Grupo de Trabajo Consulta sobre Digital Services Act de la Comisión Europea

September 7th, 2020

From FIDE and Alastria we set up a Working Group to respond to the European Commission's public consultation on the "Digital Services Act" with the aim of collecting its implications, alternatives and possible future scenarios, in short, a series of proposals that can help the European legislator to determine how the regulation of the scenario referred to in the consultation can be addressed. This work was presented to the EC on 7 September.

I. How to effectively keep users safer online?

Online services and platforms play a key role in the promotion of freedom of expression, culture and art, pluralism, education, and access to information for users. However, that generalization of access and speech has also served as a floor for certain users to disseminate content which is illegal, misinformative or otherwise harmful for other users.

It is apparent that a wide variety of fundamental rights are affected, such as freedom of information or expression. The Digital Services Act (DSA) should balance all rights at stake and avoid barriers which may be a potential detriment to fundamental rights, or that limit freedom of expression, or creativity of users. In addition, the DSA should take into account that what makes sense for one type of online service providers may not be appropriate, or technically feasible, for others (e.g., content-sharing platforms are different to a search engine, or a platform that hosts mobile apps). Regulation must also ensure the fundamental right to respect for user privacy, where users communicate privately or in small groups, Cloud customers own their data and cloud providers process it based on their instructions. Further, the protection of rights should also be balanced with an adequate development of minors and their progressive access to content and services: it is important to maintain a degree of flexibility in the way that services are developed, to ensure that children are adequately protected without unintentionally curtailing their online access and digital development.

The current legal framework has enabled the plurality and growth of online platforms and businesses and users to enjoy and benefit from these online services. This is because the liability regime foreseen by the E-commerce Directive has proven to provide legal certainty to all players. Legal certainty needs to be preserved.

However, in recent years law-makers and courts have passed (or are in their way to pass) laws and issued decisions on areas such as hate speech, harmful online content, minor protection, misinformation or dissemination of terrorist content that have resulted, or may result, in the fragmentation of the internal market while still not resolving the underlying desired protective purpose holistically, and hampering key principles of EU law such as the country-of-origin principle, the freedom of establishment and the freedom to provide cross-border services.

The European institutions have issued a variety of documents and position papers as well. Namely:

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, dated September 28, 2017.

- Commission Recommendation dated January 3, 2018, on measures to effectively tackle illegal content online.
- EU Code of Practice on Disinformation.
- EU Code of Practice on countering illegal hate speech online.
- European Parliament legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online.
- Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA and the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, on EU strategy for a more effective fight against child sexual abuse, dated July 24, 2020.
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.
- Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Harmonization across the Single Market should be a priority for the DSA. The DSA should avoid fragmentation and secure a balanced legal framework that enables the protection of all players' rights and interests. The DSA should ensure that all users may freely exercise their right to receive and provide information and opinions, to be creative and to learn, and to contribute to the pluralism of media and political diversity. Based on this harmonization goal, the DSA should ensure a legal framework that is clear, proportionate and precise in order to act against illegal content, while it protects and balances all fundamental rights at stake and safeguards the principles of country-of-origin, freedom of establishment and freedom to provide cross-border services.

Consequently, decisions on illegal content removal cannot be based on market or business criteria of online services and business, but on transparent and harmonized rules. Users trust on the legal framework applicable to unlawful content removal plays a key role. Thus, the DSA should not leverage private companies such as online platforms or businesses to make decisions that may limit the exercise of fundamental rights. Deciding whether content is illegal under local laws can often be challenging, due to incomplete factual records and/or complexity as regards legal determinations. To that end, the DSA should maintain a liability regime based on the notice-and-takedown system, in which there is no liability without effective knowledge. The current notice-and-takedown system provides users with proper and sufficient tools and procedures to identify and act against unlawful content.

Adequate take-down requirements should include, at minimum: a clear identification of the content at issue by specific reference (e.g. by URL, video timestamp, or other unique identifier), state the law and basis of the legal claim; a clear identification of the identity of the sender of the notice where the nature of the rights asserted requires identification of the rightsholder; a personal attestation of the good faith and validity of the claim; and an acknowledgement of the rights impacted so that a copy of notice may be sent to the original content creator.

Given the state of technology, over-reliance on automation presents a real risk of blocking lawful content and impacting the fundamental rights of European citizens (technology is still unable to discern differences in context that can be critical to determining whether content is legal or not).

Therefore, the prohibition on general monitoring obligations in Article 15 of the e-Commerce Directive should remain, as the effective knowledge regime based on appropriate notice-and-takedown grants clarity to all players, as it ensures a balanced framework for businesses and protects the interests of users. However, the effective knowledge regime should not prevent or disincentivize online service providers from taking voluntary actions to remove illegal content by considering that those actions are a general active selection or monitoring of content.

Likewise, the DSA should ensure a proper balance between timely actions and accuracy of removals. In particularly harmful cases (e.g. terrorist content, child pornography) there may be specific rules to speed up removals. The situations where such specific rules on timing apply should be clearly defined by the DSA to avoid leaving the decision on the hands of any of the involved parties (which would likely lead to disputes and therefore to lack of legal certainty).

Also, the DSA should bear in mind the distinction between illegal and harmful (but not illegal) content and focus on acting against content that is strictly and clearly illegal. To this end, online platforms should count with a clear, harmonized, and objective framework on what is "illegal" content subject to be removed under the DSA. It cannot be expected that online platforms act against content that is not illegal against which Member States cannot limit based on the rule of law.

The DSA should consider that the affected online service providers should have clear content policies, systems for reviewing user flags of content, and a system to notify users when their content has been removed with an opportunity to appeal. That would contribute to transparency and clarity. However, that is not equivalent to opening up the underlying algorithms besides a general understanding of how the algorithm works. Disclosing the underlying algorithms could open up such systems for abuse and risks to trade secrets.

In sum, the DSA must ensure harmonization in the European internal market, provide legal certainty to all stakeholders while striking an adequate balance between the individual rights at stake, and take into account that technology and its use evolve and therefore the law should be flexible enough to accommodate those changes.

II. Reviewing the liability regime of digital services acting as intermediaries?

Keywords: intermediaries, hosting, access, duty of care, notice and take down.

Several years after the enactment of Directive 2000/31 of 8 June 2000, on electronic commerce (DCE), it is necessary to adapt its liability regulatory framework to the new Internet business models.

The evolution of the DCE should represent a great opportunity for the European lawmakers so that they can begin to consider the advantages that blockchain technology can offer in terms of algorithmic transparency, as well as think about the role and responsibilities of those companies which provide some services to third parties using this type of distributed ledger technologies. The advantages offered by blockchain technology should be considered in the future Digital Services Act (DSA)[1].

[1] https://academy.binance.com/blockchain/how-does-blockchain-work

Here some ideas to be considered by the European lawmakers.

2 The liability regime for online intermediaries is primarily established in the E- Commerce Directive, which distinguishes between different types of services: the so called 'mere conduits', 'caching services', and 'hosting services'. In your understanding, are these categories sufficiently clear and complete for characterizing and regulating today's digital intermediary services?

DCE differentiates between three types of intermediaries: those of "mere transmission" (focused on transmitting in a communications network data provided by the recipient of the service or facilitating access to a communications network); those of "buffer memory (Caching)" (focused on transmitting data provided by the recipient of the service over a communications network); and those of "data hosting" (focused on storing data provided by the recipient of the service).

While "mere transmission" and "buffer memory" are still fit for purpose, "data hosting" is no longer able to fit other type of services emerged after the DCE came into force. That would be the case of the loading up software or music services, social networks, peer-2-peer services, blogs, or other discussion forums. All these "new" services have been categorized as "hosting activity", even though this function was initially reserved for the inert accommodation of data, such as web pages[2]. Hence, the scenario resulting from the entry of all these new service providers has raised uncertainties that need some clarification from European lawmakers.

