Tuesday 20 October 2020

P9_TA(2020)0274

Digital Services Act and fundamental rights issues posed

European Parliament resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020/2022(INI))

(2021/C 404/03)

The European Parliament,

— having regard to the Treaty on European Union (TEU), in particular Article 2 thereof,

— having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Article 16 and Article 114 thereof,

— having regard to the Charter of Fundamental Rights of the European Union, in particular Article 6, Article 7, Article 8, Article 11, Article 13, Article 21, Article 22, Article 23, Article 24, Article 26, Article 38, and Article 47 thereof,

— having regard to 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') ([1]),

— having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('General Data Protection Regulation', (GDPR)) ([2]),

— having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications') ([3]),

— having regard to Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities ([4]),

— having regard to Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC ([5]) ('Copyright Directive'),

— having regard to the Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online ([6]),

— having regard to the Europol Internet Organised Crime Threat Assessment (IOCTA) of 18 September 2018,

— having regard to the relevant case law of the Court of Justice of the European Union,

— having regard to Rule 54 of its Rules of Procedure,

— having regard to the opinions of the Committee on the Internal Market and Consumer Protection and the Committee on Culture and Education,

— having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A9-0172/2020),

([1]) OJ L 178, 17.7.2000, p. 1.
([2]) OJ L 119, 4.5.2016, p. 1.
([3]) OJ L 201, 31.7.2002, p. 37.
([4]) OJ L 303, 28.11.2018, p. 69.
([5]) OJ L 130, 17.5.2019, p. 92.
([6]) OJ L 63, 6.3.2018, p. 50.

Tuesday 20 October 2020

A. whereas fundamental rights, such as the protection of privacy and personal data, the principle of non-discrimination, as well as freedom of expression and information, need to be ingrained at the core of a successful and durable EU policy on digital services; whereas these rights need to be seen both in the letter of the law, as well as in the spirit of their implementation;

B. whereas the types of digital services and the roles of digital service providers have drastically changed since the adoption of the e-Commerce Directive 20 years ago;

C. whereas the trust of users can only be gained by digital services that respect users' fundamental rights, which would not only uptake of services, but would also offer a competitive advantage and stable business model for companies;

D. whereas the data protection rules applicable to all providers offering digital services in the EU's territory were recently updated and harmonised across the EU with the General Data Protection Regulation; whereas privacy rules for electronic communications, which are a subset of digital services, are covered by the Directive on privacy and electronic communications and are currently under revision;

E. whereas the amount of all types of user-generated content shared and services provided via online platforms, including cloud services, has increased exponentially and at an unprecedented pace facilitated by advanced technologies; whereas this includes illegal content such as images depicting child sexual abuse material (CSAM) online and content that is legal but that may be harmful for society and democracy, such as disinformation on COVID-19 remedies;

F. whereas online hate speech and disinformation have become increasingly widespread in recent years as individuals and disruptive actors make use of online platforms to increase polarisation, which, in turn, is used for political purposes; whereas women, persons of colour, persons belonging to or perceived as belonging to ethnic or linguistic minorities and LGBTIQ persons are often targeted by discriminatory hate speech, bullying, threats and scapegoating online;

G. whereas this trend has been aided by online platforms whose business model is based on the collection and analysis of user data with a view to generating more traffic and 'clicks', and, in turn, more profiling data and thus more profit; whereas this leads to the amplification of sensationalist content; whereas hate speech and disinformation harm the public interest by undermining respectful and honest public discourse and pose threats to public security since they can incite real-world violence; whereas combating such content is key in order to ensure respect for fundamental rights and to defend the rule of law and democracy in the EU;

H. whereas social media and other content distribution platforms utilise profiling techniques to target and distribute their content as well as advertisements; whereas data collected from the digital traces of individuals can be mined in ways that allow for a highly accurate inference of very intimate personal information, especially when such data is merged with other data sets; whereas the Cambridge Analytica and Facebook scandals showed the risks associated with opaque data processing operations of online platforms by revealing that certain voters had been micro-targeted with political advertising and, at times, even with targeted disinformation;

