Key points

Principles for a revision of the e-commerce directive/proposal for a digital services act | liability issues

13 May 2020

Summary

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (directive on electronic commerce – eCD) was adopted on 8 June 2000. A discussion is currently ongoing in the European institutions on a "digital services act" (DSA) which addresses, inter alia, themes which have so far fallen within the regulatory ambit of eCD and may lead to a revision of the directive. Although no formal proposals have yet been presented, Bitkom would nevertheless like to take this opportunity to submit a constructive contribution to the debate surrounding issues linked to the liability of service providers ahead of the consultation.

The planned amendment should be used to give providers of digital services a clear, uniform and up-to-date, innovation-friendly legislative framework for combating illegal content; in this regard, the ability to protect and enable users accessing on digital services is central. In addition, it is important to ensure the necessary cooperation between the Member States as well as adequate supervision of suppliers of digital services in the EU. Services which are active on the European market must comply with the legal provisions applicable in the EU. To this end, it is of decisive importance that all relevant players work together in order to secure a functioning digital single market and sufficient protection for consumers.

That is why we would like to draw attention to a number of important points which it is essential for a revision to take on board in order to reach the above-mentioned objectives and at the same time avoid unduly heavy regulation with potential for collateral damage and/or undesirable side effects. We call for appropriate and measured regulation tailored to the objectives to be met.

First of all, the most recent legislative measures (e.g. directive on audiovisual media services, platform-to-business (P2B) regulation and regulation on market surveillance and compliance of products) should be taken into account and legislative processes underway (e.g. regulation on preventing the dissemination of terrorist content online)

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Marie Anne Nietan

P +49 30 27576-221
m.nietan@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

www.bitkom.org

should be anticipated in order to ensure coherence. Where there is no need for more far-reaching regulation for specific themes/sectors, DSA should not create any new rules.

The e-commerce directive is a fundamental building block for the success of the Internet and has played a decisive role in enabling the development of successful services. Without the so-called liability privilege and the ban on imposing a general monitoring obligation established through the directive, the Internet economy would probably not have been able to develop into what we see today; service providers would face considerable challenges which would in many cases make the development of new services, platforms and business models substantially more difficult.

Similarly important for the success of Internet services in Europe is the country-of-origin principle enshrined in the directive; this enables service providers established in the EU to offer their goods and services across the entire EU without having to apply the various rules enacted by individual Member States. This principle was and is a decisive factor for the economic success of the European and international Internet economy which needs to be preserved.

As they were 20 years ago, the ground rules of eCD are today of great importance for the functioning of the digital economy. But at the same time, the significance of information society services for society and economy has increased massively, sometimes creating new policy challenges. Moreover, many instances of the need for accountable information society services have been manifested in the legal, societal and economic spheres in the framework of specific individual cases.

With regard to liability issues, we support the plan for more precise terminology and up-to-date definitions in areas where eCD no longer reflects technical and market-related progress. It could also be examined whether and to what extent the notice-and-take-down procedure needs to be streamlined and harmonised. However, we specifically warn against imposition of a general obligation on all information society services to observe and monitor all content generated, disseminated and shared in the Internet. Such an obligation would prevent a large number of providers from offering their services in any form whatsoever. Rather, we call for a differentiated approach oriented on the nature of the content of services offered.

Detailed considerations

- **Maintaining the system of graduated liability**: It is urgently necessary to maintain the so-called liability privilege or the system of graduated liability which eCD enshrines for the various information society services (articles 12-14 eCD). As described above, it is the fundamental building block for the continued success of the free Internet and has been decisive in helping to enable the development of successful services.

- **Strengthening the country-of-origin principle**: With particular regard to liability rules, Bitkom argues against a move away from but rather for a strengthening of the country-of-origin principle (article 3.2 eCD), since this constitutes a basic condition for providers' free choice of place of establishment and the free movement of digital services in the digital single market in the European Union.

- **Maintaining the ban on general monitoring obligations:** In any event, the ban on imposing a general obligation to monitor for all information society services (article 15 eCD) should be maintained, since this constitutes a further fundamental building block of Internet regulation and is an important condition for the generation and development of platforms and further services. Enabling such a blanket monitoring obligation is not the solution for the complex challenges generated by illegal content and poses enormous risks for collateral damage. We are heartened by the Commission's promises to maintain the ban on a "general obligation to monitor".

  It is also important that this ban is not hollowed out through an appeal to the imposition of "monitoring obligations in a specific case" excluded from the ban as set out in recital 47. Relevant rulings by the European Court of Justice make it clear that a specific monitoring obligation only encompasses cases which do not entail monitoring of all uploaded content for the presence of particular legal infringements for an unlimited period of time.

- **Horizontal but still differentiated regulatory approach:** We broadly welcome the idea that the horizontal regulatory approach of the e-commerce directive which covers each and every information society service is to be further developed. It is important to preserve the central, fundamental, generally valid and hence horizontally applicable principles of the directive such as liability privilege, the ban on a general monitoring obligation and the country-of-origin principle.

