DIGITALEUROPE

MAY 2020

DIGITALEUROPE contribution to TRIS notification 2020/65/D (German proposed law on combating right-wing extremism and hate crime)

Executive Summary

In this paper, DIGITALEUROPE provides comments on the proposed German Draft law on combating right-wing extremism and hate crime, adopted by the German government on 19 February 2019 and now being reviewed by the European Commission under the framework of the notification procedure. The draft law notified concerns 'rules on services' in the meaning of Article 1(1) (e) (i) of the Directive.

DIGITALEUROPE's membership agrees with the overall ambition to fight against the dissemination of hate speech and hateful content online. However, we express several concerns with the feasibility and efficacy of the proposal, as well as with its potential disruption to the EU's Digital Single Market.

On several fronts, the proposed German law contains issues which are disproportionate and do not balance the rights of all stakeholders, not in the least that of the freedom of expression of users and right to do business, which may cause further legal uncertainty and confusion, or which run counter to established EU law. As an overall point, DIGITALEUROPE would also recommend that regulation to tackle digital policy issues of this nature takes into account the overall EU-wide debate and leads to a harmonized approach, to avoid further fragmentation of the digital single market. In that context, we recommend the German legislator to await proposals from the European Commission on the announced Digital Services Act.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Compatibility with the e-Commerce Directive

In addition to tightening national criminal law, the draft law expands compliance obligations for social network providers under the German Network Enforcement Act (Netzwerkdurchsetzungsgesetz) with the aim of more effective criminal prosecution for hate crime. The providers are required to forward content reported to them and the IP address of the user to the Federal Criminal Police Office. The draft law establishes the competent public prosecutor's office in order to enable effective prosecution of hate speech. The forwarding obligation is limited to certain punishable offences. The obligation is punishable by fine. The draft establishes the Federal Office of Justice as the competent administrative authority.

The social networks under the scope of the notified draft constitute information society services within the meaning of Article 1 and 2 of the e-Commerce Directive. The notified new obligations fall within the field of the e-Commerce Directive as defined in its Article 2 (h), as they concern the obligations for social networks as regards illegal content provided by third parties. These obligations would apply to social networks meeting a threshold of two million registered users in Germany, regardless of whether they are established in Germany, which means that social networks established in other Member States are covered as well, in as far as they provide relevant services and exceed the user threshold for the German territory.

In DIGITALEUROPE's view, the new obligations set out in the draft law constitute an interference with the cross-border provision of information society services, questioning the reach of Article 3 (2) of the e-Commerce Directive, in as much as they apply to providers of social networks established in other Member States. This is the case, in particular, for especially burdensome obligations for social networks, such as the forwarding obligation.

The German authorities argue that it is compatible with EU law because Article 3(4)(a) E-Commerce Directive 'allows Member States, under certain conditions, to take appropriate measures to protect public order, in particular the prevention, investigation and prosecution of criminal offences, including the protection of minors and the fight against racial agitation, gender, belief or nationality, as well as violations of human dignity against service providers from other Member States'. However, Article 3(4) (a) also contains several other requirements to be fulfilled to derogate from the prohibition to restrict the freedom to provide information society services, notably that any derogation has to be targeted as well as proportionate to the objective pursued. As regards the targeted nature of the measures, DIGITALEUROPE is not convinced that this requirement is met since the notified draft applies generally to any social network. A targeted measure which fulfils the requirement of the Directive could be a proceeding against a specific social network (judicial or administrative), for example. As regards proportionality,

DIGITALEUROPE has doubts as well: It should be assessed whether less restrictive means to obtain a similar result could be envisaged.

The German authorities also argue in their justification for the draft law that it is compatible with EU law because Article 15(2) E-Commerce Directive allows Member States to 'require information society service providers to notify them of suspected illegal activity or information'. However, according to that Article, 'obligations to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements' is explicitly restricted to communication of information to the authorities at the request of those authorities. The proposed forwarding obligation, however, does not involve a request by the authorities but requires social networks to communicate the information (in form of an IP address) proactively without a dedicated request.

