Council of the European Union

Brussels, 21 December 2020
(OR. en)

14124/20
ADD 2

Interinstitutional File:
2020/0361(COD)

COMPET 641
MI 576
JAI 1116
TELECOM 268
CT 119
PI 92
AUDIO 65
CONSOM 222
CODEC 1404
IA 126

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	16 December 2020
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2020) 348 final PART 2/2
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT ANNEXES Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

Delegations will find attached document SWD(2020) 348 final PART 2/2.

Encl.: SWD(2020) 348 final PART 2/2

EUROPEAN
COMMISSION

Brussels, 15.12.2020
SWD(2020) 348 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

ANNEXES

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

{COM(2020) 825 final} - {SEC(2020) 432 final} - {SWD(2020) 349 final}

Annexes

Annex 1: Procedural information

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

This Staff Working Paper was prepared by the Directorate-General for Communications Networks, Content and Technology.

The *Decide* reference of this initiative is PLAN/2020/7444.

This includes the Impact Assessment report as well as, annexed to the report, the evaluation report for the E-Commerce Directive.

ORGANISATION AND TIMING

The Impact Assessment was prepared by DG CONNECT as the lead Directorate-General.

The Inter-Service Steering Group established for the work streams on online platforms was associated and consulted in the process, under the coordination of the Secretariat-General, including the following services: DG AGRI (DG for Agriculture and Rural Development), DG COMP (DG Competition), DG ECFIN (DG Economic and Financial Affairs), DG EMPL (DG Employment, Social Affairs and Inclusion), DG ENV (DG Environment, DG FISMA (DG for Financial Stability, Financial Services and Capital Markets Union), DG GROW (DG Internal Market, Industry, Entrepreneurship and SME), DG HOME (DG Migration and Home Affairs), DG JUST (DG Justice and Consumers), JRC (Joint Research Centre), DG MOVE (DG Mobility and Transport), DG RTD (DG Research and Innovation), DG REGIO (DG Regional and Urban Policy), SJ (Legal Service), DG SANTE (DG for Health and Food Safety), DG TRADE, EEAS (European External Action Service).

The last meeting of the ISSG, chaired by the Secretariat-General of the European Commission was held on 6 October 2020.

CONSULTATION OF THE RSB

The Regulatory Scrutiny Board gave a positive opinion with reservation on the draft impact assessment report submitted on 8 October 2020 and discussed in the hearing that took place on 4 November 2020. To address the feedback given by the Regulatory Scrutiny Board, the following changes were made in the Impact Assessment report and its annexes:

Findings of the Board	**Main modifications made in the report to address them**
1. The report does not sufficiently explain the coherence between the Digital Services Act and the broader regulatory framework, in particular the relation to	The report was amended to explain in more detail the coherence considerations, both in the problem statement section and in the coherence analysis for the options.

sectoral legislation and the role of self-regulation.	
2. The policy options are not complete and not sufficiently developed. They lack detail and their content is not well explained.	The policy options were revised to give further details on each of them and their components. For option 3, governance sub-options were further explained. Further information was added on the threshold for the very large platforms both in the main report and in Annex 4
3. The report does not clearly present the evidence that leads to the choice of the preferred policy option. The assessment of compliance costs is insufficient.	Building on the additional specifications of the options, the analysis of impacts was further refined, including more granular presentation of costs. The presentation and analysis of the comparison of options was updated accordingly.
Stakeholder views	The main report and the annex present stakeholder views with more granularity

EVIDENCE, SOURCES AND QUALITY

Studies commissioned or supported by the European Commission

Dealroom. (2020). *Global platforms and markerplaces.* Report for the European Commission.

Eurobarometer - TNS. (2018, July). *Flash Eurobarometer 469: Illegal content online.* doi:10.2759/780040

Eurobarometer - TNS. (2016). Flash Eurobarometer 439: The Use of Online Marketplaces and Search Engines by SMEs. Retrieved from https://ec.europa.eu/information_society/newsroom/image/document/2016-24/fl_439_en_16137.pdf

ICF, Grimaldi, *The Liability Regime and Notice-and-Action Procedures*, SMART 2016/0039

LNE. (forthcoming). SMART 2018/37 Exploratory study on the governance and accountability of algorithmic systems

Optimity Advisors, SMART 2017/ 0055 Algorithmic Awareness building – State of the art report

Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission

Van Hoboken J. et al., *Hosting Intermediary Services and Illegal Content Online*

Selective list of relevant case law

C- 18/18, *Glawischnig.* ECLI:EU:C:2019:821.

C-390/18 Airbnb Ireland

C-484/14, McFadden, ECLI:EU:C:2016:689.

CJEU -149/15, Sabrina Wathelet v Garage Bietheres & Fils SPRL

C-434/15 Asociación Profesional Elite Taxi v Uber Systems Spain SL

C-314/12, UPC Telekabel Wien, EU:C:2014:192.

C-360/10, SABAM, ECLI:EU:C:2012:85;

C-70/10 (SABAM v Scarlet)

C 360/10 (SABAM v Netlog NV)

C-324/09, L'Oreal v eBay, ECLI:EU:C:2011:474.

C-236/08 to C-238/08, Google France and Google v. Vuitton, ECLI:EU:C:2010:159.C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.

Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989,

C-101/01 Lindqvist [2003] ECR I-12971

ECHR, Application no. 24683/14 ROJ TV A/S against Denmark

French Supreme Court, 12 July 2012, no. 11-13.666, 11-15.165/11-15.188, 11-13.669

Hizb ut-Tahrir and Others v. Germany, No. 31098/08

Kasymakhunov and Saybatalov v Russia, No. 26261/05 and 26377/06

ECHR, Application no. 56867/15 Buturugă against Romania, judgment of 11 February 2020

Gerechtshof Amsterdam, 24 June 2004, 1689/03 KG, Lycos gegen Pessers.

Zeran v AOL, 129 F.3d 327 (4th Cir. 1997).

Antwerp Civil Court, 3 December 2009, A&M, 2010, n.2010/5-6

President of the Brussels Court (NL), n 2011/6845/A, 2 April 2015

OLG Karlsruhe Urt. v. 14.12.2016 – 6 U 2/15

GRURRS 2016, 115437

Milan Court of Appeal, R.T.I. v. Yahoo! Italia, n. 29/2015;

Rome Court of Appeal, RTI v TMFT Enterprises LLC, judgment 8437/2016 of 27 April 2016

Turin Court of First instance, judgment 7 April 2017 No 1928, RG 38113/2013, Delta TV v Google and YouTube

Supreme Court of Hungary Pfv.20248/2015/9.

Supreme Court, OGH 6 Ob 178/04a.

Judgement of Appellate Court in Wroclaw of 15 January 2010, I Aca 1202/09.

Judgement of 15 April 2014, ECLI:NL:HR:2014:908 (interpretation Art. 54a Sr).

LG Leipzig, judgement of 19 May 2017 (05 O 661/15).

Selective bibliography

Alastair Reed, J. W. (2019). Radical Filter Bubbles. Social Media Personalisation Algorithms and Extremist Content. *Global Research Network on Terrorism and Technology*(Paper No. 8). Retrieved from https://www.rusi.org/sites/default/files/20190726_grntt_paper_08.pdf

Alrhmoun, A., Maher, S., & Winter, C. (2020). Decoding Hate: Using Experimental Text Analysis to Classify Terrorist Conten*t*. Global Network on Extremism and Technology. https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content.pdf

Ali M., e. a. (2019). Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes. *Proceedings of the ACM on Human-Computer Interaction.* Retrieved from https://arxiv.org/pdf/1904.02095.pdf

Angelopoulos, C., Smet S. (2016) 'Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability' (October 21, 2016). In *Journal of Media Law,* Taylor & Francis. Retrieved from SSRN: https://ssrn.com/abstract=2944917

Artificial intelligence and the future of online content moderation. (2018, March 21). Freedom to Tinker — Research and expert commentary on digital technologies in public life. "https://freedom-to-tinker.com/2018/03/21/artificial-intelligence-and-the-future-of-online-content-moderation/

Bridy, A. (2019). The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform . Forthcoming in Vanderbilt Journal of Entertainment & Technology Law, p. 115. http://dx.doi.org/10.2139/ssrn.3412249

Bridy, A. (2017). Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation . Washington and Lee Law Review, 74(3), 1345–1388 https://scholarlycommons.law.wlu.edu/wlulr/vol74/iss3/3/"

Cobbe J., Singh J. (2019) 'Regulating Recommending: Motivations, Considerations, and Principles', European Journal of Law and Technology, 10 (3)

Coppock, A. (2020, September 2). The small effects of political advertising are small regardless of context, message, sender, or receiver: Evidence from 59 real-time randomized. Science Advances, 6(36). doi:https://advances.sciencemag.org/content/6/36/eabc4046

Crabit, E. (2000). La directive sur le commerce électronique. le project "Méditrranée'. Revue du Droit de l'Union Européenne(4), 749-833.

Datta A., D. A. (2018). Discrimination in Online Advertising. A Multidisciplinary Inquiry. Proceedings of Machine Learning Research . 81, pp. 1-15. Conference on Fairness, Accountability, and Transparency. Retrieved from http://proceedings.mlr.press/v81/datta18a/datta18a.pdf

De Streeel A.,, Husovec M. (2020) The e-commerce Directive as the cornerstone of the Internal Market - Assessment and options for reform, Study for the IMCO committee PE 648.797, retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf

Duch-Brown N., Martens B. (2015). The European Digital Single Market. Its Role in Economic Activity in the EU. (I. f. Studies, Ed.) Digital Economy Working Paper(17). Retrieved from https://ec.europa.eu/jrc/sites/jrcsh/files/JRC98723.pdf

European Commission. (2018, September 12). SWD(2018) 408 final, Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf

European Commission. (2019). Report on the EU customs enforcement of intellectual property rights: results at the EU border in 2018. Luxembourg: Publications Office of the European Union. Retrieved from https://ec.europa.eu/taxation_customs/sites/taxation/files/2019-ipr-report.pdf

European Commission. (2020). SWD(2020) 116 final/2 Commission Staff Working Document: Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet. Retrieved from https://ec.europa.eu/docsroom/documents/42701

Feci, N. (2018). Gamers watching gamers: the AVMSD soon the one calling the shots?.

Floridi, L., & Taddeo, M. (2017). The Responsibilities of Online Service Providers. Springer

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7(1), 2053951719897945.

Grygiel, J. (2019, July 24). *Facebook algorithm changes suppressed journalism and meddled with democracy*. The Conversation. HYPERLINK https://theconversation.com/facebook-algorithm-changes-suppressed-journalism-and-meddled-with-democracy-119446

Hawkinson, J., & Bates, T. (1996). Guidelines for creation, selection, and registration of an Autonomous System (AS).

Hoeren, T., & Völkel, J. (2018). Information Retrieval About Domain Owners According to the GDPR . Datenschutz und Datensicherheit. https://doi.org/10.2139/ssrn.3135280

How Facebook can flatten the curve of the coronavirus Infodemic. (2020). Avaaz. https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation

INHOPE. (2019). Annual Report 2018. Amsterdam: INHOPE Association. Retrieved from https://www.inhope.org/media/pages/the-facts/download-our-whitepapers/3976156299-1591885517/2019.12.13_ih_annual_report_digital.pdf

Iusi Li, J. C. (2016). Advertising Role of Recommender Systems in Electronic Marketplaces: A Boon or a Bane for Competing Sellers? Retrieved from https://ssrn.com/abstract=2835349 or http://dx.doi.org/

Keller, D. *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*, 2017 http://cyberlaw.stanford.edu/blog/2017/04/%E2%80%9Cright-be-forgotten%E2%80%9D-and-national-laws-under-gdpr

Kojo, M., Griner, J., & Shelby, Z. (2001). Performance enhancing proxies intended to mitigate link-related degradations.

Kuerbis, B., Mehta, I., & Mueller, M. (2017). In Search of Amoral Registrars: Content Regulation and Domain Name Policy. Internet Governance Project, Georgia Institute of Technology.https://www.internetgovernance.org/wp-content/uploads/AmoralReg-PAPER-final.pdf

Landmark data sharing agreement to help safeguard victims of sexual abuse imagery. (2019, December "https://www.iwf.org.uk/news/landmark-data-sharing-agreement-to-help-safeguard-victims-of-sexual-abuse-imagery"

Law, Borders and Speech Conference: Proceedings and Materials, https://cyberlaw.stanford.edu/page/law-borders-and-speech

Madiega, T. (2020). Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act. European Parliamentary Research Service.

Mandola Project, *Best practice Guide for responding to Online Hate Speech for internet industry,* http://mandola-project.eu/m/filer_public/29/10/29107377-7a03-432e-ae77-e6cbfa9b6835/mandola-d42_bpg_online_hate_speech_final_v1.pdf

Matias, M. P. (2020). Do Automated Legal Threats Reduce Freedom of Expression Online? Preliminary Results from a Natural Experiment. Retrieved from https://osf.io/nc7e2/

Moura, G. C., Wabeke, T., Hesselman, C., Groeneweg, M., & van Spaandonk, C. (2020). Coronavirus and DNS: view from the. nl ccTLD.

Iacob N. et al.(2020). *How to Fully Reap the Benefits of the Internal Market for E-Commerce?*, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648801/IPOL_STU(2020)648801_EN.pdf

National Research Council. (2005). Signposts in cyberspace: the Domain Name System and internet navigation. National Academies Press

Niombo L., Evas T. *Digital services act - European added value assessment*, Study for the European Parliamentary Research Service PE 654.180. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf.

Nordemann, J. B. (2018). Liability of Online Service Providers for Copyrighted Content–Regulatory Action Needed. Depth Analysis for the IMCO Committee.

Nordemann J. B. (2020), *The functioning of the Internal Market for Digital Services: responsibilities and duties of care of providers of Digital Services*, Study for the IMCO committee, PE 648.802. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648802/IPOL_STU(2020)648802_EN.pdf.

OECD/EUIPO. (2019). Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade. Paris: OECD Publishing/ European Union Intellectual Property Office. Retrieved from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/trends_in_trade_in_counterfeit_and_pirated_goods/trends_in_trade_in_counterfeit_and_pirated_goods_en.pdf

OECD. (2020). Connecting Businesses and Consumers During COVID-19 Through Cross-Border Trade In Parcels. https://read.oecd-ilibrary.org/view/?ref=135_135520-5u04ajecfy&title=Connecting-Businesses-and-Consumers-During-COVID-19-Trade-in-Parcels

Penney, J. (2019, September 1). Privacy and Legal Automation: the DMCA as a Case Study. Stanford Technology Law Review, 22(1), 412-486. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504247

Piper, D. L. A. (2009). EU study on the legal analysis of a single market for the information society–new rules for a new age?. DLA Piper, November.

Reale, M., 'Digital Markets, Bloggers, and Trendsetters: The New World of Advertising Law' in MDPI, 3 September 2019, P. 9.

Rosenzweig, P. (2020). The Law and Policy of Client-Side Scanning (Originally published by Lawfare).

Schulte-Nölke H. et al, (2020), *The legal framework for e-commerce in the Internal Market - State of play, remaining obstacles to the free movement of digital services and ways to improve the current situation*, Study for IMCO committee PE 652.707. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652707/IPOL_STU(2020)652707_EN.pdf.

Schwemer, S.F. (2018). On domain registries and unlawful website content. Computer Law & Security Review

Schwemer, S.F. (2020). Report on the workshop on the liability of DNS service providers under the ECD, Prepared for Directorate-General for Communications Networks, Content and Technology (Unit Next-Generation Internet, E.3Schwemer, S., Mahler, T. & Styri, H. (2020). Legal analysis of the intermediary service providers of non-hosting nature. Final report prepared for the European Commission

Sluijs, J. et al. (2012). Cloud Computing in the EU Policy Sphere, JIPITEC, 12, N 80.Smith M. (2020), *Enforcement and cooperation between Member States - E-Commerce and the future Digital Services Act*, Study fot IMCO committee, PE 648.780. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648780/IPOL_STU(2020)648780_EN.pdf?utm_source=EURACTIV&utm_campaign=247d4049f5-digital_brief_COPY_01&utm_medium=email&utm_term=0_c59e2fd7a9-247d4049f5-116254339

Sohnemann N., Uffrecht L.M, Constanzehartkopf M, Kruse J. P., De Noellen L. M., *New Developments in Digital Services Short-(2021), medium-(2025) and long-term (2030) perspectives and the implications for the Digital Services Act*, Study for IMCO committee, PE 648.784. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648784/IPOL_STU(2020)648784_EN.pdf

Stalla-Bourdillon, S. (2017). Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well. In The Responsibilities of Online Service Providers (pp. 275-293). Springer, Cham.

Stephan Lewandowsky, L. S. (2020 (forthcoming)). Technology and democracy: Understanding the influence of online technologies on political behaviour and decision-making.

Tech Against Terrorism (2019), Case study: Using the GIFCT hash-sharing database on small tech platformshttps://www.counterextremism.com/sites/default/files/TAT%20--%20JustPaste.it%20GIFCT%20hash-sharing%20Case%20study.pdf

Truyens, M., & van Eecke, P. (2016). Liability of Domain Name Registries: Don't Shoot the Messenger. Computer Law & Security Review, 32(2), 327–344.

Urban, J. e. (2017, March). Notice and takedown in everyday practice. UC Berkeley Public Law Research Paper No. 2755628. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628

Van Hoboken, J., Appelman, N., Ó Fathaigh, R., Leerssen, P., McGonagle, T., van Eijk, N., & Helberger, N. (2019). De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties: Tussenrapportage (Oktober 2019).

Van Hoboken, J. and coll. (2018). *Hosting intermediary services and illegal content online: An analysis of the scope of Article 14 ECD in light of developments in the online service landscape*. Final report prepared for the European Commission.

Wagner B., Rozgonyi K. et al. (2020). *Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act*

Weber, R.H. & Staiger, D.N. (2014). *Cloud Computing: A cluster of complex liability issues*, 20(1) *Web JCL*., http://webjcli.org/article/view/303/418

Wilman, F., *The responsibility of online intermediaries for illegal user content in the EU and in the US*, 2020 (forthcoming)

Annex 2: Stakeholder consultation

1. THE STAKEHOLDERS ENGAGEMENT STRATEGY

The Commission has consulted broadly on issues related to digital services and platforms in the last years. The consultation process around these issues is built on recent and past consultation steps, which have already narrowed down the spectrum of pertinent options and have singled out specific issues.

A series of meetings and a consultation on the inception impact assessment published on the 2 June 2020 informed the problem definition and led to preliminary policy options. An open public consultation, open between June 2020 and September 2020, also contributed to the design and testing of policy options. For gathering the views of the general public, the Commission also ran a Eurobarometer survey in 2018 with a representative sample of over 33,000 respondents form all EU Member States.

Targeted consultations have also been conducted over the past years, including a series of workshops, conferences, interviews with experts and judges, expert groups, as well as a long-list of bilateral meetings and the reception of position papers and analytical papers from organizations, industry representatives, civil society and academia.

In developing the stakeholder engagement strategy, the stakeholder mapping included:

1. **Private sector**: capturing views of businesses of different sizes and reach within the European market. The private sector includes but is not limited to information society services. Businesses and associations representing their interests primarily pertain to the following categories:
    a) **Online intermediaries** including, but not limited to, internet service providers, caching services, storage and distribution services (e.g. web hosting, online media sharing platforms, file storage and sharing, IaaS/PaaS), networking, collaborative production and matchmaking services (e.g. social networking and discussion forums, collaborative production, online marketplaces, collaborative economy, online games), and selection, search and referencing services (e.g. search tools, ratings and reviews services).
    b) **Other digital services which are not online intermediaries:** e.g. website owners, private bloggers, private e-tailers, etc.
    c) **Third parties** involved in the ecosystem around digital services including, but not limited to, advertising providers, providers of content moderation tools, providers of payment services, data brokers, other services built as ancillary to online platforms, or primarily based on data accessed from the online platforms, other interested parties such as content creators, rights holders, etc.
    d) **Offline and online services** that provide their services through online intermediaries, such as retailers on marketplaces, app developers, publishers, hotel owners, etc.
    e) **Innovative start-ups and associations representing start-ups pertaining to the categories above.**

f) **Trade and business associations** representing the different interests of the businesses in the above categories.

2. **Users of digital services, as well as civil society organisations** representing their interests in terms of e.g. digital rights, interests of vulnerable groups and victims of online crimes.
3. **National authorities** including law enforcement, data protection and consumer protection authorities, and other relevant regulatory bodies and government departments in member states and, to the extent possible, in regions and municipalities.
4. **Academia** from the technical, legal and social science communities.
5. **Technical community** such as the Internet Architecture Board, ICANN, Internet Engineering Task Force, etc.
6. **International organisations** dealing with the issues at stake at different governance levels e.g. the UN, the Council of Europe, OSCE.
7. **General public**, in particular through a dedicated section in the open public consultation. Representative statistics on certain aspects have been computed on the basis of the Eurobarometer survey of 2018.

The different consultation tools as well as brief summaries of their results are described below.

2. OPEN PUBLIC CONSULTATIONS

The Commission has conducted several open public consultations on the related issues (i) in 2010 in the context of the evaluation of the e-Commerce Directive (ECD)[1]; (ii) in 2012, with a focus on notice-and-action procedures for all types of illegal content[2]; (iii) in 2016, part of the broader open public consultation on online platforms[3]; (iv) in 2018 on measures to further improve the effectiveness of the fight against illegal content online and finally[4]; (v) in 2020 in the context of the Digital Services Act Package.

[1] https://ec.europa.eu/information_society/newsroom/image/document/2017-4/consultation_summary_report_en_2010_42070.pdf
[2] https://ec.europa.eu/information_society/newsroom/image/document/2017-4/consultation_summary_report_en_2010_42070.pdf
[3] https://ec.europa.eu/digital-single-market/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud
[4] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal

2.1. Open Public Consultation on the Digital Services Act (2 June 2020 – 8 September 2020)[5]

In total, 2,863 responses were submitted by a diverse group of stakeholders. Most feedback was received by citizens (66% from EU citizens, 8% from non-EU citizens), companies/ businesses organizations (7.4%), business associations (6%), and NGOs (5.6%). This was followed by public authorities (2.2%), others (1.9%), academic/research institutions (1.2%), trade unions (0.9%), as well as consumer and environmental organisations (0.4%) and several international organisations. Additionally, around 300 position papers were received in the context of the open public consultation.

The organisation SumOfUs organised a campaign with a parallel and more general questionnaire on citizens' concerns related to online platforms, gathering around 738 replies mostly from UK (56%), FR (10%) and DE (8%). Most contributions centred on the rising problems surrounding fake news and hate speech online. Respondents jointly called for action, but also formulated concerns regarding free speech.

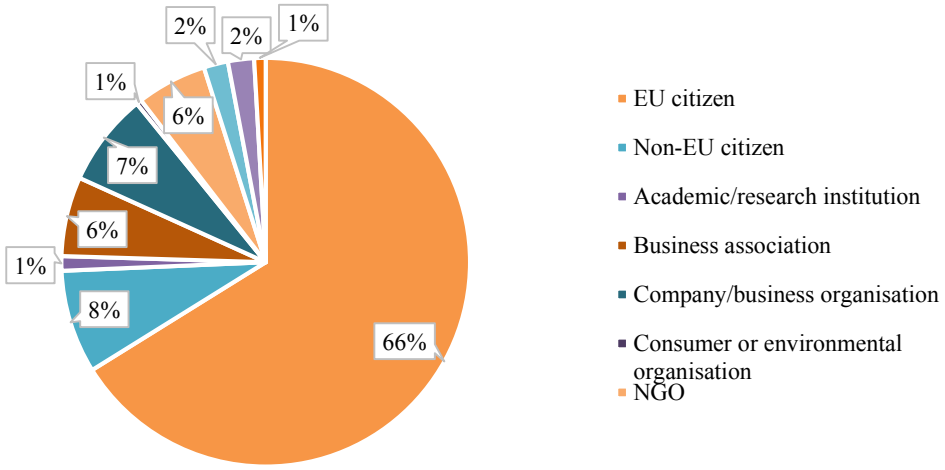


Figure 1: Type of Respondent

In terms of geographical distribution, most of the respondents are located in the EU, with a majority of contributions coming from Germany (27.8%), France (14.3%), and Belgium (9.3%). Internationally, the highest share of respondents that participated were from the UK (20.6%) and the US (2.8%)[6].

[5] The report on this open public consultation includes but is not limited to an analys of the replies performed by College of Europe contracted by the Commission to support in the qualitative and quantitative analysis.

[6] Countries with ≤15 submissions include Czechia, Hungary, Norway, Luxembourg, Romania, Greece, Latvia, Slovakia, Canada, Lithuania, Australia, Cyprus, Malta, Japan, Slovenia, Bulgaria, Croatia, Estonia, Russia, China, Greenland, Iceland, India, Iran, Micronesia, Thailand, Ukraine, Åland Islands

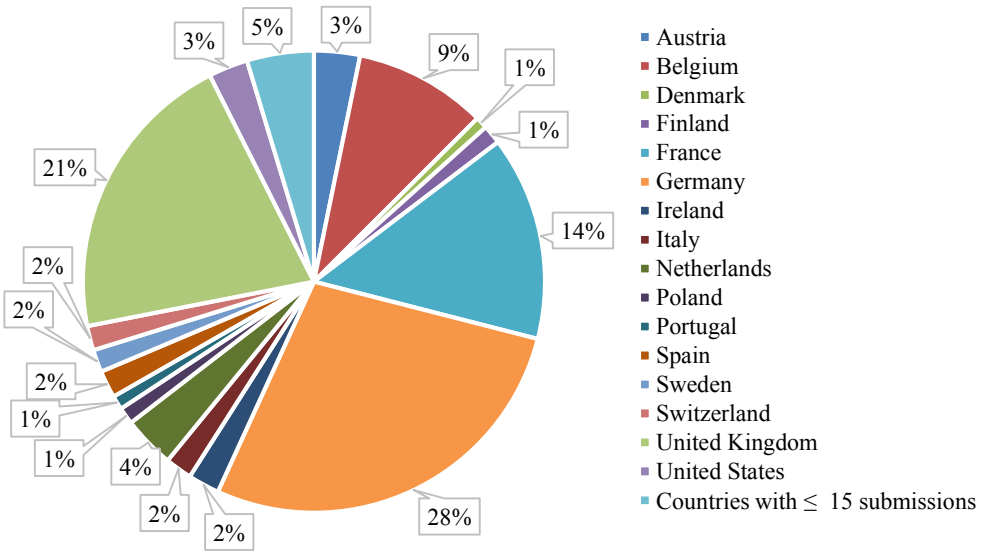


Figure 2: Country of Origin of Respondents

Zoom-in: the three largest respondent groups

Companies/Businesses organizations and business associations

Of the 211 participating companies/business organizations, 80.1% specified that they were established in the EU and 11.4% indicated that they were established outside of the EU.

26.5% described themselves as a conglomerate, offering a wide range of services online. 21.3% identified as a scale-up and 6.6% as a start-up. In terms of annual turnover, more than half of the participating companies/business organizations indicated a turnover of over EUR 50 million per year. 13.3% make an annual turnover of smaller than or equal to EUR 2 million, 3.8% of the respondent revealed an annual turnover of smaller than or equal to EUR 10 Mio, whereas 6.2% specified an annual turnover of smaller than or equal to EUR 50 Mio. 28.4% of the responding companies/business organizations were online intermediaries, 24.6% were other types of digital services. 12.3% indicated that they were an association, representing the interest of the types of businesses named prior. Of the 180 participating business associations, 15% indicated that they were representing online intermediaries, 19.4% specified that they are working on behalf of digital service providers other than online intermediaries, and 40% indicated that they represented the interests of other businesses.

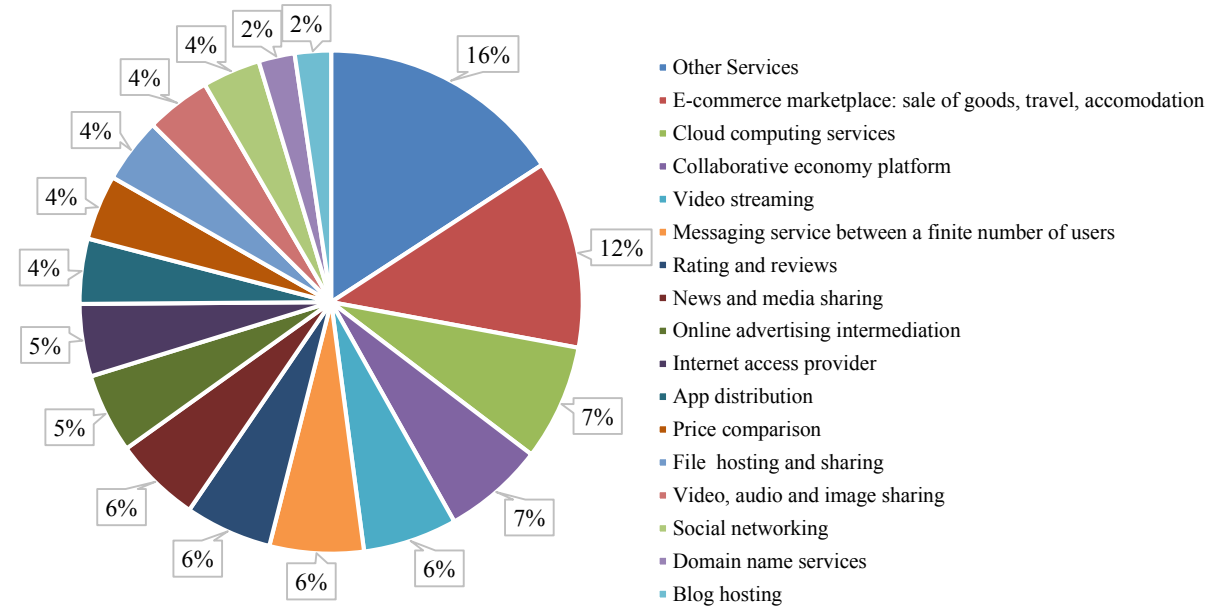


Figure 3: Type of Services provided by responding companies/business organisations

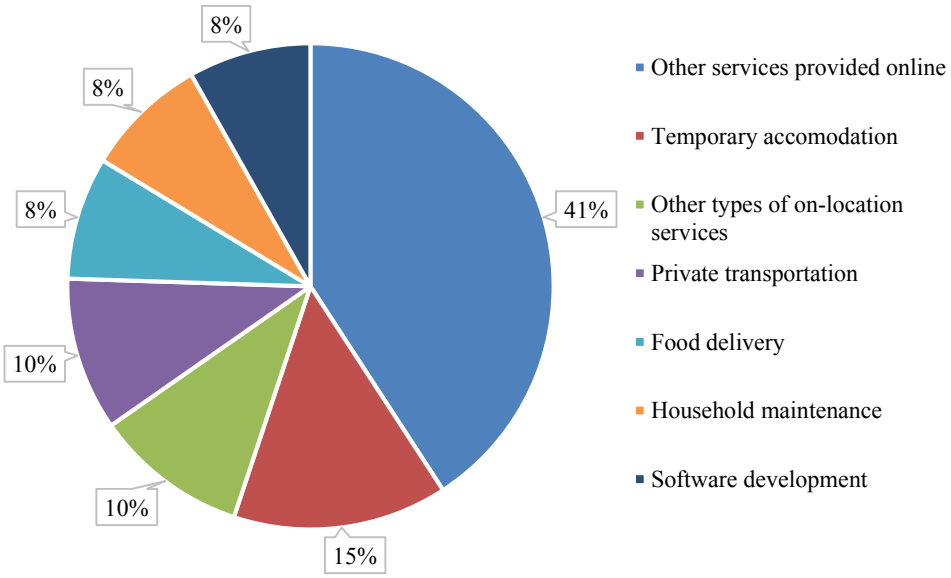


Figure 4: Intermediated Services by responding platforms

NGOs

Of the 159 participating NGOs, almost half (49.7%) stated, that they represented fundamental rights in the digital environment. 22.6% dealt with flagging illegal activities or information to online intermediaries for removal, and 22% represented consumer rights in the digital environment. Furthermore, 18.9% specified that they were fact checking and/or cooperating with online platforms for tackling harmful, (but not illegal) behaviours and 13.2% represented the rights of victims of illegal activities online. 10.7% represented

interests of providers of services intermediated by online platforms, including trade unions, and 10.7% gave no answer. 30.8% of the responding NGOs indicated "other".

Public authorities

59 public authorities participated in the open public consultation, of which 43 representing authorities at national level (72.9%), 8 at regional level (13.6%), 6 at international level (10.2%), and 2 at local level (3.4%). Among EU Member States, authorities replied from Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Luxembourg, and Poland. About half of the responding public authorities were governments, administrative or other public authorities other than law enforcement in a member state of the EU (49.2%). 15.3% indicated that they were a law enforcement authority in a Member State of the EU and 15.3% specified that they were another independent authority in a member state of the EU. These replies are complemented by a targeted consultation ran by the Commission with Member States.

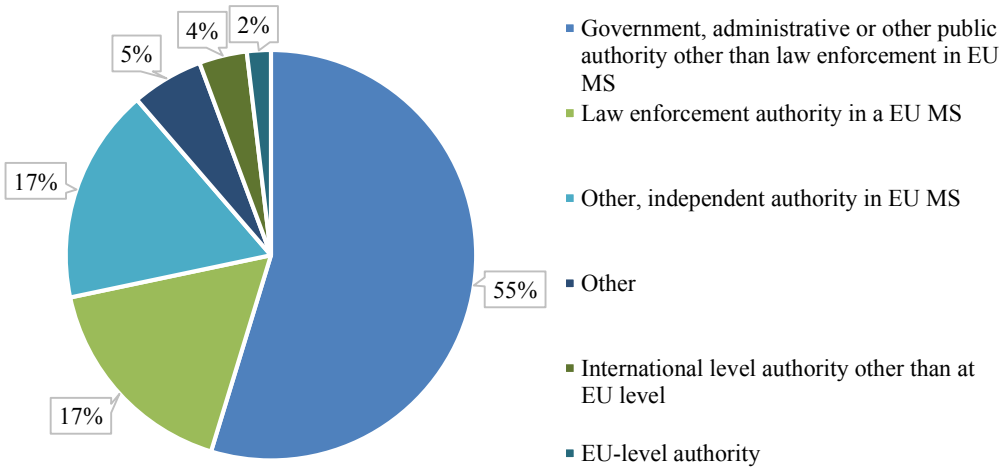


Figure 6: Type of responding public authority

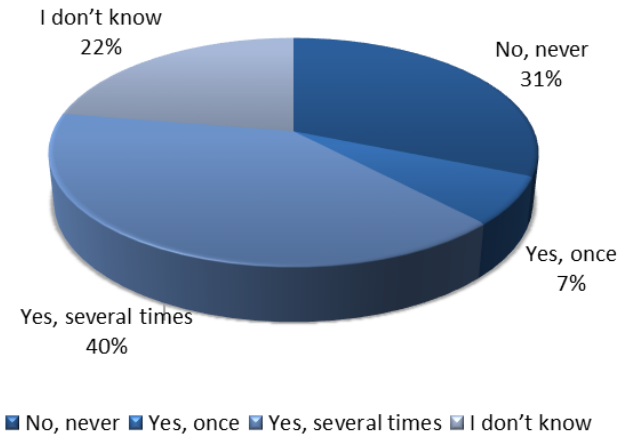
Summary of Results

Exposure to illegal content, goods or services online and related issues

A majority of respondents, all categories included, indicated that they had encountered both harmful and illegal content, goods or services online, and specifically noted a spike during the Covid-19 pandemic More specifically, 47% of respondents who replied to the relevant question indicated, that they had come across illegal goods, on online platforms at least once, as shown in Figure 1[7]. 67% stated that they had encountered illegal content online. The main issues reported by the respondents in relation to goods are deceptive advertising especially in relation to food, food supplements, drugs and COVID-19; advertising on pet

[7] Sample size: 2,312

Figure 7. Illegal Goods found on Online Platforms



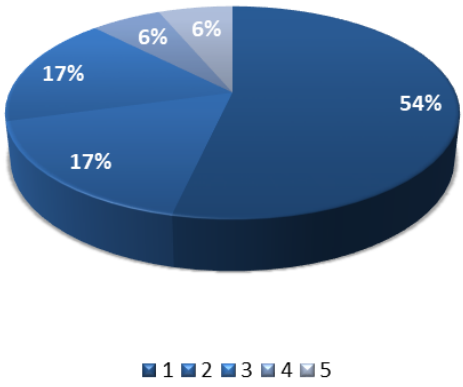
and wildlife trafficking; counterfeit and defective or stolen goods, electronics and clothes. Regarding services, the main issues raised by the respondents are fake event tickets or cases in which platforms illegally re-sell tickets and inflate their prices, cryptocurrencies and trading online, as well as general cases of phishing. Finally, in relation to content, the respondents report significant issues related to hate speech (racism, anti-Semitism, white supremacy, calls for violence against migrants and refugees, extremism, far-right propaganda, homophobia, sexism, defamation); general incitement to violence; unwanted pornography and prostitution ads; child sexual abuse material; IP infringement for movies, copyrighted content, political disinformation and fake news.

A large share of respondents who said they had notified illegal content, goods or services to platforms, expressed their dissatisfaction with the platforms' response, and the ineffectiveness of reporting mechanisms after the exposure took place. Furthermore, the majority of users, who replied to the relevant questions, were not satisfied with the actions that platforms take to minimise risks e.g. when consumers are exposed to scams and other unfair practices online. They mostly consider that platforms are not doing enough to prevent these issues from happening. In general, these users perceive a difference between the official positions of platforms on what they do and what they actually do.

In addition, several concerns arose in relation to the reporting of illegal goods/content/services. For the majority of the users, reporting is not simple both in terms of easiness of finding the procedure for reporting and in terms of easiness of use of the reporting procedure. Moreover, 54% of the respondents are not satisfied with the procedure following the reporting, are not aware of any action taken by the platform as a follow up on their reporting and consider that there is a lack of transparency following a notification.[8] In addition, users point out that the notice and action procedures are very different from one platform to another, making the procedure of reporting illegal content/goods/services even more difficult and uncertain. In this regard, consumer protection authorities have highlighted their struggle with effective enforcement when the sellers are not established in the EU.

[8] Sample size: 898

Figure 8. Satisfaction with Procedure Following the Reporting of Illegal Goods: 1-very dissatisfied to 5-very satisfied



Respondents from all categories consider that during the COVID-19 crisis they have witnessed the dissemination of misleading information on the causes of the outbreak, the treatment, and vaccines. They also point out a general increase in hate speech, price gouging, fake news and political misinformation, in addition to a significant number of illegal goods available online and scams connected to the emergency including phishing, business email compromise, malware distribution, scams, and many other types of attacks, ranging from fake web shops, credit card skimming and illicit pharmacies to ransomware. The general public has particularly praised the fact that the WHO and in general the scientific community had partnered with tech companies to promote accurate information about COVID-19.

Respondents have stated that they use an array of different systems9 for detecting and removing illegal content, which also include, in addition to the notice-and-action systems (18% of respondents, i.e. 65 out of 362), automated systems (12% of respondents, i.e. 45 out of 362), systems for penalising repeated offenders (12% of respondents, i.e. 45 out of 362), and collaborations with the authorities and trusted organizations (11% of respondents, i.e. 40 out of 362). Only 9 out of the 362 respondents (i.e. 2.5%) do not have any system in place for addressing illegal activities conducted by the users of their service such as sale of illegal goods (e.g. a counterfeit product, an unsafe product, prohibited and restricted goods, wildlife and pet trafficking), dissemination of illegal content or illegal provision of services.

Exposure to harmful behaviours and related issues

Respondents from all categories have pointed out several issues in relation to harmful behaviours online, which is considered an opaque term, creating legal uncertainty. With regards to exposure to harmful content, the general public has mentioned the issue of deceptive and misleading ads, also in relation to minors and political advertising.

Publishers, companies that sell products or services online, the general public, as well as digital users' and consumers' associations expressed concerns about the lack of transparency and accountability regarding how targeted advertising and algorithmic systems shape online content. Furthermore, the limited disclosure of ad content and the lack of ad targeting policy enforcement was flagged.

[9] Sample size : 362

Political disinformation is seen as a widespread issue among all categories of stakeholders. Among the measures proposed to tackle this issue, the respondents mention more transparency with regards to political advertising, flagging of disinformation and enhanced data sharing with researchers and digital rights' associations. While respondents are worried about the negative impact of political disinformation and fake news, the view of several digital users' associations as well as of news publishers is that it is important that restrictions to free speech are strictly limited to what is necessary and proportionate.

Among respondents, there is a general consensus that children are not adequately protected online. Respondents make reference to online grooming and bullying, disinformation, possible manipulation through deceptive ads targeting minors, violent content, deceptive paid add-ons on video games, among other issues.

With regards to measures against activities that might be harmful but are not in themselves illegal, the highest share of respondents (17%, i.e. 53 of 314) replied that their terms and conditions and/or terms of service ban activities that are harmful, 16% ban hatred, violence and insults other than illegal hate speech (i.e. 51 of 314) and 14% ban harmful content for children (i.e. 43 of 314), etc.

Opportunities and risks of automated tools for tackling illegal or harmful content/goods/services

The issue of the use of automated tools to automatically detect illegal content, services and goods is considered very controversial among respondents. On the one hand, among content creators and brand owners there is a general support for the use of automated tools, but they also state that hosting services should be subject to transparency requirements and mostly supported by manual/human review. Several respondents pointed to the usefulness of such tools for addressing illegal content at scale, but there is also a strong call for caution in the use of such tools for a series of risks to over-removal of legal content.

Research institutes, associations representing companies selling through platforms and digital rights' associations discourage the use of automated detection and restrictions, pointing out the risks of taking down legal content and that the technology used is still imperfect. In particular, digital rights' associations consider that the risks for fundamental rights such as freedom of expression, discriminatory outcomes, privacy and freedom to conduct business still outweigh possible advantages for countering illegal content or activity online.

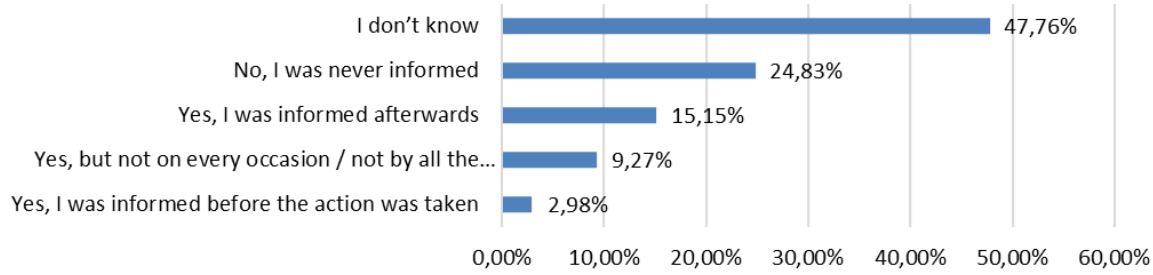
Overall, online intermediaries consider that they should not generally be asked to police and remove content unless a specific report for an individual piece of content is received. Otherwise, online intermediaries will, where they are available, need to rely on automated tools and technologies that may not be fit for purpose or fully developed, resulting in a vast number of false positives and over-blocking. Smaller platforms also point out that automated tools are also very costly to develop and maintain. They state that, while automated tools offer promise for content moderation at scale in the future, it is important to understand that developing, implementing, and iterating effective tools requires significant resources and machine learning capabilities, which may be out of reach for start-ups and scale-ups with ambitions to compete with larger players on the market.

Content amplification and information flows on online platforms

Respondents, in particular among academics and civil society, point however to the particular role of algorithmic systems on online platforms to shape access to online content and play a prominent role in the way platforms' systems are used for reaching very wide audiences with content that might be inciting violence, hate speech or disinformation. Several stakeholders, amongst them citizens, civil rights associations, NGO's, academic institutions as well as media companies and telecommunication operators pointed out the need for algorithmic accountability and transparency audits, especially with regards to how content is prioritized and targeted. In addition, especially in the context of addressing the spread of disinformation online, regulatory oversight and auditing competence over platforms' actions and risk assessments was considered as crucial (76% of all stakeholders responding to the relevant question).

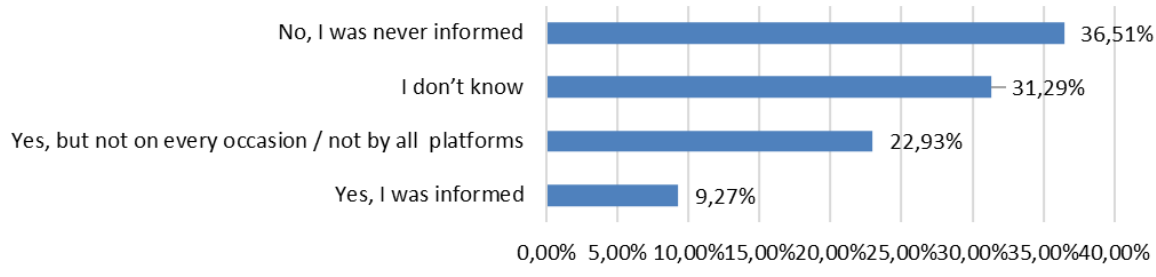
Risks for freedom of expression

Figure 9. Informed by the platform if Content/Goods/ Services were Removed/Blocked



Only 3% of the 1.208 respondents to the relevant question stated that they were informed by the platform before their content/goods/services were removed or access to it disabled. Most of them were not able to follow-up on the information.

Figure 10. Notice provided to a Digital Service asking for the Removal of access to such Content/Goods/ Services, and Informed about Request Follow-Up



In addition, the vast majority of users were not informed after they provided a notice to a digital service asking for the removal or disabling of access to contents/goods/services (only 9% were informed, 23% were informed in some occasions and 37% were not informed at all).

There is a perceived lack of transparency by digital users with regards to what violates the rules of the portal and in particular the "Community Guidelines", with potential risks for freedom of expression.

In order to protect the freedom of expression of their users, several measures that service providers should take have been rated as essential by the majority of respondents, such as: high standards of transparency on their terms of service and removal decisions (84%, i.e. 1700 of 2035 replies), maintaining an effective complaint and redress mechanism (83%, i.e. 1681 of 2030 replies), diligence in assessing the content notified to them for removal or blocking (82%, i.e. 1653 of 2012 replies), high accuracy and diligent control mechanisms, including human oversight, when automated tools are deployed for detecting, removing or demoting content or suspending users' accounts (82%, i.e. 1649 of 2011 replies), diligence in informing users whose content/goods/services was removed or blocked or whose accounts are threatened to be suspended (76%, i.e. 1518 of 2007 replies), and enabling third party insight – e.g. by academics – of main content moderation systems (56%, i.e. 1121 of 1993 replies).

Differentiating across categories of respondents, the only category of stakeholders which do not appear concerned about possible content over-blocking are the creative industry and brand owners, which consider that the percentage of false positives (that is, content which is wrongly identified as illegal) is very low.

Public service media make reference to the need to establish safeguards to prevent platforms from applying additional or secondary control over content published by these independent providers. Similarly, news publishers consider that they should not be subject to any editorial moderation by platforms, as to preserve media pluralism and the freedom of the press. This argument is also supported by trade associations that argue that content published under editorial responsibility should not be removed without a court order.

Respondents from several stakeholders' categories point out the need for platforms to have a clear and transparent redress mechanism. Digital users' associations point out that the users have no way to appeal to anyone independent or neutral and "allowing the platforms to police their own decisions does not seem to work in these situations as there is overwhelming evidence of their bias."

The E-Commerce Directive

There is a very broad convergence towards the continued relevant of the E-Commerce Directive. The respondents point to several issues that could be included in a possible revision of the e-Commerce Directive, with platforms and trade associations emphasising the need to focus the regulatory attention at specific actions and perceived market failures. The three main general issues raised by stakeholders relate to the harmonisation of the notice and action procedures, the clarification of several terms in the Directive and the clarification of the scope of the liability safe harbour:

1. A stronger harmonisation at EU level of the notice and action process and timeframes would contribute to a more rapid response to illegal content online and enhance legal certainty for all stakeholder categories. Such a procedure should be easy to access and use, and it should be defined in EU law in order to overcome the existing divergence among Member States that makes it difficult, especially for small and medium-sized companies to offer their service in the whole single market.
2. Terms which are considered to require a clarification are: taking action 'expeditiously', 'actual knowledge' and 'harmful' content. In particular, platforms

stress the need to clarify and harmonize the definitions of illegal and harmful content among different Member States.

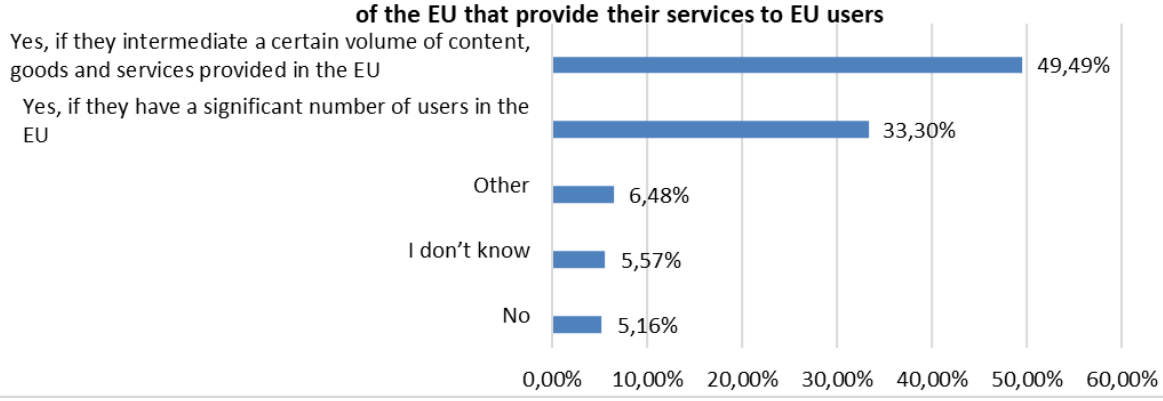
3. Revised definition of passive and active hosts: it is argued that there is a lack of clarity of what type of providers qualify for the liability safe harbour and which degree of 'active' involvement with third party content is required for the liability safe harbour to be no longer available.

Regarding the territorial scope, respondents from all stakeholder categories generally agree with the fact that there is a need for an expansion of the obligations as regards any good/content/service offered to EU consumers, regardless of the place of establishment of the seller or the platforms. Yet, some national authorities clarify that this should be done in accordance with international law, and especially the commitments undertaken at the WTO level. Several stakeholders among telecom operators, digital rights' and consumers' associations as well as representatives of the creative industry and national authorities make reference to a potential requirement for undertakings in third countries to have a legal representative in the EU.

The country of origin principle is often cited by platforms and trade associations as an important principle to ensure legal certainty and provide clarity on the rules that govern the companies. They also consider that full harmonization of rules among Member States would be the best scenario. At the same time, some national authorities have pointed out that the effectiveness of this principle has been limited in practice and it is complex for the authority of the country of destination to intervene if the authority of the country of establishment fails to comply with its obligations. This is considered an important issue to be addressed to avoid forum shopping.

Among the 988 respondents who replied to the relevant question, 83% consider that there is a need to ensure similar supervision of digital services established outside the EU when they provide services to the EU users[10].

Figure 11. Need to ensure similar supervision of digital services established outside of the EU that provide their services to EU users



[10] Sample size: 988

There is a general agreement among respondents that 'harmful content' should not be defined and addressed in the Digital Services Act, as this is a delicate area with severe implications on the protection of free speech. Although respondents are divided on this issue, most of them consider that platforms cannot be trusted to strike, with their internal practices alone, the balance between democratic integrity, pluralism, non-discrimination, freedom of speech and other relevant issues at stake in relation to potential harmful content.

New obligations for online platforms

There is broad consensus among respondents on the need to harmonise at EU level obligations for online platforms to address illegal content they host. Among the most widely supported measures, including by online platforms, are simple, standardised, and transparent notice and action obligations harmonised across the single market. A large majority of stakeholders want all platforms to be transparent about their content policies, support notice and action mechanisms for reporting illegal activities, and request professional users to identify themselves clearly (90%, 85% and 86% respectively). There is a general call, especially among citizens, for establishing more transparency in the content moderation processes and outcomes.

Stakeholders disagree on the information which should be required for reporting illegal activities and information. On one hand, the creative industry considers that it would be, for example, extremely time-consuming to provide all URLs, while large platforms consider that they should be provided with precise information to retrieve the content concerned, including URLs, an explanation of why the content is considered unlawful, related laws that the content violates, and other supporting evidence.

Regarding the removal of illegal content, some research institutions, representatives of the internet tech community, telecom operators and digital rights' associations point out the need to remove the alleged illegal content as close to its source as possible, and to require the intervention of internet infrastructure services only as a last resort option. Some digital rights' associations refer to unduly short timeframes for removing content and compliance target to pose threats to freedom of expression.

Representatives of the creative industry have expressed the need to introduce 'stay down' obligations. In addition, they consider necessary the introduction of 'repeat infringer' policies and clear and fast-track procedures for 'trusted flaggers.'

Yet, such obligation creates significant concerns among digital rights' associations and platforms both in terms of legal uncertainty and risks on privacy and freedom of expression. Such monitoring is also considered a significant barrier for small platforms, which would not be able to develop the necessary capabilities. National authorities are generally against a monitoring requirement, but several of them consider the need to reassess the balance

between rights, obligations and responsibilities of online intermediaries, given the exceptional influence of certain platforms in today's economy. Most of the digital rights' associations are strongly opposed to such measures. Some respondents consider that the 'stay down' obligation should be an exceptional measure, that can only be granted by a court in an injunction that is specific in terms of content and length of the measure, that must abide by the principle of proportionality and that should only apply to content that is identical. Platforms, research institutions and digital rights' associations consider that the issue of reappearing illegal content is delicate and can cause serious threats to freedom of expression as, for example, an 'identical' post may be unlawful if repeated in the same context and lawful in a different context.

Some large platforms also suggest that independent third-party experts can play a key role in addressing the challenge of tackling illegal online content and suggest that, when it comes to the concept of 'trusted flaggers', it is essential to have a clear definition of their roles, obligations and responsibilities. Telecom operators and national authorities also consider the need to strengthen and harmonise the use of reliable notifiers, such as trusted flaggers. Several digital rights' associations appear highly concerned with delegating to platforms the development of human rights and due diligence safeguards, and some of them have put forward detailed governance proposals to tackle this issue.

In response to specific questions concerning online marketplaces, some respondents including consumers' associations, trade associations, national authorities and online sellers flagged the need for further accountability, irrespective of the size of the marketplace. Among the specific requirements suggested, there is the need to verify the sellers ('Know-Your-Business-Customer'), to inform consumers who purchased a fake product; to enforce efficient measures to tackle repeat infringers (blacklisting sellers); to implement a proactive risk management system; to offer a clear set of transparency and reporting obligations; to consult information on recalled and dangerous products on RAPEX; and some also pointed to the implementation of proactive measure to prevent illegal products from reaching the platform's website.

Transparency obligations have been widely suggested by all categories of stakeholders. It is argued that platforms should be clearer about how they address illegal content/goods/services. In particular, it is argued that more transparency is needed regarding the platforms terms of services' violation given that the vast majority of content (96% according to one association) is deleted as a result of violations of these terms. More procedural accountability would enable interventions on content to be more precise and effective. Transparency reports are suggested by all stakeholder groups as a means to respond to the perceived lack of transparency on moderation of content and to create more accountability for platforms.

More transparency is also considered necessary with regards to how content is prioritized and targeted, and several digital rights' associations, research institutions, national authorities, representatives of the creative industry and other companies have pointed out the need for algorithmic accountability and transparency audits. According to several digital rights' associations, these audits would also require the sharing of data for public-interest research by the civil society and academia. Several digital rights' associations also argued that users should have more control over the content they interact with, the use of their personal data by platforms and they should be able to decide not to receive any algorithmically curated content at all. One digital rights' association suggested that the

personalised content recommendation systems should work with an 'opt-in' system rather than the current default 'opt out'. Digital rights' associations also consider that extremely detailed profiling leads to strong personalisation of content, which impacts users' right to freedom of expression and information as well as media pluralism.

On the other hand, while platforms acknowledge the possibility for more transparency, they also warn against possible implications in terms of compromising commercially-sensitive information (including their trade secrets), violations of privacy or data disclosure laws, and abuse from actors that could game their systems.

Regarding online advertising, more transparency is considered necessary on the identity of the advertiser, on how the content is targeted and personalised, and on the actions taken to minimise the diffusion of illegal content/goods/services. Efforts to implement features that explain why certain ads are shown to users, and the creation of ad libraries are considered good practices to build on. Political advertising and micro targeting is considered to raise specific and urgent challenges, including in relation to individuals' autonomy and deliberation. Some respondents flagged that wide-transparency requirements are necessary for these evolving issues, as well as a capability for detecting risk and harms.

A large share of the general public responding to the consultation pointed to deceptive and misleading advertisements as being a major concern in their online experience. Users, academic institutions and civil society organisations are particularly concerned about targeted advertisements to minors and political advertising.

Academic institutions pointed to persistent difficulties when conducting research, and explained the difficulty of observing emerging issues and phenomena online, blaming an inconsistent access to relevant data. Several pointed to the need for a generally disclosed ad archive, as well as an independent auditing of ad systems.

Digital rights' associations consider that users should have the rights to opt out of micro-targeting and that it could be prohibited for advertisers to target users with content based on very sensitive personal data like psychological profiles, political opinions, sexual orientations, or health status.

Regarding minors, digital rights' associations and international organizations suggest to conduct child impact assessments, mitigate risks for minors 'by design', implement age verification systems, and focus on educational programs.

Moreover, whilst there is a strong call for action, many categories of stakeholders, including citizens, online intermediaries, civil society organisations, academic institutions, NGO's and national authorities emphasized that any new measure to tackle illegal content, goods or services online, should not lead to unintentional, unjustified limitations on citizens' freedom of expression or fundamental rights to personal data and privacy.

At the same time, most stakeholder groups acknowledged that not all types of legal obligations should be put on all types of platforms. According to various stakeholder groups, especially business organisations and start-ups, enhanced obligations are especially needed for larger platforms, but these obligations might be disproportionate for smaller ones. Start-ups especially stressed the point that a "one-size-fits-all" approach would be most beneficial for very large platforms, but could have detrimental effects on medium-

sized or smaller platforms and businesses at the core of the European digital ecosystem. They stress that their growth and evolution should not be hindered by disproportionate rules.

Respondents also generally agree that the territorial scope for these obligations should include all players offering goods, content or services, regardless of their place of establishment.

Cooperation with trusted flaggers and authorities

Cooperation with civil society and other third parties such as trusted flaggers is considered an important means for improving the oversight over platforms. Some digital users' associations caution that there should be clear roles and obligations, also to avoid shifting responsibility from platforms to third parties. Some research institutes also caution that there should not be voluntary agreements centred around trusted flaggers as this concept is still not clear and these entities might lack high standards of due process.

Regarding national authorities, several stakeholders acknowledge the need to share data with these authorities for oversight. However, some digital rights' associations, platforms and news publishers caution that law enforcement authorities should not send requests outside the appropriate legal framework involving judicial authorities. The general public is also concerned about mandated sharing of data with the public authorities and ask for platforms to only be mandated to share data based on specific law enforcement requests in accordance with the countries' laws. In general, it is argued that there is a need for transparency on supervisory and enforcement activity of authorities.

There was also a broad convergence among all stakeholder categories around the need to preserve the prohibition of general monitoring obligations for online intermediaries in order to preserve a fair balance and protect fundamental rights, including the right to privacy and freedom of expression.

Proposed changes to the current liability regime

On the topic of the liability of intermediaries, a large majority of stakeholder groups broadly considered the principle of the conditional exemption from liability as a precondition for a fair balance between protecting fundamental rights online and preserving the ability of newcomers to innovate and scale. With regards to consumer protection, some organisations defending consumer rights supported changes to the liability regime in support of a faster resolution of damages for consumers. .

Some intermediaries, national authorities, research institutes and civil society organisations consider that the current regime creates disincentives to act and call for the removal of disincentives for voluntary measures, in order to limit the risks of liability for intermediaries that voluntarily implement preventative measures to detect illegal content. Yet, some digital users' associations, trade associations and representatives of the creative industry warn against such a clause that is expected to weaken the responsibilities of intermediaries without additional positive obligations.

In particular representatives of smaller service providers, but also some civil society organizations pointed to legal uncertainty and disincentives for service providers to act against illegal goods, services or content disseminated through their service. Start-ups strongly called for a legislative framework that reaffirms the principles of the e-Commerce

Directive, while supporting the introduction of a clarification of the liability regime with regards to voluntary measures they might take.

The distinction between passive and active players is considered to be still relevant and valid by some respondents (mainly telecom operators), whereas some other respondents from different stakeholder categories consider the need to move towards the use of other concepts, such as the degree of control over the content and a well-defined concept of actual knowledge. Telecom operators nevertheless also consider that there should be a clarification on the definition and responsibilities of active and passive hosts, following the recent jurisprudence of the CJEU. In addition, they consider that the regulatory focus should be directed to those hosting services that play an 'active' role. Some large platforms argue that a strict interpretation of what 'passive' hosts are would discourage online intermediaries from exploring innovative and personalised user experience, in addition to deterring them from taking voluntary proactive steps to identify and remove unlawful content.

Cloud services call for the creation of a new category of 'cloud infrastructure services' to be established and to get proper safe harbour protections. Search engines argue that they clearly fall under the category of caching services. Some intermediaries and representatives of the creative industry also consider the possibility to create a fourth category of 'online platforms' that would allow to distinguish between providers which have no editorial control over the content and those that use algorithms to display content to their users. Other information society services argue that DNS services should be explicitly covered as intermediaries.

Except for the creative industry, all categories of stakeholders consider it important to limit the responsibility of host providers, content distribution services, cloud infrastructure, DNS services and other intermediaries to prevent IP infringement, including piracy and counterfeiting.

Governance in the single market and supervision of digital services

There is a broad alignment from all categories of stakeholders that the internal market principle enshrined in the E-Commerce Directive is crucial for the development of innovative services in the Union and should be preserved.

With regard to the burdens for companies in the single market, business associations and medium-sized companies in particular pointed out that the legal fragmentation around rules for tackling illegal content, goods and services, is limiting most businesses, but especially SMEs and start-ups, from scaling up. More specifically, business associations pointed out that SMEs and start-ups are facing a competitive disadvantage, since they are affected in a disproportionate manner as opposed to larger companies. Start-ups and SME's confirmed this observation, by pointing to the business risks of having to adapt their services to potentially 27 different sets of rules, which does not just inhibit their growth across the Union, but also globally.

At the same time, besides the need to address the refragmentation of rules, there is also a general understanding among stakeholders that cooperation between authorities should be improved in the cross-border supervision of digital services, and in particular online platforms. 66% of the respondents to the relevant question in the open public consultation noted that a unified oversight entity for EU oversight is very important. Many stakeholder

groups, but especially business associations and companies, considered, that the degree of oversight should vary depending on the services' obligations and related risks.

Authorities and other respondents, in particular academic institutions as well as civil society organizations point out the fact that the supervision of such cross-border services comes with specific challenges in terms of accessing appropriate data, as well as capability in terms of adequate financial and human resources in competent authorities tasked with supervision of online platforms. Many groups of stakeholders, especially digital rights associations, identified the need for interdisciplinary skills in the oversight entity, particularly in-depth technical skills, including data processing and auditing capacities, which would allow for the reliable and thorough assessment of algorithmic abuses.

While some authorities consider that the quality of the cooperation is good and reference to the Consumer Protection Cooperation (CPC), the European Regulators Group for Audiovisual Media Services (ERGA) and Body of European Regulators for Electronic Communications (BEREC) as good example of well-functioning cooperation, other authorities consider that the quality of their cooperation could be significantly improved.

Content creators and right holders are concerned with the fact that, while copyright is largely harmonised across the EU, there is no system in place for national authorities to cooperate on the enforcement of those rights.

Regarding the future governance structure, it is generally argued that EU cooperation is crucial and different suggestions of hybrid enforcement mechanisms with different elements of centralised and decentralised structures have been presented by the respondents. The majority of respondents, however, appears to favour a unified oversight entity, which would collaborate with national authorities. Some respondents have also pointed out the need to increase cooperation with international entities.

Some representatives from digital rights' and consumers' associations, trade associations, platforms and the creative industry consider that the oversight or the direct enforcement mechanisms could be better left in the hand of authorities operating at the national level, but overseen or coordinated by a central authority at the EU level. Some national authorities in the media sector in particular consider that online content regulation could go under the umbrella of the media regulator to endure consistency in the application of regulatory principles and to increase efficiency. While the internal market principle is often mentioned by respondents as a crucial pillar of the liability regime, some national authorities consider that the country of destination should be given greater capacity to intervene to discipline platforms who do not comply with the regulations, especially when the platform is established in one country but directs its content exclusively to other countries. Yet, this issue is controversial among national authorities.

The respondents show clear concerns about the lack of adequate financial and human resources and make often reference to the need to cooperate with civil society organisations and academics for specific inquiries and oversight. The stakeholders identify the need for interdisciplinary skills in the competent authority. These skills should include economics, law, sociology, media studies, computer science and data analysis. Particular interest is given especially to technical skills, which would allow to read and interpret algorithms' source codes and assess if abuses occur such as self-preferencing, divergent treatment of equivalent content, intended or unintended failure with content recognition systems, etc.

Some stakeholders also mention the need for the personnel in the competent authority to have some past experiences in the private sector, ideally in digital platforms or at least the digital ecosystem.

2.2. Open Public Consultation on measures to further improve the effectiveness of the fight against illegal content online[11] (30 April – 25 June 2018)

The Commission also consulted on some of these issues over the past few years through several other open public consultations. The most recent, was launched on the 30th April 2018 and ran for 8 weeks, with a total of.8,961 replies, of which 8,749 were submitted by individuals, 172 by organisations, 10 by public administrations, and 30 by other categories of respondents.

Overview of the replies:

Hosting services

Overall, hosting services did not consider that additional regulatory intervention would be conducive to better tackling illegal content online, but supported, to a certain degree, voluntary measures and cooperation.

Associations representing large numbers of HSPs considered that, if legal instruments were to be envisaged at EU level, they should in any case be problem-specific and targeted. They broadly supported further harmonisation of notification information, but expressed substantial concerns as to the feasibility of establishing strict time limits on takedown of content (from upload), pointing to burdensome processes especially for SMEs, and to general incentives of over-removal. They also pointed to the need to have a cautious approach concerning proactive measures, highlighting the general cooperation and good results in the actions taken through the sector specific voluntary dialogues.

Contributions from different companies highlighted the differences in available capabilities across businesses, as well as the different incentives and technical possibilities depending on their value propositions. Companies were also generally open to cooperation including with government agencies or law enforcement when it comes to flagging illegal content.

While big companies reported using, besides notice and action systems, proactive measures, including content moderation by staff, automated filters and, in some cases other automatic tools to flag potentially illegal content to human reviewers, responses also showed that smaller companies are more limited in terms of capability. Amongst the respondents, it seemed that SMEs were generally relying on notices for flagging all types of illegal content. One SME described difficulties in implementing semi-automated tools – without having access to the tools developed by the big industry players – and the trade-off experienced between increasing performance in removing illegal content, and the higher incidents of erroneous removal of legitimate content of their users.

Competent authorities, including law enforcement authorities, internet referral units, ministries or consumer protection authorities:

The main concerns expressed by those public authorities who responded were about illegal commercial practices (three respondents), child sexual abuse (two respondents) and copyright (two respondents).

[11] https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal

Six respondents declared to identify and refer illegal contents to hosting service providers. Illegal content was mainly detected through trusted flaggers or by means of direct reporting by the right holders. For instance, one public authority declared that under national law, in case of infringement of copyright, the only party entitled to report the violation of such right is the right holder, whose right has been infringed. Automated tools are generally not used by the public authorities responding to the consultation.

Public authorities outlined the increasing difficulty to judge which content is harmful or illegal and which is not. Other public authorities reported their difficulty to identify the sources of the illegal content online and therefore the lack of evidence for any related judicial action. The turnaround time for removing illegal contents is considered as a critical point as well.

Some respondents required a clear and precise legislation which would take into account the different actors that operate in the EU, whereas others emphasised the importance of having strong and effective cross-border cooperation between the national regulatory authorities.

Trusted flaggers, notifiers with a privileged status and organisations representing victims

Amongst the respondents, 26 were mainly concerned with copyright infringements, five with child sexual abuse material and three with illegal commercial practices online.

Concerning the tools used to detect copyright infringements, 22 reported to use content monitoring and report by their own staff, whereas 18 declared to use automated tools. In such respect, more than half of the respondents reported that both public and private investments in research and development would be necessary to uptake and deploy automated tools for the removal of illegal contents online.

Some respondents warned as to the challenges in using automated tools and claimed that any technological system put in place to intercept content must be able to recognize new material quickly and accurately to account for changes. To ensure such result, human assessment had to be included in the decision-making process.

Furthermore, the not-for-profit organisations considered the standardised access and user-friendly interfaces for reporting illegal content to be very effective in order to enable HSPs to make diligent decisions. Conversely, the explanation of reasons and grounds of illegal content and anonymous notices were reported as being inefficient for some types of illegal content such as IPR infringements.

Amid the respondents, 21 declared the setting of time limits for processing referrals and notifications from trusted flaggers as important in supporting cooperation between HSPs and trusted flaggers.

Civil society organisations representing civil rights interests:

Despite having issues with the current framework, especially in terms of transparency of the processes for removing illegal content or contesting a removal, civil society organisations representing civil rights interests expressed concerns about the impact proactive measures or new legislative measures may have on freedom of expression and information. In this context, they were concerned that decisions by platforms about controversial content according to their terms of service in a non-transparent way may impact the rule of law and ultimately endanger freedom of expression.

Respondents agreed with reinforcing public authorities' capabilities in fighting illegal content online and were not particularly in favour of attaching privileges to trusted flaggers

or imposing an obligation on platforms to report all alleged illegal content to law enforcement bodies. Like respondents in other groups, they were not keen on out-of-court dispute resolution procedures either.

Several civil society organisations (and some respondents from other groups as well) considered that the focus should be put on searching and prosecuting providers of illegal content rather than on removing illegal content as this might have a negative impact on users' rights, whilst they also acknowledged that reaching and prosecuting the perpetrators is not always possible.

IP rights holders

Intellectual rights owners and their associations surfaced via different respondent groups in the public consultation. They include publishers, film and music labels, media and sports companies, as well as trademark owners.

In their view, the voluntary approach is rather ineffective and it puts companies doing more than required by law at a competitive disadvantage. Brand owners noted that counterfeiting does not only damage industry rights but consumer safety as fake products are often produced without complying with security standards. They criticized the enforcement of transparency obligations in Directive 2000/31/CE and considered that the "follow the money" approach has been difficult to implement. They claimed for a system of shared enhanced responsibilities for intermediaries supported by a stronger legal framework. Establishing "stay-down" obligations features in individual submissions too. Companies holding rights in sports events contended that platforms should enable them to take down content in real time.

Other industry associations

This group includes 76 replies from IT companies' associations, other industry associations and other stakeholders such as the Council of Europe, one political party, civil rights advocates and Intellectual Property (IP) right holders.

Respondents reported low levels of feedback from platforms on notices to take down content. When content was removed, it was mainly done within days. One respondent noted that it is easier to report user generated content such as hate speech comments than false advertisements.

Although the majority of respondents saw a need for some level of EU action, many industry associations advised against complex regulations. In this regard, some of them highlighted that policies oriented along capabilities of large corporations create barriers to market entry and innovation. Prominent IT companies' associations underlined that the variety of policies and voluntary schemes in place should be given time to prove their results and be properly assessed before legislating. In their view, self-regulation and public-private cooperation should in any event be stepping-stones towards ensuring illegal content online is kept at bay. One respondent was however favourable to tackling terrorist content by legislating.

With the caveat of costs for small businesses, they are supportive of proactive detection tools counterbalanced by safeguards like transparency and the "human-in-the-loop" principles. They also agreed with the need for arrangements to prevent illegal content from spreading, but preferred best practice, voluntary sharing of databases or software tools to ensure the deployment of automated tools across HSPs. They were also in favour of

standardising notice and action procedures, with a relevant industry association opposing this view.

Research or academic organisations:

Like other groups, respondents considered that different kinds of illegal content needed different frameworks. As regards the notice and action procedure, one respondent noted that outside Europe the take-down mechanism is unclear and sometimes non-existent.

They pointed to the lack of real incentives (despite sporadic media attention) for companies to deal with counter-notices, whereas non-treatment of notices can more easily lead to legal consequences. They also underlined that existing counter-notice procedures are by and large underused, with the few companies who do report on counter-notices listing on a yearly basis only one-to-two digits numbers.[12]

They were particularly concerned about the use of automated tools in detecting illegal content online and advised caution when incentivising hosting services to apply proactive measures, and underlined the need for human rights safeguards and transparency to the process of detecting and removing alleged illegal content online.

They side with some other respondents in giving priority to public authorities' notices over trusted flaggers' ones; preferring public investments in research and development and in favouring publicly supported databases for filtering content, training data or technical tools.

Individuals

Is the internet safe?

- Over 75% of individuals[13] responding considered that the Internet is safe for its users, and 70% reported never to have been a victim of any illegal activity online. In cases, where respondents were victims, this concerned, for nearly 12%, some form of allegedly illegal commercial practice.

Measures to take down illegal content

- Regarding notice and action procedures: 33% of the individual respondents reported to have seen allegedly illegal content and have reported it to the hosting service; over 83% of them found the procedure easy to follow.
- The overwhelming majority of respondents to the open public consultation said it was important to protect free speech online (90% strongly agreed), and nearly 18% thought it important to take further measures against the spread of illegal content online. 70% of the respondents were generally opposed to additional measures.

Over-removal

- 30% of the respondents whose content was wrongfully removed (self-reported) had issued a counter-notice.
- 64% of the respondents whose content was removed found both the content removal process, and the process to dispute removal as lacking in transparency.

Transparency and information

[12] ICF study (forthcoming). Comparative analysis of transparency reports of several companies points to negligible numbers of counter-notices per year.

[13] Out of 8.749 responses from individuals

- Nearly half of the individuals who had flagged a piece of content did not receive any information from the service regarding the notice, while one third reported to have been informed about the follow-up given to the notice. For one fifth, the content was taken down within hours.
- One fifth[14] of the respondents who had their content removed from hosting services reported not to have been informed about the grounds for removal at all.

Need for action & options

- 30% of respondents considered that the current legal framework for tackling each of the different types of illegal content was effective. Nearly 40% found that actions currently taken by HSPs are effective.
- Nearly half of the respondents considered that hosting services should remove immediately content notified by law enforcement authorities, whereas 25% opposed such fast processing.
- Half of the respondents opposed fast removal for content flagged by organisations with expertise (trusted flaggers), other than law enforcement, but 25% agreed with such fast procedures.

2.3. Open Public Consultation on "Regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy" (September 2015-January 2016)

This consultation received 1,034 replies, although one of them (an advocacy association) included 10,599 individual contributions.[15] Its results, as far as the liability of intermediary service providers is concerned, can be summarized as follows:

- The majority of respondents think that the existing liability regime in the ECD is fit-for-purpose.
- The majority of respondents demanded either clarification of existing or the introduction of new safe harbours. The most often discussed safe harbour was hosting (Article 14), in particular its concept of "passive hosting". When asked specifically about this concept, many respondents complained rather about the national interpretations of this concept. Several respondents supported clarification by means of soft-law measures such as recommendations issued by the European Commission.
- 71% of respondents consider that different categories of illegal content require different policy approaches as regards notice-and-action procedures, and in particular different requirements as regards the content of the notice.
- 61% of online intermediaries state that they have put in place diverse voluntary or proactive measures to remove certain categories of illegal content from their system.

[14] 450 out of nearly 2,000

[15] https://ec.europa.eu/digital-single-market/en/news/full-report-results-public-consultation-regulatory-environment-platforms-online-

- 61% of the respondents are against a stay down obligation.
- 77% of the respondents are in favour of increasing transparency with regard to the duties of care for online intermediaries, with regard to the general content restrictions policies and practices by online intermediaries.
- 82% of the respondents are in favour of a counter-notice procedure.
- Views were particularly divided over (i) the clarity of the concept of a 'mere technical, automatic and passive nature' of information transmission by information society service providers, (ii) the need to clarify the existing categories of intermediary services (namely mere conduit/caching/hosting) and/or the potential need to establish further categories of intermediary services, (iii) the need to impose a specific duty of care regime for certain categories of illegal content.

2.4. Open Public Consultation on notice-and-action procedures (2012)

The public consultation revealed broad support for EU action (among all categories of respondents). More specifically it revealed strong support for clarification on certain notions of the ECD, for rules to avoid unjustified actions against legal content (in particular consultation of the content-provider and counter-notification by the content provider), for requirements for notices and for feedback to notifiers.

However, respondents appeared to be divided on the final instrument of the initiative.

- 48% considered that if an HSP takes proactive measures it should be protected against liability that could result ("Good Samaritan clause").
- 53% affirmed that action against illegal content is often ineffective and lacks transparency.
- 55% considered that concepts of "hosting", "actual knowledge" and "awareness" are unclear.
- 64% considered that HSPs often take action against legal content.
- 66% considered that a notice should be provided by electronic means.
- 71% considered that HSPs have to consult the content providers first.
- For 72% of the respondents, different categories of illegal content require different policy approaches.
- 77% considered that the sender of the notice should be identified.
- 80% considered that there should be rules to avoid unjustified or abusive notices.
- 83% considered that the notice should describe the alleged illegal nature of the content.

2.5. Open Public Consultation on the E-Commerce Directive[16] (2010)

Full report available at http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf.

3. Other, targeted consultations and engagement activities

3.1. Bilateral meetings and contributions

In the course of the preparation of this Impact assessment, the Commission has had bilateral meetings and/or has received position papers from the following stakeholders:

1. "Challenger" (Dropbox, Spotify, Snap, Cloudflare, Mozilla, Etsy, TransferWise and Stripe)
2. 13 organisations including Amnesty, FIDH, EFJ
3. AAFA - TRACIT
4. ACCC Australian Competition and Consumer Commission
5. Access Now
6. ADIGITAL
7. Advisory Council for Consumer Affairs (SVRV - Sachverständigen Rat für Verbraucherfragen)
8. AER – Commercial Radios
9. AFEP - Association française des entreprises privées
10. Ah Top
11. AIG Advertising Information Group
12. AIM
13. AirBnB
14. AK Europa
15. Algorithm Watch
16. Alibaba
17. Allegro
18. Alliance for Safety Online Pharmacy
19. Allied for Startups
20. Amazon
21. AmCham
22. Amway
23. APC - Association for Progressive Communications
24. Apple
25. ARD - ZDF
26. Article 19
27. Article 29
28. Association of Charity Lotteries
90. EURACTIV
91. Eurocities
92. Eurocommerce
93. Eurogroup for animals
94. Federation of veterinarians of Europe
95. EuroISPA
96. European Partnership for Democracy (EPD)
97. European Public Health Alliance (EPHA)
98. European Publishers Council EPC
99. European Tech Alliance (EUTA)
100. Expedia
101. Facebook
102. Fédération française des télécoms
103. FiCom ITAS
104. FID – Forum for Information and Democracy
105. Finnish Commerce Federation
106. FreeNow (former My Taxi)
107. FTI Consulting
108. Gant - Lacoste
109. German Association for the Digital Economy (BVDW)
110. GESAC
111. Google
112. Homo Digitalis
113. Human Rights Monitoring Institute (HRMI)
114. IAB Europe
115. IBM
116. ICANN Internet Corporation for Assigned Names and Numbers
117. IFPI
118. IKEA

[16] http://ec.europa.eu/internal_market/consultations/docs/2010/e-commerce/summary_report_en.pdf

29. Association of the internet industry (ECO)
30. Avaaz
31. BASCAP
32. BDKV Bundesverband der Konzert- und Veranstaltungswirtschaft e.V.
33. Beat
34. BEUC
35. Bitkom
36. Bolt
37. Business Europe
38. Cabify
39. Calibermedia
40. CCIA
41. CDiscount
42. Center for Democracy & Technology
43. Center for Democracy & Technology
44. CENTR
45. Chanel
46. CISPE/Europa Insights
47. Civil Liberties Union for Europe (Liberties)
48. Civil Rights Defenders
49. Clever
50. Cloudflare
51. Confederation of CZ industry
52. Considerati
53. Copyright Stakeholders
54. Counter Extremism Project
55. Cyfrowa Polska
56. Dangerous speech . org
57. Danish Enterpreneurs
58. Danish Entrepreneurship Association (DINL)
59. DSA 4 Start-Ups
60. Dansk Ehverv
61. Deliveroo
62. Democracy Reporting International
63. Deutsche Startups
64. Developers Alliance
65. Digital Action
66. Digital Europe
67. Digital Rights Ireland
68. Digitale Gesellschaft
69. Direct Sellers Ass
70. DNS Belgium
71. Dropbox
72. EASA - European Advertising Standards Alliance
119. Incopro
120. INTA trademark association
121. Internet Watch Foundation
122. IOGT-NTO
123. IT & Telekomföretagen
124. ITI – The Information Technology Industry Council
125. IVSZ szövetség a digitalis gazdasagert
126. Julian Jaursch, SNV
127. Justitia
128. Kapten
129. Liberty Global
130. LVMH
131. Match group
132. Meetingselect
133. Motion Picture Association
134. Mozilla Foundation
135. MPA Motion Picture Association
136. Netflix
137. News Media Europe (NME)
138. Nielsen
139. Nike
140. NL Digital
141. OLX
142. Online marketplaces
143. Orange
144. OSEPI-BEUC
145. Panoptykon
146. PGEU online pharmacies
147. Pinterest
148. Polish Confederation Lewiatan
149. PubAffairs
150. QVC/Freshfields
151. Rakuten
152. Renaissance numérique
153. Reporters Sans Frontières
154. RIPE - Regional Internet Registries
155. Schibsted Media group
156. Sky
157. Skyscanner
158. Slack
159. Snap inc
160. Spotify
161. Startup Amsterdam
162. Svensk Handel
163. TechLeapNL
164. Telefónica

73. EBU
74. ECCIA - European Cultural and Creative Industries Alliance
75. Ecosia
76. Edima
77. eDreams ODIGEO
78. EDRi
79. EHHA - European Holiday Home Association
80. EGTA
81. Electronic Frontier Foundation (EFF)
82. eMag
83. EMMA-ENPA - European Magazine Media Association/European Newspaper Publishers' Association
84. Epicenter.works
85. ETNO-GSMA
86. Etsy
87. ETUC - European Trade Union Confederation
88. EU Travel Tech
89. GARM – Global Alliance for Responsible Media
165. The Digital New Deal Foundation
166. The Marketplace Coalition
167. The Peace Institute
168. TIE Toy Industries of Europe
169. TripAdvisor
170. Twitch
171. Twitter
172. Uber
173. UK Trust
174. UK Business Consumer Coordination group
175. Verbraucherzentrale Bundesverband
176. Verisign
177. Virke
178. Vivendi Group-Canal+ group
179. VNG NL
180. Vodafone
181. Walmart
182. Welfare in Pet Trade
183. Wikimedia
184. World Federation of Advertisers
185. YouTube
186. Zalando
187. ZN consulting

3.2. Targeted consultations and feedbacks

The Commission has been consulting stakeholders during the last years and working towards specific due diligence measures, such as notice-and-action procedures, since 2012. These works informed the adoption of the 2017 Communication on tackling illegal content online[1] and the 2018 Recommendation on measures to tackle illegal content online[2]. A detailed reference to past events and consultations[3] (until mid-2018) can be found in the Impact Assessment accompanying the document Proposal for a Regulation on preventing the dissemination of terrorist content online[4].

3.2.1. Feedback to the targeted survey for the Member States, 3 September 2020

During the summer 2020, the European Commission asked Member States to share their experiences on the overall functioning of the ECD. Altogether, 21 replies from 17 Member States (in one Member State 5 authorities replied) were received.

Although the survey mainly focused on the Member States' experiences with the **provision covered by Article 3** ECD – replies to this part are granularly described in Annex 7 and 14; the Commission also inquired about Member States' experiences with other parts of the Directive, as well as about challenges and opportunities recognised on the Member States' level.

Regarding Member States' experiences with **information requirements** provided by the ECD (Art. 5 – 8), nine respondents reported that service providers are fully or mostly compliant with duties encoded in Art. 5 and 6, while three respondents explained that particular types of service providers (social media, web stores, marketplaces and third party sellers) usually or often do not comply with these provisions. One Member State reported that service providers are compliant only with Art. 5. One Member State noted that new ways for B2C communication with consumers might be reflected in the new framework (chat windows, direct messaging).

In their replies to questions covering **conclusion of contracts by electronic means** (Art. 9 - 11), six Member States were of the opinion that these provisions might be generally simplified and modernised, e.g. by codification of electronic signature, introduction of technological neutrality, omitting exceptions in Art. 9(2) that are not relevant any more,

[1] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

[2] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[3] In particular: Feedback of Member States on the application of Recommendation on measures to effectively tackle illegal content online C(2018) 1177 final, of 1st March 2018; E-Commerce Expert Group meeting held on the 14th June 2018; Feedback on the Inception Impact Assessment 76 (2nd to 30th March 2018); Meeting with trusted flaggers on the 7th February 2018; High level meeting with online platforms held on the 9th January 2018; Semi-structured interviews with judges across the EU; Workshop on Digital Platforms and Fundamental Rights, held on 12 June 2017; Workshop on notice and action in practice, held on 31 May 2017; E-Commerce Expert Group meeting on notice and action procedures, held on the 27th April 2017; Workshop with intermediary service providers on voluntary measures, held on 6th April 2017.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN

alignment with relevant consumer acquis or by introduction of smart contacts in the new framework; one respondent noted though that lack of adaptation on national level in this regard might be an issue. Three Member States reported that the respective provisions still serve well their purpose. One Member State expressed an opinion that harmonisation of international private law regarding these provisions is important to smoothen cross-border sales.

In replies to the questions concerning **liability provisions** (Art. 12 - 15), Member States positions covered several aspects. Two Member States reported that possibility to issue third countries notifications should be included in the new regulation. One Member State informed about use of point of contact in cooperation with service provider outside of its territory to report illegal content; one Member State reported that it does not issue removal requests to service providers established outside of its territory. One Member State explained that it uses a dedicated notice and action procedure and two Member States issue injunctions within their territory; one Member State reported it has no experience with injunctions. Two Member States further reported that they miss the statutory basis to issue injunctions. Two Member States reported that voluntary cooperation with service providers works in practice; another Member State reported in this regard that it has bad experience with administrative cooperation and subsequent content removal. One Member State called for clarification of the term "active" hosting, responsibilities of such service providers and for introduction of a duty to reply to any notices received. One Member State was of the opinion that alternative or online dispute resolution mechanisms are not appropriate for illegal content. Two Member States reported that cooperation with dedicated authorities, e.g. CERT (Computer Emergency Response Team), to signal illegal content, works well. One Member State expressed an opinion that non-compliance with legislation concerning notice and action procedure might be strictly prosecuted.

Regarding Member States experiences with **codes of conduct** (Art. 16) relevant for complying with the obligations laid down in the ECD, most of the respondents explained that they have not encouraged or developed such a practice. Three replies reported existence of dedicated codes for areas covered by Art. 5 – 8 to help deal with particular issues related to consumer protection online. Two Member States issued guidelines to help companies implement the Directive, while one of them ceased the scheme three years after introduction. One respondent explained that a dedicated cooperation was introduced in the past to tackle particular types of content online.

As far as it concern **out-of-court dispute settlements** (Art. 17 and 2018 Recommendation), majority of Member States replied that no dedicated procedures have been introduced or used, although five Member States clarified that ADR and ODR mechanisms works well for consumer protection issues and complement each other appropriately. Two Member States noted in this regard that the implementation of the AVMS Directive might introduce such a scheme for dedicated types of service providers. One Member State is preparing an update of sectoral legislation that might improve out-of-court dispute settlement via dedicated procedure.

Three Member States reported on the experience with **contact points** (Art. 19(4)) that they provide information and advice to both consumers and service providers; one of them further added that contact point also cooperates with LEAs, NRAs, NGOs and consumer centres. Two respondents explained that most of the queries raised to the contact point concern consumer related issues; one Member State noted that very little queries are being posed to the contact point. One Member State replied that manifestly illegal content is

handled via CERTs and that the procedure has proven to be efficient in the take down of content. A Member State also runs a dedicated website to notify illegal content.

Member States did not share information about **significant administrative or judicial decisions** taken in their territory (Art. 19(5)) in the past five years; only one Member States provided information on relevant court decisions.

Concerning future **challenges and opportunities**, seven Member States perceived applicability of the new regulation to the third countries providers as important, while two Member States raised that the EU regulation should remain friendly to third countries. Five Member States explained that they see the lack of digital skills as one of the main challenges. Four Member States reported that they feel that internal market principles are endangered, also due to fragmentation of rules and lack of cooperation among Member States; one Member State explained in this regard that European body might solve insufficient cooperation among Member States. Compatibility with other relevant EU laws and importance of clear rules for companies, consumers and authorities was underlined as well. Three Member States explained that they perceive favourable conditions, including sufficient financial resources for SMEs as crucial element for continuous development of digital single market. One Member State reported enforcement and one access to public data as one of the biggest challenge.

3.2.2. Feedback to the Inception Impact Assessment on the 'Digital Services Act - deepening the internal market and clarifying responsibilities for digital services'[5], 2 June 2020

A total of 110 contributions were submitted. The replies present broadly the whole stakeholder spectrum: online intermediaries, associations of businesses and trade organizations, telecom operators, startups, civil society, citizens and users of digital services, national authorities and academia. In this report, the common comments on the most mentioned topics are identified.

In general, it can be concluded that stakeholders are aligned on the common threat of the IIA. The focus of different stakeholder groups is however divergent; different stakeholder groups put more emphasis or importance on different topics. Generally, all stakeholders however agree that a horizontal harmonization for digital services in the EU is necessary and welcome.

As to the **scope** of the future legislative proposal, most online intermediaries, telecommunication operators, retail and media/audio-visual business associations and civil society organisations are in favour of including the services of third countries into the scope of the upcoming rules. Most start-ups, citizens, academia and national authorities did not say anything specific about the probable future scope of the DSA.

In general, online intermediaries, telecommunication operators, start-ups and national authorities are strong supporters of the **Internal Market principle**. Furthermore, none of the other stakeholder groups are against the principle either. Consumer organisations advocate for preserving the consumer contracts derogation of the ECD and national authorities call for additional deviation areas to be assessed.

[5] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services

Most stakeholders have shared views on **liability**. Especially online intermediaries and telecommunication operators are overwhelmingly supportive of maintaining the current liability exemption as defined in the ECD. Also most associations of businesses and trade organizations are in favour of maintaining the regime of the ECD. Consumer organizations strongly call for a special liability regime for online market places to make them directly or jointly liable in case they exercise a predominant influence over third parties or in case the platform fails to properly inform consumers or fails to remove illegal goods or misleading information. Most stakeholders also ask for clarification on the liability rules and are in favor of duty of care obligations and responsibilities for online intermediaries. Online intermediaries themselves stipulate that every party in the online ecosystems should hold some portion of responsibility. Very divergent views between all stakeholders exist on the question of whether a Good Samaritan clause should be introduced or not, and about the current distinction between 'active' and 'passive' digital services.

Especially online intermediaries, associations of businesses and trade organisations, civil society organisations and some academia emphasize the need for **harmonised notice and action procedures** across the EU. Most of them also call for the establishment of minimum information requirements that a notice should contain and touched upon the 'knowledge requirement' of the ECD, often asking for it to be clarified.

Online intermediaries, telecommunication operators, start-ups and civil society organisations are strong supporters of maintaining the **general monitoring prohibition**. Whereas civil society and online intermediaries largely consider the protection of fundamental rights the main argument for keeping the general monitoring prohibition, start-ups emphasized that freedom of speech is not their only reason, as general monitoring would simply be impossible for most start-ups to carry out. Apart from one civil society organisation, none of the other stakeholders indicated that the general monitoring prohibition should be cut out in the DSA.

Most stakeholders did not share particular views on the distinction between or definitions of **illegal and harmful content**. The majority of the online intermediaries however believe that the DSA should solely focus on illegal content and that harmful content should not be included in the DSA. In all other stakeholder groups, some respondents shared a similar view, and some respondents did not say anything about it. No contributions have strongly called for harmful content to be defined in the DSA.

In general, most stakeholders recognize the problem of the lack of **transparency** and call for increased transparency. Especially civil society organisations identified the lack of transparency as one of the major problems and call for more transparency obligations. Most stakeholders that touched upon the issue of transparency are in favour of reporting obligations. Online intermediaries furthermore specified the possible risks of far reaching obligations, such as infringements upon trade secrets or intellectual property rights. Some of the telecom operators, associations of businesses, civil society organisations and academia particularly highlighted the need for more transparency in automated and algorithmic systems.

Associations of businesses and trade organisations are the firm supporters of introducing **KYC obligations** on online intermediaries. Online intermediaries themselves also agree that such requirements could be useful, but emphasize that they should be proportionate, privacy-friendly and supported by the right infrastructure in order to be scalable. Most contributions of other stakeholder groups did not particularly specify whether to be in favour or against introducing KYC obligations in the DSA.

Particularly online intermediaries, civil society organisations, academia and national authorities emphasized the need for **fundamental rights** safeguards and shared their views on this. The freedom of receiving information, the freedom of expression and the freedom to conduct a business are mostly mentioned by online intermediaries, whereas civil society organisations put most importance on the preservation of the freedom of expression, freedom to receive information, right to fair trial and right to adequate remedy. Civil society organizations and academia are particularly worried that automated tools might not guarantee the protection of fundamental rights due to illegitimate takedowns.

The vast majority of stakeholders did not share specific views on **online advertising**, and the ones that did so touched upon divergent issues about it.

Most stakeholders emphasize the need of strong **enforcement** and **regulatory oversight** to hold platforms to their promises. Online intermediaries highlight that any regulatory oversight mechanism should be proportionate, increase legal certainty and should be based on the Internal Market principle. National authorities, telecommunication operators and civil society organisations specifically indicate that better cooperation between Member States is essential. Not many stakeholders clarified how this regulatory oversight should be in practice and did not touch upon the question whether a new EU body/agency should be established, but some of them think this would be a good solution.

3.3. Workshops, events and Expert Group meetings

3.3.1. Workshop on online violence against women, 8 September 2020

In September 2020, DG JUST in cooperation with DG CNECT organised an online workshop with a panel of six academics as well as representatives from the Commission to discuss the issue of violence against women in the online environment. Academics agreed that Digital Services Act could be an opportunity to overcome the existing fragmentation, and agree on more common definition/standards. An opinion resonated among the academics that parts of the Digital Services Act package should be perceived as complementary to tackling the issue together with supplementing sectoral initiatives. As the problem is structural, the solution should be based on complex market approach, so the users can switch to other platform that provides for different moderation may it be their wish. Some academics further concluded that an amplification element is important to distinguish harmful content and illegality, and that the horizontal solutions included in the Digital Services Act should cover all users in vulnerable situations, including women users, users with minority backgrounds and children. They also reported that the decision between the self- and co-regulatory approach on one side and "hard" regulation on the other should not be taken. At the same time, they acknowledged that here are clear positives and negatives of self- and co-regulatory approach, and its success depends a lot on the Member States' as well on platforms' approach. In this regard, an agreement was reached that scope for existing authorities to develop their role concerning privacy and different forms of online violence might be created by the new regulation. The academics also summarised that there is a need to adapt obligations according to the layers of the internet, as well as to ensure redress and support to individuals when considering illegal acts according to the existing rules.

3.3.2. Seminar on the Future of Liability of Platforms under the EU's Digital Services Act: An Academic Perspective, 31st July 2020

On 31st of July, Martin Husovec, Assistant Professor at London School for Economics, organized a small-scale workshop about the future of liability of digital platforms under the EU's upcoming Digital Services Act. The virtual event connected a small group of leading academics researching intermediary liability issues and the EU Commission officials at DG Connect working on the file of the Digital Services Act. The academic participants included Christina Angelopoulos (University of Cambridge), Joris van Hoboken (University of Amsterdam) and Aleksandra Kuczerawy (University of KU Leuven). The event's goal was to share the latest academic research with the EU officials and discuss potential solutions for the reform of the ECD, including drafting suggestions for the provisions related to intermediary liability and notice-and-action mechanisms.

3.3.3. Workshops on online marketplaces, 8, 10, 13 and 17 July 2020

The workshops were co-organised by DG CNECT and DG JUST, as part of a broader engagement with stakeholders and evidence collection strategy for the Digital Services Act package as well as the revision of the General Product Safety Directive.

The objective of the workshops was to gather up-to-date information on the state of play concerning the main challenges in addressing the sale of illegal goods online. It focused in particular on measures and good practices from marketplaces and the cooperation with authorities and responsible third parties. Panellists and participants – which included online marketplaces, retail associations, consumer organisations, national market surveillance authorities as well as representatives from the European Commission - were invited to share their experiences and engage in a discussion on potential new policy and regulatory measures.

The event was made of four separate online sessions:

Session 1: Sellers and products identification mechanisms, 8 July 2020 **-** The first session was focused on the information online marketplaces are currently gathering on their sellers. Online marketplaces started with a short overview of practices in identifying their business sellers and product listings on their platforms. Most of the participating online marketplaces specified that business sellers are required to submit background information (e.g. company name, VAT number, address, etc.) before being admitted to sell. Some participating market surveillance authorities stated that while seller identification is key, the essential point to ensure proper control is the traceability and identification of the dangerous product itself.

Overall, all participants agreed on the importance of having transparency as regard business traders. Some participants highlighted that more should be done in this context, especially when it comes to sellers established outside the EU and therefore not always covered by EU rules. Some stakeholders considered that more cooperation with authorities in Member States could also help identifying rogue sellers.

Session 2: How to tackle dangerous goods and product safety issues online: notice and action procedures and the role of the Safety Gate/RAPEX **- The** first part of this session concerned best practices on notice and action procedures to tackle dangerous goods, including notices from authorities, consumer associations, consumers and other actors. Generally, all participants agreed that a harmonised notice and action procedure would facilitate the fight against dangerous products online. Some participants highlighted that often notices are not accurate enough and online marketplaces have difficulties in identifying the dangerous products notified. In this regard, many participants called for a minimum information requirement for notices. Online marketplaces also stated that filters

are not entirely reliable and that such tools should always be accompanied by human review and notice and action mechanisms.

The second part of the session concerned Safety Gate/RAPEX. In this regard, a number of investigations carried out by consumer organisations, retail associations and market surveillance authorities were also presented, with results on the number of dangerous products available online raising clear concerns. Marketplaces are taking some action, such as periodically checking Safety Gate/RAPEX (as they have committed in the Product Safety Pledge). Some participants pointed out, the information in the Safety Gate only shows only part of the issue and more needs to be done in this regard. Some remedies were proposed by national authorities, such as establishing an obligation to cooperation with market surveillance and custom authorities. Some participants also suggested to have an API interface to Safety Gate/RAPEX which would then be linked to online marketplaces and allow them and consumers to have real-time information on product safety.

Session 3: What other measures and challenges for keeping consumers safe from dangerous goods online? – The session focused on other preventive measures that marketplaces can take to ensure that no dangerous product is placed on the market. Three main aspects were mentioned by participants. First, the importance of data, that in many cases is not provided by the seller, making enforcement very difficult. Second, online sales and product safety are global issues, therefore international cooperation is key to address these challenges. Thirdly, many participants mentioned the issue around traceability, and how it needs to be enhanced so dangerous products sold online can be correctly identified and corrective measures can be enforced by both platforms and authorities. The challenge of reappearance of dangerous products already removed was also addressed, although not specific measures or solutions were mentioned by participants.

Session 4: Consumer law and online marketplaces, 17 July 2020 -The main focus of this session was to address content that is illegal because it constitutes a violation of applicable EU consumer law.

The session started with a short presentation held by DG JUST on the relevance of EU consumer law for a) online marketplaces regarding their own activities and content; b) the business users of online marketplaces; and c) online marketplaces in their capacity as hosts of their business users.

The discussion then zoomed in on third-party content and the measures that online marketplaces are taking to prevent activities that violate applicable EU consumer law. Online marketplaces specified that their objective is to create trust on the platform, both for consumers and sellers. They further stated that sellers are in charge of their own compliance, but that they are responsible to give them the means to be able to be compliant with EU law.

Some participants flagged that the main problem with EU consumer law is the lack of resources and enforcement.

Cooperation was also mentioned by many participants as being the key to ensure a coherent enforcement of EU consumer law. According to many participants, all the actors in the supply chain should work together to raise awareness around consumer rules.

3.3.4. Workshop on Recommender Systems and Online Ranking, 9 July 2020

In July 2020, DG CNECT and the *Laboratoire national de métrologie et d'essais* (LNE) organised a workshop with six experts on recommendation systems.

Participants recognised that recommender systems have important impact in the online dissemination of information and can bring serious societal harms. This is also exacerbated by the fact that moderation processes are often opaque and there is a clear lack of governance, while recommender systems are core part of the platforms' business model and value proposition.

Participants emphasized the importance of regular oversight to account for the rapid evolution of these systems and the risks they bring. According to some experts, among the biggest challenge when observing recommendation systems is the access to data. In particular, accessing relevant output data for observing the effects and prioritisations made by the systems, differs from one system to the other – platforms sometimes make available interfaces for download, sometimes are completely opaque. Web scraping is relatively costly, and is not reliable for observations of the evolution in time. It can also be explicitly in violation of platforms' terms of service.

The experts also discussed the methodological challenges and emerging research in tools to test and compare outcomes of recommender systems. Experts also pointed to the costs in conducting research in these areas, as well as the pressing need for further insights and protections to users who would need to be meaningfully informed and empowered, but should not be solely responsible for protecting themselves. Experts emphasised the need for further independent oversight.

3.3.5. E-Commerce Experts Group meeting, 26 May 2020

During the meeting of the Expert group on 26 May 2020[6], preparation of Digital Services Act package was presented in details and discussed with the Member States. During the discussion, Member States underlined that the new rules should be in particularly friendly towards small and medium enterprises, and stressed that some aspects should be regulated and harmonised especially carefully. In particular Member States stressed the corner stones of the ECD – country of origin, liability exception, prohibition of no general monitoring – should be kept while expressing the willingness to modernise them.

3.3.6. Workshop on the liability of Domain Name Systems service providers under the ECD, 14 February 2020

The Workshop was co-organised by E3 and F2 Units DG CNECT as part of a broader engagement with stakeholders and evidence collection strategy for the Digital Services Act package.

The objective of the workshop was to discuss within panel of academics what is the EU legal framework for Domain Name registries and registrars, whether there is further precision needed in this regard to ensure legal certainty and fair balance between the safety objectives and the protection of fundamental rights. While the panellist has not reached consensus on all aspects discussed during of the workshop, they agreed that a clarification of the role of the DNS going forward appeared beneficial. The most prominent aspects concerning the ECD relate to other intermediaries, namely hosting providers or online platforms. Compared to these, the DNS, i.e. the logical layer, plays a less prominent role. Also in the future, the DNS is likely to play a subordinate role in relation to content compared to hosting providers or platforms. Yet, in some instances the clear borders between intermediaries on the infrastructure and intermediaries on the application layer are

[6] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21180

becoming blurrier. Several experts noted the increasing interest in the DNS in content debates.

In conclusion, panellist suggested several **areas of interest** in relation to the DNS:

- **The clear inclusion of DNS** actors amongst service providers enjoying liability exemptions;
- **Cascade of intermediary functions:** The distinction from other intermediaries based on the nature of the DNS and how different roles impact the balance of interests and fundamental rights concerned;
- **Distinction among DNS actors in relation to DNS functions:** Whether distinctions should be made between domain name registries, registrars, resellers, actors involved in handing out IP addresses and other service providers;
- **Transparency and procedure of domain-name related actions:** Consider the framework for actions in relation to transparency and procedure e.g. in the context of Recommendation (EU) 2018/334 and its applicability to voluntary arrangements.

3.3.7. E-Commerce Experts Group meeting, 8 October 2019

During the E-Commerce Experts Group meeting on 8 October 2019[7], the main principles of the ECD has been discussed with Member States, as well as the latest development on national levels. **On the ECD principles**, some Member States agreed that one of the main difficulties is in devising a common effective law against harmful or hateful content. Fundamental rights in relation to tackling harmful content online were discussed as well. Managing fragmented rules is often only possible for large platforms; mutual recognition was suggested by some as a possibility to solve the issue. On **liability**, the Member States discussed how the exemption from liability fits within the changes in the online environment that have taken place over the last 20 years, as well as within its enforcement. The possibility to introduce a Good Samaritan clause as a legal provision was also discussed. A group of Member States was of the opinion that some services currently covered by the liability regime should not continue to be covered in the future. This could include the provision of services that can no longer be claimed are provided passively. As a result, large platforms should be the subject of stricter rules. During the discussion of the **Commission's Communication and Recommendation on tackling illegal content online**, Member States expressed the need to preserve freedom of expression. Some Member States noted a perceived convergence of measures that tackle illegal content online and harmful content online and raised concerns that as illegality is not harmonised, this can cause jurisdiction problems. Member States also reported that the increased fragmentation, on both the national and the EU level, makes it difficult for online service providers, particularly SMEs, to comply with legislation. They also underlined that self- and co-regulatory initiatives should also be considered for particular types of actions. On **cooperation mechanisms** that are set-up by the ECD, Member States confirmed usefulness of cooperation, but they also highlighted issues requiring more attention. Member States reported different experience, with some using the IMI mechanisms relatively often and some not at all. Some Member States emphasised the importance of contact points, with some Member States suggesting harmonisation via one contact point for illegal content and requested that the cooperation procedure should be easy to use. Member States also reported

[7] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=16890

that the increased fragmentation, on both the national and the EU level, makes it difficult for online service providers, particularly SMEs, to comply with legislation. On the **sustainability of the framework for SMEs**, the Member States stressed that the basic internal market principle and liability exemptions are crucial for companies to grow. They also explained that SMEs encounter obstacles when they want to expand their business, arising very often from different national rules and lack of (full) harmonisation.

3.3.8. Semi-structured interviews with judges across the EU, July 2017[8]

In total five judges were interviewed over June and July 2017, including representatives from the United Kingdom, Germany, Italy, the Court of Justice of the European Union and the European Court of Human Rights. General views collected through these interviews include:

- Different levels of experience in cases involving intermediary services among Member States. That affects understanding and consistency in applying the liability regime.
- The liability regime is still useful but will require more flexibility as technology evolves. Any replacement of this regime would require a careful balancing of interests.
- Different categories of illegal content should be treated differently.
- Need to decide case-by-case whether an intermediary plays an active or a passive role.
- More clarity and standardisation of minimum requirements of notices would be useful.
- Setting one fixed deadline to take action on notices would not be appropriate.
- Lack of clarity of recital 42 of Directive 2000/31/EC. Uncertainty as to whether the use of algorithmic or automatic process to detect illegal content renders service providers active.
- The use of automated processes is pushing in the direction of a general monitoring obligation. The ban on such obligation is still useful, although for several judges it might become less so in the future.
- Relying on intermediaries to police the Internet is risky. If the Commission wishes to encourage this, it should provide clear guidelines on what content is considered illegal.
- Judges considered that in principle judicial oversight was more appropriate in regards to rule of law than private standards.
- There was calls for new legal processes (such as Internet courts) to allow judges to deal with potentially illegal content online quickly.

[8] Initially included in the annexes of the Impact assessment for the Proposal on preventing the dissemination of terrorist content online of 2018.

Annex 3: Who is affected and how?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

Main positive impacts and the affected stakeholders

The initiative would have a **positive effect on the functioning of the single market**. In particular, it would support access to the single market for *European platform service providers* and their ability to scale-up by reducing costs related to the legal fragmentation. Moreover, it would improve legal clarity and predictability regarding the liability of *online intermediaries*, among others. It would also increase transparency about content moderation, recommender and advertising systems, and the business users of online platforms to the benefit of *consumers, regulators, researchers and civil society*. The new EU level governance structure would improve trust and cooperation between *Member States*, facilitate effective enforcement across borders, and reinforce the internal market principle of the E-Commerce Directive.

With regards to **competition**, the harmonised legal requirements would establish a level playing field across the single market, while the limitation of asymmetric obligations to *very large online platforms* with a systemic impact in Europe would make sure that *smaller, emerging competitors* are not captured by disproportionate measures. The initiative is proportionate and would not impose dissuasive requirements for service providers.

With the additional legal certainty, the initiative is expected to have a positive impact on **competitiveness, innovation and investment** in digital services. The harmonised measures would cut the costs of the evolving legal fragmentation and the extended scope would create a true regulatory level playing field between *European companies and those targeting the single market without being established in the EU*. The intervention would preserve the equilibrium set through the conditional liability exemptions for *online intermediaries*, ensuring that online platforms are not disproportionately incentivised to adopt a risk-averse strategy imposing too restrictive measures against their users, but they can take voluntary measures against illegal activities. The initiative would also have a positive effect on the competitiveness of *legitimate business users of online platforms, manufacturers or brand owners*, by reducing the availability of illegal offerings such as illegal products or services. Additional profits are expected to largely overcome the costs of the notice and action mechanism. More transparency would build further resilience into the system, giving more choice and agency to *users* and stimulating an innovative and competitive environment online.

The initiative is expected to **diminish illegal trade into the Union** without having an adverse effect on *legitimate platforms targeting the single market from third countries*.

The initiative would greatly increase **online safety** for *consumers* by adding more harmonisation to the tackling of all types of illegal content, goods and services across the Union. It would accelerate cooperation with *law enforcement, national authorities and trusted flaggers* under EU level supervision, and it would stimulate *online platforms* to take additional measures, proportionate to their capability, adapted to the issues and illegal content they most likely host, and in full respect of fundamental rights. The reinforced EU

level supervision and cooperation would be able to monitor the performance of the notice and action and broader moderation, as well as recommender and advertising systems to protect *legitimate users* and avoid over-removal of legal content.

The intervention would also **tackle systemic risks** posed by online platforms particularly through transparency obligations and asymmetric measures imposed on *very large platforms*. It would correct information asymmetries and empower *citizens, consumers in particular, businesses and other organisations* to have more agency in the way they interact with the digital environment. Accountability mechanisms would ensure that *researchers and competent authorities* could assess the appropriateness of measures taken by platforms in co-regulatory processes.

Costs for businesses, SMEs, public authorities and the EU

The **costs incurred** by online *intermediaries* would represent a significant reduction compared to those incurred under the present and evolving fragmented and uncertain corpus of rules. At *company* level, the legal intervention could lead to a cost reduction of around EUR 400.000 per annum for a medium sized enterprise, but this could go up to 4-11 million EUR per annum for a larger company. Direct costs for the main due diligence obligations depend to a large extent on the number of notices and counter-notices received by a platform and cases escalated to an out of court alternative dispute resolution system. The existence of alternative dispute resolution mechanisms is likely to append negligible costs compared to the current system. The additional design, maintenance and reporting costs for the information and transparency obligations are expected to be marginal and absorbed into the general operations and design costs of online platforms and ad intermediaries, respectively. Costs related to information requirements would equally be reduced rather than increased, compared to the baseline, due to streamlining and harmonising. The only potentially significant increase of costs would result from the enhanced due diligence obligations that are limited to *very large online platforms* with systemic role and competitive advantage fuelled by network effects. These costs would vary depending on the design of the systems but are expected to be absorbed in the services' operations in any event.

For **SMEs**, the costs of the legal fragmentation seem completely prohibitive today. The initiative would make it much more feasible for *SMEs* to enter into the single market and scale up. However, the introduction of standard, minimum requirements for notices, procedures and conditions, as well as reporting templates, should further decrease the expected costs for small companies.

For **public authorities**, any additional measures to mutualise resources and expertise and to establish sound IT infrastructures for cooperation can have a net positive effect in assisting all Member States in the medium to long term. Compared to the baseline, the initiative should cut significantly the costs brought by the inefficiencies and duplication in the existing set-up for the cooperation of *public authorities*. Net cost reductions, however, are not expected, due to the volume of illegal activities online. *Member States* where a large number of services are established are likely to need some reinforcements of capabilities, but these will be attenuated through the creation and use of the Digital Clearing House. National Digital Coordinators would incur some costs, but the efficiency gains from mutualisation of resources, better information flows and straight-forward processes are expected to overweight them in every Member State. The additional cost of the EU level

oversight, including the *EU Board and Secretariat*, would be born at EU level, creating further efficiency gains in the cooperation across Member States.

2. SUMMARY OF COSTS AND BENEFITS

I. Overview of Benefits (total for all provisions) – Preferred Option		
Description	***Amount***	***Comments (main recipients)***
Direct benefits		
Reduced costs related to legal fragmentation (i.e. compliance costs)	Cost reduction of around EUR 400.000 per annum for a medium enterprise (up to 4-11 million EUR for a company present in more than 10 Member States)	All intermediary services, especially small and medium sized hosting services and small and medium sized online platforms
Improved legal clarity and predictability		All intermediary services
Increased transparency regarding content moderation, recommending and advertising systems	Cutting costs of uncertainty over which reporting system to use Agency based on information for making real choices rather than dependent on design features from platforms	Citizens, businesses, regulators, researchers, civil society
Stronger and more efficient cooperation between Member States	General cost reduction by streamlining the cooperation mechanisms, cutting inefficiencies and obtaining results	Member States, national authorities – primary recipients, and better results overall for citizens, services and other businesses
Increased transparency of potential business wrongdoers (Know Your Business Customer)	Dissuasive for the majority of sellers of illicit products	Legitimate businesses, national authorities, consumers
Reduced information asymmetries and increased accountability	User empowerment to make informed choices	Users, including citizens, businesses and society at large
Fundamental rights and protection of legitimate users and content		All citizens and businesses, in particular journalists and other content providers
Indirect benefits		

Increase of cross-border digital trade and a more competitive and innovative environment	1 to 1.8% (estimated to be the equivalent of an increase in turnover generated cross-border of EUR 8.6 billion. and up to EUR 15.5 billion)	All digital services and businesses
Diminished illegal trade into the Union Increased online safety Reduced systemic risks posed by large online platforms		Citizens, businesses, smaller digital services and society at large

II. Overview of costs – Preferred option							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Notice and action	Direct costs		Minimal time spent on sending a notice – this should not be a significant costs, but rather an overwhelmingly important reduction of costs compared to the current unclear and deeply fragmented system	1500 – 50.000 EUR	Depends on volume of notices, expected to decrease overall (estimated range: 0 to 16 mil EUR)		
	Indirect costs						
Complaint and redress mechanism	Direct costs			Costs of technical design (minimal)	Costs of maintenance (absorbed in the costs for notice and action estimated above)		
	Indirect costs						
Alternative dispute resolution	Direct costs	Depending on dispute		Depending on dispute		Negligible	Negligible
	Indirect costs						

Know Your Business Customer	Direct costs			Costs of design	Marginal costs per business customer		
	Indirect costs						
Transparency obligations	Direct costs			Marginal technical design costs for development, data collection, absorbed in the development of technical systems	0.1 and up to 2 FTEs		
	Indirect costs						
Legal representative	Direct costs				Estimated between EUR 50.000 to EUR 550.000 per annum, depending on the FTE necessary to complete the tasks. These costs can be partially or fully absorbed, for most companies, in existing requirements for legal representatives.		
	Indirect costs						
Risk management obligations	Direct costs				Risk assessments: estimated between EUR 40.000 and EUR 86.000 per annum Audits: between EUR 55.000 and 545.000 EUR per annum Risk mitigation measures are variable costs		

					and can range from virtually no costs, to significant amounts, in particular when the platforms' systems are themselves causing and exacerbating severe negative impacts. The duration and level of expenditure for such measures will also vary in time. Similarly, participation in Codes of conduct and crisis protocols require attendance of regular meetings, as a direct cost, but the streamlined targeted measures can vary.		
	Indirect costs						
Ad archives	Direct costs			Up to 220.000 EUR for building APIs to give access to data and quality controls for data completeness, accuracy and integrity, and for system security and availability	Marginal maintenance costs		
	Indirect costs						
Compliance officer	Direct costs			Between 1 and 5 FTEs for very large platforms			
	Indirect costs						

Digital Clearing House	Direct costs					2 mil per annum over the first two years for technical developmen t.	Maintenance and additional development over the next 3 years of approx. EUR 500.000 in total
	Indirect costs						
EU Board and Secretariat	Direct costs						0.5 – 1 FTE for participation in the Board – per Member State European Commission : 50 FTEs + EUR 25 mil operational budget
	Indirect costs						
Supervision and enforcement (Digital Services Coordinator national level)	Direct cost						For core due diligence obligations on intermediaries : varying from 0.5 FTEs up to 25 FTEs, depending on scale of services hosted1 For supervision of very large platforms Costs expected to fluctuate depending on inspections launched. For one

[1] Benchmarked against resources currently reported by DPAs, and estimating 0.5 FTE for investigators per 15 million users reached by a digital service hosted in the Member State, with efficiencies of scale accounted for

							inspection/audit, estimates between EUR 50.000 and EUR 300.000
	Indirect costs						

Annex 4: Analytical methods

1. COST OF NON-EUROPE: LEGAL FRAGMENTATION AND CROSS-BORDER PROVISION OF SERVICES

The identification of the costs of non-Europe related to legal fragmentation focused in particular on the different approaches of rules transposing the E-Commerce Directive (ECD) governing how services, and in particular intermediaries and platforms, shall deal with illegal content, pursuant to Article 14 ECD.

