THINK-TANK
DIGITAL
NEW DEAL

DEFENDING THE RULE OF LAW IN THE AGE OF PLATFORMS

FIGHTING ILLEGAL SPEECH ON THE INTERNET AND PROTECTING FREEDOM OF EXPRESSION

by Gilles Le Chatelier and Denis Olivennes

June 2021

Digital New Deal

CONTENTS

GILLES LE CHATELIER

Gilles Le Chatelier associate professor of public law (Paris X Nanterre 2003-2005, Lyon II, 2005-2008, Ecole Normale Supérieure de Lyon 2008-2020), has also been Chairman of the Board of Directors of the IEP [Institute of Political Studies] of Lyon since 2012. He is also a member of the scientific board of the "Actualité Juridique des collectivités territoriales" (AJCT) [Legal News of Regional and Local Authorities] and regularly publishes in numerous legal journals specialised in public law.

After a career of just over 20 years in the administration which led him to hold important responsibilities within the State and local authorities (State Councillor, Assistant Rapporteur to the Constitutional Council, expert at the European Commission,...), Gilles Le Chatelier became a lawyer in March 2011 and on that occasion joined the firm ADALTYS , of which he became chairman in January 2020.

DENIS OLIVENNES

Denis Olivennes, a former senior civil servant, is a business leader and author.

Currently co-manager of the newspaper Liberation. He was notably CEO of Canal+, Chairman and CEO of Fnac, Nouvel Observateur and then Lagardère Active (Europe 1, Paris Match, Elle, Journal du dimanche...).

Inter alia, author of La gratuité, c'est le vol : quand le piratage tue la culture (2007), Mortelle transparence avec Mathias Chichportich (2018) and Le délicieux malheur français (2019). Also author of the Olivennes Report on cultural supply and the fight against illegal sharing on the internet (2008).

INTRODUCTION

The fight against illegal speech (racist, anti-Semitic, homophobic, defamatory, insulting, etc.) on the internet is a challenge for all our democracies. The widespread distribution of these messages constitutes a real danger to the normal functioning of the institutions, not to mention the manipulation to which social networks have given rise during several recent elections.

For many years, initiatives have been taken to combat this scourge. The unanimous opinion is that the results are still insufficient. The propagation of such speech promotes the polarisation of our societies and fosters hatred in an unhealthy climate. Until now, the reaction of the hosting providers, mostly passive, has not been able to combat this danger effectively.

But at the same time, the desire to limit such content raises delicate questions regarding respect for freedom of expression.

As the Constitutional Council recalled in its decision rendered on the AVIA law on 18 June 2020, referring to Article 11 of the Declaration of the Rights of Man and of the Citizen guaranteeing the constitutional principle of freedom of expression: *"In the current state of the media and in view of the widespread development of online public communication services and the importance of such services for participation in democratic life and the expression of ideas and opinions,* ***this right implies the freedom to access and express oneself in such services".***

In this context, the recent initiatives of several platforms censoring content on their own initiative or blocking accounts of political figures, including prominent ones, necessarily raise questions.

The balance to be struck is complex.

And it must be sought at European level, rather than in the chaos of scattered national reactions.

The national legislator has intervened on several occasions on this subject, with varying degrees of success. The censure of most of the Avia law of 24 June 2020 by the Constitutional Council has largely deprived this initiative of effect. The inclusion in the bill to strengthen republican principles of some of its concerns, as contained in the text adopted by the National Assembly on 16 February 2021, is intended to remedy the shortcomings identified at the national level.

However, given the power of the largest platforms and the highly cross-border nature of their activities, only a European initiative could be truly relevant.

As the National Consultative Commission on Human Rights (CNCDH) noted in its opinion of 9 July 2019 on the AVIA bill, *"the CNCDH also regrets the lack of coordination between States, both at the European Union and international levels".*

Likewise, in its opinion on the same text issued on 16 May 2019, the Council of State stated that *"only the adoption of new provisions by the European Union would give a common basis and considerably greater effectiveness to a fight that the values enshrined in the Treaties require to be conducted at the same time as the market develops".*

However, the legal framework in force today appears to be largely deficient (1). The Commission has just tabled a proposal for a European regulation, the "Digital Services Act", which is to be commended for going in the right direction on a number of points (2). However, even at the stage of this proposal, which still has to be endorsed by the European Parliament and the Council, certain gaps remain which need to be filled by additional proposals (3).

1. A CURRENTLY INSUFFICIENT EUROPEAN LEGAL FRAMEWORK

1.1 THE 2000 DIRECTIVE

The provisions applicable in this area stem from a text which is now somewhat old, **Directive 2000/31/EC of 8 June 2000** on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

As its very title indicates, this text focuses on electronic commerce and implements the means of removing any obstacles to its development in the European area. The legal basis for this text is the Treaty articles on the internal market.

Nevertheless, several provisions of this text deal with the issue of content, in particular in Articles 12 to 15 of this text.

As stated in § 40 of the grounds of the Directive, *"this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information"*.

The subjects of illegal content and the means of controlling it are dealt with in Articles 12 to 15 of the Directive.