Therefore, a harmonized, graduated, and conditional exemption scheme continues to be needed as a foundational principle of the Internet. We understand the need to ensure the framework reflects the nature of today's services.

DSA should also represent a fantastic opportunity to consider the case of the digital services providers on a Blockchain Network. Moreover, regarding the information and data that is distributed over a Blockchain Network for the sole effect of the software, should the concept of "mere conduits" of data hosting be applied to all the companies that provide digital services to third parties managing regular nodes?

3. Are there aspects that require further legal clarification?

DSA should clarify some issues that have been addressed by domestic courts or by the Member States themselves. For instance, the Court of Justice of the European Union has stated that Wi-Fi network access provider should be under the protection of art. 12 DCE, provided that these services constitute an economic activity[3]. Likewise, the Court of Justice of the European Union has also classified as a hosting services provider the platform focused in managing an online social network[4]. However, the Court of Justice of the European Union has not clarified under which classification the domain name services providers[5] might be located.

---

[2] ARROYO AMAYUELAS E. (2020). Liability of internet intermediaries safe and future-proof harbours? Cuadernos de Derecho Transnacional, Vol. 12, No 1, pp. 811.

[3] STJUE C-484/14, Tobbias MacFadden

[4] STJUE C-360/10, Netlog

[5] 19 STJUE C-521/17, SNB-REAC

DCE does not establish either whether the exclusion of liability should apply to those intermediary service providers who, being recipients of the hosting service, allow their own users to create their content, as long as this activity can be considered a service of the information society. In Spain, for instance, third-party comments on a blog and messages on a forum or chat have been subsumed in the rules on exclusion of liability of the service provider of hosting[6].

Also, it would be necessary to clarify if the liability exemption extends to those services providers who carry out purely free activities that are not even financed through advertising banners (i.e. personal blogs). If these providers were outside the definition of "information society services", since DCE only applies to information society service providers (all service provided in exchange for fees, remotely, electronically and at the individual request of a recipient of those services) they would not be able to enjoy the liability exemption privilege. Nevertheless, some Member States do apply the exemption when the service is provided free of charge[7].

The aforementioned assumptions would be just some examples to be considered by the DSA.

4. Does the current legal framework dis-incentivize service providers to take proactive measures against illegal activities? If yes, please provide your view on how disincentives could be corrected.

Perhaps current "best efforts rules" are not effective enough to combat illegal content online.

Therefore, DSA might encourage service providers to establish complementary mechanisms to the timely removal of illegal content, goods or services (take down) in order to prevent them from being reloaded on online platforms (stay down) after they have been removed. Also, they should be encouraged to take pro-active measures to detect and remove illegal content, without losing their liability exemption, as long as these measures do not constitute general monitoring.

The new regulatory framework should also clearly lay out responsibilities under a notice & action system and further might impose online service providers to take additional action against unlawful content and activity on their services, in a manner that preserves the foundational principles of the open Internet.

Without prejudice to the foregoing, the basic legal principle that passive online intermediaries should not be held liable for the acts of their users, since these digital services have no knowledge, control or management activity over the content their users upload and exchange when using their services, should be preserved by the European Commission.

To conclude this section, in any event, repeated non-compliance should lead to the loss of the exemption provided for in art. 14 of the LDC[8].

[6] ARROYO AMAYUELAS E. (2020). Liability of internet intermediaries safe and future-proof harbours? Cuadernos de Derecho Transnacional, Vol. 12, No 1, pp. 814.

[7] ARROYO AMAYUELAS E. (2020). Liability of internet intermediaries safe and future-proof harbours? Cuadernos de Derecho Transnacional, Vol. 12, No 1, pp. 816.

[8] https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/

5. Do you think that the concept characterizing intermediary service providers as playing a role of a 'mere technical, automatic and passive nature' in the transmission of information (recital 42 of the E-Commerce Directive) is sufficiently clear and still valid? Please explain.

The distinction made by the recital 42 DCE between active and passive providers only refers to access and caching intermediaries. However, those requirements have been extended to hosting activities thanks to the work of Court of Justice of the European Union (C-236/08 - C-238/08, of March 23, 2010, Google France v Vuitton, regarding AdWords Google service). Unfortunately, the Court of Justice of the European Union unanswered what might be considered more than merely technical, automatic, and passive nature, leaving that task to national judges[9]. Hence, DSA is a good opportunity to harmonize a "there is no clear view" in Member State court rulings of what this distinction means and which services are, or are not, "active". Art. 14 DCE is not applicable in case of the hosting activity exceeds the mere technical, passive service. The Commission should consider an amendment of art. 14 DCE to recognize a new category of 'active' hosts who have a certain degree of control of the content shown and uploaded users.

Therefore, DSA should clarify and differentiate between the services offered by active and passive intermediaries and the role they are playing nowadays. The standard used by the Court of Justice of the European Union in the *L'Oréal v eBay* case to determine whether an information society service is acting as a mere intermediary or not is no longer valid, considering the different business models applicable to intermediaries. In this sense, DSA should evolve the unclear concept of "active" and "passive" hosts and perhaps replace it with more appropriate concepts/contents reflecting the technical reality of today's services.

6. The E-commerce Directive also prohibits Member States from imposing on intermediary service providers general monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users. In your view, is this approach, balancing risks to different rights and policy objectives, still appropriate today? Is there further clarity needed as to the parameters for 'general monitoring obligations'?

The general prohibition of monitoring obligations or obligations to seek facts or circumstances of illegal activities conducted on their service by their users, is perfectly balanced and still appropriate nowadays. The intermediaries should not be forced to carry out any active searches for illegal activities or contents, in the same way that they cannot carry out supervision activities of the contents that users can host, which would not be consistent with their own nature and activity.

Nevertheless, 'active' hosting service providers should be encouraged to take targeted and pro-active measures to detect and remove illegal content, without losing their liability exemption, as long as these measures are targeted and do not constitute general monitoring. Such solutions would use technical tools to make detection and enforcement of copyright infringements more effective while stopping short of general monitoring (e.g. solutions like Smart Protection, a technology-based anti-piracy platform that detects and removes pirated contents on the Internet by searching for infringements and requesting its removal in an automated and effective way.)

[9] ARROYO AMAYUELAS E. (2020). Liability of internet intermediaries safe and future-proof harbours? Cuadernos de Derecho Transnacional, Vol. 12, No 1, pp. 815.

Bibliography

DG CONNECT PAPER: https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf

ARROYO AMAYUELAS E. (2020). Liability of internet intermediaries safe and future-proof harbours. Cuadernos de Derecho Transnacional, Vol. 12, No 1, pp. 808-837.

MAESTRE RODRIGUEZ J. (2017). The responsibility of service providers of the information society and the concept of new public. Revista Derecho & Sociedad, N° 49 / pp. 77-86.

SANGÜESA, R. (2018). Artificial intelligence and algorithmic transparency: It's complicated. BID: textos universitaris de biblioteconomia i documentació, núm. 41.

III. What issues derive from the gatekeeper power of digital platforms?

This module of the consultation seeks informed views from all stakeholders on this framing: on the scope, the specific problems and their implications, the definition and parameters for addressing possible issues deriving from the economic power of large, gatekeeper platforms.
The aim is to ensure that markets characterised by large platforms with significant network effects acting as gatekeepers remain fair and competitive for innovate companies and new market participants.
Once the text of the review has been analysed and the questions established, there are several relevant questions about the application of the power of control by gatekeepers on digital platforms:

1. Unfair competition and abuse of dominant positions.

The most powerful online platforms can also take over (potential) competitors. It is hard for an existing competitor or a potential new entrant to overcome the competitive advantage of these online platforms.

The law does not punish the position of dominance, not that of a monopoly in the market, but rather the abuse of its market position.

Although current Competition toolbox is still fit for purpose, there is a need to update and adapt the tools and methodologies of the current rules to the new digital environment, as the ex-post intervention over digital has shown to be insufficient due to the dynamism of digital markets.

2. Lack of transparency in the offer of products and services on digital platforms.

Sometimes it is not easy to know who provides the service. It is necessary to avoid that the provider of the service “disguises himself” as an intermediary to avoid the application of the sectoral regulation corresponding to said service. This means that transparency about the role of the platform is essential. Accordingly, all the transparency requirements gathered in the P2B Regulation and Consumer Law Framework, have as well to be fulfilled by digital platforms with the aim of being compliant with law.

In this regard, it might be necessary that consumers and customers are aware about who is actually providing goods or services, in order to keep and reinforce intermediaries’ safe harbour role.

In addition, the need arises to establish rules to regulate the offer of products and services on legal platforms within legal parameters, to avoid unilateral modifications or changes by companies that are not in accordance with the legal terms and conditions and thus comply with a more equitable and transparent environment for all operators.

These contracts, clauses and terms and conditions imposed by digital platforms, must be written in an easily accessible, simple, and understandable way. It also must communicate in advance the changes in their general conditions of service.

3. **Search engines: The service of classifying websites, search results that may favour some results over others, favouring or disfavouring certain companies. Establishment of clear positioning rules.**

The algorithms of social networks and search engines are based on criteria that are not transparent and that affect diversity and pluralism, making some information and opinions invisible or relegated, and generating a segmentation of public debate.

It is required to establish fair and transparent rules to allow effective competition and equal user access under the DSA proposal on ex-ante rules, as Regulation P2B2C or the Omnibus Directive

4. **Configuration of dispute resolution mechanisms between users and merchants and means through which any user / third party can send complaints, claims or reports about illegal or abusive practices.**

Facilitate these mechanisms through internal, regulated, and controlled systems, to process these disputes and claims. They need to be easily accessible, free, with deadlines and always based on the principles of transparency and equality. In this sense, P2B Regulation must be respected in any event, reinforcing all the mechanisms that must be required.

5. **Guarantee the application of the principles established in the RGPD, especially in relation to the rights established in the RGPD, with special attention to the right of portability.**

As a requirement of the power of control by gatekeepers on digital platforms, it is essential to comply with the RGPD: protecting the privacy and integrity of the individual.
The portability right that users have, the possibility of the user to control their personal data and to be able to extract, delete or migrate them from one digital platform, or from one to another, must be very well specified.

These digital platforms must include certain information in their terms and conditions on technical and contractual access, or lack thereof, that professionals have to personal or non-personal data provided by professional users or consumers using the services of intermediation, or that are generated through the provision the services.

6. **Guarantees of interoperability between digital platforms.**

The aim is to ensure the free circulation and exchange of information between platforms, which also guarantees cost reduction and management efficiency.

The study and review of interoperability between digital platforms are more than necessary, and are essential for cooperation, integration, and the possibility of joint service provision by various organizations.

The normal development of electronic administration and the Information Society itself will depend on it, as a field for public policies, the transfer of technology and principles and rights.

7. **Implementation of internal mechanisms to control publications (fake news; protection of minors; illegal / offensive content or promotion of violent actions, etc.) making a judgment weighing freedom of expression and the public interest.**

It is important to establish ethical standards, of good practice and good use, to avoid fake news where the scope of publications can be very harmful at times.

Moreover, self-regulation in digital platforms must be fostered. In this sense, they should establish a clear distinction between illegal and harmful or offensive contents, in order to identify specific measures to be implemented.

The conditions for the introduction of national duties of care (currently regulated at whereas (48) of the ECD) must be also reconsidered in order to avoid market fragmentation.

8. **Guarantee of impartiality and transparency of the actions carried out by the platforms, advertising systems, etc. (configuration of algorithmic systems).**

Algorithms are responsible for fundamental decisions about the content that we can effectively access, facilitating or hindering access to the content available on the Internet. It is true that an architecture of algorithms and the use of types of artificial intelligence that select the content that we can visualize based on people's predilections and that aim to leave them satisfied, may have good intentions and be a successful commercial strategy to attract customers, but some measures adopted by these intermediaries to limit the dissemination of digital content, such as to combat fake news, through algorithm-based content removal systems, are not transparent and violate the minimum standards of due process and / or limit improperly limit access to content or its dissemination.

This conditional access to the contents, as well as the removal of those understood as "inappropriate" or "offensive" - in the opinion of the companies themselves and their "moderators"- are carried out with a lack of transparency and due process for making their decisions or the possibility to appeal against them. The main companies in the sector do not even publicly report how many removals of their own choosing they carry out. All these practices distance intermediaries from international standards on legitimate restrictions on freedom of expression. There would probably be no interoperability problem if all operations were managed on a single Blockchain.

As already explained before, there must be consistency with the rules already implemented by the Regulation P2B2C (for B2B scenarios) and the Omnibus Directive (for B2C scenarios). Nevertheless, utmost precaution shall be taken in order not to interfere with platforms' commercial secrets.

International organizations for the protection of freedom of expression have begun to warn about this problem.

9. The role of the gatekeeper in digital platforms.

Companies that provide platforms and applications on the Internet play a key role in accessing an open and free Internet due to the role they occupy as intermediaries between users and the content available on the Internet. But this vital new role makes them a potential risk to freedom of expression and the free flow of information on the Internet.

These "intermediaries" are not only capable of monitoring all the content produced by third parties, but they can intervene in them, ordering and prioritizing their access and, therefore, determining which content and sources of information a user can view and which not. They can also block and delete content, which can be discourses protected by the right to freedom of expression, as well as user accounts or profiles. These actions are often forced by external pressure from government authorities or other private actors, but also by their own decisions.

It would be necessary to establish specific rules to address any negative social and economic effects that the gatekeeper function has on online platforms, and a specific regulatory authority is also necessary to enforce these rules, at the European level, to avoid regulatory dispersion. Thus, establishing a regulatory framework for the EU, and that each country can transpose into its standard.

Some of the most relevant characteristics that the gatekeepers have in its role in large online platform companies are:

- ✓ Large user base.
- ✓ They capture a large share of total revenue of specific markets.
- ✓ They build on and exploit strong network effects.
- ✓ They raise barriers to entry for competitors.
- ✓ They accumulate valuable and diverse data and information.
- ✓ They are able to extend their dominant position rapidly to adjacent markets.
- ✓ They have access to non-rivalrous data.

In addition to the foregoing about the criteria combination, it would be really useful and interesting to create a sort of a European quality label according to minimum requirements and standards which may allow people to identify clearly companies that assume a gatekeeper role. In this regard, the EC must provide a clear definition of “gatekeeper” and “future-proof”. On the other hand, it becomes essential to provide transparent, reliable, and clear information about the specific characteristics and services provided by the online platforms that may reinforce its role as guardian.

In this sense, platforms aiming to take a gatekeeper role, should meet strict criteria, validated by a supranational authority, after having satisfactorily fulfilled a minimum of standards set in a transparent manner. All this should be conveniently informed to the users, so that they may be aware of the platforms that, effectively, comply with the requirements and standards that enable them to assume the role of gatekeeper, reinforcing the principles of quality, transparency and information security.

Moreover, “gate keeper role” definition and the different criteria that they have to comply with, need to be clear and strictly defined in a first stage, supported by evidences, in such a way that only online platforms meeting the basic minimum criteria established may be identified as companies with an effective gatekeeper role, as long as, additionally, other standards and

requirements are fulfilled. In this sense, not any business model or technology should be discriminated (an "agnostic business model" must be settled).

IV. Other emerging issues and opportunities, including Online Advertising and Smart contracts

1. Online advertising

Online advertising has made possible the proliferation of business models based on the monetization of users' attention. Thus, consumers may access a myriad of services 'for free' in exchange of their personal information, including their interactions with online platforms (e.g. search engines, social media, display of videos and music, etc.).

Advertising has contributed for having made the Internet the free, open, pluralistic place it is today. Websites, blogs, social networks, mobile apps, videos, etc.—nearly all of that is funded by ads. From the very beginning, the ad-supported Internet was a net neutrality-driven innovation where anyone with a good idea could scale up, reach a mass audience, and make a living. This was true for publishers and advertisers alike; never was it as easy to find a niche global audience if you had something unique to offer. Besides, advertising has contributed significantly to reducing the digital divide. An alternative web, one dependent on subscriptions and full of paywalls, would be out of reach for too many people without the income to pay for it.

Despite the central role of online advertising for digital platforms, there is no common legislation on this area[10]. Therefore, Member States are increasingly resorting to national legislation to impose new obligations on digital platforms, including ex-ante duties of care[11] (*e.g.* hate speech, fake reviews, etc.). In this context, the DSA can be an invaluable opportunity to better legislate the legal framework applicable to online advertising, mitigating market fragmentation and achieving a more predictable legal framework for all the players participating in the online advertising value chain.

1.1. Risk related to content curation based on targeted advertising

Concerns have arisen about the way online platforms curate content to increase revenues from advertising. Simply put, the profiling of users is used to display content capable of keeping their attention while showing targeted advertising. The Committee of Legal Affairs of the European Parliament considers that "*a business model that determines the visibility of content exclusively based on the aptitude of content to generate advertisement revenues is detrimental to digital societies*" [12] and, therefore, suggest the DSA to incorporate the following measures.

---

[10] It is worth mentioning the existence of a relevant self-regulatory system coordinated by the European Advertising Standards Alliance.

[11] According to recital (48) of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("**e-Commerce Directive**"), Member States can require "service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities". In other words, although the e-Commerce Directive does not impose a duty of care on digital platforms, it gives room to Member States to do so.

[12] Draft report: Motion of a European Parliament Resolution with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019 (INL). Committee on Legal Affairs of the European Parliament. April 22, 2020 ("**EP Draft Report**").

- First, promoting contextual rather than targeted behavioral advertising, the latter being considered more intrusive. To this aim the European Parliament recommends to set clear boundaries for targeted advertising by (i) introducing fair contractual obligations to facilitate data sharing, such as facilitating data interoperability and portability; and (ii) allowing users' control over the use of targeted advertising based on their behavior on the platform or a third party site[13]. Nevertheless, in our view, this legislation should be consistent with the current regime established by the RGPD, to avoid potential uncertainties regarding the validity of the consent provided by users.
- Second, to ensure users' influence over the criteria used to curate content addressed to them, including the possibility of opting out from any content curation[14]. Besides, the European Parliament suggests the creation of a European Agency on Content Management having, among other tasks, the regular auditing of curation algorithms. More importantly, failure to provide access for the European Agency to curation algorithms would entail fines at up to 4% of the total worldwide turnover of the infringing platform[15]. The implementation of such measures shall not affect, by any means, platform's right to keep curation algorithms confidential subject to the conditions set forth by Directive 2016/943 of June 2016 on the protection of undisclosed know how and business information (trade secrets). Therefore, utmost precaution must be taken when specifying the actual information to be disclosed by digital platforms.

1.2. Increased transparency

1.2.1. Regarding advertisements displayed

The EP Draft Report also promotes more transparency and fairness regarding the conditions in which online advertising is displayed by online platforms. To this aim, the European Parliament recommends online platforms to "*make available an archive of sponsored advertisements that were shown to their users, including the following:*

- *whether the advertisement is currently active or inactive,*
- *the timespan during which the advertisement was active,*
- *the name and contact details of the advertiser,*
- *the total number of users reached,*
- *information on the group of users targeted,*
- *the amount paid for the advertisement*"[16]

The regulation of online advertising contractual terms in the DSA makes sense when considering that Online advertising tools and online advertising exchanges which are not provided with the aim of facilitating the initiation of direct transactions and which do not involve a contractual relationship with consumers are expressly excluded from the Regulation (EU) 2019/1150 on promoting fairness and transparency. Nevertheless, doubts arise as to whether the information imposes an undue burden on digital platforms.

Technology and marketing companies seem reluctant to introducing prescriptive measures on transparency, alleging that such measures could impair innovation and quickly become

[13] Sections 11-13 EP Draft Report.

[14] Section 14 EP Draft Report.

[15] Page 9 EP Draft Report.

[16] Draft report: Motion of a European Parliament Resolution with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019 (INL). Committee on Legal Affairs of the European Parliament (April 22, 2020).

outdated[17]. In the alternative, they suggest industry-driven approaches and technical standards to foster transparency.

1.2.2. Regarding disinformation

In addition, the DSA could be used as an effective tool to enhance digital platforms collaboration in the fight against disinformation. An effective tool would be to demand increased transparency regarding the tools and strategies used by the platforms to remove harmful and illegal content (*e.g. fake news, fake reviews…*). To this aim, the EP Draft "*proposes that the Digital Services Act include a regulation that establishes contractual rights as regards content management, lays down transparent, binding and uniform standards and procedures for content moderation, and guarantees accessible and independent recourse to judicial redress*"[18]. Such measures shall be reinforced through an obligation to publish reports describing the main actions that digital platforms have taken to achieve these aims.

1.2.3. Among players

A certain amount of transparency among players is necessary for the entire online advertising ecosystem to flourish. For example, publishers wish to inform advertisers about their available inventory, which in turn helps advertisers make better decisions about their financial investments and return. It is a mutually dependent set of relationships, where the success of each participant enables and furthers the success of the others.

However, transparency and disclosures must be crafted in a way that benefits all participants and avoids making it easy for ad ecosystem participants to "game the system," for example, to try to appear more relevant than they are, or allowing competitors to copy innovations, free-ride on others' intellectual property and undermine the incentive to make improvements.

Third party measurement providers, industry initiatives, and standards organizations have worked together to increase transparency and consistency in reporting. For example: IAB Ads.txt project, Trustworthy Accountability Group (TAG) -especially its Business Transparency Committee-, the Code of Conduct for Programmatic Advertising of the BVDW (IAB Germany) or the IAB Transparency and Consent Framework (TCF), among others. Government recognition of the industry's efforts in this space would be extremely helpful to encourage greater stakeholder participation.

1.2.4. Actions digital service providers could take in order to increase transparency

Depending on the agents involved, digital services providers could undertake several actions addressed to increase transparency.

- **For advertisers:** Digital service providers could provide advertisers with ad placement controls that allow both small and large advertisers to reach their desired audience consistently with their brand marketing goals, as well as tools that allow advertisers to evaluate their ad performance and effectiveness. In addition, digital service providers should integrate with third party measurement providers and organizations dedicated to developing industry standards, so advertisers have access to not only accurate, but also uniform ad measurement. See, e.g., Media Rating Council and. the IAB Tech Lab's Open Measurement Working Group.
- **For publishers:** Digital service providers could provide publishers with transparency, flexibility, and the ability to review and control the types of ads that appear on a publisher's website or apps.

[17] IAB Europe's preliminary comments on the review of legal framework for digital services (Digital Services Act) – Executive Summary May 28, 2020.
[18] Section 2 EP Draft.

- **For users:** Digital service providers could give users information, choice, and control as to the ads they see. For example, whether they wish to have ads personalized at all, or stop seeing a specific ad.

1.3. Online platforms liability regarding advertising

In general terms, the DSA must maintain the safe harbor provided by article 14 of the e-Commerce Directive. Thus, an online platform will not be liable for advertisements uploaded by third parties if (i) it does not have 'actual knowledge' or is 'not aware' of facts or circumstances from which the illegal activity is apparent; or (ii) upon obtaining such knowledge or awareness, the platform acts 'expeditiously' to remove or to disable access to the advertisement. This liability system is reinforced by the prohibition on general monitoring set forth by its article 15, meaning that Member States shall not impose a general obligation on intermediaries to monitor the information they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Online platforms liability regarding the display of online advertising can be related to both, the identification of the advertisement or its content.

1.3.1. Identification of advertisements: Disclosure labels

Disguised advertising is currently prohibited by article 7.2 of the Unfair Commercial Practices Directive[19], considering misleading the failure to identify the commercial intent of the commercial practice if not already apparent from the context. That is, disguised advertisement can be defined as any type of commercial communication intended not to be perceived as such by an average consumer.

As a general rule, liability regarding disguised advertising shall be on the entity controlling the form and content of the advertisement: the advertiser. By way of illustration, online platforms acting as intermediaries are not aware of whether content uploaded by influencers shall be labelled as 'advertising' or not. Nevertheless, according to the EU Commission, the safe harbor must not apply to native advertising. The Commission considers that digital platforms are responsible of creating website structures intended to mislead consumers and, therefore, must be liable for the contents published under their structures: "*The formats for the presentation of content and for the presentation of labels disclosing commercial intent are under the control of [online social media] providers. In addition, in some cases OSM platforms actively engage in the process of native advertising, given their rules and systems for checking and approving content. In short, in those cases OSM providers go beyond mere hosting*"[20]. The liability of digital platforms regarding disguised advertising in the context of native advertising shall be analyzed on a case-by-case basis, without automatically rejecting the application of the safe harbor to all digital platforms, in all circumstances.

1.3.2. Illegal advertising: NTD proceedings and a sound Good Samaritan Defense

Regarding illegal advertising (e.g. tobacco products, gaming, drugs, spirits, etc.), the current ex post liability regime must apply. Nevertheless, the introduction of a regulated notice-and-take down procedure should be followed by a proper counter-notification process allowing the protection of users without jeopardizing freedom of speech, which also extends to commercial speech.

---

[19] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market.

[20] European Commission Behavioral study on Advertising and Marketing in Online Social Media. Final report prepared by the GfK Consortium (June 2018), *see* page 45.

Besides, following the EU Commission Recommendation on Illegal Content Online[21], digital platforms must be encouraged to adopting voluntary measures to tackle illegal content online. Nevertheless, the adoption of such measures shall not translate in the platform being considered as going beyond mere hosting, thus losing its liability safe harbor. To this aim, the introduction of a sound Good Samaritan clause should be introduced in the DSA, meaning that the introduction of proactive measures to tackle illegal content should not automatically lead to the intermediary losing its liability shield. Such measures are of the essence in order not to disincentive voluntary measures to tackle illegal content.

Nevertheless, perpetrators of scams or fraud will always try to find ways to game platforms and systems to commit cybercrime. Whatever guise these cybercrimes come in, it is central to all responsible parts of the online advertising industry to combat this behaviour to ensure a sustainable future for the ecosystem. Digital service providers in this area must have mandatory ad policies prohibiting illegal behaviour and be designed to protect users. These policies should evolve as abuse vectors evolve, including where and when consumer needs change (e.g., abuses that arose in connection with COVID 19). Nevertheless, success in this area cannot be achieved by targeting the bad ads on their own, and there is scope for relevant agencies outside advertising, *including within government*, to work to target the perpetrators of these crimes.

Finally, digital services that help publishers monetize their content should help maintain trust in the ecosystem by setting limits on what is monetized, prohibiting the monetization of content that is illegal, promotes illegal activity or infringes on the legal rights of others. Digital services should be encouraged to develop clear policies and enforcement tools to address these issues.

2. - Smart contracts

Is there sufficient legal clarity in the EU for the provision and use of "smart contracts" – e.g. with regard to validity, applicable law and jurisdiction? Explanation of the difficulties.

One of the main problems that regulation of "smart contracts" faces is that there is no definition of the concept, and it is a fact that depending on who uses this concept they are speaking about a different thing. A "smart contract" for a software engineer is different to the same concept for a blockchain expert, for an electronic identity specialist or for a contractual lawyer. Therefore, any regulation should focus on defining the matter that it wants to regulate.

Once the concept has been defined and a decision has been made regarding the object of the regulation, an analysis can be made regarding how to focus that regulation and what approach it should take.

If the concept of "smart contract" refers more to a set of automated instructions that trigger a consequence when one or more conditions are met, the regulation should take into consideration the legislation regarding software development.

If the concept of "smart contract" includes also the legal conditions for the validity of a contract as an agreement between two or more parties regarding the assumption of obligations to give something or to carry out an action, the regulation would take into consideration the existing approach to contracts law.

[21] Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online.

Very probably, once the definition is clear, it will be clear that many of the problems that can be perceived when discussing “smart contracts” are already solved, either as software development issues or as purely legal issues. However, it would still be necessary to focus on use cases and applications of “smart contracts” to determine if there are specific issues that need special regulation. As a methodology, it could be very helpful to analyze a broad list of uses cases of “smart contracts” and the problems that can arise by using them and try to solve those problems with the existing regulations.

It would probably be very helpful to establish a set of recommendations or minimum requisites to organize a common approach the validity of “smart contracts” in the European Union. For instance, from the technical side, listing a number of minimum items that should be contained in any “smart contract”; from the legal side, the minimum requisites that would be necessary to be able to consider any “smart contract” as a valid legal contract. Nevertheless, a global view should be taken regarding these aspects, as any technical development, especially when it is based in the use of communications networks, cannot be regulated regionally and independently from the rest of the world.

2.1. Are there other emerging issues in the space of online advertising you would like to flag?

The interpretation proposed by the EDPC regarding what should be understood as free consent to receive online advertising raises some very serious problems for the development of online activity, which make it advisable to reconsider this issue.

In particular, the referred problem arose in November 2018, when the UK and Austrian data protection authorities issued two resolutions interpreting Article 7(4) of the GDPR in the opposite direction.

In its resolution, the ICO considers that Article 7(4) of the GDPR, concerning the safeguards to assess the freedom of consent required for some secondary data processing activities (such as advertising), must be interpreted in accordance with the reasoning in Whereas 43 of the GDPR, which states that in these cases, consent has not been freely granted.

Also in November 2018, the Austrian data protection authority pronounced on the interpretation of the same article, but in the opposite sense to the UK authority, stating that the freedom of consent cannot be questioned when it is requested as a condition to receive a service, because users can always choose another provider or not consume the service.

The Austrian authority considers that, to interpret Article 7(4) of the GDPR, account should be taken not only of recital 43 but also of recital 42, which states that, in order to assess whether consent is freely given, it is necessary to check whether the person concerned can refuse or withdraw his consent without detriment. The Austrian authority thus concludes that where the data subject has other options, or can choose not to use the service for which consent to advertising is required, that consent is valid, because the data subject is exercising his freedom. Finally, the EDPC has resolved this difference of opinion in May 2020 by publishing "Guidelines 05/2020 on consent under Regulation 2016/679". In this document, the EDPC opts for a restrictive interpretation, stating that: "Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-

performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred". (§26)

In §27 it adds that "*As data protection law is aiming at the protection of fundamental rights, an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service*".

It is true that later the EDPC states in §35 of the same document that Article 7(4) of the GDPR does not establish an absolute prohibition, but it concludes that the cases in which this condition could be established under that article are very limited, in view of the presumption in Recital 43. However, given the level and authority of the EDPC, this interpretation is not the only possible one.

First, because, whereas 43 does not make a general or abstract reasoning, applicable to any case, it defines in the beginning the scenario it takes into consideration: '*in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority*'. This initial description leads to think that the presumption of lack of freedom of the conditioned consent can only be applied in cases where there is an imbalance between the controller and the data subject.

Secondly, because it is whereas 42 develops the interpretation of what is to be understood by valid consent, reasoning with respect to freedom that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".

Therefore, the key to assessing whether consent is free is to check whether the subject has freedom of choice, that is, whether he or she can really decide whether to consent or refuse, or whether, if he or she refuses what is asked of him or her, he or she is faced with the need to endure some detriment.
If the subject must refrain from using the conditional service if he or she does not want to accept the unnecessary treatment, this waiver would, in the opinion of EDPC and the British authority, be detrimental. However, this reasoning leads to the assertion that consent to any contract would lack freedom: no one would pay the price of a good or service freely, because if he did not pay it, he would have to renounce the thing or service he wants to consume.

The condition proposed in Recital 42 can only be understood as disproportionate or unfair prejudice. However, in those cases where the option affects a service that is neither necessary nor essential, the need to waive it if the conditions are not accepted cannot be described as a detriment, but as the lack of sufficient will to pay the price established by the entity in order to be able to access the service.

Thirdly, from a strictly legal point of view, any relationship between persons that is established and governed by the consent of the interested parties is a contract. This is how Maurice Hauriou defined it in the nineteenth century and this postulate is one of the main foundations of the law of contractual relations. According to this postulate, consent to the processing of personal data is also a contractual consent, identical to any contract.

In fact, by means of consent, it disposes not only of goods, but also of fundamental rights and freedoms, when the law allows it, by concluding contracts, for example, for medical services that affect our physical integrity and health, when a doctor is hired to perform a surgical operation

on people, or when one is committed to carry out an activity during a day by signing an employment contract, renouncing to her/his freedom, etc. Similarly, when one agrees that an entity may hold certain personal data for a certain purpose, that consent is contractual and subject to the same validity requirements as other contracts. For this reason, the definition of consent that the GDPR establishes coincides and fits perfectly with the regulation of consent in civil and commercial law.

The consent of the GDPR is identical to the consent of the rest of the contracts and, in any contract, the person who consents always waives some aspect or interest in order to receive a good or right that he considers appropriate. This renunciation, the price of the contract, cannot be considered as an element that annuls the freedom of choice of the interested party.

When article 6.1(a) of the GDPR establishes that the processing of personal data can be based on the consent of the data subject, it simply establishes that the data subject can have his privacy available when he considers it convenient, that is, when an advantage is offered that motivates him to accept the processing of the data.

It is true that Article 7(4) of the GDPR states that where access to a service is conditioned on the data subject's consent to processing of data which is not necessary for that service, precautions must be taken to verify that that condition is not unlawful. This would be the case, as reasoned in Recital 42 of the GDPR, in cases where the service is essential to the data subject and he or she has no real capacity to give it up or, as justified in Recital 43, when there is an imbalance between the entity establishing that condition and the person interested in accessing the service (for example, when the person is an employee of the entity), or in cases where a public administration establishes unnecessary conditions for access to a public service.

However, the GDPR does not set any conditions to the free consent of the data subjects, but, by regulating this consent, it attributes to the data subjects a capacity of disposition over their privacy so that they can act as they wish, and one of these possibilities is, precisely, the cases in which they are offered to perceive a benefit in consideration of their consent.
The development of the Internet has been largely based on the so-called freemium services, which establish some aspect of privacy as the price of the contract. Denying the individual, the ability to dispose of his or her personal data is emptying Article 6.1(a) of the GDPR of its content and interpreting Article 7(4) differently from what it literally states. This article only encourages precautions to be taken in these cases, to guarantee individuals that, when they have their privacy to receive a service, they do not do so without sufficient freedom, but it does not state that these assumptions annul the freedom of the subject, nor does it limit these assumptions to cases that are impossible in practice.

The interpretation of this rule in accordance with recitals 42 and 43 of the GDPR leads to the conclusion that the freemium has no place in cases of imbalance between the subject and the entity or in public services, nor in cases where the service is essential to the subject, but it fits perfectly with the GDPR in the rest of cases.

V. How to address challenges around the situation of self-employed individuals offering services through online platforms

Key words: online platforms; platform work(er); self-employed; bogus self-employed; atypical employment, bias, gender, minority

Conclusion

1. Technological progress has transformed citizen life and employment relations and will continue to do so. However, these changes demand a legislative response. At EU level it would be advisable to pass the necessary laws further to the current research (academic and field studies, statistics, and surveys) to address the specific needs of the self-employed in each field.

2. Freelancers rendering services through online platforms, are left unprotected under the current laws. In particular, their needs are not covered, such as regularized contractual relations (contractual terms and conditions), health and safety protection, collective representatives and, above all, the technological presence of artificial intelligence and algorithms, which play a leading role in the assignment of tasks.

3. The importance and relevance of this study should be pointed out that it ultimately seeks to implement regulations, in the near future, to cover the legal situation of the self-employed and bogus self-employed, accordingly, who are providing their services through online platforms, which demands immediate legal attention.

4. The EU should also take this opportunity to ensure that the gender and minority issues are addressed, to avoid discrimination and ensure equality.

There is a large number of self-employed workers both in Spain and in Europe in general.

5. As of 31 December 2019, there were around 3,300,000[22] self-employed workers[23], according to the Ministry of Employment and Social Economy (pending to confirm the effect of COVID in such number). See the importance of the freelance workers compared to Spain's total workforce which, according to the National Statistics Institute (INE), registered 18,607,200[24] workers in 2Q 2020. Furthermore, numerous small or micro companies in Spain merely act as vehicles to for the self-employed, possibly to take advantage of the company's limited liability.

In Europe, according to Eurostat employment data published in 1/04/2020, "*in 2018, self-employment provided work to around one in seven (14%) employed persons aged 20-64 years across the EU (26 million persons)*"[25] In this sense, the region with the highest rate of self-employment was Greece with around 31% rate while Germany, Norway and Denmark had the lowest rates around 7%.

Lack of EU legislation specifically addressing the status of the self-employed.

6. Until the date of this paper no specific UE legislation has been passed to regulate the situation of the self-employed; however, instead, regulations do in fact exist (in great detail) regarding capital stock companies. Certainly, although other directives regulate similar situations, specific needs are not covered or these laws may be simply obsolete,

[22] http://www.mitramiss.gob.es/ficheros/ministerio/sec_trabajo/autonomos/economia-soc/autonomos/estadistica/2020/1TRIMESTRE/Resumen-de-Resultados-1-trim-2020-.pdf

[23] We shall consider self-employed as those persons registered under the specific Social Security regime for self-employed workers.

[24] https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176918&menu=ultiDatos&idp=1254735976595

[25] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200401-1

as is the case of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce).

7. Of relevance are the definitions of the following terms (amongst others) provided by the European Commission[26] in the "Study to gather evidence on the working conditions of platform workers VT/2018/032 Final Report dated of 13 March 2020": (i) "online platform"; (ii) "platform work(er)"; (iii) "atypical employment/work"[27] as opposed to standard employment[28] and traditional employment[29].

8. Consequently, according to the definition of "online platforms" and "platform work(er)", which are closely interrelated, an online platform is "*An online service that facilitates communication between one or more parties, especially to exchange services for payment*" and platform work(er) is defined as "*All labour provided through, on or mediated by online platforms, in a wide range of sectors, where work can be of various forms, and is provided in exchange for payment*".

9. Once some of these basic terms are defined and further to the foregoing, it should be bared in mind, in relation to this topic, that the definition of "worker" may include persons employed under an employment contract, and those hired under a commercial services agreement, i.e. the self-employed and bogus self-employed, as they are usually known[30].

10. Self-employed workers are analysed in the EU 13 March 2020 report, although as a category of the group "worker". Do their specific needs not require a special treatment, different from that given to the actual employees?

Bogus self-employed

11. The figures available in Spain (or Europe) on bogus self-employees are hard to determine, at least to obtain accurate results. In some cases, a suggestion has been made to cross-refer data held by the Social Security and Tax authorities. However, several studies have evidenced approximately 72,120 bogus self-employees in Spain, at least on 26 February 2020[31] (again, to be adjusted post-COVID).

12. Nevertheless, at least 9,000 people have been subtracted from this figure that represent a grey "TRADE[32]" area (i.e. self-employed personnel who invoice one single client or one which client weighs over 75% in the self-employed total turnover).

[26] Study to gather evidence on the working conditions of platform workers VT/2018/032. Final Report. 13 March 2020.
[27] Work that differs in one or mor e issues from standard work.
[28] Employment relations between a natural person (employee) and a legal or natural person (employer), for an indefinite period of time (of undetermined duration) and full time.
[29] Employment relations between a natural person (employee) and a legal or natural person (employer), for an indefinite period of time (of undetermined duration) and full time, particularly before a platform economy.
[30] Ditto.
[31] https://cincodias.elpais.com/cincodias/2020/02/24/economia/1582563977_484963.html
[32] Article 11 of the professional regime for the self-employed.

13. Online platforms gained prominence and became popular following the global economic crisis in 2008 and subsequent years, given the huge democratization they entailed as well as access to new jobs, particularly at a time of high demand. However, not only were new job positions created as the main source of income; for some, this became a way of making extra money. Such additional source of income is frequently non-taxed, non-insured, and irregular.

The self-employed are in a weaker position (online and offline), yet platforms provide chances

14. When the time comes to negotiate a deal, the self-employed are naturally in a weaker position, both with respect to the online platforms and their clients, as well as offline. Some of the issues that weaken their negotiating power are lack of clarity in the pricing situation in the platform; uncertainty in the assignment of tasks, working schedule and benefits; lack of information on professional careers at a specific company, etc.

15. At the same time, however, platforms may provide self-employed larger visibility vis-à-vis the offline business. A creative yoga instructor can attract more attention in YouTube that in their local studio. A small honey producer can reach a larger market selling through Amazon than anywhere else. A language teacher can promote their successful results with happy clients through Instagram.

16. The challenges being faced by self-employees providing their services through online platforms are particularly important given that, from the very start, they have triggered a drastic change in "standard" employer-employee relations, or even freelance-client relations. Platforms have created a new triangular relationship, i.e. there are three parties: (i) the employee or service provider; (ii) the intermediary or online platform; and (iii) the client or recipient of the service.

17. Finally, this point refers to dispute resolution channels. Although it is possible for a clause to be included in standard contracts of some companies, it is also possible that it may not cover many situations, such as "occupational accidents" or accountability towards the client as a result of the service rendered.

Gender and minority aspects

18. Gender and minority issues should also be addressed. Of the total 3.3 million self-employed in Spain in December 2019, 64.4% were male, and the remaining 35.6% were female. As indicated by the Ministry of Employment and Social Economy, these percentage figures change by geographical area or sector of activity. However, of interest is the fact that the services sector has registered the highest percentage of women- 42.3%-, with this sector representing 73.2% of total activity. Consequently, women are highly represented in this field. Since services are overrepresented in platforms, this point should be considered with a view to achieving gender equality.

19. As regards work management, assignment and organisation, the European Commission has explained in the work cited above (see point 7) (published on 12 March 2020) that a large part of work assignments is carried out through algorithms using artificial intelligence. Online platforms are algorithm-based (to include artificial intelligence and machine learning). Every effort should be made to prevent bias and discrimination; thus, resulting in equal opportunities that level the playing field.

Some areas of interest to self-employees in their relationship with platforms

20. The sector is undergoing rapid change ahead of the law, where regulations are not being enacted at the same speed. Whether this is a problem or benefit is open for discussion. The current survey seems highly relevant in order to gather and bring together relevant data and information, as well as any disputes that may have arisen, consequently handling any issues or circumstances as objectively and accurately as possible, implementing regulations that conform to reality whilst always upholding legal principles.

21. Some relevant challenges to be addressed in the new legislation: under-regulation; ambiguity in work management and assignment (algorithm); lack of transparency when providing information on recruitment terms and conditions (such as working hours, rights, etc.); collective rights (representation); and dispute resolution channels.

22. This system generates unease about how work is assigned and organised, as it seems to lack transparency, i.e. the gathering, analysis and outcome of information in most processes may be biased, from the start, in spite of using accurately designed algorithms. This is because if the databases gathering information contain data errors (which could discriminate on the grounds of gender, race, religion and sex, for example) that are left unfiltered, obviously the outcome will still be inaccurate producing biased results, i.e. a "snowball effect". The problem here is that once biased results are published, tasks will be inaccurately assigned, through a non-transparent and discriminatory assignment, or which is not equivalent.

23. As for the clear wording of a contract's terms and conditions, which are very often lengthy, not explanatory or reader-friendly, or unclear, or which include invalid clauses (e.g. clauses stating that the relationship is commercial, not employment-related, when there is a clear employment relationship), a self-employed worker, lacking legal counsel, may only be able to "take it or leave it". In addition to the foregoing, companies use standard contracts which, obviously, are non-negotiable for both the client and worker. As a result, the contractual equilibrium between the parties is broken, at least in negotiation terms (or due to a lack of negotiation).

24. It is certainly true that workers' obligations and rights (in particular) are not upheld in these contracts. Very often, obligations and rights are misleadingly drafted or simply, to avoid an employment relationship altogether, a worker's rights are overlooked (leaving the salary aside) and no extra benefits are granted. Clearly, this is a very serious situation that needs to be given priority. An example is working schedules, limited workdays, employment benefits, days' rest, holidays or vacation, careers within the company, and other perks such as private health insurance.

25. Any possible employee representation is fairly limited. Logically, the self-employed (or bogus self-employed) are less likely to belong to trade unions[33] or to their company's trade union, if any. Although there is a possibility of joining sector trade unions, this does not guarantee that they will be represented if the situation so requires.

[33] This affirmation will depend on special employment laws in each European Union Member State.

ADDENDUM
Statistics of interest

26. Below are statistics gathered by the European Commission (available in the 2020 study cited), showing results by country on the percentage of people who have used or are using online platforms. The information is based on two sources: (i) the number of hours spent on online platforms (less than 10 hours, between 10-19 hours or more than 20 hours); and (ii) how much of their income is generated this way (less than 25%, between 25-50%, more than 50%).

Table 3: Platform worker prevalence estimate as percentage of population 16-74 years

Country	Sporadic (%)	Marginal (%)	Secondary (%)	Main (%)
Netherlands	2.8	3.4	5.1	2.7
Spain	4.1	4.7	6.7	2.6
Ireland	2.6	3.2	5.2	2.0
UK	2.0	3.5	5.7	1.6
Portugal	4.2	3.7	3.9	1.5
Germany	3.2	3.4	4.2	1.5
Romania	2.2	3.4	3.5	1.4
Hungary	1.7	1.4	2.2	1.4
Lithuania	3.8	3.6	2.7	1.2
Croatia	3.3	2.8	3.5	1.1
Sweden	3.0	2.6	3.7	0.9
Italy	1.5	2.5	3.9	0.9
France	1.5	2.6	2.8	0.9
Slovakia	1.2	2.2	1.8	0.9
Czechia	1.5	1.6	1.9	0.9
Finland	3.1	1.4	1.8	0.6
Total	**2.4**	**3.1**	**4.1**	**1.4**

Source: COLLEEM II survey data (Brancati et al., 2019)
Note: the total is for the available 16 countries. While no comparable estimates are available for the remaining Member States, Norway and Iceland, the data on available countries is assumed to be fairly representative for the EU, as a variety of regions, industrial relations systems, and government traditions are covered.

VI. What governance system would be best for reinforcing a single market digital services?

The European Single Market requires a modern legal framework to ensure the safety fusers online, and to allow innovative digital businesses to grow, while respecting the basic principles of the e-commerce directive, but what is the Single Market Digital Services?

It is a European Policy that covers digital marketing, e-commerce and telecommunications, that grows around three pillars:
- Access to online products and services.
- Conditions for digital network and services to grow and thrive.
- Growth of the European digital services.

Having said this, it is important to, in the first place, establish a concept of governance in the European Union regarding the Single Market Digital Services. A governance system can be

defined as the way in which member states adopt decisions that affect them, and how are those processes designed and implemented (or modified). If the Union is a 28-member state-based institution, the Digital Single Market aims to tear down regulatory walls and move 28 national markets into one. In this scenario, transparency reporting from operators should be considered as one of the main regulatory tools.

Nevertheless, governance in the European Union has certain peculiarities when referring to a self-organizing, inter-organizational networks that need to find a way of complementing each other, in order to authoritatively allocate resources and exercise control and coordination, in a geopolitical space. Thus, governance will necessarily need to include the element of multi-level governance, this is, "the dispersion of authority to multitask, territorially mutually exclusive jurisdictions in a relatively stable system".

Before analyzing the sort of governance system that would best serve the reinforcement of the Single Digital Market, two different points need to be made. The challenge here is how to design and enforce a legal framework that can cover an economic industry that is building upon the cyber space. So, there are two critical points:

a) The structure and process of the design of a governance system that can effectively enforce a legal framework.
b) The difficulties that arise regarding regulation enforcement on a pure digital ecosystem.

A. The structure and process of the design of a governance system that can effectively enforce a legal framework

Attending to legal texts, if one investigates the Maastricht Treaty, it shows that conceptually, "collectively perceived problems are dealt with by means of targeted public policy with the aim of collectively binding decisions". This means, or it implies, a process in which to collectively address common problem, Nation States must voluntarily transfer sovereignty and the ability of adopting political decisions. It is the only way of having a real and effective super national community that can achieve the original goals, and that has action capacity of its own.

This is a dynamic and continuous process of integration of the different member states. Integration seems to be crucial specially in those areas or challenges that do not distinguish boundaries. This is, transnational issues, and of course Digital Services are one of these. It is therefore important to propose alternatives to the European governance systems that set off from its own identity and culture. The truth is that now coordination between multiple players that believe that joint problem solving and that have special interest in building strong legislative and regulatory networks is needed.

Now, perspective matters. Especially when sovereignty comes into place. And it is necessary to understand how these integrations processes are not excluding or eliminating member state power to several other actors. This leads to the need of making a new approach to the idea of "Governance beyond the State", leaving behind the concept of State system and introducing new formulas, beyond territorial boundaries.

A good empirical example is the European Court system. With its current limitations (due to some non-harmonized frameworks), the European Court ruling are not only accepted and respected in every single member state, but they can also be directly invoked, and form jurisprudence in the whole of the Community territory. In this sense, European Courts do

contribute to building and conserving a single judicial criterion over law cases, which also supports and thrives stability in the European territory.

Another one, are the Working Groups that inspire certain policies and initiatives, especially regarding new technological issues. This hybrid formula, seen at the European Blockchain Forum and Observatory, where specialists from every member state gathered and worked on drafting reports that could then serve regulatory bodies. It is an excellent example of how countries in the European Union collaborate for a common purpose, in an effective way, allocating resources for a communitarian interest.

We believe that any cooperation between regulators should be structured around clear purposes, and a thorough consideration of second and third order consequences should inform the terms of any cooperation and the process safeguards.

B. Difficulties derived from regulating cyber space activity.

Once discussed about "how" can the governance be structured, the "how" common issues inside this governed community can be regulated effectively, specifically in the digital world, needs to be addressed. Citing Lessig, "*In real space, we recognize how laws regulate – through constitutions, statutes and other legal codes. But in cyberspace, we must understand how a different "code" regulates. Cyber space does need governance too, but differently to how real-world works. Enforcement in the digital space can be rather tricky. The first thing to bear in mind is that digital/cyberspace regulation must be designed from the thorough understanding of the architecture (software) that people like Lawrence Lessig envisioned during the 90s: "cyberspace is different because of the relative anonymity it permits*". This is just one of the peculiarities of cyberspace that regulators must understand when designing the governance for these networks.

Overall, the capacity of Governments to regulate behaviors of citizens while on the Internet is referred to as regulability. Regulability that gets even more complex if there are competing sovereigns, thus, it is crucial to address the Single Market and Digital Services Act from a European perspective, like it has been done for instance, with Blockchain tech. One sovereign institution that technically understands the complexities of the subject it is trying to regulate and that has external advising from specialists in the field, who are the ones capable of envisioning and foreseeing potential legal issues.

It must be noted that for the effectiveness of a Digital Single Market, there must be place for enforceability, so the EU should be able to enforce agreements, rules, rulings…etc inside online environments. An alternative would be a system of penalties for those platforms that will not implement the content of rulings, or aren't compliant, which already exists and has been proven inefficient for certain types of virtual communities (such as decentralized finance). This implies the need to have the actual capability of influencing and actually having the power of programmatically doing so, by for instance, having some sort of administrator key or similar. Then, the EU should have a body of coders, or IT profiles that can help this enforcement.

In conclusion, the governance system regarding digital regulation and market building needs to, beforehand, understand the architecture and functioning of the businesses and economic flows of the space. Given the gradually increasing technicalities of software development, it may be unavoidable and very important to include inside this system technical profiles and hybrid ones, this is, regulatory experts that have sufficient expertise in the field.

A regulatory and enforcing body constituted by technical experts, and legal advisors, that understand the online environment, its community, the complexities around its regulation and that are supported by the IT profiles that can physically influence those system in order to make enforcement as a second resource, if compliance is not met. All of the aforementioned, would need to be developed under strict rules of transparency.

Members of the working group:

The conclusions drawn are the result of the discussions held by all the members of the group.

We stand in solidarity with the proposal as a whole. The proposal is signed in a personal capacity and does not represent the official position of the institutions to which we belong.

1. **Ana Abade,** Public policy analyst, Spain and Portugal, Google
2. **Ane Alonso,** Lawyer, Cuatrecasas
3. **María Álvarez,** Head of the Competition Department, Google
4. **Segismundo Álvarez,** Notary
5. **Javier Aparicio,** Partner, Finreg360
6. **Álvaro Bourkaib Fernández de Córdoba,** Partner, Cuatrecasas
7. **Cristina Carrascosa,** Of counsel, Pinsent Masons
8. **Eusebio Felguera Garrido,** Public Policy & Internet, Telefonica S.A.
9. **Cristina Fernández Caldueño,** Managing partner, Castroalonso
10. **Luis Ignacio Gil Palacios,** Lawyer, Mavens
11. **Carmen Hermida,** Managing Director, Fide
12. **Cristina Jiménez Savurido,** President, Fide
13. **Teresa Martín Castro,** Managing Partner of Mavens Abogados and Chairperson of Tech Spain Advocates
14. **Cristina Martínez Laburta,** Lawyer. Chief Legal Officer at Alastria Blockchain Ecosystem
15. **Andrea Matador,** Lawyer, Castroalonso
16. **Cristina Mesa,** Partner, Industrial and Intellectual Property Departament, Garrigues
17. **Alejandro Padín,** Partner, Garrigues
18. **Teresa Pereyra,** Head of Data Protection and Information Technology, Roca Junyent
19. **Yolanda Ríos López,** Magistrate Commercial Court number 1 of Barcelona
20. **Jesús Sieira Gil,** Land and Mercantile Registrar. Public Law Corporation of Land and Mercantile Registrars of Spain
21. **Sonia Vázquez Cobreros,** Lawyer, Castroalonso