European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

2020/2018(INL)

16.7.2020

OPINION

of the Committee on Civil Liberties, Justice and Home Affairs

for the Committee on the Internal Market and Consumer Protection

with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market
(2020/2018(INL))

Rapporteur for opinion (*): Paul Tang

(Initiative – Rule 47 of the Rules of Procedure)

(*)Associated committees – Rule 57 of the Rules of Procedure

PA_INL

SUGGESTIONS

The Committee on Civil Liberties, Justice and Home Affairs calls on the Committee on the Internal Market and Consumer Protection, as the committee responsible:

– to incorporate the following suggestions into its motion for a resolution:

1. Underlines that digital services and their underlying algorithms need to fully respect fundamental rights, especially privacy, the protection of personal data, non-discrimination and the freedom of expression and information and the rights of the child, as enshrined in the Treaties and the Charter of Fundamental rights of the European Union; calls therefore on the Commission to implement an obligation of non-discrimination, transparency and explainability of algorithms, penalties to enforce such obligations, and the possibility of human intervention, as well as other compliance measures, such as monitoring, evaluation, independent audits and specific stress tests to assist and enforce compliance; believes that a risk-based approach should be followed where stricter rules would be applied for algorithms that pose potential threats to fundamental rights and freedoms; underlines that the core of the concept of transparency and explainability of algorithms should be that the information provided for the user is presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child;

2. Emphasises that the rapid development of digital services requires a strong futureproof legislative framework to protect personal data and privacy; notes that the e-Commerce Directive dates back to 2000, however, the data protection regime is significantly updated since then; recalls therefore that any future provision of the DSA fully respects the broad framework of fundamental rights and the European regime on privacy and data protection; stresses in this regard that all digital service providers need to fully respect Union data protection law, namely Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and Directive (EC) 2002/58 of the European Parliament and of the Council (ePrivacy), currently under revision the freedom of expression and non-discrimination, and to ensure the security and safety of their systems and services;

3. Stresses the importance to apply effective end-to-end encryption to data, as it is essential for trust in and security on the Internet and effectively prevents unauthorized third party access; underlines that the DSA should provide a level-playing field by offering legal clarity regarding the concepts and definitions included in the legislation and by applying to all relevant actors offering digital services in the Union, regardless of whether they are established inside or outside the Union; stresses that the DSA should be future-proof and applicable to the emergence of new technologies with an impact on the digital single market; stresses that the DSA should uphold the right to use digital services anonymously, where the nature of the service or the existing legislation does not require the identification or authentication of the user or the customer;

4. Notes that since the online activities of individuals allow for deep insights into their personality and make it possible to manipulate them, the general and indiscriminate

collection of personal data concerning users actions and interactions online interferes disproportionately with the right to privacy; confirms that users have a right not to be subject to pervasive tracking when using digital services; stresses that in the spirit of the jurisprudence on communications metadata, public authorities shall be given access to a user's subscriber and metadata only to investigate suspects of serious crime with prior judicial authorisation; is convinced, however that digital service providers must not retain data for law enforcement purposes unless a targeted retention of an individual user's data is directly ordered by an independent competent public authority in line with Union law;

5. Notes the unnecessary collection of personal data by digital services at the point of registration for a service, such as gender, mobile phone number, e-mail address and postal address, often caused by the use of single-sign in possibilities; calls on the Commission to create a public service as an alternative to private single sign-in systems. Underlines that this service should be developed so that the collection of identifiable sign-in data by the sign-in provider is technically impossible and data gathered is kept to an absolute minimum; calls on the Commission to introduce an obligation on digital services to always also offer a manual sign-in option, set by default; recommends the Commission as well to create, as a public service, an age verification system for users of digital services, especially in order to protect minors; emphasises that both public services should not be used to track the users cross-site or used commercially, should be secure, transparent, only process data necessary for the identification of the user, and should not apply to any other digital services than those that require personal identification, authentication, or age verification, and should only be used with a legitimate purpose, and in no way be used to restrain general access to the internet; underlines that where a certain type of official identification is needed offline, an equivalent secure online electronic identification system needs to be created;