Article 14 of the Directive deals with the obligations of hosting providers. It establishes **the principle of non-liability of the latter for the information stored**. However, their non-liability is subject to the double condition that:

- *"the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent;*
- *the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."*

This provision is minimal and leaves some latitude to the Member States, since Article 14.3 of the Directive allows a court or administrative authority of a Member State to require the hosting provider to put an end to the presence of illegal content or to prevent this situation.

Likewise, Member States are free to establish procedures governing the removal of illegal content and actions to make access to it impossible. However, § 46 of the grounds of the Directive specifies that these operations must be carried out *"in the observance of the principle of freedom of expression and of procedures established for this purpose at national level"*.

Article 15 of this text lays down the second major principle on these issues: **the absence of any general obligation for hosting providers to monitor.**

As stated in Article 15.1 of the Directive:

> *"Member States shall not impose a general obligation on providers… to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity".*

Article 15.2, however, provides that these provisions do not address monitoring obligations applicable to a "specific case". Member States may thus provide for systems whereby hosting providers would be obliged to report illegal content of which they become aware and to respond to requests from the authorities to identify the recipients of their services who might be disseminating such content.

The CJEU thus ruled that these provisions did not prevent a court of a Member State from ordering a hosting provider to delete or block access to information it stores, the content of which is identical to that of information previously declared unlawful, regardless of who requested the storage of that information (CJEU 3 October 2019 Glawischnig-Piesczek Case C-18/18).

1.2 A DATED TEXT

The text of the directive, which predates the phenomenal development of digital platforms, is clearly inadequate to take into account the issues mentioned above. As the Council of State wrote in its opinion of 16 May 2019 on the AVIA PPL *"the provisions of the e-commerce directive predate the creation of social networks by several years and the scale of the outpouring of odious content calls for urgent action to defend individuals".*

The European Council shares the same observation, stating that *"the extension and diversity of new digital business models and services have significantly changed over time and some services have raised new challenges which the existing regulatory framework does not always address" ("Shaping Europe's Digital Future - Council conclusions 9 June 2020").*

Above all, the affirmation of the dual principle of limited liability of the hosting provider and the prohibition of a general monitoring obligation leads to situations where, in practice, illegal content can remain online for long periods of time at the risk of causing serious damage and/or harm.

In response to these shortcomings, the European institutions have developed codes of conduct to encourage hosting providers in particular to implement the necessary means to combat the presence of illegal content, as provided for in Article 16 of the Directive of 8 June 2000.

Therefore duly concluded, at the initiative of the European Commission, on 31 May 2016 was a "code of conduct on countering illegal hate speech online" to which Facebook, Twitter, YouTube and Microsoft subscribed, joined in 2018 by Google+, Instagram, Snapchat and Dailymotion.

Likewise, on 1 March 2018, the Commission issued recommendations on measures to effectively tackle illegal content online (C (2018) 1177 final).

However, these initiatives, even though they may be interesting, are part of a "soft law" approach that is not very restrictive for operators. The resulting degree of protection is thus necessarily limited, particularly for those who may be affected by hate speech.

Conversely, in the European texts currently in force, there is no provision for the hosting provider to block content or remove an account, even though such actions may constitute a

serious violation of respect for freedom of expression.

Thus, the current texts do not provide sufficient guarantees either for the fight against hate speech or for freedom of expression.

2. THE COMMISSION'S PROPOSAL FOR A EUROPEAN REGULATION ON THESE ISSUES – THE DIGITAL SERVICES ACT (DSA)

This inadequacy largely explains the proposal made by the European Commission on 15 December 2020 for a new European regulation on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC, known as the "Digital Services Act" (DSA), whose welcome initiative must be applauded.

This text contains a number of significant advances that deserve to be highlighted and supported.

The proposed Regulation repeals Articles 12 to 15 of the Directive of 8 June 2020 and replaces them with a new regime. However, it retains the fundamental principles as we shall see later.

The text adds a number of additional obligations which significantly change the current regime with a view to increasing its effectiveness.

It is organised in three parts: the definition of a number of general obligations applicable to all players (2.1.), a gradation of obligations according to the size of the operators (2.2.) and the strengthening of national control mechanisms in conjunction with the Community institutions (2.3.).

2.1 STRENGTHENED GENERAL OBLIGATIONS

The proposal for a Regulation contains new rules, applicable to all operators, to strengthen the fight against illegal content and to allow better control of the removal of content on the internet.

As stated in § 34 of the grounds of the draft regulation: *"In order to achieve the objectives of this Regulation… it is necessary to establish a clear and balanced set of harmonised due diligence obligations for providers of intermediary services. Those obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including minors and vulnerable users, protect the relevant fundamental rights enshrined in the Charter, to ensure meaningful accountability of those providers and to empower recipients and other affected parties, whilst facilitating the necessary oversight by competent authorities."*

The Regulation also **defines illegal content** (Article 2(g)) as "any information which, in itself or by its reference to an activity… 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".

§ 12 of the grounds states that *"that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit*

products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law".