  However, beyond this, it is important to bear in mind that these services are characterised by highly varied business models and that there can be no "one-size-fits-all" solu-

tions for dealing with illegal content over and above the generally applicable principles. Accordingly, these differences must not be lost from sight in assignment of rights and obligations and in particular definition of the acceptability of measures that can be taken by providers.

- **Taking into account the technical architecture of services**: The current regime of the e-commerce directive distinguishes among information society providers between "mere conduits" whose service consists of "the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network" (article 12 eCD), providing "caching" services or "the automatic, intermediate or temporary storage" of information "performed for the sole purpose of making more efficient the information's transmission to other recipients of the service upon their request" (article 13 eCD), and "hosting" providers whose service consists of "storage of information provided by a recipient" (article 14 eCD). Any of these providers can benefit from the liability privilege, albeit under different conditions. This horizontal and yet differentiated approach is important, since it takes into account the different technical architecture of services and hence a particular provider's *de facto* insight into and possibilities for dealing with illegal content. For instance, Internet access providers have neither knowledge about or control over information transmitted via their communication network, not least because this is forbidden by regulation on network neutrality.

  It is appropriate in some circumstances to supplement or subdivide the existing provider categories under eCD (host provider, access provider, caching provider) with further categories and specific rules, still taking the technical architecture of service providers into account. For example, cloud services tend to act passively and usually have neither knowledge about nor control over content stored on their platform. Given their technical architecture and their contractual relations with users, these services are therefore more restricted in their possibilities to combat illegal content uploaded by their users. Expecting such passive services to make efforts to manage content comparable to those required of publicly accessible services for shared use of content runs counter to their technical and operational character and would lead to unjustified data protection, security and commercial overlaps. Thus, whether or not a service allows the sharing of content with the public could also be adduced as a criterion for an overlap between services.

- **Taking into account the different sectors and types content:** Service providers in a very wide range of sectors are also covered within the category of hosting provider – from social networks and suppliers of short-term lets through to online marketplaces. Fur-

thermore, the focus is on a large number of different types of content – from audiovisual media or user-generated content and holiday home offers through to offers of physical goods. A differentiated approach in the structuring of service providers' rights and obligations and in particular definition of acceptable measures which they can take should also take into account the different types of content and possible measures for dealing with these content types. The specific risk potential is also central for the differentiation of content types.

- **Proportionality and threshold values:** The public debate largely revolves around services with a large market presence and reach. Linking regulation to threshold values such as user volume broadly reflects a notion of proportionality – the idea that small enterprises should not be burdened with the same obligations as their larger counterparts which have more resources – and the circumstance that services with a high user volume have a greater societal and economic relevance. Even if this notion of proportionality is basically right, it is often difficult and sometimes also not generally appropriate to link regulation to specific threshold values, e.g. because of the nature of the market. Threshold values, i.e. a strictly quantitative approach, always go hand in hand with a danger of legal inaccuracy through to circumvention. In addition, depending on the framing of the provision, the result may be distortions of competition if competitors face different degrees of regulatory intervention. In the case of many provisions, a blanket limitation to, say, large market players is certainly inappropriate, e.g. for notice-and-take-down. It would run counter to the objective of removing illegal content if only large undertakings had to comply with such a provision.

- **Protecting small companies**: Irrespective of potential rules on the basis of market status, regulation should not constitute an unduly heavy burden on companies, in particular small enterprises. Governments should earmark more resources for the support of SMEs and micro-enterprises with limited resources. For start-ups and smaller providers, it can be a challenge to make considerable investments in the development of new technologies to ensure user security.

- **Notice-and-take-down procedure**: Within the existing regime, an improvement to the notice-and-take-down procedure at European level is necessary where deficits have been identified. This procedure must comprise a solid guarantee of fundamental rights and eliminate current legal uncertainties. For the notice-and-take-down procedure, guidelines are needed as to what conditions a communication must meet in order to be valid, as well as what is necessary to prevent inadmissible communications, errors and abuse. For all legal remedy and anti-abuse mechanisms, information is decisive for iden-

tification. The more specific the conditions for a communication, the better, more seamless and rapid the processing operation and reaction.

In addition, there could be uniform provision for what is to be done in a disputed case of a take-down. In this regard, it is important to bear in mind and recognise that, because they offer different services and content, different providers face different challenges which can be met in different ways through notice-and-take-down. In other words, providers also have different expectations of a notice-and-take-down procedure. In any event, notice-and-take-down procedures must take into account the specific features of individual sectors, always be oriented around the principle of proportionality and be structured differently where necessary. Alternatively, thought could be given to a counternotice procedure in line with the DMCA provisions. Unfortunately, there can also be abusive recourse to the notice-and-take-down procedure posing a business threat. This must be taken into account, e.g. through explicit provisions on how to deal with (repeated) abusive communications.

- **Flexibility instead of rigid deadlines**: We generally warn against setting unduly rigid deadlines for removing content. The concept of "without delay" as currently to be found in the e-commerce directive offers the necessary flexibility called for by the different types of illegal content and of service, and nevertheless indicates the need for urgent action.

- **Incentivising proactive measures**: Hosting providers in particular should be encouraged to take proactive voluntary measures to remove illegal and potentially harmful content from their platforms. Thus, it should be made clear that these efforts do not affect the continued existence of the liability privilege. Proactive measures can indeed lead to the provider acquiring knowledge about illegal activities or illegal information. However, the hosting provider has the possibility in such cases to remove or block access to questionable information as soon as it has acquired knowledge about it. If the hosting provider does this, it continues to enjoy exemption from liability. This is in line with the European Commission's 2017 communication on tackling illegal content online[1] (pages 10-12).

  It should also be made clear that proactive measures do not lead to the provider automatically having knowledge about all the information it stores. It is therefore important to create legal certainty about the standard of knowledge required in the framework of the liability protection regime. In this context, the following should be clarified:

[1] https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF

a) if a service provider voluntarily checks some content in order to ensure that it does not infringe one or more laws, it is assumed that this provider does not have any knowledge about the illegality of other content on its platform which it has not checked for such purposes; and
b) if a service provider voluntarily checks content in order to remove content which infringes a particular law, it is assumed that this provider does not have any knowledge about all other possible legal infringements which could be committed by the same content but which were not part of the check.

Without this clarity, the risk that a service provider taking proactive measures in good faith will be assumed to have knowledge about all content of its services could act as a deterrent to taking such responsible steps. Furthermore, thought could also be given to provisions which give a positive incentive to introduce such voluntary measures – e.g. through a lighter division of the burden of proof for the providers in question.

- **Responsibility | liability**: The distinction between taking on voluntary responsibility and legal liability is important. While maintaining the general liability privilege, possibilities for taking on responsibility as a function of the type of service provider and content should be discussed.

- **Protecting fundamental rights**: In the framework of regulation of service providers, fundamental rights must always be taken into account and secured through appropriate protective arrangements. Freedom of speech should be highlighted in the area of media providers and social networks, free movement of goods in the area of online commerce.

- **Provisions on customer protection & transparency**: Provisions on customer protection such as transparency are an important factor for trust. A whole series of consumer protection provisions have been introduced at EU level in recent years, most recently the so-called modernisation directive for example. In the meantime, provisions in eCD have been overlaid by new laws. It is therefore questionable whether the upcoming amendment constitutes the right framework for consumer protection.

  In addition, some service providers already deliver information which goes beyond legal requirements. Irrespective of their size, service providers have a strong interest in the trust of their users. Where transparency deficits nevertheless occur, further consumer protection provisions such as transparency obligations can certainly make sense. With an eye to possible new transparency rules for the ranking in Internet service offers, it is important to understand that this is influenced by a range of factors and filters. Moreo-

ver, any transparency obligation should comprise protective measures against passing on business secrets. Under no circumstances should consideration be given to general provisions which make disclosure of concrete algorithms obligatory, since in many cases they constitute a core element of a provider's business model. Revelation of too much information about the functioning of algorithms can also lead to them being compromised by fraudulent players (hackers, spammers, etc.), which can ultimately harm the consumer. Rather, the publication of generic and general information should be required at most. This is already clarified in the relevant provisions of the modernisation directive and in the P2B regulation.

Whereas a verification of the business identity of players on the platforms of some service providers could be useful in order to deter harmful online players and underpin criminal prosecution, the introduction of such obligations must be proportionate and comprise appropriate measures to protect the privacy of users in the framework of their legitimate and legal activities. The verification must be limited to data which are genuinely necessary and sufficient to meet the purpose.

- **Harmful vs. illegal content**: Content (in particular user-generated content) on media platforms which is classified as "legal but harmful", e.g. false intelligence, can often be addressed better through self-regulation than through strict regulatory requirements. This is a more efficient instrument in this area, since constantly changing harmful content can be better taken into account through greater flexibility and more rapid adjustment. But first and foremost, the necessary legal framework for dealing with this type of content is completely different from that for illegal content, and there is a stronger link to restriction of personal rights. It is often very difficult to evaluate whether or not content is illegal. Whether content is "harmful" is often less easy to decide on the basis of clearly defined criteria, since this depends even more strongly on the relevant context/user group. Provisions on harmful media content should not be covered by the digital services act and should be addressed in the democracy act. Nevertheless, it must continue to be possible for providers to moderate unwanted content in their service offer in line with their own (transparent) rules.

- **Improving legal enforcement**: Improving legal enforcement is a central factor and is a complementary building block for the discussion on introduction of updated obligations. An important role is played here by measured, efficient supervision as well as enforcement of existing obligations. Better cooperation between national supervision authorities is also necessary here, and support is desirable in order to prevent divergent application and enforcement of provisions designed to be uniform across the EU and to

ensure consistency. In addition, the instrument of the regulation rather than the directive could offer better harmonisation.