anyone can see from the infodemic that has accompanied the COVID-19 crisis since it started, and which appears to be particularly virulent in France, online disinformation can take a range of forms, including more or less elaborate and detailed conspiracy theories. Even before this infodemic, however, researchers were already studying the negative effects of conspiracy theories on individuals' beliefs and attitudes: studies prior to the pandemic had hence already established that exposure to conspiracy theories about vaccines reduced intentions to get vaccinated or to have one's children vaccinated.
Conspiracy theories circulating on social media challenge the scientific consensus on many other subjects than just vaccines. For example, some of them maintain, contrary to what scientists, governments and the media would have us believe, that climate change is not an established fact or is not caused by human activity. It has been shown that exposure to these types of conspiracy theories reduces intent to adopt pro-climate behaviour.
More generally, exposure to conspiracy theories of all kinds fosters mistrust of authorities and institutions, discourages democratic participation by voting, and fuels negative prejudice, if not hostile attitudes to various population groups. Even more worrying is that there are strong suspicions that certain conspiracy theories play a role in radicalization in extremist groups (such as Islamist and extreme right-wing groups) and hence facilitate these groups' transitions to violent or terrorist acts. A number of recent studies have moreover observed the existence of a significant statistical link between subscribing to COVID-19 conspiracy theories and displaying intent to commit violent acts.
Evidently, disinformation can have all sorts of deleterious effects on individuals and society. What do we know about the psychosocial mechanisms that enable false information to exert its harmful effects on people's minds?

I.3. Discerning truth from falsehood online

Disinformation is often political in nature in that it is designed to discredit members of opposing parties or their positions or, conversely, to promote the camp behind the disinformation. In the light of this, it has been put that subconscious motivated reasoning might make us particularly susceptible to taking as true political information that is actually false or hyperpartisan: we might want to believe information that is consistent with our own political ideology, irrespective of its veracity. However, recent data has cast some doubt on this hypothesis.
Although individuals do tend to give more credence to information that aligns with their political position, studies nonetheless show that, "Politics does not trump truth." On average, true but politically incompatible information is believed more than politically consistent fake news. Therefore, partisan bias is not alone enough to lend credit to certain political disinformation encountered on the internet and social media.
The reason why individuals may trust in false information probably has less to do with a motivation to believe than with a straightforward inability to identify it as false. We generally evaluate the veracity of new information based on our previous knowledge. Information that agrees or aligns with our knowledge will be easily accepted whereas we will tend to reject information that contradicts our knowledge. So it comes as no surprise that we should be more at risk of taking fake news for truth when we lack knowledge or have erroneous knowledge of the subject in question. For example, one study has found that people with a low level of scientific knowledge are more likely than others to believe false information on COVID-19.
However, knowledge does not systematically make people impervious to the risk of giving credence to false information, which can make an impression on individuals by taking advantage of their lack of vigilance, distraction or even a certain form of lazy thinking. Weighing up and analysing new information before accepting or rejecting it requires greater cognitive effort than trusting in our first impression of it. Yet we generally behave as 'cognitive misers', preferring to minimize our mental efforts.
Nevertheless, there are differences across individuals in the propensity to settle or not for following solely our intuition with respect to a new piece of information or data. Research into how human beings reason shows that we are all equipped with two information processing systems: the first is fast and intuitive, while the second is slower and more deliberative, and liable to make us reconsider an assessment made by the first. However, some people defined as 'reflective' or 'analytic' are more inclined than others defined as 'intuitive' to call on their second information processing system and consequently revise, if necessary, a first mistaken impression. These differences in types of thinking across individuals can be measured by cognitive tests.
A series of empirical studies using these tests shows that people who are more 'reflective' are better at discerning fake news from reliable information and are less likely to believe fake news. One experimental study has moreover found that if individual vigilance with respect to new information is constrained, making individuals trust solely in their intuition, then their ability to identify fake news diminishes. It would therefore appear that credulity often results from a lack of cognitive vigilance. And social media most certainly does not encourage such vigilance insofar as serious information content often gets lost among the entertainment content. In addition, a great deal of fake news is shared on social media in the form of images without hyperlinks to any source whatsoever, which makes it hard for users to check the soundness of the facts put forward.
The social media set-up is also deemed to negatively impact on the tendency of its users to themselves share

false information on it. Individuals may decide to share information on social media that they do not consider to be true when asked to assess that information. This behaviour may have less to do with intent to mislead others than with distraction and the quest for 'likes'. Two experimental studies have indeed found that subtly shifting attention to the concept of the accuracy of the content significantly reduces individuals' intentions to share information that they are capable of recognizing as false.

In addition to the effects of a lack of previous knowledge and lack of vigilance, the scientific literature has identified other mechanisms liable to blur the distinction between true and false information in people's minds, particularly on the internet and social media. One of them is the statement repetition effect. Numerous studies have shown that the more a piece of information – true or false – is repeated to an individual, the more that individual will tend to believe that it is true. It has been shown that merely one prior exposure to content is sufficient to be able to increase its credibility when it is seen a second time.

This phenomenon is reinforced by the fact that although people generally remember the message in question, they tend to forget the source. So false information that had initially appeared dubious due to its unreliable source may subsequently appear to be true when encountered again in a different context; it will be seen as all the more true since it has already been encountered before. Social media probably cultivates this mechanism, since some fake news stories that circulate on social media are shared by many accounts and can therefore reappear regularly on users' 'walls' or news 'feeds' – a process amplified by engagement algorithms whose work consists of presenting users with similar content to that with which they have already interacted. More insidiously, fact-checking operations could also contribute to making fake news appear credible via a repetition effect by lending visibility to the very fake news they are tackling.

Lastly, mistrust of media, institutions and government is a factor correlated as much with the online frequentation of unreliable information sources as with adherence to conspiracy theories. This is probably due to the fact that this mistrust leads the people concerned to search for information among 'alternative' sources to traditional media, which they consider to be biased, corrupt or government mouthpieces. These information sources give pride of place to conspiracy theories, which can then potentially win over individuals who distrust the media and authorities precisely because they challenge the explanations of historical events and news presented by the media and institutional players. These individuals' distrust is then reinforced by their exposure to such conspiracy narratives.

We also know that people with feelings or fears of vulnerability, stigmatization or downward social mobility are particularly at risk of succumbing to conspiracy theories. If they are, it is most probably because conspiracy theories give them an interpretation of the world that can make sense of their situation and point the finger at an unequivocal cause of the social injustices and threats of which they feel they are victim.

I.4. Conclusion

In view of the research findings, cognitive vigilance and the development of analytic thinking are probably the best individual shields against false information. The most promising course of action to counter the deleterious effects of disinformation would therefore appear to be to develop the teaching of critical thinking and media and information literacy (MIL) (R27 & R29). Critical thinking must be taught using teaching materials whose effectiveness has been scientifically assessed. This calls for scientific procedures and a research structure to be set up to carry out these assessments (R24). We will come back to these recommendations in Chapter 6 of this report on critical thinking and MIL.

In addition, scientific research on the prevalence of online disinformation, its effects and the mechanisms by which it affects individuals needs to be supported and developed in our country (R1). Data on France is too thin on the ground in the scientific literature and the conclusions of studies based on data from other countries – mainly the United States – cannot necessarily be transposed to our country.

France, via the European Union, should also require the digital platforms to give researchers broader access to their data so that they can study the different aspects of online disinformation phenomena. The terms of access could be those proposed by the European Commission in the Digital Services Act currently being negotiated (R20).

To conclude, it is important to point out that countering disinformation in our country cannot be achieved solely by measures to encourage individuals to exercise vigilance on the internet or measures to improve the use of algorithms on social media. Underlying these measures is the bond of trust between citizens and the media and institutions that needs to be reforged.

II
Algorithmic Dynamics

Recent events – the Facebook Papers Affair comes to mind in particular – remind us of the role that the digital environment and algorithms can play in the spread of false information and radicalization. This environment, as discussed in the previous chapter, cannot be considered to be the only factor of democratic disruption, but the way in which it alters and shapes opinions warrants its discussion in a chapter of this report.

We will first focus on how the influence of algorithmic effects should not be exaggerated, before going on to show that the particularities of the digital world nevertheless expose democracy to new risks and explaining why further measures are urgently needed to address them. To conclude, we will see that, despite the limits of their actions, the platforms are not totally passive in the face of the dangers they engender.

II.1. The real f

II.1. The need for nuance

Scientific knowledge about how algorithms fashion our beliefs and behaviour, especially politically speaking, has not yet stabilized and sometimes puts forward seemingly contradictory data and arguments. Some research, for example, has shown that social media tends to confine us to ideological echo chambers in which we encounter essentially arguments in line with our own opinions. However, other studies posit that contradiction is customary on social media and that interactions with individuals with different opinions are generally more frequent on social media than is often believed: a situation liable to generate fierce exchanges among internet users can even lead to the expression of hate speech. Similarly, some studies find that social media exposes its users to a wider range of information sources than those they consult offline. However, this point is somewhat misleading. In fact, the supply of traditional media on social media (in the form of sharing articles, for example) is fragmented by nature. Those who consume press information by this means generally only read one article, and are less likely to read the entire newspaper than those who access it by other means. Consequently, it will often be the subjects rather than the media that dominate digital curation. In view of this, such diversity can be artificial since the reading will be of preferential subjects processed by transverse media rather of a real diversity of subjects.

On the subject of the news, if there is one promise that the internet has clearly not kept, it is to qualitatively expand supply as much as demand. An observation of the flows of exchanges of online news reveals that the cognitive market for online news is driven by short, sudden and massive concentrated attention effects. This temporal concentration of attention is what some refer to as buzz. This becomes most tangible when observing on a large scale how our collective attention is drawn to a story that will make news for a brief moment before steering us to another, which will not have any longer life expectancy. Three computer scientists analysed 90 million articles published on mainstream media sites and blogs over a three-month period. Their analysis of news lifecycles shows how fierce competition is for attention and how fleeting – days at most – our collective peak of attraction to a topic. Their model confirms as much the massive spread of sources (1.6 million) as the convergence of topics. In other words, the huge increase in the number of sources and the volume of information flows driven by the development of the internet has not reversed the trend towards the homogenization of the news topics that draw public attention en masse.

It is often said that the internet and social media are rife with false information, an idea that is nowhere near as cut-and-dried as it seems, as seen in the previous chapter: a number of studies conducted in both the United States and France point out that disinformation probably forms a minority of the total volume of news accessed on social media and the internet in general. Yet we should guard against concluding from this finding that online disinformation is not a problem. The studies are silent on the question of the threshold at which tangible disinformation effects can be observed, focusing instead on the proportion of the population exposed to this information. Moreover, although fake news sites do not always have the direct influence they are alleged to have, one study shows that traditional media tend to take up certain stories from these dubious sources when they are compatible with their partisan leanings, thereby actively participating in their coverage.

Just as online disinformation should not be overestimated, we should guard against exaggerating its influence or major social events. Political polarization, for example, can only be partially explained by the online context, and the scientific literature offers up no definite answer to the question of the role that social media and the internet play in it. Furthermore, the impact of disinformation on election results also calls for sounder scientific evidence. It is most probable that multiple factors are involved in these phenomena and therefore that their explanation cannot be found solely in the influence of the digital world and the disorder it creates.

More importantly, we are not incompetent when it comes to detecting false information and, on the whole, we find it less plausible than authentic news. We possess the resources we need to guard against some of the dangers of false news, a point that is developed in the chapter on critical thinking and media and information literacy (MIL).

II.2. Algorithmic disruption

Caution is therefore called for when addressing the correlation between algorithms and platform configurations and the negative social impacts of which they are accused. Nevertheless, digital networks do present particularities that exacerbate these harmful effects in an unprecedented manner. First of all, the size of the digital networks, the number of contacts possible on them and the potential visibility of the messages circulated have all reached record levels. Second, spatial proximity between individuals in offline interactions generally encourages them to avoid incivility or invective: social media does not offer this conciliatory characteristic. Online discussion often encourages intolerance and what is termed online disinhibition. Third, the multitude of information sources tends to foster a splintering of perceptions of reality, as mentioned in the introduction to this report.

The main effects of the algorithmic revolution on the organization of information can be subdivided into three areas, which will be explored in turn in the rest of this chapter:

- Algorithmic curation: how algorithms manage both the rank and frequency of appearance of information based on its attention-drawing capacity;
- Social calibration: how social media alters the perception of the representativeness and popularity of certain points of view;
- Asymmetric influence: the fact that the internet enables motivated individuals to gain online visibility that far exceeds their representativeness, hence enabling the prevalence of certain extreme narratives that benefit from online conditions to emerge from their space of radicalism and disseminate their arguments.

One of the roles of the media is to curate the news, i.e. to select and rank the news for its audience. There is such a mass of data available that it is impossible for us to take it all in at a single glance, especially since the development of the internet. In the case of a traditional newspaper, for example, it is the editorial staff and editor-in-chief who choose and organize the information they deem relevant, ideally in keeping with the profession's ethical standards. Everyone knows that an article on the front page, taking up more columns or with photos, will have more visibility. Platforms likewise curate information. However, they do so using an algorithmic process that remains opaque for users. When a search is made on Google or YouTube, or when a Facebook feed is opened, some information is positioned toward the top of the page and therefore has more chance of being selected by the user.

Search requests sent by users to their search engine may well accentuate their biases, especially their political biases, since artificial intelligence is sensitive to individuals' partisan preferences as revealed by the keywords they use. These searches can alter our perceptions of certain topics, especially since the top results returned by a search are cognitively prevalent. The discreet information curation work done by algorithms could even, in certain circumstances, influence users' voting preferences.

What we may think is free choice is hence sometimes the product of digital architectures influencing our behaviour. This architectural question prompts us to consider, in addition to the algorithmic dynamic, the question of the algorithm's actual design. In recent years, the unsettling term 'dark patterns' has come to crystallize concerns about the ability of a platform's design to trick the regularities of our cognitive system, even to the point of leading us to make decisions in spite of ourselves.

The question of dark patterns (interfaces designed to manipulate or mislead users) and whether they can be regulated calls for a focus on user interface design. Over and above the question of any malicious intent, the choice of design necessarily has an influence on the behaviour of online platform users. The design defines the context in which individuals exercise their decision-making power. This is why Cass Sunstein proposes seeing the designers as 'choice architects', thereby highlighting the responsibility they have.

This power to steer individuals' choices raises important social, ethical and political questions, including the question of the collection of personal data. Do these design practices comply with our societies' democratic norms? Can we consider, for example, that informed consent to share personal data has been given if the opt-out option is hard to access or see? Is it tolerable that some of our cognitive biases are manipulated to capture our attention and make a profit? In general, how can individuals' choices really constitute personal decisions in this context?

It cannot be left to the platforms alone to answer these questions, since they extend beyond a strictly technical or legal frame and call for the engagement of the regulator and civil society. We need to set to work now on a thorough analytic grid of design practices and their repercussions on individuals and society. This task, which will serve to establish what qualifies as an abusive or deceptive design practice, will require the expertise and knowledge of both design professionals and human and social sciences specialists (psychologists, sociologists and philosophers).