The proposed amendments are thus of several kinds.

- **Injunctions** (Articles 8 and 9): the first set of injunctions provided for in this article concern illegal content. The text requires the service provider to inform the referring authority "without undue delay" of the action taken. The authority issuing the injunction must give reasons for its request, as well as information identifying the sender of the content (exact URLs or "additional information"). It should also provide information on the remedies available against the injunction.
  A similar mechanism is foreseen for the injunctions that national authorities can issue to hosting providers asking them to provide certain information.
- **Single contact point** (Article 10): intermediary service providers must establish such a contact point vis-à-vis national or European authorities to facilitate relations with them and make them more fluid.
- **Legal representatives** (Article 11): this provision requires suppliers who do not have an establishment within the European Union to appoint a legal or natural person to represent them legally. These representatives must be able to answer to the national and Community authorities on all matters relating to the fulfilment of the obligations contained in the Regulation. To this end, they must have the "necessary powers" to cooperate and may be "held liable for non-compliance".
- **Transparency in moderation operations** (Article 13): service providers must periodically report on any moderation operations they have carried out, whether on injunction or on their own initiative, or in response to complaints.

2.2 OBLIGATIONS OF INCREASING INTENSITY DEPENDING ON THE SIZE OF THE OPERATOR

As stated in § 35 of the grounds of the draft regulation, *"it is important that the due diligence obligations are adapted to the type and nature of the intermediary service concerned".*

This differentiation of obligations according to the size of the operators is one of the major innovations of the proposal. It does indeed go in the right direction by modulating the intensity of the obligations according to the size of the operator to which they apply.

The proposed Regulation thus imposes increasing obligations on hosting service providers, online platforms (OLPs) and very large online platforms (VLOPs).

First, it defines **hosting service providers** as those whose business consists of *"the storage of information provided by, and at the request of, a recipient of the service".*

Second, Article 2(h) of the draft defines **online platforms** as *"a provider of a hosting service which, at the request of a recipient of the service, stores and* ***disseminates to the public information****, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability*

of this Regulation".

§ 13 of the grounds of the proposal makes it possible to distinguish more clearly between online platforms, which thus constitute a subcategory of hosting service providers:

> *"Online platforms, such as social networks or online marketplaces, should be defined as providers of hosting services that not only store information provided by the recipients of the service at their request, but that also disseminate that information to the public, again at their request. However, in order to avoid imposing overly broad obligations, providers of hosting services should not be considered as online platforms* ***where the dissemination to the public is merely a minor and purely ancillary feature of another service and that feature cannot, for objective technical reasons, be used without that other, principal service****, and the integration of that feature is not a means to circumvent the applicability of the rules of this Regulation applicable to online platforms. For example, the comments section in an online newspaper could constitute such a feature, where it is clear that it is ancillary to the main service represented by the publication of news under the editorial responsibility of the publisher."*

Finally, Article 25 of the draft regulation defines **very large online platforms** as those *"which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million".*

As the Commission states, *"given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service, in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online, it is necessary to impose specific obligations on those platforms, in addition to the obligations applicable to all online platforms".*

Thus, the draft text provides for obligations applicable to accommodation services, to OLPs and additional obligations applicable only to VLOPs.

A. OBLIGATIONS APPLICABLE TO ALL HOSTING SERVICES

Two new measures are provided for here, which are binding on all content hosting providers:

- **Notification mechanisms** (Article 14): service providers must provide standardised and simple mechanisms for anyone to notify them of content deemed illegal. These notifications are considered as elements that bring this situation to the attention of the hosting provider and oblige it to act, under penalty of being liable in case of inaction. The hosting provider must acknowledge receipt of this notification and inform the person who referred the matter to it of the action taken.

- **Statement of reasons for decisions to remove content or access** (Article 15): the hosting provider must inform the person concerned of this decision at the latest at the time of removal or blocking. It must also indicate the reasons for this decision, the possible use of "automated means" to make the decision and the legal references explaining why it considers the content to be illegal. It must also inform the person of the remedies available to him or her to contest the decision.

B. ADDITIONAL OBLIGATIONS APPLICABLE TO ONLINE PLATFORMSEN LIGNE

In addition to the above obligations, the draft regulation imposes specific rules.

- **Internal complaint-handling system** (Article 17): OLPs must set up internal complaints mechanisms against decisions taken by them regarding illegal content or content "incompatible with their terms and conditions" and resulting in the removal of content or blocking of access, suspension or termination of the provision of the service, suspension or termination of the beneficiary's account. OLPs must deal with these claims "in a timely, diligent and objective manner". Beneficiaries of OLP services subject to one of the above-mentioned decisions must be able to consult an out-of-court dispute settlement body certified by the national authorities (Article 18).
- **Trusted flaggers** (Article 19): it is up to the national authorities to qualify certain entities as such, whose notifications, as provided for in Article 14 of the draft regulation, must be given priority by the OLP "and without delay". In order to qualify, the organisation must have particular expertise in identifying illegal content and represent collective interests distinct from those of the OLP.
- **Measures and protection against misuse** (Article 20): this new provision aims to combat repeated infringements by the same users. To this end, the OLPs may suspend, after warning them, the beneficiaries of services "which frequently provide manifestly illegal content". The same mechanism is provided for persons abusing the notification (Article 14) or complaint (Article 17) mechanisms. The OLP judges the abusive nature of this behaviour with regard to the number of abuses identified, the seriousness of their consequences and the intention of the person involved.
- **Notification of suspicions of criminal offences** (Article 21): where an OLP becomes aware of information giving rise to suspicion that "a serious criminal offence involving a threat to the life or safety of persons has been committed, is being committed or is likely to be committed", it shall "promptly" inform the competent law enforcement authorities in the Member State.