An estimation of the costs made by JRC draws on the cross-trade barriers the differences of applicable laws in different Member States may create. To estimate those barriers, an indicator of the legal distance (i.e. differences) in transposing/applying Article 14 across different pairs of Member States has been drawn, and correlation with cross-border traffic as a proxy of cross-border trade has been verified, on the basis of a general trade model. The models and the methodologies applied are described in detail in Annex 4.

Legal distance

"Legal distance" is a concept that represents differences in laws and regulations across countries. JRC identified an indicator that quantifies a legal distance between EU MS in regards to the transposition and subsequent implementation of the intermediary liability exemption for hosting services, as introduced in Article 14 ECD. The process of constructing the indicator had two distinctive parts.

First, JRC performed a legal analysis of the ECD and reviewed relevant literature relating to the issue of liability of Intermediary Service Providers (ISPs). This was followed by an analysis of previous studies dealing with the issue of legal fragmentation stemming from the transposition and implementation of the ECD.

Second, JRC quantified a legal distance between EU MS with respect to the transposition of Article 14 ECD. The indicator builds on the updated results of the Report produced for the European Commission in 2018.[1] In the construction of the indicator, JRC considered the burden of adaptation that ISPs have to face in order to comply with the legal rules that transpose the ECD into national systems. The final values of the indicator convey information on how the different MS transposed Article 14 of the ECD into their national legislations. The "legal distance" between two countries is simply the absolute difference of the values of this indicator, and shows how "close" or "far away" the legislation of two MS is. The indicator includes the following components:

[1] EC, "Overview of the legal framework of notice-and-action procedures in Member States", Report for the European Commission DG CNECT, written by ICF in cooperation with Grimaldi Studio Legale and 21c Consultancy, Brussels, July 2018, available at https://op.europa.eu/en/publication-detail/-/publication/c5fc48ac-2441-11e9-8d04-01aa75ed71a1/language-en/format-PDF/source-102736628. This report sheds light on the differences in the implementation of Article 14 ECD across all EU MS. The evidence collected in this report is based on the review of national legislations, literature, case law as well as surveys of both ISPs and competent legal authorities. The result is a comprehensive overview of the legal fragmentation resulting from the implementation of the Article 14 ECD in the EU.

- Obtaining knowledge – this indicator's component reflects coerciveness of a particular way of "obtaining knowledge." The most coercive option is considered the most costly and is ascribed with the highest value. The component ascribes the following values: 1-various ways of obtaining knowledge or no specification, 2-minimum requirements notice, 3-court/authority order or manifestly illegal content (most coercive);

- Existence of a specific and platform-managed N&A procedure – this indicator's component reflects the cost of adaptation driven by the laws introducing N&A procedures. The components ascribes the following values: 0-no procedure, 1-horizontal laid down in law, including co-regulation, 2-sectorial procedures only (regardless their legal status). The lowest value indicates that there is no legal requirement to adapt. Horizontal procedures are less costly than sectorial, since they introduce uniform compliance mechanisms;

- Specification of information to be provided in a notice – this indicator's component ascribes two values: 0-not specified, 1-minimum requirements. The more a national legislation regulates the level of information required, the more the platform needs to adapt to each system, therefore, the minimum requirements are more costly for an service provider;

- Timing of the removal – this indicators component ascribes the following values: 0-no specification of timing, 1-timing specified > 24h , 2-timing specified < 24h. The shorter the timing, the more an ISP needs to adapt, which incurs costs;

- Existence of the counter-notice procedure – this indicator's component ascribes two values: 0-No, 1-Yes. The existence of the counter-notice procedure incurs costs for an ISP;

- Abusive notice remedies – the indicator's component ascribes two values: 0-there are remedies, 1- no remedies. The value "1" is ascribed when there are no remedies, to reflect the burden relating to the increased number of notices;

- Reporting obligation – this indicator's component ascribes the following values: 0-no reporting obligations, 1-Yes, there are reporting obligations;

- Internal appeal system – this indicator's component ascribes two values depending on the existence of the obligation of appeal system internal to an ISP: 0-No, 1-Yes.

- Extraterritorial application of the rules on N&A – this indicator summarises whether a Member State requires its rules to be applied also to ISP established in other Member States (including through a legal representative): 0-No, 1-Yes[2].

All the components of the indicator are valued for each EU MS. The differences in total values of the indicator between MS illustrate a legal distance between the national regimes with respect to the transposition of Article 14 of the ECD.

[2] At the moment this indicator only reports DE, as rules in FR have been subject to constitutional scrutiny and in AT are still under notification to the Commission.

Description of traffic data and methodology the gravity equation and trade costs

In order to study empirically trade costs and the barriers to market integration, the standard procedure in economics is to employ the gravity model of trade. This model captures the interactions between country pairs. In this case, the variable of interest is internet traffic, i.e., the set of cross-border visits to websites located the EU MS originating from visitors located in a different MS in 24 different categories of activities.

With regard to the traffic data, the top 100 websites per each of the 24 categories of digital activities and for the 20 EU MS[3] Similarweb collects data for have been identified. First, through a DNS[4] lookup, we have identified to which country the different domains correspond. Second, we have downloaded the geographic breakdown of the traffic directed to this domains for three different moments in time: the months of April 2018, April 2019 and April 2020. Third, we have restricted the analysis to domains that appear in all three periods. In so doing, we are able to build internet traffic origin-destination matrixes, as the measure of trade in digital services. Accounting for duplicates in the top 100 lists, and the fact that some domains only appear in one time period, this procedure gives a total of 31084 different domains used for the empirical analysis. Figure 1 shows the evolution of the total volume of visits, while figure 2 shows the distribution by category.

Figure 3: Evolution of total internet traffic in the EU (in M visits) - Source: JRC elaboration with data from similarweb.com

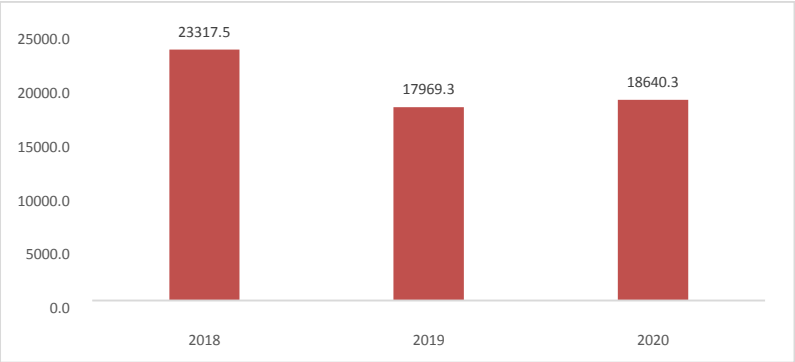
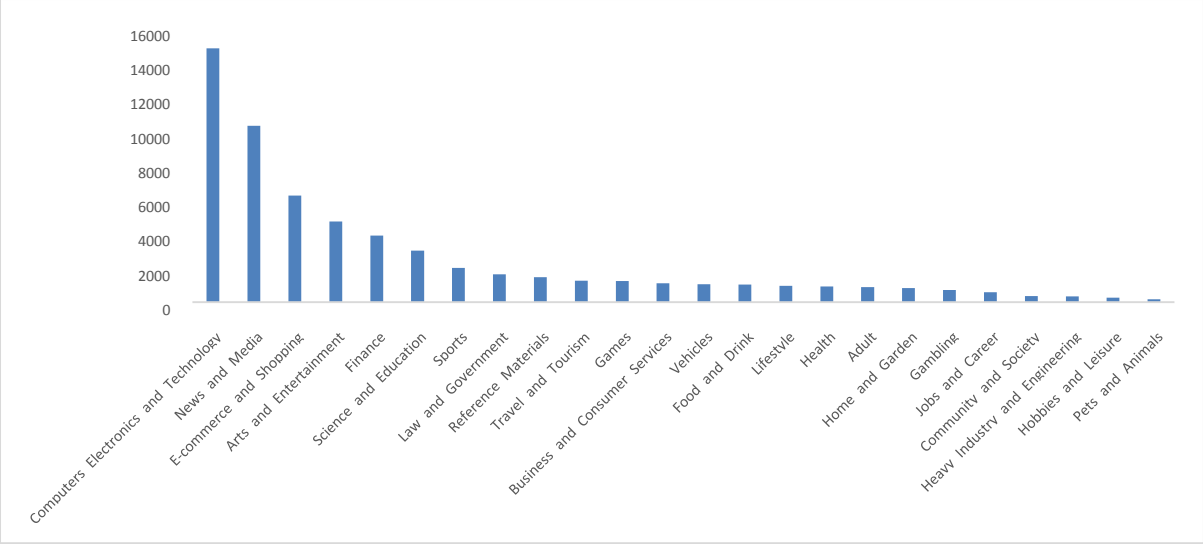


Figure 4: Distribution of total internet traffic in the EU, by category (in M visits) - Source: JRC elaboration with data from similarweb.com

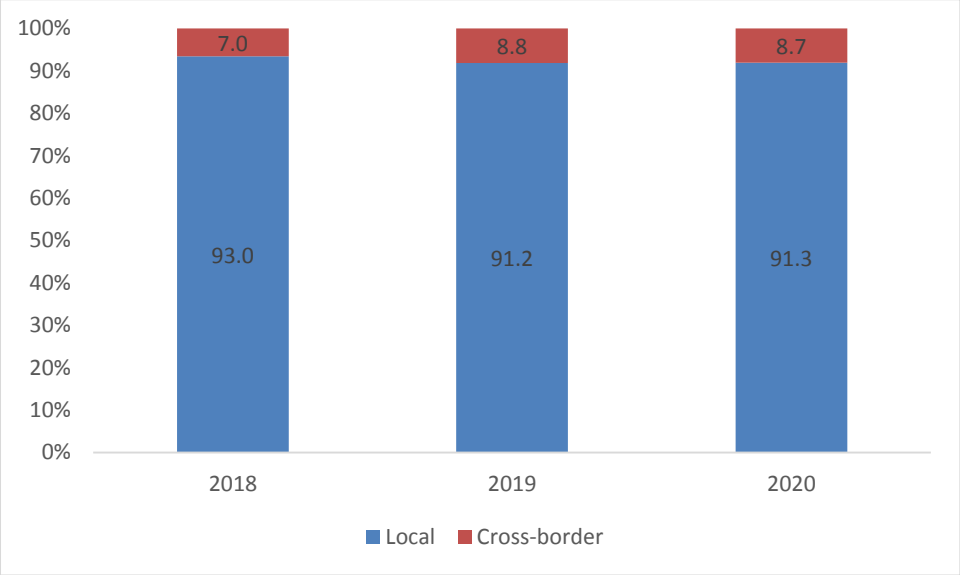
[3] AT, BE, BU, HR, CZ, DK, FI, FR, DE, GR, HU, IE, IT, NL, PL, PT, RO. SK, ES, SE.

[4] Domain Name System. The identification of the country is done by checking the server where the domain is stored.



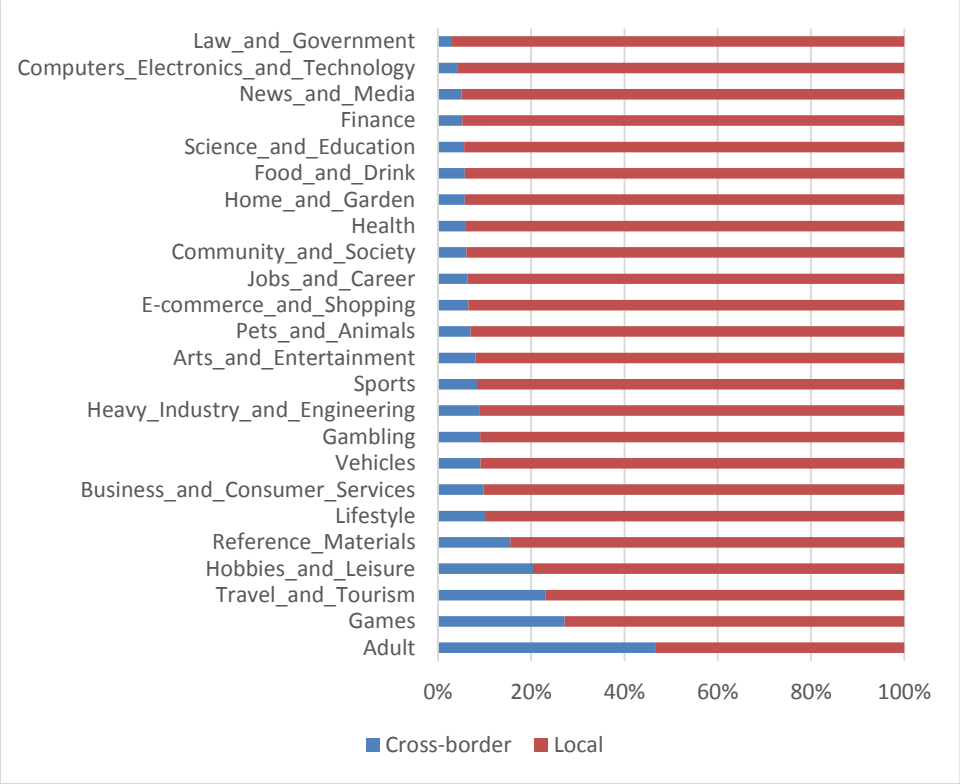
The majority of traffic to websites comes from local users, i.e., there is relatively little cross-border volume of internet visits, as shown in figure 3:

Figure 5: Evolution of local vs. cross-border Internet visits in the EU - Source: JRC elaboration with data from similarweb.com



However, there are important differences by sector given by how tradable some services are. Figure 4 indicates that services such as Law and Government and News and media, for instance, tend to be more local than the average since public services and news tend to be tailored to local tastes, preferences and needs. On the other hand, Games and Tourism show a higher volume of cross-border trade.

Figure 6: Local vs cross-border Internet visits in the EU, by category - Source: JRC elaboration with data from similarweb.com



The gravity model of trade also includes local visits, visits to residents in one country to websites located in the same country, as a measure of "domestic" trade or "home bias".

Including domestic trade in gravity estimations is justified by several arguments. First, since consumers face the option to consume both domestic and foreign products, this guarantees consistency with theory and also with stylised facts about consumer behaviour. Second, it allows the identification of the effects of bilateral trade policies in a theoretically-consistent way (Dai et al., 2014). Third, it measures the relative effects of distance on international trade with respect to the effects of distance on internal trade (Yotov, 2012), the so-called "distance puzzle" in trade. Finally, it controls for the effects of globalization on international trade and corrects the potential biases in the estimation of the impact of trade agreements on trade (Bergstrand et al., 2015).

In the literature, the basic log-linearised regression equation is:

$$ln(X_{ij,d,t}) = \alpha + \gamma Z_{ij} + \mu_{ij} + \pi_d + \tau_t + \varepsilon_{ij,d,t} \qquad (1)$$

The variable $X_{ij,d,t}$ indicates internet traffic from country i to destination j, directed to website d in time t. When i and j differ, X captures international trade, and when i=j, then X reflects intra-national trade, or the so-called home bias. Since we have different websites in each country, we differentiate between domains through the sub-index d, while t is the month.

Additionally, Z_{ij} indicates a vector of different bilateral distances that are commonly used in trade studies to capture trade costs, such as contiguity, physical distance, common language or common currency. The term μij denotes the set of country-pair fixed effects, which serve

one main purposes: it will absorb most of the linkages between the endogenous trade policy variables and the remainder error term εij,t in order to control for potential endogeneity of the former. In principle, it is possible that the error term in gravity equations may carry some systematic information about trade costs. However, due to the rich fixed effects structure in equation (1), we are more confident to treat and interpret εij,t as a true measurement error. Next, the term π_d is the set of domain fixed effects, to control for the heterogeneity of sizes and categories of the different websites, as well as for additional factors that may influence consumer behaviour such as brand or type of website. Similarly, τ_t represents month fixed effects and controls for the time effects due to seasonality or trends in e-commerce interest. Finally, εij,t is the error term.

Results

The results of the trade model identified a negative correlation[5] between the legal distance indicator and the cross-border traffic (the higher the legal distance, the lower the cross-border traffic), outlined in the table below. A reduction/harmonisation of rules in this regard could improve cross-border trade in terms of traffic between Member States in a range between [1% and 1,5%].

VARIABLES	(1)	(2)	(3)	(4)	(5)
Physical distance (log)	-0.121***			-0.122***	-0.121***
	(0.00188)			(0.00188)	(0.00189)
Legal distance (log)			-0.0107***		-0,0155***
			(0.00133)		(0.00131)
Contiguity	0.104***	0.209***	0.210***	0.101***	0.104***
	(0.00252)	(0.00188)	(0.00187)	(0.00252)	(0.00252)
Common language	0.222***	0.233***	0.233***	0.222***	0.222***
	(0.00304)	(0.00304)	(0.00305)	(0.00304)	(0.00304)
Common currency	0.0517***	0.0498***	0.0516***	0.0496***	0.0517***
	(0.00188)	(0.00188)	(0.00187)	(0.00189)	(0.00188)
Home bias	0.780***	0.979***	1.009***	0.752***	0.780***
	(0.00381)	(0.00222)	(0.00227)	(0.00418)	(0.00428)
Constant	1.978***	1.203***	1.169***	2.019***	1.978***
	(0.0145)	(0.00766)	(0.00764)	(0.0148)	(0.0148)
Observations	1,222,164	1,222,164	1,222,164	1,222,164	1,222,164
R-squared	0.316	0.313	0.314	0.316	0.316

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Dependent variable: visits to domains located in the different MS, from users located in the same country and from users from other EU MS (online trade captured by internet traffic –information flows over the internet).
Legal distance: how different the transposition of the ECD has been in the different MS pairs.

[5] Also cross-checked vis à vis other possible relevant variables such language, size, physical distance, etc…

2. ESTIMATES FOR COMPANY-LEVEL COSTS

Estimates are based on averages established based on data reported by companies for the notice and action and transparency obligations in the German law over a period of 6 months. As there are significant differences in the scale of notices received and resources invested by different companies, estimates were corrected based on simulated data from a model built by the JRC for a full content moderation process a company could put in place.

To estimate the duplication of costs across Member States, the indicators for the legal distance[6] were also used to correct coefficients for the duplication of costs in scenarios of the evolving legal fragmentation.

For the additional costs on very large platforms, estimates are based on:

- Average FTE costs of EUR 110.000
- Benchmarks of risk assessments in the financial sector[7] and estimated costs of technical audits[8]
- Reported data from stakeholders for maintenance of databases.

3. DEFINITION OF 'VERY LARGE PLATFORMS'

An important driver of the identified problems is the unique situation of the largest online platforms, such as social networks or online marketplaces. A relatively small number of online platforms concentrate a very high number of users – consumers and traders alike. Very large platforms represent a higher level of societal and economic risk because they have become *de facto* public spaces, playing a systemic role for millions of citizens and businesses. In other words, they have a significantly higher impact on society and the Single Market than smaller platforms because they **reach a large audience**.

When designing the definition of very large platforms, it seems therefore that the most important factor is the number of users, as a clear proxy for the levels of risks they pose. This is the key metric that propels rapid growth and leads to significant societal and economic impacts.

A similar methodology of focusing on the number of users as a proxy could be observed in recent policy initiatives regarding online platforms around the world (e.g. NetzDG (DE) – special obligations on online platforms with more than two million registered users (2.5% of DE population); ACCC Digital Platforms Inquiry (AU) – special recommendations for platforms with more than one million monthly active users (4% of AU population); Online Harms White Paper and Furman Report (UK) – significance of the largest platforms). As a different but comparable benchmark, the recent DSM Copyright Directive provides for a lighter liability regime for start-up content sharing platforms as long as their average number of monthly unique visitors does not exceed 5 million (1% of the EU population).

[6] *Supra,* p. 43
[7] https://op.europa.eu/en/publication-detail/-/publication/4b62e682-4e0f-11ea-aece-01aa75ed71a1
[8] LNE, forthcoming

Reaching 10% of the EU population (currently around 45 million people) directly, and many more indirectly through family members for example, represents a significant share of the EU population and can lead to a significant impact, regardless of the risks and harms considered. This value is set as a reasonable estimate for a significant reach in the EU prone to significant negative effects considering all societal risks in scope of this intervention. It is a proxy value, which is not tailored to the impact of a particular risks, such as the dissemination of a given type of illegal content or manipulation of democratic processes, but a cumulative approach. Its proportionality is considered also in relation to the horizontal measures and corresponding costs on service providers.

The benchmark for the EU-27 population has remained in a +/-5% fluctuation range since the 1990s. However, the legal technique for designing the precise threshold should take into account possibilities of more significant fluctuations.

Exploring available data – see below - all considered platforms with at least 45 million users in the EU are present in multiple Member States. Most of the very large platforms would be either social networks, online marketplaces or video-sharing services.

Using the number of users as the only criterion for the definition of very large platforms has clear regulatory advantages. It creates a simple, future-proof system where it is easy to determine whether a platform has a significant reach in the single market, which will ensure legal certainty. Information on the number of users is already widely available, though precise methodology and reporting is necessary for establishing legally reliable measurements.

When designing the threshold for very large platforms, alternative criteria were also considered:

a) Qualitative criterion of significant societal and economic impact – The collected evidence suggests that the largest online platforms all have significant impact on society and the economy. At the same time, this intervention is horizontal and considers different types of societal risks. Obligations imposed are due diligence, procedural obligations and the proportionality of the intervention in terms of costs on the service provider are considered in relation to the horizontal obligations and a general and cumulative assessment of societal risks, not individual risks for specific types of illegal content or societal harms. Such a case-by-case approach would lead to considerable legal uncertainty and disproportionate costs and long procedures for establishing the scope of the measures.. Also, these assessments would necessarily involve subjective elements and could lead to discrimination between service providers. The threshold regarding the number of users has been determined in a way that it implies potentially significant societal and economic impact.

b) SME status, turnover, market capitalisation – The reason to add such criteria would be to ensure that the enhanced obligations for very large platforms do not represent a disproportionate burden for a smaller company behind the platform. However, given the business model of large online platforms, it is highly unlikely that a platform with 45 million users would be a micro or small enterprise. In this unlikely and hypothetical case, the public interest objectives pursued by the initiative would outweigh the economic interest of the platform because the risks and harms are

determined by the reach and impact of the platform, not the size of the company. In any event, the enhanced obligations for very large platforms have been designed to be proportionate for services of such scale.

The definition of 'gatekeeper platforms' in the Digital Markets Act (DMA) initiative is different in nature and scope from the definition of 'very large platforms' falling within the scope of the asymmetric obligations under the Digital Services Act (DSA). The DMA seeks to tackle primarily specific economic concerns associated with the gatekeeper power, which enables a small number of gatekeeper platforms to undermine fair commercial conditions and contestability of digital markets concerned. On the other side, the DSA seeks to address primarily societal risks, including some economic risks that are however very different to the ones related to the gatekeeper power, associated with the fact that some very large platforms represent de facto public spaces, playing a systemic role for millions of citizens and traders.

Irrespective of the different objectives pursued by the two sets of rules, there may be an overlap between these two categories. Very large platforms in the DSA are determined based on the number of their users. At the same time also in the DMA a provider of core platform services (i.e. online intermediation services; online search engines; operating systems; cloud computing services; and related advertising services to these core platform services) needs to have a minimum number of active users to be considered as a gatekeeper platform. However, contrary to the determination of very large platform under the DSA, the number of active users is just one of the criteria determining a gatekeeper platform. As the criteria will be different, not all very large platforms will be gatekeeper platforms.

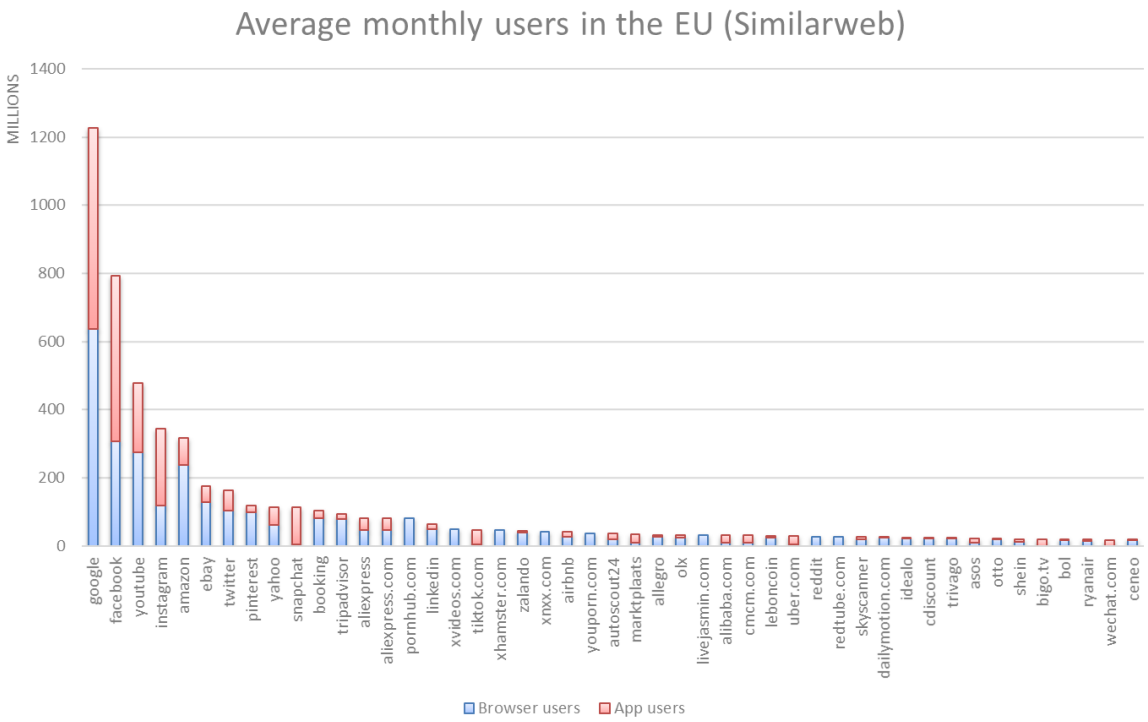
Preliminary data used to estimate the scale of reach in the Union, is based on SimilarWeb extracted information (measured as average monthly users in 2019). The graph below presents average monthly users for a selection of online platforms based on the top ranking services.

The graph below shows cumulatively app users and browser users - it is important to note that the two user bases overlap to certain extent and this differs from one platform to another. To contextualise, . for Facebook, the actual user base in the EU is reported to be just under 400 million in the same period (2019); for Snapchat, most of the user base would be accurately represented by app users and is not an exhaustive list of platforms. App stores, for example, are not represented here.

This data suggests two important conclusions

(1) the differences in scale between the user base of platforms are staggering.

(2) there are methodological limitations in establishing with accuracy the scales of users of a digital service and an online platforms. Third party traffic data, such as the SimilarWeb source cannot accurately address duplication of measurements, and publicly available data on mobile vs browser use. To date, the most precise indications are reported by services themselves.



4. MACROECONOMIC IMPACT ANALYSIS

At a basic level, economic impact analysis examines the economic effects that relevant business and/or economic events (infrastructure project or governmental policy, for example), have on the economy of a geographic area. At a more detailed level, economic impact models work by modelling two economies: one hypothesised economy where the economic event being examined occurred and a separate (real) economy where the economic event did not occur. By comparing the two economies, it is possible to generate estimates of the economic impact the event under analysis had on the area's economic output, earnings, and employment. In many cases, sophisticated Computable General Equilibrium (CGE) models are used. In others, a simpler but equally robust analysis comes from an estimation method known as an input-output model. This is the method used in this case.

Input-output models are designed to examine all of the industries in an economy and estimate all of the ways that spending in one sector influences each of the other sectors in that economy. For example, what happens when an e-commerce website faces an increase in demand due to a government policy that addresses consumer protection? To meet the sales increase, the e-commerce website will procure more items from wholesalers or manufacturers. In turn, in order to increase production to meet the e-commerce demand, the manufacturer will need to hire more workers, as well as the logistics firms that distribute the items to the finals consumers, which indirectly increases total employment. However, the manufacturer will also need to purchase more raw materials and intermediate goods and services that are needed in the manufacturing process. As the manufacturer purchases more

intermediate goods and services, the producers of those goods and services respond to the increase in demand by hiring more workers and purchasing more of their own inputs. Overall, the increase in e-commerce sales results in a direct increase in total employment caused by the website hiring more personnel to handle the increase in demand, as well as indirect increases in total employment caused by the other producers of goods and services involved in the value chain. Input-output models generate their estimates by examining three types of economic effects. The first effect is the direct impact of the spending or economic event. When a new business enters a city, it may employ 100 workers and sell €1 million in goods and services each year, which is the direct effect the business has on the local community. The business also has another effect on the community, called the indirect effect. In input-output modelling, the indirect effect is the impact the new business has on other local industries when it purchases goods and services for the operations of the business. In addition to the indirect effect, the new business or project also creates an induced effect within the regional economy. The induced effect is the result of the new employees and business proprietors spending the new income they are now receiving from the new business within the community. In the end, input-output models estimate the **total economic impact** new spending has on a local economy by combining the direct, indirect and induced economic effects. In this case, the figures underlying the estimation rely on the assumption that a revised policy for illegal content online will bring more certainty and confidence to users, which in turn will be translated in greater expenditure in e-commerce and more usage of other digital services. These assumptions are then translated to increases in expenditure and investment, a direct impact of the policy, while the total impact comes from the computation of the indirect and induced effects.

Input-output models, and economic impact analysis in general, are useful tools to estimate the effects new policy proposals, or changes in spending, will have within an economy. However, input-output models are based on a set of assumptions that need to hold for the results to be valid. One key assumption is that the new spending patterns are the same as the spending patterns made in the past. Another weakness of many input-output models is the assumption that inputs are infinitely available without prices having to increase. Finally, many economic impact analyses that use input-output models assume that the increased spending being modelled comes from outside the area the impact analysis examines, resulting in an increase in total spending. However, if the money is a simply transfer from one typo of expenditure to another, the total spending and employment in the city may not change at all.

Summary of the computation of the model:

Option		Δ GDP (B€)	% GDP (2019)	% benefit
1	Consumers	8.9		23.1
	Providers	29.7		76.9
	Total	38.6	0.3	
2	Consumers	19.1		30.9
	Providers	42.7		69.1
	Total	61.8	0.4	
3	Consumers	27.7		33.9
	Providers	54.0		66.1
	Total	81.7	0.6	

Annex 5: Evaluation report for the E-Commerce Directive

1. INTRODUCTION

1.1. Purpose of the evaluation

This evaluation concerns 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[1] (hereinafter "*the e-Commerce Directive*" or "*Directive*").

The e-Commerce Directive, unchanged since its adoption in 2000, provides a horizontal legal framework for digital services[2] in the Internal Market by harmonising the basic principles and thereby allowing the cross-border provision of digital services. The Directive has been a foundational cornerstone for regulating digital services in the EU.

At the same time, the advent of internet and digital services revolutionised the everyday lives of Europeans in a way often compared to the industrial revolutions of the previous centuries. The digital technologies are profoundly changing European citizens' daily life, their way of working and doing business, and the way they travel, consume cultural or entertainment content and communicate with each other.

Yet, it does not stop there. Digital technologies, business models and societal challenges are evolving constantly and with ever-increasing pace. The wider spectrum of digital services is the backbone of an increasingly digitised world, which incorporates a wider range of digital services, such as cloud infrastructure or content distribution networks. Online platforms like market places, social networks, or media-sharing platforms intermediate a wide spectrum of activities and play a particularly important role in how citizens communicate, share and consume information, how businesses trade online, and which products and digital services are offered to consumers.

Since the entry into force of the Directive, the Commission has gathered evidence indicating that the Directive has removed series of obstacles to the cross-border provision of digital services.[3] But recent evidence also shows that the Directive may not have fully achieved its objectives and that the issues relevant today, especially given regulatory, market and technological developments, may not all be addressed by the Directive.

---

1 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 ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

2 The term 'digital service' is used interchangeably here with 'information society service', defined as '*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'* (Directive (EU) 2015/1535)

3 Commission Communication of 11 January 2010 to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM(2011) 942 final.

The political guidelines of the President of the Commission announced her intention to put forward a Digital Services Act, to *'upgrade our liability and safety rules for digital platforms services and products, and complete our Digital Single Market'*.[4]

In its *Strategy on Shaping Europe's Digital Future*[5], the Commission announced that it intends to propose new and revised rules to deepen the Internal Market for digital services, by increasing and harmonising the responsibilities and obligations of digital services and, in particular, online platforms and reinforce the oversight and supervision of digital services in the EU.

In light of this, it is prudent and necessary to evaluate provisions regulating digital services in the Internal Market to assess whether they are still fit for purpose given the recent regulatory, market and technological developments in the last two decades.

In June 2020, the Commission therefore published combined Evaluation Roadmap/Inception Impact Assessment outlining its plan for the evaluation.[6] The purpose of the evaluation is to gather evidence on the functioning of the e-Commerce Directive, which will serve as a basis for the Commission to further define the problem analysis and the policy options and to compare their impacts in the Impact Assessment.

This evaluation systematically reviews and analyses all available evidence, from a variety of sources, which include information shared by the concerned stakeholders. It builds on detailed evidence gathered over the past years, in particular concerning the legal assessment of current implementation of the e-Commerce Directive and evidence of emerging legal fragmentation. In addition, it takes into account more granular data that is being collected regularly on specific types of illegal content and goods in the context of the structured dialogues and voluntary cooperation coordinated by the Commission on several policy areas. These area include unsafe products, illegal hate speech, child sexual abuse material (and related cooperation between law enforcement, hotlines and industry), counterfeit products, dissemination of terrorist content, amongst others.

Evaluation results will directly inform future policy decisions. They provide a starting point for a possible revision of the e-Commerce Directive.

This evaluation does not deal with the impact of the COVID-19 outbreak, given that these developments are very recent and the evidence gathered in the evaluation could not take them into account. Moreover, the duration and impact of the COVID-19 crisis cannot be predicted at the current stage, and it is therefore not possible to evaluate the effects of the COVID-19 crisis on the rules subject to the evaluation.

---

4 A Union that strives for more, *My agenda for Europe: political guidelines for the next European Commission 2019-2024*, https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1.

5 Digital Strategy "*Shaping Europe's Digital Future*" of 19 February, 2020 https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

6 *Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services*, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

1.2. Past evaluations of the e-Commerce Directive

Since the adoption of the e-Commerce Directive, the Commission adopted several policy documents concerning the evaluation of the e-Commerce Directive and more generally EU rules seeking to facilitate well-functioning internal market for digital services.

In its 2003 Evaluation Report[7], the Commission concluded that the Directive has had a substantial and positive effect on e-commerce within Europe. Together with the Directive on transparency for information society services[8], which establishes a mechanism allowing the Commission to assess draft national legislation as to its compatibility with EU law, it creates a straightforward internal market rules, which allows e-commerce to grow across national borders.

In its 2012 Communication on "*a coherent framework to build trust in the digital single market for e-commerce and online services*"[9], the Commission found that the principles and the rules of the e-Commerce Directive continue to be sound, but that some improvements were needed, in particular regarding the functioning of the notice-and-action systems. To this end, the Commission also organized a public consultation concerning procedures for notifying and acting on illegal content hosted by online intermediaries.[10]

Finally, in its 2016 Communication on "*online platforms and the digital single market opportunities and challenges for Europe*", the Commission found again that the principles and the rules of the Directive were sound. However, the Commission also observed the increasing importance of online platforms and identified several new risks that may lead to further fragmentation of the digital single market. To this end, the Commission adopted in 2017 the *Communication on tackling illegal content online*[11], which was followed by the 2018 Recommendation on tackling illegal content online[12].

1.3. Scope of the evaluation

The substantive scope of the evaluation includes the e-Commerce Directive in its entirety. Within this context, the evaluation specifically focuses on the following areas:

---

7 *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of 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 (Directive on electronic commerce)*, COM/2003/0702 final.

8 At the time, Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 204, 21.7.1998, p. 37–48. Now Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance), OJ L 241, 17.9.2015, p. 1–15.

9 See reference in footnote 3.

10 Outcome of the public consultation available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-4/consultation_summary_report_en_2010_42070.pdf.

11 Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, *Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms*, COM(2017) 555 final.

12 Commission Recommendation on measures to effectively tackle illegal content online, C(2018) 1177 final.

a. Functioning of the Internal Market for digital services, including functioning of the cooperation mechanism between the competent authorities of the Member States.
b. Liability of online intermediaries that manage content provided by third parties that use their services (e.g. internet service providers; cloud services; web hosts; online marketplaces).
c. Other measures setting the basic regulatory requirements for digital services in the Internal Market, in particular the ones concerning commercial communications and online advertising as subset of it.

The temporal scope of the evaluation covers the period since the adoption of the Directive in 2000.

The geographic scope of the evaluation extends to all EU Member States.[13]

As required by the Commission's Better Regulation Guidelines, the evaluation examines whether the objectives of the e-Commerce Directive were met during the period of its application (*effectiveness*) and continue to be appropriate (*relevance*) and, whether the e-Commerce Directive, taking account of the costs and benefits associated with applying it, was efficient in achieving its objective (*efficiency*). It also considers whether the e-Commerce Directive as legislation at EU level provided added value (*EU added value*) and is consistent with other pieces of the EU legislation relevant for the provision of digital services in the Internal Market (*coherence*).

2. BACKGROUND TO THE INTERVENTION

2.1. Grounds for the intervention

The e-Commerce Directive is the legal framework for information society services in the internal market.

In 1990s and in the wake of the establishment of a well-functioning internal market, the Commission also considered it important to facilitate a growth of the electronic commerce that was providing a unique opportunity to create economic growth, a competitive European industry and new jobs.

Within this context, the Commission identified several obstacles to the potential economic growth that required attention:[14]

i. Lack of legal certainty

The preparatory work pointed to significant differences in certain legal provisions applicable to information society services in different Member States. These differences meant that an information society service provider wishing to offer a service throughout the internal market had to comply not just with the legislation of a Member State in which it is established but also all other Member States to which it direct its activity.

[13] Since the e-Commerce Directive was fully applicable in the United Kingdom during the period under review, the evaluation includes evidence gathered in relation to the United Kingdom.

[14] Proposal for a European Parliament and a Council Directive on certain legal aspects of electronic commerce in the internal market, 18 November 1998, COM(1998)586 final.

In addition, several Member States were in the process of enacting new legislation, analysis of which showed difference in approaches and risk of fragmentation of the internal market. In particular, legal interventions at national level on liability of intermediary services considered instrumental for the exchange of views on line hampered the development of a rising use of online services, and detrimental for the free expression of views online.

ii. Significant economic costs

The analysis at the time showed that the existing legal framework gives rise to significant costs for operators wishing to develop their activities across borders. The survey undertaken pointed to significant legal costs due to the differences in national legal regimes and need to comply with often very diverge national legal requirements.

iii. The chilling effect on investment and competitiveness of the European companies

In view of the complexity of the legal framework and associated economic costs it has been considered that operators, particularly SMEs and microenterprises, who are unable to afford high-quality legal advice, are discouraged from exploiting the opportunities afforded by the internal market and investing in the European development of their businesses.

This was considered also a disincentive for investment in innovation and factor that could lead operators to design their services in a manner to meet the requirements of the most severe national legal requirements. This subsequently meant that some SMEs and microenterprises are less competitive than businesses with the funds to invest in an evaluation of the risks of securing access to the new market in electronic commerce while remaining within the law. .

iv. The lack of confidence on the part of consumers

Finally, it has also been consider that consumers, and more generally, recipients of services may feel that they are in an unclear and vague situation with few guarantees as to the level of protection afforded under different national rules. They may therefore be unwilling to conclude on-line contracts and exploit new opportunities. or express their views online.

Beyond a general objective of establishing an internal market for electronic commerce there were two further drivers of regulatory changes. First, several reports at the time showed that Europe is lagging behind in particular the USA when it comes to the development of e-commerce and digital services. Second, penetration and use of internet has been growing.

2.2. Description of the intervention

The approach of the e-Commerce Directive was to interfere as little as possible with national legal rules and to do so only where it is strictly necessary for the proper functioning of internal market. It has been considered at the time that the Directive does not need to cover complete areas of law and it can therefore target specific aspects.

In addition, the Commission considered that until an international regulatory framework is established, the Directive should only cover service providers who are established in a Member State. The Directive therefore did not cover information society service provided by a service provider established in a third country.

In practice, this meant that service providers who are not established in the Community could not exploit the opportunities afforded by the internal market. To do so, they would have to establish themselves in one of the Member States.

2.2.1. Information society services

The Directive applies to information society services, which encompass any service normally provided for remuneration, at a distance[15], by electronic means[16] and at the individual request[17] of a recipient of services.[18]

Such services may include today:

- A general category of information society services: e-commerce websites selling any type of goods, online encyclopaedias, online newspapers, games, payment services, online travel agents, blogs etc.;
- In particular, a subcategory of information society services considered 'online intermediaries', ranging from the very backbone of the internet infrastructure, with internet service providers, cloud infrastructure services, content distribution networks, to messaging services, online forums, online platforms (such as app stores, e-commerce marketplaces, video-sharing and media-sharing platforms, social networks, collaborative economy platforms etc.) or ads intermediaries.

On the other side, the e-Commerce Directive itself clarifies that it does not apply to some areas and activities, the main ones being taxation, data protection, competition law, and gambling[19] activities.

The below figure provides a simplified overview of the taxonomy of information society services.

Figure 7: Information society services and scope of the e-Commerce Directive

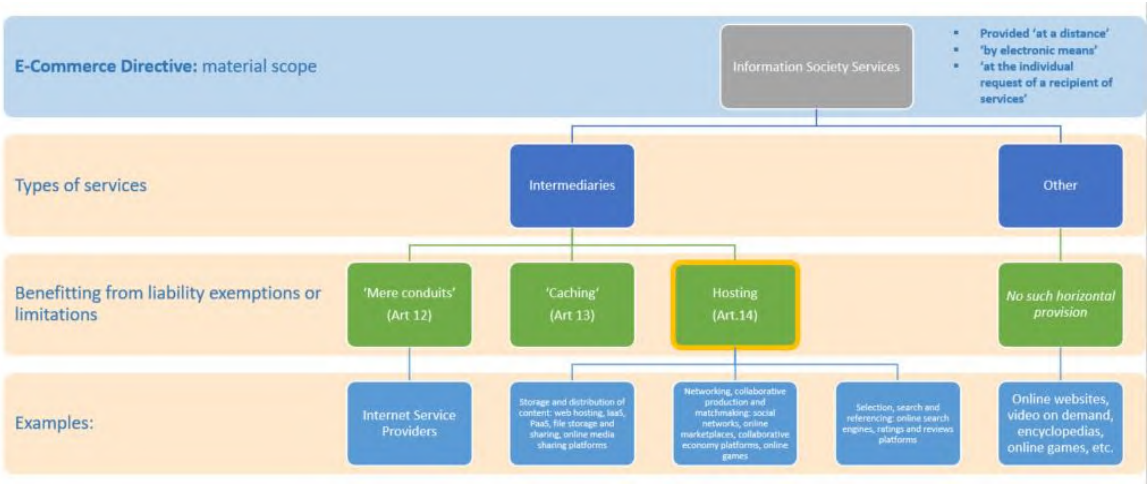
15 Means that the service is provided without the parties being simultaneously present

16 Means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means.

17 Means that the service is provided through the transmission of data on individual request.

18 Article 1(b) of the Directive 2015/1535/EU. The definition had been introduced for the first time in the Directive 98/48 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations.

19 Any activity involving wagering a stake with monetary value in games of chance, including lotteries and betting transactions.



Finally, since many digital services are provided to consumers free of charge, it is important to clarify that this in itself does not mean they would not qualify as information society services (e.g. service provider could be remunerated by advertising revenue)[20].

2.2.2. Geographical scope of application of the Directive

The e-Commerce Directive applies to any information society service provider established in the European Union, but does not apply to information society services supplied by service providers established in a third country.[21]

2.2.3. Core elements of the e-Commerce Directive (i.e. core regulatory pillars)

Freedom to provide services (Article 3) and freedom of establishment (Article 4)

One of the core provisions of the e-Commerce Directive is the **internal market clause**[22]. It establishes that:

i. providers of "*information society services*" are subject to the law of the Member State of their establishment ("***internal market principle***"),

ii. the Member State of establishment needs to ensure that the service comply with the national provisions applicable in the Member State in question which fall within the "***coordinated field***"[23], and

20 See further information in section 3.5 below.
21 Recital 58 of the e-Commerce Directive.
22 Article 3 of the e-Commerce Directive.
23 Requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them. The coordinated field therefore includes all laws (harmonised or not at EU level) which are applicable in the national legal system of the Member State of establishment of the service provider to information society services.

iii. other Member States may only restrict information society services in very specific circumstances and pursuant to the procedure laid down in Article 3(4) of the e-Commerce Directive itself.

This means that as regards the rules covered by the "coordinated field", the provider of information society services can "freely" offer its service across the single market by complying with the rules of the country in which it is established (hereafter "*country of establishment*"). In parallel, none of its host Member States (i.e. Member States where it provides its service; hereafter "*country of destination*") can require the same service provider to comply with additional rules in this Member State. Thus, as a matter of principle the information society service provider cannot face any restriction from another Member State.

Exceptionally, on a case-by-case basis, a Member State of destination can adopt measures to derogate from the internal market principle under strict material (e.g. principle of proportionality; limited list of derogation conditions) and procedural conditions (i.e. notification obligation to the Commission and other Member States).[24]

Furthermore, the single market clause does not apply to eight fields mentioned in the Annex of the Directive[25].

The Directive also ensures the freedom of establishment, by prohibiting so-called prior authorisation regimes specifically and exclusively targeted at information society services in the Member State of establishment.

To address the need for smooth enforcement of the 'coordinated field' across jurisdictions, the Directive provides for a basic information and cooperation mechanism across national authorities, including a requirement for the appointment of one or more points of contacts in relation to the implementation of the e-Commerce Directive. Additional provisions on court actions, sanctions, and injunctions complement these core clauses.

Liability of intermediary service providers (Section 4 of the e-Commerce Directive)

The e-Commerce Directive, in Articles 12 and 13, harmonises the liability exemptions and in Article 14 liability limitations for so-called intermediary services. These range from 'mere conduits' like internet service providers ensuring the very backbone of the network, to 'caching services', and to 'hosting services' which are now understood to cover services such as web hosting, some types of cloud services, online platforms such as online marketplaces, app stores, video-sharing platforms or social networks.

The conditional liability exemptions and limitations cover all types of illegal activities and content, as defined in EU or national law, and provide intermediaries with safe harbour for

[24] Article 3(4) of the Directive.
[25] Article 3(3) of the Directive and Annex.

all legal categories of liabilities, provided they meet certain conditions. Recently adopted Copyright Directive introduces a sector specific regime in this context.

For hosting services (covered by Article 14 of the Directive), the conditionality is two-fold: the provider can benefit from the exemption if it does not have actual knowledge about the illegal activity of content (or, in the case of claims for damages, awareness of facts of facts or circumstances from which the illegal activity or information is apparent), and if, upon obtaining such knowledge or awareness, it 'acts expeditiously' to remove or disable access to the illegal information.

The Directive also clarifies that courts and administrative authorities can require, in accordance with the Member States' legal systems, a service provider to terminate or prevent an infringement if the law of the Member State concerned provides for such a possibility.

Article 15 of the e-Commerce Directive prohibits that Member States impose general monitoring obligations on online intermediaries or a general obligation to actively seek facts or circumstances indicating illegal activity.

Measures protecting users of information society services

The e-Commerce Directive lays down several measures that seek to protect users (e.g. consumers, business users, public authorities) by harmonising certain obligations, primarily concerning transparency requirements imposed on providers of information society services. Such examples of transparency obligations are:

- Obligation on information society service provider to make available its identity, name, geographic address, and details enabling rapid contact, and relevant registration information (in trade or similar registers), VAT number where relevant.
- Obligation to clearly identify commercial communications designed to promote directly or indirectly the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession as well as the natural or legal person on behalf of whom the commercial communication is made.

In addition, the e-Commerce Directive requires that Member States ensure that contracts can be concluded electronically, which means that they must remove legal obstacles which would:

- prevent the use of electronic contracts; and
- deny online contracts legal validity on the ground that they are formed by electronic means.

In this context, the Directive enshrines certain basic principles and transparency requirements as regards the conclusion of contracts by electronic means.

Finally, the Directive encourages the Commission and Member States facilitate the drawing up of codes of conduct at the Union level, by trade, professional and consumer associations or organisations, designed to contribute to the proper implementation of the e-Commerce Directive.

Mechanisms for effective cooperation between Member States and enforcement of the e-Commerce Directive

The e-Commerce Directive also lays down basic principles seeking to ensure effective cooperation between Member States and effective enforcement of the Directive, which is effectively to be carried out by the Member States.

To this end, the Directive envisages that any sanction in case of a violation of the e-Commerce Directive should be effective, proportionate and dissuasive. In addition, the available national court actions should be effective allowing for the rapid adoption of corrective measures, including interim measures.

The Directive also envisages and encourages cooperation and mutual assistance between Member States and with the Commission for the implementation of the Directive, in particular through the establishment of national contact points. Such a cooperation is particularly relevant in view of the envisaged close cooperation between country of origin and country of destination as regards implementation of the internal market principle laid down in Article 3 of the Directive.

Finally, the Directive encourages the use of alternatives enforcement instruments such as codes of conduct at the EU level or out-of-court dispute settlement schemes.

2.3. Objectives of the e-Commerce Directive

The general objectives of the Directive can be summarized as follows:

- Ensuring the freedom of providing digital services in the internal market, leading to **growth and competitiveness in the EU**; and
- Offering consumers a wide-range of choices and opportunities, including by ensuring that the Internet remains **safe, trustworthy, fair and open**.

At the same time, the specific objectives of the Directive can be summarised as follows:

I. Ensuring well-functioning internal market for digital services

- Its main objective is the **proper functioning of the internal market** for information society services. This is emanation of a principle of free movement of services as enshrined in the Treaty. It aims at ensuring the **freedom to provide information**

society services and **freedom of establishment** for the providers of information society services within the single market. This aims to create a pro-competitive environment for business, also across borders, and to enhance choice, affordable products, services and content online and facilitate other opportunities for EU citizens.

This is achieved through the internal market clause[26], which says that information society service providers are subject to the law of their home Member State (i.e. Member State in which they are established), and that other Member States (i.e. host Member States) can restrict their services only in exceptional circumstances[27]. It also establishes a notification and cooperation procedure with the Commission and Member States for those (urgent) cases where host Member States deem necessary to derogate from the provisions of the Directive.

- The prohibition of prior authorisation requirements[28] and the harmonisation of certain consumer-facing rules[29] throughout the Directive contribute to the objective of a well-functioning internal market for digital services.

II. Ensuring effective removal of illegal content online in full respect of fundamental rights

- For information society services acting as *online intermediaries,* the liability provisions of the ECD aim to establish a careful balance between the following objectives

    1. to **promote innovation on the internet**, by shielding intermediaries that transmit or organise 3rd party content from disproportionate liability for each piece of content transmitted or hosted, and from general monitoring obligations related to the content they transmit or store;

    2. to **ensure the effective removal of illegal content** by making the liability exemption conditional on knowledge, but leaving operators free to design their systems to address this objective;

    3. to **safeguard fundamental rights online**, such as freedom of expression and right to privacy, by avoiding over-removal of (legal) content or surveillance, by limiting the scope of the liability provisions to illegal content and by banning general monitoring obligations.

---

26 Article 3 of the e-Commerce Directive.
27 Those circumstances are laid down in Article 3(4) of the Directive.
28 Article 4 of the e-Commerce Directive.
29 For example, Article 5 on information requirements on service providers, Article 6 on requirements concerning the use of commercial communication that is, or form part of, information society services or Article 10 on information requirements on service providers before consumer place an order.

III. Ensuring adequate level of information and transparency for consumers

- A number of provisions of the ECD aim to **enhance trust in digital services.** In particular, they aim to protect consumers and users not only against illegal content and activities, but also from lack of information and transparency when it comes to the nature and identity of the information society service provider, commercial communications (which are part of, or constitute, an information society services), unsolicited commercial communications, or certain pre-contractual or contractual obligations. The objective of promoting trust in online services is also achieved by acknowledging electronic contracts.

The following chart visualises the intervention logic – i.e. the way in which its main legal provisions are meant to contribute to the achievement of well-identified policy objectives - of the e-Commerce Directive.

Figure 8: Intervention logic of the e-Commerce Directive

2.4. Baseline

The baseline describes those developments (throughout the evaluation period) that could have been expected in the absence of the Directive. Any actual effective changes, attributable to the Directive, are measured against this hypothetical baseline scenario. This section describes the previous baseline assumptions of the original intervention and discusses whether any policy or market developments that have occurred since then have influenced these assumptions.

General outline

As shown above, before the introduction of the Directive, some Member States had adopted regulatory measures applicable to different aspects of the provision of information society services. But, where existent, many of these measures were diverging and they were undermining the well-functioning internal market, raised operational costs for service providers and served as disincentive for further investments as well as negatively impacted European competitiveness.

It was expected that absent the regulatory intervention the trend towards regulatory fragmentation would continue[30], which would lead to further increased operational costs for service providers. It was considered that inefficiencies in the digital market would continue, possibly hampering the development of the internal market for information society services, limiting its innovation potential and have a deterrent effect on the competitiveness of the information society service providers.

Internal market principle

In the absence of the e-Commerce Directive the basic principles of the Treaty, in particular principle of free movement of services as enshrined in Article 56 TFEU, would have applied. This means that restrictions in each Member State of reception of information society service could be applicable, to the extent that they are justified based on an overriding reason of general interest (e.g. public policy; public health, but also tax coherence, protection of consumers), are proportionate and non-discriminatory.[31] Moreover, no coordination mechanisms as regards possible requirement for non-established information society service providers would have applied in those cases where the country of destination decided to restrict the provision of information society services cross-border.

As from 2009, the horizontal rules laid down in the Services Directive[32] would have applied for a wide (although not all) range of information society services, including Article 16 with regards to derogations to the freedom to provide services and the more general rules on administrative cooperation. This would have allowed each Member State of reception to make subject service providers established abroad to an open range of possible general requirements (except those explicitly banned) supported by any overriding reason of general interest. Moreover, as regards cooperation between Member States, each Member State where services are received would be entitled to restrict the provision of specific service provider for compliance with applicable national requirements, without obligation to consult and/or inform the Member State of establishment nor the Commission except in specific circumstances. Taking into account the potential accessibility of information society services from any Member State (and often the lack of specific registration to access services and/or limitation[33] of access from other Member States), this could potentially trigger liability for compliance with 27 different legal regimes and enforcement actions.

Liability of intermediary service providers

Before the adoption of the e-Commerce Directive, there were no harmonized EU principles as regards (exemption from) liability for intermediary service providers that provide certain digital service for third parties (e.g. access to the internet infrastructure; storage of information).

In the absence of the e-Commerce Directive - and before the adoption of some sector specific rules concerning liability of intermediary service providers at the EU level (see

30 As shown later in this Evaluation Report, even with the adoption of the e-Commerce Directive trend of regulatory fragmentation has not disappeared, in particular in recent years (see in particular Section 3.2).

31 Article 3(4) of the e-Commerce Directive envisages narrower and closed list of derogations as would in principle be possible under Article 56 TFEU (e.g. protection of workers).

32 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, OJ L 376, 27.12.2006, p. 36–68.

33 Also forbidden by the Geo-blocking Regulation to the extent that it is unilaterally decided by the trader.

section 3.3 below and Annex 6 of the Impact Assessment for detailed information about these developments) – the question of possible (exemption from) liability would be governed by each Member States' own legislation.

Since at the time of the adoption of the e-Commerce Directive several Member States have already adopted, or at least considered adopting, legislation in this area, it is very likely that the fragmentation of the rules in this area and therefore legal uncertainty would further increase. In addition, while it could be expected that some of the issues at the national level would have been submitted via preliminary ruling references to the CJEU, hence unifying interpretation, this in itself is unlikely to have significantly positive effects on tackling an increased trend of regulatory fragmentation.

For the internal market these divergences could be the source of further obstacles for the cross border provision of information society services (e.g. if a country of destination decides to disable access to information stored in the server of a service provider established in another Member State where the applicable liability regime is deemed to be unsatisfactory). In some Member States, such fragmentation may hinder activities such as the provision of hosting.

In the 2017, Communication and 2018 Recommendation the Commission clarified the e-Commerce Directive by laying down the soft law framework concerning tackling illegal content online. The objective of the two policy instruments was to improve the effectiveness and transparency of the notice-and-action process between the users and the hosting service providers, incentivize voluntary measures by hosting service providers, and increase cooperation between providers of hosting services and the specific stakeholder, such as trusted flaggers and public authorities.

Finally, this baseline regime of the e-Commerce Directive has been across the years complemented for a particular type of illegal material by sectoral rules and co/self-regulatory measures. Such rules and measures have been adopted in areas such as child sexual abuse material online, terrorist related content, audio-visual media services or copyright (see section 3.3 below and Annex 6 of the Impact Assessment for further details about these developments).

Protection of users of information society services

Before the adoption of the e-Commerce Directive there were already several user protection measures in place at the EU level.[34] Having said that, the preparatory work for the e-Commerce Directive pointed to several open questions both as regards possible rights of users as well as obligations of information society service providers when providing such services.

These issues in particular concerned the use of commercial communications that may in themselves constitute information society services or form part of it, including in relation to provision of regulated services, and the ability to conclude contracts by electronic means.

In the absence of the e-Commerce Directive it could be expected that Member States would continue with their legislative initiatives in relation to both sets of issues identified above,

[34] See in particular recital 11 of the e-Commerce Directive.

which would likely lead to further regulatory fragmentation, at least until further harmonization initiatives may have been adopted at the EU level.

Within this context, it should be noted that also that since the adoption of the e-Commerce Directive in 2000, the EU has been the strengthening and further harmonizing consumer protection, in particular with the adoption of the Unfair Commercial Practices Directive[35] in 2005 and the Consumer Rights Directive[36] in 2011. In 2019, both of these Directives were revised by the Omnibus Directive[37] to improve their enforcement and better adapt the protection of consumer in the digital age.

These Directives complement the e-Commerce Directive and ensure complementary protection of the users of the information society services when they act as consumers, i.e. for purposes outside their trade, business, craft or profession.

On the other side of the spectrum, the protection of business users has been strengthened through the adoption of the Platform-to-Business Regulation[38] in 2019. This Regulation imposes a series of transparency obligations in favour of the business users when dealing with providers of information society services offering intermediation or search services. It furthermore imposes the establishment of specific enforcement mechanisms such as internal complaint-handling system, mediation and collective actions.

Finally, the data protection rules, which have also been specifically referred to in the e-Commerce Directive, have also been revised and strengthened in 2016. The new General Data Protection Regulation[39] re-confirms the main rights of the data subjects of the previous regulatory framework and creates new ones, in particular the right to be forgotten, right to data mobility and right of explanation for automated decisions.

Mechanisms for effective cooperation between Member States and enforcement of the e-Commerce Directive

35 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 and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance), OJ L 149, 11.6.2005, p. 22–39.

36 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304, 22.11.2011, p. 64–88.

37 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1, OJ L 328, 18.12.2019, p. 7–28.