I. whereas the automated algorithms that decide how to handle, prioritise, distribute and delete third-party content on online platforms, including during political and electoral campaigns, often reproduce existing discriminatory patterns in society, thereby leading to a high risk of discrimination for persons already affected; whereas the widespread use of algorithms for content removal or blocking also raises concerns over the rule of law and questions related to legality, legitimacy and proportionality;

J. whereas a small number of mostly non-European service providers have significant market power and exert influence on the rights and freedoms of individuals, our societies and democracies by controlling how information, services and products are presented, which therefore have a significant impact on the functioning of the Member States and on their

citizens; whereas the decisions of these platforms can have far-reaching consequences for the freedom of expression and information and for media freedom and pluralism;;

K. whereas the policy approach to tackle illegal content online in the EU has mainly focused on voluntary cooperation and court-order-mandated takedowns thus far, but a growing number of Member States are adopting further national legislation addressing illegal content in a non-harmonised manner; whereas provisions to address certain types of illegal content were included in recent sectoral legislation at EU level;

L. whereas a pure self-regulatory approach of platforms does not provide adequate transparency, accountability and oversight; whereas such an approach neither provides proper information to public authorities, civil society and users on how platforms address illegal content and activities and content that violates their terms and conditions, nor on how they curate content in general;

M. whereas such an approach may not guarantee compliance with fundamental rights and creates a situation where judicial responsibilities are partially handed over to private parties, which poses the risk of interference with the right to freedom of expression;

N. whereas regulatory oversight and supervision is sector-specific in the EU; whereas further and more comprehensive coordination between the different oversight bodies across the EU would be beneficial;

O. whereas the lack of robust, comparable public data on the prevalence of illegal and harmful content online, on notices and the court-mandated and self-regulatory removal thereof, and on the follow-up by competent authorities creates a deficit of transparency and accountability, both in the private and public sector; whereas there is a lack of information regarding the algorithms used by platforms and websites and the way platforms address the erroneous removal of content;

P. whereas child sexual exploitation online is one of the forms of illegal content that is facilitated by technological developments; whereas the vast amount of CSAM circulating online poses serious challenges for detection, investigation and, most of all, victim identification efforts; whereas, according to Europol, reports of online sharing of CSAM that were made to US-based NCMEC increased by 106 % within the last year;

Q. whereas according to the Court of Justice of the European Union (CJEU) jurisprudence, content should be removed following a court order from a Member State; whereas host providers may have recourse to automated search tools and technologies to detect and remove content that is equivalent to content previously declared unlawful, but should not be obliged to monitor generally the information that it stores, or to actively seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31/EC;

R. whereas a trusted electronic identification is elementary in order to ensure secure access to digital services and to carry out electronic transactions in a safer way; whereas currently only 15 Member States have notified the Commission of their electronic identity scheme for cross-border recognition in the framework of the Regulation (EU) No 910/2014 ([7]) ('eIDAS Regulation');

S. whereas the internet and internet platforms are still a key location for terrorist groups' activities, and they are used as a tool for sowing propaganda, recruitment and promotion of their activities;

([7]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73).

Tuesday 20 October 2020

1. Believes in the clear societal and economic benefits of a functioning digital single market for the EU and its Member States; welcomes these benefits, in particular improved access to information and the strengthening of the freedom of expression; stresses the important obligation to ensure a fair digital ecosystem in which fundamental rights as enshrined in the Treaties and the Charter of Fundamental Rights of the European Union, especially freedom of expression and information, non-discrimination, media freedom and pluralism, privacy and data protection, are respected and user-safety is ensured online; emphasises the fact that legislative and other regulatory interventions in the digital single market aiming to ensure compliance with this obligation should be strictly limited to what is necessary; recalls that content removal mechanisms used outside the guarantees of a due process contravene Article 10 of the European Convention on Human Rights;

2. Urges the Commission to adopt a tailored regulatory approach in order to address the differences that still persist between online and offline worlds and the challenges raised by the diversity of actors and services offered online; considers, in this regard, it essential to apply different regulatory approaches to illegal and legal content; stresses that illegal content online and cyber-enabled crimes should be tackled with the same rigour and on the basis of the same legal principles as illegal content and criminal behaviour offline, and with the same guarantees for citizens; recalls that the e-Commerce Directive is the legal framework for online services in the internal market that regulates content management;

3. Deems it necessary that illegal content is removed swiftly and consistently in order to address crimes and fundamental rights violations; considers that voluntary codes of conduct only partially address the issue;

4. Calls on digital service providers to take content offline in a diligent, proportionate and non-discriminatory manner, and with due regard in all circumstances to the fundamental rights of the users and to take into account the fundamental importance of the freedom of expression and information in an open and democratic society with a view to avoiding the removal of content, which is not illegal; requests that digital service providers, which on their own initiative want to restrict certain legal content of their users, explore the possibility of labelling that content, rather than it taking offline, thus giving users the chance to choose to access that content on their own responsibility;

5. Takes the position that any legally mandated content take-down measures in the Digital Services Act should concern illegal content only, as defined in EU and national law, and that the legislation should not include any undefined concepts and terms as this would create legal uncertainty for online platforms and put fundamental rights and freedom of speech at risk;

6. Acknowledges, however, that the current digital ecosystem also encourages problematic behaviour, such as micro-targeting based on characteristics exposing physical or psychological vulnerabilities, the spreading of hate speech, racist content and disinformation, emerging issues such as the organised abuse of multiple platforms, and the creation of accounts or manipulation of online content by algorithms; notes with concern that some business models are based on showing sensational and polarising content to users in order to increase their screen time and thereby the profits of the online platforms; underlines the negative effects of such business models on the fundamental rights of individuals and for society as a whole; calls for transparency on the monetisation policies of online platforms;

7. Emphasises, therefore, that the spreading of such harmful content should be contained; firmly believes that media literacy skills, user control over content proposed to them and public access to high-quality content and education are crucial in this regard; welcomes, therefore, the Commission initiative to create a European Digital Media Observatory to support independent fact-checking services, increase public knowledge on online disinformation and support public authorities in charge of monitoring digital media;

8. calls on the Commission and the Member States to support independent and public service media and educational initiatives on media literacy and targeted awareness-raising campaigns within civil society; points out that special attention should be paid to harmful content in the context of minors using the internet, especially as regards to their exposure to cyberbullying, sexual harassment, pornography, violence and self-harm;

9. Notes that since the online activities of an individual allow for deep insights into their personality and make it possible to manipulate them, the general and indiscriminate collection of personal data concerning every use of a digital service interferes disproportionately with the right to privacy and the protection of personal data; highlights, in particular, the potential negative impact of micro-targeted and behavioural advertisements and of assessments of individuals, especially minors and vulnerable groups, by interfering in the private life of individuals, posing questions as to the collection and use of the data used to personalise advertising, offer products or services or set prices; confirms that the right of users not to be subject to pervasive tracking when using digital services has been included in GDPR and should be properly enforced across the EU; notes that the Commission has proposed to make targeted content curation subject to an opt-in decision in its proposal for a new regulation concerning the respect for private life and the protection of personal data in electronic communications (2017/0003(COD));

10. Deems that misleading or obscure political advertising is a special class of online threat because it influences the core mechanisms that enable the functioning of our democratic society, especially when such content is sponsored by third-parties, including foreign actors; underlines that when profiling is deployed at scale for political micro-targeting to manipulate voting behaviour, it can seriously undermine the foundations of democracy; calls, therefore, on digital service providers to take the necessary measures to identify and label content uploaded by social bots and expects the Commission to provide guidelines on the use of such persuasive digital technologies in electoral campaigns and political advertising policy; calls, in this regard, for the establishment of strict transparency requirements for the display of paid political advertisement;