C. OBLIGATIONS IMPOSED ON VERY LARGE ONLINE PLATFORMS

Additional devices are finally required for the VLOPs.

- **Assessment of systemic risks** (Article 26): the VLOPs must analyse at least once a year any systemic risk arising from the operation and use of their services within the Union.

The following three systemic risks are identified:

- The dissemination of illegal content, in particular the dissemination of child pornography and hate speech;
- The challenge to fundamental rights, including freedom of expression and information, the right to privacy, the right to non-discrimination and the rights of the child. § 57 of the grounds of the draft mentions the design of algorithmic systems that can produce these harmful effects;

- Intentional manipulations of their services with foreseeable negative effects on health, civic discourse, electoral processes, public safety and the protection of minors;

In this risk assessment, VLOPs must take into account their moderation systems, as well as their content recommendation, selection and display systems.

The VLOPs must therefore take measures to mitigate these systemic risks (Article 27): adapting moderation systems, strengthening internal procedures for monitoring activities, and establishing closer cooperation with trusted signalmen.

- **Organisation of independent audits** (Article 28): each year, the VLOPs must organise an independent audit at their own expense to verify compliance with their obligations under the draft Regulation. Audits carried out by qualified bodies independent of the VLOPs shall issue recommendations at the end of their investigations to which the VLOPs must respond with implementation measures within one month.
- **Recommender systems** (Article 29): VLOPs using such systems must set out "in a clear, accessible and easily comprehensible manner" the main parameters of these systems, as well as the options available to the recipients of their services to modify or adapt them.
- **Access to and monitoring of data** (Article 31): the VLOPs shall provide the Member States or the Commission with access to the data necessary to monitor and evaluate their compliance with the obligations thus laid down. Accredited researchers may be appointed by public authorities to carry out the analysis of the systemic risks referred to in Article 26 of this draft regulation.
- **Compliance officers** (Article 32): VLOPs must designate one or more persons to monitor their compliance with this Regulation. They must ensure that they can perform their duties independently.

2.3 NATIONAL AND EUROPEAN CONTROL MECHANISMS

The draft regulation contains numerous provisions relating to the ways in which national and European authorities can monitor compliance with these obligations by hosting providers. This is an important novelty, as the Directive of 8 June 2000 does not contain any provisions on these issues.

Several mechanisms are thus provided for to oblige Member States to put in place the necessary means to ensure compliance with the rules contained in this draft regulation. The question of the Member State responsible for this control is also settled, taking into account the location of the hosting provider. Similarly, increased powers are proposed for European bodies to play a greater role in managing these issues.

- **Establishment of national coordinators** (Article 38): each Member State must designate a national authority as coordinator for digital services, responsible for the application of this Regulation throughout the territory of the Member State. It oversees the activities of all national bodies likely to intervene in the application of the proposed rules.

It has extensive investigative powers (Article 41), including the power to conduct on-site inspections. It may also order the cessation of the violations found and impose corrective measures and fines or periodic penalty payments.

The national coordinators may conduct joint investigations (Article 46) for hosting providers operating in several Member States. They may also refer the matter to the Commission for investigation if the shortcomings are the result of the activity of the VLOPs. The national coordinators are grouped together in a European Digital Services Committee, which must assist them in carrying out their tasks (Article 47).

- **Jurisdiction (Article 40):** the Member State in which the hosting provider has its principal place of business shall have jurisdiction under this Regulation. If the hosting provider does not have an establishment within the EU, the Member State where its legal representative is established shall be competent. More innovatively, if neither of the above conditions is met, all EU Member States can take action against the hosting provider that fails to meet its obligations. This rule thus makes it possible to introduce a logic of power of action according to the place of destination of the service, and not necessarily according to the headquarters of the hosting provider.
- **Penalties** (Article 42): Member States must provide for mechanisms to penalise hosting providers who fail to comply with their obligations. They must be "effective, proportionate and dissuasive". They must not exceed 6% of annual income or turnover (5% for standby duty).
- **Special control measures for VLOPs:** the draft European regulation provides for special control measures for VLOPs in which the European Commission plays an important role in conducting investigations (Article 51 et seq.). This mission can go as far as imposing penalties of up to 6% of the total turnover.

The proposed Regulation considerably strengthens the obligations of hosting providers and the control and sanction systems to which they are subject. However, despite these advances, which must certainly be supported, several issues remain unresolved by the proposal at this stage and certainly require more significant progress.

3. A PROPOSAL THAT STILL NEEDS TO BE COMPLETED

Despite significant progress, the proposed European regulation needs to be amended on several important points.

Indeed, it is not clear that the text responds to the "roadmap" outlined by the Council in its conclusions of 9 June 2020 calling for *"the need for clear and harmonised evidence-based rules on responsibilities and accountability for digital services that would guarantee internet intermediaries an appropriate level of legal certainty".*

3.1 THE LIABILITY REGIME

As mentioned above, **the proposed Regulation does not call into question the principle of limited liability for hosting providers.**

Article 5 of the draft regulation thus recalls the principle that "the service provider shall not be liable for the information stored at the request of a recipient". Its liability may be called into question if the hosting provider has actual knowledge of the unlawful activity or content, and, once it has knowledge of such a situation, it has not acted "promptly" to remove the unlawful content or to make access to it impossible.

In reality, this is a pure and simple reiteration of the provisions currently contained in Article 14 of the Directive of 8 June 2000, which the present draft regulation does not fundamentally amend.

The Commission justifies this position by stating that *"the legal certainty provided by the horizontal framework of conditional exemptions from liability for providers of intermediary services, laid down in Directive 2000/31/EC, has allowed many novel services to emerge and scale-up across the internal market.* ***That framework should therefore be preserved****."*

The only effective step forward is the system of notifications provided for in Article 14, which makes it possible to formalise a series of situations in which the hosting provider cannot be held liable, the latter then being considered to have been aware of the presence of illegal content on its platform as soon as it has received such a notification.

For the rest, the principle of limited liability of hosting providers remains.
This situation does not seem to be sustainable. In fact, it is becoming increasingly clear that, far from passively receiving contributions, hosting providers are making editorial choices: by highlighting and recommending content or by censoring some of it according to their own moderation rules.

There are several ways to improve this.

The first must be the question of **the "triggering event"** to provoke the hosting provider's intervention.

Several provisions are included in the draft regulation:

- The notification mechanism (Article 14) at the initiative of natural and legal persons who report illegal content to the hosting provider;
- The trusted alerts (Article 19) whose notifications of illegal content "are processed and decided upon with priority and without delay";
- The establishment of compliance officers (Article 32) only in the VLOPs, responsible for monitoring compliance with its obligations
- The powers of online coordinators "to order the cessation of violations and to impose such remedies as may be necessary to bring the violation to an end" (section 41.2).

These new provisions must be effectively supported for adoption in the final regulation.

The second question relates to **the response time** available to the hosting provider in the presence of content that is reported to it as unlawful.

In the European Commission's proposal, the obligation to react **"expeditiously"** - the wording of the Directive of 8 June 2000 - remains just as vague as to the question of the assessment of the hosting provider's reaction time, since this point determines whether the hosting provider is liable. Yet in the absence of a clearer definition of the time limit for the hosting provider to react, there is a great risk that the illegal content in question may remain online for a long time. However, the way is narrow on these issues. As we have indeed recalled, the AVIA law had stumbled on this point by imposing, according to the constitutional judge, deadlines too short to react (1 hour for terrorist or child pornography content, 24 hours for a very important list of illegal content), failure to comply with these obligations potentially entailing heavy penalties (1 year of imprisonment and a €250,000 fine).

Similarly, the Constitutional Council had also sanctioned the fact that the AVIA law did not contain any clear exemption clause for the hosting provider, that the list of offences made the examination particularly delicate and that the criminal sanction was particularly heavy[1].

However, several proposals could be made to improve the Commission's proposal without risking censure by the French constitutional court[2]:

- The first could be to set a very short deadline (24 hours) for reacting to a referral by a trusted signatory. This obligation could only concern the very large online platforms (and not the other hosting providers). It should be noted that the code of conduct concluded in May 2016 already assigned such an objective to the VLOP signatories of the agreement[3];
- The time limit could be reduced to a shorter period for certain duly listed offences corresponding to particularly serious offences (child pornography, incitement to terrorism, etc.);

[1] *All of these elements explain why the CNCDH gave a very negative opinion on the AVIA bill, considering that the proposed mechanism could lead hosting providers to adopt such cautious attitudes that freedom of expression would ultimately be threatened*

[2] *In this respect, it should be recalled that according to case law of the Constitutional Council, the rules of European law remain subject in the hierarchy of norms to the rules contained in the Constitution (CC decision of 19 November 2004)*

[3] *By signing this code of conduct, the IT companies commit to continuing their efforts to tackle illegal hate speech online. This will include the continued development of internal procedures and staff training to guarantee that they review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary."*

- In the same way, the time limits for intervention should not be identical depending on the audience of the beneficiary considered; the presence over a long period of time of content that may be seen by thousands (millions) of internet users does not have the same consequences as the same infringement that would concern only a few people.
- Penalties for non-compliance with these review periods could also be varied according to the nature of the illegal content in question and the precise exemption clauses for the hosting provider defined by the future regulation;
- Hosting providers should draw up internal charters for combating illegal content (which is defined exclusively by national or European law and not by internal rules of the platforms) which would be legally binding on the users of their services and whose disregard would make them liable. This charter would include elements relating to the functioning of moderation, the ordering of content and the parameters of the algorithms and their evolution; the control of the respect of these commitments would obviously be ensured by the public authorities, any infringement of these obligations being likely to call into question the liability of the hosting providers;
- The obligation of a certain duty to monitor content (see below), which does not call into question the principle of the absence of a general obligation to monitor, but which falls within the framework provided by Article 15 of Directive 2000/31/EC of 8 June 2000.