38 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance), PE/56/2019/REV/1, OJ L 186, 11.7.2019, p. 57–79.

39 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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

At the time of the adoption of the e-Commerce Directive, which introduced a specific cooperation mechanism in Article 3(4), there were no mechanisms in place to facilitate coordination between Member States when enforcing EU or national rules that may have an impact on the cross-border provision of information society services.

This uncertainty as to "*who supervises what*" was considered an important hindering factor for the development of the internal market and free movement of free movement of information society services. In particular, it was considered that it would be necessary to improve *the level of mutual confidence between* national authorities.

Since the adoption of the e-Commerce Directive, and its cooperation mechanism in Article 3(4), several additional sector and/or issue specific cooperation mechanisms have been set up since 2000. The main purpose of these was to facilitate the cooperation and mutual assistance between the competent authorities of the Member States in the specific areas concerned (e.g. dangerous goods; consumer protection). The most relevant in the present context are:

- The **expert group on electronic commerce**, which was set up in 2005 and is composed of the different national contact points and chaired by the Commission;
- The **Consumer Protection Cooperation (CPC) Network**, which was established in 2006 and is composed of the national consumer protection authorities;
- The **rapid alert system for dangerous non-food products** (i.e. Safety Gate), which was set up in and facilitates the rapid exchange of information between national authorities and the European Commission on dangerous products found on the market.

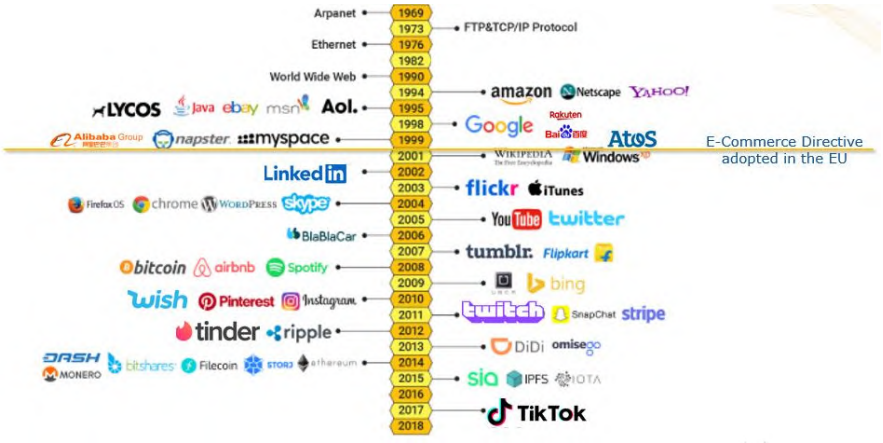
At the same time, the **Internal Market Information (IMI) System**, which is a multilingual secure online application to facilitate communications and support cooperation between the competent authorities of the Member States, has been set up as an underlying technical facility to support different cooperation mechanisms.

3. IMPLEMENTATION / STATE OF PLAY

3.1. Market context and developments

Digital services have developed tremendously over the past 20 years since the adoption of the e-commerce Directive in 2000, becoming an important backbone of the digital economy and supporting fundamental societal digital transformations. The below figure in a simplified manner shows how some of the today's most prominent digital services or business models were already there in 2000; however, the scale and impact of old and newly arrived services have expanded to all pores of the society.

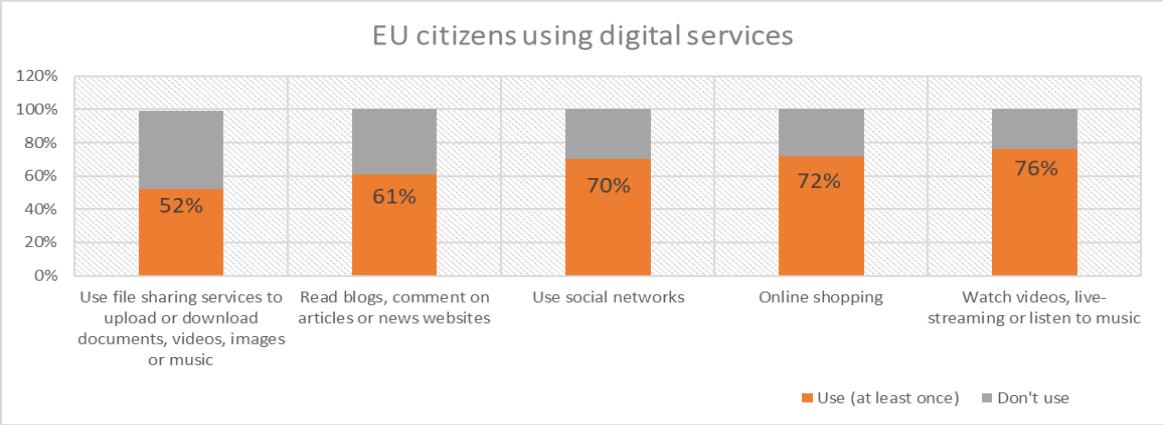
Figure 9: Development of digital services (example)



The landscape of digital services is by no means static: it continues to develop and change rapidly along with the technological transformations and innovations increasingly available. For example, services providing the technical infrastructure for the internet are diverse and important for the development of various sectors, such e-commerce, connectivity, cloud services or advertising. The Court of Justice has not hesitated to apply the e-Commerce Directive provisions to some services (and business models) that did not exist when it was adopted.

The below table shows how widely different digital services, in particular different forms of online platforms, are used by the European citizens.

Table 1: Use of digital services by EU citizens



However, an important trend that is different from the beginning of the century is the increasing "platformisation" of the online space. While the rise of the "2.0" services, allowing users to publish, comment, buy and sell directly led to dis-intermediation of the traditional economy channels, the last decade has witnessed an important re-intermediation of the online economy. These intermediation services, widely known as online platforms are widely used in Europe; 76% of Europeans said in 2018 that they were regular users of video-sharing or music streaming platforms, 72% shopped online and 70% used social networks. In addition, more than 1 million EU businesses already selling goods and services via online platforms and more than 50% of SMEs selling through online marketplaces sell cross-border.

3.1.1. Increased exposure to illegal activities online

With such an exponential increase in the use of digital services and the opportunities for information sharing and electronic commerce, came also the increasing misuse of intermediary services for various types of illegal activities, such as:

- **dissemination of illegal content**, such as illegal hate speech, child sexual abuse material, terrorist content, IPR infringing content);
- **illegal sale of goods**, such as sale of dangerous goods, unsafe toys, illegal medicines, counterfeits, scams and other consumer protection infringing practices, or even wildlife trafficking, illegal sale of pets or protected species); or
- **illegal provision of services**, such as non-compliant accommodation services.

For example, for dangerous products, the Rapid Alert System for dangerous non-food products (Safety Gate/RAPEX) registers between 1850 and 2250 notifications by Member States per year[40].I In 2019, around 10% were confirmed to be also related to online sales[41], while the likely availability of such products online is very likely higher. In this regard, the COVID-19 crisis has also cast a spotlight on the proliferation of illegal goods online (e.g. products falsely presented as able to cure or prevent COVID-19 infections or bear false conformity certificates, etc.), especially coming from third countries.

Another example, for child sexual abuse material, the past few years have seen an increase in reports of child sexual abuse online concerning the EU (e.g. images exchanged in the EU, victims in the EU, etc.): from 23 000 in 2010 to more than 725 000 in 2019, which included more than 3 million images and videos.[42]

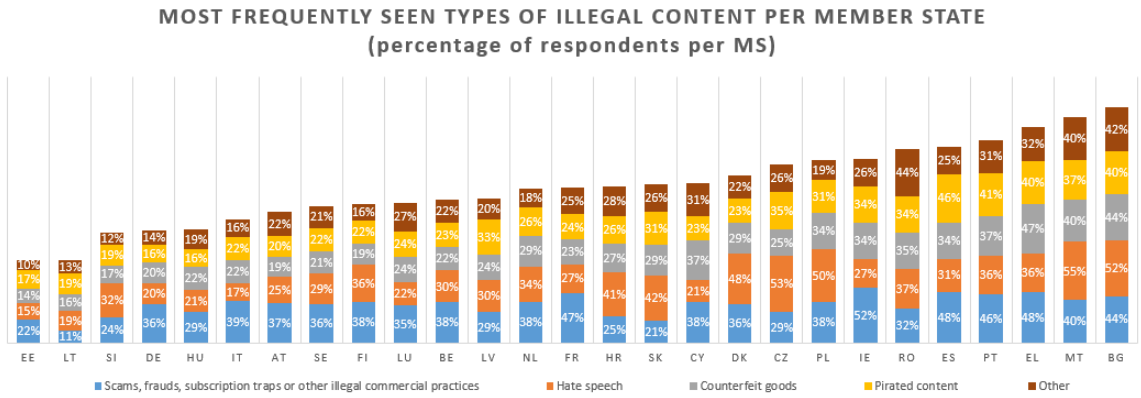
To assess the size of the problem, the Commission ran a Flash Eurobarometer survey among a random sample of over 30 000 Internet users in all Member States, testing user perception of the frequency and scale of illegal activities or information online. The below figure shows most frequently seen types of illegal content per Member State.

40 https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm

41 Member States have the possibility to indicate in their notifications if they are aware if the unsafe product has been sold online. However, if not indicated, that does not necessarily mean that such product is not available online.

42 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *EU strategy for a more effective fight against child sexual abuse*, COM(2020) 607 final.

Figure 10: Most frequently seen types of illegal content per Member States



In this context, it is important to note that not all types of illegal activities are appropriately addressed. For example, for certain types of illegal activities, the post-e-Commerce Directive adopted legislation, laid down a series of adapted obligations on online intermediaries, defining the specific responsibilities in areas such as:

- child sexual abuse material;[43]
- terrorist offences online;[44]
- copyrighted content;[45]
- explosive precursors;[46]
- other types of illegal products subject to market surveillance[47]; or
- for the specific case of audiovisual content on video-sharing platforms, the Audiovisual Media Services Directive[48], currently being transposed by Member States.

The respondents to the open public consultation referred to different types of illegal and harmful activities and information that they perceive are increasingly exposed to.

---

43 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, OJ L 335, 17.12.2011, p. 1–14.

44 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, OJ L 88, 31.3.2017, p. 6–21.

45 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 (Text with EEA relevance.), PE/51/2019/REV/1, OJ L 130, 17.5.2019, p. 92–125.

46 Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 (Text with EEA relevance), PE/46/2019/REV/1, OJ L 186, 11.7.2019, p. 1–20.

47 Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance.), PE/45/2019/REV/1, OJ L 169, 25.6.2019, p. 1–44.

48 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, PE/33/2018/REV/1, OJ L 303, 28.11.2018, p. 69–92.

The main issues reported by the respondents in relation to goods are: deceptive advertising especially on food, food supplements and drugs, also COVID related, advertising on pet and wildlife trafficking or counterfeit and defective (and even stolen) goods, electronics and clothes.

Regarding services, the main issues raised by the respondents are: fake event tickets or cases in which platforms illegally re-sell tickets and inflate their prices, cryptocurrencies and trading online or general cases of phishing.

Finally, in relation to content, the respondents report significant issues related to hate speech (e.g. racism, anti-Semitism, white supremacy, calls against migrants and refugees, extremism, far-right propaganda, homophobia, sexism, defamation), general incitement to violence, unwanted pornography and prostitution ads, child sexual abuse material, IP infringement for movies and copyrighted other content or political disinformation and fake news.

The vast majority of users that replied to the open public consultation are not satisfied with the actions that platforms take to minimise risks for consumers to be exposed to scams and other unfair practices. The users mostly consider that platforms are doing very little and not enough to prevent these issues from happening.

For some categories of illegal activities, such as hate speech, dangerous products or counterfeits, the Commission has facilitated self- and co-regulatory efforts in cooperating with national authorities and/or trusted third parties to address concerns identified.

Yet many categories of illegal content, goods or services are outside the scope of such interventions and there is no set process for tackling them.

The only horizontal document addressing all types of illegal activities horizontally is the Commission's Communication from 2017 and, as a non-binding legal act, the Recommendation of 2018, which sets guidelines for all hosting services for any type of illegal activity in efforts to curb illegal activities online. However, this instrument and measures identified therein are only selectively applied by some hosting service providers and by Member States.

3.1.2. Lack of information or awareness for addressing other risks online

Since the adoption of the e-Commerce Directive, the volumes of information and commercial offers available online have increased tremendously, resulting in some information society service providers (e.g. online platforms) becoming important players in the 'attention economy'. They increasingly not only intermediate access to information and business offers, but also optimise the discoverability of the most relevant information for each of their users individually. Today, there is virtually no online service, website or app that does not make some decisions on what they consider relevant to each of their users, and that defines criteria for matching the information they present to their users. This includes ranking systems on embedded search functions (or on search engines), recommender systems, and, indeed, more or less complex advertising placement services, including micro-targeting.

Where wide audiences can be reached, potential negative effects of such information amplification systems are more prominent. These negative effects may be manifold,

reaching from amplification of illegal content through such systems to the amplification of content, which is not *per se*, illegal, but may be harmful[49].

During the open public consultation, users expressed mixed views as regards the understanding of whether they know why certain content or products is recommended to them. Some consider that it is hardly impossible to understand why a certain product/content is addressed to them, while others consider that what they see is related to other products they bought, searches done on the platform and on the web (cookies). Users are unhappy about the fact that they are not provided with information on their behaviours that are tracked on the web and how their data is used to build recommendation algorithms.

Furthermore, several digital users' associations have pointed to the fact that, beyond the hosting of illegal content, the actual problem is the dissemination of it through algorithms predicated on increasing platform engagement, not the health, safety, and wellbeing of the user. Algorithms seem to promote content with a high level of engagement and often disregard the fact that this content might be inciting violence or misinformation.

While the reflections and evidence on the extent of the possible issues and harms is evolving, there are several problems cutting across such systems:

- Users lack meaningful information about how these systems function and they do not have any possibility to influence them.
- There are very few ways of researching and testing the effects of such systems. Most of the evidence and information about harms relies on the investigations and willingness cooperate of information society service providers themselves.

3.2. Transposition and implementation of the Directive

3.2.1. General outline

The e-Commerce Directive entered into force on 8 June 2000 and the deadline for its transposition was 17 January 2002.

Whilst compliance with the Directive's requirements are to be primarily controlled by the competent national enforcement authorities, the Commission has monitored on a regular basis the transposition and application of the Directive by individual Member States (see also section 1.2 above for information about past evaluations of the Directive).

The Commission's experience with the implementation of the e-Commerce Directive shows that the majority of the Member States have largely literally transposed the provisions of the Directive itself and to date there were only few cases where the Commission was required to assess the compliance of the national implementing measures with the e-Commerce Directive. None of these cases led to a referral of a Member State in question to the Court of Justice for non-compliance with the e-Commerce Directive.

[49] For example, extreme selfies and instigation to violence or self-harm (harmful in particular to children), conspiracy theories, disinformation related to core health issues (such as the COVID-19 pandemics) or political disinformation. The same amplification tools can also tilt consumer choice on marketplaces, for instance, with little awareness of the consumers.

Having said that, in particular the experience from the notifications of national legislative measures under the Transparency Directive, points to an increasing number of national measures that result in legal fragmentation of the rules applicable to information society services providers in the internal market, raise questions of compliance and hinder the cross-border provision of information society services.

This concerns in particular the compliance with the internal market principle laid down in Article 3 of the e-Commerce Directive, which was one of the main elements of comments of the Commission in the notifications applicable to information society services of national measures under the Transparency Directive. It also concerns compliance of increasing number of national legislative measures with Article 14 of the e-Commerce Directive.

3.2.2. Extraterritorial application of national laws and fragmentation of the internal market for information society services

The Commission observes in the last few years, in particular through the notifications on national measures applicable to information society services under the Transparency Directive, an increasing trend of the regulation of information society services in Member States. This is mainly true as regards the duties and obligations for online platforms to address content hosted in their services that would be illegal under national law.[50]

Some of the recent national measures adopted by Member States in this regard aim to apply to any provider of hosting services with a distinctive presence in their national territory, irrespective of its place of establishment. This means that under these national laws the country of destination would also be competent to supervise compliance of the relevant services with the applicable national rules and obligations including, where foreseen in the law, to impose cross border sanctions.

Member States have justified the adoption of national laws with cross-border application on the need to protect their citizens against the rise of illegal content being intermediated on hosting services. They claim the regime set out in the e-Commerce Directive, and in particular the available derogations from the internal market principle, do not cover these practices or is not sufficient to ensure the protection of their national users in view of the realities of the online environment.[51]

In the absence of harmonized obligations for online platforms to address this issue, this situation is prompting Member States to put forward new initiatives aimed at protecting their citizens from illegal content online. Regardless of the legitimacy of the policy goal, the extraterritorial application of most of these national measures to online platforms established outside the concerned Member States adds to the existing legal fragmentation in the internal market.

---

50 For more detailed examples of such national measures see Annex 5 of the Impact Assessment.

51 This is not to say that in certain circumstances such national measures are not considered incompatible with the EU law, as some recent examples show (e.g. judgement of the Conseil d'Etat in case of Avia Law: https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm; expert opinion of the Research Services of the German Bundestag concerning proposed Hate Speech Law (NetzDG): https://international.eco.de/presse/eco-legal-expert-opinions-on-german-hate-speech-law-confirm-internet-industry-concerns/).

Respondents to the open public consultation point to several issues, which are stifling the development of internal market for digital services such as legal fragmentation and definitional vagueness, jurisdictional conflicts or lack of regulatory consistency.

3.2.3. Cooperation between Member States and lack of clarity on the use of appropriate cooperation mechanism

General outline

The evaluation shows that the competent authorities have difficulties in supervising information society services, in part because they lack the necessary data and information, in part due to a lack of capability and technical resources. The evaluation points to several issues:

- First, the experience points to instances of lack of cooperation and trust among authorities and assistance mechanisms provided by the E-Commerce Directive are underutilized by Member States (see analysis further below). In some instances, Member States preferred the avenue of national legislation fuelling the legal fragmentation with important costs on service providers and an unequal and inefficient protection of European citizens, depending on the Member State where they reside.
- Second, authorities lack data and information, as well as means to gather such evidence, and lack technical capability for processing and inspecting technically complex services. Similarly, they lack means for supervising the underlying activity intermediated by online platforms. For example, in the area of collaborative economy in the accommodation sector, complaints from cities mainly relate to access to data requests which often go unanswered by online platforms that facilitate interaction between provider of an accommodation services and consumer. These are often refused on the basis of GDPR or are not satisfied due to the inefficient cooperation mechanism with the country of origin. Finally, aggregate data that these online platforms may be providing or publishing do not address Member States' need for specific individualised data.
- Third, several authorities within each Member State are responsible for supervision of the different aspects of the information society services. In the targeted consultation of Member States, eight of them pointed to the multiple mechanisms for sending and receiving requests for investigation in various areas such as consumer protection or audiovisual content, and the need for clarity and ensuring timely cooperation within and across instruments (see further analysis of the issue below).
- Fourth, the evaluation shows that the competent authorities often have very few, if any means, to intervene when services are established outside the EU, while they can easily be used by the European consumers.

Functioning of the existing cooperation mechanisms

Compared to the 2012 e-Commerce Directive "*implementation report*"[52] the application of the internal market principle, the features of the cooperation mechanism and the effects of notification have been subject to some developments.

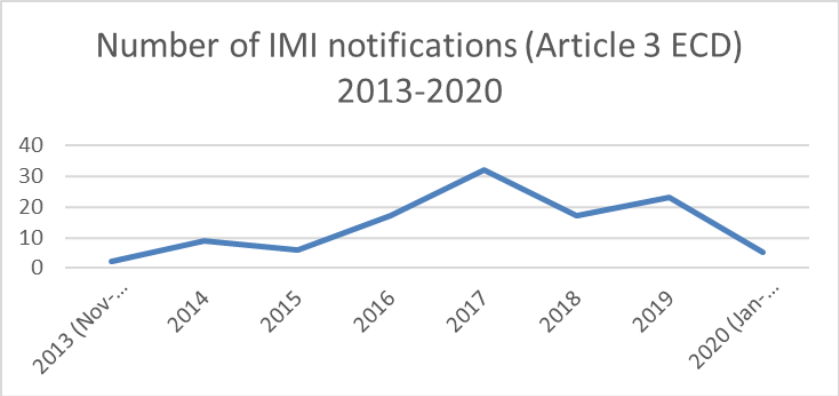
[52] Commission Staff Working Document, Online services, including e-commerce, in the Single Market, SEC(2011)1641 final.

First of all, pursuant to Article 29(3) of the IMI Regulation[53] a pilot project has been launched since 2013 with a view to evaluate the use of the IMI information system as an efficient, cost-effective and user-friendly tool to implement Article 3(4), (5) and (6) of the c-Commerce Directive. Since 2013 requests to take measures from authorities of country of destination to the country of origin of the service provider, as well as those to the Commission and country of origin notifying the intention to adopt measures derogating from the internal market principle in view of insufficient or lack of measures by the country of origin, are normally channelled through IMI. This pilot project aimed at ensuring a comprehensive platform for notifications between Member States and the Commission, even if few individual cases have been reported where notification has been done through other means, as this tool is not specifically mandated in the e-Commerce Directive.

Within this context the trend identified in the 2012 e-Commerce Directive "implementation report", showing a very low number of notifications (approximately 30 in the first 9 years), partially evolved, even if the number remain low compared to the extent of cross-border on-line activities[54].

Between 2013 and July 2020, 111 notifications have been filed with the Commission, with a request to derogate from the internal market principle[55].

Figure 11: Number of IMI notifications



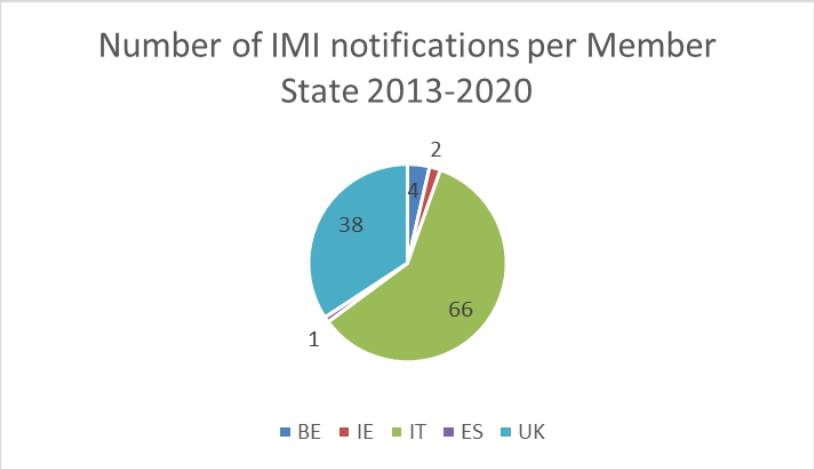
Still, the use of the platform appears quite concentrated with a handful of Member States having used it and an overwhelming number of notifications originating by only two Member States (Italy and, at the time, the United Kingdom, the latter only concerning value-added phone services).

[53] Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation').

[54] For example, in 2018 almost 10% of all EU enterprises sell on-line across the border, see Eurostat E-commerce data (2020) https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200420-1.

[55] Direct contacts between Member States to inform the county of origin of the issue, before notifying the intention to take measures, are also channelled through IMI and they are supposedly more, as in a number of cases the issue is addressed by the country of origin. However, the 2019 survey suggests that a majority of Member States did not take measures following the notification from the country of destination.

Figure 12: Number of IMI notifications per Member State



In the majority of cases (57), moreover, the urgency procedure is activated, in spite of the fact that this should be used only in exceptional circumstances. All notifications, moreover, are justified on the basis of the protection of consumers (only in a couple of cases accompanied with protection of health), for which also another cooperation mechanism is available for the enforcement of EU consumer protection legislation under the Consumer Protection Cooperation (CPC) network, whose new provisions[56] became applicable as from January 2020 and whose cooperation mechanism is, as from 2020, also hosted by the IMI platform.

Finally, no decision has been adopted by the Commission so far as regards the measures adopted, taking also into account that these are normally very much linked to the specific facts at stake. It is not clear, however, whether a relatively low number of notifications reflects a very limited number of cross-border issues or rather an under-utilisation of the tool by some or all authorities in different Member States.

Surveys among the competent authorities in the context of the evaluation of the pilot ECD-IMI project show that awareness and utilisation of the tool is very different among Member States and, within Member States, among different competent authorities. Out of 26 Member States replying to the survey in 2019, 10 never used the tool; moreover, a majority of responding MS (11), while supporting the use of IMI, suggested to improve support and awareness of the system.

More generally, some issues for clarifications are highlighted by some Member States participating to the survey, and in particular the interrelationship with other cooperation systems, and in particular the CPC cooperation network, as well as the kind of measures to be notified and the interrelationship with other notification systems (such as TRIS). Moreover a majority of responding Member States (16) expects that the current practice of national authorities will change, following the recent ruling of the Court of Justice in the *AirBnB* case.

[56] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance), OJ L 345, 27.12.2017, p. 1–26.

The lack of notification under Article 3 of the e-Commerce Directive have also been recently clarified by the Court of Justice in the context of the Airbnb case[57] (C-190/18), where the court stated that "*an individual may oppose the application to him or her of measures of a Member State restricting the freedom to provide an information society service which that individual provides from another Member State, where those measures were not notified in accordance with that provision*". This hence provides for the non-enforceability of measures where Member States failed to notify them according to Article 3(4) of the e-Commerce Directive.

At the same time the Court, while confirming that the notification is due also for provisions predating the e-Commerce Directive, did not clarify which and when measures are to be notified, nor the interrelationship with other notification systems such as that provided for by the Transparency Directive. While some aspects may be further specified in the forthcoming judgement on on-line pharmacies[58], currently the e-Commerce Directive does not provide any indication.

During the meeting of the e-Commerce expert group in October 2019, the issues of cooperation and use of IMI were discussed as well. Despite the differences in the use of IMI, Member States widely expressed the need to have a functioning, strengthened but also simple cooperation mechanism in the future, as this is important to ensure public interests in cross-border issues.

In the context of the evidence gathering for the purposes of the present evaluation the Commission sent also a targeted questionnaire to Member States enquiring about the national experiences on the e-Commerce Directive in the wider framework of challenges and opportunities brought forward by the evolution of digital services.

Overall, 21 replies from 17 MS (in one Member State 5 authorities replied) were received. Concerning the functioning of the cooperation mechanism and the COO enshrined in the ECD, different aspects are stressed, taking also into account that a number of authorities (7) did not report direct experience of the system in sending and/or receiving cooperation requests.

A number of Member States expressed dissatisfaction with the average timing or quality of the feedback (ES, LV, AT, DE) received by other authorities. The cooperation was considered to work better in issues harmonised by EU law (consumer protection, transparency requirements). Some Member States reported concerns about the use of the system in the application of national requirements, for which the country of origin might not have corresponding powers to enforce the request.

Eight Member States highlighted the parallel use/existence of specific cooperation systems alongside that of the e-Commerce Directive, for both sending and receiving requests of investigation (e.g. CPC Network).

According to some Member States, the low number of cooperation requests is explained by the low awareness of the system (EL) but also by the well-functioning system of injunctions/N&A, ensuring removal of illegal content by the provider directly (LU). Few

[57] Case C-390/18 *Airbnb Ireland UC*, ECLI:EU:C:2019:1112.
[58] Case C-649/18 A () and vente de médicaments en ligne).

MS (DE, AT) indicate in any case an increasing trend of cross-border issues, in particular as regards content.

In view of the significant consequences of the failure to notify on the individual acts restricting the provision of information society services, therefore, it is sometimes still uncertain to what extent the existing cooperation mechanism provided for under the e-Commerce Directive ensures the necessary legal certainty and transparency for all parties involved about the compliance with such requirement.

During the open public consultations several stakeholders expressed their view on the question of cooperation among national authorities.

Trade associations, digital users' associations and companies consider that cooperation should be improved significantly both between Member States and between different authorities within each Member State. In addition, the quality of intervention varies greatly between authorities and there is often a need for more capabilities and resources.

Content creators and right holders are concerned with the fact that, while copyright is largely harmonised across the EU, there is no system in place for national authorities to cooperate on the enforcement of those rights. They state that "cooperation mechanism for cross-border cases established in the e-Commerce Directive does not function in practice" and that "the 2004 IPRED Directive, as currently implemented by different EU Member States, varies tremendously and leads to a lack of clarity".

Several national authorities consider that the quality of cooperation is good (Spain, Malta, Greece, Italy, Finland, Hungary, Portugal, France, Austria). Some point out to some issues and room for improvement (Sweden, Belgium, the Netherlands, Ireland). The Netherlands Authority for Consumers and Markets points out that cooperation could be improved and that the new CPC regulation entered into force from January 2020 is considered a potential important improvement on the EU enforcement of consumer protection rules. The Belgian government points out the need for better cooperation for tackling and preventing the dissemination of illegal content online.

3.2.4. Fragmented national laws applicable to hosting service providers

National implementing measures range from an almost literal transposition of Article 14 e-Commerce Directive, without any further clarification on the obligations for hosting services, to stricter and more detailed rules on the systems to be put in place by such services to remove or disable illegal content. The lack of a harmonized system to trigger "*actual knowledge*" has been understood by some Member States as pointing to a so-called "*notice-and-takedown*" system.

In this context, nine Member States (Finland, France, Germany, Greece, Hungary, Italy, Lithuania, Spain and Sweden) have implemented a notice-and-action procedure in their legislative frameworks. For five of them (Finland, Greece, Hungary, Italy and Spain) this only applies to copyright infringements and related rights thereof.

Furthermore, in a few Member States (Finland, France, Hungary, Lithuania), minimum requirements for the notice are defined within law, to ensure that it is sufficiently motivated. In Member States without statutory requirements for notices, the case law has provided indications concerning the content of the notice and the mechanism.

Recently, the Commission commissioned and published an external study to look into the different regimes adopted by Member States in their transposition of Article 14 of the e-Commerce Directive.[59] The findings of the study point at a clear national fragmentation in the national legal mechanisms adopted.[60]

The information available in the study shows that the majority of Member States have followed an almost verbatim transposition of Articles 14 of the e-Commerce Directive. Having said that, some Member States have provided for specific liability exemptions for information location services (search engine services) and hyperlinking services. For example, Austria, Hungary, Spain and Portugal have adopted specific liability exemptions for search engines according to which a company can benefit if it meets the conditions that hosting service providers are required to meet in order to secure a liability exemption. Similarly, Austria, Spain and Portugal have adopted liability exemptions for hyperlinks applying the same conditions as the Directive's liability exemption for hosting activities.[61]

Among the rest of Member States, not only do Member States have different options as to contemplate notice-and-action procedures and minimum requirements for notices, but also with regard to when 'expeditious removal' occurs, what is understood by 'knowledge' and what specific provisions Member States have in terms of safeguarding the freedom of expression.

There are different interpretations amongst Member States' national laws as to the exact conditions under which a hosting service provider is deemed to have actual knowledge of the illegal activity or information stored by a third party. Most Member States leave it to be decided by national courts on a case-by-case basis. The open public consultation has shown some uncertainties as to the application of Article 14 ECD to hosting services; national courts have taken divergent stances whether these services must be regarded as hosting activities within the meaning of Article 14 ECD or not.

Also, some Member States require a declaration of illegality from a competent authority or limit it to 'manifestly illegal content'. For example in Romania, the hosting service provider must have '*knowledge of the fact that the activity or information is illegal'* when its illegal character was witnessed by a decision of a public authority.

Finally, the removal or disabling access to a certain content can have a negative impact on the exercise of the rights to freedom of expression and information. It is therefore important that content providers, as also stipulated in *2018 Commission Recommendation on tackling illegal content online*, offer an opportunity to submit a counter-notice to defend the legality of the information at issue.

However, the analysis of the existing situation shows that there are again differences between Member States. In 13 Member States, some form of opportunity to dispute the allegation exist. Yet, the situation and conditions in which counter-notices are possible

---

59 An analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report, available at: https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en.

60 Idem, p. 156.

61 Commission Staff Working Document, Online services, including e-commerce, in the Single Market, SEC(2011)1641 final.

differ greatly amongst Member States. For example, a counter-notice in Estonia is only possible when the removal order is ordered by a government agency; in Finland, Greece, Hungary, Ireland, Italy and Spain counter-notices are only possible in the context of copyright; and in Luxembourg, it is only possible during the merit procedure.

In eight Member States (Bulgaria, Estonia, France, Germany, Greece, Lithuania, Portugal and Sweden), some sort of alternative dispute settlement mechanism exist. For example in Portugal, there is an out-of-court preliminary dispute settlement possible in case the illegality of the case is not obvious; in Estonia, a specific alternative dispute regime exists for copyright infringements, in which a specific committee can resolve disputes.

3.2.5. Lack of clarity and transparency on content moderation activities

The evaluation also shows that some information society service providers, in particular larger online platforms, set the rules of the game on their services that however have a wider societal impact. They not only set their own content and market policies and enforce them, but also choose what to report on and to whom as well as what information to give to their users.

Only 2% of the respondents (among those that provided reply to the relevant question) to the open public consultation state that they were informed by the platform before their content/goods/services were removed or blocked. Most of them were not able to follow-up on the information. In addition, the vast majority of users were not informed after they provided a notice to a digital service asking for the removal or disabling of access to contents/goods/services (only 13% were informed, 21% were informed in some occasions and 66% were not informed at all).

There are several aspects in the opacity and lack of accountability of online platforms:

First, users lack effective ability to:

- Report illegal activities they are witness or subject to on a particular service and to follow actions taken as a follow-up.
- Seek redress when their content is taken down, to be appropriately informed of the rules and measures taken by service provider.
- To clearly understand how information, services and goods are prioritised, on what grounds and what choices they have at hand.
- Know and understand when being presented with ads, in particular when they are being profiled and targeted.

Second, users - citizens, but also small businesses and organizations using very large platforms - cannot be sole responsible for 'supervising' such complex and impactful systems. At the core of the matter there are large information asymmetries and there are only very limited means for researchers, civil society or other third parties to inspect or understand platforms' systems, in particular where algorithmic tools are used.

Finally, authorities very often lack sufficient information to appropriately supervise information society services.

3.3. The legislative developments outside the e-Commerce Directive

Since the adoption of the e-Commerce Directive in 2000, several new pieces of EU legislation applicable to information society services have been adopted. These legislative measures cover various aspects of the provision of information society services in the internal market.

Some of the most relevant examples of such legislative measures[62] are:

- Directive 2019/790 on copyright and related rights in the Digital Single Market (the "***Copyright Directive***"), which introduces a new conditional liability regime for online content sharing services.
- Directive 2018/1808 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 ("***AVMSD***"). The AVMSD requires that Member States ensure that video-sharing platform services take appropriate measures to protect minors from harmful content, and to protect the general public from illegal hate speech and content whose dissemination constitutes a criminal offence under Union law as well as measures to ensure compliance with commercial communications requirements under the AVMSD.
- Directive (EU) 2017/541 on **combating terrorism**, which requires Member States to take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence. In addition, a Regulation specifically addressing the obligations of online hosting service providers with regards to terrorist content disseminated by their users was proposed in 2018 and is currently under negotiation between the co-legislators.[63]
- Regulation 2019/1020 on **market surveillance and compliance of products** and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011. This Regulation for example requires information society service providers to cooperate with the market surveillance authorities, at the request of the market surveillance authorities and in specific cases, to facilitate any action taken to eliminate or, if that is not possible, to mitigate the risks presented by a product that is or was offered for sale online through their services.
- Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography ("***CSAM Directive***"). This Directive obliges Member States to take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory.
- Unfair Commercial Practices Directive ("***UCPD***").[64]
- Consumer Rights Directive ("***CRD***").[65]

---

62 The examples referred to in the evaluation report are not exhaustive. Further information about legislative measures relevant for the present evaluation can be found in Annex 6 of the Impact Assessment.

63 Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, COM/2018/640 final.

64 See footnote 35.

65 See footnote 36.

- Directive (EU) 2019/770 on certain aspects concerning **contracts for the supply of digital content and digital services**,[66] which lays down common rules on certain requirements concerning contracts between traders and consumers for the supply of digital content or digital services.

While majority of the legislation adopted post-e-Commerce Directive also lays down the relationship between the different sets of rules, it is important to note that several stakeholders, including Member States, raise the question of interplay between different set of rules or, as shown further below, different cooperation mechanisms (see section 3.2.3 below).

3.4. The developments of the case law

The role of the CJEU in interpreting the provisions of the e-Commerce Directive has been instrumental both in view of the significant developments since its adoption as well as many open questions about the relationship between digital services and underlying services that some of these facilitate. Preliminary ruling references have been the key source of more than 20 preliminary ruling judgements concerning the interpretation of the e-Commerce Directive. Conversely, no case has been brought to the Court by the Commission in its capacity of the guardian of EU law for a possible infringement of it.

As shown above, the digital markets and services have developed significantly since the adoption of the e-Commerce Directive and appearance as well as disappearance of many services that have not existed at the time of the adoption of the Directive could have been observed. Unsurprisingly, several notions and principles of the e-Commerce Directive have therefore been subject to an interpretation of the Court of Justice, as shown further below.

Definition of information society services

Since the e-Commerce Directive applies to the information society services its precise meaning is essential for qualification of a specific service.

While an information society service should normally be provided for remuneration, the Court of Justice clarified in *Papasavvas* and *Mc Fadden* cases that "*the information society services does not have to be paid by the recipient of the service (and can be free for her) but the service can be paid with income generated by advertisements*".[67]

In Ker-Optika the Court clarified that "*activities which, by their very nature, cannot be carried out at a distance or by electronic means, such as medical advice requiring the physical examination of a patient, are not information society services, and consequently, do not fall within the scope of that directive*."[68]

Furthermore, the question of the legal qualification of a specific service is becoming increasingly important in the context of the collaborative economy to determine whether the

[66] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.), PE/26/2019/REV/1, OJ L 136, 22.5.2019, p. 1–27.

[67] Case C-291/13, *Papasavvas*, ECLI:EU:C:2014:2209 and case C-484/14, *Tobias McFadden v. Sony Music*, ECLI:EU:C:2016:689.

[68] Case C-108/09, *Ker-Optika*, ECLI:EU:C:2010:725.

platforms providing collaborative services could be considered as providers of information society services.

For example, in *Elite Taxi*[69] case the CJEU held that "*an intermediation service that enables the transfer, by means of a smartphone application, of information concerning the booking of a transport service between the passenger and the non-professional driver who will carry out the transportation using his or her own vehicle, meets, in principle, the criteria for classification as an 'information society service'*."

However, the Court held in that specific context that the intermediation service must be regarded as forming an integral part of an overall service whose main component is a transport service and must therefore be classified as 'a service in the field of transport' and not 'information society service'. The Court reached this conclusion based on the following factors:

- Uberpop[70] provided drivers with an app which if it was not used, the transport service would not have taken place; and
- Uberpop exerted a decisive influence over the conditions under which the transport service was provided by setting the fare, controlling the quality of the vehicles or setting minimum safety standards

In another case concerning the relationship between intermediation accommodation platform and providers of accommodation services, the Court reached a conclusion that intermediation services such as those provided by Airbnb cannot be regarded as forming an integral part of an overall service, the main component of which is the provision of accommodation.[71]

The Court notably held that Airbnb Ireland did not exercise a decisive influence over the conditions for the provision of the accommodation services to which its intermediation service relates, particularly since it:

- Did not determine, directly or indirectly, the rental price charged; nor

- Did it select the hosts or the accommodation put up for rent on its platform.

On the other hand, in a case about the regulation of short-term letting of furnished premises, the Court subjected the provision of such services to the rules set out in the Services Directive. In this way, the Court clearly distinguished the provision of the offline accommodation services from the online intermediation service.[72]

---

69 Case C-434/15 *Asociación Profesional Élite Taxi*, ECLI:EU:C:2017:981. See also case C-320/16, *Uber France,* ECLI:EU:C:2018:221.

70 This case related to the Uberpop app which facilitated contacts between non-professional drivers and users. In contrast to this Case, in Case C-62/19, *Star Taxi,App SRL,* the Advocate General found that a service consisting in putting taxi passengers directly in touch, via an electronic application, with taxi drivers constitutes an Information Society service where that service is not inherently linked to the taxi transport service so that it does not form an integral part of the taxi transport service within the meaning of the judgment in Asociación Profesional Elite Taxi.

71 Case C-390/18 *Airbnb Ireland UC*, ECLI:EU:C:2019:1112.

72 Joined Cases C- 724/18 and C- 727/18, *Cali Apartments SCI*, ECLI:EU:C:2020:743.

Internal market principle

The internal market principle as an important pillar of the e-Commerce Directive has also been subject to several important preliminary ruling reference judgements since 2000.

In *eDate Advertising* case, the Court held that according to the **internal market clause** Member States must ensure that, "*in relation to the 'coordinated field' and subject to the derogations authorised, the provider of an information society services is not made subject to stricter requirements than those provided for by the substantive law applicable in the Member State in which that service provider is established*".[73]

In *Cornelius de Visser* case, the Court held that "*Article 3(1) and (2) of e-Commerce Directive does not apply to a situation where the place of establishment of the information society services provider is unknown, since application of that provision is subject to identification of the Member State in whose territory the service provider in question is actually established*."[74]

In a recent case on on-line sale of medicines without prescription, the Court held that "*a Member State of destination of an online sales service relating to medicinal products not subject to medical prescription may not prohibit pharmacies that are established in another Member State and sell such products from using paid referencing on search engines and price comparison websites*."[75]

As regards the scope of the '***coordinated field***' to which the internal market clause applies, the Court held in *Ker-Optika* case that "*the coordinated field covers the online selling of contact lenses but does not cover the physical supply of contact lenses as the former is online while the latter is not*".[76] Furthermore in *Vandenborght* case the Court decided that "*the coordinated field covers a national law imposing a general and absolute prohibition of any advertising relating to the provision of dental care services, inasmuch as it prohibits any form of electronic commercial communications, including by means of a website created by a dentist*".

Finally, in as much as the derogation clause in Article 3(4) of the Directive is concerned, the Court in *Airbnb Ireland* case that "*if a Member State takes measures that derogate from the principle of the freedom to provide information society services without complying with the procedural conditions of the e-Commerce Directive (in particular, the notification to the Commission and the other Member States), those measures cannot be applicable against such provider of an information society service*".

Liability of intermediary services providers

Since the adoption of the e-Commerce Directive there were several cases dealing with an interpretation of the provisions dealing with the liability safe harbour for intermediary service providers. Large majority of these cases came from the area of intellectual property rights.

---

73 Joined Cases C-509/09 and C-161/10, *eDate Advertising*, ECLI:EU:C:2011:685.
74 C-292/10, Cornelius de Visser, ECLI:EU:C:2012:142.
75 Case C-649/18, *A (Publicité and vente de médicaments en ligne)*, ECLI:EU:C:2020:XXX.
76 Case C-108/09, *Ker-Optika*, ECLI:EU:C:2010:725.

Several points in the case law are relevant in this context:

- **Services that can benefit from the liability safe harbour**: the case law clarified that a number of services can qualify for one of the safe harbours, such as a social network[77], an online marketplace[78], keyword advertising service[79], internet access providers[80] or "provider" of a Wi-Fi network[81]. This is a particularly important point having in mind that many of the services that exist today have not existed at the time of the adoption of the e-Commerce Directive, or have at least not existed in the current format. Such services include for example content delivery networks ("CDNs"), virtual private networks ("VPNs"), Infrastructure as a Service ("IaaS") or Platform as a Service ("PaaS").
- **Existence of an actual knowledge about illegal information**: the case law clarified that the e-Commerce Directive does not harmonise the procedures for acquiring knowledge, but it requires hosting providers to behave as diligent economic operators.[82] It also clarified that Article 14 of the Directive requires knowledge about illegality of information, and not just its existence.[83] Finally, the Court also clarified that the actual knowledge can be obtained by means of a notification that is "*sufficiently precise or adequately substantiated*".[84]
- **Scope of the hosting safe harbour**: the case law clarified that the scope of the safe harbour depends on the distinction between active or passive role that the intermediary service provider may play in relation to the content provided by the third party. An important question is to establish whether "*an operator has not played an active role allowing it to have knowledge or control of the data stored*".[85] For example, an operator of an online marketplace "*provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them*". The Court also clarified that "*the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability*".[86]
- **Prohibition of a general monitoring obligation**: the case law clarified that abstract non-targeted filtering which was requested by a court against a social network and an internet access provider is prohibited under the e-Commerce Directive.[87] On the other hand, the Court clarified as well that a national court can impose, within the limits of "*specific monitoring obligations*", determined remedies such as:
    i. measures against repeated infringers by a trading platform;[88]
    ii. disabling access to a specific website by an internet access provider;[89]

---

77 Case C-360/10, *SABAM*, ECLI:EU:C:2012:85; Case C- 18/18, *Glawischnig*. ECLI:EU:C:2019:821.
78 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474.
79 Cases C-236/08 to C-238/08, *Google France and Google v. Vuitton*, ECLI:EU:C:2010:159.
80 Case C-70/10, *Scarlet*, ECLI:EU:C:2011:771; Case C-314/12, *UPC Telekabel Wien*, EU:C:2014:192.
81 Case C-484/14, *McFadden*, ECLI:EU:C:2016:689.
82 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474.
83 Cases C-236/08 to C-238/08, *Google France and Google v. Vuitton*, ECLI:EU:C:2010:159.
84 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474.
85 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474; Cases C-236/08 to C-238/08, *Google France and Google v. Vuitton*, ECLI:EU:C:2010:159.
86 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474.
87 Case C-360/10, *SABAM*, ECLI:EU:C:2012:85; Case C-70/10, *Scarlet*, ECLI:EU:C:2011:771.
88 Case C-324/09, *L'Oreal v eBay*, ECLI:EU:C:2011:474.

iii. protecting open Wi-Fi network by a password;[90]
iv. injunction extended to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal.[91]

4. EVALUATION QUESTIONS

This evaluation assesses the e-Commerce Directive against the five Better Regulation criteria, namely effectiveness, efficiency, relevance, coherence and EU added value, using the specific evaluation questions for each of them.

4.1. Effectiveness

1. Has the e-Commerce Directive attained its initial objectives?

2. What gaps have been identified?

3. To what extent has legislative developments in recent years been able to contribute to the attainment of the objectives of the e-Commerce Directive?

4.2. Efficiency

4. Are the costs of the e-Commerce Directive proportionate to the benefits that the Directive brings for stakeholders?

4.3. Relevance

5. How well, if at all, do the objectives of the e-Commerce Directive still correspond to the needs?

4.4. Coherence

6. Is the e-Commerce Directive coherent with other EU legislative instruments that apply to information society services?

4.5. EU added value

7. What is the added value resulting from the e-Commerce Directive compared to what could be achieved without such intervention?

---

89 Case C-314/12, *UPC Telekabel Wien*, EU:C:2014:192.
90 Case C-484/14, *McFadden*, ECLI:EU:C:2016:689.
91 Case C- 18/18, *Glawischnig.* ECLI:EU:C:2019:821.

5. METHODOLOGY

5.1. Short description of methodology

The evaluation of the e-Commerce Directive started in June 2020 with the publication of the joint roadmap/impact assessment. The Inter-service Steering Group (details in Annex 1 of the Impact Assessment) was consulted and gave input to this evaluation report.

Open public consultations

The Commission has conducted several open public consultations on the issues related to the present evaluation (see Annex 2 of the Impact Assessment for further details). This evaluation also takes account of the input to the public consultation on the joint roadmap/impact assessment concerning the Digital Services Act.

Workshops with stakeholders

This evaluation also takes account of the information collected through numerous workshops organized with stakeholders on number of issues covered, such as national measures for tackling illegal content online or market and technological developments concerning intermediary service providers (see Annex 2 of the Impact Assessment for further details).

E-commerce Expert Group meetings with Member States

In particular, during the e-Commerce Experts Group meeting of 8 October 2019[92], the main principles of the e-Commerce Directive has been discussed with Member States, as well as the latest development on national levels (see Annex 2 of the Impact Assessment for further details).

Targeted consultation of the Member States

As part of the evaluation process, the Commission also sent a targeted questionnaire to all Member States raising in particular questions about their experience with the cooperation mechanisms under Article 3 of the e-Commerce Directive, but also experience with the implementation and application of other provisions of the e-Commerce Directive.

The information collected from these groups of stakeholders supported the analysis of the take-up and impacts of the measures. A core part of the evaluation relies on legal analysis, not least in light of the coherence of interpretations in case law. This was analysis also relies on interviews with a number of judges involved in the headline cases as well as other legal experts (see Annex 2). Further, economic data was exploited to understand the evolution of the digital sector.

5.2. Limitations and robustness of findings

As regards the evaluation criterion of efficiency, it proved difficult to collect quantitative evidence on the costs of applying the e-Commerce Directive. While some data has been

[92] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=16890

obtained through the open public consultation, the assessment of costs has been primarily based on the assumed costs based on the modelling of costs for specific type of options considered in the Impact Assessment.

6. ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS

6.1. Effectiveness

Under this section the evaluation was trying to assess to what extent have the initial objectives of the e-Commerce Directive been met and whether some gaps have been identified.

6.1.1. Facilitating the internal market for information society services by removing legal fragmentation

The evaluation shows that in particular, Articles 3 and 4 of the e-Commerce Directive allowed provision and accessibility of information society services cross-border in the internal market. This has been happening across all layers of the internet and the web and has enabled successful entry and growth of many EU companies in different segments of the market (e.g. Zalando, Spotify, Deezer, Booking, 1&1, Seznam, etc.). At the same time the evaluation also showed that some very large platforms with global scale have also managed to enter the internal market and managed to reshape several segments of it.

At the same time, there is clear evidence of legal fragmentation[93] and differentiated application of the existing rules by Member States, including national courts. There is also an increased tendency of Member States to adopt legislation with extraterritorial effects and enforce it against service providers not established in their Member State. Such enforcement in consequence reduces the necessary trust between the competent authorities and undermines the well-functioning internal market for information society services.

In particular, Member States have begun to regulate at national level, increasing the fragmentation of the single market, especially for hosting service providers as one form of intermediary service providers, which includes online platforms.

Furthermore, a number of MS have introduced diverging 'notice-and-action' rules. National rules do not only diverge in scope, but also in the specific requirements they set – e.g. minimum content of a notice, limitations to 'manifestly illegal' content, interpretation of different means for obtaining 'actual knowledge' about an illicit activity and interpretations of 'expeditious' removal of content. Furthermore, Member States are starting adopt legislation, which not only sets specific obligations and sanctions, but also allocates competence for country of destination on some services established elsewhere, by requiring

[93] The Commission gathered extensive evidence of legal fragmentation with regards to the transposition of Art 14 and 15, as well as through the divergent interpretations from courts at various levels, through two legal studies ICF, *Overview of the Legal Framework of Notice-and-Action procedures in Member States* (2018), and Joris van Hoboken et al., *Hosting Intermediary Services and Illegal Content. An analysis of the scope of article 14 of the E-Commerce Directive in light of developments in the online service landscape* (2018). Further detailed analysis is also presented in a study commissioned by the Council of Europe, *Comparative study on blocking, filtering and takedown of illegal content on the Internet* (2016)

a legal representative within the territory of the country of destination if the service reaches a certain threshold of users on that territory.

In addition, there is also evidence of considerable lack of trust between Member States, as some countries seriously doubt the willingness of the authorities of the country of destination to protect the interests of their citizens. The evaluation also shows that Member States often do not use the cooperation mechanism provided for in the e-Commerce Directive.

As a result, this fragmentation makes it even harder for smaller EU companies to scale up at home, and gives an edge to very large platforms who can put legal teams in every country. This also leads to uncertainties in the application and enforcement of law across the internal market.

6.1.2. Removing legal uncertainty in relation to liability of intermediary service providers

The liability safe harbour provisions laid down in Section 4 of the e-Commerce Directive have provided for a necessary minimum of legal certainty for online intermediaries to emerge and scale across the single market and to develop innovative services catering to the needs of consumers. However, conflicting interpretations in national court cases (sometimes even within the same Member State) have introduced a significant level of uncertainty; in addition, an increasing fragmentation of the single market raises barriers for EU scale-ups to emerge.

The liability regime has only partially reached its objective to incentivise the effective removal of illegal content in particular in the absence of legally binding, common procedural obligations ("notice-and-action") across the internal market. This has in turn also lead to an increased fragmentation of requirements at national level (see also section 6.1.1 above).

In addition, several stakeholders referred to an uncertainty brought by case law interpretations[94] on what activities would qualify a hosting service as an 'active' host, in opposition to a 'passive' as necessary to benefit from the conditional liability limitation, created disincentives for platforms, in particular SMEs, to apply voluntary, proactive measures against illegal activities.

In addition, in view of the significant developments of the digital economy and services, the question arises under which conditions new type of intermediary services (e.g. virtual private networks; content delivery networks) could be benefit from the liability safe harbour.

Other factors equally contribute to the lack of effectiveness: exclusion of operators established outside of the EU and emergence of mega-platforms that, by their sheer reach,

[94] Case C-324/09, L'Oreal v eBay, ECLI:EU:C:2011:474 and joined cases C-236/08 to C-238/08, Google France and Google v. Vuitton, ECLI:EU:C:2010:159 are most often referred to in this context.. Further complexities spur from conflicting decisions by different levels of courts as to the active or passive role of the same type of service – e.g. video-sharing hosting services – with conflicting views over the extent to which the same type of service can benefit from liability limitations.

aggravate the extent of harm caused by the dissemination of illegal content, and a lack of transparency and reliability of results when platforms do take measures.

Similarly, the provisions have only partially achieved the balancing objective of protecting fundamental rights. They provide stronger incentives for the removal of content than to protect legal content and also lack appropriate oversight and due process mechanisms especially in situations of so-called 'privatised law enforcement'.

Finally, the current system tends to ask platforms in particular to take decisions on the legality and removal of content, often also without meaningful transparency on processes and outcomes.

6.1.3. Removing disincentives for consumers going online and concluding transactions online

The e-Commerce Directive seeks to harmonize all steps in the provision of an information society service (from an establishment of the information society service provider and information about its services, to provisions of contracts, advertising the service, etc.). The objective of the e-Commerce Directive was to ensure that consumers are clear about guarantees when going online and that the provision of digital services is ensured across the internal market.

To ensure this the e-Commerce Directive identified primarily set of embryonic transparency obligations concerning general information about the information society service provider (Article 5), (unsolicited) commercial communications (Articles 6-8), recognition and treatment of contracts (Article 9) and information prior to placing orders (Articles 10-11).

The evaluation shows that while the provisions have set the minimum conditions for consumer trust and provision of digital services and are still valid today, they have been largely complemented by a rich corpus of further rules and harmonisation measures in the areas such as consumer protection and conclusion of contracts at a distance, including by online means. Furthermore, as shown through several enforcement actions by the CPC Network, some provisions, such as the information requirements applicable to the information society service providers, suffer from a patchy and very different compliance by the information society service providers.

Furthermore, the fundamental changes in the variety and scale of information society services, as well as of the technologies deployed and online behaviour, have led to the emergence of new challenges, not least in terms of transparency of online advertising and algorithmic decision-making consumers and businesses are subject to.

In addition, there are several new technological developments that raise many important questions as to their use and possible legal implications. For example, in relation to electronic contracts the use of blockchain technology and smart contracts is increasingly getting traction, which raises certain regulatory questions.

Finally, the evaluation does not allow concluding on the actual scope of the implementation and use of codes of conducts and out-of-court dispute resolution mechanisms by Member States in relation to digital services in general or limited scope therefore more specifically.

6.1.4. Preliminary conclusion on effectiveness

It can therefore be concluded that while the e-Commerce Directive, and in particular Articles 3 and 4 of the e-Commerce Directive, has provided an important incentive for the growth of the internal market for information society services and enabled entry and scaling up of new service providers, the initial objectives have not been fully achieved.

In particular, the exponential growth of the digital economy and appearance of a new type of service providers raises certain new challenges that require reflection of possible update to the existing objectives. In addition, these developments and challenges put an additional strand on achieving already existing objectives as the increased legal fragmentation and undermining of the well-functioning of internal market for information society services shows.

Several new regulatory instruments (see in particular section 3.3 above) make valuable contributions to the attainment of some of the policy objectives set out in the e-Commerce Directive. Yet, while providing sector specific solutions for some of the underlying problems (e.g. in addressing the proliferation of specific type of illegal activity), they do not necessarily address the same issue for the entire digital ecosystem (e.g. because they are limited to certain types of services, certain types of content, or to operators established within the EU territory). Furthermore, while the voluntary measures have generally shown positive results they cannot be legally enforced nor do they cover all participants in the digital economy.

In addition, these measures do not adequately address the problem of fragmentation of the single market, due to a growing number of national legal measures, nor do they address the problem of uneven and ill-coordinated enforcement across the internal market (although sector-specific regulators, such as in the area of media, clearly contribute to that objective as well).

Moreover, these measures do not solve the problem of lack of legal clarity concerning the scope of the liability provisions of the e-Commerce Directive itself (e.g. which types of services would be covered by the relevant provisions of the e-Commerce Directive). As a result, they cannot address the disincentives for intermediary service providers to act more proactively nor do they provide for the overall transparency and accountability for the behaviour of measures of (in particular large) intermediary service providers (concerning the effectiveness of their measures and their impact on freedom of expression and information).

6.2. Efficiency

A core efficiency test for the E-Commerce Directive relates to the costs and frictions in the cooperation across member states' authorities, in line with Article 3 of the Directive.

The principle in itself, and the cooperation across Member States, has been fundamental to cutting a significant duplication of costs across authorities and ensuring the level of effectiveness in the supervision of digital services (see previous sections).

However, there is a lack of clarity and reliability of response in the cooperation mechanism, which increases the uncertainties for Member States. In addition, with several mechanisms available (see Annex 7), several Member States reported that it is not clear which channel

should be used. The duplication of efforts and the lack of procedural clarity generates significant costs. Quantification of these costs was not possible on the basis of the available and reported data from the Member States. Based on the differences in the use of the cooperation mechanisms[95], it is clear that Member States experience these costs to different extents.

In terms of costs for businesses, the E-Commerce Directive only imposes a limited number of obligations – such as information requirements (Article 5) or disclosure regarding commercial communications (Article 6). Instead, the Directive harmonises measures and provides legal certainty to reduce costs and make sure that there is a level playing field across the Union.

At the same time, in light of the evolution of the digital sector, evolving case law and, importantly, increasing legal fragmentation, significant costs have emerged for digital services. These are presented in detail in the Impact Assessment report, and relate in particular to the legal uncertainties and fragmentation emerged 'on top' of the E-Commerce Directive. The loss of internal market in this regard is estimated between 1 and 1.8% of total turnover from cross-border provision of digital services.

6.3. Relevance

Under this section of the evaluation was trying to assess to what extent are the initial objectives of the e-Commerce Directive still relevant today.

6.3.1. Facilitating the internal market for information society services by removing legal fragmentation

The evaluation shows that the proper functioning of the internal market for information society services very much remains a valid objective.