11. Deems it necessary that illegal content is removed consistently and without undue delay in order to address infringements, especially those relating to children and terrorist content, and fundamental rights violations with the necessary safeguards in place, such as the transparency of the process, the right to appeal and access to effective judicial redress; considers that voluntary codes of conduct and standard contractual terms of service lack adequate enforcement and have proven to only partially address the issue; stresses that the ultimate responsibility for enforcing the law, deciding on the legality of online activities and ordering hosting service providers to remove or disable access to illegal content rests with independent competent authorities;

12. Acknowledges the fact that, while the illegal nature of certain types of content can be easily established, the decision is more difficult for other types of content as it requires contextualisation; warns that current automated tools are not capable of critical analysis and of adequately grasping the importance of context for specific pieces of content, which could lead to unnecessary takedowns and harm the freedom of expression and the access to diverse information, including on political views, thus resulting in censorship; highlights that human review of automated reports by service providers or their contractors does fully not solve this problem, especially if it is outsourced to private staff that lack sufficient independence, qualification and accountability;

13. Notes with concern that illegal content online can easily and quickly be multiplied and its negative impact therefore amplified within a very short period of time; nevertheless believes that the Digital Services Act should not contain any obligation for hosting service providers or other technical intermediaries to use automated tools in content moderation;

14. Recalls that illegal content online should not only be removed by online platforms, but should also be followed up by law enforcement and the judiciary where criminal acts are concerned; calls on the Commission to consider obliging online platforms to report serious crime to the competent authority when they have received knowledge of such a crime; finds, in this regard, that a key issue in some Member States is not the fact that they only have unresolved cases but also unopened ones; calls for barriers to filing complaints with the competent authorities to be removed; is convinced that, given the borderless nature of the internet and the fast dissemination of illegal content online, cooperation between service providers and national competent authorities, as well as cross-border cooperation between national competent authorities, should be improved and based on the principles of necessity and proportionality; stresses, in this regard, the need to respect the legal order of the EU and the established principles of cross-border cooperation and mutual trust; calls on Member

States to equip their law enforcement and judicial authorities with the necessary expertise, resources and tools to allow them to effectively and efficiently deal with the increasing number of cases involving illegal content online and with dispute resolution concerning the taking offline of content, and to improve access to justice in the area of digital services;

15. Underlines that a specific piece of content may be deemed illegal in one Member State but is covered by the right to freedom of expression in another; highlights that in order to protect freedom of speech, to avoid conflicts of laws, to avert unjustified and ineffective geo-blocking and to aim for a harmonised digital single market, hosting service providers should not be required to remove or disable access to information that is legal in the Member State that they are established in, or where their designated legal representative resides or is established; recalls that national authorities can only enforce removal orders by independent competent authorities addressed to service providers established in their territory; considers it necessary to strengthen the mechanisms of cooperation between the Member States with the support of the Commission and relevant Union agencies; calls for a structured dialogue between Member States in order to determine the risk of specific types of content and to identify potential differences in assessment of such risks between Member States;

16. Underlines that illegal content should be removed where it is hosted, and that mere conduit intermediaries should not be required to block access to content;

17. Strongly believes that the current EU legal framework governing digital services should be updated with a view to addressing the challenges posed by the fragmentation between the Member States and new technologies, such as the prevalence of profiling and algorithmic decision-making that permeates all areas of life, as well as ensuring legal clarity and respect for fundamental rights, in particular the freedom of expression and the right to privacy in a futureproof manner given the rapid development of technology;

18. Welcomes the Commission's commitment to introducing a harmonised approach addressing obligations for digital service providers, including online intermediaries, in order to avoid fragmentation of the internal market and inconsistent enforcement of regulations; calls on the Commission to propose the most efficient and effective solutions for the internal market as a whole, while avoiding new unnecessary administrative burdens and keeping the digital single market open, fair, safe and competitive for all its participants; stresses that the liability regime for digital service providers must be proportionate, must not disadvantage small and medium-sized providers and must not unreasonably limit innovation and access to information;