However, the question of sanctioning hosting providers in the event that they are not diligent enough to remove illegal content remains entirely open. At present, the sanctions imposed in this respect remain symbolic (see CNCDH report of 10 July 2015 on the fight against hate speech on the internet). However, sanctions that are too severe must not appear "disproportionate", as this could lead to self-censorship on the part of the platforms, which would ultimately be detrimental to the exercise of freedom of expression.

3.2 THE ABSENCE OF A GENERAL MONITORING OBLIGATIONE

Once again, the draft European regulation does not amend in any way the provisions of the directive of 8 June 2000 on this point.

Article 7 thus provides that: *"no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers".*

This is an almost identical reproduction of the provisions of Article 13 of the Directive of 8 June 2000.

However, without imposing this general monitoring obligation, which is understandably delicate in terms of respect for fundamental freedoms in general and freedom of expression

[1] *L'ensemble de ces éléments explique la raison pour laquelle le CNCDH avait donné un avis très négatif à la proposition de loi AVIA en estimant que le dispositif proposé risquait de conduire les hébergeurs à des attitudes si prudentes que ce serait la liberté d'expression qui serait au final menacée*

[2] *On rappellera à ce titre que selon la jurisprudence du Conseil constitutionnel, les règles de droit européen restent soumises dans la hiérarchie des normes aux règles figurant dans la Constitution (CC décision du 19 novembre 2004)*

in particular, in several instances the text refers to situations in which the hosting provider would be informed of the presence of illegal content. This is in particular the uncertain status in this respect of the notion of moderation, which is understood to be exercised spontaneously by the hosting provider.

While there is no general monitoring obligation, the hosting provider does exercise a form of monitoring over the content. Since this surveillance may result from checks carried out using "automated means", i.e. algorithms, the question arises as to the criteria according to which hosting providers carry out this random check.

The absence of a general monitoring obligation is thus solely to the benefit of hosting providers, freeing them from any legal responsibility for the presence of illegal content on their platforms. Thus, Article 6 of the draft regulation expressly states that these "voluntary investigation" activities may not have the effect of calling into question the principle of non-liability of hosting providers. However, it says nothing about the conditions under which the latter ensure a form of random monitoring of content.

This is why the system should be developed here too. Our democracies impose an extremely restrictive liability regime on press publishers, for example, even though their audience is incomparable to that of the major platforms. These constraints have never been perceived as impeding freedom of expression and have allowed democratic debate to take place under good conditions. It therefore seems paradoxical to assert that new constraints that can now be imposed on platforms, without reaching the intensity of those that apply to press publishers, are in themselves likely to undermine freedom of expression

The principle of the lack of a general monitoring obligation must be maintained. However, it is the possible consequences that the hosting provider draws from this, in particular with regard to decisions to remove content or access, which must change. This point deserves attention in its own right (see below).

Moreover, as mentioned above, this "lack of obligation" does not prevent hosting providers from exercising some form of monitoring over content.

Several additional proposals could be made under this heading.

- A monitoring obligation on the part of hosting providers with regard to beneficiaries of services that have already been sanctioned because of the dissemination of illegal content; with regard to these persons, the powers of removal of content and access of hosting providers in the event of a "repeat offence" could be reinforced;
- An obligation of monitoring for beneficiaries beyond a specific audience; it seems legitimate to subject to exceptional monitoring those persons whose number of subscribers is singularly important and for whom the consequences of a possible infringement could be particularly heavy;
- Platforms carrying out monitoring operations on the content they host should also periodically report on this activity to the national coordinators; this obligation would make it possible to measure the intensity and nature of the activities carried out in this respect.

The question of the means used to effectively prohibit illegal content is legitimately raised.

However, since most of the burden falls on the platforms themselves, through algorithmic or human moderation, the task of the public authorities is twofold: on the one hand, to check that the platforms' rules only prohibit illegal content and to audit their human or automatic moderation resources; on the other hand, to carry out judicial review of the decisions they take.

3.3 THE QUESTION OF APPEALS AGAINST THE REMOVAL OF CONTENT AND ACCESS

This issue was largely absent from the Directive of 8 June 2000. Nothing was said about the conditions under which the VLOPs could remove content they considered illegal on their own initiative or suspend or even cancel the services they offered to certain beneficiaries.

This issue is crucial in terms of respect for fundamental freedoms and in particular freedom of expression. We can also see how a policy of withdrawing content or access in critical periods, such as electoral campaigns, could have a potential impact on the meaning of the vote and thus on the overall functioning of democracy.