Given that user interfaces are bound to evolve and gain increasing importance in our social relations, it is vital to develop enduring means to analyse and regulate their influence. We also need to encourage strengthening regulator expertise by making it standard procedure to call on experts in the interrelation between design, psychology and ethics. In this, discussion should be cultivated with the research world to ensure responsive and effective public action.

Recommendation:

Launch discussions, with a view to regulation, on the importance of the issue of user interface design (R2).

The purpose behind the design of these digital architectures is generally purely economic: the aim is for online platforms to hold the attention of their users for as long as possible to be able to convert it into financial resources using paid advertising spaces, or to prompt users to share more, and ultimately monetizable, information than is strictly necessary to provide the service they are offering. They will use all manner of tactics to achieve this end, as long as they are not unlawful. The platforms hence constantly adjust to our behaviour and the traces we leave in the digital world. These adjustments are designed to satisfy our natural cognitive inclinations, drawing us deeper and deeper into these online meanders until we end up stuck in a bubble.

The problem is that this bubble is not only harmful to individuals – which would be reason enough in itself for concern – but that it also generates negative collective effects. Mark Zuckerberg himself acknowledged in 2018 that engagement-based ranking algorithms could be dangerous. Facebook, for example, observed that an 'angry' emoji generally prompted more engagement with a social media post than a mere 'like'. To make the most of this engagement effect, the company then calibrated its algorithm to assign five times more weight to these expressions of indignation, thereby giving the content concerned maximum visibility in the news feeds. In this light, it should come as no surprise to find that affective polarization effects are observed.

Likewise, the shift to boost MSI (Meaningful Social Interactions) was supposed to correct the overweighting of the most viral content by introducing a 'network well-being' criterion measuring the probability of a post being liked and reshared. Yet this change intended to foster interactions with a small social circle had the perverse effect of boosting the most extreme content. This could be explained by the fact that people generally pay little attention to reshared content unless it comes from their five closest friends or unless the content is extreme enough to attract their attention. Nevertheless, their discovery of this perverse effect did not make Facebook

deactivate MSI.
These remarks obviously apply to other digital platforms, including YouTube, which also seeks to maximize the time its users spend on the platform by means of a personalized recommendation algorithm. A study by ex-Google engineer Guillaume Chaslot showed that the YouTube algorithm steered people towards increasingly extreme content, hence paving the way for radicalization. This algorithm has been deemed responsible for part of the spread of the German and American far-right.

II.3. Disruption to social calibration
The cognitive mechanisms of coalition and social affiliation are deeply engrained in our nature. Our nascent opinion about a given issue can hence be largely influenced by the visibility of the opinion that others have expressed on the subject, in particular if they are part of our network of friends or appear to be socially similar to us. The digitization of social relations and the proliferation of information content producers are greatly disrupting our social calibration, i.e. the reasoned access we have to other people's opinions. Altering our perception of the prevalence of others' opinions can have at least two repercussions.
First, it places a premium on content that digital metrics have made popular. The purpose of the algorithms behind information visibility is to maximize user attention and engagement rather than to propose reliable, balanced sources. They do so, for example, by boosting the content that receives the most comments, 'likes' or shares. This may seem reasonable based on the principle that collective intelligence is more likely to come to sound, well-argued points of view. Yet it does nothing of the sort due to the existence of what is known as popularity bias, which, as research has shown, reduces the overall quality of the information. At a certain level of popularity, dissemination of an article, for example, will constantly grow: the more a person is exposed to an idea, the greater the chances that they will embrace it and end up sharing it in turn. Putting information through the digital metric grinder therefore affects our social calibration.
Recommendation:
Offer users a more accurate snapshot of the network and the true prevalence of opinions by deactivating algorithmic curation and popularity metrics by default, and by focusing on metrics enabling users to gauge the content's epistemic quality (notably its sharing history) (R3).

Second, we tend to associate on social media (as in real life) with like-minded people who share our points of view and to distance ourselves from those who we feel are too dissimilar (for example, by unfriending or blocking them). This homophilic tendency is commonplace, but it is facilitated on social media, since individuals' points of view as well as some of their psychological and social characteristics (tastes, preferences, group membership, etc.) are often more immediately visible and measurable on social media than in offline life. By gradually surrounding ourselves unwittingly with like-minded people who share our opinions and show it by 'liking' our posts and publishing like-minded content, we risk getting the impression that our ideas are very much in the majority. This means that we can easily forget that our online environment is in no way representative of the population as a whole. Hence, epistemic communities can form within which false senses of consensus emerge and where opinions are mutually reinforced.

II.4. Asymmetric influences and radicalization
Very early on, studies showed that a small number of motivated individuals on the internet could influence opinion. The internet has driven the emergence of what some call, in reference to Columbia School theory, 'super opinion leaders'. The colossal audiences that some internet users attract place a question mark over the idea that the internet can 'democratize democracy': in reality, on the virtual public square, some have much more voice than others. In keeping with the winner-takes-all rationale, their audience is increased by the system of recommendation used by the platforms. This would not necessarily be problematic if this system promoting the most visible digital influencers had not been shown to be a key factor in the viral propagation of false information. These influencers are not necessarily producers or providers of false information, but when they succumb to the temptation to share that information, they become the main causes of disinformation cascades.
Recommendation:
Encourage platforms to more carefully moderate influencers to make them accountable. The consequences of information produced or disseminated by accounts with high online visibility are potentially greater than for accounts with small audiences (R4 + see also the Law and Cyberspace chapter).

In general, the motivation of players on this cognitive market can give them visibility in excess of their representativeness. For better or for worse, some motivated groups have shown that they are capable of cornering a disproportionate share of online visibility. On Facebook, for example, anti-vaccine movements managed – before the pandemic – to take up a position of dominance over pro-vaccine groups. Some analyses propose scaling these observations, showing that the tendency on social media is to render moderates all but invisible to the benefit of extreme opinions.
Recommendations:
- Enhance the visibility of specialized knowledge by promoting experts' accounts and amplifying their content (on subjects relating to their field of expertise) (R5).
- For certain firmly-established subjects, prevent algorithmic ranking from misleading the public with regard to the true state of knowledge. To this end, encourage dialogue among platforms and scientific institutions to ensure that any prevailing consensus is reflected in the visibility granted to the various opinions. (R6)

ensure that any prevailing consensus is reflected in the visibility granted to the various opinions. (R6)

Social media aside, the rankings proposed by search engines such as Google can be influenced by the more or less coordinated activity of certain militant networks. For example, web spamming can alter a search engine's ranking of results. A well-identified technique used by some movements – especially white supremacists – is to exploit data voids. These refer to search engine queries that turn up few results and are therefore easily appropriated by coordinated manipulation. Such is the case, for example, with a breaking news situation (such as a terrorist attack) that has not yet generated many articles. If a group motivated by opinion manipulation moves fast, it can, at least temporarily, divert early searches to ideologized versions of the event.
Action by such motivated groups can play a role in producing epistemic bubbles, digital spaces within which critical thinking struggles to win through. In these virtual communities, false information can be spread without encountering much contradiction. There is documented evidence that they fuel extremism and affective polarization. These groups may also take more or less coordinated action to mass report accounts at odds with their ideological battle and secure suspensions or bans.
Recommendation:
Guard against the risk of over-moderation through closer analysis of user reports (mass reporting) (R7).

II.5. Conclusion
The leading digital platforms are not entirely unresponsive to the danger of false information. Facebook has promoted banners encouraging its users to exercise vigilance when it comes to discussions of vaccines or COVID-19. The online video platform YouTube has also officially made it known that it does not allow "content on YouTube if it includes harmful misinformation about currently approved and administered vaccines on [...] vaccine safety (content alleging that vaccines cause chronic side effects [...]), efficacy of vaccines (content claiming that vaccines do not reduce transmission or contraction of disease), ingredients in vaccines (content misrepresenting the substances contained in vaccines)." More than 130,000 videos have been removed for this reason in the last year. Twitter has added a pop-up inviting users to read content before sharing a link. A full 59% of people who share stories on Twitter have only read the headline and nothing of the content. Audrey Herblin-Stoop, Twitter's External Communication & Public Affairs director, reports that this measure has indeed resulted in a large number of users deciding not to retweet an article that they have not read. TikTok's representatives also reported measures of this kind when they were interviewed by the commission.
For years now, leading digital platforms have been members of the Global Network Initiative, which commits them to the defence of human rights and transparency. In 2010, Google launched an annual transparency report, focusing in particular on the thorny issue of content and profile removal (YouTube and Google), followed by Twitter in 2012, Facebook in 2013 and many others since.
The most radical response by the digital companies in this area is the closure of accounts considered as problematic, a measure now known as 'deplatforming'. Is this an effective way of countering disinformation? In the United States, members of QAnon, white supremacists and conspiracy theorists have all paid the price for this policy. In France, the same has happened to figures such as Alain Soral and Dieudonné on both Facebook and YouTube where they had large audiences. A growing body of scientific literature on 'deplatforming' suggests that it is effective on the whole. Obviously, those who are banned from the leading networks seek to migrate to alternative platforms, such as Telegram and Parler, but everywhere that such migration has been observed, the shift has resulted in a fragmentation of the communities, thereby weakening them, even though there is a risk of their greater radicalization on these platforms. Whatever the measurements used to assess the effectiveness of 'deplatforming', the observation is always one of a reduction in the influence of the banned individuals. For example, 11,000 deleted YouTube accounts that migrated to the BitChute platform experienced a sharp decline in audience figures.
Elsewhere, an analysis of 49 million tweets found that banning the accounts of conspiracy theorists' such as Alex Jones significantly reduced the toxicity of their support on social media.
Social media only has drawing power if users do not feel they are on their own. On this point, Donald Trump's ban from social media should give pause for thought. The former president remains a prominent figure in the United States and his Twitter account was followed by 89 million people. Given that, his intention to create his own social media platform, Truth Social, in 2022 is no trifling matter. Its design will closely resemble Twitter, but there is a risk of seeing moderation rules so permissive as to power an unprecedented boom in expressions of radicalism. After using social media as a means of disintermediation between the voters and himself, he now claims to be standing up to the "tyranny of Big Tech" and could well win his bet. Of all the 'post-truth' society players, Donald Trump has the largest capital of social visibility, which is precisely what could enable him to break the ceiling that no other alternative platform has managed to break to date. Should he succeed, the divide between the two sides of American society could widen further.

III
The Fake News Economy

The circulation of fake news and conspiracy theory content is amplified by the unprecedented visibility and virality that disinformation and misinformation have acquired in recent years. Fake news is responsible for

considerable costs that weigh on the entire economy.
In public health, the United States spends an estimated $9 billion a year on treating people suffering from vaccine-preventable diseases such as measles. Most of this cost concerns unvaccinated individuals influenced by content hostile to vaccines, as highlighted by a study by economist, Professor Roberto Cavazos at the University of Baltimore published by cybersecurity firm CHEQ. Professor Cavazos estimates that fake news cost the global economy nearly $78 billion in 2019. The study finds that fake news inflicts damage on global stock markets, resulting in estimated losses of up to 0.05% of total market value or $39 billion in monetary terms. The study also estimates that expenditure by large corporations on reputation management and debunking false claims made against them could grow to over $9.5 billion by 2022.
Even though these figures are estimates, they show that disinformation substantially weakens our economies. This state of affairs is only made possible by the earnings that disinformation manages to generate, through multiple channels: the sale of products (conspiracy theory books and DVDs, clothing, electric equipment, cryptocurrencies, etc.) and services (training courses, insurance policies, etc.), collection of donations, crowdfunding and advertising revenue, which is reportedly a lucrative resource for many disinformation media outlets. As Roberto Cavazos puts it, "The proliferation of fake news is related to the development of an ultra-lucrative, ultra-competitive online advertising market. All things extreme and sensationalistic attract clicks and thereby inflate earnings. So myriads of unidentified media mass-produce content, and this false information leads to poor decision-making."

III.1. Programmatic advertising: a substantial source of earnings for disinformation
One of the main ways for website and blog publishers to generate earnings on line is to monetize their audience by integrating advertising space into their platforms in the form of banners, skyscrapers (vertical format) and background formats.
There are two types of digital advertising services: classic advertising, which consists of buying advertising space, and 'programmatic' advertising.
Programmatic advertising is popular with many businesses as a way of reaching a large number of targeted internet users at a relatively low cost in financial and human resources terms. NewsGuard, the news site credibility rating company, estimates that programmatic advertising represents, "more than 85% of all digital advertising, totaling $80 billion in annual spending in the U.S. in 2020."
Its originality resides in the fact that the campaigns do not display an advertisement in a specific advertising space (a given website) to which all visitors are equally exposed for a given period of time, but is tailored to a specific target audience. To do so, programmatic advertising uses an auction system. This automates advertising space buying for advertisers (the bidding process takes on average 120 to 150 milliseconds from start to finish for a total of approximately 15 to 20 billion bids per day in France) while targeting users based on their interests, age, gender or even geographic location. These criteria are algorithmically inferred from personal data and the digital footprints left by users from their online activities. As defined by Decree 2017-159 of 9 February 2017 on digital advertising services, these campaigns are, "based on real-time service buying methods for non-guaranteed spaces, mainly by means of auction mechanisms, for which the determining criteria are the internet user's profile and optimization of message performance."
However, it has emerged in recent years that this programmatic advertising is frequently to be found on websites propagating patently and often repeatedly hate speech, conspiracy thinking, content prejudicial to human dignity and gender equality, incitement to sectarian excesses, blatant disinformation and content liable to disturb the public peace. The advertising revenue that these websites make from this advertising represents a considerable financial boon that perpetuates information pollution.
Programmatic advertising service providers are currently asked to inform the advertiser of, "all measures taken [...] to avoid the dissemination of advertising messages on unlawful media or media in dissemination universes notified by the advertiser as being detrimental to its brand image and reputation." However, nothing obliges them to provide the full list of websites where their advertisements may be found.
For example, the advertising budgets of a cancer research foundation ended up effectively contributing to the earnings of a website proposing 'alternative' treatments for cancer. Likewise, a leading NGO in environmental protection found itself taking part in funding a website featuring climate change denial content. And tech giants allocate budgets to combat false information while contributing with the other hand, mainly through their 'Ad Tech' services, to funding some of the websites that propagate false information.
In addition to the aberrations to which such a system can lead, it also enables a myriad of toxic websites to thrive on capturing a virtually unlimited source of earnings. NewsGuard reports that many are the purveyors of disinformation, "which would not have financial support without this unintended advertising."
Yet this type of advertising campaign is growing. A study by Integral Ad Science (IAS) found that 52% of advertisers said that half or more of their advertising budget is now transacted programmatically. A full 80% declared that this type of advertising accounted for one-third or more of their expenditure. Some 42% of the advertisers felt that programmatic advertising lacked transparency, preventing them from knowing where their campaigns are being shown or the identity of those they are consequently helping to remunerate.
In most cases, it appears that brands use the services of an advertising agency to configure and disseminate their online campaigns. These agencies regularly propose using brand safety tools to their clients to prevent their advertisements from being displayed on websites that could damage their brand image (pornographic sites, sites selling arms, etc.). Yet the websites featuring damaging and harmful content, classified in a sort of

'grey' area (content that is not patently unlawful and has not formed the subject of a court ruling), are largely absent from these brand safety tools, to the extent that many brands find themselves paying for brand safety and inadvertently funding conspiracy theory or misleading content regardless.