19. Considers that the reform should build on the solid foundation of and full compliance with existing EU law, especially the General Data Protection Regulation and the Directive on privacy and electronic communications, which is currently under revision, and respect the primacy of other sector-specific instruments such as the Audiovisual Media Services Directive; underlines that the modernisation of the e-commerce rules can affect fundamental rights; therefore urges the Commission to be extremely vigilant in its approach and to also integrate international human rights standards into its revision;

20. Highlights that the practical capacity of individual users to understand and navigate the complexity of the data ecosystems is extremely limited, as is their ability to identify whether the information they receive and services they use are made available to them on the same terms as to other users; calls, therefore, on the Commission to place transparency and non-discrimination at the heart of the Digital Services Act;

21. Insists that the Digital Services Act must aim to ensure a high level of transparency as regards the functioning of online services and a digital environment free of discrimination; stresses that, besides the existing strong regulatory framework that protects privacy and personal data, an obligation for online platforms is needed to ensure the legitimate use of algorithms; calls, therefore, on the Commission to develop a regime based on the e-Commerce Directive that clearly frames the responsibility of service providers to address the risks faced by their users and to protect their rights and to provide for an obligation of transparency and explainability of algorithms, penalties to enforce such obligations, the possibility of human intervention and other measures such as annual independent audits and specific stress tests to assist and enforce compliance;

22. Stresses that some digital service providers have to be able to identify users unambiguously in an equivalent manner to offline services; notes an unnecessary collection of personal data, such as mobile phone numbers, by online platforms at the point of registration for a service, often caused by the use of single sign-in possibilities; underlines that the GDPR clearly describes the data minimisation principle, thereby limiting the collected data to only that strictly necessary for the purpose; recommends that online platforms that support a single sign-in service with a dominant market share should be required to also support at least one open identity system based on a non-proprietary, decentralised and interoperable framework;

23. Underlines that where a certain type of official identification is needed offline, an equivalent secure online electronic identification system needs to be created; believes that online identification can be improved by enforcing eIDAS Regulation'scross-border interoperability of electronic identifications across the European Union; asks the Commission to explore the creation of a single European sign-in system as an alternative to private single sign-in systems and to introduce an obligation for digital services to always also offer a manual sign-in option, set by default; underlines that this service should be developed so that the collection of identifiable sign-in data by the sign-in service provider is technically impossible and data gathered is kept to an absolute minimum; recommends, therefore, that the Commission also explore the creation of a verification system for users of digital services, in order to ensure the protection of personal data and age verification, especially for minors, which should not be used commercially or to track the users cross-site; stresses that these sign-in and verification systems should apply only to digital services that require personal identification, authentication or age verification; recalls that the Member States and Union institutions have to guarantee that electronic identifications are secure, transparent, process only the data necessary for the identification of the user and are used for a legitimate purpose only and are not used commercially, and are not used to restrain general access to the internet or to track the users cross-site;

24. Deems it indispensable to have the full harmonisation and clarification of rules on liability at EU level to guarantee the respect of fundamental rights and the freedoms of users across the EU; believes that such rules should maintain liability exemptions for intermediaries that do not have actual knowledge of the illegal activity or information on their platforms; expresses its concern that recent national laws to tackle hate speech and disinformation lead to an increasing fragmentation of rules and to a lower level of fundamental rights protection in the EU;

25. Calls, to this end, for legislative proposals that keep the digital single market open and competitive by providing harmonised requirements for digital service providers to apply effective, coherent, transparent and fair procedures and procedural safeguards to address illegal content in line with national and European law, including via a harmonised notice-and-action procedure;

26. Believes, in this regard, that it is crucial for online platforms to be provided with clear rules, requirements and safeguards with regard to liability for third-party content; proposes that a common regulatory framework be put in place in order to efficiently identify and remove illegal content;