6. Emphasises the importance of user empowerment with regard to the enforcement of their own fundamental rights online; reiterates that digital service providers must respect and enable their users' right to data portability as laid down in Union law; stresses the difficulties that arise for individuals who want to enforce their individual data protection and privacy rights against dominant platforms, which are active on multiple markets and have multiple affiliates; requests therefore Member States and digital service providers to put in place transparent, easy, effective, fair, and expeditious complaint and redress mechanisms to allow individuals to avail of and enforce their rights under the GDPR, as well as to allow users to challenge the taking offline of their content; encourages digital service providers to create a single point of contact for all their underlying digital platforms, wherefrom user requests can be forwarded to the correct recipient; further notes that users should always be explicitly informed whether they are engaging with a human or a machine;

7. Points out that biometric data is considered to be a special category of personal data with specific rules for processing; notes that biometrics can and are increasingly used for identification and authentication of individuals, including in a number of sensitive areas such as banking and essential services such as healthcare, which, regardless of the potential advantages it might provide specifically the higher level of authenticity compared to alphanumeric security features or PIN codes, when physical presence,

when obtaining essential services, is difficult, entails significant risks to and serious interferences with the rights to privacy and data protection, particularly when carried out without the consent of the data subject, as well as enabling identity fraud; calls therefore on the Commission to incorporate in its DSA the obligation upon digital service providers to store biometric data only on the device itself, unless central storage is allowed by law, to always give users of digital services an alternative for using biometric data set by default for the functioning of a service, and the obligation to clearly inform the customers on the risks of using biometric data; stresses that a digital service may not be refused where the individual does not consent to use biometric data;

8. Notes the potential negative impact of personalised advertising, in particular micro-targeted and behavioural advertisement, as carried out by ad-tracking intermediaries and real-time bidding platforms, and of assessment of individuals without their consent, especially of minors, by interfering in the private life of the individuals, posing questions as to the collection and use of the data used to personalise advertising and to its potential to disrupt the functioning of democratic processes and elections, offering products or services or setting prices; is aware of the initiative of online platforms to introduce safeguards for instance transparency and enhanced user control and choice as outlined in the Code of Practice on Disinformation; calls therefore on the Commission to introduce strict limitations on targeted advertising based on the collection of personal data, starting with introducing a prohibition on cross-context behavioural advertisement without hurting small and mediums sized companies; reminds that currently, the ePrivacy Directive only allows targeted advertising subject to an opt-in consent, otherwise making it illegal, and calls on the Commission to prohibit the use of discriminatory practices for the provision of services or products;

9. Observes how digital services cooperate with the offline world, for example in the transport and the hospitality sectors; notes that local governments and the public sector can benefit from data of certain types of digital services to improve, for example, their urban planning policies; reminds that the collection, use and transfer of personal data, also between the private and the public sector is subject to the provisions of the GDPR; calls therefore on the Commission to make its proposal for the DSA not be incompatible with this aim;

10. Calls for increased cooperation with regard to regulatory oversight of digital services, therefore calls on the Commission to set up, a system for the supervision of the application of DSA and digital services, through cooperation of national and European oversight bodies and annual independent, external audits, that focus on digital service providers' algorithms, internal policies and the correct working of internal checks and balances with due regard to Union law and in all circumstances to the fundamental rights of the services' users, taking into account the fundamental importance of non-discrimination and the freedom of expression and information in an open and democratic society, and to task EU agencies and competent national supervisory authorities with the oversight of the implementation of the DSA;

11. Notes with concern that supervisory authorities in the Member States are under strain given the increased tasks and responsibilities to protect personal data and their lack of adequate financial and human resources; calls on the Commission to consider the

possibility of having large multinational tech companies to contribute to the resources of supervisory authorities;

12. Notes that digital services use advanced algorithms to analyse or predict personal preferences, interests or behaviour, which are used to disseminate and order the content shown to the users of their services; stresses that how these algorithms work and order the shown material, are not visible or explained to the users, which takes away their choice and control, enables the creation of echo chambers and leads to distrust in digital services; calls therefore on the Commission to compel in its DSA proposal digital services to offer the possibility to see content in a non-curated order, give more control to users on the way content is ranked to them, including options to a ranking outside their ordinary content consumption habits and to opt out completely of any content curation; calls on the Commission also to work out a duty of care regime that makes digital services responsible and accountable for content curation, which should be defined in detailed sectoral guidelines and to oblige transparency on the way digital services curate content;