Article 17 does establish a complaints system, which is also open to persons who have had their service provision suspended or terminated. Article 17.3 states that these complaints must be dealt with *"in a timely, diligent and objective manner"*.

It will be agreed that the level of requirement is minimal in this respect.

There is no guarantee in this text that access can be restored quickly enough to prevent this situation from having too disruptive an effect on the free flow of debate.

This means that responsibility will rest with a national judge who will not necessarily have the means to intervene effectively, particularly in the face of a sanction whose scope will most often go beyond the national territory.

Similarly, the grounds for removing content or access remain unclear. While the concept of illegal content is defined by the draft regulation (see above) and covers any non-compliance with national or European law, the same draft also provides that removal decisions may be based on the "incompatibility of the information with the terms and conditions of the provider" (Article 15 of the draft regulation). In this respect, it should be noted in particular that these general terms and conditions frequently refer to laws other than EU law and also refer to the jurisdiction of non-European courts to deal with certain disputes that may arise in this respect.

For example, the May 2016 Code of Conduct states that operators will consider reports for the removal of online content "against their rules and community guidelines, and, where necessary, national laws transposing Framework Decision 2008/913/JHA"[4]. Similarly, they must inform users of "the types of content not permitted under their rules and community guidelines".

The use of automated means is a concern in itself, as they may appear *"unable to reliably*

[4] *This is the Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law. Its Article 1 requires member states to enact criminal sanctions against any incitement to violence or hatred, regardless of the medium on which such messages are disseminated.*

differentiate illegal content from content that is legal in a given context" European Parliament resolution of 20 October 2020.

In this context, the following proposals can be made.

- In the name of respect for freedom of expression, removal of content or access must only be justified by its unlawful nature, i.e. ignoring a European or national standard. The European Parliament in its resolution of 20 October 2020 also calls for such a change. Moreover, one may wonder about the constitutionality of a removal for another reason in view of the case law of the Constitutional Council, which considers that free access to the internet is today one of the modalities of the constitutional principle of freedom of expression. With regard to the protection of the operating rights of hosting providers, it would be surprising if the civil and commercial provisions applicable in this field did not effectively protect their rights on this precise point too. Therefore, "incompatibility with the terms and conditions of the provider" should no longer be a reason to remove content or access in the future.
- It is also questionable whether certain "content publishers" should not benefit from enhanced protection against the risk of content and/or access removal. Indeed, such measures can have a major impact on the conduct of public debate or the functioning of democracy. Thus, one could imagine a special procedure for the following beneficiaries of services: political parties, associations receiving special recognition from the public authorities, media, for example. For the media, one could imagine that the hosting provider would not have the right to proceed unilaterally with a decision to remove the information and that this decision would have to be preceded by a prior formal notice allowing the person concerned to put forward his arguments. Similarly, for this particular category of beneficiaries, appropriate means of redress, particularly judicial, should be provided to enable them to challenge removal decisions quickly and effectively.
- Finally, the issue of measures through which a hosting provider, without actually removing content, leads to its "invisiblisation", i.e. tends to make it disappear by means of sophisticated filtering devices, must also be addressed. These processes should not be overlooked as they result in a form of quasi-removal of content, with no guarantee for the person who issued it. This potentially serious situation, in addition to raising the question of the platform acting as a genuine content publisher, must be taken into account and given special treatment, either by requiring the hosting provider to notify the author of the content of the "decision" thus taken, or by prohibiting it altogether.

3.4 THE ISSUE OF ANONYMITY

This is the great absentee in this text, which says nothing about this issue.

This is fundamental. As the CNCDH reminds us in its aforementioned 2015 report, *"the possibility of anonymity and the use of pseudonyms, which lead to a strong feeling of impunity"*, are one of the primary causes of the development of hate on the internet.

This is a major issue because it raises the question of the effectiveness of the sanction when

the author of the incriminating remarks will in fact escape prosecution.

In our view, it is not a question of calling anonymity into question, but of making the transmission of identification data unavoidable in cases where they are necessary for the proper functioning of justice.

The text should impose an obligation on the beneficiaries of services to prove their identity in order to access them. This would also be an effective way of preventing minors from being present on services to which they should not normally have access.

In this respect, Article 8 of the draft regulation on injunctions that may be addressed to hosting providers by national authorities appears to be largely insufficient to combat the impossibility of transmitting identification data to judicial authorities.

This question must therefore respect a major distinction.

The transmission of data should only concern hosting providers. Indeed, for removal measures to be effective, they must be able to be applied effectively to the persons who are the authors of the content concerned. Similarly, if the violation requires the courts to be seized, it is normal that the latter can effectively prosecute the persons responsible, after their identity has been communicated by the hosting provider.

On the other hand, there is no question of any lifting of anonymity with regard to third parties. First of all, it may be other beneficiaries of the same service, in which case anonymity may protect the author of the content from certain forms of retaliation for the comments made online. Anonymity is then a form of protection of freedom of expression.