A NewsGuard study conducted in association with the American media measurement and analytics company Comscore states that the misinformation industry is, "booming–with $2.6 billion in estimated advertising revenue being sent to publishers of misinformation and disinformation each year by programmatic advertisers, including hundreds of millions in revenue supporting false health claims, anti-vaccine myths, election misinformation, partisan propaganda, and other forms of false news."

Some 'super-disinformers', with traffic in the region of millions of users per month, attract a large number of advertisers. For example, the American conspiracy theory website The Gateway Pundit (approximately 30 million visits per month) is estimated to have made the equivalent of €200,000 per month on average from programmatic advertising in 2020.

Advertisers display a range of attitudes to this problem. Some brands make it a point of honour not to appear on any disinformation websites. Others appear to be unaware of the problem, having not been informed of it. Some advertisers do not wish to know whether their advertisements end up on disinformation websites. A last category of advertisers are well aware of the fact that they fund disinformation websites and accept it.

The Sleeping Giants France collective, which uses awareness-raising methods developed in North America here in France, alerts advertisers to the fact that their advertisements are being served – most often without the advertisers' consent – on sites that are extremist and/or dedicated to massive dissemination of fake news and conspiracy theories. In its four years of activity, the collective has received nearly 2,000 positive responses to its alerts from advertisers and advertising agencies. Several thousand more advertisers are thought to have withdrawn, in that same period, their commercials from these toxic sites, albeit without making any public announcement on the issue.

In 2018 a firm specialized in solutions for combating online disinformation contacted more than 200 advertisers affected by the issue of funding toxic players via programmatic advertising (including supermarket, mobile phone and automobile industry brands, most of which are endowed with corporate social responsibility, or CSR, departments) in order to offer them a free audit of their advertising campaigns. Less than 10% of the companies contacted agreed to follow through.

No description of the programmatic advertising sector landscape would be complete without mention of its ad tech (advertising technology) providers who are, among the sector's various players, the ones who enable the placement of programmatic advertising such as Google Ads (leader in the field), Xandr (AT&T subsidiary), Taboola and Criteo. Each of these ad tech companies takes a commission whenever a user is exposed to one of its commercials.

In March 2020, the American NGO, Global Disinformation Index (GDI), which aims to defund disinformation sites, estimated that 76 million dollars in advertising revenue is being "inadvertently" spent in the European Union on such sites by brands such as Amazon Prime, Burger King, Mercedes Benz, Samsung, Spotify and Volvo. In September 2019, GDI estimated that 235 million dollars in advertising revenue was paid to the 20,000 disinformation sites on their global database, through programmatic advertising. According to several interviewees, the most high-risk disinformation websites – regardless of country –are actually relatively few in number: approximately 1200. Therefore, if ad tech companies like Google and Criteo were to decide to withdraw their business with these sites, the societal impact would be significant. It is worth noting that these companies have rules (publisher policies) that largely prohibit monetisation of such websites, but these policies are all too often ignored. In March 2021, NewsGuard launched its Responsible Advertising for News Segments (RANS) label, which takes into account not only the non-funding of disinformation, but also the reorientation of this advertising expenditure toward websites displaying quality journalism. Label awardees are required to undergo regular audits (at least two audits per year) to verify, in particular, that the inclusion and exclusion lists used by the advertisers are indeed up to date. Indeed, any hitherto reliable website may, in just a short lapse of time, become a toxic platform offering disinformation content.

III.2. The indirect traffic generated from mainstream media websites toward "clickbait" websites

Several mainstream websites rely partly on recommendation modules with sponsored links from the likes of Outbrain (which sometimes also appears as SmartFeed) for their income. Mainstream news sites frequently resort to this kind of arrangement. Yet these sponsored links may lead to clickbait websites offering at times dubious content, especially on health-related issues.

Screenshot from the France Culture website (9 April 2019).

As we can see, a suspect article, stemming from an internet site (Santé Nature Innovation) which, according the French daily Le Monde, "sometimes disseminates material that is false, exaggerated or unsubstantiated, for example regarding miracle foods or the supposed dangers of vaccination, refuted by the overwhelming majority of specialists," came to feature alongside recommended sponsored content via a Smartfeed module embedded in the France Culture webpage.

It is thus clear that achieving a healthier digital environment, especially for the mainstream press, is going to require disincentives for redirecting users to clickbait sites.

The commission holds that the different programmatic advertising stakeholders need to be made accountable

by implementing the following Recommendations (R9):

- Promote responsible corporate advertising investment by encouraging advertisers, advertising sales entities, advertising agencies and, above all, ad tech companies to use dynamic 'website exclusion and inclusion lists', such as those created, for example, by NewsGuard, the Global Disinformation Index and Storyzy.
- Engage in dialogue with ad tech providers so that they utilise this system, which would significantly help dry up the fake news economy.
- Ensure that any public administrations or enterprises using programmatic advertising exhibit exemplary practices through the widespread recourse to dynamic inclusion lists.
- Envisage requiring all firms engaged in CSR to undergo thorough independent annual audits of their programmatic advertising campaigns, making it possible to establish exhaustive lists the web addresses (URLs) of the sites where their campaigns are served, and make these lists publicly available.
- Encourage certification entities such as AFNOR to duly consider, when issuing 'responsible' labels, the issue of funding disinformation, by mandating regular audits for firms applying for such labels.
- Envisage requiring ad tech companies to alert their customers to the risk of funding toxic sites should the latter fail to use dynamic exclusion lists.
- Recommend that mainstream media websites ban any sponsored links in their advertising spaces that send users to disinformation clickbait sites. Encourage them to cease working with advertising companies that associate them with such sponsored links.

MONETISATING A YOUTUBE CHANNEL

Disinformation or conspiracy theorist content is rife on the online video platform YouTube. Some of this content is published by channels that are monetised through advertising.

The agreement enabling creators to generate income on YouTube is called the YouTube Partner Program. There are certain eligibility requirements for this programme: having at least 1,000 subscribers and 4,000 viewing hours, and not being the recipient of an "active" (ongoing) warning for having breached the platform's rules on content.

Once a channel is monetised, YouTube reserves the right to take down content that contravenes its rules and to issue a warning, without sanctions, to the channel holder concerned by e-mail. If such breaches continue, the channel holder may receive a warning. The accumulation of three warnings within a 90-day period leads to the channel's termination. In exceptional cases (serious violation, even if only once, of the platform's community guidelines), YouTube reserves the discretionary right to terminate the user's channel.

III.3. Feeding disinformation through crowdfunding

Crowdfunding platforms enable companies, associations or individuals to raise funds in their community to finance a kitty, a project or an event. They are remunerated either by commission or by soliciting voluntary donations (as is the case for the HelloAsso).

There are different types of platforms: those that rely on recurrent donations, such as Tipeee and Patreon; platforms centred on a 'money pot' like Leetchi and HelloAsso; and finally participative financing platforms that offer a reward system, such as Ulule and KissKissBankBank.

Some of these platforms have received media attention for having offered or for continuing to offer fundraising solutions to spurious projects. Others have established in-house procedures aiming to avoid funding projects that could be compromised with content involving disinformation, conspiracy theories or hate speech.

The commission is of the belief that the good practices deployed by crowdfunding platforms ought to be encouraged (R9):

- Envisage imposing an obligation on crowdfunding platforms to indicate explicitly to their users all measures implemented to avoid indirect participation in the funding of projects involving hate speech or the propagation of disinformation.
- Urge crowdfunding platforms to utilise the services of website credibility rating companies or to obtain a recognized label that includes the issue of avoiding funding toxic sites. This incentive could be in the form of tax relief for these companies on their taxable profits.

III.4. Public funding for online media spreading disinformation

There are some press titles that, despite being accused on a regular basis of peddling fake news or hate speech, are nevertheless recognized as providing 'political and general interest' (PGI) content. This PGI qualification is granted by France's Joint Commission for Publications and Press Agencies (known as the CPPAP) and creates entitlement to benefit from France's special economic treatment of the press.

This arrangement includes preferential postage costs and tax rates (notably, the ultra-low VAT rate of 2.1%) and access to subsidies for titles with PGI status. Registration with the CPPAP thus confers upon the press title the right to indirect taxpayer funding.

The CPPAP is an independent body with equal representation from the administration (Ministries of Culture and Finance in particular) and representatives of the profession. The Ministry of Culture runs the CPPAP secretariat.

France's Post and Electronic Communications Code and its General Tax Code both set forth conditions regarding the respect for human dignity as a prerequisite for eligibility for these special economic arrangements for the press. As a matter of principle, therefore, no publication would be eligible if it denies the Holocaust, incites racial hatred or xenophobia, or violates human dignity".
In her report submitted to the Minister of Culture, the head of the CPPAP, Laurence Franceschini, proposes various regulatory changes concerning both the printed press and online press services, with tighter restrictions for the more heavily subsidized publications with PGI status. Discussions on reforming the regulations that govern eligibility for the special press regime are currently underway with professional press organisations and journalists' trade unions. The reform may give the CPPAP greater leverage for controlling access to the special economic regime for the press.

IV
Foreign interference and influence

In less than two decades, cyberspace has become a primary arena for confrontation and strategic competition among States, and even, for France as for other countries, a new military domain. Information operations now feature prominently in digital combatants' arsenal. Information warfare is far from being a novel concept; indeed, it is an inherent part of military strategy, whether it be convincing people of a war's legitimacy, countering an adversary's influence or devising ruses to trick the enemy and gain a tactical advantage. But the shift to the digital world raises new problems that pose a threat to democracy. An illustration of this is the decision not to allow electronic voting for French citizens casting their ballot from abroad during the 2017 presidential election, because of Russian interference operations in the 2016 American electoral campaign.
The reasons for these upheavals and the difficulties curbing them are many and varied. On the one hand, the changing global geopolitical context has led to a mindset of ongoing confrontation which is now a feature of the antagonism of the digital era. This logic has led to the emergence of increasingly hybrid threats, involving a wide variety of stakeholders and modi operandi, which complicates the ability to understand, detect and prevent them. On the other hand, the digital world is dual by nature and ultra-dynamic. Consequently, considerable interactions between the civilian, economic and military worlds blur the notions of domestic/foreign theatre and produce effects that in turn fuel the threat.

IV.1. The emergence of increasingly hybrid threats
As of the late 2000s, the world's major powers made cyberspace a strategic priority and invested massively in their offensive and defensive cyber warfare capacities so as to assert their strength and ward off a menace that was initially perceived as essentially technical and military in nature. Yet the wave of jihadist attacks in the mid-2010s awoke them to a double realization. Firstly, the cyber threat could be information-based. Expert use of social media by Islamic State to spread its propaganda, push radicalization, raise finance and organize departures for Syria came as a complete strategic surprise, although precedents were observable in Iraq as of 2004. But above all, European States realized how little power they had to force the platforms, who were initially in denial as to their own responsibility, to prevent the spread of such content.
Despite this experience, the interference operations undertaken by Russia during the 2016 presidential election caught completely off guard not only the American administration, but also the platforms, and added a layer of complexity to the problem. By combining cyber-attacks (electoral registers, hijacking Democrat messaging services), the publication of e-mails on Wikileaks, amplification (botnets, troll farms) of polarizing messages (gun control, police violence, racism) on social media or the use of targeted advertisements, with more conventional forms of influence (State media, human networks), these operations heralded the emergence of a threat that is more hybrid, protean; difficult to apprehend and even more difficult to curtail.
These practices have also targeted France, such as with the Macron e-mail leaks just prior to the presidential run-off election in 2017. They have furthermore been exported to places of strategic interest, notably in Africa where France was the target of smear campaigns. The commission therefore recommends protecting the integrity of the electoral process through closer cooperation with platforms and researchers (R10).
Lastly, these information-related manoeuvres have become internationalized over the last two years with the increasingly strained strategic context and the heightened geopolitical tensions related to the health crisis. Public declarations and publications have indicated influence operations run by Russia, Turkey, Iran and even China.
With a view to avoiding any escalation of conflicts and to addressing emergency situations, the commission recommends the creation, at the European Union level, of a crisis management mechanism and exercises for information-related threats (R14).
Hybrid threats allow for the creation of ambiguity in a geopolitical context where the line between peacetime and wartime is becoming increasingly blurred, giving rise to a grey area that could more accurately be characterized by notions of competition, contestation and confrontation. Such threats also feature a growing diversity of stakeholders – State and non-State –, modi operandi and effects produced, which generates widespread semantic confusion and makes it difficult to understand the phenomena and the appropriate response thereto.

IV.2. A wide variety of stakeholders, strategies and modi operandi
The range of terms used (disinformation, information manipulation, info-ops or information warfare, cyber

The range of terms used (disinformation, information manipulation, info-ops or information warfare, cyber influence) attests not only to this semantic confusion, but also to the challenges of studying, understanding and describing these phenomena. Research has boomed over the last five years but is hampered by difficulties in accessing platforms' data and by biases stemming from the vagaries of open-source data collection, limited by technical and legal constraints designed to safeguard users' rights. Some studies consequently rely on data sets, the quality of which varies, which platforms agree to share. But these only offer, at best, a partial view of the problem, whereas hybrid operations are being rolled out across multiple channels. Other studies are based on specific campaigns (elections, pandemics) in given countries through the analysis of different vectors, but these encounter difficulties identifying the perpetrators of the operations, their intentions and potential connections with States. This is because the relative prevailing impunity in this area has encouraged myriad private players (entrepreneurs of influence, mercenaries, criminals) to launch their own campaigns, making the entire ecosystem even more complex.

State actors, academics and individuals all study these issues from vastly different standpoints, with no shared analysis or common interpretive framework, nor any institutionalized mechanism for pooling information. This encourages a focus on the tactical aspects of these operations, at the expense of a comprehensive understanding of their strategic objectives, their scope or actual effects on our societies.

There is therefore a need to require that platforms grant researchers access to their data (R20) and to organize consistent, structured data-sharing among those studying these phenomena (R11).

In light of this semantic confusion, Camille François proffers an analytical framework in the form of an ABC of Disinformation : A is for Actors (manipulative Actors) who knowingly engage in online deception campaigns while obfuscating their identity and intentions; B is for Behaviour (deceptive Behaviour), encompassing a variety of techniques and vectors (platforms, websites, blogs) used to amplify the reach, virality and impact of the campaigns on line; C is for Content (harmful Content), the most subjective and complex criterion to define. It is considered foreign interference if the manipulator is a foreign power, or acting on the behalf of a foreign power. Establishing this is not, however, always clear-cut: a foreign stakeholder may weaponize a national player in order to relay their malevolent content; an entrepreneur of influence may run a campaign in order to curry favour from a foreign power without actually being an agent thereof; a manipulator may resort to transparent (non-deceptive) behaviours in order to spread politically objectionable (though lawful or even legitimate) content and enjoy organic (non-artificial) virality, because their content finds favour and is spread by others.

It is therefore important to see the problem as a spectrum along which diverse (more or less manipulative) stakeholders utilise a range of (more or less deceptive) techniques to spread wide-ranging (and more or less harmful) content. Kevin Limonier proposes a grid showing diverse situations in accordance with a typology of Russian information-related techniques and players, which he classifies into three categories: transparent, opaque and hidden. Depending on the combination of these techniques and the players deploying them, the operations are easier or harder to detect and trace back to their perpetrators.