13. Stresses that in line with the principle of data minimisation established by the GDPR, the DSA should require intermediaries of digital services to enable to the maximum extent possible the anonymous use of their services and payment for them wherever it is technically possible and not restricted by specific legislation, as anonymity effectively prevents unauthorized disclosure, identity theft and other forms of abuse of personal data collected online; highlights that only where existing legislation requires businesses to communicate their identity, providers of major market places could be obliged to verify their identity, while in other cases the right to use digital services anonymously should be upheld;

14. Emphasises that there are certain differences still between online and offline worlds, for instance, in terms of anonymity, the absence of a governing entity, between the balances of power and technical capabilities; highlights that because of the nature of the digital ecosystem, illegal content online can be proliferated easily and therefore its negative impact amplified within a very short period of time; notes that illegal content online can undermine trust in the digital services, as well as may also have serious and long-lasting consequences for the safety and fundamental rights of individuals; considers it is important to outline that what is regarded illegal content offline should be regarded as illegal content online;

15. Takes the position that, in this regard, any measure in the DSA should concern illegal content only as it is defined in Union law and national jurisdictions and should not include legally vague and undefined terms, such as “harmful content”, as targeting such content could put fundamental rights, especially the freedom of expression at serious risk;

16. Stresses that the responsibility for enforcing the law, deciding on the legality of online activities and content, as well as ordering hosting service providers to remove or disable access to illegal content, rests with independent competent public authorities; underlines the need to ensure that official decisions to remove content or disable access to it by independent competent public authorities are accurate, well-founded and respect fundamental rights;

17. Calls for the cooperation between independent competent public authorities and hosting service providers to be improved to ensure swift and correct flow of information, correct and timely removal or disabling access to illegal content, thus ordered by the independent competent public authorities and to guarantee the successful investigation and prosecution of potential crimes;

18. Reiterates that access to judicial redress should be available to content providers to satisfy the right to effective remedy; urges therefore the Commission to adopt rules on transparent notice-and-action mechanisms providing for adequate safeguards, for transparent, effective, fair, and expeditious complaint mechanism and possibilities to seek effective remedies against content removal;

19. Highlights in this context that in order to protect freedom of expression, avoid conflicts of laws, avert unjustified and ineffective geo-blocking and to aim for a harmonised digital single market, hosting service providers should not be required to apply one Member State's national restrictions on freedom of expression in another Member State or to remove or disable access to information that is legal in their country of establishment;

20. Notes consequently with concern, the increasing fragmentation of national laws concerning the fight against illegal content, or content that can be considered harmful; therefore emphasises the need to strengthen cooperation between the Member States; underlines the importance of such a dialogue, in particular regarding the differing national designations of what constitutes illegal content;

21. Calls on digital service providers, who on their own initiative take allegedly illegal content offline, to do so 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 especially 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; highlights, in this regard, that transparency obligations should be imposed on online intermediaries regarding the criteria applied to decisions on removals or disabling of access to content and the technology used to guarantee the application of necessary safeguards, non-discrimination and unnecessary removals or disabling of access; further calls on digital service providers to take the necessary measures to identify and label content uploaded by social bots;

22. Notes in this regard, that automated tools are currently unable to differentiate illegal content from content that is legal in a given context and underlines that any such tool be subject to human oversight and to full transparency of design and performance; highlights that a review of automated reports by service providers, their staff or their contractors does not solve this problem as private staff lack the independence, qualification and accountability of public authorities; therefore stresses that the DSA should explicitly prohibit any obligation on hosting service providers or other technical intermediaries to use automated tools for content moderation; requests instead, that digital service providers, who on their own initiative want to restrict certain legal content of their users, to explore the possibility of labelling rather than taking that content offline;

23. Stresses that public authorities should not impose a general obligation on digital service providers, neither de jure nor de facto, including through ex-ante measures, to monitor the information which they transmit or store, nor a general obligation to actively seek, moderate or filter content indicating illegal activity; is also convinced that digital service providers should not be required to prevent the upload of illegal content; suggests therefore, where technologically feasible, based on 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 the content of which 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[1], are identical or equivalent to the extent that would not require the host provider to carry out an independent assessment of that content;