This applies in particular to third parties whose knowledge of the author of the content could cause serious harm to those concerned. This is the case, for example, with whistleblowers, who must be protected by the rule of anonymity; otherwise they will be exposed to significant risks in the course of their work.

It should be noted that the Law of 22 December 2018 on the fight against information manipulation already imposes obligations on OLP operators to inform users of their services about the natural or legal persons who pay them remuneration in return for the promotion of information content relating to a debate of general interest.

This measure does not seem to us to threaten individual freedom in our democracies. The mechanisms for the protection of rights and freedoms are sufficiently effective and proven to protect citizens from the use of this power, which could jeopardise their situation or their rights.

CONCLUSION

The Commission's proposal of 15 December 2020 is clearly an undeniable step forward in view of the deficient nature of the regulations resulting from the directive of 8 June 2000. This text was mainly drawn up to allow the development of trade on the internet in the context of the completion of the internal market, but it is now out of date as it does not take into account the tremendous technological and usage developments that have occurred since then.

This text contains important advances that deserve to be supported in a process of adoption that is likely to be fraught with difficulties both before the Council and the European Parliament.

However, one may wonder about its lack of ambition with regard to certain fundamental principles which, by maintaining the principle of the non-liability of hosting providers and the absence of a generalised monitoring obligation, does not modify the foundations of a legal system which, up to now, has above all shown its inadequacies.

Similarly, the major issue of the removal of content and access decided unilaterally by hosting providers, which can seriously disrupt the functioning of our democracies, is still treated too lightly in this proposal.

Finally, the question of the "de facto non-liability" of the authors of illicit content, due to the absence of identification data, is not even addressed, even though it ensures a form of intolerable impunity.

Supporting the Commission's proposal will not be enough to solve the formidable challenges that the internet poses to our democracies. It is absolutely necessary to amend it thoroughly.

DIGITAL NEW DEAL
THE NEW DEAL THINK-TANK

The aim of the Digital New Deal think tank is to shed as much light as possible on the developments at work within the phenomenon of "digitalisation" (in the widest sense of the word) and to develop concrete courses of action for French and European companies and decision-makers. With the expertise of the various contributors and their insertion in the public debate, the work of the think tank will be able to play a part in the development of a French and European understanding of digital regulation supporting the implementation of a balanced and sustainable framework.

LE CONSEIL D'ADMINISTRATION

The members of the Digital New Deal Board of Directors are all founding members. They come from various backgrounds while having direct contact with the digital transformation of companies and organisations. Given their shared interest in digital issues, they decided to deepen their debate by creating a formal framework for production and publication within which they can dedicate their complementary experience to serve public and political debate. They're personally involved in the life of Digital New Deal. Arno Pons, executive officer, is responsible for strategic steering with Olivier Sichel, founder and chairman, and supervises a project manager that coordinates all the think tank's daily activities.

SÉBASTIEN BAZIN
PDG AccorHotels

NICOLAS DUFOURCQ
DG de Bpifrance

AXELLE LEMAIRE
Ex-Secrétaire d'Etat du Numérique et de l'Innovation

ALAIN MINC
Président AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
Délégué général du think tank Digital New Deal

JUDITH ROCHFELD
Professeur agrégée de Droit, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

ROBERT ZARADER
PDG Equancy

contact@thedigitalnewdeal.org

www.thedigitalnewdeal.org

OUR PUBLICATIONS

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe
Laurence Houdeville and Arno Pons - *May 2021*

Livres blancs : Partage des données & tourisme
Fabernovel et Digital New Deal - *April 2021*

Partage de données personnelles : changer la donne par la gouvernance
Personal data sharing: governance as a game changer
Matthias de Bièvre et Olivier Dion - *September 2020*

Paiement mobile sans contact – libérer les smartphones et leurs utilisateurs
Contactless mobile payment: liberating smartphones and their users
Various - *June 2020*

Réflexions dans la perspective du Digital Services Act européen
Reflections in the perspective of the European Digital Services Act
Liza Bellulo - *March 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française
Marie-Christine Levet - *November 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude
Big Tech Regulation: Empowering the Many by Regulating A Few
Sébastien Soriano - *September 2019*

Sortir du syndrome de Stockholm numérique
Jean-Romain Lhomme - *October 2018*

Le Service Public Citoyen
Paul Duan - *June 2018*

L'âge du web décentralisé
Clément Jeanneau - *April 2018*

Et si le CAC 40 ubérisait…sa R&D
Paul-François Fournier - *November 2017*

Fiscalité réelle pour un monde virtuel
Vincent Renoux - *September 2017*

Réguler le « numérique »
Joëlle Toledano - *May 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique
January 2017

La santé face au tsunami des NBIC et aux plateformistes
Laurent Alexandre - *June 2016*

Quelle politique en matière de données personnelles ?
Judith Rochfeld - *September 2015*

Etat des lieux du numérique en Europe
Olivier Sichel - *July 2015*

THINK-TANK
DIGITAL
NEW DEAL

June 2021

www.thedigitalnewdeal.org