27. Highlights that rules on notice-and-action mechanisms should be complemented by requirements for platforms to take specific measures that are proportionate to their scale of reach as well as their technical and operational capacities in order to effectively address the appearance of illegal content on their services; recognises, therefore, where technologically feasible, on the basis of sufficiently substantiated orders by independent competent public authorities, and taking full account of the specific context of the content, that digital service providers may be required to execute periodic searches for distinct pieces of content that a court had already declared unlawful, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message whose content remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, which, in line with the judgment of the Court of Justice of 3 October 2019 in case C-18/18 ([8]), are identical or equivalent to the extent that would not require the host provider to carry out an independent assessment of that content;

([8]) Judgment of the Court of Justice of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18, EU:C:2019:821

28. Maintains that the choice of the concrete measures should be left to the platforms; supports a balanced approach based on a dialogue with stakeholders and an assessment of the risks incurred by the platforms, as well as a clear chain of responsibility to avoid unnecessary regulatory burdens for the platforms and unnecessary and disproportionate restrictions on fundamental rights, in particular the freedom of expression, access to information, including on political ideas, and the right to privacy; stresses that certain obligations can be further specified by sectoral legislation; emphasises that any measure put in place to this end cannot constitute, either de jure or de facto, a general monitoring requirement;

29. Stresses the need for appropriate safeguards and due process obligations, including a requirement for human oversight and verification, in addition to counter notice procedures, to allow content owners and uploaders to defend their rights adequately and in a timely manner, and to ensure that removal or blocking decisions are legal, accurate, well-founded, protect users and respect fundamental rights; highlights that persons who systematically and repeatedly submit wrongful or abusive notices should be sanctioned; recalls that besides counter-notice procedures and out-of-court dispute settlements by platforms in accordance with the internal complaints system, the possibility of effective judicial redress should remain available to satisfy the right to effective remedy;

30. Supports the preservation of the current framework on the limited liability for content and the country of origin principle, but considers improved coordination for removal requests between national competent authorities to be essential; underlines that illegal content should be removed where it is hosted; emphasises that such requests should be subject to legal safeguards in order to prevent abuse and ensure full respect of fundamental rights; highlights that removal requests from competent authorities should be specific and clearly state the legal basis for removal; stresses that an effective oversight and enforcement mechanism, including proportionate sanctions taking into account their technical and operational capacities, should apply to those service providers that fail to comply with lawful orders;

31. Recalls that digital service providers must not be legally required to retain personal data of their users or subscribers for law enforcement purposes, unless a targeted retention is ordered by an independent competent authority in full respect of Union law and CJEU jurisprudence; further recalls that such retention of data should be limited to what is strictly necessary with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted;

32. Believes that in order to protect fundamental rights, the Digital Services Act should introduce rules aiming to ensure that the terms of service of digital service providers are clear, transparent, fair and made available in an easy and accessible manner to users; deplores the fact that the terms of service of some content platforms force law enforcement officers to use personal accounts to investigate certain complaints, which poses a threat both to these investigations and to personal safety, calls for more efficient coordination between Member States regarding the follow up of law enforcement on flagged illegal content; recalls that take-down-orders from independent competent authorities have to always be based on law, not on the terms of service of the service providers;

33. Calls on the Commission to ensure that users have access to diverse and quality content online as a means towards ensuring that citizens are adequately informed; expects the Digital Services Act to ensure that quality media content is easy to access and easy to find on third-party platforms and that removals of content are in line with human rights standards and limited to content that is manifestly illegal or has been found illegal by an independent competent authority; stresses that legal content should not be subject to any legal removal or blocking obligations;