24. Calls on the Commission to consider obliging hosting service providers to report illegal content constituting a serious crime to the competent law enforcement authority, upon becoming aware of it; calls also on the Commission, Member States and hosting service providers to establish transparent notice mechanisms for users to notify the relevant authorities of potentially illegal content; requests further the Member States to improve access to and the efficiency of their justice and law enforcement systems in relation to determining the illegality of online content and in relation to dispute resolution concerning deleting or disabling access to content;

25. Highlights that, in order to constructively build upon the rules of the e-Commerce Directive and to ensure legal certainty, applicable legislation should be proportionate and should spell out the explicit duties of digital service providers rather than imposing a general duty of care; emphasises that certain duties can be further specified by sectoral legislation; highlights that the legal regime for digital providers liability should not depend on uncertain notions such as the ‘active’ or ‘passive’ role of providers;

26. Believes that infrastructure service providers, payment providers, and other companies offering services to digital service providers, should not be held liable for the content a user uploads or downloads on their own initiative; believes that digital service providers, who have a direct relationship with a user and who have the ability to remove distinct pieces of the user content, should only be held liable if they fail to expeditiously respond to sufficiently substantiated removal orders by independent competent public authorities, or where they have actual knowledge of illegal content or activities.

---

[1] Judgment of the Court of Justice of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Case C-18/18; ECLI:EU:C:2019:821.

INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

Date adopted	16.7.2020
Result of final vote	+: 40 –: 4 0: 23
Members present for the final vote	Magdalena Adamowicz, Konstantinos Arvanitis, Katarina Barley, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Saskia Bricmont, Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Lena Düpont, Laura Ferrara, Nicolaus Fest, Jean-Paul Garraud, Sylvie Guillaume, Andrzej Halicki, Balázs Hidvéghi, Evin Incir, Sophia in ‘t Veld, Patryk Jaki, Lívia Járóka, Fabienne Keller, Peter Kofod, Moritz Körner, Juan Fernando López Aguilar, Nuno Melo, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Martin Sonneborn, Sylwia Spurek, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Jadwiga Wiśniewska, Elena Yoncheva, Javier Zarzalejos
Substitutes present for the final vote	Abir Al-Sahlani, Bartosz Arłukowicz, Malin Björk, Delara Burkhardt, Gwendoline Delbos-Corfield, Nathalie Loiseau, Erik Marquardt, Sira Rego, Domènec Ruiz Devesa, Paul Tang, Hilde Vautmans, Tomáš Zdechovský
Substitutes under Rule 209(7) present for the final vote	Sven Mikser

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

40	+
PPE	Bartosz Arłukowicz
S&D	Katarina Barley, Pietro Bartolo, Delara Burkhardt, Caterina Chinnici, Sylvie Guillaume, Evin Incir, Juan Fernando López Aguilar, Sven Mikser, Javier Moreno Sánchez, Domènec Ruiz Devesa, Sylwia Spurek, Paul Tang, Bettina Vollath, Elena Yoncheva
Renew	Abir Al-Sahlani, Sophia in 't Veld, Moritz Körner, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu, Hilde Vautmans
ID	Nicolaus Fest, Peter Kofod, Annalisa Tardino, Tom Vandendriessche
Verts/ALE	Saskia Bricmont, Damien Carême, Gwendoline Delbos-Corfield, Erik Marquardt, Terry Reintke, Diana Riba i Giner, Tineke Strik
GUE/NGL	Konstantinos Arvanitis, Malin Björk, Clare Daly, Sira Rego
NI	Laura Ferrara, Martin Sonneborn, Milan Uhrík

4	-
PPE	Javier Zarzalejos
ID	Nicolas Bay, Jean-Paul Garraud, Marcel de Graaff

23	0
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Andrzej Halicki, Balázs Hidvéghi, Lívia Járóka, Nuno Melo, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Tomas Tobé, Tomáš Zdechovský
Renew	Fabienne Keller, Nathalie Loiseau
ECR	Joachim Stanisław Brudziński, Jorge Buxadé Villalba, Patryk Jaki, Nicola Procaccini, Jadwiga Wiśniewska

Key to symbols:
+ : in favour
- : against
0 : abstention