The overwhelming majority of the replies to the open public consultation point to the importance of preserving the internal market principle if one is to ensure that any type of digital service provider that aspires to start up and grow in Europe may do so. The evaluation confirms that the internal market principle is instrumental for service providers to grow and expand cross-border. It also shows that only very large, well established information society service providers have the capacity to comply with 27 potentially diverging legal obligations and with 27 ill-coordinated enforcement systems.

In addition, information society services are subject, to a varying extent, to sectorial regulation enforced by a number of national and European regulators – from data protection authorities for personal data protection, to media, telecom, competition or consumer protection authorities. This means that all regulators are confronted with a similar set of challenges in the extremely diverse and technology-savvy environment of digital services. Subsequently stronger means of cooperation, sharing of best practices and technical information, and coordination in enforcing the law, remain paramount for the robustness of the internal market, the effectiveness in enforcing the law and the protection of all EU citizens.

[95] *Supra,* p.28

6.3.2. Removing legal uncertainty in relation to liability of intermediary service providers

The evaluation shows that the clarifications in the c-Commerce Directive concerning the liability of intermediary service providers for third part information and activities have been an important contributor to the growth of the digital economy and services in the internal market.

The evaluation also showed that the absence of a liability exemption safe harbour could incentivise the over-removal of legal content, and therefore be at odds with the fundamental freedoms, such as freedom of expression and information. The same applies to the existing prohibition in the e-Commerce Directive to impose general monitoring obligations on intermediary service providers, which would disproportionately burden these providers while at the same time incentivising them to "over-remove" (legal) content so as to avoid the risk of fines or litigation.

The evaluation also confirms that the objectives to have in place an effective tools that would ensure effective removal of illegal activities or information while safeguarding the freedom of expression and information are more relevant than ever for several reasons:

- First, the volumes of content intermediated by information society service providers continue to grow at an unprecedented pace, and so does their reach into society. This also increases the risk of illegal activity as well as its potential impact.
- Second, increasing endeavours by information society service providers to reduce their users' exposure to illegal or harmful content – triggered by legal requirements and/or the increasing automation of content management systems – also increases the risk that legal content is removed erroneously. As some digital platforms are now one of the main venues for information and expression, including for political expression, any content moderation rules have a direct and immediate impact on fundamental rights, and a careful balance needs to be struck.

6.3.3. Removing disincentives for consumers going online and concluding transactions online

As for the objective to promote trust in the digital ecosystem by providing consumers and users with adequate information, the evaluation shows that the overall objective remains valid, while the underlying problems have evolved in view of the significant developments in the area.

This applies in particular to the area of online advertising that has evolved from the commercial communications activities existing at the time when the e-Commerce Directive was adopted. While a number of public policy concerns such as privacy and data protection (i.e. GDPR, ePrivacy Directive), content of advertisements and consumer information (i.e. UCPD, AVMSD), or follow the money solutions to counter illicit activities (e.g. *Memorandum of Understanding with online advertising industry against counterfeit*) are being addressed elsewhere, the evaluation shows that several issues deserve further assessment. In particular, as also raised by several stakeholders during the open public consultation, a chain of intermediary services has emerged in between the publishers and the advertisers, and further clarity as to their status and responsibility is needed. In addition, and as regards new developments, the evaluation shows that the ad placement process remains

largely opaque, to both consumers and related services, and therefore lacks meaningful transparency.

Furthermore, the evaluation also shows that today digital services are fundamentally shaped by a series of algorithmic processes designed to optimise the way information flows are intermediated, from ranking algorithms and recommender systems, to content detection and filtering technologies. Some aspects of this are already regulated through an existing EU legislation. For example, the GDPR sets specific rules for a sub-set of such processes, based on the processing of personal data, and the Platform-to-Business Regulation sets obligations on disclosure of the main parameters of online ranking on platforms intermediating relations between business users and consumers, as well as search engines.

However, these measures do not cover the entire spectrum of issues emerging when algorithmic decision-making is used at scale.

Furthermore, as shown above (see section 6.1.3), while the e-Commerce Directive supported the use of electronic means for conclusion of contracts, there have been significant technological developments in this area. In particular, with the increased use of blockchain technology and smart contracts there is a question whether the existing framework laid down in the Directive remains fully relevant in its current scope.

6.3.4. Preliminary conclusion on relevance

The evaluation shows that the objectives of the e-Commerce Directive continue to remain valid, while at the same there are several new developments that may not be well reflected in the existing public policy objectives, including as they have developed since the adoption the e-Commerce Directive.

In the first place, the open public consultation as well as targeted submissions by stakeholders, reports[96] prepared for the European Parliament or Council conclusions[97] confirm that the existing principles and objectives of the e-Commerce Directive remain very valid also today. This is particularly the case for ensuring the well-functioning internal market for information society services built on internal market principle and preserving liability safe harbour for intermediary service providers while clarifying the application of the conditions to new services that developed since the adoption of the e-Commerce Directive.

In addition, while many of the issues identified at the time of the adoption of the e-Commerce Directive have been complemented by a series of laws concerning consumer protection, contract law, misleading advertising, and the like. That said, new information asymmetries have arisen in the meantime – such as in the areas of algorithmic decision making (with an impact on how information flows are intermediated online), or in online advertising systems – that render this objective as relevant as ever. In some cases, the sale of advertising is a core part of platform's business models and, while the platform offers

[96] The e-commerce Directive as the cornerstone of the Internal Market, Assessment and options for reform, available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)648797.

[97] Shaping Europe's digital future, available at: https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf.

distinct services, there is a dependency of incentives across the components of the business model.

6.4. Coherence

Under this section of the evaluation was trying to assess to what extent is the e-Commerce Directive coherent with the other regulatory interventions applicable and relevant for the provision of the information society services in the internal market.

6.4.1. General assessment

Since the adoption of the e-Commerce Directive not only is the market and technological landscape significantly different, but also regulatory framework applicable to information society service underwent numerous changes.

As shown in section 3.3 above and in Annex 6 of the Impact Assessment, several EU legal acts have been adopted since the adoption of the e-Commerce Directive that deal with specific aspects of the information society services.

Having said that, the present evaluation did not identify any instance of in-coherence with the existing rules or other policy initiatives in the areas concerned. There are several reasons for this:

- First, the e-Commerce Directive was adopted at an early stage of the internet and development of e-commerce, which allowed the European co-legislators to adopt a horizontal framework applicable to information society services at the time when many of the challenges that appeared later did not exist yet.
- Second, the legislative intervention of the e-Commerce Directive was based on a principle that it should address only what is strictly necessary to ensure well-functioning internal market for information society services and already recognized that there are several aspects that are adequately addressed elsewhere (e.g. consumer protection; data protection).
- Third, subsequent legislative interventions, such as AVMSD, Copyright Directive, CSAM Directive or even some elements of the consumer *acquis*, clearly recognized that horizontal principles of the provision of information society services are laid down in the e-Commerce Directive. In this context, all subsequent legal interventions clarified that these acts do not to replace principle of the e-Commerce Directive, but build on and complement them or deal with specific regulatory issues that e-Commerce Directive as a horizontal instrument does not.

In this context, the subsequent EU legal acts did not interfere with basic horizontal principles of the e-Commerce Directive and preserved the coherent interplay with the rules in place. Annex 6 of the Impact Assessment provides an overview of how some of the most relevant rules adopted subsequent to the e-Commerce Directive, but dealing with some of the aspects of the e-Commerce Directive, interplay with its rules. As shown, in none of the cases any in-coherence has been identified.

Finally, the evaluation of the e-Commerce Directive also did not point to any internal in-coherence in the Directive itself.

6.4.2. Preliminary conclusion on coherence

The evaluation showed that the e-Commerce Directive is generally coherent with other EU interventions that took place since its adoption. The evaluation also did identify any internal in-coherence of the e-Commerce Directive.

6.5. EU added value

Under this section of the evaluation was trying to assess to what extent has the e-Commerce Directive added value as oppose to a scenario where the Directive would have never been adopted.

6.5.1. General assessment

Before the e-Commerce Directive came into force some Member States had already made use of regulatory systems for information society services, which however differed in objectives and means. Other Member States had no rules in place. This had resulted in a significant regulatory fragmentation, which consequently led to fragmentation of the internal market and lack of legal certainty for providers and recipients of information society services.

In this context, the adoption and implementation of the e-Commerce Directive established for the first time a common framework applicable to all Member States. There had been no substantial trend towards coordination of a common framework on information society services by Member States before the evaluation period. Although it cannot be excluded that some rules on e-commerce could also be established at the international level in particular in the context of multilateral regulatory frameworks (e.g. GATS), there are no indications that either WTO or any other body had the intention to do so. This is also confirmed by the fact that only recently some members of the WTO, including the EU, announced intention to launch talks98 on e-commerce, which could address some, but not all, of the issues that the e-Commerce Directive deals with.

Based on the above it thus does not seem to be an overly strong assumption that, without EU intervention, Member States would have continued applying their own regulatory systems without any common set of principles also during the evaluation period. This assumption was also used as baseline scenario of the explanatory memorandum of the e-Commerce Directive and the present evaluation, while the latter taking also into account that some aspects relevant for the provision of information society services in the EU have been subject to further harmonization measures (e.g. consumer protection; measures against specific type of illegal content).

The evaluation confirms that the different and diverging legal regimes applicable to information society services increase compliance costs while also being the source of legal uncertainty as to the applicable obligations across the EU and of unequal protection of EU citizens. In addition, the effects of any action taken under national law are limited to a single Member State and there are no guarantees that in absence of an EU intervention a common set of principles would underpin provision of such services in the internal market.

[98] More about the announced intention is available here: http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974.

The principles of the e-Commerce Directive, in particular country of origin and prohibition of prior authorization, as well as legal certainty deriving from clearly established horizontal rules enabled growth of information society services and their cross-border expansion. The latter trend has been further facilitated through sector and issues specific rules that were adopted since the e-Commerce Directive adoption.

However, the evaluation also shows that while the initial objectives remain relevant, the current regulatory trends in some Member States put a significant pressure on their achievement, since the increasing trend of regulatory fragmentation can be observed again. This does not only risk undermining the exercise of fundamental rights under the Treaty, such as free movement of services, but raises risks of legal uncertainty both for service providers and recipients, which in turn leads to lack of trust between Member States and in the internal market itself.

6.5.2. Preliminary conclusion on EU added value

At least part of the actual benefits of the e-Commerce Directive that the evaluation identified could be considered as EU added value. It is likely that Member States would have continued applying their own regulatory systems without any common set of principles and that some Member States would have continued to have no horizontal rules in place at all.

In the absence of robust evidence, it is however not possible to draw firm conclusions on the extent of this EU added value.

7. CONCLUSIONS

The aim of the e-Commerce Directive was to ensure the freedom of providing digital services in the internal market, leading to growth and competitiveness in the EU and offering consumers a wide-range of choices and opportunities, including by ensuring that the Internet remains safe, trustworthy, fair and open.

The specific objectives of the Directive were (i) ensuring well-functioning internal market for digital services, (ii) ensuring effective removal of illegal content online in full respect of fundamental rights and (iii) ensuring adequate level of information and transparency for consumers.

As regards the **effectiveness** of the e-Commerce Directive the evaluation shows that while the e-Commerce Directive, and in particular Articles 3 and 4 of the e-Commerce Directive, has provided an important incentive for the growth of the internal market for information society services and enabled entry and scaling up of new service providers, the initial objectives have not been fully achieved.

In particular, the dynamic growth of the digital economy and appearance of a new type of service providers raises certain new challenges that require reflection of possible update to the existing objectives. In addition, these developments put an additional strand on achieving already existing objectives as the increased legal fragmentation and undermining of the well-functioning of internal market for information society services shows.

The evaluation showed that while several new regulatory instruments make valuable contributions to the attainment of some of the policy objectives set out in the e-Commerce Directive, they provide sector specific solutions for some of the underlying problems (e.g. in addressing the proliferation of specific type of illegal activity). They therefore do not necessarily address the same issue for the entire digital ecosystem (e.g. because they are limited to certain types of services, certain types of content, or to operators established within the EU territory). Furthermore, while the voluntary measures have generally shown positive results they cannot be legally enforced nor do they cover all participants in the digital economy.

In addition, these measures do not adequately address the problem of fragmentation of the single market, due to a growing number of national legal measures, nor do they address the problem of uneven and ill-coordinated enforcement across the internal market (although sector-specific regulators, such as in the area of media, clearly contribute to that objective as well).

Moreover, these measures do not solve the problem of lack of legal clarity concerning the scope of the liability provisions of the e-Commerce Directive itself (e.g. which types of services would be covered by the relevant provisions of the e-Commerce Directive). As a result, they cannot address the disincentives for intermediary service providers to act more proactively nor do they provide for the overall transparency and accountability for the behaviour of measures of (in particular large) intermediary service providers (concerning the effectiveness of their measures and their impact on freedom of expression and information).

As regards the **efficiency** of the e-Commerce Directive, the Directive imposed only limited additional costs for Member States' administrations and providers of digital services. The evaluation has not revealed particularly high or disproportionate costs and no substantial concerns have been raised regarding impacts on SMEs. As noted above, the Directive has had a positive impact on the well-functioning internal market for digital services and contributing to legal certainty in areas such as liability of intermediary service providers. In the absence of the Directive, it is unlikely that any of these benefits would have materialised.

The Directive’s efficiency has nevertheless been reduced by the limitations to its effectiveness, in particular due to the numerous developments since its adoption, discussed above. The main concern in this regard is related to the lack of clarity in the cooperation mechanism across member states, creating burdens and duplication of costs, despite the opposite objective of the Directive. This has essentially reduced its efficiency in maintaining the functioning of the internal market.

In relation to question of continued **relevance** of the objectives pursued by the e-Commerce Directive, the evaluation shows that the objectives of the e-Commerce Directive continue to remain valid, while at the same there are several new developments that may not be well reflected in the existing public policy objectives.

In the first place, the open public consultation as well as targeted submissions by stakeholders, reports[99] prepared for the European Parliament or Council conclusions[100] confirm that the existing principles and objectives of the e-Commerce Directive remain very valid also today. This is particularly the case for ensuring the well-functioning internal market for information society services built on internal market principle and preserving liability safe harbour for intermediary service providers while clarifying the application of the conditions to new services that developed since the adoption of the e-Commerce Directive.

In addition, while many of the issues identified at the time of the adoption of the e-Commerce Directive have been complemented by a series of laws, new information asymmetries have arisen in the meantime. This is for example the case in the areas of algorithmic decision making (with an impact on how information flows are intermediated online), or in online advertising systems that render this objective as relevant as ever.

The evaluation showed that the e-Commerce Directive is generally **coherent** with other EU interventions that took place since its adoption. The evaluation also did identify any internal in-coherence of the e-Commerce Directive.

Finally, at least part of the actual benefits of the e-Commerce Directive that the evaluation identified could be considered as **EU added value**. It is likely that Member States would have continued applying their own regulatory systems without any common set of principles and that some Member States would have continued to have no horizontal rules in place at all. In the absence of robust evidence, it is however not possible to draw firm conclusions on the extent of this EU added value.

[99] The e-commerce Directive as the cornerstone of the Internal Market, Assessment and options for reform, available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)648797.

[100] Shaping Europe's digital future, available at: https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf.

Annex 6: Supporting analysis for legal basis and drivers – legal fragmentation

As the Inception Impact Assessment advanced, the intervention addresses the freedoms of establishment and to provide services and the proper functioning of the Single Market for digital services. As such, the legal basis considered likely would be Article 114 of the Treaty of the Functioning of the European Union and, potentially, Articles 49 and 56 (to the extent that the conditions of establishment would represent an overweighting element of the legal intervention).

The Inception Impact Assessment already identifies the existing and increasing legal fragmentation as a main problem: in response to the increasing role of digital services in the online trade in or dissemination of illegal goods and content, Member States are increasingly passing laws with notable differences in the obligations imposed on digital services, in particular online platforms, and with a variety of different enforcement mechanisms. This creates a fragmentation of the single market that can negatively affect EU citizens and businesses in the absence of harmonised rules and obligations. It also entails a lack of legal clarity and certainty for digital services in the internal market, and is likely to be less effective in achieving the underlying public policy objectives.

The increasing legal fragmentation of the digital single market underpins the need to set up harmonized rules for information society services offered in the EU. The present annex presents the evidence on the potential choice of Article 114 TFEU as a relevant legal option for the legal instrument.

Article 114 TFEU establishes that the European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.

Following well-established case-law of the CJEU[1], this Article is the appropriate legal basis where there are differences between Member State provisions which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market, and a possible legal basis for measures to prevent the emergence of future obstacles to trade resulting from differences in the way national laws have developed.

While Article 114 TFEU is the legal basis for measures improving the Internal Market, and usually only EU services providers can benefit from the EU Internal Market, this Article can also be used to impose obligations on services providers established outside the territory of the EU where their service provision affects the internal market, when this is necessary for the desired internal market goal pursued. This has been the case already for the Regulation on Geoblocking[2], the Regulation on promoting fairness and transparency for business users

[1] See, for all, C-380/03 Germany v European Parliament and Council, judgment of 12 December 2006.

[2] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC: " The effects for customers and on the internal

of online intermediation services[3] or the Commission proposal for a Regulation on terrorist content online[4].

Finally, Article 114 TFEU can also serve as a legal basis to impose an obligation to third country companies to appoint a representative within the territory of the Union, insofar as this is merely incidental with regard to the main purpose or component of the act. This is the case, for instance, for the NIS Directive, exclusively based on Article 114 TFEU.

In order to consider whether Article 114 TFEU constitutes an appropriate legal basis for the proposed instrument, the following chapters present the existing legal fragmentation in the field of measures targeting online platforms in particular, be it to specify the conditions of secondary liability, or to impose specific duties of care of due diligence obligations vis-à-vis users as regards the way they conduct business.

1. Main drivers leading to regulatory fragmentation

Examination of the current regulatory context for information society services in the EU shows that those services, and especially online intermediaries, are subject to significant regulatory fragmentation across the digital Single Market.

The ECD constitutes the horizontal regulatory framework for information society services established in the EU. It contains the core principles and rules governing digital services across the EU. Despite the wide scope of its coordinated field, the ECD seems to lack a sufficient level of harmonization to provide a uniform application of its main rules and principles across the EU.

In particular, the ECD does create a limited liability regime for online intermediaries regarding potentially illegal content being transmitted or hosted in their service. It does not, however, provide harmonized rules on how online intermediaries are to address such content. As a result, Member States have adopted national rules applicable to the service providers established in their territory creating specific obligations to tackle illegal content.

According to our research and available information, this situation is the result of: (i) the diverging way taken by Member States to transpose the ECD as regards Articles 12-15, (ii) country-specific notice-and-action procedures or other due diligence obligations as regards the content they host[5]; and, (iii) recent national laws being increasingly adopted by Member States whose scope would also apply to cross border services.

2. Transposition of Directive 2000/31/EC as regards Articles 12-15

---

market of discriminatory treatment in connection to transactions relating to the sales of goods or the provision of services within the Union are the same, regardless of whether a trader is established in a Member State or in a third country. Therefore, and with a view to ensuring that competing traders are subject to the same requirements in this regard, this Regulation should apply equally to all traders, including online marketplaces, operating within the Union"

[3] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, p. 57–79

[4] Proposal for a Regulation of the European parliament and of the Council on preventing the dissemination of terrorist content online, 12.9.2018

[5] Overview of the legal framework of notice-and-action procedures in Member States SMART 2016/0039, Final report

The ECD sets out the liability regime applicable to online intermediaries of information online, mere conduit, caching and hosting services. For the purposes of this report, we will focus on the category of hosting services regulated under Article 14 of the Directive, which are most concerned by the ramping legal fragmentation.

Hosting services are defined as those information society services consisting of storing information at the request of the recipient of the service. For these services, Article 14 establishes a limited exemption of liability for third party content under certain conditions:

- The provider does not have actual knowledge or is not aware of the existence of illegal content; and
- Upon obtaining such knowledge or awareness, takes expeditious action to remove or block access to the content.

In the context of the transposition of Article 14 into their national legal systems, Member States have adopted various legal regimes applicable to their home hosting services.

National legal systems range from a quasi-literal transposition of Article 14, without any further clarification on the obligations for hosting services, to stricter and more detailed rules on the systems to be put in place by such services to remove or disable illegal content. In particular, the lack of a harmonized system to trigger "actual knowledge" has been understood by some Member States as pointing to a so-called "notice-and-takedown" system. The Commission has also taken this approach in the 2017 Communication on tackling illegal content online and the subsequent 2018 Recommendation on effective ways to tackle illegal content online, which encourage Member State to establish such notice and action obligations for the hosting services under their jurisdiction.

The Commission already pointed at these divergences in its third Implementation report of the ECD[6]. Recently, the Commission commissioned and published an external study to look into the different regimes adopted by Member States in their transposition of Article 14.[7] The findings of the study point at a clear national fragmentation in the national legal mechanisms adopted.[8]

The information available in the study shows that the majority of Member States have followed an almost verbatim transposition of Articles 14. Among the rest of Member States, not only do Member States have different options as to contemplate notice-and-action procedures and minimum requirements for notices, but also with regard to when 'expeditious action' occurs, what is understood by 'knowledge' and as defined in Article 14, and what specific provisions Member States have in terms of safeguarding the freedom of expression.

"Expeditiously"

[6] Commission staff working document Online services, including e-commerce, in the Single Market /* SEC/2011/1641 final */

[7] Overview of the legal framework of notice-and-action procedures in Member States SMART 2016/0039, Final report

[8] Overview of the legal framework of notice-and-action procedures in Member States SMART 2016/0039, Final report, pages 156 to 160.

Article 14 ECD requires HSPs to act "expeditiously" upon obtaining actual knowledge or awareness of illegal content. However, the exact meaning of this term is unclear, in particular because of an absence of EU case-law and diverging national legislations and case-law[9]. It can be concluded that national courts interpret "expeditiously" on a case-by-case basis taking into account a number of factors such as: the completeness of the notice, the complexity of the assessment of the notice, the language of the notified content or of the notice, whether the notice has been transmitted by electronic means, the necessity for the HSP to consult a public authority, the content provider, the notifier or a third party and the necessity, in the context of criminal investigations, for law enforcement authorities to assess the content or traffic to the content before action is taken

"Actual knowledge"

There are different interpretations amongst Member States' national laws as to the exact conditions under which a hosting service provider is deemed to actual knowledge of the illegal activity or information stored by a third party.

As already analyzed in full in the Impact Assessment accompanying the document Proposal for a Regulation on preventing the dissemination of terrorist content online[10], when transposing the ECD or during its application, some Member States have limited to courts or administrative authorities the power to refer illegal content to an online platform or to trigger the platform's liability when doing so. In such national regimes, only the referral by courts or administrative authorities is able to generate sufficient knowledge on the service provider over the specific illegality.

In addition, mention should be made to the interpretation that national courts have been making of the national provisions transposing Article 14 ECD. The resulting national case law provides further detail on how the national measures need to be interpreted in particular cases. Similarly, the CJEU, in particular through the case law resulting from preliminary

[9] See Annex 7 of the Impact Assessment accompanying the document Proposal for a Regulation on preventing the dissemination of terrorist content online.

[10] Annex 7 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN: In France, the Conseil Constitutionnel declared unconstitutional a provision of the transposition of the e-Commerce Directive and limited the liability to intermediary service providers to manifestly illegal content reported by a third party; for non-manifestly illegal content, only a Court order can trigger that liability; in Italy, Article 16 of Decree law 70/2003, which transposes Article 14 of the e-Commerce Directive, requires that the illegal material be removed only upon the order of the competent authority. Therefore, only the authority's order triggers actual knowledge. Only recently courts have admitted that actual knowledge may be acquired by a complete notice send by the person/right holder; in Romania, a service provider is reputed to have knowledge only if the illegal character of the information has been declared as such by a public authority; in the Netherlands, the Gerechtshof Amsterdam established that, for establishing when a service provider "obtains actual knowledge", a mere notice by a third party of the presence of unlawful information was not sufficient; in the specific field of copyright and intellectual property rights, however, it has been traditionally assumed that rights holders' notifications trigger that liability. In other legal systems, like in the US' DMCA, notice-and-takedown procedures are exclusively foreseen for copyright claims. For other types of illegal content, the Fourth Circuit established a foundational and expansive interpretation of § 230 of the Communication Decency Act, by considering that "liability upon notice has a chilling effect on the freedom of Internet speech." In Europe, the legislators opted for a different solution, and established a conditional exemption of liability – rather than unconditional – for all types of illegal content. This opens the way to notice-and-action procedures that are not limited to copyright infringement. While usually all known online platforms provide with a reporting mechanism, a different question is whether those private reports trigger actual knowledge by the service provider and hence potential civil or criminal liability.

rulings, has also clarified and interpreted how some of the notions set out in Article 14 ECD, and thus the edges around the safe harbour for hosting services, shall be understood.

As a result, the current framework set out in the ECD does not lead to harmonized and uniform rules for hosting services as regards illegal activities or information intermediated on their platforms. On the contrary, the current scenario shows a mosaic of varied national regimes applicable to hosting services based on the Member State of establishment.

Consequently, users and customers in the EU are not offered a minimum level of uniform protection against illegal content and products intermediated on hosting services. The protection of users and costumers, as well as their ability to participate in the process of addressing illegal content online (for instance via notice systems) greatly depends on the Member State of establishment of the service provider. . This is also true when it comes to the safeguard of their fundamental freedoms online, mainly freedom of expression. Users accessing service providers established in Member States that have enacted specific provisions to safeguard freedom of expression in the process of content moderation online will benefit from stronger protection of their fundamental freedoms.

The specific duties and obligations regarding the processing of illegal content to which they will be subject is likely to be a factor of consideration for hosting services when deciding where to establish themselves in the EU. In accordance to the internal market principle, in complying with relevant national rules hosting services established in a Member States will, in principle, be able to lawfully offer their services across the Single Market. Consequently, hosting service providers are likely to establish themselves in Member States with less stricter regimes for the take down of illegal content.[11] This form of forum shopping has a direct impact on the protection of users and costumers in the EU, both as regards illegal content and to what concerns the safeguard of their fundamental freedoms.

An additional aspect to be considered is the growing importance of hosting services being offered in the EU from third countries. The ECD applies to service providers established in one of the Member States of the EU. Consequently, the regulation of hosting service providers established is not harmonized at EU level, which leaves a vacuum in the protection of EU citizens from illegal content being intermediated on this countries and available in the Single Market.

3. Country-specific notice-and-action procedures or other due diligence obligations as regards the content they host

The ECD does not, however, harmonize the duties or procedural obligations for hosting services in addressing illegal information and activities on their services. Paragraph 3 of the Article 14 expressly recognizes the ability of Member States to adopt national rules in this regard for hosting services established in their territory.

An extensive overview of national initiatives to put in place a notice-and-action procedure was included already in the Impact Assessment accompanying the document Proposal for a

[11] As a means of example, we may observe the situation in Ireland, which is home to many popular hosting service providers. At the time of drafting this report, Ireland does not have in place notice and action system nor defined timelines for removal of content for illegal content intermediated via hosting services established in their territories.

Regulation on preventing the dissemination of terrorist content online[12]. Furthermore, some Member States have in the meantime legislated in the field (France, Germany) or have notified their intention to do so (Austria). Summarising details, it results that:

- Nine Member States (Finland, France, Germany, Greece, Hungary, Italy, Lithuania, Spain and Sweden) have implemented a notice-and-action procedure in their legislative frameworks. For five of them (Finland, Greece, Hungary, Italy and Spain) this only applies to copyright infringements and related rights thereof.
- Furthermore, in several Member States (Finland, France, Hungary, Lithuania), minimum requirements for the notice are defined within law, to ensure that it is sufficiently motivated. In Member States without statutory requirements for notices, the case law has provided indications concerning the content of the notice and the mechanism.

Furthermore, the mentioned Annex shows that key elements such as the minimum content of the notice, the possibility to issue a counter-notice, the timeframe to react to a notice, potential mandatory measures against abusive notices or the possibility to submit contentious cases to an independent third party diverge greatly from one Member State to another.

As a consequence, an online platform offering for instance a video uploading feature, established in one EU Member State, should adapt its reporting functionalities to allow for copyright claims under the specific conditions established by law in Finland, Hungary, Lithuania, the United Kingdom, Spain, Sweden and by case-law in Belgium, the Czech Republic, Germany or Italy (and try to comply with contradicting rulings). For that purpose, it should probably hire and maintain in-house specialists and subcontract local legal experts in each and every Member State where it desires to offer its services. Furthermore, users will see their fundamental rights protected differently when posting content or when signalling illegal content, depending on the place where the content is hosted, or the citizen lives.

Specific provisions safeguarding the freedom of expression

The blocking of certain content can have a negative impact on the exercise of the rights to freedom of expression and information. Therefore, in recital 46 the ECD states that the removing or disabling of access 'has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level'.

In practice, this requirement often translates in certain obligations on hosting providers to set up and operate content moderation processes that allow affected users to submit counter-notices to defend the legality of the information at issue.

- In 13 Member States, some form of opportunity to dispute the allegation exist. However, the situation in which counter-notices are possible differ greatly amongst Member States. For example, a counter-notice in Estonia is only possible when the removal order is ordered by a government agency; in Finland, Greece, Hungary, Ireland, Italy and Spain counter-notices are only possible in the context of copyright; and in Luxembourg, it is only possible during the merit procedure.

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:408:FIN

In eight Member States (Bulgaria, Estonia, France, Germany, Greece, Lithuania, Portugal and Sweden), some sort of alternative dispute settlement mechanism exist. For example in Portugal, there is an out of Court preliminary dispute settlement possible in case the illegality of the case is not obvious; in Estonia, a specific alternative dispute regime exists for copyright infringements, in which a specific committee can resolve disputes.

4. Recent national laws being increasingly adopted by Member States whose scope would also apply to services provided from another Member State[13]

Points (i) and (ii) above already present a very fragmented picture of the legal framework to which a hosting service provider has to comply in the EU, and the different degrees of impact on the content shared by users over their services. This general fragmentation is furthermore exacerbated by recent trends in some Member States to regulate services regardless of their place of establishment, despite the general prohibition to restrict the cross-border provision of services.

Indeed, in the past few years we have observed an increasing interest in the regulation of information society services in Member States. This trend targets mainly duties and obligations for online platforms to address content hosted in their services that would be illegal under national law, but also other kinds of "duties of care", transparency and cooperation with national authorities, not least by imposing obligation to appoint a legal representative in the territory of several Member States.

Some of the recent national measures adopted by Member States in this regard aim to apply to those hosting services with a distinctive presence in their national markets. As such, these national laws would also cover hosting services, regardless of their establishment, including the possibility to impose sanctions.

Member States have justified the adoption of national laws with extraterritorial application on the need to protect their citizens against the impact of online platforms when intermediating content, be it illegal content or not. They claim the regime set out in the ECD, and in particular the available derogations from the internal market principle, is not sufficient to ensure the protection of their national users in view of the realities of the online environment.

Regardless of the justification, proportionality or adequacy of the policy goal behind such national initiatives, the extraterritorial application of most of these national measures to online platforms established outside the concerned Member States adds to the existing legal fragmentation in the Single Market.

4.1. Examples[14]

[13] This report does not reflect any position of the Commission as regards the compatibility of national laws mentioned in this section with EU law.

[14] This section contains a non exhaustive list of recent laws adopted by Member States aimed at fighting illegal content online which apply on an extraterritorial manner. The list focuses on national measures imposing obligations on online platforms, mainly hosting services, to remove or disable access to content which would be illegal under national law. It does not, however, cover national laws applicable to foreign online services covering other policy areas.

- ***Network Enforcement Act of 2017 (Netzwerkdurchsetzungsgesetz or "NetzDG")***

In force since 1 January 2018, in 2017 the German authorities adopted the first national law of this kind imposing on social networks certain obligations to allow for the swift detection and removal of content that would constitute a criminal offence under national law. The aim was to improve the enforcement of German criminal law online, notably in terms of deletion of content.

In terms of scope, the obligations set out in the NetzDG apply to social networks with at least two million registered users in the Federal Republic of Germany. The NetzDG lists a set of 22 criminal offences covered by such obligations, including some as criminal defamation and hate speech which determination is largely contextual.

The NetzDG main obligations include a requirement for social networks under its scope to set up a notification system allowing users to report to the platform individual pieces of content which would constitute a criminal offence under German national law. Social networks are also required to implement procedures that ensure obviously unlawful content is deleted within 24 hours of receiving a complaint. If there is any doubt regarding a takedown decision, the procedure may take up to seven days. After that deadline, a final decision on the lawfulness of a post must be reached and unlawful content needs to be removed, that is, either blocked or deleted. The fines for a breach of this obligation can reach up to €50 million.

In addition to complying with this operational provision, social media platforms are also obliged to publish bi-annual reports. In July 2019, the Federal Office of Justice issued an administrative fine of 2 million EUR against Facebook for incomplete reporting. The main argument was related to the relatively low number of complaints filed under the NetzDG compared to other social media providers, which the authorities took as an indication for the complaint from being too difficult to find.

- ***Draft Act combating right-wing extremism and hate crime***

On 18th June 2020, Germany enact a new Act that would, among others, amend the 2017 NetzDG. The aim of the amendment would be strengthen the fight against illegal content on social networks by facilitating the prosecution of criminal offences by German law enforcement authorities.

With this aim, the amendment would impose new obligations to social networks under the scope of the original NetzDG. In particular, it creates a new requirement for such services to report to German law enforcement authorities certain content which has been removed/disabled and which constitutes sufficient evidence of a serious criminal offence. This obligation to report also includes user data of the uploader, including IP address and passwords.

In practice, this obligation is likely to require social networks to carry out an additional assessment of the content removed or disabled to determine whether it can be deemed to constitute sufficient evidence of a serious crime and would thus need to be reported. The assessment as to whether there is such evidence is often highly contextual and therefore complex. Moreover, the assessment is not guided by a legal standard that would help the providers determine whether or not there is sufficient evidence to justify reporting the

content in question. Failure to comply with the new obligations is subject to the same financial penalties as foreseen in the current NetzDG.

- ***Draft Act amending the Network Enforcement Act***

Separately, at the time of drafting this report, the German authorities are also working on an additional amendment to the 2017 NetzDG. According to the information facilitated by the German authorities[15], this amendment aims at further improving the systems set out in the current NetzDG in order to make the fight against illegal content online more effective.

The amendment would impose on social networks under the scope of the NetzDG further and more detailed obligations in terms of the systems to allow users to send notices, the procedure for the removal or disabling of access and the reporting and transparency requirements. These new duties thus constitute new or stricter obligation for social networks having at least 2 million registered users in Germany, including those providing cross border services into Germany. Failure to comply with the new obligations is subject to the same financial penalties as foreseen in the current NetzDG.

- ***Law aimed at combating hate content on the internet (Loi contre la cyberhaine or Avia Law)***

In May 2020 the French National Assembly adopted the so called Avia Law which imposed strict obligation on online platforms and search engines as regards notice and take down or disabling access to illegal content. The Law was aimed at fighting against hate speech and other forms of illegal content disseminated making use of hosting services.

The French authorities argued that the adequate protection of French citizens from content that would be illegal under French law called for strict regulation of online platforms and search engines available in the French territory, regardless of their place of establishment. As such, the Law would apply to those services surpassing a certain threshold of connections from the French territory (to be established at a later stage by decree).

The text adopted by the National Assembly imposed on online platforms and search engines strict obligations in terms of systems to send notices and, specially, of removal or disabling access to notified content. According to the Law, services would be required to remove or disable access to individual pieces of manifestly illegal content within 24 hours of receiving notification; and within 1 hour for child pornography and terrorist content.

Services under the scope of the Law would also be subject to reporting and transparency obligations on their content moderation activities and technical and human means devoted to it. The French regulatory authority would also be granted broad powers of supervision and enforcement, including the issue of binding guidelines.

The Law would subject individual failures to comply with the removal or disabling of access to individual pieces of content, within the prescript timeframes, to significant financial penalties of up to EUR 250.000.

[15] https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=174

By decision of June 2020, the French Conseil Constitutionnel concluded that the main obligations set out in the Law would create a disproportionate impact on fundamental rights and would thus be contrary to the French Constitution. Consequently, most of the requirements for online platforms and search engines were declared nulled.

Some other Member States are currently working on or have announced their intention to enact national laws aimed at imposing obligations of online platforms to tackle illegal content online. From the information available at the time of drafting this report, it is likely that these upcoming laws would also be designed to apply to services available in the concerned territory, regardless of their establishment. As such, these would add to the already increasingly fragmented legal framework for online services in the EU.[16]

4.2. The specific requirement of appointing a legal representative

Under EU law, in general a service can be provided from one Member State to recipients established in a different Member State. Limitations to that free provision of services can only be justified based on overriding reasons of general interest, and insofar as they are proportionate and adequate. Under the ECD, an information society service provider only needs to comply with the rules under its place of establishment. Member States cannot regulate (or impose restrictions to the provision of services to) providers established in a different Member State.

However, as explained above, more and more Member States target services regardless of their place of establishment. This generates an enforcement challenge, as these services –not established in their territory- are outside their jurisdiction. In order to be able to enforce those rules, in recent years, laws enacted in several Member States and targeting online platforms in different sectors include an obligation, for platforms in scope but not established in their territory, to appoint a legal representative within their territory.

This has been the case, for example and not exhaustively, in the German NetzDG, the French Avia Law, the recently notified Austrian draft law to combat hate speech online, the German draft law to protection of minors[17] or the Italian "Airbnb" law[18].

Furthermore, in a case related to a similar obligation in Spain[19], the Court of Justice already established that a national provision imposing an obligation to appoint a tax representative resident in that Member State would contravene Article 56 TFEU for being disproportionate to the objective pursued.

4.3. National laws on data sharing

[16] In 2019 the UK published its Online Harms White Paper, which sets out the government's plans to impose on online services available for UK users, new duties of care and responsibilities to safeguard users' safety online.

On 2nd September 2020, Austria notified to the Commission a national law to combat hate speech online, increasing the responsibilities of online platforms and very much inspired on the German NetzDG.

[17] Entwurf eines Zweiten Gesetzes zur Änderung des Jugendschutzgesetzes, notified to the Commission via TRIS (reference number 2020/411).

[18] Decree no. 50/2017.)

[19] Case C-678/11.

Member States are increasingly regulating the access of public authorities to data that online platforms hold. The majority of these national laws are applicable to online platforms offering services in the area of collaborative economy. The rationale behind these laws is that Member States need data from platforms so that they can enforce the obligations applicable to the providers of the underlying services (e.g. obligations related to taxation, health and safety, planning, registration and so on).

In March 2020, the European Commission reached an agreement with 4 large platforms in the area of short term rental accommodation services on data sharing. This agreement allows Eurostat to publish aggregate data on short-stay accommodations offered via these platforms across the EU. However, cities do not consider aggregate data to be sufficient for the purposes of enforcement of local rules.

Some examples of the regulatory fragmentation regarding data reporting are the following:

-**Spain:** a Royal Decree[20] imposed the obligation on platforms intermediating short-term rental accommodations for touristic purposes to provide the Tax Authorities with data on a quarterly basis as from January 31st, 2019 and through the Government platform. The data relate to the identity of the homeowner, the property, the guest, number of renting days, amounts perceived by the homeowner for the renting of the property.

Another draft Royal Decree still to be finally adopted would also set out obligations relating to document registration and information for natural or legal persons offering accommodation and motor-vehicle rental services is under preparation. The draft Royal Decree establishes the same obligations simultaneously for providers of underlying services (accommodation or motor-vehicle rental services) and for digital platforms dedicated to intermediation in these activities via the Internet. Digital platforms must collect and register information related to the provider of the underlying service, the place where the service is provided, the user and the transaction itself. The notified draft provides a lighter regime for 'web portals which act exclusively in the area of publishing classified ads, which do not directly or indirectly provide payment functionalities' by not obliging them to collect and register additional data than the ones collected in the normal course of their activities.

- Czech Republic: A recent law[21] imposes data sharing obligations on online short-term accommodation platforms. The data to be communicated to the authorities are the number of tourism service contracts concluded, the total price for tourism services for the period specified, the address of the place where the tourist services are provided, the price for the service or the number of contracts concluded per host, the designation of the service provider with which it has mediated the conclusion of a contract relating to the provision of tourism services to the customer (for a natural person, his or her name and surname, date of birth and permanent address must be provided).

- France: Law N°2018-898 enacted on October 23rd, 2018 and entered into force on January 31st, 2020 requires short-term rental platforms to share with the French Tax Administration a yearly report regarding the vacation rental properties advertised through

[20] Royal Decree 1070/2017 of 29 December

[21] The amendment No 10 on Certain Conditions of Business and on the Execution of Certain Activities in the Field of Tourism (Platné znění dotčených částí zákona č. 159/1999 Sb., o některých podmínkách podnikání a o výkonu některých činností v oblasti cestovního ruchu, s vyznačením navrhovaných změn)

online platforms. Data to be provided relate to the identification of the providers of accommodation services, revenue etc.

- Austria: Several laws have been adopted at regional level regulating data sharing in the area of tourism. The Act on tourism promotion in **Vienna** (Vienna Tourism Promotion Act – WTFG)[22] provide that platforms need to notify to the authorities the contact data of the accommodation providers registered with them, along with all the addresses of the accommodation (accommodation units) registered with them within the territory of the city of Vienna. The provincial Act promoting tourism in **Upper Austria** (Upper Austrian Tourism Act 2018)[23] sets out obligations for platforms to forward (upon request) data about the service providers to the Upper Austrian authority responsible for collecting tourist tax. The Act amending the **Styrian** Act on Overnight Accommodation and Holiday Home Tax[24] online platforms are requested to forward information on service providers, not upon request, but automatically following a new registration of a host. Platforms are also requested to submit an overview of bookings every 3 months.

- Italy: Law Decree No. 50/2017 and its implementing measure[25] impose the obligation on online platforms intermediating short-term rental services to transmit data relating to the short lease contracts concluded on their platforms to the Agenzia delle Entrate.

- Greece: A law[26] in Greece introduces data sharing obligations for online platforms. According to the rules, platforms must share specific data related their sellers with the tax authorities, upon their request.

4.4. Impact on hosting services and users in the EU

Without prejudice to the legitimacy of the policy objective and capacity to block illegal content, the application of several, diverging national laws imposing obligations on the same online platforms as regards intermediated content increases the legal fragmentation in the Single Market. As such, it has considerable repercussions for both digital service and users across the EU.

Contrary to the scenario based on the internal market principle, online platforms wishing to scale up and offer their activities across the EU are required to comply with various national legal systems.

---

[22] Article 15(2) of the Wiener Tourismusförderungsgesetz, available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrW&Gesetzesnummer=20000355.

[23] Article 49(3) of the Landesgesetz zur Förderung des Tourismus in Oberösterreich, available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrOO&Gesetzesnummer=20000953&FassungVom=2023-12-31.

[24] Article 4a of the Steiermärkisches Nächtigungs- und Ferienwohnungsabgabegesetz, available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrStmk&Gesetzesnummer=20000711.

[25] Provvedimento 12 luglio 2017, n. 132395; Disposizioni di attuazione dell'articolo 4, commi 4, 5 e 5-bis del decreto legge 24 aprile 2017, n. 50, convertito, con modificazioni dalla legge 21 giugno 2017, n. 96, recante disposizioni urgenti in materia finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo, available at http://def.finanze.it/DocTribFrontend/getContent.do?id={D33D12CA-3C16-4E2A-AE49-79C6ABFD253D

[26] Par. 3a of article 15 of law 4174/2013 applicable as of 12/12/2019

This entails that online platforms are faced with higher compliance costs. Although complex to quantify, information provided to the Commission in the context of the recent amendments to the NetzDG indicate an additional cost per provider of EUR 2.1 million annually and one-time compliance costs of EUR 300 000, for the first amendment, and one-time compliance cost of EUR 284 000, for the second amendment.[27]

In the specific case of obligations to appoint a legal or tax representative, for instance, and having in mind that –without prejudice to the cost estimations made by the Commission in this document- the German NetzDG estimated that such an obligation would imply a cost of EUR 1 million annually, this would mean that a platform of a relative size –to be covered by the mentioned national laws- would need to invest EUR 4 or 5 million yearly only to comply with these obligations.

Aside from higher economic costs, online platforms wishing to offer their services in more than one Member State are also faced with higher legal uncertainty. In fact, service providers would need to closely monitor and follow the legislative processes and case law in all Member States were they are present. They would need to constantly adapt their policies to the various national legislative and judicial developments.

In practice, this fragmented regulatory environment is likely to result in only large online platforms being able to innovate and scale up in the EU, to the detriment of smaller or emerging services. Regulatory fragmentation thus endangers the full completion of the digital Single Market.

The extraterritorial application of these national rules aimed at counteracting illegal content online does not ensure an adequate and uniform protection of all EU citizens. Users residing in Member States having enacted stricter rules are likely to be afforded a higher level of protection against illegal content in such Member State. This level of protection would not extend to other EU citizens. An indirect incentive of this unlevelled protection may be an additional pressure on other Member States to enact similar rules, which would in turn add to the already increasing legal fragmentation in the EU.

5. Concluding remarks

The current ECD does not harmonize the rules applicable to online intermediaries as regards third party illegal information (content or products) being disseminated on their services, or other due diligence obligations such as transparency reporting. Especially in the context of hosting services, this lack of a European wide harmonized framework has resulted in increasingly regulatory fragmentation in the EU.

The recent regulatory trends existing at national level create clear risks for the digital Single Market and prevent both businesses and users from reaping all its potential benefits.

[27] This information was facilitated to the Commission by the German authorities and is available in the following link: https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=352 ; https://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2020&num=174

In this context, in order to complete the Single Market for online platforms while ensuring an adequate and uniform level of protection of all EU citizens, it seems necessary to create harmonized rules for online platforms available in the EU.

Annex 7: Regulatory coherence

a) Initiatives taken to address the problem of illegal content and suspicious activities online

Initiatives	***Purpose and Scope***	***Relationship with ECD; assessment***
Commission Recommendation of 2018 on measures to effectively tackle illegal content online - C(2018) 1177	Hosting service providers to exercise a greater responsibility in content governance to swiftly detect, remove and prevent the re-appearance of illegal content online, based on: • Clearer 'notice and action' procedures. • More efficient tools and proactive technologies, where appropriate. • Stronger safeguards to ensure fundamental rights. • Special attention and support to small companies. • Closer cooperation with authorities.	As a non-binding instrument, the Recommendation cannot be enforced and it does not reach "bad-faith" operators nor operators established in third countries
Directive 2019/790 on copyright and related rights in the Digital Single Market (the "Copyright Directive")	The Directive covers online content-sharing services (services giving public access to large amount of copyright-protected content uploaded by their users). Art 17 introduces a new conditional liability regime for online content sharing services.	Article 14(1) of the ECD does not apply to the situations covered by Article 17 of the Copyright Directive The obligation for online content-sharing services to make their best efforts to ensure the unavailability of specific works and to prevent their future re-uploads, which should be carried

		out in cooperation with right holders, "shall not amount to general monitoring obligation" provided for by article 15 of the ECD The Copyright Directive does not cover any hosting service providers other than those captured by the definition of "online content sharing services"
Directive 2018/1808 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 ("AVMSD")	The Directive covers video-sharing platform services providing programmes or user-generated videos to the general public Art 28(b) requires that MS ensure that video-sharing platform services take appropriate measures to protect minors from harmful audiovisual content, and to protect the general public from audiovisual content constituting illegal hate speech and audiovisual content whose dissemination constitutes a criminal offence under Union law (i.e. terrorist content, CSAM), as well as appropriate measures to ensure compliance with audiovisual commercial communications requirements under the AVMSD	In the event of a conflict between the ECD and the AVMSD, the AVMSD shall prevail, unless otherwise provided for in the AVMSD Article 28(b) is "without prejudice to Art 14 ECD" and "shall not lead to ex-ante control or upload filtering which do not comply with Article 15 ECD Does not cover any hosting service providers other than those captured by the definition of "video-sharing platform services". It only covers certain categories of illegal audiovisual content and harmful content for minors. Art 28 provides for a "notice" mechanism for VSP, but not for a general notice and action system, e.g. for hateful text comments. Does not cover types of illegal audiovisual content other than Illegal hate speech, terrorist content, CSAM, as well as content which is harmful for children (i.e. may impair their physical, mental or moral development) and content infringing audiovisual commercial

		communications rules set by the AVMSD
Directive (EU) 2017/541 on combating terrorism	Article 21 of the Terrorism Directive requires Member States to take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence, as referred to in Article 5 that is hosted in their territory. Article 21 also stipulates that measures of removal and blocking must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress.	The Directive should be without prejudice to the rules laid down in the ECD, in particular to the prohibition of general monitoring and the limited liability regime.
Proposal for a Regulation on preventing the dissemination of terrorist content online COM/2018/640 *(*negotiations between the co-legislators are ongoing, hence some of the provisions in the Commission's proposal can be modified)*	The Regulation covers hosting service providers (which make information available to third parties). The proposal requires such providers to: - Remove or disable access to content within 1h of receiving a legal removal order from a competent authority in any MS. Give feedback to the competent authority. - Assess as a matter of priority the content identified in referrals from competent authorities in any MS and give feedback to them.	The Regulation is "without prejudice to Art 14 ECD"; a recital introduces "Good Samaritan" elements. The decision to impose specific proactive measures does not, in principle, lead to the imposition of a general obligation to monitor, as provided in Article 15(1) ECD. In exceptional circumstances, the authorities can derogate from Article 15 ECD, by imposing specific, targeted measures, the adoption of which is necessary for overriding public security reasons. A balance should be struck a fair balance between the public interest objectives and the fundamental

	- Report on the proactive measures taken, if they are exposed to terrorist content. These may include measures to detect, remove and prevent reappearance of terrorist content, following a removal order by a competent authority. When putting in place proactive measures, providers should ensure that users' right to freedom of expression and information is preserved. If the measures are not considered sufficient, the authority in the place of establishment can impose appropriate, effective and proportionate proactive measures. - Comply with a set of transparency and information obligations - Establish complaint mechanisms and adopt other safeguards to ensure that decisions taken concerning content are accurate and well-founded. - Inform national authorities, when they become aware of evidence of terrorist offences. Have a legal representative established within the Union, if they are not established within the Union. All providers should appoint a contact point with authorities.	rights involved, in particular, the freedom of expression and information and the freedom to conduct a business, and provide appropriate justification. Only addresses the relationship between providers and public authorities (including Europol), setting out procedures for legal removal orders, as well as for referrals of content sent by the authorities – does not directly address notices coming from users.
Regulation 2019/1020 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011		
Regulation (EU) 2017/2394 of the European Parliament	Sets minimum powers for competent authorities to require, 'where no other effective means are available',	The e-Commerce Directive is included in the

and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 ("CPC Regulation")	for a hosting service provider to remove, disable or restrict access to an online interface (i.e. website) or, where appropriate, to order domain registries or registrars to delete a domain name infringing rules in the Union laws that protect consumers	corpus of laws in scope of the Regulation as 'union laws that protect consumers' interests Competence for consumer protection authorities to require the removal of content is set in observance of Article 14 (3) of the e-Commerce Directive.
Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography	Established minimum rules for a harmonised definition of criminal offences related to sexual exploitation of children, child pornography and solicitation of children for sexual purposes. It sets a clear definition of child pornography (child sexual abuse material - CSAM), and defines as criminal offences acts of acquisition, knowingly obtaining access to, distributing, disseminating or transmitting, or offering, supplying or making available CSAM Article 25, obliges Member States to take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory. It also provides that Member States may take measures to block access to webpages containing or disseminating child pornography toward the Internet users within their territory, and refers to the need to provide safeguards. Such measures can take different	The Directive does not make direct reference to the e-Commerce Directive.

	forms (including legislative, non-legislative or judicial action) and are without prejudice to voluntary action by industry.	
Regulation (EU) 2019/1148 on the marketing and use of explosives precursors	The Regulation covers online marketplaces. It include obligations to report suspicious transactions (and actively seek facts or circumstances indicating illegal activity)	While there is no explicit reference to the ECD, recital 16 clarifies that online marketplaces "*shall not be held liable for transactions that were not detected despite […] having in place […] procedures to detect such suspicious transactions*"
Voluntary measures to address the problem of illegal content and activities online		
Code of conduct on hate speech (2016)	Voluntary cooperation between the major social media platforms and specialised NGOs as trusted flaggers of illegal hate speech. It establishes a privileged channel for Notice and Action processes for removing illegal hate speech, as well as a general cooperation including trainings platforms prepare for the NGOs, and transparency reporting	The Code of conduct supports the enforcement of the Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia. In line with obligation on the European Commission to encourage codes of conduct as provided for in Article 16 ECD
Memorandum of understanding on the sale of counterfeit goods on the internet (2011) and MoU with advertising platforms	Voluntary cooperation between brand owners and online market places and advertising platforms, respectively. Includes exchanges of information and privileged Notice and Action channels for brand owners, as well as regular transparency reporting and	In line with obligation on the European Commission to encourage codes of conduct as provided for in Article 16 ECD

	best practice exchanges.	
Product Safety Pledge	Seven online marketplaces have voluntarily committed to improving the safety of non-food consumer products sold on their online marketplaces by third party sellers. The ultimate goal is to improve the detection of unsafe products marketed in the EU before they are sold to consumers or as soon thereafter as possible, and to improve consumer protection.	In line with obligation on the European Commission to encourage codes of conduct as provided for in Article 16 ECD
Commission Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament	Ask Member States to in line with their applicable rules, encourage and facilitate the transparency of paid online political advertisements and communications. Member States should promote the active disclosure to citizens of the Union of information on the political party, political campaign or political support group behind paid online political advertisements and communications. Member States should also encourage the disclosure of information on campaign expenditure for online activities, including paid online political advertisements and communications, as well as information on any targeting criteria used in the dissemination of such advertisements and communications. Where such transparency is not ensured, Member States should apply sanctions in the relevant electoral context. Provided analogous recommendation to national and European political parties	

Code of practice against disinformation	The Code of practice is the first worldwide self-regulatory set of standards to fight disinformation. The Code was voluntarily signed in October 2018 by online platforms and trade association representing the advertising industry. It covers five areas: 1) Disrupting advertising revenues of certain accounts and websites that spread disinformation; 2) Making political advertising and issue based advertising more transparent; 3) Addressing the issue of fake accounts and online bots; 4) Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content; 5) Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms' data.	In line with obligation on the European Commission to encourage codes of conduct as provided for in Article 16 ECD

b) Initiatives of relevance for other provisions of the ECD

Examples of initiatives	*Related provisions in the ECD*

Consumer acquis: • Unfair Commercial Practices Directive 2005/29 • Consumer Rights Directive 2011/83 • Directive of the European Parliament and of the Council 2018/0090 amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules ("*New Deal for Consumers*")	Transparency and requirements on commercial communications already established in Art 6-8 in the ECD are further reinforced by the consumer acquis – e.g. in making clearly identifiable a sponsored result on a search engine. The New Deal for Consumers has established additional information obligations specifically for online marketplaces to make sure that consumers fully understand the legal status of the supplier of products (goods and services) and how this status affects their consumer rights. It has also established inter alia a new information requirement to inform the users about the default parameters for ranking search results, e.g. price, distance, consumer ratings, or a combination of those. Moreover, traders must be transparent when search results are influenced by payments. These obligations apply to both EU-established online platforms and platforms established outside the EU provided they target consumers in the EU. The interplay between consumer law obligations and other requirements or exemptions stemming from the ECD is currently addressed through a very general provision ensuring the coexistence of the two frameworks "without prejudice" to each other. Their applicability however has to be assessed on a case-by-case basis.
Contracts-relevant legislation: • Unfair Contract Terms Directive 93/13 • Consumer rights directive 2011/83 • Digital Contracts Directive 2019/770	Article 9 of the ECD provides a framework for the equivalence of contracts concluded by electronic means. There is no overlap with the relevant consumer protection acquis.

Out of court dispute resolution • Regulation (EU) 524/2013 on ODR for consumer • Directive 2013/11/EU on ADR for consumer disputes • Regulation on promoting fairness and transparency for business users of online intermediation services (P2B) 2019/1150	Article 17 encourages the establishment of out-of-court dispute settlement between information society services and the recipient of their service (both consumers and businesses) This is further strengthened by the ADR and ODR provisions, as well as the relevant provisions of the Platform-to-Business Regulation.

Annex 8: Cross-border cooperation

1. ECD COOPERATION MECHANISM

Article 3 ECD embodies the fundamental principle of the country of origin for digital services in the EU. According to Article 3(1), providers of information society services in the EU must comply with the laws of the Member State where they are established, rather than the laws of 27 Member States in which they potentially offer their services. Member States are not allowed to restrict the provision of services offered by a provider established in another Member State for reasons falling within the coordinated field.

Article 3(4) ECD sets out strict conditions under which a Member State can derogate from the above principle in respect of a given information society service. In particular, a host Member States may take restrictive measures against a given information society service under the following conditions: (a) the measures are necessary and proportionate for the protection of public policy, public security, public health or consumers, and (b) the Member State of destination firstly asks the Member State of establishment to take adequate measures in respect of a given information society service and if the latter does not do so, the Member State of destination notifies the Commission and the home Member State of its intention to take such measures.

As from 2013, the procedural requirements set out under letter b) above are normally fulfilled through the use of the Internal Market Information System (**IMI system**)[1].

Based on the evidence collected the last 20 years, the following trends can be observed:

Member States are generally supportive of a well-functioning cross-border mechanism…

In the context of the evidence gathered for the purposes of the present Impact Assessment, the Commission sent also a targeted questionnaire to Member States enquiring about the national experiences on the ECD in the wider framework of challenges and opportunities brought forward by the evolution of digital services. Overall, 21 replies from 17 Member States (in one Member State 5 authorities replied) were received. The data show that Member States are generally supportive of the need for a cooperation mechanism for cross-border issues but highlighted the shortcomings of the current system. This also reflects the results of the 2019 Survey[2].

During the meeting of the e-Commerce Expert Group in October 2019, the issues of cooperation and use of IMI were discussed. Despite the differences in the use of IMI, Member States widely expressed the need to have a functioning, strengthened but also simple

[1] Pursuant to Article 29(3) of the IMI Regulation[1] a pilot project has been launched since 2013 with a view to evaluate the use of the IMI information system[1] as an efficient, cost-effective and user-friendly tool to implement Article 3(4), (5) and (6) of Directive 2000/31/EC.

[2] A questionnaire was sent to Member States in 2019 for the evaluation of the use of IMI for the purposes of the e-Commerce Directive.

cooperation mechanism in the future, as this is important to ensure public interests in cross-border issues.

… but they are dissatisfied with several aspects of current system

In the 2020 questionnaire, a number of Member States expressed **dissatisfaction with the average timing or quality of the feedback** received by other authorities. The cooperation was considered to work better in issues harmonised by EU law (consumer protection, Article 5 ECD). Some Member States reported concerns about the use of the system in the application of national requirements, for which the country of origin might not have corresponding powers to enforce the request.