Russian information-related operations

Understanding this continuum is the key to finding the most appropriate response and avoiding the pitfalls that would mean playing right into manipulators' hands.

IV.3. Complex responses

The information operations from abroad targeting France and Europe are transboundary in nature and use the most frequented platforms, which are mostly based in the United States, as a vector. Consequently, any response is going to require international cooperation not only with sovereign stakeholders when it comes to applying the law, but also with platforms' private-sector stakeholders, who are gatekeepers to both the data and formidable leverage for action. Depending on whether it is malicious players, deceitful behaviour or content that is being tackled, the response and the stakeholders involved will differ.

Cooperation between States and the mobilization of international law

In order to combat malicious State actors, States can mobilize the existing tools of international law. In 2016 for example, the Obama administration publicly accused the Russian Federation of interfering in the presidential election and expelled its ambassadors in protest. Applying the principle of non-intervention in such cases is, however, not straightforward (difficulties ascribing the source, in classifying the attack, in selecting appropriate responses) and is a double-edged sword, since it is authoritarian regimes' instrument of choice for justifying institutionalized online censorship. In all, it is hardly the most effective way of stymying the phenomenon or deterring its perpetrators.

With regard to content, the fight against terrorism paved the way, paradoxically, to an international consensus, despite longstanding divisions among countries concerning the control of terrorist content. But this consensus was built largely on the joint designation of an enemy, Islamic State, whose actions had been declared a threat to international security and peace. Apart from the lack of consensus surrounding the definition of the problem, the human rights and freedom of expression safeguards conferred by international law make any international regulation on information manipulation unlikely. The initiatives under way aim, rather, at regulating behaviour, in cooperation with the private sector. This is why the commission instead recommends a co-regulation regime, providing for exacting cooperation with platforms within the framework of digital services legislation (R23).

Cooperation between States and platforms

Most platforms were initially reluctant to work with governments for fear of losing their users' trust, already on thin ice since Edward Snowden's revelations, but also of having to explain their actions vis-a-vis authoritarian regimes that were continually pushing to remove content and close accounts. With their business model founded on a maximalist conceptualization of the freedom of expression, they were ill-prepared for this kind of pressure from the State.

In 2015, however, the proliferation of decapitation videos and the boom in youngsters' departures to Syria sparked enormous pressure from users and governments alike for platforms to shoulder their share of responsibility and find ways to staunch the flow of Jihadist propaganda. For want of effective international legal cooperation mechanisms, they established processes for cooperating with governments and civil society, based on their community standards, so as to facilitate reporting and takedown of terrorist content. It was not until 2017 that platforms joined forces to combat violent extremism on line with the creation of the Global Internet Forum to Counter Terrorism (GIFTC). Results were somewhat limited, as was evidenced by the circulation of the video of the 2019 attacks in New Zealand, which lead to the launch of the "Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online" by Prime Minister Ardern and President Macron (2019).

With the revelations about the information operations directly targeting American democracy in 2016, platforms had no choice but to face their own power and responsibilities. Their efforts centred chiefly on targeting misleading behaviours. Manipulators were utilizing, albeit for purposes other than their intended use, the technology and business models that the platforms had built: easy creation of multiple accounts, targeted advertising, recommendation algorithms and fast, easy sharing. The definitions put forward by the major platforms converge around the notions of "coordinated inauthentic behaviour" (Facebook), "inauthentic influence campaigns" (Twitter) and "deceptive behaviour" (Google); as of 2018, the US government initiated close and public cooperation with the major platforms, notably by way of FBI warnings to the platforms upon the detection of any new operations.

Despite genuine efforts to thwart the menace and offer greater transparency as to their practices, initiatives remain fragmented, both across different platforms and between different platforms of a single group.

For this reason, the commission proposes the creation of an OECD working group for drafting common minimum standards applicable across all platforms and harmonizing national legislation regarding their obligations (R15).

The choices made by platforms in this regard are still relatively opaque and fall completely outside the scope of European legislation. Above all, their efforts tend to peter out as pressure from Washington wanes. Because the 2020 presidential election showed that this time the information-related threat hanging over the electoral process came from within: from the far right, from conspiracy theorists (QAnon), and even from the White House.

Strategies for responding to information manipulation from abroad are often based on media coverage of the dismantling of networks of accounts or campaigns identified by States or platforms. This naming-and-shaming approach sends a diplomatic message while simultaneously raising public awareness as to the risks and techniques of disinformation. It does, however, inherently run the risk of raising the profile of operations or players whose visibility, admittedly difficult to measure, was hitherto limited. Such public accusations can be skilfully exploited for political gain, whether by the manipulators or by their accusers (Benalla affair; yellow vest crisis).

Finally, escalation in information operations has led to a kind of militarization of the information space, certain aspects of which threaten in turn to further intensify the threat.

IV.4. The militarization of the information space

In France, it was the cyber-defence command that was on the front line for countering the threat of terrorist information operations, seen as a major strategic sea change. It was the military who ran operations to halt the flow of Jihadist propaganda, as eradication proved impossible.

Since then, there has been an observable proliferation of information manoeuvres that have pushed governments to consider the information arena a national security domain and to develop their capacity not only for defence, but also for counter-attack. On 20 October 2021, Florence Parly, Minister for the Armed Forces, announced unequivocally that France was developing an anti-cyber-influence doctrine in order to "detect, characterize and repel attacks", but also to "engage in deception, whether independently or in combination with other operations".

This shift constitutes the continuation of a digital arms race and raises the same issues. On the one hand, it is impossible to restrict the desired effects to the military sphere alone, because this digital information space is shared across the civilian, economic and military domains. The propagation of content is difficult to control and any actions taken are potentially observable by multiple stakeholders. They may help weaken levels of trust in digital information and in institutions.

On the other hand, information operations enable different stakeholders to learn from one another. States and criminals can exploit the same vulnerabilities, copy modi operandi and reuse them. During the 2020 American presidential election, young pro-Trump activists were accused of copying troll farm methods to support their candidate. Their accounts were closed.

For these reasons, the commission recommends obtaining the opinion of the Defence Ethics Committee of the

Ministry for the Armed Forces on the doctrine for countering digital influence operations (R13).
There are, moreover, a number of stakeholders who have fully grasped and exploited this dual nature of the digital world, weaponizing civilian players as a vector of cyber-influence, thereby further clouding the distinction between foreign interference and domestic threat, as part of a hybrid approach that even further complicates democracies' response options. This creates a climate of tension in which States are constantly having to second-guess whether or not information is the instrument or the outcome of a strategic influence manoeuvre and whether or not they are in control of the situation, which in turn accelerates the race to build capacity.
The approach to digital risks thus needs to be holistic because threats are increasingly hybrid and cross-cutting in nature; hence the need to create an interministerial digital governance mechanism to set forth strongly coordinated responses, strategies and public policies with regard to defence, security and diplomacy, taking into consideration the multiple interactions that typify this shared domain (R12).

V
Law and cyberspace

Preventing and combating the dissemination of false information requires the coordinated implementation of different mechanisms which, for the most part, are centred more on policy incentives or self-regulation than on binding legal provisions. It is vital, however, for any country honouring the rule of law, to have some legal instruments for countering and sanctioning certain serious forms of such dissemination, in particular on digital networks.
A study of the legal provisions that might be useful for the prevention and punishment of the different forms of disinformation (in the sense of the malicious dissemination of false news) supports refraining from amending or replacing the current Article 27 of the 1881 Press Law. However, criminal sanctions could be extended to include a mechanism engaging the civil liability of persons maliciously disseminating false news potentially harmful to others. Such civil liability could be proportionate to the level of virality of dissemination and the online popularity of its perpetrator.
Alongside legal provisions for the prosecution of acts of disinformation, it is also vital to develop moderating and regulating mechanisms and to impose these on digital platforms, which are central to the viral dissemination of disinformation content. Similarly, the meagre prerogatives afforded in recent years to the French Higher Audiovisual Council (future ARCOM) need bolstering in order to guarantee digital platforms' cooperation for the detection and swift removal of false information capable of disturbing public order and to oversee their actions in this regard, or even impose penalties. Ultimately, it needs to be at the European level, under the future Digital Services Act, that platforms are obliged to implement effective moderation of false news posing a potential threat to public order, even if it means resorting to independent expertise for assessing the case for removing or deindexing content, while also taking into account due respect for freedom of expression.

V.1. Legal definition and sanctions of criminally reprehensible false news

In a liberal system, spreading a news item that proves to be partially or totally false is not, in and of itself, a reprehensible act. On the contrary, case law from the European Court of Human Rights (ECtHR) holds that the possibility of publicly imparting unsubstantiated information or ideas is an integral part of exercising one's right of freedom of expression, protected by Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and inviolable save for legally justifiable exceptions based on the greater good. The ECtHR's Handyside decision, notably, affirmed that freedom of expression "is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population".

In French law, the Constitutional Council recalled, in its decision dated 18 June 2020, the relevance of Article 11 of the 1789 Declaration of the Rights of Man and of the Citizen, which states that: "The free communication of ideas and of opinions is one of the most precious rights of man. Any citizen may therefore speak, write and publish freely, except what is tantamount to the abuse of this liberty in the cases determined by Law." It concluded that only certain particularly harmful categories of false news could be subject to restrictive administrative procedures.

It would therefore be incompatible with both France's Constitution and its international commitments to aim at imposing legal sanctions on all forms of spreading false information, which would furthermore severely conflate "misinformation" with "disinformation". Yet it would also be dangerous, from a legal perspective, to define acts of "disinformation" using excessively broad criteria or those vulnerable to an overly extensive interpretation. Quite the contrary, in this highly sensitive domain it is important for the legal framework to apply only to a narrow and particularly deleterious category of false news.

This category of false news, which we could henceforth describe as 'reprehensible' so as to distinguish it from categories that may in principle be freely disseminated (but for which any abuses will have to be answered in due civil process under general law), has already been defined in French law: in 1881 with the adoption of the law on press freedom. It is Article 27 of this legislation that we suggest conserving as one of the main pillars of

the legal apparatus supporting the national and European policy for preventing and combating disinformation that could seriously undermine democracy and which some authors openly refer to as "digital public order".

In its present, currently applicable wording, Article 27 of this 29 July 1881 Press Law provides for sanctions of:

"The malicious publication, dissemination or reproduction, by whichever means, of false news or documents which have been fabricated, falsified or mendaciously attributed to third parties, when this has disturbed the public peace, or was capable of disturbing it."

The reprehensible nature of a false news item is therefore determined by three conditions:

- that it has been communicated publicly (by any means whatsoever, including via an online service),

- that it disrupts or has the potential to disrupt public order,

- and that its dissemination was carried out in bad faith.

Since case law has already settled the interpretation of these conditions, we already have a solid, albeit restricted, basis upon which to determine the boundary between immoderations of freedom of expression which are not – per se – reprehensible and those which, on the contrary, fulfil these conditions and are thus criminally penalized or can become the object, if need be, of binding administrative measures.

In this way, only the dissemination of "news" within the meaning of an "announcement of a recent occurrence to someone with no prior knowledge thereof" (and not of a commentary regarding information that has already been made public) can be penalized. Said news needs to be "false, that is to say mendacious, erroneous or untrue in the substance and in the circumstances". As concerns the disruption of public order, the definition encompasses different scenarios of collective disorder, including the risk of disturbance in public places, influence on international relations, but also the risk of tensions among citizens. Moreover, there is no requirement to prove the existence of an already ongoing disturbance; it is sufficient to demonstrate that the dissemination in question would be capable of creating such a disturbance.

Furthermore, the State is particularly well-protected against false news stemming from foreign information interference. Indeed, Article 411-10 of France's Criminal Code sets forth markedly heavier penalties for "the fact of, with a view to serving the interests of a foreign power, a foreign or foreign-controlled organization or firm, providing France's civilian or military authorities with any false information likely to mislead them and undermine the fundamental interests of the nation".

Other categories of false news are covered by special provisions:

- false information leading to belief in an imaginary incident (false disaster, false accident, false hazardous deterioration or degradation) (Article 322-14 of the Criminal Code);
- "false or misleading indications" that could affect prices on the financial markets, or their indices (Articles L.465-3-1 to L.465-3-2, Monetary and Financial Code);
- "untrue or misleading allegations or imputations regarding a fact that are likely to alter the fairness" of an election (Article L. 163-2, Electoral Code);

At most, we could remark that there is no specific provision penalizing the dissemination of false news affecting only one or several private individuals. It is generally only under "defamation" (Art. 29 of the 29 January 1881 Press Law), that the justice system can punish the fact of harming a private individual by publishing something that is untrue or that constitutes a misrepresentation of facts with the intent of causing harm. Moreover, French case law allows for action to be taken (including in interim proceedings) to halt the dissemination of information that is damaging to privacy (in application of Article 9 of the Civil Code). But a more specific civil law provision could prove useful, as is mentioned below, without affecting the scope of the criminal law provision under the 1881 Press Law.

It is thus clear – as indicated by the Conseil d'État in its opinion dated 19 April 2018 – that "the fight against false information is a long-standing and recurrent concern for legislators, and one that is already covered by numerous provisions, albeit in a scattered manner".

Additionally, and more broadly speaking, it is heartening that the 29 July 1881 Press Law, although designed to penalize offences in the written press, has also become the legal framework for the public communication of information on all digital supports.
Consequently, and also bearing in mind the risk of legislative overcrowding – or even of impingement on freedom of expression – that could be arise from the adoption of a new provision reprimanding disinformation, the recommendation is to keep Article 27 of the 29 July 1881 Press Law as the cornerstone of the criminal law

system sanctioning the malicious dissemination of reprehensible false news (as the 2016 Senate report had indeed rather advised.)
At most, providing for associations to be able to take legal action in this domain – enabling them to take part in proceedings as plaintiffs – could strengthen the system because it would allow recourse to the incrimination process and its dissuasive effect to grow, while also fostering the development of case law that is detailed and tailored, in particular, to cases of disinformation across digital networks.

Recommendations:
· Retain Article 27 of the 29 July 1881 Press Law as currently worded (R16):
- as the basis of criminal proceedings for public dissemination of fake news on digital communications networks and platforms,
- and also as the benchmark definition for determining what constitutes reprehensible false news, the removal of which would not be an unwarranted violation of the right to freedom of expression.
· Expand Article 48-1 of the 29 July 1881 Press Law so as to permit associations combating fake news that is likely to endanger public order to exercise their rights as plaintiffs in proceedings for offences covered by Article 27 of the Press Law (R17).

V.2. Civil law sanctions proportionate to the dissemination of false news
Although repression via criminal proceedings is an essential instrument in the fight against disinformation phenomena owing to their powerful collective impacts, the potential effectiveness of civil law action should not be underestimated. In several domains, such as anti-piracy and privacy protection, civil lawsuits have proven effective alongside criminal prosecution. Article 9 of the Code Civil (created by the Law dated 17 July 1970) thus provides for civil liability proceedings against persons infringing in any way other people's right to privacy.

One of the advantages of this complementary avenue is the possibility of facilitating the court's due consideration of the online popularity or influence of the party knowingly spreading false information. Over and above the victim's moral and pecuniary damages, the law could require that civil law judges also take two variables into account when gauging the proportionality of their ruling: firstly, the virality of the dissemination; and secondly, the relative influence of the party disseminating the content or relaying the offending dissemination.

The abovementioned 2016 parliamentary report by the Senate had indeed proposed enabling "reparations for damages resulting from freedom of expression abuses on the basis of civil liability under general law".

Additionally, civil case law that could evolve on the basis of such a civil law provision may afford wider protection than that conferred, under the criminal system, by Article 27 of the 1881 Press Law, since it would not focus solely on false news likely to disrupt public order, but would aim more broadly at any harmful dissemination of false news.

While France's Court of Cassation limits the jurisdiction of French judges in criminal proceedings when it comes to penalizing content published online abroad, the competence of judges in civil proceedings is more easily recognized with regard to foreign dissemination if the contentious content is accessible online from France and at least part of the damages caused thereby occurs in France.

Recommendation (R18):
Add a new Article to the Confidence in the Digital Economy Act setting forth the civil liability of anyone maliciously circulating harmful false news, which could be worded as follows:

"Any person using digital means to disseminate news that is known to be false and which harms others shall be held liable for this act, as well as any person who knowingly re-disseminates it.
When ruling on damages, the following shall be given due consideration separately:
Firstly, any pecuniary losses caused by the dissemination;
Secondly, any moral harm caused thereby;
Thirdly, the extent and speed of its propagation;
and Fourthly, the scale of the audience and online popularity of its perpetrator."

V.3. Intervention by an independent oversight body
Although legal action centred on breaches of the 1881 Press Law is now eligible for the immediate referral procedure (since the 24 August 2021 law reinforcing respect for the French Republic's core principles was adopted), court case lead-times (in particular to obtain a final decision on the merits of a case) remain basically inadequate in the face of viral circulation of certain false news stories.

It is therefore worthwhile encouraging the earliest initiatives, taken in recent years, to empower an independent national administrative authority and enable it to act ex officio or upon request with a view to ordering the digital services concerned to take swift preventive measures or remove content.

It is this supervisory role that the recent 24 August 2021 law reinforcing respect for the French Republic's core principles already conferred upon the French Higher Audiovisual Council (or CSA, which is to become the Audiovisual and Digital Communications Regulatory Authority, ARCOM, on 1 January 2022), tasking it (via Article 42 of this 2021 law) with oversight of compliance by the platforms with their obligations to rapidly remove certain serious illegal content (albeit excluding false news covered by Article 27 of the 1881 Press Law).

However, in terms of disinformation, the law dated 22 December 2018 – moreover centred on combating fake news likely to skew electoral processes – also granted the self-same CSA (the future ARCOM) greater jurisdiction in the fight against the propagation of false news.

Article 12 of this 2018 law indeed affirms its authority to combat false information that could undermine electoral fairness, as well as to more broadly combat the dissemination of any information likely to disturb public order (which is to say, false news deemed potentially reprehensible within the meaning of the abovementioned Article 27).

In particular, the expectation is that the future ARCOM be able "as need be" to issue the major platforms with "recommendations aiming to enhance the battle against the spread of such information" and moreover ensure that these platforms duly respect the preventive measures that they need to adopt in particular to combat "accounts that are massively propagating false information" (Articles 11 and 12 of the 22 December 2018 law).

In its first report on this subject, published in July 2020, the CSA did indeed express its support for "prescriptive and targeted regulation of social media accountability implemented by an independent administrative authority" (a role that it expected to take on). However, upon reading this initial report, as well as the provisions of the 22 December 2018 law, it is clear that the future ARCOM's potential action vis-à-vis the major platforms remains a prerogative that is too vaguely outlined to be truly effective and therefore requires reinforcement.

Indeed, what appears to be missing is, at the very least, a formal ARCOM reporting procedure open to all citizens. The aim of this reporting procedure should not be to request removal of content that could constitute false news likely to disrupt public order. Rather, it would be to notify ARCOM a posteriori of (i) any difficulties that petitioners have encountered in getting a given platform to take their complaint seriously regarding content that they consider harmful, or (ii) on the contrary, complaints by authors whose content has been removed by a platform and who feel that the takedown was unjustified. In either scenario, ARCOM could engage with the platform in question to ensure that petitioners' points of view have been duly taken into consideration and received an appropriate response from the platform.

Recommendation (R19):
Expand Article 17-2 of the 30 September 1986 Law in order to provide for:
- on the one hand, the lodging of complaints to ARCOM by any person encountering difficulty obtaining a platform's action or cooperation in preventing or halting massive dissemination of content potentially conveying fake news that could disrupt public order, or by persons contesting a decision affecting their content;
- and on the other hand, ordering the platform in question – once warned by ARCOM – to swiftly submit a summary of any measures that it has taken in the case at hand and to cooperate with ARCOM in the identification and implementation of appropriate preventive or remedial measures for handling such a case.

V.4. Making platforms accountable in order to prevent massive dissemination of reprehensible false information

The globalized nature of the digital space and of the main platforms active therein means that no purely national legal measures could ever hope to suffice against the phenomenon of dissemination of 'fake news'. That is why it would appear most appropriate to encourage, when the upcoming Digital Services Act (DSA) is adopted, the establishment of binding rules imposed on the so-called very large online platforms (VLOPs) so as to combat the dissemination of false news.

As has been quite rightly remarked by the CSA, the battle against harmful content is a "public policy that needs to strike a balance between repressive policy and greater accountability for stakeholders through ex ante regulation".

To achieve this, it is important for the 'content moderation' obligation that should be imposed on these platforms to target with sufficient explicitness false news likely to disrupt public order. The draft under discussion in 2020 merely referred, with regard to platforms and intermediary service providers, to "illegal content" and to "information incompatible with their general conditions".

Admittedly, the proposed definition for "illegal content" does include any information that "is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law", which could encompass reprehensible false news within the meaning of Article 27 of the 1881 Press Law. But rather than leaving the door open for different Member States' platforms and jurisdictions to quibble over interpretations of France's press freedom legislation, it would be preferable for the 'content moderation' obligation that to be imposed by the forthcoming DSA to aim, in particular, on "false news likely to disrupt

public order."
If the new rules fail to include explicit wording in this regard, we could at least aim to have the criteria of reprehensible false news' sensitivity and virality duly discussed and agreed upon beforehand, as part of a co-regulation mechanism that could be instituted among European authorities, national regulators and the main platforms.
Moreover, we could suggest complementing the implementation of content moderation mechanisms with the creation – initially on a national basis (but which could subsequently be rolled out across Europe if successful) – of a mechanism for voluntary recourse to an independent body of experts. Referrals could be made to this body – if the complainant so agrees – at very short notice by the platform so as to elicit its advice as to whether or not some given content constitutes false news likely to disrupt public order.
Such a mechanism could be further bolstered by inclusion, in the general conditions of willing platforms, of a specific contractual clause under which any user who flags potentially reprehensible false information will be held to have given prior agreement to a possible referral of the matter to the external expert body and to refrain from initiating legal proceedings in any jurisdiction until the expert body has issued its opinion.

Recommendations:

- Include explicitly in the DSA a provision recognising that any false news likely to disturb public order constitutes reprehensible content that needs to be duly taken into consideration by the content moderation mechanism imposed on platforms (R21).
- Establish an independent body with which platforms could sign an agreement enabling them, if issued with a request for removal of content allegedly constituting reprehensible false news, to refer the case to these external experts, whose decision they agree to respect (R22).
- In a more extensive version of the previous recommendation, the platforms' general conditions could set forth that the complainant is contractually deemed to accept the principle of recourse to this external expertise and bound to refrain from initiating any legal action until the outcome is known.
- Create a co-regulation regime among platforms, regulators and civil society within the framework of the Digital Services Act. Institute a stringent cooperation mechanism with platforms for designing, implementing and evaluating the measures applied by the platforms to moderate content while safeguarding the freedom of expression and human rights (R23).

VI

An opportunity for democracy: developing critical thought and Media and Information Literacy (MIL)

As some researchers highlight, many phenomena blamed on algorithms are in fact triggered by our online behaviours and subsequently amplified by algorithmic models, which is not necessarily bad news. Indeed, this means that our destiny, in a sense, is still in our own hands, as long as we understand the mental processes that lead to said behaviours and how to remedy them. We have within us the resources that we need to avoid the pitfalls of false information and erroneous reasoning. Developing these resources has become a key issue in a digital world in which everyone can have their say – through a blog, a Facebook account or even by leaving comments on a mainstream news website – in the public arena. These resources entail, firstly, aiming to reason as freely and fairly as possible; in other words, to develop methodical reasoning, which might also be termed critical thinking. As Descartes recalls in his Discourse on the Method: "It is not enough to have a good mind; the main thing is to apply it well."
There are two things to bear in mind before getting into the definition of critical thinking and what contemporary science can tell us about it. Firstly, critical thinking does not mean doubting everything as a matter of principle. This default doubtfulness, often vindicated by pro-conspiracy thought, claims to exist for its own sake and to know no bounds. Yet this unfettered scepticism can easily become a form of nihilism. The search for alternative versions of historical realities or current events, without due respect for the canons of methodical reasoning and collection of evidence, leads all too often to narratives devoid of any epistemic substance.
Secondly, critical thinking does not boil down to debunking false information, the kind of exercise undertaken by fact-checkers, either. The current state of science shows us that such efforts are worthwhile and offer one possible response to the dissemination of false information. Nevertheless, the very people who are most likely to fall for misinformation happen to also be the least receptive to fact-checking exercises. To make matters worse, attempts to re-establish facts may further entrench their convictions, especially if the corrections are likely to challenge their worldview. These paradoxical reinforcing effects are well documented in the literature, and are known as "boomerang" or "backlash" effects. We may feel tempted to seek out information that aligns with our beliefs in order to feel reassured or, on the contrary – although it, too, amounts to a defence of our convictions – undertake research on the counter-arguments with a degree of disingenuousness regarding the facts laid out before us.
It is worth noting that rational contradiction is less likely to fail if it comes from a member of our own social or political group. Generally speaking, contradiction has a lower probability of being rebuffed a priori if it endogenous. Pushing this observation to its logical extreme, then, the obvious conclusion is that the most

effective kind of critique is the one coming from… our very selves; which is a rough outline of what critical thinking is all about. To fully flesh out the concept, however, a little further exploration is first required.

VI.1. Defining critical thinking

The literature offers us several definitions for what is understood by 'critical thinking'. The common denominator among them is to define critical thinking as the ability to correctly evaluate the content and sources of information available to us enabling better judgement, better reasoning or better decision-making. Assessing the epistemic quality of information consists of determining how likely it is that information will correspond to reality, and therefore whether or not we can consider it trustworthy. We can therefore define critical thinking as the ability to trust intelligently, after considering the quality of the information, opinions and knowledge at our disposal, including our own. It so happens that human beings are predisposed to possess this ability.

For example, children at the age of three choose their informants according to how close a bond they share. Familiar adults are less likely to have reason to deceive them, and children show a preference for information coming from caring adults or adults who show respect for socio-moral norms, while discounting informants who have been described as nasty or as liars by others. These three-year-old children similarly prefer the opinions of individuals who display a certain level of general knowledge or who have direct and perceptual access to the information.

Consequently, human beings are equipped from a very young age with epistemic vigilance tools that enable us to detect a portion of misleading information given out through deception or incompetence. In a digital environment, however, these tools enabling us to reason and to disregard suspicious sources of information clash with others that incite us to believe all too easily and that deceive us. As we saw in our chapter on the psychosocial mechanisms of disinformation, our mind is sorely tempted to accept plausible ideas which do not involve intellectually taxing analytical processes. Our tendency to be misinformed stems in part from a sort of cognitive avarice. Furthermore, the usual epistemic vigilance mechanisms can prove deceptive, especially on social media which upsets our social calibration – as we saw in the chapter on algorithmic regulation. The trust that we place in other people's judgement, insofar as it can be assessed by their social visibility, is deeply affected by the shift of our social life to the online world. We can no longer solely rely on our natural propensity for intuitively evaluating information; rather, we need to cultivate new mental aptitudes, chiefly through education and developing critical thought.

VI.2. The reasonable prospect that critical thinking can be developed

Several studies give us cause to believe that critical thinking and analytical thought, over and above reasonable scepticism, enable us to improve our resistance to false information and notably to conspiracy theories. They also make us more capable of altering our judgement when necessary. These encouraging results are not only found in laboratory studies; they can also be observed in pedagogical materials that have demonstrated the positive effects of teaching critical thought with skills transfer, in particular if the teaching is specifically designed to encourage this transfer (for example through repeated practice, the use of examples of different students and the explanation of the general rules to apply regarding a variety of contexts and content). In other words, the analytical skills acquired in one given exercise can be mobilized in other types of exercises if the way in which critical thinking is taught is adequate.

Similarly, a meta-analysis of the scientific literature has underscored the overall benefit of instruction aimed at developing critical thought when such training includes dialogue and exchange among the students, specific, situated and realistic problems on which to practice, tailored mentoring, and meta-cognitive exercises, that is to say allowing learners to become aware of their own thought processes.

There is still much work to be done, however, for the initiatives for developing critical thinking to become operational. Indeed, what can be called the 'teaching of critical thought' encompasses very disparate situations. In the two abovementioned recent meta-analyses, the authors indicate that what makes their task difficult is the immense diversity across studies in terms of duration of teaching, intensity, content, target ages, measurement methods for impact and quality. While in some cases, teaching is limited to a handful of lessons aiming to provide students with argumentation skills, in others it is conducted on a long-term countrywide scale, although the effects of skills transfer in the long term and across distance are seldom evaluated. Additionally, the aims for teaching critical thinking vary so widely that the concept seems to cover vastly disparate activities ranging from improving reasoning, reading and textual interpretation, to enhancing scientific or argumentation competence.

Numerous initiatives are being taken by the national education system, associations and journalism schools to develop critical thinking and Media and Information Literacy (MIL). Yet even when they do evaluate their pedagogical outcomes and produce statistics concerning their work, which is far from systematic, the data often remains scattered and heterogeneous, making it difficult to develop a knowledge base and programme of actions.

Recommendation (R24)

- Entrust an entity, the aim of which is to pool all of the fragmented data produced, with the task of devising standardized protocols and launching an evaluation of teaching material and training arrangements. For this project to succeed, a special interministerial delegation will be needed, comprising the key protagonists (ministries, associations, media, libraries, etc.), responsible for organizing, pooling and optimizing available

resources.

Recommendation (R25)
- Draw upon teachers' experience so that they can identify the aspects of the programmes that appear most counter-intuitive to students and the most frequent mistakes that stem therefrom, notably in terms of reasoning. This cartography of cognitive difficulties would make it possible to lay the groundwork for teaching metacognition.

These typical errors of reasoning that are to be identified may arise in any subject (physics, biology, mathematics, economic and social sciences, history, philosophy, etc.), which is why the idea is not to create new critical thinking courses, but rather to underscore the fact that learning to reason is every bit as important as learning the three Rs, and draw conclusions for the pedagogical process as a whole.
School programmes are peppered with these cognitive difficulties that have yet to be systematically inventoried. To take but one example, the theory of evolution clashes with pupils' spontaneous cognitive barriers. The challenge here is not only to fully grasp Darwin's theory, but also to show pupils why it is hard for them to understand. In this way, they will be learning to develop their own way of thinking while starting on a metacognition learning path.
To take another classic example of cognitive bias, the frequent confusion between correlation and causality could create an opportunity for a very poignant teachable moment, whether in mathematics, physics, economic and social sciences, history or even in philosophy. More thought could also be given, in a critical manner, to the argument is fecit cui prodest (guilt lies with whomever the crime benefits), surely the prologue to each and every conspiracy theory. This point could also be addressed just as easily in history or economic and social sciences, as in philosophy. There are ample teachable moments and examples that could be usefully illuminated by critical thinking. Research is unanimous in considering that initiation to analytical thought can be achieved as of a very young age, in full accordance with the theory of inoculation, which entails pre-exposing individuals to misleading arguments that they could subsequently encounter on social media. This advance messaging acts almost like a booster for people's intellectual immune system, so that they are better placed to identify false information and its arguments, to reject it or at least to be wary of it. These types of techniques are particularly well-suited to young, still-developing minds since they can be gamified, in games where users are initiated to disinformation practices and the way in which our illusions are exploited.

VI.3. MIL and critical thinking: two complementary approaches
In parallel to developing the teaching of critical thinking, it is worthwhile – and complementary – to improving people's media and information literacy. In France, the national education system conceptualizes it as teaching that allows learners to become truly conversant in media, information, digital and civic culture. MIL was included in the Framework Law for Restructuring Schools of 8 July 2013 and is one of the subjects taught under "citizenship education" (2016) to primary and secondary school pupils.
Its positive effects on the stimulation of our intellectual immune system, amply demonstrated in Finland and in northern European countries more generally, have also been measured in France, where one study demonstrated MIL's positive influence on young people's news consumption.
The development of MIL is all the more crucial given that the media ecosystem is becoming increasingly complex and that there is an observable contamination of traditional media (newspapers, radio and television) by digital approaches. Consequently, editorial considerations now increasingly take the attention economy mechanisms into account, seeking to optimize the visibility of their products and to adapt to the design of digital platforms. In the words of Jean-François Dumas, head of Influence Communication, a media analysis agency that offers quantitative monitoring of the professional news landscape, "the problem is that traditional media are acting and behaving just as social media do. The social media culture is being transposed into traditional media." The media are thus tempted to promote attention-grabbing hooks, notably news items based on fear or conflict. Historically, the media have always led by example with this reciprocal supply and demand adjustment, but the internet paved the way for its massification. It would appear, moreover, that this trend of digital world contamination of the traditional media is firmly entrenched in France.
And this is all the more significant given that a sizeable portion of advertising manna has migrated away from conventional media to the internet giants. In the United States in 2016, 85% of advertising revenue was absorbed by Google and Facebook. In ten years, traditional newspapers have lost half of the billions of dollars that they had hitherto raked in annually in advertising income, while that of Google multiplied fifty-fold. One direct result of this situation was employment losses in the press sector. In 2008 in the United States there were 71,000 journalists working in the printed press industry, but by 2017 that number had dropped to a mere 39,000, a reduction of 45% in jobs, according to figures provided by the US Department of Labor. Obviously, in these conditions, news quality and editing cannot remain unaffected.
Competitive pressures on the news market necessarily leave less time for verifying information, increasing the risks of cascading consequences. The timeframes for interviewing experts have also shrunk. How to ensure that the process of identifying relevant experts, for example during a pandemic, is duly following a rational process, rather than hurried decisions taken in the heat of the moment and knee-jerk searches through potentially out-of-date address books? The answers given in the course of interviews on this subject conducted by the commission were hardly reassuring. On the subject of expertise, there is clearly a need for some kind of intermediary

between the world of science and that of the media. These factors invite us to ponder ways of guaranteeing editorial freedom for journalists, unwillingly caught up in digital approaches that may seriously affect the quality of their work.

It is for all of these reasons that MIL has become so vital; it enables one and all to become initiated to the complex realities of the media ecosystem, which remains one of the pillars of democracy.
In France's education system, MIL is taught throughout children's school years: instead of being listed as a separate subject, MIL is considered a cross-cutting skill set, even though, according to the Director of the CLEMI (Liaison Centre for Media and Information Literacy, an agency of the French Ministry of National Education): "the teaching of MIL still lacks legibility and continuity across a pupil's learning at school".
Effective teaching of MIL in schools varies greatly, with marked disparities across the country: "Despite being considered the province of all teachers, across all subjects, citizenship education, of which MIL is the pillar, is seldom formalized, coherent and assessed. For MIL to flourish, it needs to be taken on board by all of the different stakeholders involved in the education process."
More often than not, MIL is taught by history/geography teachers, notably as part of the moral and civic education syllabus and by teacher-librarians whose goal is to enable "all students to acquire knowledge about information and the media". But these teachers' MIL interventions usually occur during the class time of their own subjects, which therefore impinges on their teaching time for their own syllabus. They cannot currently meet today's needs for both teaching and imparting MIL. The CLEMI has a strategic role in that it not only trains teachers, but also creates teaching resources and makes them available. Indeed, each local education authority has CLEMI coordinators, seconded teachers, who constitute a network and who focus on MIL. What is undermining the CLEMI's capacities is a shortfall in resources, even though its services are increasingly in demand.
There have been recent developments, however, at the MENJS (Ministry of National Education, Youth and Sport), which is drafting a MIL teaching guide, broken down by school level right from the start of primary school, for teachers to use.
Digital skills testing for pupils of Year 10 (troisième, final year of middle school) and Year 13 (terminale, final year of secondary education) have been rolled out, under the PIX project.
Pre-primary and primary education: There are plans to have pupils take a test and work towards an 'internet permit' at the end of their final year of primary school (Year 6, CM2).
Secondary education: In Year 11 (seconde, typically ages 15 and 16), a Digital Sciences and Technology course has just been established, including MIL modules; and MIL skills have been included in the final oral examination for the Baccalaureate.
Continuing Education is also under the remit of the local education authorities, and is covered by their respective Training Plans, but these courses are too few in number and the training is still perceived as insufficient by many of those involved.
Furthermore, a network of Continuing Education Schools is to be set up in each local education authority in January 2022 in order to run training courses and pedagogical activities with material made available.
Pre-service training is not available everywhere, and although some of the higher teacher training institutes offering pre-service teacher training have indeed started including MIL modules in their programmes, this kind of teaching is not yet very widespread at all. The arrival of PIX certification has meant that Year 10 and Year 13 learners can validate 16 digital skills, including the use of social media and knowledge of the phenomena of misinformation and disinformation. This certification is not, however, a scientific assessment of the effectiveness of these teaching innovations on offer. It is clear that in this field, as in that of critical thinking, the solutions on offer are multiplying, but they lack coordination, standardization and evaluation.

Recommendation (R27)
- Systematize the teaching of critical thinking and MIL, on the one hand for school children, throughout primary school and beyond secondary school, and on the other hand for trainee and in-service teachers. For this to be successful, it is also important to substantially bolster the network of local education authority coordinators and points of reference in these fields.

In addition, as with the teaching of critical thinking, MIL must not be planned with only school children in mind, given that the issue of misinformation and disinformation affects all citizens. In this regard, the French Higher Audiovisual Council advocates reinforcing media literacy initiatives for adults.
The range of stakeholders involved in the field of MIL is vast (institutions, local authorities, activity facilitators, educators, press ombudsmen, librarians, news and information professionals, media, digital players, etc.). They offer activities in myriad structures open to the wider public (associations, community centres, play centres, libraries and multimedia libraries, etc.). Yet there is no inventory of the country's MIL initiatives (outside of the education system), nor is there, here again, any assessment of these disparate mechanisms.

Recommendation (R29)
- Create a continuum between time spent at school, at university, in the world of culture and the world of work and take into consideration the fact that learning critical thinking and MIL is important for all citizens, identifying social scenarios conducive to this kind of teaching and learning.

From this perspective, MIL is a trans-ministerial subject which, apart from the MENJS, concerns in particular the Ministries of Culture, of Higher Education, Research and Innovation, and for Territorial Cohesion and Relations with Local Government. Numerous initiatives have been taken, but in a slightly chaotic and non-coordinated manner.
Another network to call upon in the field of MIL is that of libraries and multimedia libraries. Indeed, 63% of French people view multimedia libraries as a primary source of digital resources. The country's 12,429 libraries and 480 university libraries are privileged intermediaries that reach out to every imaginable audience, young and old.
Despite the wealth of MIL resources in libraries, library involvement is inconsistent and the initiatives under way are not very visible or seldom identified. The Ministry of Culture therefore introduced a MIL component in its 2018 "Library Plan", providing for the rollout of training courses in the regions as well as online training.
Librarian training entities have started incorporating MIL in their programmes and numerous resources for librarians have been produced by the BNF (France's National Library), the BPI and Libraries Without Borders.
To complete this picture, let us not forget the growing involvement of some media and of the CSA. Close to 1,700 media took part in the latest edition of "Press and Media Week in Schools" in March 2021 and throughout the year through collectives or associations (Entre les Lignes, Cartooning for Peace, Lumières sur l'Info, Globe Reporters, Fake Off, etc.).
The main journalism schools also include MIL in their programmes, some with more structure than others, indicating awareness of the problem of false information.
France also has a plethora of associations (La Ligue de l'Enseignement, the progressive education organization CEMEA, the network of youth and community centres, the La Main à la Pâte Foundation, the Union of Family Associations , etc.) and they are very active when it comes to proposals concerning critical thinking and MIL. Community education associations have been invested therein for several years already, including MIL modules for their educators both in their standard curricula and in in-service training programmes. But MIL content is still being invented and developing.

To round off this panorama, there is another social arena that is ripe for MIL initiatives and critical thinking training: the private sector. We note that some corporate foundations of major brands (such as GAFA, and the foundations established by AXA and EDF) help fund educational endeavours on MIL but that the visibility of their initiatives, especially with regard to in-service training, remains relatively low.

Recommendation (R28)
- heighten awareness among heads of school, National Education inspectors and local education authority directors as to the importance of MIL and teaching critical thought, as well as among elected officials, Human Resources Directors of local authorities and chief librarians.

Continuing vocational training enables the acquisition for new skills in a person's working life, whether for employment re-entry or continuation, or to ensure or optimize professional career development. It is a legal requirement in France (Article L6311-1 of the Labour Code). It could constitute another ideal opportunity for promoting critical thinking and MIL.

VI.4. Conclusion
Enabling each and every citizen to develop their intellectual autonomy through the teaching of critical thinking and of MIL (whether part of pre-service or in-service training) needs to be declared an Issue of National Interest, a priority objective for democracies facing disruptions engendered by the digital world. This could be done by enhancing their visibility through the dissemination of messages of general interest in the media (R26).
On the one hand, this is the least liberticidal way of regulate today's out of control information marketplace. Since each and every one of us has become operator in this market, it is up to us to decide whether or not to share, whether or not to like, a given piece of information. That is why the health of our democracy involves every single citizen enhancing their intellectual vigilance.
On the other hand, this approach is a way for a nation to wrest back some control over its destiny. Indeed, as we have seen, some essential recommendations that this report proposes depend on the goodwill of the major digital operators or on a power struggle with them. The development of critical thinking and MIL, however, depends solely on the firm and coordinated resolve of a national policy. The best way for us to rid ourselves of the shackles of algorithmic enslavement is undoubtedly to arm ourselves with the brain's formidable resources. This objective is fundamental, lastly, because it means that a worrying situation can be transformed into a wonderful political opportunity: educating people to become autonomous citizens in their judgement thanks to the development of metacognition skills. Opting for this will help us to take the right path from this societal crossroad where we now stand, promoting a democracy of knowledge.

Conclusion

This report was never designed to serve as a fact-checker or eradicate online disinformation or misinformation; the aim was to consider the technical, legal and societal means for limiting the negative consequences that they

have on democracy. One possible way of achieving this goal would be to take action both upstream of the dissemination of falsehoods through proposals aiming at making platforms and online advertisers accountable, and also downstream. This implies, on the one hand, strengthening media literacy and critical vigilance with regard to content being circulated and, on the other hand, enabling researchers to understand the exact extent and nature of the phenomenon. As such, data held by the digital world's giants need to be considered, ultimately, as a common good.

This report was written, firstly, with the ambition of taking into account the present state of knowledge and the many and varied initiatives already on offer or under way. It was written, secondly, considering Europe's position of strategic dependence with regard to the major American platforms, over which it has no jurisdiction. It was written, finally, with the conviction that safeguarding the freedom to express points of view is vital.

Our deliberations were taking place in an auspicious context, because precisely as we draw our work on this report to a close, the European Parliament's Committee on Internal Market and Consumer Protection (IMCO) has just approved the text of the legislative proposal for the Digital Services Act, including considerably tougher obligations of transparency and liability of the very large online platforms than the European Commission's initial text, so as to better protect users and their fundamental rights on line. The next step will be the final vote in the European Parliament in early 2022.

As our work comes to an end, we firmly believe that the digital revolution, in the midst of which we find ourselves, is causing an escalation in upheavals that we can as yet barely comprehend. Our ponderings have afforded us a glimpse of certain things that will surely lead, tomorrow, to new questions. The announcement by Mark Zuckerberg, creator of Facebook, of the advent of the metaverse is one of these. The troubling questions for social media will arise afresh with regard to this new "holy grail of social interactions", as Zuckerberg likes to call it, which looks set to swiftly invade our lives. This alternative universe, in which we will be immersed through an avatar to meet up with friends, play, work, or even go shopping, does not yet exist. But the issue of moderation will be even more essential for the metaverse than it is for social media, since this technology is immersive, and we can only begin to imagine the scale of destruction that could result if online hatred or harassment were to hold sway there. This is no idle concern: Andrew Bosworth, the CTO of Meta (ex-Facebook) has even voiced it directly, in an internal memo divulged 12 November 2021, and underlined that recurring moderation errors could endanger the company's very existence.

One final suggestion that we could make therefore concerns our need for prospective attentiveness with regard to these innovations being announced, the effects of which could wreak havoc on our relation to reality and to information. Especially since the Meta initiative is not a one-off wonder. The city of Seoul announced in November the creation of "Metaverse Seoul", a 3D virtual world, built on augmented and virtual reality technologies, which will become the first ever virtual public service centre where citizens will be greeted by avatars. Seoul's Mayor aims for South Korea's capital to be the first major city to enter the metaverse, making it "a city of coexistence, a global leader, a safe city, and a future emotional city". The metaverse symbolizes our gradual immersion in a universe where there will eventually be a blend of real worlds and virtual ones.

We consequently believe that it would be worthwhile examining the ethical issues of these immersive digital worlds, which are continuously pushing the boundaries of the physical world and which promise social interactions of an entirely new kind. This reflection could be spearheaded by the National Digital Ethics Steering Committee, as a continuation of its opinion on chatbots, adopted September 2015 (R30). In time, this could lead to broader contemplation at the international level, involving experts from the digital tech industry, academia, civil society and governments.

Beyond these challenges, we are also very mindful that the digital revolution has made astounding advances possible and of its untapped potential. The COVID-19 pandemic accelerated our societies' digital transformation, thanks to which we were able to switch almost overnight to teleworking, monitor the spread of the virus and its variants in real time around the world, create a vaccine in record time and organize massive vaccination campaigns.

Already, new forms of collaborative teamworking have emerged, hinting at promises of newly intensified scientific exchange. One such example is the Tela Botanica initiative, through which tens of thousands of botanists, some professional, others amateur, can network together to efficiently revise the nomenclature of all plants growing in France in its entirety. Such collaborative platforms also facilitate the identification of threatened species and the pooling of data enabling the identification of fish, fungi, plants, birds and such like.

Such crowdsourcing work can go much further than this: the game Foldit, developed by the computing and biochemistry departments of the University of Washington, invites online gamers to solve scientific puzzles through collective exploration of what is possible. In the game players can, for example, freely test out different molecular combinations in an attempt to identify the way in which certain proteins unfold in space: moving these sections here, adding a bit there, or even destroying bonds altogether. Through this collaborative online construction game, it took just three weeks to solve a problem that scientists had been trying to figure out for the last ten years: the true structure of an enzyme in an AIDS-like virus in rhesus macaques.

In the same vein, one of the clearest expressions of 'collective intelligence' is surely the online encyclopaedia Wikipedia, which may have its share of criticism but which has nonetheless proved that it can easily rival even the best conventional encyclopaedias.

Digital technology thus provides resources enabling our collective intelligence to assume its most efficient expression yet and to become the support for a revitalization of democracy. As of the 1960s, many theorists

predicted what is now known as the crisis of democracy, reflected notably by record levels of people's mistrust in the media or politics. These authors called for a renewal of democracy in a more participative form. Theorists like Carole Pateman and Benjamin Barber notably hold that any genuine political freedom depends on the involvement of one and all in public affairs. Until recently, this universal involvement was hampered by technical obstacles that digital tools can counteract.

Hopes for a tech-driven revitalization of democratic life are being manifested in very concrete examples, such as the experimentation under way in Taiwan under the aegis of Audrey Tang, Digital Minister, promoting the use of platforms for citizen deliberation and for co-drafting of legislation. These new democratic consultation mechanisms have made decision-making possible on difficult subjects, such as online alcohol trade or the regulation of Uber – although observers have commented that citizen participation, set up on a voluntary basis, remains limited and is still the province of the very well-informed.

These initiatives are but a foretaste of the wide-ranging array that the internet is able to offer. We are living in the age of the datasphere, in which most of our humanly activities rely on technology and leave digital traces, thus producing a whole new space, a sphere of data that interacts with the physical world. The datasphere's exponential growth raises the issue of digital governance as we face the great challenges of our century, starting with environmental degradation and climate change which threaten, over and above our democracies, humanity as a whole.

The sole ambition of our report was to contemplate, urgently, solutions for quelling a problem that has been exacerbated – transformed even – by digital technology: disinformation. This work in no way exonerates us from our duty of collective deliberation in order to contemplate the world of tomorrow. Digital technology is a formidable lever. The question remains as to which kind of society and which kind of democracy we wish to build in this evolving digital world.

Recommendations

Disinformation is to a large extent a lawful phenomenon and is protected under the principle of freedom of expression in our democracies. Our Recommendations do not, therefore, seek to eradicate it, which is neither possible nor desirable. They aim, rather, to limit the propagation of content that damages democracy, to deter malicious behaviour, to punish illicit practices, to enhance risk prevention and to heighten user vigilance.

There is no silver bullet. Online disinformation comes in many forms, uses ever-evolving techniques and produces diverse effects across wide-ranging target audiences. It is already being addressed via different routes, which we have categorized under four major headings: regulation, good practices, digital governance and education.

Disinformation occurs within a digital ecosystem whose governance is complex and involves myriad stakeholders (platforms, governments, civil society) who are all affected by this problem, irrespective of any rivalries driving them or disputes dividing them. None of them can effectively take action alone. This is why, in the diagram below, we show different spheres of action (public, private, civil society) which all overlap. Many of the measures that we suggest require cooperation or co-regulation among these stakeholders and are at the intersection of these groups. Finally, we have identified several levels of governance, because France cannot take action alone.

Our deliberations were centred around key themes, each constituting a chapter; our Recommendations are to be read in the context of these chapters. We decided to present our Recommendations in the same order as the corresponding chapters, for the sake of clarity and coherence. Many of our Recommendations are, however, cross-cutting in nature and thus spill beyond these compartmentalisations. This is particularly true of the Recommendations concerning digital law and research. We have therefore decided, in some chapters, to cross-reference Recommendations located in other chapters.

Psychosocial mechanisms

1. Foster public research

- Support and bolster scientific research in France into online disinformation and foreign cyber-interference. Such support could be provided through earmarked research funding or the creation of research posts.
- France should encourage the European Union to support scientific research on these subjects at its respective level.

Algorithms

2. Consider regulating the design of user interfaces

Commence deliberation, with a view to regulation, on the importance of the issue of user interface design.

3. Counter popularity bias

Offer users a more accurate snapshot of the network and the true prevalence of opinions by deactivating algorithmic curation and popularity metrics by default, and by focusing on metrics enabling users to gauge the content's epistemic quality (notably its sharing history).

4. Accountability for influencers

Encourage platforms to improve their moderation of influencers so as to hold the latter to account.

5. Promote expertise

Enhance the visibility of specialized knowledge by promoting experts' accounts and amplifying their content (on subjects relating to their field of expertise).

6. Reflect the present state of knowledge

For certain firmly-established subjects, prevent algorithmic ranking from misleading the public with regard to the true state of knowledge. To this end, encourage dialogue among platforms and scientific institutions to ensure that any prevailing consensus be reflected in the visibility granted to the various opinions.

7. Prevent the risk of over-moderation

Guard against the risk of over-moderation through closer analysis of user reports (mass reporting).

The fake news economy

8. Make programmatic advertising players accountable

- Promote responsible advertising investment in the private sector by encouraging advertisers, advertising sales entities, advertising agencies and, above all, advertising technology providers to use dynamic "website exclusion and inclusion lists", such as those created, for example, by NewsGuard, Global Disinformation Index or Storyzy. Engage in dialogue with advertising technology providers so that they also utilize this system, which could significantly dry up the fake news economy.
- Ensure that any public administrations or enterprises using programmatic advertising exhibit exemplary practices through the widespread recourse to dynamic inclusion lists.
- Envisage requiring all firms engaged in CSR to undergo thorough independent annual audits of their programmatic advertising campaigns making it possible to establish exhaustive lists of the web addresses (URL) of the sites where their campaigns are served, and make these lists publicly available.
- Encourage certification entities such as AFNOR, when issuing "responsible" labels, to give due consideration to the problem of funding disinformation, by mandating regular audits for firms applying for such labels.
- Envisage requiring advertising technology providers to alert their customers to the risk of funding toxic sites should the latter fail to use dynamic exclusion lists.
- Recommend that mainstream media websites ban any sponsored links in their advertising spaces that send users to disinformation clickbait sites. Encourage them to cease working with advertising companies that associate them with such sponsored links.

9. Encourage the good practices deployed by crowdfunding platforms

- Consider imposing an obligation on crowdfunding platforms to explicitly notify their users as to all measures implemented to avoid indirect participation in the funding of projects involving hate speech or the propagation of disinformation.
- Urge crowdfunding platforms to utilise the services of website credibility rating companies or to obtain a recognised label that includes the issue of avoiding funding toxic sites. An example of such an incentive is to offer tax relief for these companies on their taxable profits.

Foreign cyber-interference

At the national level

10. Protect the integrity of electoral processes

- Analyse the data on foreign interference campaigns targeting French democracy so as to better anticipate any risk.
  - Gather data from social media and meta-data collected by a broad range of researchers and institutions, as well as existing analyses
  - Undertake an in-depth analysis so as to better apprehend and anticipate threats
- Establish a cooperation mechanism across platforms, institutions and academia so as to respond swiftly to any operations detected.

11. Enable data sharing among trusted stakeholders

- Adapt the open-source public platform Open CTI for sharing data on disinformation among researchers, government, platforms and journalists:
  - Create any missing technical modules
  - Initiate reflection among a community of stakeholders on modelling the threat
  - Define a fair use doctrine that respects personal data privacy in partnership with the CNIL, France's data protection authority
  - Encourage the formation of a community of users who are working on the analysis of cyber-interference, including human and social science research centres

12. Create an interministerial digital governance mechanism

- A holistic approach to digital risks is needed (encompassing both cyber threats and information manipulation) because threats in this shared space are increasingly hybrid in nature and cross-cutting (transboundary State-sponsored threats).
- The challenge is to develop a digital security culture that includes the risk of information manipulation and involves all State and government stakeholders.
- The idea is also to comprehend any unintentional effects and interactions across different domains and to better identify solutions.

13. Consult the Defence Ethics Committee of the Ministry for the Armed Forces on the doctrine for

countering digital influence operations

Cyber-enabled influence operations must be stringently supervised from an ethics point of view so as to best assess the balance between strategic advantages and ethical risks concerning such information operations. The Ethics Committee could examine, inter alia, the target audiences, the selected operating modes or even the proposed types of discourses and narratives.

At the European level

14. Create a crisis management mechanism at the European Union level and create crisis management exercises in order to:

- respond swiftly to massive information operations
- improve preparedness for handling information-related aspects of global crises (health or security)
- better counter information-related threats

At the international level

15. Propose the creation of a working group at the OECD

- Work toward establishing common minimum standards applicable across all platforms.
- Build on the European Union's current code of good practices, the good practices tested by platforms and the outcomes of academic research regarding: community guidelines, fact checking, certification, bot takedowns, algorithmic moderation, political advertising, verification procedures, transparency and remediation.
- Work toward harmonisation at the international level of legislation governing the obligations incumbent on platforms.

Law and cyberspace

16. Retain Article 27 of the 29 July 1881 Press Law as currently worded, as:

- the basis of criminal proceedings for public dissemination of fake news on digital communications networks and platforms,
- the benchmark definition for determining what constitutes a reprehensible falsehood, the removal of which would not be an unwarranted violation of the right to freedom of expression.

17. Expand Article 48-1 of the 29 July 1881 Press Law

The aim of this is to enable associations combating fake news that could endanger public order to exercise their rights as plaintiffs in proceedings for offences covered by Article 27 of the Press Law.

18. Add a new article to the Confidence in the Digital Economy Act

Include a new article stipulating the civil liability of those maliciously circulating harmful false news, which could be worded as follows:

"Any person using digital means to disseminate news that is known to be false and which harms others shall be held liable for this act, as well as any person who knowingly re-disseminates it.

When ruling on damages, the following shall be given due consideration separately:

Firstly, any pecuniary losses caused by the dissemination;

Secondly, any moral harm caused thereby;

Thirdly, the extent and speed of its propagation;

and Fourthly, the scale of the audience and online popularity of its perpetrator."

19. Expand Article 17/2 of the Law dated 30 September 1986, in order to provide for:

- on the one hand, the lodging of complaints to ARCOM by any person encountering difficulty obtaining a platform's action or cooperation in preventing or halting massive dissemination of content potentially conveying fake news that could disrupt public order;
- and on the other hand, ordering the platform in question – once warned by ARCOM – to swiftly submit a summary of any measures that it has taken in the case at hand and to cooperate with ARCOM in the identification and implementation of appropriate preventive or remedial measures for handling such a case.

20. Require platforms to grant researchers access to their data

Ensure that in the final version of the Digital Services Act (DSA) the modalities concerning platforms' obligation to provide access to their data (DSA Article 31) constitute an optimal framework enabling researchers to pursue research that helps identify and comprehend systemic risks (including disinformation - DSA Article 26) in the best possible conditions.

21. Include in the Digital Services Act a provision on false news

Include explicitly in the DSA a provision recognising that any false news capable of disturbing public order constitutes reprehensible content that needs to be duly taken into consideration by the content moderation mechanism imposed on platforms.

22. Establish an independent external expert body

Establish an independent body with which platforms could sign an agreement enabling them, if issued with a request for removal of content allegedly constituting reprehensible fake news, to refer the case to these external experts, whose decision they agree to respect.

In a more extensive version of the previous recommendation, the platforms' general conditions could set forth that the complainant is contractually deemed to accept the principle of recourse to this external expertise and bound to refrain from initiating any contentious action until the outcome is known.

23. Create a co-regulation regime among platforms, regulators and civil society within the framework of the Digital Services Act

Institute a stringent cooperation mechanism with platforms for designing, implementing and evaluating the measures applied by the platforms to moderate content while safeguarding the freedom of expression and

measures applied by the platforms to moderate content while safeguarding the freedom of expression and human rights

- regulators establish an overarching framework outlining the major principles
- co-regulators translate these principles into applicable standards
- platforms implement the standards with due respect for their obligations as set forth by the DSA
- regulators monitor the implementation of the standards and assess the effectiveness of the measures taken by the platforms

Critical thinking and MIL

24. Create an interministerial unit for developing critical thinking and MIL for one and all

Create an interministerial unit focused on the development of critical thinking and MIL for the public at large, involving the main protagonists (ministries, associations, the media, libraries, etc.); a delegation under the aegis of the French Prime Minister tasked with organising, pooling and optimising resources and commissioning a body or creating a structure to commence assessment of teaching materials and training schemes using standard scientific protocols.

25. Identify cognitive difficulties in students

Draw upon the experience of teachers so as to map out the most frequently encountered cognitive difficulties among students, with a view to initiating a process of reflection on how to teach metacognition.

26. Declare the development of critical thinking and MIL an Issue of National Interest.

Raise their profile by disseminating messages of general interest in the media.

27. Systematize the teaching of critical thinking and MIL in schools

Systematize training for pupils as of primary school and throughout and beyond secondary school as well as for trainee and in-service teachers, and substantially bolster the education system's network of coordinators and points of reference in these fields.

28. Heighten awareness among education authorities as to the importance of MIL

Raise awareness among heads of school, National Education inspectors and regional education authority directors as to the importance of MIL and teaching critical thought, as well as among elected officials, Human Resources Directors of local authorities and chief librarians.

29. Develop the teaching of critical thinking and MIL in civil society

It is important to create a continuum between time spent at school, at university, in the world of culture and the world of work. The teaching of critical thinking and MIL thus needs to be systematized not only in regional educational projects and the Educational Cities scheme for disadvantaged schools, but also in employment services, from youth volunteers engaged in civic service through to retirees and people in continuing education.

30. Call upon the National Digital Ethics Steering Committee to examine the issue of digital worlds and virtual and augmented reality

Growing user immersion in digital worlds where the distinction between the real and the virtual becomes increasingly blurred can engender ethical risks. The metaverse project announced by Meta (ex-Facebook) or the Metaverse Seoul project could accelerate this phenomenon. Launching initial deliberations at the national level could lead to the constitution of an international multi-stakeholder group for envisaging an ethics framework for the development of these digital environments.

List of people and institutions contacted

Andler, Daniel

➢ Director of the TESaCo project, Academy of Moral and Political Sciences, Institut de France

Angaud, Bernard

➢ Bureau of France's press ombudsman and ethics office (Conseil Déontologie Journalistique et de Médiation)

Arata, Fabienne

➢ Country Manager and Senior LTS Director, LinkedIn

Astolfi, Charles-Pierre

➢ Officer for Digital Regulations and Commons, Ministry of State for the Digital Transition and Electronic Communications

Audinet, Maxime

➢ Researcher, Military Academy Strategic Research Institute (IRSEM)

Avia, Laetitia

➢ Member of the National Assembly for Paris (12th – 20th districts)

Bail, Chris

➢ Professor, Duke University, and Director, Polarization Lab

Barbet, Serge

➢ Assistant Director, CLEMI (Liaison Centre for Media and Information Literacy, an agency of the French Ministry of Education)

Battesti, Anton'Maria
➢ Head of Public Policy, Facebook France

Beaudouin, Pierre-Yves
➢ President, Chair of the Board, Wikimédia France

Belin, Celia
➢ PhD in political science, University Panthéon-Assas, currently visiting scholar Center on the United States and Europe, at the Brookings Institution (Washington DC)

Benabou, Valérie Laure
➢ Professor of Private Law, Paris Saclay University

Benard, Yohann
➢ Director of Strategy, Amazon

Benoualid, Shani
➢ Advisor for Digital and Social Media, Interministerial Delegation for the Fight against Racism, Anti-Semitism and Anti-LGBT Hate (DILCRAH)

Berkouk, Hannah
➢ Director General, HelloAsso

Bienaimé Besse, Carole
➢ Board Member, French Higher Audiovisual Council (CSA)

Blanchot, Guillaume
➢ Director General of the French Higher Audiovisual Council (CSA)

Blanquer, Jean-Michel
➢ Minister of National Education, Youth and Sport

Borry-Estrade, Elisa
➢ Public Policy Manager, Facebook

Borst, Grégoire
➢ Professor of Psychology, University of Paris

Bothorel, Éric
➢ Member of the National Assembly for Côtes-d'Armor, 5th constituency

Bouillon, Stéphane
➢ Senior Prefect, General Secretariat for Defence and National Security (SGDSN)

Bourdet, Julienne
➢ Educator, Médiat Rhône-Alpes, Grenoble Alpes University

Cabannes, Laurent
➢ Lecturer in Technology, Créteil education authority

Cardon, Dominique
➢ Director, Médialab, Sciences Po University

Caroti, Denis
➢ Officer for Critical Thinking, Aix-Marseille education authority

Cathelineau, Yolaine
➢ Doctoral student, GEODE, Paris 8 University

Cattan, Jean
➢ Secretary General, French Digital Council (CNNum)

Charon, Paul
➢ Director, "Intelligence, Anticipation and Hybrid Threats", Military Academy Strategic Research Institute

➢ Director, "Intelligence Anticipation and Hybrid Threats", Military Academy Strategic Research Institute (IRSEM)

Chérel, Ronan
➢ History-Geography Teacher, Collège Rosa Parks middle school (Rennes)

Chirouze, Aline
➢ School teacher, education in the prison setting

Claerr, Thierry
➢ Head of the Public Reading Office (Ministry of Culture)

CNews
➢ No response to our request for contact

Cointet, Jean-Philippe
➢ Researcher, Médialab, Sciences Po University

Colrat, Philippine
➢ Public Policy Manager, Amazon

Conference of Journalism Schools (CEJ)

Corbin, Noël
➢ Delegate-General for Transmission, Territories and Cultural Democracy (DG2TDC)

d'Aubert, François
➢ Head of France's advertising verification bureau (ARPP)

Dagnaud, Monique
➢ Research Director, National Centre for Scientific Research (CNRS)-School of Advanced Studies in Social Sciences (EHESS)

Duguin, Stéphane
➢ Chief Executive Officer, CyberPeace Institute

Daviet, Emmanuelle
➢ Mediator, Radio France

de la Chapelle, Bertrand
➢ Director and Co-Founder, Internet and Jurisdiction Policy Network

Deloire, Christophe
➢ Secretary General, Journalist, Reporters Without Borders

Delouvée, Sylvain
➢ Researcher in Social Psychology, Rennes II University

Dey, Aurélie
➢ Lieutenant-Colonel, Commander of the Hate Crime Division (DLCH), Crimes against Humanity, Genocide and War Crimes Office (OCLCH)

di Palma, Cyril
➢ Delegate-General, "Génération Numérique" association

Dieguez, Sébastian
➢ Researcher in Neuroscience, Cognitive and Neurological Sciences Laboratory, University of Fribourg (Switzerland)

Doucet-Bon, Pascal
➢ Assistant Director of Information, in charge of strategy, France Télévisions

Dufour, Mathias
➢ President of the think tank and action lab #Leplusimportant

Durand, Pascale

➢ Federation Affairs Director, Federation of Parents Associations (FCPE)

Durand-Viel, Laure
➢ Delegate for Digital Platform Regulation, Ministry of Culture

Élizéon, Sophine
➢ Prefect, Member of the Interministerial Delegation for the Fight against Racism, Anti-Semitism and Anti-LGBT Hate (DILCRAH)

Eveno, Patrick
➢ Bureau of France's press ombudsman and ethics office (Conseil Déontologie Journalistique et de Médiation)

Ferriol, Gabriel
➢ Head of the Service for Vigilance and Protection against Foreign Cyber-Interference (Viginum)

Fogiel, Marc-Olivier
➢ Director General, BFMTV

Forestier, Florian
➢ Philosopher at the think tank and action lab #Leplusimportant

Forteza, Paula
➢ Member of the National Assembly representing French expatriates, 2nd constituency, co-author of the report "Liberté, Egalité… Vérité"

Franceschini, Laurence
➢ President, Joint Commission for Publications and Press Agencies (CPPAP)

François, Camille
➢ Chief Innovation Officer, GRAPHIKA

Frau-Meigs, Divina
➢ Professor of Communication and Information Sciences, Paris III University

Freyssinet, Éric
➢ Brigadier General, Deputy Commander for Cyberspace, Gendarmerie. Doctor of computer science, associate member of the LORIA research unit

Froissard, Laureline
➢ Director, Legal and Public Affairs, Union des Marques association

Garandeau, Éric
➢ Director, Public Policy and Government Relations, TikTok France

Garnier, Marie Caroline
➢ Managing Director, CORPCOM Agency

Gautellier, Christian
➢ Head of the Advisory Board of the Media, Cyberspace and Critical Education Division, at the National Association progressive education centres (CEMEAs)

Gayraud, Jean-François
➢ Advisor to the National Intelligence and Counter-Terrorism Coordination, National Counter-Terrorism Centre

Geffray, Edouard
➢ Director General of School-Level Education (DGESCO)

Gérard, Colin
➢ Doctoral student at GEODE, Paris 8 University

Gérard, Olivier
➢ Coordinator for Media-Digital Use at the National Union of Family Associations (UNAF)

Gery, Aude
➢ Post-doctoral fellow at GEODE, Paris 8 University

Giret, Vincent
➢ Director of News and Sports, Radio France

Gourdin, Jean-Baptiste
➢ Director General of Media and Cultural Industries, Ministry of Culture

Grosset, Kathleen
➢ Bureau of France's press ombudsman and ethics office (Conseil Déontologie Journalistique et de Médiation)

Grumbach, Stéphane
➢ Senior Researcher at France's National Research Institute for Digital Science and Technology (INRIA), Internet Data at the Heart of the Economy (DICE) head of team, and Director of the Rhône-Alpes Complex Systems Institute

Guiroy, Thibault
➢ Government Affairs Manager, Google France

Haugen, Frances
➢ Data engineer and scientist, and project manager, former Facebook employee

Hecketsweiler, Jean-Philippe
➢ President, Descartes Foundation

Herblin-Stoop, Audrey
➢ Public Affairs Director, Twitter France

Huchon, Thomas
➢ Journalist, Spicee and LCI

Innes, Martin
➢ Professor, Director of the Crime and Security Research Institute, Cardiff University

Jacquier, Sarah
➢ Policy Officer reporting to the Legal Affairs Service, Ministry of Culture

Jean, Aurélie
➢ PhD in Computational Mechanics in Material Sciences

Jeangene Vilmer, Jean-Baptiste
➢ Director, France's Military Academy Strategic Research Institute (IRSEM)

Jézéquel, Gwénaël
➢ Advisor, Institutional Relations and Communication, General Secretariat for Defence and National Security (SGDSN)

Jolion, Jean-Michel
➢ Advisor to the office of the Minister for Higher Education, Research and Innovation

Jounot, Olivier
➢ Head of CSR, AFNOR Group

Khemis, Sarah
➢ Government Relations and Public Policy Senior Manager, TikTok France

Klein, Olivier
➢ Professor of Psychology at ULB in Brussels

Koutchouk, Alexandre
➢ Deputy-Director, Print Media and Information Professions, Ministry of Culture

Labbé, Chine
➢ Managing Editor and Vice President Partnerships, Europe at NewsGuard

➢ Managing Editor and Vice President Partnerships, Europe at NewsGuard

Laboulais, François
➢ Head of "Media Education" at the National Association of progressive education centres (CEMEAs)

Laffont, Sandra
➢ Journalist, President of the association "Entre les Lignes"

Larrieu, Mathilde
➢ MIL missions Coordinator, National Scool for Information and Library Sciences (ENSSIB)

Le Monde
➢ No response to our requests for contact

Le Roux, Yann
➢ Managing Director for Southern Europe, Integral Ad Science (IAS)

Lee Bouygues, Helen
➢ Founder of the Reboot Foundation; CEO of Conforama

Lesage, François
➢ Head of Communications, Twitter France

Limonier, Kevin
➢ Lecturer at GEODE, Paris 8 University

Loutrel, Benoît
➢ Board Member, French Higher Audiovisual Council (CSA)

Machet, Julien
➢ Member, Trans-Disciplinary Critical Thinking Resource Group of the National Education Scientific Advisory Board (CSEN)

Macron, Brigitte
➢ President of the Hospitals Foundation (Hôpitaux de Paris-Hôpitaux de France)
Magnin, Olivier
➢ Director of Visual, Media and Information Literacy, Ligue de l'Enseignement

Maistre, Roch-Olivier
➢ President of the French Higher Audiovisual Council (CSA)

Melford, Clare
➢ Co-Founder and Executive Director, The Global Disinformation Index

Mercadal Delasalles, Françoise
➢ Co-Chair of the French Digital Council (CNNum)

Mercier, Hugo
➢ Research Scientist, National Centre for Scientific Research (CNRS)

Mercier, Arnaud
➢ Professor, Information and Communication Sciences, Paris II University

Missoffe, Sébastien
➢ Director General of Google France

Morel, François
➢ Auvergne Rhône Alpes Directorate of Réseau Canopé, the publishing arm of France's National Education service

Motte, Stanislas
➢ CEO and co-founder of Storyzy

Moukheiber, Albert
➢ PhD in Cognitive Neuroscience

Nathan, Michaël
➢ French Government's Communication and Information Service (SIG)

Ndior, Valère
➢ Professor of Public Law, Western Brittany University

Nguyên Huang, Lê
➢ Mathematician teaching the Swiss Federal Institute of Technology in Lausanne and presenter on the channel Science 4all

Nicolas, Laurent
➢ Director, Implcit

Novel, Catherine
➢ President, Association of National Education Teacher-Librarians (APDEN)

Novel, Anne-Sophie
➢ Collective "Informer n'est pas un délit" (To Inform is Not a Crime)

Nuñez, Laurent
➢ Prefect, National Intelligence and Counter-Terrorism Coordinator, former Minister of State attached to the Minister of the Interior

Oeuvrard, Béatrice
➢ Public Policy Manager, Facebook France

Ohayon, Esther
➢ Group Manager, Corporate Communications, LinkedIn

Orphelin, Matthieu
➢ Member of the National Assembly for Maine-and-Loire, 1st constituency, co-author of the report "Liberté, Egalité… Vérité"

Pasquinelli, Elena
➢ Post-doctoral fellow in Philosophy, Jean Nicod Institute

Petit, Laurent
➢ Digital policy officer, National Higher Institute for Education and Teacher Training (INSPE), Paris

Picquet, Gautier
➢ CEO, Publicis Media; President, Union of Media Purchasing and Consulting Firms (UDECAM)

Pigalle, Céline
➢ Managing Editor, BFMTV

Pospisil, Marek
➢ Senior Lead Public Policy, LinkedIn

Quattrociocchi, Walter
➢ Professor in Computer Science, Sapienza University of Rome

Renard, Yves
➢ Director, Higher School of Journalism (ESJ), Lille

Robin, Valérie
➢ "Artistic and Cultural Education – MIL" Policy officer, Public Information Library (BPI)-Centre Pompidou

Rolle, Pierre-Louis
➢ Director of the Digital Society Programme and New Place, New Links Programme, National Agency for Territorial Cohesion (ANCT)

Ruquier, Pierre-Albert
➢ Marketing Director and co-founder, Storyzy

Schapiro, Jacob
➢ Professor of Political and International Affairs and Director of the Empirical Studies of Conflict Project

➢ Professor of Politics and International Affairs and Director of the Empirical Studies of Conflict Project, Princeton University

Schiffrin, Anya
➢ Director of Technology, Media and Communications at the School of International and Public Affairs, Columbia University

Schmidt, Philipp
➢ Executive Director, Prisma Media Solutions

Schwartz, Arnaud
➢ Director, Bordeaux Aquitaine Institute of Journalism (IJBA)

Séjourné, Stéphane
➢ President of the Renew Europe group of the European Parliament

Servan-Schreiber, Emile
➢ PhD in Cognitive Psychology, founder of Hypermind

Signoux, Martin
➢ Public Policy Manager, Facebook

Simon-Nahum, Perrine
➢ Research Director, National Centre for Scientific Research (CNRS) and Guest Lecturer at ENS, Department of Philosophy

Simonet, Vincent
➢ Engineering Director, Google France

Sleeping Giants France
➢ Collective combating the funding of hate speech

Taguieff, Pierre-André
➢ Political scientist, historian, Research Director, National Centre for Scientific Research (CNRS)

Théobalt, Jean-Christophe
➢ Digital Mediation and MIL Policy Officer, Ministry of Culture

Tisseyre, Didier
➢ General, Commander of cyber-defence of the French Armed Forces

Vachet, Carole
➢ Chief of staff for the Ministry of State for the Digital Transition and Electronic Communication

van Prooijen, Jan-Willem
➢ Researcher in social psychology, Maastricht University

Verdier, Henri
➢ Ambassador for Digital Affairs

Vincent, Emmanuel
➢ Editor in charge of multimedia publishing, Éditions EHESS (Publisher of the School of Advanced Studies in Social Sciences)

Wagner-Egger, Pascal
➢ Researcher in social psychology, University of Fribourg (Switzerland)

Watrin, Laurent
➢ Deputy Mayor of Nancy in charge of innovation of public policies and digital technology, for journalist for the audiovisual public service, municipality of Nancy

We Report
➢ Collective of independent journalists

Yesilaltay Sacha
➢ PhD student in cognitive science, National Centre for Scientific Research (CNRS)

Zuckerman, Ethan
➢ Associate Professor, Director of the Initiative on Public Digital Infrastructure, University of Massachusetts Amherst

The members of the commission also wish to extend their thanks to all those who facilitated the successful completion of the commission's work:
Margot Godefroi, Izabela Luniak, Samuel Leenhardt, Guilhem Marotte, Sasha Morinière, Astrid Roucher.