34. Supports greater dialogue between the Member States, competent authorities and relevant stakeholders with the aim of developing, evaluating and improving soft law approaches, such as the EU Code of Practice on Disinformation, in order to further address categories of legal content, including disinformation; expects the Commission to issue guidelines including increased transparency rules on content moderation and advertising policy in a specific instrument accompanying the Digital Services Act to ensure that the removal and the blocking of legal content on the basis of

terms and conditions are limited to the absolute minimum; calls, further, on the Commission to establish a framework that prohibits platforms from exercising a second layer of control over content that is provided under a media service provider's responsibility and that is subject to specific standards and oversight;

35. Emphasises, moreover, that users should be given more choice and control with regard to the content that they see, including more options on the way content is ranked to them and the possibility to opt-out from any content curation; strongly believes that the design and performance of recommendation systems should be user-friendly and subject to full transparency;

36. Deems that accountability, both in the private and public sector, and evidence-based policy making require robust data on the incidence and the tackling of illegal activity and the removal of illegal content online, as well as robust data on the content curation algorithms of online platforms;

37. Calls, in this regard, for an annual, comprehensive and consistent public reporting obligation for platforms, proportionate to their scale of reach and operational capacities, more specifically on their content moderation procedures, including information on adopted measures against illegal activities online and standardised data on the amount of content removed and the underlying legal reasons and bases, the type and justification of removal requests received, the number of requests whose execution was refused and the reasons therefore; stresses that such reports, covering actions taken in a given year, should be submitted by the end of the first quarter of the following year;

38. Calls, moreover, for an annual public reporting obligation for national authorities, including standardised data on the number of removal requests and their legal bases, on the number of removal requests that were subject to administrative or judicial remedies, on the outcome of these proceedings, with a mention of the outcomes that specified content or activities wrongly identified as illegal, and on the total number of decisions imposing penalties, including a description of the type of penalty imposed;

39. Expresses its concern regarding the fragmentation and the documented lack of financial and human resources for the supervision and oversight bodies; calls for increased cooperation between the Member States with regard to regulatory oversight of digital services;

40. Considers that in order to guarantee proper enforcement of the Digital Services Act, the oversight of compliance with procedures, procedural safeguards and transparency obligations laid down in this act should be harmonised within the digital single market; supports, in this regard, strong and rigorous enforcement by an independent EU oversight structure that has the competence to impose fines on the basis of an assessment of a clearly defined set of factors, such as proportionality, technical and organisational measures, and negligence; believes that this should include the possibility for fines to be based on a percentage of the annual global turnover of the company;

41. Stresses that audits of digital service providers' internal policies and algorithms should be made with due regard to Union law, in particular to the fundamental rights of the services' users, taking into account the importance of non-discrimination and the freedom of expression and information in an open and democratic society, and without publishing commercially sensitive data; urges that there is the need to assess, upon complaint or upon initiative of the oversight bodies, whether and how digital service providers amplify content, for example through recommendation engines and optimisation features such as autocomplete and trending;

42. Considers that the transparency reports drawn up by platforms and national competent authorities should be made publicly available and analysed for structural trends in removal, detection and blocking at EU level;

43. Underlines the importance of empowering users to enforce their own fundamental rights online, including by means of easily accessible, impartial, transparent, efficient and free complaint procedures, reporting mechanisms for illegal content and criminal behaviour for individuals and companies, legal remedies, educational measures and awareness-raising on data protection issues and child online safety;

44. Believes that past experience has proved the effectiveness of allowing innovative business models to flourish and of strengthening the digital single market by removing barriers to the free movement of digital services and preventing the introduction of new, unjustified national barriers, and that the continuation of this approach would reduce the fragmentation of the internal market; considers, furthermore, that the Digital Services Act can offer opportunities to develop citizens' knowledge and skills in the field of digitalisation, while at the same time guaranteeing a high level of consumer protection, including by safeguarding online safety;

45. Emphasises the indispensability of agreed standards of essential security in cyberspace in order for digital services to provide their full benefits to citizens; notes, therefore, the urgent need for the Member States to take coordinated action to ensure basic cyber hygiene and to prevent avoidable dangers in cyberspace, including through legislative measures;

46. Instructs its President to forward this resolution to the Council and the Commission.