When adopting measures on a matter under Article 15 e-Commerce Directive, national authorities and courts must strike a fair balance between the various, conflicting fundamental rights that are often at stake in this connection, including freedom of expression, right to protection of privacy and personal data, and freedom to conduct a business. Already the current Network Enforcement Act with its comprehensive catalogue of obligations, short time periods for deletion of content and high threat of fines gave reason to worry about chilling effects on freedom of expression. This is all the more serious now that service providers are to be obliged to forward identifying information about users to the German authorities on large scale.

From the above considerations, DIGITALEUROPE concludes that the notified draft amendments to the Network Enforcement Act are likely to create additional restrictions to the free cross-border provision of information society services and thereby fragmentation of the digital single market which are not justifiable by the derogations provided for in the E-Commerce Directive.

Compatibility with the General Data Protection Regulation (GDPR)

The proactive forwarding of personal data represents a far-reaching intervention in the fundamental right to data protection and informational self-determination and raises questions of compatibility with data protection regulations. The GDPR provides for exceptions for the processing of personal data by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences (Article 2 (2) (d)) and the disclosure of personal data by social networks could also be based in principle on the authorisation under Article 6 (1) (c) in conjunction with Article 6 (2) GDPR if 'processing is necessary for the fulfilment of a legal obligation to which the controller is subject'. Article 23 of the

GDPR allows Member States to restrict the principles relating to processing of personal data (Article 5 GDPR and related rights and obligations in Articles 12 and 22 GDPR), in particular regarding 'the prevention, investigation, detection or prosecution of criminal offences' (Article 23(1) d)). However, Article 23 GDPR provides several limits to these national restrictions: first, in Article 23 (1) GDPR the respect of 'the essence of the fundamental rights and freedoms', flanked by a proportionality test. In addition, Article 23 (2) GDPR puts up a set of criteria which has to be met by Member States in case of legislative restrictions to data protection rules. In particular, such laws have to provide inter alia for 'safeguards to prevent abuse or unlawful access or transfer' (d) and to take into account '(g) the risks to the rights and freedoms of data subjects'. Consequently, the notified draft regulations must be measured against the fundamental rights and freedoms assessments of the GDPR (and, where applicable, the JHA Directive for police processing of data). Doubts remain at present as to the constitutionality of such far-reaching data extraction and transmission obligations.

In addition, we have doubts about the territorial applicability of the law, since the obligation to hand over data under the Network Enforcement Act depends solely on German law - regardless of whether the person concerned is a German citizen, whether the offence actually constitutes an offence in the home country of the person concerned and from which location the relevant infringement is committed. The notified draft would, therefore, have an impact on users and service providers beyond the territory of Germany.

Under the notified draft law, social networks are only allowed to inform their users about the forwarding of their data (IP address) to prosecution authorities four weeks after the data transfer has taken place. Thereby, rights of the data subjects are largely undermined, as the information and disclosure obligations of service providers vis-à-vis their users are restricted. In this context, knowledge of the processing of personal data is the basic prerequisite for the assertion of all data subject rights. Data subjects who are not even aware that their data is being transferred are left defenceless under the draft law. Effective information obligations must therefore be included in any case, so that data subjects are safely and fully informed about the procedure and can still exercise their rights afterwards. Moreover, during transmission and processing, the authorities must ensure additional security obligations, such as strict purpose limitation and initially pseudonymous processing.

Interplay with the proposed Terrorist Content Online Regulation

The notified draft regulates a number of aspects that are also covered by the proposed Terrorist Content Online Regulation (TCO Regulation) since social networks constitute 'hosting service providers' according to the draft TCO Regulation.

The Commission's proposal for the TCO Regulation also requires hosting service providers, to 'preserve terrorist content which has been removed or disabled […] and related data removed as a consequence of the removal of the terrorist content and which is necessary for: (a) proceedings of administrative or judicial review, (b) the prevention, detection, investigation and prosecution of terrorist offences. The terrorist content and related data referred to in paragraph 1 shall be preserved for six months. The terrorist content shall, upon request from the competent authority or court, be preserved for a longer period when and for as long as necessary for ongoing proceedings of administrative or judicial review' (Article 7).

The Commission's proposal for the TCO Regulation also requires hosting service providers, where they 'become aware of any evidence of terrorist offences, […] [to] promptly inform authorities competent for the investigation and prosecution in criminal offences in the concerned Member State or the point of contact in the Member State pursuant to Article 14(2), where they have their main establishment or a legal representative' (Article 13 (4)).