Eight Member States highlighted the **parallel use/existence of specific cooperation systems** alongside that of the ECD, for both sending and receiving requests of investigation, in particular the CPC network but also that of the AVMSD as regards media content.

The cooperation was considered to work better in issues harmonised by EU law (consumer protection, Article 5 ECD). Few Member States reported the use of the system in the application of national requirements and highlighted that for these aspects the country of origin might not often have corresponding powers to enforce the request.

Moreover, there is a general consensus about the need to ensure **the right to be heard** of providers, although it is also often stressed that this is ensured already in the context of national procedures for the application of any measure.

Nine countries stressed the **challenge in enforcing requirements against third country ISS**.

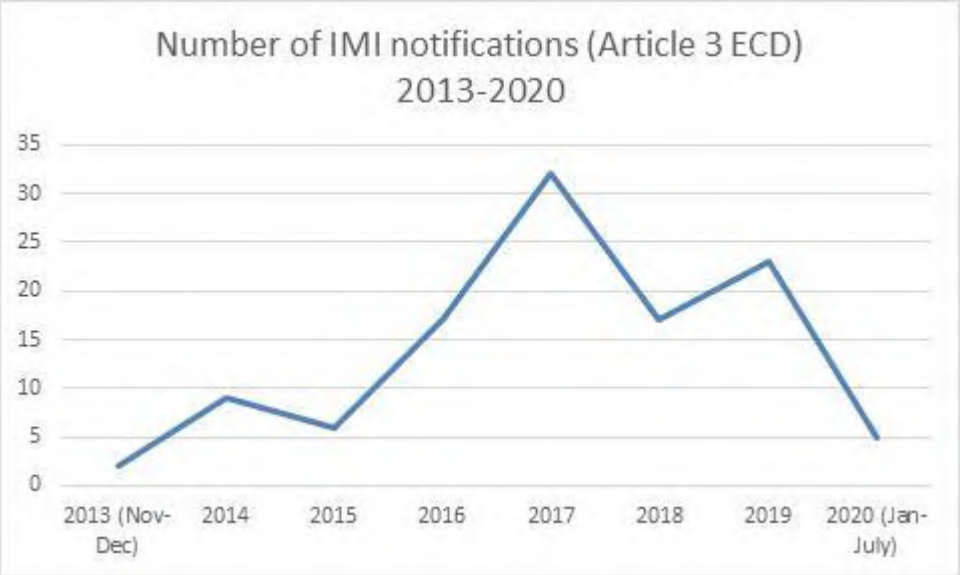
In the 2019 survey, Member States suggested improvements regarding the **awareness of the system** by the public authorities. Member States also highlighted that some aspects needed further clarifications, such as the **interrelationship between the ECD cooperation mechanism and other cooperation systems** (see analysis below), in particular the Consumer Protection Cooperation (CPC) mechanism. Member States also expressed the need for clarifications on the measures to be notified and the **interrelationship with other notification systems** (such as the notification obligation under Directive 2015/1535).

All the above contributed to the low use of the cooperation mechanism

In its 2012 Staff Working Document on Online services, including e-commerce, in the Single Market[3], the Commission reported a very low number of notifications (approx. 30 in the first 9 years after the entry into force of the ECD). Continuing this trend, between November 2013 and July 2020, 111 notifications were submitted to the Commission requesting a derogation from the internal market principle generally concerning individual measures vis à vis specific

[3] Commission Staff Working Document on Online services, including e-commerce, in the Single Market, SEC/2011/1641 final, accompanying the Commission's Communication on A coherent framework for building trust in the Digital Single Market for e-commerce and online services, COM/2011/0942 final

providers [4]. This number is still considered quite low, given the surge of cross-border online activities during the last decade.[5]



Among these 111 notifications, an overwhelming number of notifications originated by only two Member States (IT and, at the time, UK, the latter mostly concerning Value-Added phone services). The use of the cooperation mechanism appears quite concentrated with only a handful of Member States having used it.

It is not clear, however, whether the relatively low number of notifications reflects a limited number of cross-border issues or rather an under-utilisation of the tool by some or all authorities in different Member States.

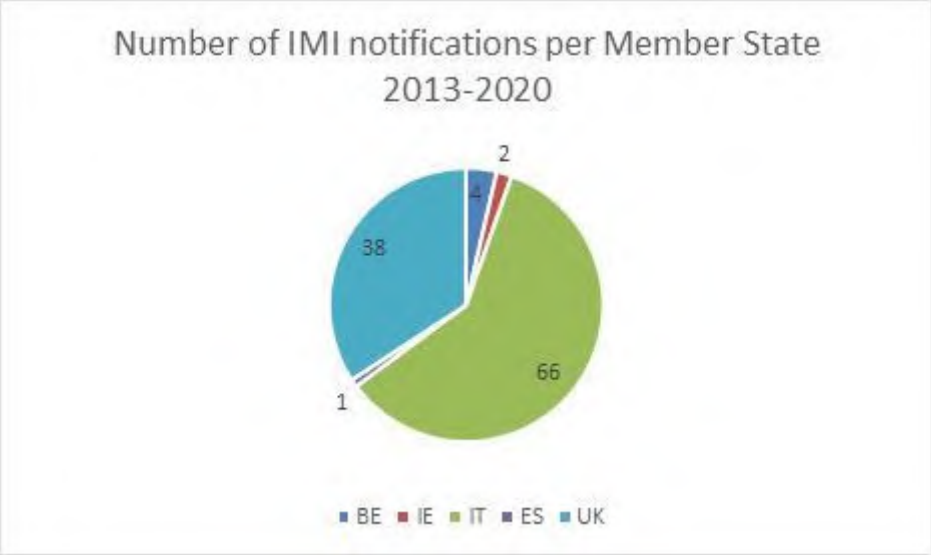
Surveys among the competent authorities in the context of the evaluation of the pilot project on the use of IMI for the purposes of the ECD show that awareness and utilisation of the tool are very different among Member States and, among different competent authorities, within Member States. Out of 26 Member States replying to a Survey[6] in 2019, 10 never used the tool. The responses to the 2020 targeted questionnaire highlighted a number of issues explaining the low use of the cooperation mechanism, taking also into account that a number of authorities (7) did not report direct experience of the system in sending and/or receiving cooperation requests. According to some Member States, the low number of cooperation

[4] Direct contacts between the Member State of destination and the Member State of establishment aiming at reaching an agreement on the measures to be taken (Art.3(4)(b) first indent of the e-Commerce Directive), which take place before the notification of the intention to take measures (Art. 3(4)(b) second indent), are also channelled through the IMI system. These are supposedly more numerous, as in a number of cases the issue is addressed by the Member State of establishment. However the 2019 Survey suggests that a majority of Member States did not take measures following Multiple goals, conflicting values and attempting to solve all the problems various business models and platform types is a recipe for confusion, conflict and unequal or failed enforcement. initial contacts from the Member State of destination.

[5] For example, in 2018 almost 10% of all EU enterprises sell on-line across the border, see Eurostat E-commerce data (2020) https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200420-1

[6] A questionnaire was sent to Member States in 2019 for the evaluation of the use of IMI for the purposes of the e-Commerce Directive.

requests is explained by the low awareness of the system but also by the well-functioning system of injunctions/N&A, ensuring removal of illegal content by the provider directly. Few Member States indicated in any case an increasing trend of cross-border issues, in particular as regards content.

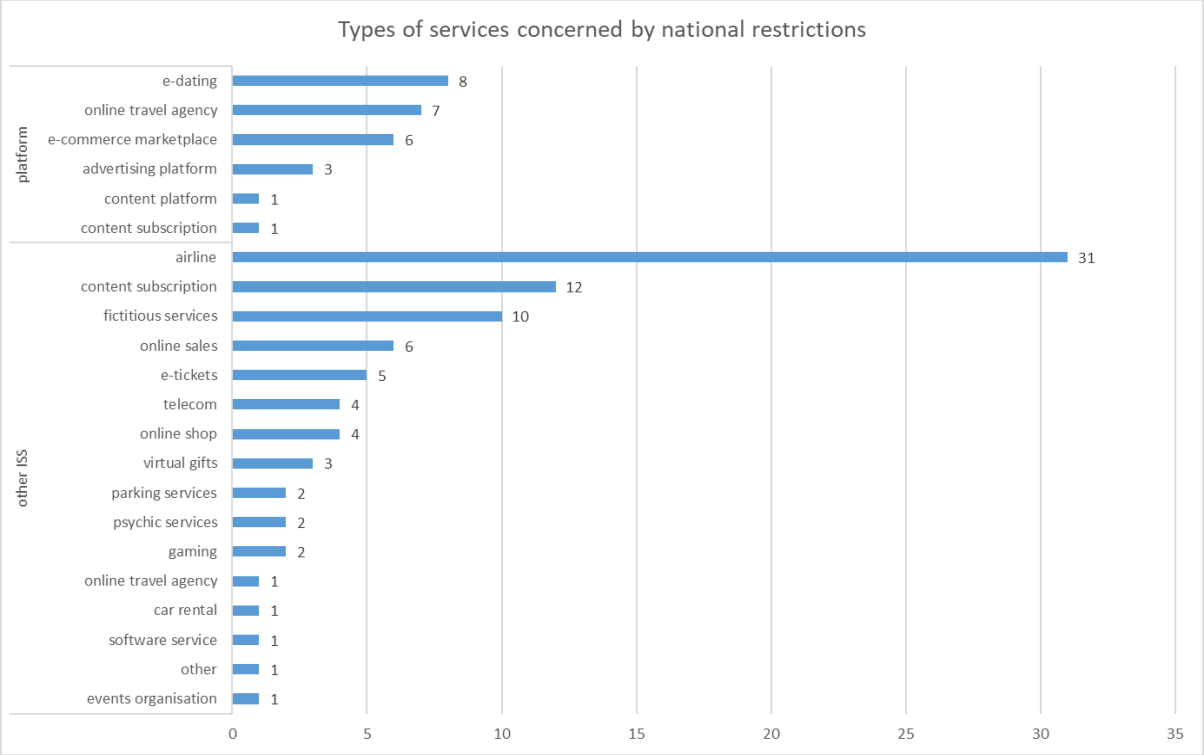


Characteristics of the received notifications

In the majority of cases (57) notified between 2013 and 2020, the **urgency procedure** was activated. Moreover, all notifications, are justified on the basis of the **protection of consumers** (only in a couple of cases accompanied with protection of health). Finally, **no decision** has been adopted by the Commission regarding the notified measures, taking also into account that these are normally very much linked to the specific facts at stake.

According to the targeted questionnaire sent to Member States for the purposes of this Impact Assessment, the **timing for responses** within the ECD cooperation system differs significantly across Member States. Some report an average response time below 1 month, and often around 2 weeks, while others mention much longer timeframes for reply, up to 1 year. Some Member States stress that the timing and quality of feedback also depends on the information provided by the requesting authority (that could be standardised), but also to the need for internal coordination with other authorities and proximity with the issue at stake.

The **types of services** which are targeted by the national measures vary significantly, with providers of airlines services to be the most common target of requests for measures.



INTERPLAY BETWEEN THE NOTIFICATION PROCEDURE UNDER THE ECD AND OTHER NOTIFICATION PROCEDURES

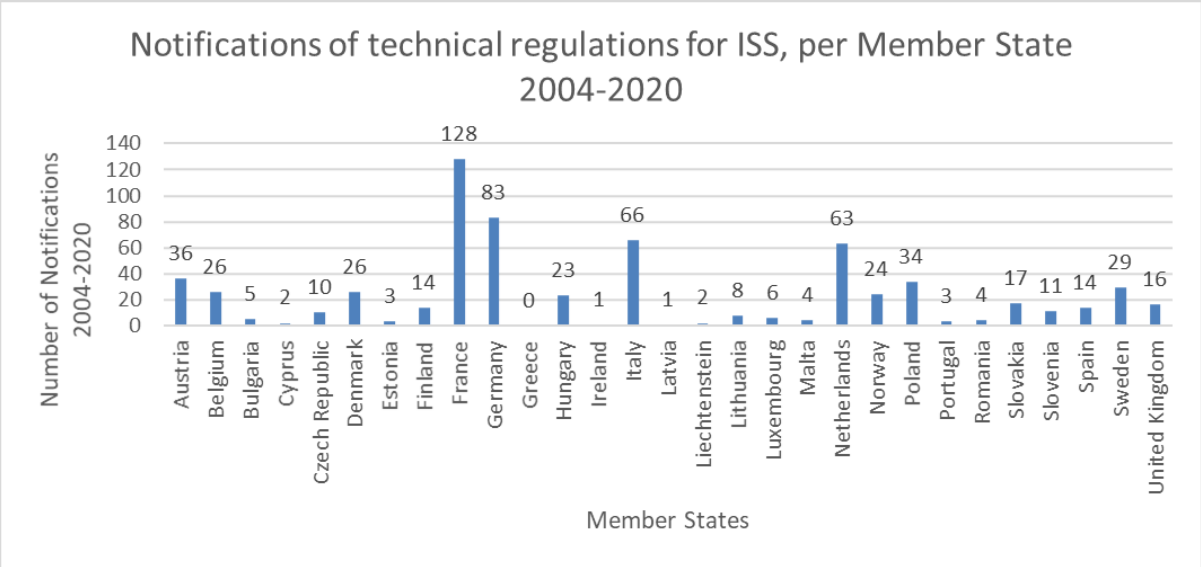
In the recent Airbnb case (C-190/18), the Court of Justice established the non-enforceability of measures which Member States failed to notify according to Article 3(4) ECD. At the same time, while the Court confirmed that the notification obligation is relevant also for provisions predating the ECD, it did not clarify in detail which measures and when these are to be notified, nor the interrelationship with other notification systems such as that provided for by Directive 2015/1535/EU. While some aspects in this regard were analysed in the AG opinion related to the on-line pharmacies case (C-649/18)[7], the Court considered that the existence of the relevant notification of the application of restrictive measures to a specific provider is a question of facts, which should be assessed by the national Court[8]. Therefore, uncertainties remain in this regard.

[7] One of the point discussed by the AG was the relationship between the notification pursuant to the Transparency Directive and that under the ECD, for which AG Opinion provides a clear distinction based on the different function and timing of the notification according to the two instruments, see para 115-121.

[8] See para 43 (*A cet égard, il convient de relever que, lorsqu'une réglementation nationale qui prévoit différentes interdictions ou obligations imposées à un prestataire de services de la société de l'information restreint ainsi la liberté des services, l'Etat membre concerné doit, en application de ladite disposition, avoir préalablement notifié son intention de prendre les mesures restrictives concernées à la Commission et à l'État membre sur le territoire duquel le prestataire du service visé est établi*) and para 45 (*Or, cette présomption ne saurait être renversée par la simple circonstance que l'une des parties au principal conteste un certain fait dont il appartient à la juridiction de renvoi et non à la Cour de vérifier l'existence*)

The **2015/1535 notification procedure** allows the European Commission and EU Member States to examine technical regulations for information society services that other EU Member States intend to introduce. According to Directive (EU) 2015/1535, Member States must inform the Commission of any draft regulation specifically aimed at information society services before its adoption. Starting from the date of notification, a three-month standstill period comes into place, during which the EU country must refrain from adopting the technical regulation in question. This procedure enables the Commission and other EU countries to examine the proposed text and respond. A breach of the obligation to notify renders the technical regulations concerned inapplicable, so that they are unenforceable against individuals.[9]

In the timeframe from 2004 to 2020, the Commission has received 659 notifications related to laws about information society services. The number of notifications varies considerably between Member States; for instance France has notified 128 laws related to information society services from 2004 to 2020, whereas Greece 0.[10]



The Commission issued comments for 131 notifications and detailed opinions for 39 notifications out of the 659.[11]

Therefore, it becomes clear that so far the ECD mechanism had been used for notifications of specific enforcement measures against specific information society service providers, while general laws applicable to information society services were notified under Directive 2015/1535.

However, given the Airbnb ruling, the above practice has been put in question. The lack of clarity regarding the use of the two notification obligations was also highlighted by Member States in the surveys conducted over the last years. In view of the significant consequences of

[9] Case C-194/94
[10] These numbers depend on the classification attributed to a notification by Member States.
[11] Detailed opinions with comments were counted individually for each reaction type

the failure to notify individual acts restricting the provision of services, brought by the Airbnb ruling, there is a need for legal certainty regarding the notification obligations.

The notification procedure of **Directive 2006/123 (Services Directive**[12] **)** could also be relevant for information society service providers. The Services Directive establishes a notification mechanism, which could incidentally also involve requirements applicable to information society services. The notification obligation set out in Directive 2006/123/EC requires Member States to inform the Commission and other Member States of requirements which restrict the access to and exercise of a service activity, including an information society service, such as authorisation schemes, (covered by Article 15(2), the third subparagraph of Article 16(1) and the first sentence of Article 16(3) of Directive 2006/123/EC). General rules entailing restrictions, *inter alia*, on information society services that would not be notifiable under the TRIS system (because not specifically aimed at information society services), therefore, would still be notifiable under the Services Directive.

In the period between 2018 and 2020, 17 notifications under the Services Directive could to some extent be considered relevant from the perspective of the ECD. The majority of the identified measures (15) were notified by Hungary and 2 were notified by Sweden. The requirements were mostly related to centralized IT services and just few of them concern retail and wholesale trade services (1), transport services (1), booking services (1), tourism (1).

OTHER COOPERATION MECHANISMS SUCH AS CPC: HOW THEY INTERFACE WITH THE ECD AND WOULD INTERFACE WITH DSA

The cooperation mechanism under Article 3 ECD provides for a general, horizontal system whereby all restrictions related to information society services need to be notified to the Member State of origin and the Commission. Other pieces of EU law provide for sector-specific cooperation mechanisms. Two of these mechanisms which are of direct relevance for information society services providers are the Consumer Protection Cooperation mechanism and the Market surveillance tool.

Consumer Protection Cooperation mechanism

The CPC Regulation (EU) 2017/2394 provides the EU-level framework for the public enforcement of EU consumer law and a series of actions to better fight cross-border infringements of consumer rights. These include a mutual assistance mechanism, alerts and coordinated actions. The framework is based on the general principle of the decentralised application of EU law: enforcement powers lie with the Member States whose authorities take relevant enforcement actions against traders infringing EU consumer law. The ECD is among the EU rules for the enforcement of which the cooperation mechanism of Regulation 2017/2394 applies (listed in the Annex of the Regulation). As from 2020 its cooperation mechanism is also hosted by the IMI platform.

According to the mutual assistance mechanism (bilateral exchanges with cooperation obligation), at the request of an applicant authority, a requested authority must take all

[12] Directive 2006/123 on services in the internal market

necessary and proportionate enforcement measures to bring about the cessation or prohibition of the intra-Union infringement. The requested authority determines the appropriate enforcement measures needed to bring about the cessation or prohibition of the intra-Union infringement and must take them without delay and not later than 6 months after receiving the request. The requested authority must use the electronic database provided by the Commission (Internal Market Information System as per the implementing decision) to notify without delay the applicant authority, the competent authorities of other Member States and the Commission of the measures taken and the effect of those measures on the intra-Union infringement.

Under the CPC Regulation, Member States' enforcement authorities can also conduct coordinated investigation and enforcement actions that are led by the Commission under mandatory timeframes when there is a reasonable suspicion of a widespread consumer law infringement with a Union dimension. Importantly, the Regulation also requires Member States to ensure that their enforcement authorities are endowed with a set of minimum powers to ensure swift and effective enforcement action in the event of cross-border consumer law infringements. Those include, inter alia, the power to block websites, carry out test purchases (so-called "mystery shopping"), request information (e.g. from domain registrars and banks) and impose fines. The Commission has a strong role in facilitating the network's activities e.g. on information gathering, monitoring and capacity building, including by regularly hosting network meetings and the network's collaborative IT tool.

Safety Gate/RAPEX and the Market Surveillance Regulation

With regard to unsafe goods, the Rapid Information System for dangerous non-food products (Safety Gate/RAPEX)[13] was established under Article 12 of Directive 2001/95/EC on general product safety as a system for quick exchanges between Member States of information about dangerous products. Where a Member State adopts or decides to adopt, recommend or agree with producers and distributors, whether on a compulsory or voluntary basis, measures or actions to prevent, restrict or impose specific conditions on the possible marketing or use, within its own territory, of products by reason of a serious risk, it must immediately notify the Commission and other Member States through Safety Gate/RAPEX, and other Member States. The General Product Safety Directive also includes market surveillance provisions related to non-harmonised products.

Under Regulation 2019/1020 (the new market surveillance Regulation), national market surveillance authorities will have the obligation to respond to mutual assistance requests and to take enforcement measures on harmonised products when requested by another authority, where bringing non-compliance with regard to a product to an end requires measures within the jurisdiction of another Member State. The requested authority must without delay take all appropriate and necessary enforcement measures using the powers conferred on it under the Regulation in order to bring the instance of non-compliance to an end. The market surveillance authorities are requested to efficiently cooperate and exchange information between themselves, the Commission and the relevant Union agencies.

According to the Regulation, a **Union Product Compliance Network** ("the Network") will also be established by January 2021. The purpose of the Network is to serve as a platform for

[13] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019D0417

structured coordination and cooperation between enforcement authorities of the Member States and the Commission, and to streamline the practices of market surveillance within the Union, thereby making market surveillance more effective.

Audiovisual Media Services Directive

Pursuant to Article 4 of the Audiovisual Media Services Directive 2010/13/EU, as recently amended by Directive 2018/1808, a cooperation mechanism is envisaged between the country of origin of a media service provider and the country where one or some of its services are wholly or mostly targeted to, with a view to ensure that certain public interest obligations in that latter country are complied with. Such system of cooperation is subject to specific substantive and procedural requirements that do prevail over those provided by the ECD (see article 4(7)), with regard the specific services at stake.

This system of cooperation applies to broadcasting and video on demand service providers. It does not, however, apply to the category of information society services constituting video-sharing platform service providers, as per Article 1 of the amended AVMSD and the Commission guidelines on the matter. Video-sharing platforms providers, as a sub category of information society services, are under the scope of the ECD, including the provisions under its Article 3.

The cooperation mechanism set out in the AVMSD aims to ensure that such services do not purposely establish themselves in the territory of one Member State while targeting another Member State with the aim of avoiding the stricter regulation of the later when it comes to matters of general interest. The main purpose is thus to reinforce the country of origin supervision and enforcement of the rules to services established in its territory while allowing certain role for the targeted Member State to safeguard certain public interests.

The deadline for the transposition of the AVMSD elapsed in September 2020. Consequently, there is still no meaningful data available that can illustrate the results of the application of this cooperation mechanism.

Relationship with ECD These sector-specific cooperation mechanisms aim at providing a system which reflects the specific needs of the areas related to consumer protection, dangerous and unsafe goods or media services wholly or mainly targeting other territories. Although similar to the cooperation mechanism under the ECD, there are significant differences among them. For example, since the CPC mechanism applies to specific legislation harmonised across the Union, it does not envisage the possibility for the requesting Member State to adopt measures instead of the country of establishment as provided for in Article 3(4) ECD. The CPC mechanism rather envisages a mechanism where disagreement between different national authorities on the actions to be taken may be referred to the Commission for its guidance[14]. Hence, the overlap between the ECD mechanism and the sector-specific mechanisms is not absolute, as the use of one or the other mechanism may lead to different outcomes. However, it is also evident that the use and interplay of the several cooperation mechanisms has been the source of confusion and lack of clarity for Member States.

[14] Article 14(4) CPC Regulation.

Additionally, given the horizontal nature of the cooperation mechanism established in the ECD and the need to provide for a future proof mechanism which will address the needs of future digital services (and the enforcement of DSA-specific obligations), there is a need for a strengthened, horizontal cooperation mechanism under the DSA. In the study commissioned by the European Parliament's IMCO Committee 'Enforcement and cooperation between Member States'[15], the author supports the need for the DSA to focus on horizontal internal processes and structures, rather than concrete risks and harms.

CONCLUSION

Since the entry into force of the ECD, there has been limited cooperation among Member States in addressing matters with a cross-border dimension. Member States have expressed **dissatisfaction** with the current framework around the administrative cooperation between national authorities, which has led to the **low use** of the system. Member States do not **trust** each other in addressing concerns about providers offering digital services cross-border, which has in turn led to **increasing regulatory activity at national level, fragmenting the digital single market.**

On the other hand, at principles level, Member States see added-value in a well-designed, efficient and effective cooperation mechanism for addressing cross-border issues. Despite the existence of sector-specific mechanisms, in light of new challenges and future services, a horizontal framework for administrative cooperation in the digital single market, capable of addressing cross-border matters, is needed more than ever.

[15] Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, Dr Melanie SMITH, PE 648.780– April 2020.

Annex 9: Liability regime for online intermediaries

1. CURRENT LIABILITY REGIME FOR ONLINE INTERMEDIARIES IN THE EU

1.1. Horizontal liability regime

Online intermediaries are facilitators of e-commerce and other activities on the internet. By nature, intermediaries provide services to third parties – the recipients of their service, including some that engage in illegal activities. If intermediaries were liable for any illegal activity on their services, they would only be able to provide a very restricted service – jeopardising the very business model of an online intermediary, or they would risk too onerous legal claims or even criminal charges.

The ECD grants harmonised conditional liability exemptions to certain intermediaries. This 'safe harbour' framework has been a core pillar of internet regulation, as it allows the proper functioning of information society services by protecting them from potential strict liability.

The ECD was adopted 20 years ago when the current variety, scale and potential of digital services were different. However, the logic behind the liability regime remains valid today. Already in 1996, the Commission considered that "the law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability"[1]. Hence, any update of the existing rules needs to bear in mind that the main principle of non-liability for third party content remains. However, it is also fair to say that when defining categories of online intermediaries in 2000, the legislator did not account for new services or for the current scale and impact of some online platforms. The evolution of services can be illustrated for instance with the economic difference between technical hosting services and consumer-facing online platforms.

The liability regime for online intermediaries is set out in Articles 12-15 of the ECD. The safe harbour framework is horizontal in nature: it can exempt these services from liability for any kind of information, most notably the categories of illegal content, and it covers both civil and criminal liability.

The Directive specifically addresses three kinds of services (see detailed examples of these services in section 2 below):

1. **mere conduit services** (Article 12), where the service is the transmission of information in a communication network, or the provision of access to a communication network (e.g. internet service providers);
2. **caching services** (article 13), where the service entails the automatic, intermediate and temporary storage of information transmitted in a communication network for the

[1] Communication from the Commission - Illegal and harmful content on the Internet (Brussels, 16.10.1996 COM(96) 487 Final).

sole purpose of increasing the efficiency of onward transmission (e.g. caching proxy servers);

3. **hosting services** (Article 14), where the service is storage of information (e.g. video-sharing and social media platforms).

The services can only benefit from the conditional liability exemptions if they fulfil the conditions laid down in the ECD, as explained in more details below. It is worth mentioning in addition that the Court has already established in a rich case-law the application of these categories to a great variety of services (some of which did not exist back in 2000). For example, ISPs, Wi-Fi hotspots or DNS registrars can be considered mere conduits, whereas cloud services, such as Uploaded, and online platforms, such as Netlog, eBay, or YouTube, can be considered hosting service providers. There is no case-law on the application of Article 13 (caching services) at European level.

At the same time, these safe harbours do not prevent the imposition of duties of care that can be reasonably expected from intermediaries (recital 48 ECD), or injunctions (by administrative authorities or courts) to detect and prevent illegal activities, to the extent that these do not constitute a general monitoring obligation. While the ECD does allow for such injunctions, it does not regulate the necessary conditions to be met. This is different from sector-specific legislation, such as in the field of intellectual property rights enforcement[2].

For all three categories, however, Article 15 ECD provides for a prohibition on the imposition of general monitoring obligations on intermediaries. In practice, this means that Members States may not require online intermediaries to monitor the information they transmit or store in a general manner, or to actively seek facts or circumstances indicating illegal activity. Member States may however oblige service providers to promptly inform the competent public authorities of alleged illegal activities or information, or to communicate to the authorities information enabling the identification of recipients of their service with whom they have storage agreements, or to monitor information "in a specific case"[3]

Article 15(1) ECD is central to the **fundamental rights** balance in the context of the ECD's liability exemption regime and also plays a particularly important role in determining the scope of injunctions as well as of duties of care.

Despite existing case-law by the CJEU on this distinction as regards national court injunctions[4], the **differentiation** between prohibited general and acceptable specific monitoring remains uncertain. It is clear, however, that service providers are not restricted by Article 15(1) ECD to **voluntarily** perform general monitoring or actively seek facts indicating illegal activity.[5]

---

[2] Injunctions against intermediaries whose services are used by third parties to infringe intellectual property rights (IPRs) are available under the Enforcement Directive (Articles 9 and 11) and the InfoSoc Directive (Article 8(3)).

[3] Recital 47 ECD

[4] E.g. C-324/09, *L'Oréal v eBay*, para. 139; C-360/10, *Netlog*, para. 38; C-70/10, *Scarlet Extended*, para. 40; C-18/18, Glawischnig-P..

[5] See also Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, COM(2018)1177 final.

1.2. Special liability regime for copyright (online content-sharing service providers)

Article 17 of the Directive on Copyright in the Digital Single Market[6] has introduced a new liability regime for online content-sharing service providers. It states that, when performing an act of communication to the public under the conditions established in this Directive, services in scope are not considered to be covered by Article 14 ECD.

Article 17 applies to online content-sharing service providers as defined in Article 2(6) of the Directive. An online content-sharing service provider is defined as an information society service provider of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes. Typical examples of online content-sharing service providers are major user-uploaded video-sharing platforms[7].

Article 17(1) provides that online content-sharing service providers perform an act of communication to the public or an act of making available to the public when they give the public access to protected content uploaded by their users, and therefore they need to obtain an authorisation from relevant rightholders, for instance by concluding a licensing agreement.

By doing so, Article 17(4) establishes a specific liability regime for online content-sharing service providers that have not obtained an authorisation from the relevant rightholders. In the absence of an authorisation, Article 17(4) sets out three cumulative conditions, which service providers may invoke as a defence against liability. The conditions in Article 17(4) are subject to the principle of proportionality, as specified in Article 17(5): service providers should be liable for unauthorised acts of communication to the public, including acts of making available to the public, unless they demonstrate they have made best efforts to obtain an authorisation; furthermore, they should be liable for the use of unauthorised content unless they demonstrate that they have made their best efforts, in accordance with high industry standards of professional diligence, to ensure the unavailability of specific works and other subject matter for which the rightholders have provided them with the relevant and necessary information; finally, online content-sharing service providers should be liable for the use of unauthorised content unless they demonstrate that they have acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, and that they have made best efforts to prevent their future uploads in accordance with Article 17(4)(b). The requirement to make best efforts to prevent future uploads of notified works or other subject matter can be qualified as a *stay down* obligation. As the stay-down obligation in Article 17(4) (c) refers back to letter (b) of the same paragraph, rightholders similarly have to provide service providers with the same type of 'relevant and necessary' information and the same technological possibilities and limitations apply.

It is important to mention that Article 17(6) provides for a specific liability regime for 'new' companies, with lighter conditions. This is in practice a two-tier regime applicable to

[6] Directive 2019/790/EC, the 'DSM Directive', to be implemented by Member States by 7 June 2021.

[7] Article 2(6) also provides a non-exhaustive list of excluded providers of services, such as not-for-profit online encyclopedias, which are not online content-sharing service providers within the meaning of the Directive. Special, less stringent rules apply to new online content-sharing service providers, which meet the conditions in Article 17(6).

services, which have been active in the EU for less than 3 years and have an annual turnover of less than 10 million euros with different rules applying to them depending on the audience they attract.

Finally, Article 17 includes the necessary safeguards to avoid that such measures have a negative effect on the enjoyment of fundamental rights by users: first and foremost, the application of Article 17 should not lead to any general monitoring obligation, in line with Article 15 of the ECD. Furthermore, it should not lead to the unavailability of content which does not infringe copyright. Article 17(7) also provides that the Member States must ensure that users in each Member State are able to rely on the exceptions or limitations for quotation, criticism, review and use for the purpose of caricature, parody or pastiche when they upload and make available their content on online content-sharing service providers' websites, making these previously optional exceptions mandatory for all Member States. Redress mechanisms should allow users to challenge the blocking or removal of their content.

2. GENERAL CONDITIONS OF THE LIABILITY EXEMPTIONS

The ECD requires two general criteria to be fulfilled: firstly, the service provider needs to provide a specific form of an **"intermediary" information society service**. The definition of "intermediary" is a broad genus and generally provided a flexible and adaptive concept that has been subject to a variety of **CJEU cases**[8], both related to Article 14 ECD and Article 12 ECD.

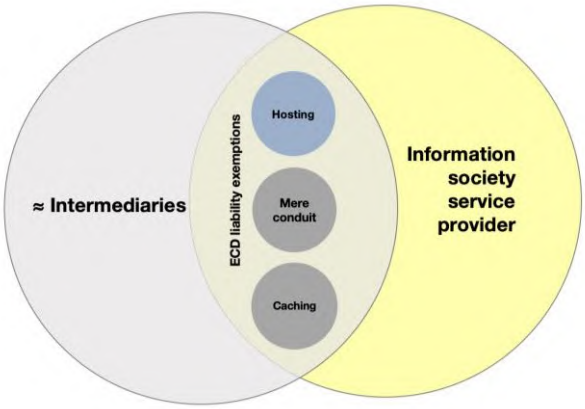


Figure: Conceptualization of existing liability exemptions in the ECD
Source: Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission, p. 29.

[8] E.g. C-484/14, *McFadden* (provider of open Wi-Fi network); C-70/10, *Scarlet Extended* (IAP); outside the non-hosting landscape see e.g. C-291/13, *Papasavvas*; C-390/18, *Airbnb Ireland*; C-324/09, *L'Oréal v eBay*; C-236/08, *Google France;* C-360/10, *SABAM v Netlog.* In the context of Art. 14 ECD, see the parallel study by van Hoboken, J., et al. (2020). *Hosting Intermediary Services and Illegal Content Online*, *A study prepared for the European Commission, DG Communications Networks, Content & Technology*, SMART number 2018/0033.

The specific liability exemptions for the three types of **intermediary activities** then come with certain – graduated – conditions. The Court has already established that the different nature of these categories has an impact on what is expected from them.[9]

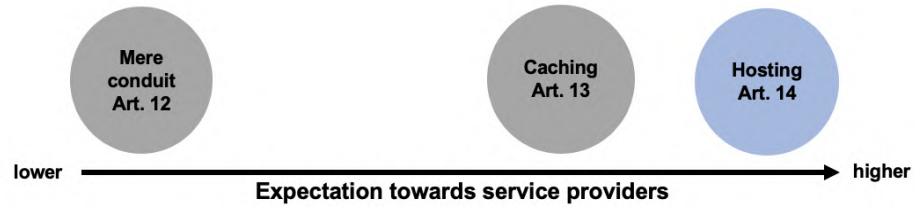


Figure: Conditions of the ECD's liability exemptions Source: Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission, p. 29.

The second general criterion is that the intermediary activity must be of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information that is transmitted or stored[10]. This means that whenever a service provider plays an active role of such a kind as to lead to knowledge or control over the stored information, it cannot benefit from the liability exemptions in the ECD.

In C-484/14 – *McFadden*, the CJEU stipulated for example in relation to "mere conduit" that "providing access to a communication network must not go beyond the boundaries of such a technical, automatic and passive process for the transmission of the required information"[11], without, however, providing further guidance on the criterion.

The CJEU has also dealt with the application of the ECD concept of "mere technical, automatic and passive nature" to hosting services providers. In particular, the CJEU extended

[9] See C-484/14, McFadden, p. 62-63: "the service provided by an internet website host, which consists in the storage of information, is of a more permanent nature. Accordingly, such a host may obtain knowledge of the illegal character of certain information that it stores at a time subsequent to that when the storage was processed and when it is still capable of taking action to remove or disable access to it. However, as regards a communication network access provider, the service of transmitting information that it supplies is not normally continued over any length of time, so that, after having transmitted the information, it no longer has any control over that information. In those circumstances, a communication network access provider, in contrast to an internet website host, is often not in a position to take action to remove certain information or disable access to it at a later time".

[10] Rectial 42 ECD, originally referring merely to mere conduits (Article 12) and caching services (Article 13). See C-521/17, *SNB-REACT v Deepak Mehta*, para. 47 and C-484/14, *McFadden*, para. 62. In the context of hosting applied by the CJEU in C-324/09, *L'Oréal and Others*, para. 113; C-236/08 to C-238/08, *Google France and Google*, para. 113; C- 291/13, *Papasavvas*, paras. 40 ff.; however, not uncontested see e.g. C-324/09, *L'Oréal v eBay*, Opinion of Advocate General Jääskinen, paras. 138–142; Riordan (2016), p. 402; Stalla-Bourdillon, S. (2016). Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the e-Commerce Directive as Well... In: In: L. Floridi L. & M. Taddeo. *The Responsibilities of Online Service Providers*, Springer, p. 13; Bridy, A. (2019). The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform. Forthcoming in *Vanderbilt Journal of Entertainment & Technology Law*, p. 115.

[10] C-484/14, *McFadden*, para. 46.

[11] C-484/14, *McFadden*, para. 46.

the definitional criteria laid down under Recital 42 for mere conduit and caching activities to hosting service providers such as Google search (in its case Google France (Cases C-236/08 to C-238/08)).

The CJEU followed the same line in the case L'Oréal/eBay: on the question whether an online market place may be acting beyond "mere technical, automatic and passive nature" it was stated that "*where, […] the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over,* ***the data relating to those offers for sale****. It cannot then rely,* ***in the case of those data****, on the exemption from liability referred to in Article 14(1) of Directive 2000/31*." (paragraph 116)

In this new judgement, the CJEU established now a closer link between the "active role" and the given piece of data or information for which the hosting service provider might be held liable.

From the rulings it can also inferred, furthermore, that the relevant test is not whether a given platform is "active" or "passive", but whether the services provided play an active role which gives the platform knowledge or control over the illegal data stored. The Court clearly determines that it is for the national judge to establish the application of the liability exemption under the given circumstances of each case, and to the extent that the active (non-neutral) role of the intermediary has lead it to have knowledge or control over that data.

The active/passive dichotomy is increasingly challenging to apply in practice, because it is in the nature of a service that it involves some degree of activity.[12] The provider is thus active in some respects, while passive in others. Given this uncertainty, further clarifications might be needed[13].

2.1. Specific conditions for the liability exemptions

The Commission services have commissioned two separate studies to analyze and better frame the discussion around the liability provisions for the services of the different categories as explained above. Many of the conclusions in this Annex are developed and represented in detail in those studies[14].

[12] In the future, also the "automatic"-criterion, which could be understood as relating to a rule-based system, might be challenged by developments in the field of machine learning and artificial intelligence, which are not necessarily rule-based.

[13] Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission, p. 32.

[14]

2.1.1. Mere conduit services

Article 12 ECD covers "mere conduit", i.e. transmission of information. It comprises two scenarios namely the "transmission in a communication network" and the "provision of access to a communication network".

The notion "**communication network**" is not further defined in the Directive. Historically, IAPs have been the clear addressee of Article 12 ECD. Also carrier services e.g. related to the internet backbone seem to clearly be in the traditional scope.

Article 12 ECD stipulates **three cumulative conditions** that an ISSP needs to fulfil in order to benefit from the liability exemption: Firstly, the provider must not initiate the communication according to Article 12(1) lit. (a) ECD. Secondly, according to Article 12(1) lit. (b) ECD, the service provider must not select the receiver of the transmission. Finally, the service provider must not select or modify the information contained in the transmission according to Article 12(1) lit. (c) ECD.[15]

2.1.2. Caching services

Article 13 ECD stipulates that a service that consists of the transmission in a communication network is not liable for the "automatic, intermediate and temporary storage of that information, performed for the sole purpose of **making more efficient** the information's onward transmission to other recipients of the service upon their request". Thus, as a starting point, similarly to Article 12 ECD, Article 13 ECD concerns a specific form of transmission in a communication network.

In order to benefit from the "caching" liability exemption, a service provider needs to fulfil **five cumulative conditions.** Somewhat similar to Article 14 ECD, Article 13 (1) lit. (d) ECD additionally stipulates an action-requirement, namely when the provider has obtained "**actual knowledge** of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement." While there exists no CJEU jurisprudence on this aspect of Article 13 ECD, the criterion is to be differentiated from the actual knowledge-standard in Article 14 ECD[16], which relates to the alleged infringing material or the illegality of the material. Thus, it seems that Article 13 ECD has not

[15] Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission, p.32-33.

[16] For the standard in relation to hosting see e.g. C-324/09, *L'Oréal v eBay*, para. 120; see also Delfi AS v. Estonia (2015) ECtHR 64669/09, para. 117.

given rise to considerable legal uncertainty[17]. It has been noted that Article 13 ECD "clearly targeted one specific technology (proxy-servers)"[18].

2.1.3. Hosting services

Article 14 ECD contains the safe harbour for hosting service providers, and contains a number of conditions. 14(1) ECD states that an intermediary service provider "is not liable for the information stored at the request of a recipient of the service", subject to two alternative conditions. First, if "the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent". Second, if "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".

Article 14(1) ECD contains two distinct knowledge standards, with reference to the illegal activity or information stored, [potentially referring to two types of wrongdoings]: (i) "actual knowledge" and (ii) "awareness of facts or circumstances" from which the illegality is "apparent", also referred to as "constructive" or "construed" knowledge. The travaux préparatoires of the ECD (Explanatory memorandum COM (1998) 586 final, 18.11.1998.) appear to support this distinction, with the result that criminal liability of hosting platforms would require actual knowledge on the part of the hosting service provider, whereas civil liability regarding claims for damages would require solely constructive knowledge.

When a hosting provider meets the conditions above, it cannot be held criminally or civilly liable (under different knowledge standards) for illegal content uploaded by users using his services. If the conditions are not met, the hosting intermediary cannot benefit from the safe harbour. However, this does not mean the service provider will be automatically held liable for the (allegedly) illegally uploaded content. Rather, its liability as an intermediary will have to be determined under largely non-harmonised national rules or doctrines applicable to persons that "do not themselves violate a right, but whose actions or omissions contribute to such violation", for example resulting from the violation of a duty of care. This means that they will typically be evaluated under doctrines of tort law for "indirect", "secondary", "intermediary", or "accessory" liability.

Article 14 ECD has been subject to interpretation by the CJEU in a number of judgments: Papasavvas (C-291/13); Google France (C-236/08), L'Oréal (C-324/09); Scarlet Extended (C-70/10), and Netlog (C360/10).

2.2. Perceived shortcomings of the existing liability regime

The Impact Assessment (p. 2.3.5) has pointed at different sources of legal uncertainty originated from the different application of some provisions of the existing liability regime, from the vagueness of some concepts included therein or, finally, from the evolution of the services that it intends to cover. In particular, this Annex would like to give more details on the alleged disincentives against "Good Samaritan" actions (actions taken in good faith to

[17] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 35.

[18] DLA Piper (2009). *EU study on the Legal analysis of a Single Market for the Information Society; New rules for a new age?* Chapter 6. Liability of Online Intermediaries, section "Ambiguities in articles 12 (mere conduit)".

tackle illegal content online), the existing case-law about the "neutral and passive role" to be played by intermediaries, and about when it is considered that a hosting service provider has actual knowledge or awareness over the illegal data stored in its service.

2.2.1. Disincentives for voluntary measures by intermediaries

The current regime entails some legal uncertainty, in particular for small players which might want to take measures for keeping their users safe, but, in order to escape legal risks, avoid doing so. The ECD as interpreted by the Court left a paradox of incentives for service providers: proactive measures taken to detect illegal activities (even by automatic means) could be used as an argument that the service provider is an 'active' service controlling the content uploaded by their users, and therefore cannot be considered as in scope of the conditional liability exemption. This places small players, who cannot afford the legal risk, at a net disadvantage in comparison with large online players which do apply content moderation processes to varying degrees of quality.

Usually, online platforms are well-placed to proactively reduce the amount of illegal content stored by them. Measures range from various filtering technologies (e.g. PhotoDNA hashing technology for child abuse content or fingerprinting technology for music files in course of upload, with their own tools as YouTube's ContentID or with commercial solutions such as Audible Magic), blocking (e.g. URL blocking based on the black-list of the Internet Watch Foundation), moderation of content by algorithms, staff or community (e.g. manual checking of algorithmically flagged comments in the discussion forums), enforcement of termination policy (e.g. toward users who repeatedly infringed rights), implementation of terms of service or of community guidelines (e.g. quality standards for customers), improved notice submission systems (e.g. by establishing "trusted flaggers" or by allowing direct removal of counterfeiting offers), degradation of service to repeat infringers and voluntary agreements in the industry (e.g. Memorandum of Understanding regarding anti-counterfeiting efforts). In particular, such voluntary measures can prevent that the same illegal content which has been once notified is uploaded or indexed again after being removed.

Some providers pointed out the legal risks of implementing voluntary measures: platforms are in general afraid that such voluntary measures would disqualify them from the safe harbours or lead to other legal issues (e.g. breach of privacy of their users). Through these voluntary proactive measures, intermediaries could be seen as no longer neutral, passive and technical – and consequently lose the benefit of the limited liability regime for hosting providers. This situation is seen as a potential source of chilling most innovation in this area, although voluntary arrangements often prove to be more effective and appropriate to their particular technology and business models than any measure imposed by public authorities.

All the above, as also suggested by the results of the public consultation, point to a need to clarify certain aspects of the application of the liability regime under the ECD to new business models. Furthermore, online platforms which take a responsible attitude and adopt proactive measures, which go beyond their legal obligations, need legal certainty as to what extent they are adopting "an active role *of such a kind as to give it knowledge of, or control over"* the data.

The Communication on tackling illegal content online[19], from 2017, already gave a first step, stating that taking voluntary proactive measures to detect and remove illegal content online does not automatically lead to the online platform losing the benefit of the safe harbour under Article 14 ECD. The point is reiterated in the subsequent Recommendation on effective measures to tackle illegal content online[20], from 2018, but none of these instruments is binding.

It is also possible to find examples of Good Samaritan provisions in Codes of Conduct. In the UK, the IPO Code of Practice on Search and Copyright states that "[n]o action undertaken in furtherance of these practices shall impute knowledge, create or impose liability, rights, obligations or waiver of any rights or obligations for any parties."(IPO Code of Practice on Search and Copyright (UK), Art. 22) In France, the Charter for the Fight against the Sale of Counterfeit Goods on the Internet provides for monitoring obligations on its parties while stating that the signing of the Charter and implementation of measures therein "shall not prejudice the legal status of the signatories nor their current or future liability regime… [and] ...have no consequences on current or future legal proceedings" (French Charter for the Fight against the Sale of Counterfeit Goods on the Internet, Par. 6 Preamble and Art. 3).

2.2.2. "Active role"

As explained above, there is still an important uncertainty as to when it is considered that an intermediary, and in particular, a hosting service provider, has played an active role of such a kind as to lead to knowledge or control over the data that it hosts. The fact that there is no such thing as an "active host", but that a provider might play an active role regarding some listings, but not others (for instance because it presents it or recommends it in a special manner) does not lead to the necessary legal certainty to provide legal intermediation services without risking claims for damages or even criminal liability. Many automatic activities, such as tagging, indexing, providing search functionalities, or selecting content are today's necessary features to provide user-friendly services with the desired look-and-feel, and are absolutely necessary to navigate among an endless amount of content, and should not be considered as "smoking gun" for such an "active role".

The Court might soon clarify this question in two upcoming cases, regarding YouTube and Uploaded.[21] In his Opinion, the Advocate General favours a clearer and stricter interpretation of when this "active role" comes into play: "the 'active role' envisaged by the Court quite rightly relates to the actual content of the information provided by users. I understand the Court's case-law to mean that a provider plays an 'active role' of such a kind as to give it 'knowledge of, or control over' the data which it stores at the request of users of its service where it does not simply engage in the processing of that information, which is neutral vis-à-vis its content, but where, by the nature of its activity, it is deemed to acquire intellectual control of that content. *That is the case if the provider selects the stored information, if it is actively involved in the content of that information in some other way or if it presents that*

[19] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms

[20] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[21] Joined Cases C- 682/18 and C- 683/18, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C- 682/18) and Elsevier Inc. V Cyando AG (C- 683/18).

information to the public in such a way ***that it appears to be its own***. In those circumstances, the provider goes outside of the role of an intermediary for information provided by users of its service: ***it appropriates that information***."[22] The Advocate General further puts the bar on the necessary confusion created on "*an average internet user who is reasonably circumspect",* to the extent that he or she does not know whether the files stored do originate from the operator or from a third party.

This interpretation is very much aligned with similar interpretations by the Court in the Wathelet case, where the CJEU has explained that it is "*essential that consumers are aware of the identity of the seller, and in particular whether he is acting as a private individual or a trader, so that they are able to benefit from the protection conferred on them*"[23]. It follows therefore that, in the circumstances in which an online marketplace act as an intermediary on behalf of a third party trader, the ignorance of a consumer on the capacity in which the online marketplace acts would deprive him/her of his/her consumer rights. In this regard, according to the CJEU "*a trader may be regarded as a 'seller' […] where he fails to duly inform the consumer that he was not the owner of the goods in question*". Consequently, in case of likelihood of confusion in the mind of consumers on the identity of the trader offering a product, a national court could assess that an online marketplace is liable for a defective product sold.

Finally, in an older case[24], relating to the liability by an online newspaper, the Court applied the "active role" test and decided that "since a newspaper publishing company which posts an online version of a newspaper on its website has, *in principle, knowledge about the information which it posts and exercises control over that information*, it cannot be considered to be an 'intermediary service provider' within the meaning of Articles 12 to 14 of Directive 2000/31, whether or not access to that website is free of charge. This suggests that where the service provider's involvement with the content is so extensive that the content in question is no longer 'user content' but should instead be 'co-attributed' to the provider, the latter can no longer reasonably be called an intermediary.

During the public consultation, some stakeholders have proposed a new concept, which takes influence of this "active role" but also from the concept of "decisive influence" elaborated by the Court in the Uber case[25]. BEUC in particular advocates for the imposition of liability to those marketplaces enjoying a "predominant influence" over third party suppliers. In this regard, they propose the following criteria as indicating such predominant influence[26]:

a) The supplier-customer contract is concluded exclusively through facilities provided on the platform;
b) the platform operator withholds the identity of the supplier or contact details until after the conclusion of the supplier-customer contract;

[22] Opinion of Advocate Gneral Saugmandsgaard Øe delivered on 16 July 2020.
[23] C-149/15, Sabrina Wathelet v Garage Bietheres & Fils SPRL
[24] C- 291/13, Pappasavas, p. 45.
[25] Judgment in Case C-434/15 Asociación Profesional Elite Taxi v Uber Systems Spain SL; Judgment in Case C-390/18 Airbnb Ireland
[26] Making the Digital Services Act work for consumers - BEUC's recommendations (https://www.beuc.eu/publications/beuc-x-2020-031_making_the_digital_services_act_work_for_consumers_-_beucs_recommendations.pdf)

c) the platform operator exclusively uses payment systems which enable the platform operator to withhold payments made by the customer to the supplier;
d) the terms of the supplier-customer contract are essentially determined by the platform operator;
e) the price to be paid by the customer is set by the platform operator;
f) the marketing is focused on the platform operator and not on suppliers; or
g) the platform operator promises to monitor the conduct of suppliers and to enforce compliance with its standards beyond what is required by law.

However, some of these criteria would actually mean, following existing case-law that the intermediary is not an information society service provider. In those cases, normal liability rules as in the offline world for services and traders would apply.

Instead, this seems to support a codification of a sort of "vicarious liability" for those cases where the service provider deliberately collaborates with one of the recipients of its service in order to undertake illegal acts or is integrated with the content provider, and as a result it should not benefit from the liability exemptions established for intermediaries. This idea is today already included in recital 44 of the ECD, and exists also in other legal systems (DMCA in the US). This has also been stressed recently in Advocate General Øe's Opinion, who proposes that where the provider deliberately facilitates the carrying out of illegal acts by users of its service, and where objective factors demonstrate the bad faith of the provider, such provider loses the benefit of the exemption from liability under Article 14(1) of Directive 2000/31[27].

2.2.3. Actual knowledge

As stated in the Impact Assessment, the ECD does not give much details as to when it is considered that 'actual knowledge' has been acquired. Importantly, the Directive does not impose a specific notice-and-action procedure nor does it specify the liability status when content is taken down, of left online.

When a hosting service provider receives a notice about allegedly illegal content that it stores, it should not be held liable even if such notice has triggered "actual knowledge" or "awareness" of such illegality as long as it took expeditious action pursuant to the ECD. However, it is not clear what is necessary for a notice to trigger such awareness. There is also uncertainty around gaining actual knowledge or awareness of illegal content as a result of the provider's voluntary actions, as explained above.

The wording of point (a) of Article 14(1) ECD indicates that, for the awareness test to be met, the facts and circumstances in question must be such that the illegality is apparent; a case of borderline illegality does generally not seem sufficient to lead to 'awareness' within the meaning of Article 14(1)(a). A well-structured notice-and-action procedure should provide legal certainty to all parties involved in order to be effective and complete.

[27] Joined Cases C- 682/18 and C- 683/18, Frank Peterson v Google LLC, YouTube LLC, YouTube Inc., Google Germany GmbH (C- 682/18) and Elsevier Inc. V Cyando AG (C- 683/18), Opinion of Advocate Gneral Saugmandsgaard Øe delivered on 16 July 2020, p. 191.

3. ALTERNATIVE LIABILITY REGIMES – OPTIONS CONSIDERED AND DISCARDED FOR THE MAIN REPORT

This section analyses the potential liability regimes that could apply to information society services in the absence of the existing regime, and the reasons why they have been discarded at an early stage in the impact assessment process. The possible liability regimes range from a complete, unconditional exemption from liability for online intermediaries to a strict liability for all illegal activities of third parties. As explained below, the expected drawbacks outweigh the possible benefits in case of these discarded options. These alternatives would lead to disproportionate burdens, restrictions or risks, without striking a balance between different policy objectives and fundamental rights.

The retained options separate the question of intermediary liability from the due diligence obligations of online platforms envisaged under the Digital Services Act, similar to the approach of the Audiovisual Media Services Directive (that imposes specific duties of care without prejudice to the exemption of liability). The due diligence obligations are compatible with and independent from the options for the liability of intermediaries, and platforms should be subject to these obligations regardless of their liability for third party content or activities.

3.1. Immunity from any type of liability for all intermediaries

On one edge of the spectrum, intermediaries could be unconditionally exempted from any kind of intermediary liability. This solution would be broadly similar to the situation in the US, governed by Section 230 of the Communication Decency Act. The lack of liability for third party content and activity would give freedom and legal certainty to platforms to run their services. However, absent any liability, the behaviour of a platform would be solely governed by market forces and commercial interests, which may not provide any incentive to prevent, limit, or stop online misconduct. In fact, platforms may benefit from illegal activities if these drive traffic and increase their income. If a platform derives most of its revenues from the presence of illicit products or content, the absence of any liability may encourage it to actively promote these goods or content. The economic and societal risks of such a 'no liability' regime would be high, also considering that platforms have proven to be able to contribute to tackling illegal content online efficiently. Indeed, Section 230 of the Communication Decency Act have been subject to broad criticism in recent years, and the US Justice Department has unveiled a proposed reform of the legislation in September 2020.

This option was analysed but not retained to be impact assessed in detail, as the option is not in line with the findings of the evaluation of the ECD as regards shortcomings of the current liability regime. The option would have negative consequences on the preservation of online safety in Europe.

3.2. Impose specific liability

As explained in the Impact Assessment, the liability exemptions under the ECD are only intended to establish the situations when liability *cannot* be applied by the Member States. It does not provide a positive basis for establishing when a service provider should be held liable. Where the conditions set by the liability exemption are not met, liability should not be

understood to follow by default. Instead, national authorities should determine whether the provider is liable in accordance with the applicable provisions of national and Union law.

Hence, the ECD harmonises the absence of liability, but not the liability itself. For such a harmonisation (of tort law rules or criminal liability rules), probably the Single Market legal basis (Article 114 TFEU) would not be appropriate. Instead, the current system has allowed Member States to determine liability following their own national rules, unless such liability has been harmonised in a different instrument.

Furthermore, the current liability regime is horizontal and neutral: it applies, horizontally, to all forms of liability which the providers in question may incur in respect of any kind of information which they store at the request of the users of their services, whatever the source of that liability, the field of law concerned and the characterisation or exact nature of the liability, be it primary or secondary liability for the information provided and the activities initiated by those users.[28] It also applies to any kind of illegal content, without determining what is considered illegal. These "neutrality" and "horizontality" have been considered key for the success of the regime.

This option was discarded, as it would not comply with subsidiarity and proportionality principles, and would not be fit for a horizontal measure.

3.3. In particular, impose specific liability on online marketplaces

During the public consultation, there have been several stakeholders, including BEUC, asking for a specific liability for damages for online marketplaces.

There are several definitions of "online marketplaces" in EU law[29]. In line with Directive 2019/2161, online marketplaces are defined as "*a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows*

[28] Advocate General Oe quotes recital 16 of Directive 2001/29; Opinion of Advocate General Szpunar in Mc Fadden (C- 484/14, EU:C:2016:170, point 64); Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market (COM(1998) 586 final (OJ 1999 C 30, p. 4)), pp. 27 and 29; and Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee of 21 November 2003, First Report on the application of [Directive 2000/31] (COM(2003) 702 final), p. 13 to substantiate these views (Opinion in Joint Cases C-682/18 and C-683/18, YouTube and Uploaded).

[29] Regulation (EU) 2019/1148 on the marketing and use of explosives precursors: "*'online marketplace' means a provider of an intermediary service that allows economic operators on the one side, and members of the general public, professional users, or other economic operators, on the other side, to conclude transactions regarding regulated explosives precursors via online sales or service contracts, either on the online marketplace's website or on an economic operator's website that uses computing services provided by the online marketplace*;"

Directive (EU) 2016/1148 ("NIS Directive"): *"'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (1) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace*";

Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes "'*online marketplace' means a service provider, as defined in point (b) of Article 2 of 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 ('Directive on electronic commerce') (1), which allows consumers and traders to conclude online sales and service contracts on the online marketplace's website*".

consumers to conclude distance contracts with other traders or consumers". As a common element to these definitions, what distinguishes online marketplaces is their position as intermediary between a trader and a consumer: they match buyers and sellers, including across borders, to facilitate online transactions. It is also undisputed that, to do so, they store the data supplied by third party sellers, which are the recipients of the online marketplace's (intermediation) service. Under the current framework, online marketplaces are subject to the horizontal limited liability regime, as provided for by the ECD for providers of hosting services. The Court has already established that such services store data supplied by its customers[30].

Consequently, thanks to the intermediation services offered by online marketplaces, many business sellers (especially SMEs) managed to survive the current Covid-19 crisis and the related physical-distancing and confinement restrictions. This is also illustrated by the growing trend of online shopping in Europe, where, by the end of May 2020, online orders were, on average, up by 50%[31]. Online marketplaces are therefore key for the recovery strategy for the European digital economy post COVID-19 crisis, as they offer an easy gateway for offline businesses to go online and navigate through existing legal fragmentation via a common interface and ancillary services supplied by a platform.

However, close to these important benefits, new risks to consumers have emerged, exposing them to a new range of illegal activities and products. Also during the Covid-19 crisis, online platforms have witnessed an increase of scams and disinformation around health issues and products[32].

The Commission is also looking at the particular problems created by the proliferation of online sales of dangerous and non-compliant goods. In this context, the question arises what is the legal status of online marketplaces in the chain and whether specific obligations could be imposed on them to avoid the distribution of illegal goods online, in particular as regards goods sold by third party sellers that are not established in the Union.

Under the Directive 85/374/EEC on the liability for defective products, the producer of a product shall be liable for damages caused by a defect in his product. Without prejudice to the producer liability, the person who imports a product into the EU shall be deemed to be producer. Where the producer of the product cannot be identified, each supplier of the

[30] eBay case.

[31] OECD, Connecting Businesses and Consumers During COVID-19: Trade in Parcels, 9 July 2020 https://www.oecd.org/coronavirus/policy-responses/connecting-businesses-and-consumers-during-covid-19-trade-in-parcels-d18de131/#figure-d1e179

[32] On 30 April 2020, the CPC network, under the coordination of the Commission, launched a broad screening ("sweep") of coronavirus related products advertised on websites and online platforms. More details on the sweep can be found in the summary document below. The main findings showed that rogue traders continue to mislead consumers with a variety of illegal practices. In May 2020, the European Commission has invited online platforms (namely Allegro, Alibaba, Amazon, Microsoft, Cdiscount, eBay, Facebook, Google, Rakuten and Verizon Media) to actively cooperate with EU consumer protection (CPC) authorities to fight rogue trading practices related to the COVID-19 crisis. The mentioned platforms replied positively to the call for building a closer partnership with national CPC authorities and the Commission. They rapidly put in place dedicated communication channels for EU consumer authorities to signal illegal practices. Other proactive measures were also adopted: https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/summaryofresponses_update_08042020.pdf

product shall be treated as its producer unless he informs the injured person, within a reasonable time, of the identity of the producer or of the person who supplied him with the product. As online marketplaces are not directly contemplated by the product liability Directive (the Directive is from 1985), the question is whether they should be considered as "supplier". In such a case, online marketplaces would be excluded from any liability linked to the sale of defective product, on condition that they clearly display the identity of the third-party seller or producer to prospective consumers.

In order to enhance the responsibility of online marketplaces in the supply chain, an obligation for online platforms to obtain accurate and up-to-date information on the identity of third-party traders offering their products or activities via the platforms (also known as "know-your-business-customer") and to communicate such information to consumers would ensure a safer and more transparent environment for consumers and discourage non-compliant sellers from offering illegal goods or services online. This has already been introduced successfully in the banking sector to tackle money-laundering activities, for instance. Such a mechanism would also allow tracing more easily rogue traders and facilitating the enforcement by the competent authorities of laws against traders offering illegal products to consumers. Furthermore, the imposition of specific channels for enforcement authorities and users or specialised trusted flaggers to report illegal content could improve and accelerate the fight against dangerous or non-compliant products. Specific measures to identify and block repeat infringers (rogue sellers who re-introduce offers for blocked listings) could avoid the reappearance of the already identified illegal products.

This option was analysed but discarded from the retained options impact assessed in the main report, as it only focuses on sector-specific concerns and does not represent a harmonisation of the liability exemptions for intermediaries, but a harmonisation of certain types of liability. Such harmonisation of strict liability could be assessed within the context of sector-specific measures, while in line with the horizontal regime. It has merits to reinforce the clarifications on certain aspects of the liability exemptions as expressed above.

3.4. Making the exemption of liability conditional to the compliance with due diligence obligations

The retained options support, in a nutshell, the general maintenance of the existing liability regime, including some clarifications, but the imposition of self-standing "due diligence" obligations which will allow a more responsible intervention by online intermediaries vis-à-vis illegal content, goods or services. The retained options impose such due diligence obligations without prejudice to the application of the liability exemptions. They would be supervised and, where necessary, sanctioned for failure to comply, under the conditions set out in the options, while the liability exemption would continue to be established on a case-by-case basis, when the service provider qualifies according to the conditions set in the law.

An alternative approach was considered but was not retained for a detailed impact assessment, allowing intermediaries to be in scope of the conditional liability exemption only if they acted with the necessary due diligence. Structuring due diligence obligations as a condition of the liability exemption would imply that compliance would be ultimately voluntary: the intermediary service would only be "incentivised", but not "required" to comply with the rules. It could make a calculation of risks, and consider that, based on national or Union laws, it would still not be held liable by a court, or that the costs of complying could be lower than the costs incurred through potential sanctions. In certain

cases, the incentive for intermediaries to comply with the conditions to qualify for the liability exemption may well be limited, for example, when damage claims are not a realistic threat. However, intermediaries should not be left the choice whether or not to comply with the relevant requirements and self-standing obligation are required to achieve this objective.

In addition, the compliance with due diligence obligations is prone to a more systematic supervision, and includes an investigation that goes beyond case-by-case assessments of facts and circumstances relevant to establish liability, or the exemption thereof, in criminal and civil proceedings. Including a conditionality of liability exemptions based on overall due diligence obligations would constitute an unjustified burden on courts and administrative authorities.

This option was considered and discarded, as failing to achieve the objectives of the intervention, placing disproportionate burdens on authorities, and introducing further legal uncertainty on service providers.

3.5. No harmonised liability exemptions

On the other extreme of the spectrum of options considered is a regime without liability exemptions – similar to the legally fragmented landscape from before the adoption of the ECD. Such a system of potential strict liability – left to the legislations of Member States – would have a number of detrimental effects on the digital environment, notably on platforms. First of all, such regime would essentially require platforms to constantly screen and moderate content, otherwise they would always be exposed to damages claims, fines and even criminal charges. This would lead to a large decrease in the level and variety of activities on platforms, and to the risk of over-removal of content, thereby undermining freedom of speech. It would limit the variety and plurality of possible online services, as providers would avoid risks by opting for business models based on authoritative, editorially curated content, and avoiding user generated content.

It would re-fragment the single market for digital services completely, on an issue where service providers would be exposed to a potentially infinite number of laws, court decisions and restrictions. Faced with legal uncertainty in every new Member State where they would be conducting their business, this would be prohibitive for any new entrant to the market. In addition, digital services are by definition cross-border: they can be accessed from other countries without intending. This would make it impossible for service providers to manage their legal risks.

This scenario would also have severe adverse effects on competition and the competitiveness of European companies. It would impose a heavy burden on small and entrant players – as they would not be able to control content "at the gates" to avoid illegal activities, and would lead to even more concentrated markets in the long run. The increased, almost monopolistic market power of certain platforms, and its possible abuse, would pose a high risk to citizens in itself and could ultimately undermine the objectives of strict liability in the first place.

This option was discarded as contrary to the innovation and competitiveness objective, as well as to the protection of fundamental rights. It is further not in line with the conclusions of the evaluation report of the ECD.

4. SERVICES IN SCOPE[33]

4.1. Article 12 – 'Mere conduit'

Usually there are **several** mere conduit intermediaries between a host and a user, e.g. internet access service, carriers, transit networks and IXPs. While such **transmissions** can also include illegal content, service providers typically cannot have any knowledge thereof, except if they engage in monitoring activities (see deep packet inspection below).[34]

Transmission of information is **asynchronous communication** when using the internet. Data is transmitted intermittently rather than in a steady stream and does not require a constant bit rate. Different parts of the electronic communications infrastructure use different technologies with different transmission speed and capacity.

Data in transit may be buffered in network nodes because of the asynchronous mode of communication, which can also involve the buffering of illegal content. **Buffering** is the intermediate and transient storage, and the data is not stored for any period longer than is reasonably necessary for the transmission. At the mere conduit level, there may also be some **network nodes** (machines), that are called **proxies**[35] or gateways that translate communication protocols in order to connect networks that are using different standards.[36] The information that is transmitted through such nodes is not changed.

Since 2000, the most significant developments have been network bandwidth and a range of services offering dynamic content adapted to each individual user. Today, a significant part of the access network is wireless technology, both **Wi-Fi access points**[37], mesh networks and mobile broadband. Mere conduit intermediaries may also use technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) and have become a part of the **cloud computing ecosystem** offering network as a service and communication as a service. If classic cloud computing is associated with data centers, the carrier cloud is associated with the network connecting data centers and cloud users. Non-IP networks[38] have always coexisted with and often been connected to IP networks[39]. A significant development is in the mobile sector where operators identified technical challenges with the TCP/IP-based technology used in 4G. TCP/IP is regarded as non-optimal for advanced 5G services and ETSI has initiated work on new protocols.[40]

---

[33] Following list provides for a non-exhaustive overview of intermediary service providers covered by the ECD.

[34] Description of technical functioning, examples of services covered by Article 12 and 13 as well as respective "grey areas" were provided by Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission.

[35] "Proxy" is a common concept in computer networking as a name for an intermediary which can be either software- or hardware-based.

[36] There also exist performance-enhancing proxies that are used to improve the end-to-end performance of some communication protocols. IETF RFC 3135, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations", June 2001.

[37] Wi-Fi hotspots are wireless access points that are connected to an IAP, but are usually not considered an IAP in itself. There are Wi-Fi subscriber services selling subscriptions to a defined group of Wi-Fi hotspots, but these are usually not an IAP. There is, however, a subclass of IAPs that is called wireless Internet service provider (WISP).

[38] Examples of non-IP networks are ITU-T X.25, IBM's SNA and AppleTalk.

[39] IP networks refer to networks where the transport layer of the OSI model is using the TCP protocol.

[40] "ETSI launches new group on Non-IP Networking addressing 5G new services" ETSI, April 7th, 2020

Internet exchange point (IXP)

In order to communicate between networks, these need to be connected, typically through a physical connection. An **interconnection** between two networks using a point-to-point link is a "private peering". The purpose of an IXP is to allow **more than two networks** to interconnect directly through a single exchange. The networks that connect to an IXP are autonomous systems[41]. An IXP is sometimes described as providing public peering, or multi-part peering. An IXP does not act as a transit provider or carrier, it just connects the networks. The interconnection can also be used for the transmission of illegal information, but the IXP function is defined such that it abstains from addressing content issues.

Virtual private networks (VPN)

VPN are a set of technologies that enables the user to extend a private network across a public network, commonly using an encrypted tunnel protocol. There are many different ways of configuring a VPN connection, but using the strictest and most straightforward setup, it will appear as if the user is using the computer from the network location where the VPN connection is terminated. This implies that any caching and CDN will assume that the user is connected to the Internet from a different location. The same applies for DNS queries, filtering, blocking and geo-blocking mechanisms, which can be circumvented, thus potentially facilitating access to the otherwise blocked illegal information.[42]

4.2. Article 13 – 'Caching'

Caching is a very common concept used in computer science. It is therefore necessary to distinguish between what is cached, either content (e.g. on a website), which may include illegal information, or addressing data e.g. related to the DNS.[43]

Twenty years ago, network bandwidth was a limited resource, and using long distance international internet carriers was expensive. A large amount of the information was file-based or static, and many users would request the same information within a limited time frame. To limit bandwidth used for data transmission and reduce the response time for end users, network nodes usually called **caching proxy servers** may be used by IAPs and in local networks (e.g. businesses and universities). The mechanism is sometimes called a **response cache** because it is the responses from the host that is cached, not the requests from end users. Caching proxy servers provide intermediate and temporary storage of information that can be requested individually by many users. From the host viewpoint, a caching proxy server aggregates demand for content from multiple users.[44]

---

[41] IETF RFC 1930, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", March 1996.

[42] A common use is for users to be able to connect their computer to their private office network in a secure manner, as if they are directly connected, from any access point on the internet. Another use of VPN is to circumvent the filtering and blocking, and to access content that only is available in other countries (i.e. not in a country from where the user and corresponding IP is located). Some IAP networks might try to block some VPN service providers or VPN technologies.

[43] Schwemer, S., Mahler, T. & Styri, H. (2020). *Legal analysis of the intermediary service providers of non-hosting nature*. Final report prepared for the European Commission, p. 16.

[44] "A shared cache is a cache that stores responses to be reused by more than one user; shared caches are usually (but not always) deployed as a part of an intermediary." IETF RFC 7234.

Caching is beneficial to the internet ecosystem as a cost saving technology and a technology that improves the quality of experience for users. In addition, for each IAP the operational cost is cut by reducing the incoming traffic on the peering connections to other service providers. The content owner can have some level of control over what is cached.

Two noteworthy caching models, that might decrease in relevance, are **transparent caching proxies**,[45] which can have the effect of hiding IP addresses of users from hosts, and **proxy prefetch caching**,[46] which anticipate and pre-load content, before a request from a user. An important change since 2000 is that much of the internet traffic using the HTTP protocol has been replaced with encrypted communication using the Hypertext Transfer Protocol Secure[47] (HTTPS). Because each communication session between a user and host using HTTPS is encrypted, the response cannot be cached by an intermediary and reused by more than one user. At present more than 60 percent of websites are using HTTPS as the default protocol[48], and websites with high volume traffic are more likely to use HTTPS as the default protocol. Implementations of the most recent version of the HTTP protocol only support secure communication.

Reverse proxy

A reverse proxy is a part of the hosting service, but it is important to include a short description as a prelude to the description of CDNs. A reverse proxy can perform many different functions. Three of them are listed below:

- It may **hide the IP addresses** and characteristics[49] of servers in a data center and may perform **load balancing** by distributing incoming requests to several servers. The public IP address of the reverse proxy becomes the IP address of the host.

- It may perform a function called **web acceleration** by caching static and dynamic content.

- It may perform the function of a Transport Layer Security (TLS) termination proxy by performing the **encryption** used by the HTTPS protocol.[50]

[45] Transparent caching proxies: To be more efficient for the IAP, the classic proxy server, that still is used in local networks, evolved into the transparent proxy. A transparent proxy intercepts the data traffic between users and hosts, and because a user sees the IP address of the hosts rather than the IP address of the transparent proxy there is an illusion of transparency for the users. Both classic and transparent proxies hide the user's IP address from the host as the connections to the host are initiated by the proxy. IETF RFC 1919, "Classical versus Transparent IP Proxies", March 1996.

[46] Proxy prefetch caching: Proxy caching server technology evolved by introducing functionality that anticipated what information users may request in the near future in order to reduce latency by prefetching the information. One method used for predicting what information users may request in the near future is by monitoring the content of cached web pages looking for new hypertext links that can be prefetched before they are requested from users. However, this kind of prefetching implies that the intermediary is monitoring the content that is transmitted and may request new content from a host without receiving requests from a user.

[47] IETF RFC 2818, "HTTP Over TLS", May 2000.

[48] W3Techs Web Technology Surveys, https://w3techs.com/technologies/details/ce-httpsdefault

[49] Systems architecture and what kind of hardware and software used in the data center.

4.3. Article 14 – Hosting

As the ECD was adopted 20 years ago and hence predates some services such as Facebook or YouTube, this has originated some diverging interpretations by national courts as to which services should be covered by Article 14 ECD[51].

However, in a number of judgements, the CJEU has clarified what can be regarded as a "hosting service". These cases are dealing with referencing services, online marketplaces and social networks:

As regards **referencing services**, in *Google/LVMH (*C-236/08 to C-238/08) the CJEU held that they can be regarded as hosting services: "*it cannot be disputed that a referencing service provider […] stores, that is to say, holds in memory on its server, certain data, such as the keywords selected by the advertiser, the advertising link and the accompanying commercial message, as well as the address of the advertiser's site.*" (paragraph 111).

As regards **online marketplaces**, in *L'Oreal/eBay (C- 324/09),* the CJEU found that *"it is not disputed that eBay stores, that is to say, holds in its server's memory, data supplied by its customers. That storage operation is carried out by eBay each time that a customer opens a selling account with it and provides it with data concerning its offers for sale*." (paragraph 110).

As regards an **online social networking platform**, in SABAM/Netlog (C-360/10) the CJEU held that *"it is not in dispute that the owner of an online social networking platform […] stores information provided by the users of that platform, relating to their profile, on its servers, and that it is thus a hosting service provider within the meaning of Article 14 of Directive 2000/31*" (paragraph 27)

These rulings show that, even though the ECD was adopted before some of the best known online platforms were in place, it was allowed for a flexible adaptation to new technologies and services, which the Court of Justice consider a "hosting service provider" within the meaning of Article 14 ECD.

Today's typology of hosting intermediaries can be divided in three broad categories[52]. The first is "**online storage and distribution**". This is the classic hosting service category:

---

[50] Note that this would usually imply that e.g. a CDN has **permission** from the content owner to buy and renew digital certificates from a Certificate Authority on behalf of the content owner (in order to encrypt the data transmitted over the HTTPS protocol).

[51] In France, Court of appeals of Paris, 7 June 2006, Tiscali v. Dargaud Lombard; C Cass, Civ. 1, 17 February 2011, Société Nord-Ouest v. Dailymotion; Civ. 1, 12 July 2012, Google v. Bach Films and Google v. Bac Films; C Cass, Civ. 1, 17 February 2011, Bloobox-net v. Martinez; where user-generated-content platforms are concerned, after refusing to consider such operators as hosting. In Spain, Juzgado de lo Mercantil de Madrid of 20 September 2010, Telecinco v. YouTube, confirmed by Audiencia Provincial de Madrid of 14 January 2014. In Italy, Corte di Cassazione, decision of 17 December 2013 – 3 February 2014; Court of Appeal of Milan n.29/2015 Yahoo! Vs. R.T.I. of 22 January 2015; Court of Turin in case Delta TV v Google/YouTube of 5 May 2014; Court of Turin in case Delta TV v Dailymotion of 3 June 2015. In Germany, OLG München, 07.05.2015 - 6 U 1211/14; OLG Hamburg, 01.07.2015 - 5 U 175/10; OLG München, 28.01.2016 - 29 U 2798/15.

services allowing their users to store content online. Such storage will always involve some degree of (potential) distribution. Once certain information is stored online, it can be retrieved on demand at a later stage. There will be variation in the extent to which the online content is made public and whether the accessibility and retrievability of the online stored content is organized for potential third-parties. Basic file storage solutions will typically at least offer their users a sharing feature. Other services may make the content that is hosted publicly available by default. Some may index it and provide a search interface, thereby facilitating and promoting consumption on the platform itself (thus creating further possibilities for monetization through advertising or other means).

The second general category is ‘**’networking, collaborative production and matchmaking’**. In this category, the central function of the platform is not (merely) to store content online, even though this always remains a part of the service, but to connect producers and users around more complex sets of networked interactions, such as an online debate and discussions, market transactions or the collaborative production of documents and other media.

The third category of “**selection and referencing**” services, refers to intermediaries that help provide further value, organization and structure to available offerings online. Review or price-comparison sites help consumers to select service providers and producers of their liking. Directories do the same, with a different technical model, gathering links instead of crawling the Web and creating an index. A complicating factor for these types of intermediaries, from a legal perspective, is that information location tools are not as clearly covered under Article 14 ECD as the other two categories of services. In fact, the ECD seems to not have covered these tools, leaving their legal treatment to the Member States and subsequent evaluations by the European Commission (Article 21 ECD). As noted above, the Court has not explicitly excluded search engines from the scope of Article 14 ECD and has concluded that advertising features of a search engine can be covered (Google Search).

Within these broader categories of (1) storage and distribution, (2) networking, collaborative production and matchmaking, and (3) selection, search and referencing, the following types of hosting intermediary services can be distinguished:

Category 1: Storage & Distribution

- **Web hosting:** The classic hosting intermediary: providing the possibility to host a website or other internet-based offering. Customers can publish their website through the services managed by the hosting company. Web hosting can vary in the extent to which it provides pre-installed web hosting and publishing features, such as analytics, programming environments, databases, etc. Examples of providers operating in this market are Leaseweb, WIX.com and Vautron Rechenzentrum AG.
- **Online media sharing platforms:** services, that provide an open platform for online publications as well as the consumption of those publications, including images and video (Youtube, Vimeo, Photobucket), music (SoundCloud, Bandcamp), blogging and journalism (Medium, Wordpress) and other forms of media.

[52] Van Hoboken, J. and coll. (2018). *Hosting intermediary services and illegal content online: An analysis of the scope of Article 14 ECD in light of developments in the online service landscape*. Final report prepared for the European Commission.

- **File storage and sharing:** Services that offer users the ability to store and share different forms of files online (including video, audio, image, software and text documents). These services range from offering individual file storage solutions, with limited functionality to share, to services that incorporate more social features to facilitate sharing of materials between users and/or with third parties, turning them into online media sharing platforms discussed above. Examples of providers offering file storage and sharing services are Dropbox, box.com and WeTransfer.
- **IaaS/PaaS:** Infrastructure as a Service and Platform as a Service cloud computing services offer a cloud-age version of Web hosting for organizations to run services and applications and making them available to online users. (Notably, these services can themselves act as intermediaries, creating a situation of double hosting.) Examples are AWS (Amazon), Google Cloud, Microsoft Azure, but many smaller and niche players exist in the market.

Category 2: Networking, collaborative production and matchmaking

- **Social networking and discussion forums:** services, like Facebook, LinkedIn and Twitter, that allow people to connect and communicate publicly or semi-publicly.
- **Collaborative production:** services that allow users to collaboratively create documents and other forms of media, and make these available to a broader audience. Wikipedia is an example of this, as well as cloud-based word processing tools, such as Google Docs or Office 365.
- **Online marketplaces:** services, like eBay, Marktplaats, eBid and Craigslist, offering the ability to place advertisements, and sell and buy goods, including second hand goods.
- **Collaborative economy:** services that allow supply and demand relating to various goods and services to connect, for instance with respect to mobility (Lyft, BlaBlaCar), labor (Twizzi), travel/real estate (Airbnb, Homestay), and funding (Kickstarter).
- **Online games:** services offering online multi-user gaming environments (with communication features), such as Xbox Live and World of Warcraft.

Category 3: Selection, search and referencing

- **search tools:** online search services, such as Google Search, Yandex, or Baidu, that provide the possibility to navigate the online environment and search for online accessible information and offerings and directories such as dmoz and startpagina.
- **Ratings and reviews:** online services, like Yelp, that provide the possibility to rate and review third-party offerings of various kinds[53].

4.4. Grey areas: services not clearly covered today

Schwemer, Mahler and Styri conclude that several **grey areas** exist. Given the technical convergence of services, according to them the question arises in some instances whether ISSPs could benefit from either Article 12, 13 or 14 ECD or alternatively do not benefit from

[53] Van Hoboken, J. and coll. (2018), p. 12-14.

any liability exemption at all. Fundamentally, there is not a single online service or activity that does not involve the activity of one or more intermediary service providers. This clearly underlines the importance of the ECD's provision and basic EU-level clarifications with respect to their liability[54].

VoIP and other **interpersonal communication services[55]**, such as e.g. Whatsapp or Telegram, are an area where the applicability of Article 12 ECD becomes relevant. Recital 10 of the EECC acknowledges that certain services may fall both under the EECC and be information society services. Thus, it is possible that certain services are regulated under the EECC and that liability exemptions apply under the ECD. Depending on the nature of the interpersonal communications service, it may involve "mere conduit", "caching" and/or hosting elements, with two or more recipients of such services. Interpersonal communications services typically at least involve some element of transmission (not initiated by the service provider) of information (provided by a service recipient) and the service provider likely does not select the receiver of the transmission or modifies the information contained in it, thus arguably satisfying the conditions in Article 12 ECD[56].

Domain name system (DNS), a **distributed database** where the nodes of the database are name servers[57], represent equally a case where the ECD has not a clear scope:

An organization running a top-level domain (TLD) is called a "registry operator", or simply, **"registry"**. An important function of a registry is to maintain a **TLD zone file** on the **authoritative name servers** (i.e. database of the domain names and associated IP addresses)**,** part of the distributed database, as visualized in the left part of the Figure 8 above. To be distinguished from registries are **registrars**, who offer domain names on the market. Separate from these DNS-related functions, is the maintenance of a **Whois database** which includes **registrant** information. This database is not part of the technical DNS system but a part of the ecosystem of registries and registrars. The Whois database is of special interest in relation to enforcement and its form is currently discussed e.g. in ICANN and has also been influenced by the GDPR.[58]

Technically, the domain name registration, in which the registries and registrars are involved, includes some element of storage, which might fall under **Article 14** ECD. However, that

[54]Van Hoboken, J. and coll. (2018), p. 11.

[55] In Article 2 (5) EECC "interpersonal communications service" means "a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service".

[56] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 33.

[57] See also Art. 4(14) NIS Directive (EU) 2016/1148.

[58] See e.g. report by CENTR (2018). Whois status and impacts from GDPR. See also Hoeren, T., & Völkel, J. (2018). Information Retrieval About Domain Owners According to the GDPR. *Datenschutz und Datensicherheit*.

storage only relates to the storage of the domain name and the related IP address(es), not to the storage of the content, for example a website. A domain name may *itself* be infringing (e.g. trademarks), for which there would be a safe harbour benefiting the registry/registrar.[59]

On the other hand, if the problem is illegal content accessible *via* a domain name, a registry or registrar arguably cannot benefit from the liability exemption in Article 14 ECD, because it is not storing information. The raison d'être of **Article 12** ECD might fit best for domain name services in a teleological reading, but was clearly not drafted with the DNS in mind.[60] The service of registries and registrars does not consist of the transmission of information in a communication network, they only provide pointers to such content through globally-unique, location-independent names. Therefore, domain names are sometimes called "signposts in cyberspace"[61] and the internet standards define the DNS as a support system. It may be argued that registries or registrars are too remotely related to infringing content, to risk liability for infringing content in accordance with national liability standards. Nevertheless, there exists some inconclusive lower court jurisprudence.[62] There have so far been no references to the CJEU regarding the DNS.

In the trademark-related case C-521/17 – ***SNB-REACT***[63], the Court addressed another question related to the addressing function, namely service related to **IP addresses**. From the judgment, it is somewhat unclear exactly what type of service is being considered.[64] Unfortunately, the CJEU refrained from giving further guidance on whether such service would qualify under Article 12, 13 or 14 ECD, leaving it for the referring Court to verify and assess the situation (paras. 50 and 52). ***De lege ferenda***, the question remains whether there ought to be such an exemption. If we consider DNS actors' proximity to the content risks, we need to distinguish *inter alia* between **business and technical proximity**, as mentioned above. Moreover, there may be significant **proportionality issues** related to the measures DNS actors can take to manage content risks. Registries or registrars can take various domain-name related measures, which however, often would be disproportionate, for two reasons. First, the precision of such measures is low because a suspension affects all content to which a domain name points (for example all of wikipedia.org), which is overly broad. At the same time, the suspension of the domain name only removes the "signpost", but the

[59] Disputes about infringing domain names are also addressed in specific procedures focusing on the registrant, e.g. ICANN's Uniform Dispute Resolution Policy.

[60] See Schwemer, S.F. (2018). On domain registries and unlawful website content. *Computer Law & Security Review*, p. 281; Schwemer, S.F. (2020). Report on the workshop on the liability of DNS service providers under the ECD, Prepared for Directorate-General for Communications Networks, Content and Technology (Unit Next-Generation Internet, E.3); Truyens, M., & van Eecke, P. (2016). Liability of Domain Name Registries: Don't Shoot the Messenger. *Computer Law & Security Review*, 32(2), 327–344.

[61] National Research Council. (2005). *Signposts in cyberspace: the Domain Name System and internet navigation*. National Academies Press.

[62] See Schwemer (2018).

[63] C-521/17, *SNB-REACT v Deepak Mehta*, ECLI:EU:C:2018:639.

[64] The plaintiff argued that the defendant had registered the internet domain names that were used to sell counterfeit goods, but this was disputed. It has therefore been interpreted by some as addressing domain registrars.

content itself will typically still be available at the machine identified by the related domain names. Thus, suspension of a domain name is not a particularly effective measure for combating illegal content or information[65].

Despite the above-mentioned conceptual distance to content, some **domain registries** have engaged in some form of voluntary **self-regulation**. There exist, for example, trusted notifier arrangements[66] both with public authorities (e.g. ccTLD *Nominet* with in the *Police Intellectual Property Crime Unit*) and industry organisations (e.g. gTLD registries with *Motion Picture Association of America*; gTLDs and ccTLDs in *Healthy Domain Initiative*), but there is generally scarce information on their workings. Some registries also address content- or technical abuse-related aspects in their ToS and there exist examples of notice-and-actions arrangements.[67] The role of accurate **domain name registration data** about registrants (often referred to as WHOIS data) is of special interest. Some ccTLD registries have noted a plausible correlation between domain names that are used for illegal purposes (related to content or technical abuse) and the quality of such registration data. In this connection, several registries have introduced some kind of data validation process.[68] Related to registration behaviour, several DNS actors have responded to issues such as the potentially abusive registrations during the Covid-19 crisis.[69]

Wi-Fi hotspots did not exist in 2000. Today, internet cafes, hotels, public places and other establishments regularly offer Wi-Fi hotspots to their customers. Furthermore, citizens sometimes share their internet access with family members, friends or visitors. There exists a variety of business models, including the inclusion of advertisement.[70] The provision of Wi-Fi hotspots has a key function for connectivity and implies significant benefits for society, particularly as a complement to existing wireless offers (such as 4G) and future 5G networks.[71] This can be illustrated by the fact that the provision of Wi-Fi hotspots and the related intermediary liability question has also been mentioned e.g. in the public consultation[72] and the Commission's proposal[73] leading to Regulation (EU) 2017/1953 as regards the promotion of internet connectivity in local communities.

---

[65] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 46-48.

[66] See Council of European National Top-Level Domain Registries (CENTR) (2019). *Domain name registries and online content*. Brussels. See also Bridy, A. (2017). Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation. *Washington and Lee Law Review*, 74(3), 1345–1388, and Schwemer (2019).

[67] In the context of ccTLDs see Schwemer (2020); in the context of gTLDs see Kuerbis, B., Mehta, I., & Mueller, M. (2017). In Search of Amoral Registrars: Content Regulation and Domain Name Policy. Internet Governance Project, Georgia Institute of Technology.

[68] Schwemer (2020).

[69] See e.g. ICANN (2020), Corona response; CENTR (2020), report on DNS; Moura, G. et al. (2020). Coronavirus and DNS: view from the .nl ccTLD, SIDN Labs Technical Report TR-2020-01.

[70] This is technically becoming more difficult as most web browsers gradually are enforcing the use of encrypted communication between user and host.

[71] But the possibility exists that they might become less relevant over time with improving 4G or 5G capabilities.

[72] See Commission, Synopsis report on the public consultation on the evaluation and review of the regulatory framework for electronic communications, 2016, p. 9.

According to the case law of the CJEU, it is now settled that the providers of Wi-Fi hotspots benefit from the **liability exemption under Article 12 ECD**.[74] However, in many cases these "service providers" do not offer Wi-Fi-based internet access as their main line of business, but in their private capacity or ancillary to other businesses, which makes it challenging to achieve a fair balance of fundamental rights. As illustrated by the case law before the CJEU, problems related to the provision of Wi-Fi hotspots often occur in the context of intellectual property rights **infringements committed by users** of such hotspots. This includes situations in which the hotspot is unsecured, thus facilitating the use (and the commission of illegal acts) by potentially anonymous third parties.

Usenet newsgroup providers[75] can be considered a grey area concerning '*caching*'. There exists, for example, national court jurisprudence that qualifies Usenet services either for the liability exemption under Article 13 ECD ("caching") or under Article 12 ECD ("mere conduit").[76] In a currently pending reference before the CJEU, C-442/19 – *Stichting Brein*, the referring Dutch court asks for interpretation of a Usenet service provider in the context of Article 14 ECD.

It has also been discussed by some whether "various decentralised content distribution systems" such as DNS providers or peer-to-peer networks could fall under Article 13 ECD.[77] In any case, it seems that these kinds of services were not in the intention of the legislator when drafting Article 13 ECD. Also the provision of services related to **CDNs** are an emerging area of interest at the borderline of Articles 12, 13 and 14 ECD, which will be discussed in detail below. Furthermore, the emerging and prevalent practice of **content adaptation** could be of interest with regard to Articles 12 and 13 ECD. Finally, **cloud computing** might make caching less significant. When computing resources, including storage (i.e. hosting), can be "*rapidly provisioned and released with minimal management effort or service provider interaction*" (definition by NIST), it may challenge delimitation between Article 13 and 14 in relation to permanent and non-permanent storage. One result of this rapid elasticity and scalability of cloud hosting could be that caching is replaced by temporary "virtual" hosting[78].

The market segment for **Content delivery networks (CDNs)** evolved from the need to maintain a large number of specialized caching proxy servers in data centers all over the world, and from the need to store large media files, for example video content, on servers in either the same data centers as the caching proxy servers or in similar data centers close to the users. Thus, in addition to traditional caching of illegal information, functions such as

---

[73] Commission, Proposal for a Regulation amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of Internet connectivity in local communities, 14.9.2016, COM/2016/0589 final.
[74] C-484/14, *McFadden*, ECLI:EU:C:2016:689.
[75] Usenet has existed since 1979 and constitutes a worldwide platform for exchanging messages in newsgroups, as further described in pending Case C-442/19.
[76] See also Nordemann (2018), p. 15 ff.
[77] DLA Piper (2009), Chapter 6. See however in detail below.
[78] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 36.

surrogate hosting and content adaptation could raise some questions on the applicable conditions of the liability exemption, if some part of the content in the CDN is illegal. CDN services are often combined with other additional related services such as DNS resolvers, cybersecurity services like DDoS protection (a further function of reverse proxy servers), hosting or domain registrar services. Today, the use of CDNs is widespread and relied on by a large number of lawful as well as unlawful services. Given the range of CDN business models consisting of a variety of **different complex functions**, the CDN notion would **not be useful** as a legal concept. Instead, it is necessary to differentiate between the respective services and functions, which may fall under different **liability exemption** rules.

Given the increased practical importance of CDNs, it is of interest to assess their role in the intermediary liability regime of the ECD. The availability of liability exemptions has also been identified to be of major business importance to CDN service providers.[79] Generally, there exists little jurisprudence on CDNs and the related technical functions. In 2019 and 2020 respectively, however, *Cloudflare* has been subject to several **national court** proceedings in the EU in the context of **injunctions**. In the case *Mediaset (RTI) vs. Cloudflare*, the Italian court ordered *Cloudflare* to terminate the account of "several pirate websites" and to transmit information on its customers to the plaintiff in order to enable the identification of hosting providers and operators of the websites.[80] The Court notes that *Cloudflare's* services fall within the scope of the ECD and differentiates two aspects: Firstly that *Cloudflare* requires its customers to name *Cloudflare* name servers of the CDN as the authoritative nameservers for their domain name, which is why a Whois-lookup only shows the CDN's name servers. Secondly, the provision of a CDN, where "in particular, a CDN takes static content and stores a copy in the node that is closest to the visitor of the website". In addition to that, the Court evaluates that *Cloudflare* also provides **hosting services** which entail the non-temporary storage of content through the service known as "Always online" (p.10). In its judgment, however, the Court left aside both the caching and mere conduit activities and focused on the transposition of **Article 14 ECD** in relation to the latter "Always online" function. The Court therefore concludes that *Cloudflare* is falling under Article 14 ECD and failed to take action after it received notice from the rightsholder.[81]

In 2020, the Court of Milan, granted another injunction against *Cloudflare*, without an assessment of the liability exemptions (cf. InfoSoc and Enforcement Directives). In 2020, *Cloudflare* also launched a test case (full merit procedure, not preliminary injunction) against

[79] In its quarterly report to the SEC, Cloudflare noted in relation to business risks: "Our customers may use our platform and products in violation of applicable law or in violation of our terms of service or the customer's own policies. The existing laws relating to the liability of providers of online products and services for activities of their users are highly unsettled and in flux both within the United States and internationally", see Cloudflare, *Quarterly Report to the United States Securities and Exchange Commission, Form 10-Q, quarterly period ended September 30, 2019*, p. 57.

[80] See Cloudflare (2020), Transparency report. *Mediaset (RTI) vs. Cloudflare*, order of Rome Commercial Court from 13 March 2019, no. 1932/2019 and confirmed in *Mediaset (RTI) vs. Cloudflare,* order of the Rome Commercial Court from 24 June 2019, no. 26942/2019.

[81] See Court of Rome VI 24 June 2019, p. 3.

Mediaset before the Tribunal of Milan arguing that it is not a hosting provider (case no. 14686/2020). Finally, there exist several administrative orders by the Italian Communications Regulatory Authority AGCOM.

In Germany, a case for a preliminary injunction before the Cologne District Court against Cloudflare concerned the provision of a CDN for the optimization and speed-improvement of content as well as the redirection via DNS-servers to the structurally copyright-infringing website "ddl-music.to".[82] *Cloudflare* claimed that it did not provide a hosting service and merely offered the transient storage of content in the sense of Articles 12 and 13 ECD[83], which was neither chosen nor adapted in its form. Furthermore, *Cloudflare* noted that the blocking of specific content available under a specific URL is technically not possible given the structure of its services and that blocking would be disproportionate.

The German court deems the conditions of **Article 12 ECD** not fulfilled, notably because *Cloudflare* –and not the website owner– is performing the **selection of addressees** of the transmitted information by filtering or sorting a part of the users based on the requesting IP address. The service aimed at the optimization and acceleration of the website that is performed by *Cloudflare* as name server via its CDN is necessarily coming with interventions in the transmission of information from and to the website of its customers, in part because *Cloudflare* guarantees the availability of the customer's website even if it is temporarily inaccessible. Thus, the Court deems that *Cloudflare* is not passive and not merely performing the intermediate storage with the purpose of acceleration of transmission of information. Furthermore, the Court confirms by relating to the existing German case law on IAPs that *Cloudflare* has **no duty** to monitor or investigate the content of domains, for which it acts as name server and CDN server.

Both cases concern structurally copyright-infringing websites and principally deal with the problem of **identifying** the infringing party. In this connection, one question is whether an infringed third party's request for customer information should be answered without a court order.

To address this gap (at least for the use of reverse proxies by CDNs), some authors propose that the lawmaker should consider extending the existing safe harbour provisions, taking into account the degree of control CDNs have over content risks[84].

Live-streaming

Live-streaming has in recent years become more topical both in a commercial context and in the context of illegal or harmful content. In principle, live-streaming without intermediaries

[82] Cologne District Court, case 14 O 171/19, 30 January 2020, *Universal Music GmbH v Cloudflare.*

[83] Furthermore, *Cloudflare* declared in lieu of an oath that only specific static content is temporarily saved on servers, whereas audio- and video-content generally is excluded because the amount of data is unsuitable for efficiency-raising caching. It is not clear from the judgment, whether the audio- and video-content is routed through the *Cloudflare* infrastructure.

[84] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 36.

storing the content is technically possible. However, in practice live-streaming is a service that usually provides simultaneous storing and real time streaming of an event, and live-streaming will use the same CDNs that are used for streaming stored content. There are many service providers offering a technical platform and hosting service for live-streaming.

Because live-streaming involves an event that is transmitted in real time, the party initiating the streaming will start transmitting when the event starts. The party initiating the streaming may decide to publish the recorded event as an ordinary streamed video immediately when the real time event terminates. Users get access to the live-stream by requesting to receive the transmission. Live-streaming is also part of the content offered by social media services like Facebook and Twitter, and live-streaming content may be suggested to anyone using these services. **Many-to-many live-streaming** is also supported by many service providers, and this service is usually called video conferencing.

Live-streaming can be a type of linear audiovisual media service that is regulated in the revised AVMSD. This Directive addresses **video-sharing platform services**, including both non-linear (on demand) and linear services, which arguably include live-streaming.[85] The revised AVMSD (Article 28b) requires providers of video-sharing platforms to take appropriate measures to address incitement to violence and some forms of hatred against individuals or groups. In addition, the providers need to protect the public from content that is illegal under Union law (related to terrorism, child abuse images, racism and xenophobia). The AVMSD explicitly states in Art. 28a (5) that Articles 12 to 15 ECD apply to video-sharing platform providers.[86]

In the context of the **ECD**, live-streaming is **difficult to locate** and there exists only scarce case law. Functionally, live-streaming is similar to hosting, but likely does not qualify as such under **Article 14**, because the streamed content is not stored before the communication, but streamed in a linear manner. Technically, live-streaming involves some element of transmission in a communications network (mere conduit)[87], but the nature of the service may be different from the one envisaged by **Article 12**, because of temporal and functional characteristics.[88] The default situation for mere conduit is the instantaneous communication of data in a network, which is over when the data is communicated. Thus, by the time a

[85] On such a service, videos are shared, and the organisation of the sharing is determined by the provider. The wording speaks of a service that is devoted to "providing" programmes, user-generated videos, or both, to the general public. In the drafting history of the revised AVMSD, the word "providing" replaced an earlier proposal focussing on "storage or live streaming". While the 2010 AVMSD classified live-streaming as television (recital 27), the 2018 AVMSD, emphasises in recital 9 "that the procedures and conditions for restricting freedom to provide and receive audiovisual media services should be the same for both linear and non-linear services". See references in N. Feci, Gamers watching gamers: the AVMSD soon the one calling the shots? (18 December 2018). See also Commission, Communication from the Commission Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive 2020/C 223/02, C/2020/4322.

[86] Moreover, according to Art. 28b(3), second subparagraph, such measures shall not lead to any ex-ante control measures or upload-filtering of content, which do not comply with Art. 15 of the ECD.

[87] See also Nordemann (2018), p. 13.

[88] See on temporal aspect C- 484/14, *McFadden*, para. 62.

notice can be issued, the communication is already over. In the case of live-streaming, content is continuously streamed for a limited time. This is somewhat **comparable to hosting** because the live-streaming service "hosts" the live-stream, which is not necessarily a stored file (like hosting), but a continuous content stream. Thus, notice-and-action may be possible, and certain measures are obligatory under the AVMSD. Live-streaming may also involve a temporary storage of content (**Article 13**), but it is uncertain whether the provider does so "for the *sole* purpose of making more efficient the information's *onward* transition".[89] Moreover, an eventual liability might be based not (only) on the temporary storage, but also on the streaming (the provision of access to the streamed content) itself, for which no dedicated exemption exists.

A more principal question is whether live-streaming falls under the ECD regime in the first place: the ISS definition requires that such service is "'at the **individual request** of a recipient of services". It could be argued that this criterion is not fulfilled in the case of live-streaming, which resembles broadcasting.[90] On the other hand, the criterion could be fulfilled, if the streamer (the person initiating the streaming) is seen as the recipient of the service – but this makes it difficult to distinguish between streaming and broadcasting. Moreover, the live-streaming provider itself can **select** the viewer of the live-stream, that is, the **receiver of the communications,** for example based on algorithms that evaluate the users' interests. This is can be the case with respect to existing live-streaming services such as *Facebook* and *YouTube*, but it would arguably void the protection afforded by Article 12(1)(b) ECD. Under a narrow reading of the ECD, at least some instances of live-streaming may therefore be neither protected under Articles 12 or 14 ECD.

A future regulation could address this gap, taking into account the control the service provider reasonably has over the content-related risks. A live-streaming services provider has a relatively **close proximity to the content**, compared to typical mere conduit providers. Technically, the live-streaming provider is directly or indirectly connected to the livestream, because the streamer is most likely its customer. Moreover, as foreseen in the AVMSD, these providers of video services are in a position to manage some aspects of the live-streaming they organize. At the same time, a service provider cannot be expected, however, to have knowledge of everything happening on its service in real time.

Processing in the cloud

[89] Article 13(1) ECD, emphasis added.

[90] Broadcasting under the AVMSD, may be subject to further requirements, such as e.g. license to operate. The Technical Standards Directive indicates in Annex I services, which are not considered to be supplied "at the individual request of a recipient of services", namely "[s]ervices provided by transmitting data without individual demand for simultaneous reception by an unlimited number of individual receivers (point to multipoint transmission)" including "television broadcasting services (including near-video on-demand services) (...)", "radio broadcasting services", and "(televised) teletext".

Remote processing operations carried out in **cloud computing** and other contexts imply the possibility that the service provider is involved with *processing* illegal content.[91] Similarly, the **remote processing of illegal information** may be problematic also in other contexts, such as with respect to **content adaptation**, for example in a CDN context.

"Cloud computing" is used as a label for a variety of business models that primarily offer the use of resources in data centers. A "cloud computing service" can be defined as a "digital service that enables access to a scalable and elastic pool of shareable computing resources."[92] Further characteristics include self-service and metered provision, meaning one only pays for the resources one is using.

Within the liability exemptions of the ECD it is not easy to locate all services offered in a cloud setting. Under **Article 14 ECD**[93], the service provider is not liable for the **information stored** at the request of a recipient of the service. Storage of information is certainly relevant in cloud settings, but the stored information is often encrypted, which makes notice-and-action challenging.[94] In addition, the relatively complex cloud business models typically go far beyond storage of information. Services involving the **processing** of data, thus going beyond storage, include **IaaS** (infrastructure as a service), **PaaS** (platform as a service) and **SaaS** (software as a service). Cloud based data processing can have a variety of use cases, including IoT and robotics.

A first question is whether **cloud processing** services can be seen as **separate from the storage,** in the sense that these would be separate actions for which the service provider could be liable. There is no clarity on whether the performance of *processing* services could be taken as an argument for constituting liability, separate from the argument of *storage* of information. It may be argued that the processing is carried out in close relation to the storage service. On the other hand, Article 14 does not explicitly include wording that would include other (e.g. processing-related) services in the safe harbour it provides.[95] Thus, one would have to identify a separate liability exemption for such services. This second question depends on an interpretation of Articles 12 and 13 ECD, respectively.

Concomitantly, Schwemer, Mahler and Styri recommend that the European lawmaker addresses the exemption gap for remote processing operations, as well as the possibility that new business models offer functions that do not fit into the existing limitations[96]

[91] The challenges with processing in a cloud context were also highlighted in van Hoboken et al. (2020), p. 15.
[92] Art. 4 nr. 16 of the NIS Directive. A more precise term than "shareable" might be "multi-tenant".
[93] Part of the literature sees Article 14 as most appropriate for cloud services, e.g. Sluijs, J. et al. (2012). Cloud Computing in the EU Policy Sphere, *JIPITEC*, 12, N 80.
[94] See, e.g., GSM ETNO Position paper on the proposal for a regulation on preventing the dissemination of terrorist content online July 2019.
[95] Weber argues that Article 14 is based on an "inflexible" definition. See Weber, R.H. & Staiger, D.N. (2014). "Cloud Computing: A cluster of complex liability issues", 20(1) *Web JCL*.
[96] Schwemer, S., Mahler, T. & Styri, H. (2020), p. 55-57.

Annex 10: Overview of voluntary measures and cooperation

1. SELF-REGULATORY EFFORTS COORDINATED BY THE COMMISSION

I. Introduction

The ECD requires Member States and the Commission to encourage the adoption of Codes of Conduct in order to help implement the Directive properly.

The Commission has set up a number of sectoral dialogues with stakeholders or initiated other self-regulatory/voluntary mechanisms which *inter alia* have dealt with the removal of (potentially) illegal content:

1. **Code of Conduct on Countering Illegal Hate Speech Online** (DG JUST)
2. **Code of Practice on** Disinformation (DG CNECT)
3. **EU Internet Forum** – terrorist propaganda (DG HOME)
4. **INHOPE network of hotlines** – child sexual abuse (DG CNECT)
5. **Memorandum of Understanding on the sale of Counterfeit Goods** on the Internet[1] (DG GROW)
6. **Memorandum of understanding on online advertising and IPR** (DG GROW)
7. **Product Safety Pledge - Voluntary commitment of online marketplaces with respect to the safety of non-food consumer products sold online by third party sellers** (DG JUST)

The above dialogues deal with different types of illegal content/ products infringing different areas of EU or national legislation (consumer law, product safety, etc.). They do not cover all types of illegal content (e.g. copyright).

II. Analysis

1. Participants

The participants in the dialogues depend on the type of illegal content.

As regards *ISPs/platforms*, on issues such as terrorist propaganda, hate speech, child sexual abuse material and illegal commercial practices, Facebook, Twitter, and YouTube (Google) as well as Microsoft (in the first three) are the most prominent representatives, although there are also others. As regards online sales of goods, food safety, counterfeit goods, large online marketplaces (eBay, Alibaba, Amazon, Allegro etc.) are the most involved. As regards, intermediation of services (i.e., in the collaborative economy), the workshops on collaborative short-term rental accommodation services brought together umbrella

1

organisations of online platforms (such as the European Holiday Home Association), while some individual platforms (e.g. Airbnb, Homeaway) were invited for targeted presentations.

Depending on the field, the *competent authorities* of the Member States (e.g. market surveillance authorities, law enforcement authorities, authorities responsible for consumer protection (CPC) or ministries, authorities responsible for tourism) take part in the dialogues, EU agencies (such as Europol in the EU Internet Forum) and the CoR.

In areas related to the take-down of illegal products, the *relevant sector of the industry* is also represented, i.e. the food industry in relation to the internet sale of food chain products or the luxury industry in the MoU on counterfeit goods.

The *civil society* (consumer and/or free speech organisations) takes part in the dialogues either as active participants (e.g. INHOPE hotlines) or as observers (e.g. Code on Hate Speech). The EU Internet Forum includes representatives from the Radicalisation Awareness Network in particular as regards discussions on engagement with and support to civil society in the development of alternative and counter narratives. Their role and involvement seems to vary depending on the dialogue.

The dialogues seem to be open to other stakeholders to join or at least to apply the standards achieved therein.

2. The procedures to tackle illegal content

In order to benefit from the liability exemption in the ECD, platforms, *inter alia,* have to disable access to the illegal content or to remove it rapidly, once they become or are made aware of it. Such "notice and action" procedures exist or are currently under preparation in several Member States with respect to some or all types of illegal content (horizontal or specific to hate speech, IPR etc.).

Who can send a notice?

Among the examined dialogues, some have established "notice and action" procedures in which stakeholders/users can send notices to the platforms. Under the MoU on Counterfeit Goods, the right owners can send notices to the platforms according to the agreed rules. Under the Code on Hate Speech, any user can send notices to the platforms which they review in less than 24 hours. Under the Product Safety Pledge, online marketplaces commit to have an internal mechanism for notice and take-down procedure for dangerous products. This should include commitments from the marketplace's side on the procedure they will follow when notices are given by authorities and other actors.

In the other dialogues, platforms agreed to act on notices of illegal content sent by authorities. In the context of the EU Internet Forum, platforms remove terrorist content on the basis of notices sent by the Europol Internet Referral Unit (IRU) as well as national IRUs. As regards the Product Safety Pledge, online marketplaces commit to react within two working days to government notices made to the single contact points in Member States' authorities to remove identified listings offering unsafe products for sale in the EU. Inform the authorities on the action taken market surveillance authorities notify the platforms (such a procedure will be mentioned in the upcoming Commission Notice). Social media companies are also requested to react to the notices from authorities responsible for consumer protection (CPC authorities).

Finally, the INHOPE network's hotlines receive notices by any user (also anonymous notices). The platforms are notified either by the hotline or by the law enforcement authority, depending on the Member State.

Are the procedures regulated in details or is it left to the platforms to establish their policies?

The dialogues do not contain detailed rules on the procedures; platforms seem to establish their own policies. The MoU on Counterfeit Goods contain some minimum requirements and so does the Code on Hate Speech when it requires a reaction from the platform within 24 hours. In the dialogue on illegal commercial practices, the Commission proposed some procedural rules to follow both by the competent authorities and the platforms (content of the notice, feedback by the platform, timeline etc.). Among the actions agreed under the EU Internet Forum, several specify details for referrals including commitments to react in the shortest time possible, streamlining of referrals and feedback (including points if contact).

Are there requirements for the content/quality of the notice? Are templates in use?

There are a number of dialogues where such requirements or recommendations are established. The MoU on Counterfeit Goods elaborates that the notice needs to be effective and efficient, understandable, simple to process etc. It should clearly identify the relevant product. Templates are not in use. The Code on Hate Speech refers to the case law on valid notifications which indicates that the notice "should not be insufficiently precise or inadequately substantiated".

In the dialogue on illegal commercial practices, the Commission made some proposals to competent authorities on the content of the notice (description of the illegal content, justification, etc.). On product safety, there are no specific requirements but the description of the product and the justification are considered essential elements of the notice.

On terrorist propaganda, the IRU uses the templates provided by the platforms. The INHOPE network's hotlines also provide templates for reporting.

Is there a possibility for a counter-notice by the uploader of the content?

Counter-notice procedures are a safeguard against excessive or erroneous removal. The MoU on Counterfeit Goods allows for a counter-notice by the seller. In practice, this seems to be the case also with respect to the safety of products sold online.

There is no room for counter-notice in the case of child sexual abuse material or terrorist propaganda. The Code on Hate Speech does not address this question.

What are the transparency requirements?

It seems that only the MoU on Counterfeit Goods and the Code on Hate Speech contains transparency requirements. In the first case, the platforms commit to adopt, publish and enforce IPR policies, which should be clearly communicated and indicated on their sites and reflected in the contracts which they conclude with their sellers. They also commit to disclose, upon request, the identity and contact details of alleged infringers.

The Code on Hate Speech does not contain any explicit commitments but it indicates that the companies and the Commission agree to further discuss how to promote transparency. A conclusion from the second monitoring exercise is that while Facebook sends systematic feedback to users and practices differed considerably among the social media platforms.

As regards terrorist propaganda, platforms have general reporting mechanisms in place; however, not all companies provide specific terrorism-related reporting (Twitter invested in such specific transparent reporting mechanisms). Under the EU Internet Forum more specific indicators for reporting on agreed actions have been developed.

Are there rules on bad-faith notices and repeat infringers?

Where notices come from authorities, provisions on bad-faith abusive notices do not seem necessary. The MoU on Counterfeit Goods *inter alia* requires right owners to notify the platform in a responsible and accurate way and to avoid unjustified, unfounded and abusive notifications. In cases where it is obvious that notices are sent without exercising appropriate care, rights owners may be denied or may have only restricted access to the procedure. The Code on Hate Speech does not contain such rules.

Also, only the MoU and the Product Safety Pledge contain rules on repeat infringers although platforms seem to have policies in place also in other areas.

Are the specific rules on trusted flaggers?

In the Code on Hate Speech, platforms commit to encourage provision of notices by trusted flaggers as well as to provide them support and training. On terrorist propaganda, the IRU is in itself a trusted flagger and platforms develop such networks. The MoU on Counterfeit Goods does not contain specific rules but the signatories are considered trusted flaggers.

Do platforms have an obligation to cooperate with authorities?

The platforms participating in the dialogue on illegal commercial practices as well as on product safety and food safety committed to provide a single email address to authorities. Under the Code on Hate Speech and the EU Internet Forum, they also committed to have a single point of contact.

The INHOPE hotlines have an obligation to cooperate with law enforcement authorities. Under the MoU on Counterfeit Goods, rights owners and platforms commit to cooperate with law enforcement authorities, where appropriate and in accordance with applicable law.

3. Pro-active measures

Do platforms commit to take pro-active measures to remove illegal content?

As regards the examined dialogues, there is such an explicit commitment in the MoU on Counterfeit Goods but not in the other cases. It does not mean however that, in some areas, platforms do not work on concrete measures, for example to avoid the reappearance of illegal content on other sites. Under the EU Internet Forum, companies were encouraged to urgently develop and use content detection and identification technology, i.e. machine learning, to find all relevant formats of new and historical terrorist content on all their services at the point of uploading and ensure robust mechanisms are in place to ensure swift decision-making and removal. Furthermore, companies were encouraged to optimise the database of hashes being developed in the context of the EU Internet Forum to feed the database with relevant content surfaced via multiple sources (flagging, automated detection, etc.) and to ensure that platforms and services are connected to the Database of Hashes.

Airbnb has also agreed to disconnect providers when offering their services beyond the number of days allowed in certain cities.

Under the Product Safety Pledge, online marketplaces commit to consult information on recalled/dangerous products available on Safety Gate/RAPEX, as well as to cooperate with

authorities and set up a process aimed at proactively removing banned product groups as appropriate.

1. Selected KPIs and results

TYPE OF CONTENT (VOLUNTARY DIALOGUE)	HOSTING SERVICES PARTICIPATING	PROACTIVE TAKEDOWN (% OF THE TOTAL REMOVED CONTENT, COMPARED TO CONTENT REMOVED FOLLOWING NOTICES)	NUMBER OF NOTICES	% REMOVALS (OUT OF CONTENT NOTIFIED	SPEED
TERRORISM (EU INTERNET FORUM)[1]	**Reached out to** 20 **platforms**, including**.** Facebook, YouTube, Microsoft, Twitter, Internet archive, Justpaste.it, Wordpress, snap, Soundcloud **After Recommendation: Baaz, Dropbox, Mega, Userscloud, Telegram**	Varies across companies: e.g. 44**% (Q2 2018) to 83% (Q4 2017)** reported by **one SME**; 99% by Facebook in Q1 2018 Database of hashes used by 13 companies	For EU IRU: Q4 2017**: 8,103 referrals** Q1 2018**: 5,708 referrals**	For EU IRU: Q4 2017: 89% Q1 2018: 61% (But between 96 and 100% for "big four": FB, YouTube, Microsoft and Twitter)	Proactive measures: 5 companies reported to remove content within 1h, out of which 3 companies could do it within 1 minute, using proactive measures. For referrals: majority of companies not removing within one hour; nevertheless some have jumped from 0% to 66% removals within one hour or 8% to 52%.
HATE SPEECH (CODE OF CONDUCT)	Since May 2016: **Facebook, YouTube, Twitter, Microsoft** Since 2018: **Instagram, Google+, Snapchat and Dailymotion** Since 2019: **Jeuxvideo.com** In 2020: **TikTok**	(not covered by the scope of the code)	**December 2016**: 600 notices **June 2017**: 2575 notices **January 2018**: 2982 notices **June 2020**: 4364 notices	**December 2016**: 28% **June 2017**: 59% **January 2018**: 70 % **June 2020:** 71%	**December 2016**: 40% of the notifications are reviewed in 24h, 43% in 48h, **June 2017**: 51.4% of the notifications are reviewed in 24h, 20.7% in 48h, **January 2018**: 81.7% of the notifications are reviewed in 24h, 10% in 48h **June 2020:** 90% of the notifications are reviewed in 24h, 4.9% in less than 48

[1] This information is dated to 2018 as this was the last comprehensive data collection exercise, pending the adoption of the terrorist content online regulation

					hours
MEMORANDUM OF UNDERSTANDING ON THE SALE OF COUNTERFEIT GOODS (MOU)	**Alibaba, Amazon, eBay, Priceminister/Rakuten, Allegro, Apple, Facebook marketplace**	**December 2016**: notices represented 13.7% of total takedowns (86.3% due to proactive measures) **June 2017**: Notices represented only 2.6% of the total takedowns (97.4% due to proactive measures) **August 2020**: Notices represented 8,8% of total takedowns (up to 98.2% as a result of application of proactive measures)	**December 2016**: 14% fake products found **June 2017**: 11% fake products found	Rights owners report that notices sent lead to takedown almost in 100 % of the cases.	Right owners suggest that takedown is made within few hours, not "without undue delay"
PRODUCT SAFETY PLEDGE	**AliExpress, Amazon, eBay,Rakuten France, CDiscount, Allegro**				-
CHILD SAFETY (INHOPE NETWORK)	Cover a wide-range of hosting services	No sector-wide data available. YouTube, for example, reports **over 85% of the CSAM** content taken down through automated means.	**2017:** Nearly 90 000 reports submitted by internet users to the INHOPE network of hotlines[2] - excluding reports to the North American hotlines on content hosted in	Nearly 100%. NB: Reports from the public are previously checked by the INHOPE network of hotlines: 20% only identified as CSAM. The overall number of reports submitted to	**2017**: 62% of the content identified was verified to have been taken down within 3 days from report to hotline, 17% within 4-6 days, 21% longer than 6 days.

2 A report is equivalent to an URL; one URL may contain several images of videos

			North America. **2019:** 183,788 reports	INHOPE hotlines is over 400,000 annually.	

2. 2018 RECOMMENDATION: UPTAKE

In the Recommendation on measures to effectively tackle illegal content online[1] from 1 March 2018, the Commission called on stakeholders to step-up their activities with fight against illegal content available online. . It encouraged Member States to take specific actions as well, in particularly to facilitate out-of-court settlements (*Point 14*), to designate points of contact for matters relating to illegal content online (*Point 22*), to cooperate with hosting service providers via fast-track procedures (*Point 23*), and to establish legal obligations for hosting service providers to inform law enforcement authorities about serious criminal offences *(Point 24*). Furthermore, some Points of the Recommendations that mainly affect hosting service providers might require Members States assistance as well: establishment of mechanisms to submit notices (*Point 5*) that are sufficiently precise and substantiated (*Point 6*), procedure concerning process of notice processing (*Points 7-13*), to encourage transparency (*Points 16-17*), proactive measures (*Point 18*) or safeguards (*Point 19*). In addition, the Recommendation foresees that Member States provide to the Commission, upon its request, all relevant information to allow for the monitoring of its effects (*Point 43*).

The Commission discussed steps that Member States haven taken prior to the Recommendation twice during the meetings of the e-Commerce Expert Group. During the meeting on 14 June 2018, Member States reported implementation of Points 14 and 22-24 of the Recommendation to their national frameworks.

- *Out-of-court dispute settlement mechanisms*: Member States attending the meeting explained that any specific out-of-court dispute mechanisms had not been adopted prior to the Recommendation, as they generally considered the already existing traditional dispute settlement mechanisms sufficient also for the purpose of illegal content online removal or disablement.
- *Points of contact for matter related to illegal content online and cooperation with hosting service providers*: Member States reported that, in general terms, the cooperation between governments, law enforcement authorities and hosting service providers' points of contact works well, and that large platforms are rather active and willing to collaborate. One Member State reported the difficulty encountered with small hosting service providers that were generally not willing to collaborate. Overall, Member States noticed a clear progress in the cooperation with different stakeholders based on already existing sectorial points of contact.
- *Fast-track procedures*: Member States reported that no new fast-track procedures were established except for one Member State, which established a simplified procedure for cases concerning child sexual abuse. Most of the experts were of the view that there is no need to implement such a procedure, as the cooperation partly works based on sectoral procedures.

Concerning overall structure and administrative and organisational measures, Member States explained that they are still identifying further steps to take. Some Member States called for a continuation of a sectorial approach. Number of Member States reported concerns of the

[1] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

national authorities as to the time for removal given to online platforms - one hour was considered as too short timeframe.

During the meeting on 8 October 2019, Member States informed about their experiences and steps they took to implement the Recommendation at national level, including legislative measures. Some Member States explained that dedicated legislations have been prepared prior to the Recommendation and have been evaluated at that time. Several Member States explained that they would welcome targeted EU approach concerning notice and action procedure that they expect to be especially positive for the SMEs. In this regard, Member States supported clear empowerment of users to sending notices directly. Some Member States explained that in relation to Delfi case[2], they have had particular difficulties with anonymous notifiers and comments in discussions online, and only registered comments were enables. Freedom of expression was recalled in this regard as well. Concerning the cooperation with large hosting service providers, Member States expressed diverse views, while they were in general positive regarding transparency measures.

[2] Delfi AS v. Estonia, http://hudoc.echr.coe.int/eng?i=001-155105

Annex 11: Content moderation tools

Online platforms typically rely on Terms of Service and Community Guidelines to provide for rules around what is and what is not allowed on any given platform. These rules do not necessarily reflect any specific legal system but do often overlap in several instances with local laws. Enforcing these rules at scale poses a significant challenge to many platforms. On YouTube alone more than 300 hours of video are uploaded to the platform every minute. There are, on average, 500 million tweets produced per day, totalling around 200 billion per year. Instagram hosts more than 500 million 'Instagram Stories' every day.[1] To moderate this vast volume of content, these platforms deploy numerous tools to identify, parse and triage what needs to be reviewed against the terms of service or community guidelines of a given platform. This not, however, the case for any type of content, neither for any type of platform.

There are a range of tools and technologies deployed with various level of performance and accuracy. These play an important role to detect content allowing prioritisation for human reviewers to make the decision on compatibility with the terms of service or community guidelines, but also to make direct decisions, without human intervention. This is often the case for so-called staydown tools, which block content previously identified for reappearing. Since the outburst of the COVID-19 pandemics, several very large platforms have relied on automated tools with prevalence, looping out the human review also for other types of detection technologies[2].

These tools can be broadly classified as technologies which *match* content to *known* images, text or video in a database and classification tools which can *classify* new images as part of pre-defined categories.[3] The graph below shows the variety of tools deployed by major industry players to detect content which is illegal and/or against their terms and conditions and the sections following it will further explain the most common tools deployed, how they are used and what are their strengths and downsides.

Table 2. Publicly reported algorithmic moderation systems deployed by major platforms, by issue area.

	Terrorism	Violence	Toxic speech	Copyright	Child abuse	Sexual content	Spam & automated accounts
Facebook	Shared Industry Hash Database (SIHD), ISIS/Al-Qaeda classifier	Community standards classifiers	Community standards classifiers	Rights manager	PhotoDNA	Non-consensual intimate image classifier, nudity detection	Immune system
Instagram			Comment filter	Rights manager	PhotoDNA		Comment filter, false account detection
YouTube	SIHD, Community Guidelines (CG) ML classifiers	CG ML Classifiers	CG ML Classifiers	Content ID	Content safety API, PhotoDNA	CG ML Classifiers	CG ML Classifiers
Twitter	SIHD		Quality filter		PhotoDNA	Sexual content interstitial	Proactive Tweet and account detection, quality filter
WhatsApp					PhotoDNA		Modified immune system

Figure 13 Gorwa et.al 2020, Algorithmic content moderation: Technical and political challenges in the automation of platform governance

[1] https://gnet-research.org/wp-content/uploads/2020/09/GNET-Report-Decoding-Hate-Using-Experimental-Text-Analysis-to-Classify-Terrorist-Content.pdf

[2] See, for example, Facebook's announcement of 19 March 2020 https://about.fb.com/news/2020/08/coronavirus/

[3] ROVERA: Automated Content Moderation Systems Case Study (forthcoming)

Hashmatching

'Hash matching', in which a fingerprint of an image, video or sound is compared with a database of fingerprints of known content is used by many platforms to detect a variety of types of material including terrorist content, child sexual abuse material as well as copyright infringements.

Traditional hash matching can identify the *exact* copy of an image which has already been identified. This, however, makes it prone to circumvention by minor changes on the image (adding watermarks or borders, cropping, flipping, or any other modification). As such, other forms of hash matching, which focus on looking for similarities between the fingerprints including fuzzy hashing, locality-sensitive hashing and perceptual hashing are often used in content moderation as these are able to detect the image even with small changes in format[4].

A key feature of hash matching tools is that they require databases of known fingerprints of already classified content. As such, the performance and quality of matching technologies is by and large dependent on the quality and governance around the database of fingerprints against which matching is conducted. The overall governance, security and integrity of such databases are of crucial importance for the robustness of the system. Considerations on the initial identification and acceptance process for a piece of content to be added to the database are particularly important.

The very large online platforms have internal databases of fingerprints of material of certain types of content which they have already deemed prohibited by their terms of service. Further, a small number of both public and industry owned databases are starting to be used by several companies to ensure that content removed from one platform can also be detected once uploaded on another platform. These are, however, of small scale at present, both in terms of types of content they cover, and the number of companies benefitting from access to these efforts. The following provides for a non-exhaustive sample of examples on certain types of content.

Child sexual abuse imagery

The largest database of hashes is that of the National Center for Missing and Exploited Children, a public-interest, non-governmental organisation established by the US Congress in 1984 to facilitate detection and reporting of child sexual abuse material (as defined in US law). Content is reported to NCMEC by companies or through direct user reports, and, before it is hashed and included in the database, every piece of content is viewed and agreed upon as being child sexual abuse material by two different experts at the National Center before it is included in the database. NCMEC's platform now contains more than 3.5 million hashes of child sexual abuse imagery[5]. In Europe, there is no database of this scale, with some INHOPE hotlines[6] maintaining databases of a few hundred images, and offering access to their members.

[4] https://journals.sagepub.com/doi/full/10.1177/2053951719897945

[5] https://www.iwf.org.uk/news/landmark-data-sharing-agreement-to-help-safeguard-victims-of-sexual-abuse-imagery

[6] IWF in the UK

The most renowned software used for hash-based filtering of child sexual abuse material is PhotoDNA[7], maintained by Microsoft and made available to qualified organizations for free under certain conditions. The rate of true false positives of the tool is virtually unknown, as no testing or performance information is available,[8] However, simple hashing, such as the precursor MD5 non-cryptographic hashing algorithm still used today, are generally good at matching perfect copies of images and significant concerns around false positives in the decade of use have not surfaced. Given that hashing technologies are unable to account for context, an important characteristic of CSAM in the reliability of using such tools is that the content is illegal under any circumstance, irrespective of the context in which it is disseminated.

Terrorist content

In 2017, the Global Internet Forum to Counter Terrorism (GIFCT) launched a hash sharing consortium among member companies. The consortium shares digital fingerprints of known terrorist images and videos between its 13 member companies. The scope of database is limited to content related to organizations on the United Nations Security Council's consolidated sanctions list with the exception of videos or images which qualify as content produced by a perpetrator during the course of a real-world ongoing attack. To date, the Hash Sharing Consortium has reached 300 000 unique hashes in the database - the result of approximately 250 000 visually distinct images and approximately 50 000 visually distinct videos having been added, with nearly ¾ classified as glorification of terrorist acts.[9] While the GIFCT has been for two consecutive years provided transparency reports outlining how many fingerprints exist and what categories they belong to, there is no independent third party oversight of the database, nor information around the frequency of the use of the database by individual companies. This makes the assessment of accuracy and efficacy of the tool impossible to assess.

Classification tools (machine learning)

Machine learning classifiers to flag content are also used by the largest online platforms. These tools are typically trained by supervised learning where they predict outcomes based on database of pre-labelled videos, text, sound or images. For example, most detection systems which are used to identify prohibited or illegal text are based on machine learning technique called natural language classification. These generally involve training language classifiers on a large corpus of texts, which have been manually annotated by human reviewers according to some operationalisation of a concept like offence, abuse, or hate speech[10]. Given that the underlying forms of prohibited speech or behaviour can change rapidly, these algorithms will require constant re-training as derogatory terms or phrases or levels of acceptability evolve[11].

There tools are used to surface a variety of types of content, for example Facebook has been using machine learning algorithms to try and surface content supporting certain groups, such as ISIS and al-Qaeda and is increasingly expanding their ability to automatize the flagging

[7] https://www.microsoft.com/en-us/photodna
[8] https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1060&context=research
[9] https://www.gifct.org/transparency/
[10] https://journals.sagepub.com/doi/full/10.1177/2053951719897945
[11] Use of AI in content moderation, Oxford consultants

and removal other groups and dangerous organisations. These tools, trained on a corpus of images and videos, create a predictive score that tries to estimate how likely a post is to violate Facebook's terrorist and violent content policies. Depending on that score, that post will be flagged for human moderation, with higher scores placing them higher in the queue for priority review by 'specialized reviewers'. In principle, such systems keeps a human in the loop for the final takedown decision unless the tool indicates with very high confidence that the post contains support for terrorism in which case it would be removed automatically[12]. The accuracy and confidence levels used by platforms for making such decisions are unknown.

While the efficacy and the accuracy of classifiers is improving, it is widely acknowledged that it is very difficult for predictive *classifiers* to make difficult, contextual decisions and that fully automated systems at scale are likely to make hundreds of incorrect decisions on a daily basis. This can be exemplified by the decisions taken by platforms during the COVID-19 pandemic, whereby vast numbers of human moderators were unable to work and companies needed to rely more on machine learning tools to identify and block prohibited content, which led to a surge in erroneous removals of content and a significant increase in appeals[13]. It is widely held belief among experts that in majority of circumstances, machine learning should be used as an assistive technology, for triage, scale, and improving human effectiveness and efficiency when making decisions about moderation[14].

Governance issues related to such tools are also related to the governance and accuracy of the training and testing data sets, and the impossibility to compare accuracy and performance across different tools due to inaccessibility of the systems.[15]

Costs of the tools

Costs incurred by online platforms for setting up voluntary filtering technologies vary depending on the type of files, type of illegal content monitored, and volumes of content uploaded on the platform. Exact data on costs is not easily obtainable and needs to consider development, deployment as well as maintenance cost. Costs for developing in house tools for monitoring and detection can be in the millions, whereas costs for connecting to a database of known content to moderate the platform can be significantly less and effectively absorbed by small platforms[16]. Further, there are several content detection tool on the market, which can be used for various purposes by different platforms or business, such as Audible Magic, Amazon Rekognition, Clarifai, NanoNets etc. The cost models there either per image, video or monthly subscriptions based on detection of a certain predetermined amount of videos or images. Ranging from $0.0008 to 0.0012 per image with lower per image costs above a million images detected. Video detection is priced $0.1 per minute of any archived video and $0.12 per minute for live streaming. Subscription based schemes can be from $19 per 10 000 pieces of content to $400 for 200 000 pieces of content[17].

[12] https://journals.sagepub.com/doi/full/10.1177/2053951719897945
[13] https://www.bbc.com/news/technology-53918584
[14] https://freedom-to-tinker.com/2018/03/21/artificial-intelligence-and-the-future-of-online-content-moderation/
[15] LNE, *ibid.,* forthcoming
[16] https://www.counterextremism.com/sites/default/files/TAT%20--%20JustPaste.it%20GIFCT%20hash-sharing%20Case%20study.pdf
[17] JRC report: Exploration of the EU User-Generated Content Moderation Market

Annex 12: Online advertising

This annex gives an overview of the different types of online advertising analysed for the purpose of the Impact Assessment and develops more in detail the legal, technical and economic evidence which underpins the arguments presented in the main report. In conclusion, it summarizes the main issues which are referred to more succinctly in the main report of the impact assessment.

1. SCOPE: ONLINE ADVERTISING

Online advertising, also referred to as digital advertising, is a type of advertising that uses the Internet to target and deliver marketing messages to customers. In many cases, consumers are offered services free of charge, which are cross-subsidized by the revenue from online advertising. In turn, the effectiveness of such advertising relies on the ability to match advertising to consumer interest and the consumer's likelihood to buy or to be interested by the content of the ad, more in general, based on the collected information – which is usually done by collecting data from users which enables effective targeting.
Online advertising covers different formats such as online display advertising; search online advertising – i.e. paid-for ranking of search results; classifieds (paying for listings/ranking) including paid listings online not on search engines but on other places such as on marketplaces or Online Travel Agencies – OTAs; and other formats -such as e.g. targeted e-mails with advertising. At the same time, online advertising is broader than the definition of 'commercial communications' currently covered by the E-Commerce Directive and other European legal acts, such as the UCPD or the AVMSD to the extent that the same advertising services are used for broader purposes than the commercial placement of products or services. Advertising is also used for promoting issues outside of the purely commercial sphere, such as issues of societal concern, humanitarian campaigns, official government information, political and electoral information, announcements by NGOs, etc.

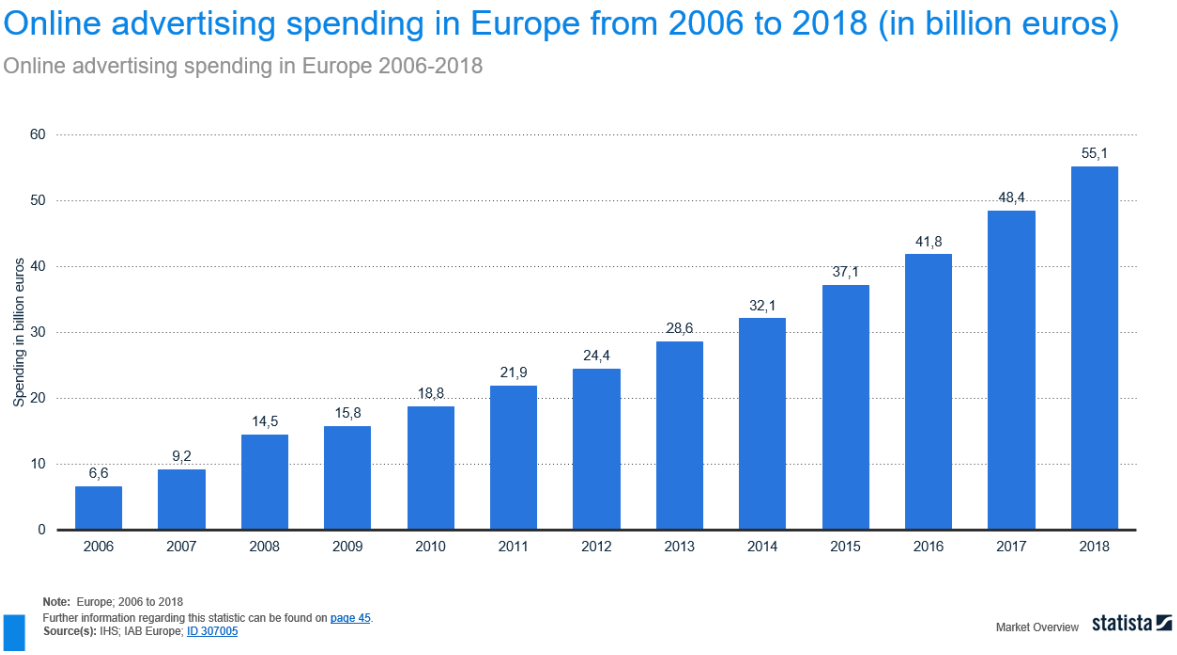
1.1. TRENDS IN ONLINE ADVERTISING

Since 2016, ad spending for online is higher than TV, and has the fastest growing rate. This makes advertising an important revenue vehicle for digital services, be it publishers, online ad intermediaries, or data brokers, as well as a core resource for all advertisers to reach consumers and citizens.

Ad spending for digital advertising has grown over 10 times since 2006, with 12.3% growth only in 2019 with a total of 64.8 bn EUR in Europe.[1] Forecasts for the COVID-19 crisis show a decrease of 5.5% for digital advertising (compared to 16,3% overall decline in ad spend, all media considered)[2]

Amongst digital advertising, search is persistently the biggest category of digital advertising (growth). At the same time, video, social and mobile are also very fast growing.

[1] Statista [link]
[2] https://advanced-television.com/2020/06/04/forecast-european-digital-ads-down-only-5-5-in-2020/



1.2. PROGRAMMATIC ADVERTISING

Online advertising is increasingly sold as 'programmatic' which can be described as the use of software and automation to buy and sell digital advertising. In contrast to traditional methods that include requests for proposals, tenders, quotes and negotiation - programmatic advertising uses algorithms to purchase display space automatically, using data to determine which spaces to buy, how much to pay and who to target.

Programmatic advertising allows advertisers to have more control over the quality of their campaigns and also enables them to tailor their creative content to individuals from specific demographics based on behavioral characteristics (behavioral advertising), or on the context in which the ads are served (contextual advertising).

The programmatic advertising ecosystem allows advertisers to purchase impressions in real-time from multiple publishers that are targeted at a particular audience segment, rather than a fixed number of impressions from one publisher at once.

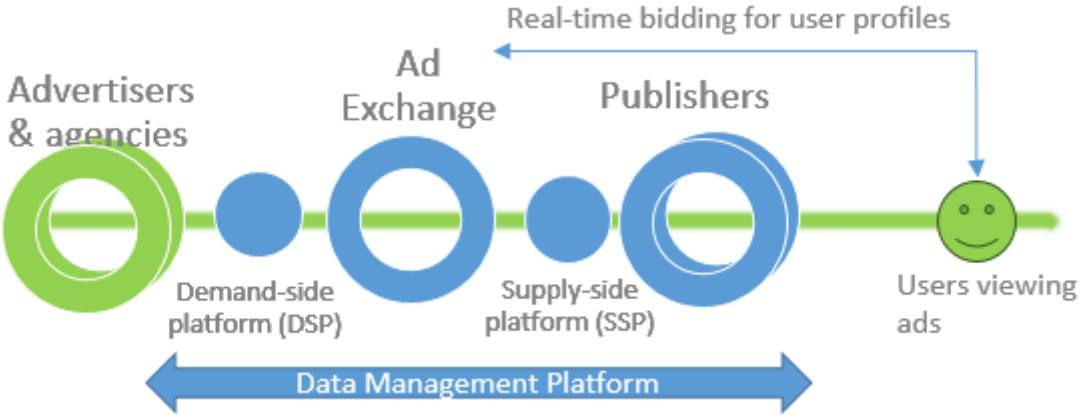
Models of programmatic advertising include:

Real-time bidding (RTB) is a subset of programmatic advertising that facilitates the buying and selling of ad inventories through an auction that occurs in the time it takes for a webpage to load. RTB occurs on a digital exchange (such as OpenRTB exchanges), which allows the transaction between the advertisers (demand side) and publishers (supply side) to occur in real-time and is relevant for search, display and video advertising content across desktops and mobile. There are several distinct functions in the programmatic advertising value chain, all of which intervene in real-time bidding models, but might be present, to a different extent, also in other advertising models:

- **The Publisher** in the context of the digital advertising ecosystem is a website or application that has a revenue stream through displaying adverts when visited by a user. The space that publishers make available to display adverts (ad space) is known as the publisher's inventory. By this broad definition, a publisher may be anything from a news outlet to a blog page, to a mobile app (in digital display advertising models), or a social media website (most often also handling itself the ad placing process).
- **The Supply-Side Platform (SSP)** helps publishers to manage/sell their inventory on a number of ad exchanges in an automated manner. It analyses the information of the user

and sends it to the exchange to maximize the price that publishers can receive for their impressions.

- **The Ad Exchange** acts as an online marketplace that allows advertisers (buyers) and publishers (sellers) to buy and sell online inventory. It does so by auctioning impressions to the highest bidder.
- **The Demand-Side Platform (DSP)** is the advertisers' equivalent of the supply side platform. It enables advertisers to store their adverts, or creatives, and allows them to track metrics and set the buying parameters for their campaigns. Here, the DSP uses algorithms to determine the 'value' of the user based on the target audience selected for the advertisers' campaign, before placing a bid in the auction for the impression if appropriate.
- **Advertisers**, both commercial and non-commercial, create advertisements to promote their goods and services. This is often done using an Ad Agency.



However, this model is the most complex chain for online advertising, and several alternatives exist, such as:

- **Private Marketplace (PMP)** - is an 'invitation only' RTB auction where one, or a select few, publishers invite select pre-approved buyers to bid on their inventory. Here, the DSP plugs directly into the source of the publisher's inventory, which eliminates the requirement for an exchange and the buyer is aware of exactly where the advert will run. Advertisers may use private marketplaces to obtain 'premium' placements in conjunction with bidding on the open ad exchange.
- **Programmatic Direct** - is a non-auction-based approach that allows advertisers to buy guaranteed ad impressions in advance from specific publisher sites. Programmatic direct arguably offers the value of increased transparency, which is a cited issue with RTB, and there are two forms of programmatic direct.
- **Programmatic Guaranteed** is a predetermined commitment from advertisers to buy a fixed amount of inventory for a fixed cost per thousand views or clicks (cost per mille – CPM) from specific publisher sites. Publishers may be more inclined to sell top-tier inventory like home-page takeover ads at a fixed price for a guaranteed number of impressions.
- **Preferred Deal** is a predetermined commitment to inventory price but not inventory amount between one buyer and one seller.

Thus, online advertising often does not involve two actors willing to buy and sell online advertising space; instead, it often involves a wide range of actors operating in a highly complex ecosystem.

2. LEGISLATIVE FRAMEWORK

2.1. THE E-COMMERCE DIRECTIVE

The E-Commerce Directive (ECD) contains several provisions that are of particular importance for the purpose of online advertising.
Article 6 of the ECD sets out the rules on commercial communications, setting a number of minimum information requirements which should be made available to consumers. According to this article, commercial communications should comply with the following obligations:

- the commercial communication should be clearly identifiable;
- the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
- promotional offers, such as discounts, premiums and gifts, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
- promotional competitions or games shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

Article 7 set certain rules on unsolicited commercial communications, setting information requirements and opt-out registries, and Article 8 specifically clarifies the freedom to advertise for regulated professions and sets certain conditions.
Further, all other provisions in the Directive equally apply to advertising services to the extent that they represent information society services: e.g. advertising agencies which do not provide their services at a distance through electronic means would typically not fall in scope of the ECD, but the Directive would govern the activity of referencing services[3] and other ad intermediaries
First, article 5 of the ECD covers all types of information society services, including those publishers hosting advertising, as well as ad intermediaries. It sets out the basic requirements on mandatory information society services need to provide, such as:

- the name of the service provider;
- the address of the service provider;
- the communication details of the service provider;
- information on the trade register in which the service provider is registered as well as the registration number;
- information on the relevant supervisory authority;
- information related to the regulated professions;
- the VAT identification number (when applicable);

Furthermore, when a service provider refers to prices, it has to provide further information on the price, for instance, the delivery costs and whether the price includes tax.

2.2. OTHER RULES

How advertising is placed: data
The **GDPR** is an important part in the legislative framework for online advertising. The GDPR applies to processing of personal data, and, since processing large amounts of (often) personal data is an important feature in the operation of online advertising, the GDPR applies. In the context of online advertising, the GDPR sets important requirements for the processing

[3] See, for instance, Google France case or eBay case of

of data, such as transparency and data minimization requirements, but also restrictions on certain types of processing, such as profiling and automated individual decision-making. Importantly, the GDPR provides for a right to object to digital marketing based on personal data (Article 21(2)) and, on many instances, it is understood that processing of personal data for targeted advertising requires the explicit consent of the data subject.[4]

The **e-Privacy Directive** further contains important consent and information requirements for non-essential cookies. This Directive is to be updated by the e-Privacy Regulation, which proposes to update these requirements.

Specific types of advertising: audiovisual

The recently amended AVMSD extends certain rules to video-sharing platforms. The Directive requires that these platforms take appropriate measures to protect minors from harmful content. In parallel, these platforms must take measures to protect the general public from content that incites to hatred or violence, or the dissemination of terrorist content, child pornographic content and racist and xenophobic content. National authorities are required to ensure that these platforms have adopted appropriate measures. These rules also extend to online advertisements on video-sharing platforms. The Directive also includes rules specific to audiovisual advertising:

- On audiovisual media services (which include on-demand services but do not include video-sharing platforms or other types of online platforms), it sets a series of requirements, such as the obligation to ensure that audiovisual commercial communications are readily recognizable as such, do not use subliminal techniques, do not prejudice human dignity, do not include or promote certain types of discrimination, do not encourage behavior prejudicial to health or safety or grossly prejudicial to the protection of the environment. It also prohibits audiovisual commercial communications for cigarettes, tobacco products or electronic cigarettes, and frames certain rules on alcohol advertising and medicinal products and treatment, as well as special rules concerning the protection of minors.
- Video-sharing platforms are bound by the same rules concerning audiovisual commercial communications 'marketed, sold or arranged by them' and to 'take appropriate measures' concerning those audiovisual commercial communications which are not, taking into account the limited control they exert.
- It requires video-sharing platforms to have a functionality for users who upload user-generated videos to declare whether such videos contain audiovisual commercial communications. Platforms should inform users where programmes and user-generated videos contain audiovisual commercial communications if the user has informed them through the provided functionality or if they otherwise have knowledge of this fact.
- It requires Member States to encourage co- and self-regulation through codes of conduct to reduce the exposure of children to audiovisual commercial communications on certain types of foods and beverages and make sure the ads do not emphasize their positive qualities.
- It clarifies that product placement should be allowed in all audiovisual media services and video-sharing platform services, subject to exceptions (e.g. news, consumer affairs programmes, religious or children's programmes).

Requirements for the content of the ad and consumer protection, other than the E-Commerce Directive

[4] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en

A strong consumer protection framework regulates the content of online advertising. Most importantly, the Unfair Commercial Practices Directive (UCPD) prohibits unfair business-to-consumer commercial practices, including misleading and aggressive practices occurring in information society services. For example, the UCPD forbids describing a product as free when it is in fact not free or creating the false impression that the consumer will win a prize when there is no prize. As part of the New Deal for Consumers, the UCPD was amended in 2019 to include an obligation to clearly disclose to consumers the criteria used to rank offers as well as if ranking results are based on payments received.
The Misleading and Comparative Advertising Directive prohibits advertising directed at businesses that is deceptive and is likely to injure a competitor. Furthermore, it lays down the conditions under which comparative advertising directed at both consumers and businesses is permitted. This Directive also applies in the context of online advertising.

Other rules regulating specific types of content also apply to the content of ads, such as those concerning illegal hate speech, or copyright and trademark rules.

A series of rules apply to marketing and advertising for specific products, such as:

- Directive 2001/83/EC on the Community code relating to medicinal products for human use[5] establishes the obligation for a marketing authorization prior to advertising for medicinal products. It sets a series of requirements for the content of the ads and prohibits certain practices, prohibits advertising to the general public medicine available by prescription only and sets a set of minimum information for the advertising, including the need to identify the message as an advertisement and clearly identify the product as a medicinal product, as well as requirements on disclosing the active substances and the name of the product, information on the correct use and an invitation to read carefully the instructions.
- Directive 2003/33/EC of the European Parliament and of the Council of 26 May 2003 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products (OJ L 152, 20.6.2003, p. 16).
- Directive 2014/40/EU of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC (OJ L 127, 29.4.2014, p. 1)

3. EMERGING LEGAL FRAGMENTATION AT NATIONAL LEVEL

This section is a preliminary summary publicly available information; it does not represent a full review of legislation in Member States.

3.1. GENERAL LAWS

Most member states (e.g. Sweden[6], Malta[7], Denmark[8], Poland[9], Portugal[10], Luxembourg[11], Italy,[12] Greece[13], Czech Republic[14], Germany[15], Finland, The Netherlands[16]) do not have a

[5] https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-1/dir_2001_83_consol_2012/dir_2001_83_cons_2012_en.pdf

[6] https://www.lexology.com/library/detail.aspx?g=5a90b740-bea9-4e49-9cdb-25a0cb29fc2b

separate or particular law for online advertising, but that their rules (which are mainly implementations of EU legislation from the consumer acquis and the ECD) apply to advertising in general; thus both to offline and online advertising.

Some Member States (Hungary, Ireland, France, Austria) have specific regulations in place on online advertising, some of them including requirements which are extraterritorial and/or diverging.

3.1.1. FRANCE

Law 93-122 of 29 January 1993 on prevention of corruption and on transparency of economy established several transparency procedures in the advertising sector. For example, it puts a requirement on sellers of ad inventory to invoice advertisers directly and to account them in the month following about the conditions in which the service was performed. Since 2015, this law also applies to online advertising, as it covers any medium connected to the internet such as computers, tablets, mobile phones, televisions and digital panels.

Moreover, in February 2017, Decree 2017-159[17] established two legal frameworks for reporting obligations. One on them is a general legal framework, and the other is especially for programmatic sales. According to this law, sellers of ad space now have to share information on the cumulative and unit cost of the ad space sold. In the general framework, this information must be shared automatically and publishers also have to communicate the date of diffusion of the ads and diffusion slots. In the framework for programmatic sales, the information on costs is shared on request. Furthermore, publisher shall share information on the effective execution and performance of the ad placement, on the technical quality of the service, on the protection of the advertiser reputation (brand safety) and on any commitments taken as part of charters of good practices.[18] According to Kadar, Wood and Shalit "*sellers of advertising space established in France – **as well as those established in another EU or EEA***

---

[7] https://www.lexology.com/library/detail.aspx?g=82248bb6-7459-4b9f-bc57-29420db79a68#:~:text=Maltese%20law%20does%20not%20specifically%20regulate%20advertising%20on%20the%20internet.&text=The%20first%20of%20these%20instruments,and%20comparative%20advertising%2C%20among%20others.

[8] https://content.next.westlaw.com/Document/I16f43ed37bcb11e598dc8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1,

[9] https://www.lexology.com/library/detail.aspx?g=eb8e59ee-c06f-4da1-b465-1a6b579542b6#:~:text=In%20Poland%20there%20are%20no%20specific%20legal%20rules%20on%20digital%20advertising.&text=of%20third%20parties.-,The%20Act%20on%20Providing%20Electronic%20Services%20and%20the%20Telecommunications%20Law,marketing%20calls%20and%20text%20messages.

[10] https://www.cuatrecasas.com/publications/the_international_comparative_legal_guide_to_telecoms_media_internet_laws_regulations_2018_portugal.html

[11] https://www.lexology.com/library/detail.aspx?g=75fcbee8-de8f-4597-bcfd-fee6eea83467

[12] https://www.lexology.com/library/detail.aspx?g=54d60deb-6afd-4e25-8efd-41de98c992bd

[13] https://www.ballas-pelecanos.com/up/files/International-Advertising-Law2014.pdf

[14] https://uk.practicallaw.thomsonreuters.com/w-017-1857?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a424230

[15] https://www.lexology.com/library/detail.aspx?g=5558095c-ab16-4e92-bc9a-65f789e7a132

[16] Instituut voor Informatierecht IViR UVA 'De verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties', Tussenrapportage Oktober 2019. file:///C:/Users/jacolau/Downloads/rapport-instituut-voor-informatierecht-ivir-faculteit-der-rechtsgeleerdheid%20(1).pdf

[17] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000034024418&categorieLien=id

[18] Study on 'Support to the Observatory for the Online Platform Economy', Analytical paper #3. P. 56

***Member State**, insofar they are not subject to similar obligations, are now subject to a reporting obligation towards advertisers on the global campaign price and on the unitary price of each advertising space, including the date and place of diffusion of the advertisements*."[19] From this quote, it seems that the scope of the French law is thus quite broad, as it applies also to other EU or EEA Member States.

3.1.2. HUNGARY

Hungary adopted in 2015 the 'Bonus Act' (Act LXXII of 2015 on Establishing the Central Budget of Hungary for Year 2016), which amended the 2008 law on commercial advertising activities (Advertisement Act). The main provisions of this Act are putting obligations on advertising agencies. First, the act sets out mandatory provisions regarding the advertising agency agreements. Second, these agreements must be concluded in writing. Third, it enables advertising agencies to conclude agreements on the publishing of advertisements with the publishers, in name of and on behalf of the advertisers. Fourth, it obliges advertisement publishers to notify the advertisers about the circumstances of publishing the advertisement and modifications thereof. And fifth, it requires publishes to issue invoices for their services to the name of the person they contract with, either the advertiser, or the agency. Such invoices must be indicate all applied discounts and be paid within 30 days.

Furthermore, the Act states that advertising agencies are only permitted to accept the fee for the agency activity and the discount received from the publisher or the sales house acting on the publisher's behalf. Also, agency fees paid by the advertisers are fixed at 15% of the fee for publishing the advertisements. Any other financial gain may not be accepted by an agency. Discounts are thus allowed under the Bonus Act, but they must be passed along to the advertisers to make sure that the advertiser benefits from it.[20]

As to scope, according to CMS *"The scope of the Advertisement Act extends to advertising activities carried out in the territory of Hungary, this, however, does not exclude extraterritorial application of the regulations herein described, e.g. in case of foreign contracting parties."*

3.1.3. IRELAND

In **Ireland**, regulating online advertising is also an important topic within the political debate. First, in December 2017, there was a proposal for an 'Act to provide for transparency in the disclosure of information in online political advertising and to provide for related matters' to the House of the Oireachtas. This proposal however lapsed in January 2020 with the dissolution of the Lower and Upper House.[21]
According to a governmental press release of 5 November 2019[22], the government brought a new law to regulate online political advertising during elections. According to the press release, '*The Government today approved a proposal to Regulate Transparency of Online Political Advertising. The detailed Proposal is outlined in 'Progress Report of the Interdepartmental Group on the Security of Ireland's Electoral Process and Disinformation*

[19] Lexology: see https://www.lexology.com/library/detail.aspx?g=77dcccfe-3173-4bf8-9412-a85c1a1105e7
[20] CMS, see: https://www.cms-lawnow.com/ealerts/2015/06/hungary-regulates-advertising-agency-bonuses#:~:text=The%20Hungarian%20Parliament%20has%20recently,and%20advertisement%20spot%20sales%20activities.
[21] https://www.oireachtas.ie/en/bills/bill/2017/150/?tab=bill-text
[22] https://www.gov.ie/en/press-release/9b96ef-proposal-to-regulate-transparency-of-online-political-advertising/

(IDG)'.[23] The proposal came after the Irish government opened a public consultation and Open Policy Forum on the regulation of online political advertising in Ireland from 21 September to 19 October 2018. The consultation got 15 responses.[24]

The overarching policy objectives of the Proposal are threefold: 1) to protect the integrity of elections and to ensure that they are free and fair, not captured by a narrow range of interests; 2) to respect the fundamental right to freedom of expression and the value of political advertising and its importance to democratic and electoral processes while at the same time ensuring that the regulation will meet requirements of lawfulness, necessity and proportionality; 3) to respect the role of the internet in the public sphere of political discourse and to ensure that the public has access to legitimate information in order to make autonomous voting decisions.[25] Hereunder a summary of the different provisions of the law will be discussed.

Scope

As to the scope of what constitutes a political ad, the proposal seeks alignment with the definition of 'political purposes' as defined under their Electoral Act.

The legislation would apply to the following groups: online platforms (either as sellers or intermediaries of political advertising), and buyers of political adverts. Furthermore, "*the obligation would be placed on the seller to determine that an advert falls under the scope of the regulation.*"[26] The seller should ascertain: 1) the content of the advertisement i.e. whether it relates to an election campaign, referendum proposal or is promoting an electoral candidate or political party; 2) whether a micro-targeting algorithm has been used if the content is political; 3) the address of the advertiser.

Information requirements

Online paid-for political advertisements should be labelled as such and clearly display the following information:

- Name and address (postal address, web or email address, i.e. reliable contact information) of person or entity who paid for the online political advertising
- Confirm if targeting was applied, and description of target audience/criteria applied and if the target audience contains 'Look alike' target lists;
- Cost of the advertising - requirement should apply to both content creation and distribution;
- Engagement metrics (e.g. no of impressions that the advert would desirably reach);
- Time period for the running of the advert;
- Information should be disclosed in real time.

Verification

Apart from the seller requiring to verify the identity and address etc. of the buyer, the buyer is required to provide evidence of their identity and address to the seller and ensure that the information they provide is truthful and accurate. Furthermore, the buyer is required to provide the seller with the information he needs such as the cost of the advertising content creation.

---

[23] https://assets.gov.ie/39188/8c7b6bc1d0d046be915963abfe427e90.pdf

[24] https://www.gov.ie/en/consultation/1217012109-regulation-of-online-political-advertising-in-ireland/

[25] See page 10 of Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation Progress Report

[26] Idem, P. 12

Compliance/Monitoring
Proposed is joint liability on both seller and buyer of the advertisement to comply with the information requirements. The forthcoming Electoral Commission will have a monitoring and oversight role for the regulation.

Access to information
Sellers must hold publicly accessible repositories of advertisements which include information about the source, source location, content production, costs and details regarding distributions such as channels, target audience and use of data.

Time Period for which Regulations would apply
Importantly, the Regulation will ***only*** apply during and before an electoral period. This will be either a) 30 days before the poll date or b) from the date the polling day order for the election has been completed.

Penalties
According to the proposal, the penalties approach for allowing the purchase and publication of an online political advert without contain he necessary information (on the seller side) or providing false or misleading information (on the buyer side) *could* include:

- Summary conviction, in accordance with the Fines Act 2010, can result in a Class A fine of €5,000 or imprisonment for the term not exceeding 12 months or both.
- Conviction on indictment can result in a term of imprisonment of up to five years or a fine, or both.

The proposal is seen as an interim measure until a Statutory Electoral Commission (which will oversee a wider reform of electoral processes) will be established.

3.1.4. AUSTRIA

On 10 October 2019, the upper house of the Austrian Parliament ('Bundesrat') approved a bill on the new digital advertising tax package ('Digitalsteuerpaket'). The bill was on 19 September 2019 approved by the lower house of the Austrian Parliament ('Nationalrat'*)*. According to the Austrian government "*The international tax system still prevailing at the moment does not take sufficient account of current developments, especially in the field of digital economy. It is based on physical presence, whereas companies with novel digital business models often achieve high added value on a market on which they have no business premises or headquarters. Distortions of competition are widespread. The OECD and the EU are working hard on solutions, but none are available yet."*[27]

Under this new tax bill, a new tax of 5% on revenue derived from online advertising was introduced and went into force on the 1st of January 2020. The assessment base for the digital tax is the remuneration that the online advertiser receives from a customer. This is reduced by expenditures on intermediate inputs by other online advertisers that are not part of the tax debtor's multinational group of companies. The tax rate amounts to 5 percent of the assessment base. The bill is targeting Austrian companies because the services provided must have a domestic nexus. According to article 1(1) online advertising services are subject to the

[27] https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html

law to the extent that they are provided for consideration by online advertising providers in Austria. An online advertising service is deemed to be provided domestically if it is received on a user's device with a domestic IP address and if it is (also) addressed to domestic users according to its content and design. Furthermore, the law defines 'online advertisers' as companies that:

A. Provide online advertising services, or contribute to the provision of online advertising services, for remuneration and that,
B. Within one business year, generate:
    a. A worldwide turnover of at least €750 million, and
    b. A turnover in Austria of at least €25 million from the provision of online advertising services.[28]

3.2. REGULATIONS ON SPECIFIC 'FORMS' OF ADVERTISING

3.2.1. 'INFLUENCER' ADVERTISING

Influencer marketing/advertising is the practice in which bloggers and other social media channels take advantage of promoting goods and services on their own platform. This concept is mainly problematic because more or less hidden advertising messages can be transmitted and lines are often blurred, as it is unclear whether products are advertised or whether it is just an influencers' own favourite product. Belgium, France, Germany, Ireland, Sweden, the Netherlands, Austria have already put in place (self-regulating) guidelines on influencer advertising.[29] Also the Nordic Consumer Ombudsmen, a cooperation set-up between the Nordic countries, reached a joint position statement on social media advertising in 2016. He stated that an advertorial post is sufficiently labelled if it is clearly marked with the word 'advertisement' in the introduction. A text like 'this is in collaboration with…' is therefore not considered sufficient.[30] Apart from self-regulating codes or guidelines, specific adopted laws or legislative proposals on influencer advertising in Member States were however not found by this research. For example in the Netherlands, the Civil Law Code states that from any advertisement it must be clear that it is an advertisement, whether this is online or offline. This therefore also applies to influencer advertising. The Dutch Advertising Code (Stichting Reclame Code) drafted extra guidelines on influencer advertising, to clarify that the rules of the Civil Law Code also apply to influencers.

3.2.2. ADVERTISING FOR ONLINE GAMBLING

Since and because of the COVID pandemic, Spain has adopted strict new restrictions on online gaming and gambling advertising.[31] Online advertising for online gaming or gambling services is in Malta governed by the Gaming Comercial Comunications Regulations that came in force in August 2018.[32] Also in Lithuania a new advertising law for gambling was adopted in 2020, which applies to all forms of gambling advertising, and thus also to offline gambling

[28] https://www.bmf.gv.at/en/topics/taxation/digital-tax-act.html; https://perma.cc/4H7G-CTUA
[29] Reale, M., 'Digital Markets, Bloggers, and Trendsetters: The New World of Advertising Law' in *MDPI,* 3 September 2019, P. 9.
[30] https://www.lexology.com/library/detail.aspx?g=5a90b740-bea9-4e49-9cdb-25a0cb29fc2b
[31] https://www.igamingbusiness.com/news/spain-restricts-igaming-advertising-amid-covid-19-pandemic
[32] https://www.lexology.com/library/detail.aspx?g=82248bb6-7459-4b9f-bc57-29420db79a68#:~:text=Maltese%20law%20does%20not%20specifically%20regulate%20advertising%20on%20the%20internet.&text=The%20first%20of%20these%20instruments,and%20comparative%20advertising%2C%20among%20others.

advertising.[33] Also in Belgium, in October 2018 a new Royal Decree with restrictions on online gambling advertising was adopted.[34] Italy and Latvia also have a total or almost total ban on online gambling advertisements.[35]

4. EXAMPLES OF ONGOING SELF-REGULATORY MECHANISMS FOR ONLINE ADVERTISING

4.1. ADVERTISING IN EU-LEVEL SELF-REGULATORY ACTIONS

The Memorandum of Understanding on Online Advertising and Intellectual Property Rights aims to facilitate cooperation between signatories – including advertising associations, ad exchanges and rights owners – and minimize the inclusion of counterfeit goods and copyright-infringing goods in online advertising. According to the Memorandum, this will, in turn, help prevent websites with these types of illegal goods thrive online.
The EU Code of Conduct on Countering Illegal Hate Speech Online aims to prevent the spread of illegal hate speech online and promote freedom of speech online. Nine IT companies, both European and non-European, signed up to the code. In the code the IT companies commit to have rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported to violate these standards. Furthermore, the companies commit to review the majority of notified illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary.

The Code of Conduct on Disinformation aims to bring online platforms and the advertising industry together to tackle disinformation. Signatories of the Code of Conduct on Disinformation have committed to adopting policies and processes to disrupt online advertising and monetization incentives for the spread of disinformation. The Code provides examples of actions that can be taken by signatories in order to live up to the commitments in the Code. The Code further contains an annex with current best practices from signatories, these includes for instance Facebook's False News Policy, Google's Annual Bad Ads Report and Twitter's Ads Policy.

[33] [33] https://calvinayre.com/2020/02/12/business/lithuania-passes-legislation-to-put-warnings-on-gambling-ads/
[34] https://www.cms-lawnow.com/ealerts/2018/12/belgium-tightens-legislation-on-online-gambling-advertising-for-better-or-for-worse
[35] https://www.egba.eu/uploads/2018/12/181206-Consumer-Protection-in-EU-Online-Gambling-EBGA-Report-December-2018.pdf

Annex 13: Overview of the European Parliament's own initiative reports on the Digital Services Act

European Parliament has invested considerable political resources to discuss and put forward views on the upcoming Digital Services Act, with the preparation of two legislative, own-initiative reports. These are a report on the 'Digital Services Act – Improving the functioning of the Single Market' prepared by the Internal Market and Consumer Protection Committee (IMCO) (rapporteur Alex Agius Saliba (S&D, MT) and one on the 'Digital Services Act: adapting commercial and civil law rules for commercial entities operating online', by the Legal Affairs Committee (JURI) (rapporteur Tiemo Wölken (S&D, DE). A non-legislative own-initiative report titled 'Digital Services Act and fundamental rights issues posed' has also been prepared by the Civil Liberties, Justice and Home Affairs Committee (LIBE). The Parliament commissioned studies to underpin its analysis in preparation of these reports.[1]

The Culture and Education Committee (CULT), the Transport and Tourism Committee (TRAN), the Legal Affairs Committee (JURI) and the Civil Liberties, Justice and Home Affairs Committee (LIBE) provided Opinions on the IMCO report. The Internal Market and Consumer Protection Committee (IMCO) and CULT gave Opinions to the JURI report. Both reports were adopted in the plenary of the Parliament on 20 October 2020, as resolutions based on **Article 225** of the Treaty on the Functioning of the European Union, requesting the Commission to submit legislative proposals.

The Commission analysed the reports while conducting the impact assessments for the Digital Services Act as well as for the Digital Markets Act. The table below maps the main areas and sections in the impact assessment reports where the calls from the European Parliament are addressed.

Reports	Measure	How does the impact assessment report address it?
Scope		
IMCO JURI	The scope of the initiative should cover 3rd country providers	The impact assessment notes the challenges related to the accessibility of services in the Union offered from providers established in third countries, which are currently not bound by the E-Commerce Directive (section 2.2.1) and acknowledges that all categories of stakeholders in their response to the open public consultation are of the view that the initiative should cover third country providers (section 2.2.2). All of the proposed options include an obligation to appoint a legal representative in the Union for those services with have a significant number of users in one or several Member States (section 5.2)
IMCO JURI LIBE	Focus on illegal content ensuring a differentiation with harmful content. The	The impact assessment analyses the serious risks and harms brought by digital services, differentiating between illegal content and other, emerging societal and systemic risks (section 2.2.1). All of the proposed

[1] See https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652712/IPOL_BRI(2020)652712_EN.pdf and https://www.europarl.europa.eu/RegData/etudes/STUD/2020/654180/EPRS_STU(2020)654180_EN.pdf

	IMCO report calling for the principle "*what is illegal offline is also illegal online*"	options include clear measures against illegal content, including a harmonised notice & action system. The preferred option further harmonises conditions for court and administrative orders for removal of illegal content (Section 5.2) and foresees obligations on very large platforms to assess the potential systemic risks on their platforms.
Country of origin and governance		
IMCO LIBE	Calls to strengthen the **country of origin principle**	The importance of the country of origin principle was emphasised by most of the respondents to the open public consultation. The evaluation of the E-Commerce Directive and all other available evidence shows that that the single market principle has been instrumental for the development of digital services in Europe. As a result, changes to the single market principle set in the E-Commerce Directive and the requirement for the country of establishment to supervise services were discarded at an early stage (Section 5.3).
IMCO JURI	IMCO report notes the need for increased cooperation between Member States in order to improve the regulatory oversight of digital services and to achieve effective law enforcement in cross-border cases. Whereas JURI recommends that the application of the Digital Services Act should be monitored at European level, through a European agency or body, ensuring a harmonised approach to its implementation across the Union, including reviewing compliance with the standards laid down for content management and the monitoring of algorithms for the purpose of content	The challenges around the current cooperation mechanism among Member States in addressing a complex set of issues modern digital services pose in terms of supervision is analysed in section 2.3.6 of the impact assessment report. The appropriate supervision of digital services and cooperation between authorities is a key objective which the proposed options have been designed to fulfil (section 4.2.4). All the options include measures to enhance cross-border cooperation, with the third option presenting two sub-options for establishing an EU level governance mechanism (Section 5.2). The preferred option retains an advisory committee formed of representatives of digital services coordinators from Member States, as well as direct enforcement by the Commission under certain conditions, as it is assessed to be the most efficient option at this point in time, in part in terms of streamlining costs, and, more importantly, the urgency of having the system ready and a swift application and supervision of the new obligations (Section 6).

	management.	
Liability		
IMCO JURI LIBE	**Maintaining the safeguards of the e-Commerce Directive** as regards the liability regime for user-generated content and the general monitoring prohibition	Fundamental changes to the approach on the **liability regime for online intermediaries** were discarded at an early stage (section 5.3). All the options maintain the liability regime with the preferred option offering targeted clarifications (section 5.3) and they all maintain the prohibition of general monitoring obligations or obligations to seek facts and circumstances for illegal activities.
IMCO JURI	IMCO report notes that **voluntary measures** to address illegal content should not lead to providers being considered as having an active role, solely on the basis of those measures and considers that clarifications on the active/passive nature of the concerned services are required. JURI report considers that mechanisms voluntarily employed by platforms must not lead to ex-ante control measures based on **automated tools** or upload-filtering of content.	The impact assessment analyses the uncertainties linked to the liability regime for online intermediaries, (section 2.2.3 and 2.3.5). Some intermediaries, academic institutions, and civil society organizations stated that the current liability regime creates disincentives to act, and called for clarification to stimulate voluntarily measures by service providers. The legal uncertainties leading to such disincentives are seen as counter-productive in the fight against illegal activities online. Start-ups strongly supported further legal clarifications to remove such disincentives and stressed that this would be a very important safeguard for smaller online platforms (stakeholder views box section 5.2) Options 2 and 3, include measures to clarify the liability of hosting service providers with regard to voluntary action (Section 5.2).
Obligations on service providers		
IMCO LIBE JURI	Minimum standards for service providers to adopt fair, accessible, non-discriminatory and transparent contract terms and general conditions and those to be made available in a **clear, transparent, fair** and in an easy and accessible manner to users	All the policy options include an obligation to clearly state in their terms of service any restrictions they may apply in the use of their service, and to enforce these restrictions with due account to fundamental rights (section 5.2)

IMCO JURI LIBE	Protection of fundamental rights and inclusion of appropriate safeguards to avoid removal of content which is not illegal	The current problems and drivers around insufficient protection of fundamental rights are analysed in the impact assessment (Sections 2.2.1, 2.3.1 and 2.3.2). Maintaining a safe online environment while protecting fundamental rights and freedom of expression in particular are key objectives in the design of the options (Section 4.2). All the options include numerous safeguards in line with these objectives (Section 5.2) to protect legitimate expression and for businesses to develop in observance of the rights and values of a democratic society. The impact of the option on the fundamental rights concerns is further detailed in the analysis in section 6.4.1.
IMCO JURI LIBE	No obligation to use fully automated tools which would lead ex-ante general monitoring	While the majority of stakeholders found it important to remove disincentives for voluntary action, also to be able to deploy automated tools, stakeholders equally warned against monitoring requirements and obligations to use of automated tools for tackling illegal or harmful content. **None of the options include an obligation to use automated tools** (Section. 5.2.)
IMCO JURI	Harmonised, transparent and effective **notice-and-action mechanism**, with accompanying **counter-notices**, **complaint mechanisms**, **measures against abusive behaviours** by users, and judicial review procedures. Independent out-of-court dispute settlement mechanisms to be put in place.	As described in section 5.2, all the options include an obligation to establish and maintain an easy to use mechanism for notifying any illegal content, goods or services offered through online platforms as well as other hosting services in accordance with harmonised standards. This is coupled with an obligation to inform users if their content is removed, including when the removal follows an assessment against the terms of service of the company, as well as specific actions around repeat offenders. The information obligations are coupled with an obligation to put in place **an accessible and effective complaint and redress mechanism** supported by the platform and the **availability of an external out of court dispute mechanisms.**
IMCO JURI LIBE	Transparency and accountability requirements regarding **automated-decision making** processes, including independent auditing of content moderation systems and annual reports.	All options include strong transparency obligations and accountability requirements on content moderation practices, including regular transparency reports. The preferred option sets a particularly high bar including specific requirements on transparency towards users on recommender systems and advertising and enhanced responsibilities for very large online platforms to asses and mitigate systemic risk, including reporting and data access to researchers and regulators as well as independent systems audits. This also includes risk assessment and mitigation measures, as

		well as annual audits with regard to content moderation systems of very large platforms, including when they use automated tools. Data requests from the supervisory authorities also concern the supervision of such systems. (section 5.2)
IMCO JURI	Obligations on platforms to evaluate the risk that their content management policies of legal content pose to society, in particular with regard to their impact on fundamental rights.	Section 5.2 outlines the measures in Option 3 (the preferred option) which include a set of enhanced obligations on very large online platforms which are designed proportionately to the systemic impacts and risks these large platforms represent for European society and the business environment, as well as to their capacities. This includes obligations to maintain a risk management system, including annual risk assessments for determining how the design of their service, including their algorithmic processes, as well as the use (and misuse) of their service contribute or amplify the most societal risks. This is combined with the obligation to carry out independent audits of the systems.
IMCO JURI	Maintaining the core principles of online anonymity.	None of the requirements in the regulation affect the core principle of anonymity. While all the options include an obligation on online platforms that facilitate transactions between traders and consumers by collecting identification information, this is strictly limited to traders and this requirement does not apply to regular users (Section 5.3).
Advertising		
JURI IMCO	Strict rules on transparency around **advertising and targeted advertising**, **user's empowerment** vis-à-vis targeted ads and accountability and fairness criteria for algorithms used in advertising, including access to advertising data and allowing for external regulatory audits.	Options 2 and 3 include enhanced transparency and reporting obligations with regard to online advertising. These would include modernised transparency obligations covering **all types of advertising** (all ads placed on online platforms, not just commercial communications, but also e.g. issues-based or political advertising). The preferred option includes measures such as enhanced information to users distinguishing the ad from 'organic' content, information about who has placed the ad and information on why they are seeing the ad (depending on the type of advertising –e.g. targeted, contextual - and, if applicable, targeting information). Furthermore, it would ensure that for very large platforms, there are data access possibilities for researchers and regulators through ad repositories and, as necessary, specific access requests, as well as independent systems audits.

Online Marketplaces		
IMCO	Specific rules for **online marketplaces**, including enhanced information obligations towards their users, accountability, cooperation with authorities, and know-your-business customer scheme. Invitation to the Commission to consider a specific liability regime for online marketplaces under certain circumstances;	The important intermediary role of marketplaces and the emerging challenges in the current online space are assessed in the problem and drivers section of the impact assessment (2.2.1 and 2.3.1) Accordingly, all the options include an obligation on online platforms that facilitate transactions between traders and consumers to collect identification information from traders to dissuade rogue traders from reaching consumers (Section 5.3)
Market power		
IMCO JURI	Clarity on the definition of **platforms with significant market power**, which should have different obligations than smaller platforms, such as with regard to interoperability, interconnectivity, and portability of data	The Commission has analysed these issues in depth in the impact assessment accompanying the proposed Digital Markets Act, which will set clearer and stronger rules applicable to some systemic digital platforms that act as gatekeepers for their business users and customers. Such rules will complement the existing regulatory framework, in particular Regulation 2019/1150/EU and EU competition rules, with clearly targeted obligations on systemic platforms that will be identified based on a clearly defined criteria.
Smart contracts		
JURI IMCO	Calls for measures on **smart contracts**, to enable the uptake of the blockchain technology and smart contracts across the single market and ensure their balanced use;	The Commission analysed the emerging opportunities and potential bottlenecks for the conclusion of smart contracts, in light of the evaluation of the E-Commerce Directive. As regards the ground rules for the cross-border conclusion of contracts, the Commission interprets the core rules set in particular in Article 9 of the E-Commerce Directive as fully applicable to smart contracts, regardless of the technological solutions adopted for the conclusion of the electronic contracts.

		The Commission continues to work towards promoting the development and deployment of blockchain technology and smart contracts. The Commission's Data Strategy already highlights the potential benefits of the blockchain in the context of data management empowering individuals to exercise their rights, provided blockchain is developed in compliance with data protection rules.