Interplay with the proposed e-Evidence Regulation

The draft German law does not take into account the proposed Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (e-Evidence Regulation). The e-Evidence Regulation aims to establish European procedures for cross-border data access requests and release when the service provider controlling the data is based in a different Member State. The draft German law takes a separate national path that ignores the system proposed in the e-Evidence Regulation where law enforcement seeks information from a service provider outside their jurisdiction by utilizing a European Production Order (EPO), which in certain instances must be authorized by a judicial officer. Social network providers which are covered by the German draft law also fall within the definition of "service provider" in Article 2(3) of the draft e-Evidence Regulation, meaning that a cross-border dimension could be triggered for data requests. The cross-border nature of these requests will require authorities to utilise the European Production Order (EPO) mechanism (Art. 5, e-Evidence Regulation) when seeking to access data on social networks for criminal investigations. The use of a domestic instrument would be in direct conflict with the goals and objectives of the draft e-Evidence Regulation.

For instance, Article 2 of the e-Evidence proposal sets out definitions of data categories. Article 2(7)(b) states that passwords or other authentication means used instead of a password that are provided or created by the user are not within the scope of the draft Regulation. Meanwhile, the draft German law includes an obligation for social networks to disclose user passwords. This creates a direct conflict with the e-Evidence Regulation proposal which clearly outlines the data categories service providers would be obligated to disclose: Article 5 of the draft e-Evidence Regulation sets out the conditions for issuing an EPO, including the strict thresholds which must be met for obtaining data. While Article 5(3) allows for

an EPO to be issued for both “subscriber” and “access” data by a judge or public prosecutor for any crime, Article 5(4) notes that an EPO seeking “transactional” or “content” data may only be issued for criminal offenses punishable by a custodial sentence of a maximum of at least 3 years. Should “usage” or “inventory” data as set out in the notified draft law meet the definition of “transactional” or “content” data, then the punishment for the investigated right-wing extremism or hate crime must meet the 3-year threshold. If not, an EPO cannot be lawfully issued on the social network for the data in question.

Furthermore, Article 4 of the e-Evidence proposal clearly outlines which authority can issue an EPO, stating that an “issuing authority” must be a judge, a court, or an investigating public prosecutor. Should the German draft law allow for an authority other than those set out above to obligate social networks to disclose data, this would be in direct conflict with the e-Evidence proposal.

Lastly, Article 6 of the e-Evidence proposal sets out the conditions for the issuing of a European Preservation Order (EPO-PR), including clear safeguards and limitations to its use. Article 6(2) clearly states that an EPO-PR may only be issued to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via an EPO. Article 10(1) clarifies that the data preservation ceases after 60-days unless the issuing authority confirms that the subsequent request for production has been launched. The notified German law includes proactive data retention obligations for social networks based on a legal assessment of the content concerned. Such an obligation would be in direct conflict with the spirit of EPO-PRs.

Announced Digital Services Act initiative

The notified draft may also overlap with the Digital Services Act (DSA) initiative announced by Commission President von der Leyen. The DSA initiative aims at addressing the need for a clear and harmonized set of rules on the responsibility of providers of online intermediary services, while avoiding regulatory fragmentation of the internal market that national initiatives can entail.

Conclusion

DIGITALEUROPE shares the German government’s objective to combat right-wing extremism and hate crime online, especially the improvement of prosecution of such online crimes. In recent years, however, regulatory proposals have multiplied at both national and European level to address different types of content online, including terrorist content, copyright infringement, counterfeit goods, misinformation and illegal hate speech. While illegal content must be removed expeditiously by ISPs once notified, each of these initiatives usually involves different obligations, sanctions, and reporting duties, thus creating an unnecessarily complex regulatory landscape. We respect the differing cultural and

legal traditions in the Member States regarding freedom of expression[1], but we fear that a separate national path pre-empting the EU's on-going or upcoming work is not helpful and, besides raising doubts as to the compatibility with Data Protection Regulation, would lead to fragmentation of the Single Market.

FOR MORE INFORMATION, PLEASE CONTACT:

Hugh Kirk

Policy Manager

hugh.kirk@digitaleurope.org / +32 490 11 69 46

[1] In accordance with art 10.2 of the European Convention of Human Rights on "Freedom of Expression"

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK