[redacted]

05. May 2017

# Legal Expertise

commissioned by

BITKOM

Bundesverband Informationswirtschaft,

Telekommunikation und neue Medien e.V.

Albrechtstraße 10

10117 Berlin-Mitte

concerning the notified German Act to Improve Enforcement of the Law in Social Networks

(Netzwerkdurchsetzungsgesetz)

[redacted]

# Table of Content

# I. Appraisal Order

The Association of German Telecommunication and Internet Enterprises (BITKOM) has mandated me to analyze the notified German act Act to Improve Enforcement of the Law in Social Networks (Netzwerkdurchsetzungsgesetz) with regard to its compliance with European law, in particular the E-Commerce-Directive and related data protection provisions.

The expertise does not to intend to analyze in depth constitutional aspects and issues of fundamental rights and freedoms.

I will in particular analyze if the new act on enforcement regarding social networks is

- compatible with the principle of country of origin as enshrined in Art. 3 of the E-Commerce-Directive[1]
- compatible with Art. 14, 15 E-Commerce-Directive with respect to recitals 46 and 48 regarding the notice-and-take-down procedure
- introducing special requirements for the notion of „knowledge“ in Art. 14 E-Commerce-Directive
- compatible with the prohibition of obligations for providers to monitor in a general way, Art. 15 E-Commerce-Directive
- treating all providers in the same way and does not disadvantage certain providers such as social networks
- compatible with the European General Data Protection Regulation (GDPR) and with that respect European fundamental rights concerning the envisaged disclosure of personal data of users in case of violation of „absolute rights“ (others than intellectual property rights)

[1] Directive 2000/31/EC of the European Parliamenent 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 No. L 178, p. 1 of 17.7.2000

## II. Executive Summary

The new envisaged German act on social networks is not compatible with European law in several regards, such as

- incompatible with the principle of country of origin as enshrined in Art. 3 of the E-Commerce-Directive2 as the act just refers to Art. 3(4) for service providers in other EU-member states. This reasoning disregards the case-by-case approach of Art 3(4) which does not allow for general derogations (cf. IV.)
- incompatible with Art. 14, 15 E-Commerce-Directive with respect to recitals 46 and 48 regarding the notice-and-take-down procedure as the act substitutes the notion of „expeditiously“ by fixed terms and thus leading to deviation from full harmonization (V.A)
- introducing special requirements for the notion of „knowledge“ in Art. 14 E-Commerce-Directive (V.B)
- incompatible with Art. 14, 15 E-Commerce-Directive by introducing an obligation to remove copies, without regarding if such copies have been stored by third parties
- treating all providers in the same way and disadvantaging certain providers such as social networks, at least introducing huge legal uncertainties (VII.)
- incompatible with the European General Data Protection Regulation (GDPR), the ePrivacy Directive and European fundamental rights concerning the envisaged disclosure of personal data of users in case of violation of „absolute rights“. Procedural safeguards for data subjects and judicial control of disclosure are missing (VIII.)

[2] Directive 2000/31/EC of the European Parliamenent 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 No. L 178, p. 1 of 17.7.2000

## III. Introduction – Chief aims and structure of the new Act

The German government proposes a new „Act improving law enforcement on social networks [Netzwerkdurchsetzungsgesetz – NetzDG]“ which has been notified to the EU-Commission on 27th of March 2017.[3] The act aims mainly – as the German notification points out – at

> „the introduction of statutory compliance rules for social networks in order to encourage them to process complaints about hate speech and other criminal content more quickly and comprehensively.“

The German government states that social networks (and alike providers) should live up to their responsibility to immediately remove infringing content – which according to the statement of the German government they still do not in a satisfying manner.[4]

To achieve a more satisfying level of removing illicit content and fake news the act provides in principal roughly two obligations:

- to report periodically to authorities as well as to the public their actions concerning complaints about illicit content and their organization to handle these complaints
- to remove in 24 hours content which is blatantly[5] illicit and within 7 days all other illicit content

If some of these obligations are not fulfilled, fines may be imposed up to 5 Mio Euro in case of deliberate or negligent non-compliance with the reporting obligations, violation of the obligation to have effective complaint management, etc., up to 50 Mio Euro for legal persons.

## IV. Conflict with country of origin principle, Art. 3 E-Commerce-Directive

### A. The international applicability of the act on social networks

The proposed act (Sec.1 (1)) applies to all operators of commercial telemedia services (roughly information society services according to the E-Commerce-Directive) who operate a platform which enables users to exchange any kind of content, to share this content or to make the content

---

[3] Notification Number 2017/0127/D - SERV60. The notificiation wrongly named the Act „Netzdurchführungsgesetz – NetzDG“.
[4] Notification „Brief statements of grounds“.
[5] It is unclear if the German Act will refer to „blatantly“ (so the wording in the notification of the German Government) or to „manifestly“ (as used in the translation of the German act by the German Government).

publicly available. Exempted are platforms with own journalistic-editorial content (journalistisch-redaktionell gestaltete Angebote) or small platforms with less than 2 Mio users in Germany.

Moreover, the application of the new enforcement obligations depends on certain illicit content which is enumerated in Sec. 1(3) of the act, referring mainly to communication offenses in criminal law such as defamation or rabble-rousing but also to treasonous forgery or antistate propaganda as well as to distribution of every kind of pornography etc.

As the act does not provide for a territorial exemption all obligations of the new act apply to providers based in Germany as well as to those based in other countries, be it in other EU-member states or in third countries. The act does not contain any provision which would be alike Art. 3 of the E-Commerce-Directive (which has been implemented in Germany in Sec. 3 of the Telemedia-Act). The international applicability of the proposed act is also reflected in Sec. 4(3) which states explicitly that violations of the duties can also be fined when they take place outside Germany.

Thus, all providers with users in Germany will be affected, regardless of the location of their headquarters or their seat. Sec. 1(2) of the proposed act reflects this approach to international applicability when the provision stipulates a minimum threshold of 2 Mio users in Germany – hence, the only relevant criteria are users in Germany of the social network.

## B. The country of origin principle

Given the applicability of the envisaged act to providers seated in other EU-Member States it is highly arguably if the act is compatible with Art. 3 E-Commerce-Directive:

### 1. Underlying rationale

The underlying rationale of the country of origin principle refers to the goal of harmonizing the legal framework for all information society providers in the EU, given the global character of the Internet. The EU clearly stated that goal in Recitals 1, 3, 5 and 10 of the E-Commerce-Directive.[6] Moreover, Recital 22 point out that:

> „(22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of

[6] See also CJEU 25.10.2011 – C-509/09 e-Date.

> services, such information society services should in principle be subject to the law of the Member State in which the service provider is established."

Once again, the E-Commerce-Directive lays stress on the „freedom to provide services" and on „legal certainty" for providers, guaranteed by the country of origin principle. The Court of Justice of the EU took the same stance in the eDate advertising decision:[7]

> „66 In relation to the mechanism provided for by Article 3 of the Directive, it must be held that the fact of making electronic commerce services subject to the legal system of the Member State in which their providers are established pursuant to Article 3(1) does not allow the free movement of services to be fully guaranteed if the service providers must ultimately comply, in the host Member State, with stricter requirements than those applicable to them in the Member State in which they are established.
>
> 67 It follows that Article 3 of the Directive precludes, subject to derogations authorised in accordance with the conditions set out in Article 3(4), a provider of an electronic commerce service from being made subject to stricter requirements than those provided for by the substantive law in force in the Member State in which that service provider is established."

Hence, it is not overemphasized to qualify the country of origin principle as one of the cornerstones of the E-Commerce-Directive.

### 2. Applicability of the country of origin principle

The country of origin principle applies to the so-called „coordinated field" which is defined by Art. 2 h). The proposed German act provides obligations for providers to install complaint management systems, to establish in Germany a person who could be held responsible, to report periodically about the state of the complaints, and to remove illicit content in a prescribed way. Thus, the planned obligations clearly fall under the coordinated field, in particular requirements concerning behaviour of the service provider.

Hence, the envisaged act on enforcement of social networks has to comply with the country of origin principle – which is confirmed indirectly by the official reasoning of the German government which states that there is no conflict with Art. 3 of the E-Commerce-Directive by invoking the exception of Art. 3 (4).[8]

### 3. Exceptions to the country of origin principle

Crucial for the evaluation of the proposed act is thus the compatibility with the country of origin principle, in particular with the exceptions which Art. 3 E-Commerce-Directive provides in Art. 3 (3) and Art. 3 (4). Whereas it is evident that Art. 3 (3) and the Annex cannot justify the planned act on social networks as no legal area or activity mentioned in the Annex is being covered the

---

[7] CJEU 25.10.2011 – C-509/09 e-Date.

[8] Begründung Regierungsentwurf NetzwerkdurchsetzungsG p. 13, 14.

German government concentrates on Art. 3 (4). As this provision is crucial for the legal assessment it shall be cited here:

> „Member States may take measures to derogate from paragraph 2 in respect of a given information society service if the following conditions are fulfilled:
>
> (a) the measures shall be:
>
> (i) necessary for one of the following reasons:
>
> - public policy, in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons,
>
> ....
>
> (ii) taken against a given information society service which prejudices the objectives referred to in point (i) or which presents a serious and grave risk of prejudice to those objectives;
>
> (iii) proportionate to those objectives;
>
> (b) before taking the measures in question and without prejudice to court proceedings, including preliminary proceedings and acts carried out in the framework of a criminal investigation, the Member State has:
>
> - asked the Member State referred to in paragraph 1 to take measures and the latter did not take such measures, or they were inadequate,
>
> - notified the Commission and the Member State referred to in paragraph 1 of its intention to take such measures."

The German government contends in particular that the act would comply with the requirements of Art. 3(4) as the act would concern „a specific information service provider". However, the reasoning misunderstands Art. 3(4) E-Commerce-Directive as this exception in Art. 3(4) applies exactly to a specific case, for instance procedures against one social network (judicial or administrative) etc. The exception in Art. 3(4) does not refer to a whole group of information service providers[9] – in contrast to the proposed act which covers all kinds of social networks or other services such as E-Mail-providers[10] and does not refer only to one specific case.

That Art. 3(4) does not refer to entire classes of information society providers is also reflected by Art. 3(4) b) i which requires the recipient state which wants to take action to ask beforehand the

[9] See also *Weller* in Beckscher Online Kommentar, Informations- und Medienrecht, § 3 TMG, Rz. 32; *Nordmeier* in Spindler/Schuster (eds.), Recht der elektronischen Medien, 3rd. ed. 2015, § 3 TMG Rz. 22; also *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, 97; *Feldmann* Kommunikation und Recht (Journal = K&R) 2017, 292, 296.

state of the origin of the service provider to take care of the (specific) provider. This procedure is clearly related to other uses of the country of origin principles enshrined, for instance, in financial markets Directive, such as the Market for Financial Instruments Directive (II).[11] The procedure addresses the coordination between supervising authorities in order to guarantee the free flow of services in the European Union, to avoid establishing national barriers to services coming from another EU member state (European Pass). However, this procedure is not related to legal acts addressing whole class of service providers.

This interpretation of Art. 3(4) E-Commerce-Directive is affirmed if we take into account the general exceptions to Art 3(1) by Art. 3(3) E-Commerce-Directive referring to the annex. This annex contains exceptions referring to legal areas such as intellectual property rights or contractual consumer protection – and not specific cases. Such an annex would rather be unnecessary if Art. 3(4) could be applied to whole classes of information service providers as member states could easily invoke one of the exceptions grounds provided for in Art. 3(4). This can also clearly be demonstrated if we look at the exceptions for consumer: Whereas Art. 3(3) and the Annex state an exception for all contractual protections concerning consumers, Art. 3(4) once again refers in general to consumer protection – the repeated (and extended) reference would not make any sense if Art. 3(4) could be understood in a way that whole classes or groups of cases are embraced by Art. 3(4).[12]

Moreover, the French version clearly indicates that all exceptions are related to just one service provider rather than to a class of them:

> 4. Les États membres peuvent prendre, à l'égard d'un service donné de la société de l'information, des mesures qui dérogent au paragraphe 2 si les conditions suivantes sont remplies:

The French version (and all other romanic versions) makes it more clear than the German or English version that a singular is being used and only one specific case is being addressed.

Finally, and very clearly, the EU-Commission took the same stance in the Communication of 2003 regarding electronic financial services and derogations by member states:

> „2.1.2. Concept of "given information society service"

---

[10] As E-Mails also serve as a means to share information etc. Thus, every E-Mail-provider also has to be qualified according to the German Act as a „social network“ as E-Mail-services can be qualified also as telemedia services.
[11] Directive (2014/65/EU) of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast), OJ L 173/349, 12.6.2014. See for instance, Art. 34 of the MiFID II and Art. 86 MiFID II concerning precautionary measures by the host state.

> A "given" service is taken to mean here that the Member State of destination may not, under Article 3(4), take general measures in respect of a category of financial services such as investment funds or loans.
>
> To be covered by Article 3(4), the measure must, therefore, be taken on a case-by-case basis against a specific financial service provided by a given operator.
>
> For example, it could be a measure such as a warning or a penalty payment taken by a country of destination against a bank proposing from its place of establishment in another EU country non-harmonised investment services to residents of that country. Such measures could, for instance, be taken on the ground that the bank was not complying with certain rules of conduct designed to protect consumers in the country of destination.
>
> However, a Member State could not, on the basis of Article 3(4), decide that its entire legislation on, say, non-harmonised investment funds was applicable in a general and horizontal fashion to all services accessible to its residents."[13]

Thus, the Commission makes it very clear that Art. 3(4) refers to a case-by-case basis. In particular, every case has to be analyzed on grounds of the proportionality test[14] – and not in a general way. Hence, there is no room for such an interpretation as the German government is undertaking.

### 4. Urgency (Art. 3(5)

Moreover, the German government argues that an instant action is needed to combat hate speech and other criminal actions in the Internet.[15] However, it is highly questionable that a case for urgency can be construed: The issues at stake has already been known for a longer time, be it at the national or European level. That the US-elections has been influenced by fake news or activities at the social networks is just a prominent emanation of this general trend concerning communication on the Internet and in particular on social networks.

Nevertheless, these issues have been well known for years[16] – for instance, the author of this expertise also has presented a large legal expertise on personality rights and enforcement problems on the Internet at the Deutsche Juristentag (the German Conference of all legal professions) in 2012.[17] Hence, it should be out of question that the matter of defamation, hate speech, and fake news were already at stake in the last decade.

---

[12] This is disregarded also by the German High Federal Court in the decision of 30.3.2006 – I ZR 24/03 BGHZ 167, 91, 101 f. – Arzneimittelwerbung im Internet. The court did not assess the relationship between the E-Commerce-Directive and other directives (here: prohibition of advertising for medical drugs).

[13] Communication from the Commission to the Council, The European Parliament and the Eurpean Central Bank – Application to financial services of Article 3(4) to (6) of the Electronic Commerce Directive, 14.5.2003 COM(2003) 259 final.

[14] Communication from the Commission, COM(2003) 259 final point 2.2.4.

[15] Begründung Regierungsentwurf NetzwerkdurchsetzungsG p 14.

[16] See also *Wimmers/Heymann*, in: Archiv für Presserecht (Journal = AfP) 2017, 93, 98.

[17] *Spindler*, Persönlichkeitsrechte im Internet, Deutscher Juristentag 2012, Gutachten F (Personality rights in the Internet, Legal Expertise for the German Conference of all lawyers, judges, and other juridical professions).

### C. Proportionality Test

Even though Art. 3(4) cannot be called into play to justify the proposed act it should be finally mentioned that the act has to pass at any rate the proportionality test. Without going into details here as these issues are out of the scope of the expertise, there are severe doubts if all categories of content foreseen by Sec. 1(3) of the proposed act would pass the proportionality test and could justify barriers to free flow of information society services, in particular with regard to risks to fundamental freedoms such as freedom of expression as granted by Art. 11 of the EU-Fundamental Rights Charta. If really all kinds of defamation could form a basis for additional obligations to information society services in other EU-member states is highly questionable.

### D. Summary

The envisaged German Act violates the country of origin principle laid down in Art. 3 (2) E-Commerce-Directive. The exceptions in Art. 3 (4) E-Commerce-Directive only apply to a case-by-case approach and do not justify general laws applying also to providers in EU Member States. Finally, there is no evidence for a case of urgency according to Art. 3 (5) E-Commerce-Directive.

## V. Specification of notice-and-take-down procedures and of „knowledge“

### A. Provisions of the proposed Act

The proposed act raises also concerns about its compatibility with the provisions laid down in Art 14 E-Commerce-Directive, in particular the notice-and-take-down procedure and the notion of „knowledge“. In the notification for the planned act the German government states:

> „The draft sets out legal standards for effective complaint management to ensure that social networks delete blatantly criminal content corresponding to an objective offence in one of the criminal provisions stated in § 1(3), as a rule 24 hours after receipt of the complaint from the user. The draft makes it compulsory to have effective, transparent methods for the prompt deletion of illegal content, including user-friendly mechanisms for registering complaints. (...) Service providers are bound to immediately remove illegal content they are storing for a user, or to block access to said content once they become aware of it. The compliance obligations laid down in this draft presuppose said requirement imposed on service providers and specify it further.“[18]

More specifically, the planned act will introduce scaled obligations for providers to remove illegal content or to block it:

[18] Note, that the translation uses the word „manifestly“ instead of „blatantly“

- First, providers have to introduce an efficient complaint management, in particular mechanism for users to file complaints (Sec. 3(1) of the act)
- Second, providers have to take care to take note expeditiously of the complaint and to assess the content on a legal basis (Sec. 3(2) Nr. 1 of the act). For blatantly[19] criminal content concerning the criminal offences mentioned in Sec. 1(3) of the act providers have to remove the content within 24 hours after having received the complaint, with the exception of longer terms agreed upon with prosecuting authorities (sec. 3(2) Nr. 2 of the act)
- Third, to remove or block any illicit content within 7 days after having received the complaint (sec. 3(2) Nr. 3 of the act)

All these duties are sanctioned by imposing fines on acting persons as well as the enterprise, in the latter case up to 50 Mio Euro (Sec. 4(1) and 4(2)).

### B. Notice-and-take-down-procedure

By these means the act specifies the obligation of (host) providers enshrined in Art. 14 of the E-Commerce-Directive. These provisions are flanked by recitals 46, 48:

> (46) In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal 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; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information.
>
> (48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply which can reasonably be expected from and which are specified by national law, in order to detect and prevent certain types of illegal activities.

The liability privileges in Art. 12 – 15 E-Commerce-Directive are fully harmonizing, giving leeway to the Member States only where explicitly stated.[20]

Whereas Art. 14 just requires that a provider „upon obtaining knowledge or awareness, acts expeditiously to remove or to block access to the information" Sec. 3(2) Nr. 2 and Nr. 3 refer to fixed terms within a provider has to act, starting with the date of having received the complaint. In contrast Sec. 3(2) Nr. 1 of the planned act refers to Art. 14 (1) E-commerce-Directive when

[19] Or as in the translation „manifestly".

requiring the provider to take note expeditiously of the complaint and assess the legality of the content. Thus, the proposed German act deviates significantly in some issues from Art. 14 of the E-Commerce-Directive:[21]

- First, instead of acting „expeditiously“ the requirement to act within 24 hrs. or at least 7 days
- Second, by calculating the term starting with the reception of the complaint instead of referring to actual knowledge

### 1. Fixed terms

As mentioned, Art. 14 of the E-commerce Directive uses explicitly the term „expeditiously“, in the French version „promptement“, in the Spanish version „con prontitud“, in the Italian version „immediatamente“, in the Netherlands version „prompt“, in the German Version „unverzüglich“.

However, the E-Commerce-Directive does not specify what has to be understood by expeditiously – thus, it seems that the E-Commerce-Directive would leave some leeway for member states to specify this term. This perspective seems to be fostered by recital 46 S. 2 of the E-Commerce-Directive which obviously allows the member states to introduce procedures for the removal:

> „the removal 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;

However, the phrase has to be read carefully: The „procedures established“ at national level refer explicitly to „this purpose“ which refers to removal or disabling of access. Thus, procedures means ways of **how** to remove or block an access – but not **when** (or at which moment in time) a content has to be removed. Recital 46 S. 1 states once again that the removal etc. has to be done expeditiously; S. 2 does not refer or specify this notion but just refers to the removal or disabling of access as such. This is confirmed by the second restriction in Recital 46 S. 2 which requires „the observance of the principle of freedom of expression“ – hence, once again a requirement which concerns the removal as such in order not to discourage users from using their freedom of expression, but not the point in time when the removal has to be done.

Furthermore, Member States could argue that Recital 46 S. 3 allows them to specify requirements for removal or disabing information:

---

[20] Cf. German High Federal Court (Bundesgerichtshof) 04.07.2013 - I ZR 39/12 NJW (Neue Juristische Wochenschrift) 2014, 552 – Terminhinweis mit Kartenausschnitt, Paragraph 19, 20.
[21] See also *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, 95.

> „this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information."

However, this part of the recital clearly refers to requirements **prior** to the removal, hence for the procedure before removing or blocking a content – such as prior information to the owner of the content. For instance, the German High Federal Court introduced such a procedure in the context of injunctions againgst defamations in blogs, requiring the blog provider to ask the blogger for a statement referring to a complaint and then vice-versa the complainer if he would upheld his complaint in the light of this blogger`s statement.[22] In contrast, the fixed terms of Sec. 3 (2) of the proposed act do not refer to such a procedure prior to the removal rather than specifies the term „expeditiously".

In sum, Recital 46 allows to establish procedures for the removal or blocking of content as such but does not allow to specify the notion of „expeditiously" in Art. 14 of the E-Commerce-Directive.

There are also good reasons on the European level not to allow member states too much leeway in specifying Art. 14: Different terms in member states which would concretise the notion „expeditiously" by introducing fixed terms could very soon lead to a scattered landscape of liability privileges in Europe. Thus, whereas Germany provides for fixed terms of 24 hours or 7 days other member states could introduce complete different terms such as 7 hrs. or 48 hrs. etc. or even longer than 7 days. The intention of the E-Commerce-Directive to fully harmonise liability of intermediaries would thus be severely undermined.

The same phenomenon already has been stated concerning different notice-and-take-down procedures in Europe.[23] Moreover, different terms in Member States have led, for instance, in consumer protection to a review of consumer protection directives and to a new directive in order to stick to fixed mandatory terms for all Member States so that legal insecurity shall be avoided.[24]

---

[22] German High Federal Court (Bundesgerichtshof), 25.10.2011 - VI ZR 93/10 BGHZ 191, 219 (Official edition of Decisions Vol. 191, p. 219) – Mallorca-Blogger; see also German High Federal Court (Bundesgerichtshof), 1.3.2016 – VI ZR 34/15 – Jameda, AfP 2016, 253

[23] Cf. *Verbiest/Spindler/Riccio/van der Perre*, Study on the liability of internet intermediaries (Markt/2006/09/E), 12.11.2007, http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf p. 15 and following with references to national reports.

[24] Directive 2011/83/EU of the Europeoan 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, OJ L 304/64 of 22.11.2011.

Finally, there is no indication that the notion of „expeditiously“ should not be interpreted on the European level by the Court of Justice of the European Union (CJEU) as an autonomous notion of the E-Commerce-Directive.

### 2. Obligation after having received a complaint

Secondly, the envisaged German act calculates all terms upon the reception of the complaint. However, Art. 14 (1) S. 2 b) explicitly refers the obligation to act to the „obtaining (of) such knowledge.“ This deviation matters in different perspectives:

#### *a) Knowledge versus reception of a complaint*

First, reception of an information cannot be equally treated as „knowledge“ according to Art. 14 (1) E-Commerce-Directive. Whereas reception of an information refers – at least according to traditional German Doctrine enshrined in Sec.130 of the German Civil Code – to achieving control of an information, such as receiving a letter in a letter box, and does not relate to the actual knowledge (such as opening the letter) the term of knowledge in Art. 14 (1) refers to human actual knowledge of a content, that a human being has noted the content in an aware manner. As Art. 14 (1) E-commerce Directive intends to privilege neutral, automatized activities (as the CJEU noted)[25] only human knowledge is relevant for the liability privilege.[26] Hence, knowledge in the sense of Art. 14 (1) E-Commcerce-Directive is not the same as the reception of the complaint. Whereas one could argue that in most cases reception of information would lead to the same result as knowledge, in particular concerning blatantly (or manifestly) criminal offenses, it may not be the same when calculating a 24 hrs. term.

#### *b) Knowledge of illicit content*

Secondly, knowledge as used by Art. 14(1) E-Commerce-Directive does not only refer to the knowledge of the content as such rather than also knowledge of illicit character.[27] Whereas the German and English version are not clear the French or Spanish version clearly indicate that knowledge in Art. 14(1) E-Commerce-Directive also refers to the legal assessment of a content:

> “le prestataire n’ait pas effectivement connaissance de l’activité ou de l’information illicites“
>
> „conocimiento efectivo de que la actividad o la informatión es ilicita“

---

[25] CJEU 12.7.2011 – C-324/09 L`Oreal v ebay Paragraph 113 and following.

[26] If not, the E-Commerce-directive would be construed in such a way that the provider would have to introduce automated decision procedures which surely cannot take into account aspects of freedom of expression.

[27] For the German discussion cf *Eck/Ruess*, Multimediarecht (Journal = MMR) 2003, 363, 365*; Freytag*, Computer und Recht (Journal = CR) 2000, 600, 608; *Dustmann*, Die privilegierten Provider, S. 107; *Wimmer/Kleineidam/Zang*, Kommunikation und Recht (Journal = K&R) 2001, 456, 460 f.; *Berger*, MMR 2003, 642, 645; *Hoffmann*, MMR 2002, 284, 288; Beckscher Onlinekommentar Informations und Medienrecht/*Paal,* § 10 TMG Rn. 30; contravening opinion: Beckscher Kommentar Recht der Teledienste /*Jandt,* § 10 TMG Rn. 18; *Härting*, CR 2001, 271, 276.

Hence, the reception of a complaint cannot be treated as the relevant knowledge in the sense of Art. 14(1) as knowledge requires also the legal assessment – which may take more time than 24 hrs.

Even though a thorough analysis of constitutional legal aspects of the planned act, such as dangers for the freedom of expression (Art. 11 Charter of fundamental rights of the European Union (2000/C 364/01)[28], is out of the scope of this analysis it should be noted that such fixed terms as they are provided for in the planned German Act could force providers into a dilemma when they have to check like a judge if a content is within the borderlines of freedom of expression (or arts etc.).[29] Hundreds of disputed decisions even between the highest courts in Europe highlighten these intrigue issues how to strike the balance between defamation and freedom of expression (for instance, of prominent persons such as Caroline of Monaco).[30]

Regarding the planned German act, the provider has to take a decision in order not to be fined up to 50 Mio Euro. In contrast, if the provider would remove the incriminated information he risks only claims for damages of the user which are hardely to assess (immaterial damages etc.) and could result in very low sums. Thus, it is very likely (and economic rationale) that the provider will make up his mind to remove the information (or to block access to it). Thus, such an obligation would highly endanger the fundamental freedom of expression.[31]

The E-Commerce-Directive takes such dangers explicitly into account: As recital 46 puts it, the provider has to take his decision with obeyance to the principles of freedom of expression. However, if the provider faces fines up to 50 Mio Euro and if no judicial act is necessary to remove the information the balance is shifted to the detriment of freedom of expression.

### *c) Knowledge and general complaints*

Thirdly – and more important than all other arguments - the term used in the German act refers to a complaint – not specifying when a complaint may trigger the obligations to act. Hence, such a complaint could be formulated in a general way, not always enabling the provider to discern immediately the incriminated content. Even very general complaints could then trigger the obligations for the provider, resulting in fact in an obligation to inspect the case thoroughly.

---

[27] See also *Eck/Ruess*, MMR 2003, 363, 365; *Gercke*, MMR 2003, 602, 603
[28] OJ No. C 364, p. 1 of 18.12.2000. Issues of the German Constitution are out of scope of this expertise.
[29] Cf. *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, in particular p. 99 and following
[30] Cf. European Court of Human Rights 7.2.2012 - 40660/08 against German Federal Constitutional Court 26.2.2008 - 1 BvR 1626/07 and German High Federal Court of Justice (Bundesgerichtshof) 6.3.2007 - VI ZR 51/06.
[31] Same result in also *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, 98.

In contrast, Art. 14 (1) E-Commerce-Directive refers to the content as such – thus, a specific content has to be named, the provider is not being held to monitor his servers (Art. 15). This perspective is affirmed by Art. 14 (1) 2nd. alternative which refers for civil damage claims to the knowledge of evident circumstances (!), in contrast to the knowledge of the content as such (Art. 14 (1) 1st. alternative). Such a distinction would not make any sense if knowledge in Art. 14 (1) 1st. alternative could be construed in such a way that also general hints would trigger already the obligation for the provider to act. Moreover, any obligation to thoroughly scrutinize a case by inspecting all circumstances and facts would contravene the objective of the E-Commerce-Directive to enhance automated business models.

Even concerning civil damages (Art. 14(1) 2nd. alternative) the CJEU clearly states that not all notifications will result in an „awareness" of facts and circumstances:[32]

> „122 The situations thus covered include, in particular, that in which the operator of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality."[33]

## C. Summary

In sum, the envisaged German Act deviates in several ways from the full harmonizing Art. 14 E-Commerce-Directive by:

- introducing fixed terms instead sticking to the „expeditiously" deletion or blocking access to an infringed information
- referring to the reception of a complaint instead to „knowledge" as required by Art. 14 E-Commerce-Directive
- not taking into account that „knowledge" according to Art. 14 E-Commerce-Directive requires also knowledge of the illegality of an information.
- triggering obligations by a mere complaint and not referring to a specific information.

[32] CJEU 12.7.2011 – C-324/09 L`Oreal v ebay
[33] Underlining by the author.

## VI. Monitoring obligations by mandatory deleting „copies“?

According to Sec. 3(2) Nr. 6 of the envisaged German act operators of social networks are also obliged to remove expeditiously or block access to „copies“ of the illicit content.

- First, the relationship of this provision to the terms fixed in Sec. 3(2) Nr. 2, 3 of the planned German act is not very clear as Nr. 6 refers to an „expeditiously“ action whereas Nr. 2, 3 obviously use an objective system of fixed terms.
- Second, this provision may enter into conflict again with Art. 14 (1) E-commerce-Directive as well as Art. 15 E-Commerce-Directive as the provider is not only obliged to remove or block access to a specific content stored on his server (with a specified location) rather than to remove all „copies“ of the relevant content.

### A. Copy versus information stored at the request of a recipient of the service (Art. 14 E-Commerce-Directive)

If this provision of the German Act is still in line with Art. 14 (1) E-Commerce-Directive depends on the interpretation of „information stored at the request of a recipient of the service“ and the related obligations of the provider to act. Reading carefully Art. 14 (1) E-commerce-Directive the obligations to remove and/or block access to the information refer always to „the information“ – thus, to the „information stored at the request of a recipient of the service“, and not to the information as such or in general. In other terms, only the information/content stored by the specific user is being concerned – and not information/content stored by other users, even if this content may be identical to the one which has been complained about. This interpretation is affirmed by provisions of the E-commerce-Directive which cope with typical actions of mirroring, in other terms of making copies of the relevant information/content. Thus, Art. 13 of the E-Commerce-Directive copes with caching used in order to enhance communication on the Internet. Such a provision would not have been necessary if Art. 14(1) E-Commerce-Directive would oblige providers to remove all identical information being stored or mirrored by third parties. Moreover, Art. 15 E-Commerce-Directive prohibits any general obligation of providers to monitor servers (or data traffic). However, if providers would be obliged to remove copies of the incriminated information they would have to search their servers in order to detect and remove this kind of information if the informations has being stored by third parties.[34]

Such an obligation to check whether a content is a copy of an incriminated information may result in a general obligation to monitor which was clearly discarded in particular for social

[34] Same result stated by *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, 95.

networks by the CJEU in the SABAM v. Netlog case. The Court laid emphasis not only on Art. 15 E-Commerce-Directive rather than also stressing the impact on fundamental rights such as freedom of expression and data protection:

> „42 As paragraphs 62 to 68 of the judgment in Case C-275/06 Promusicae [2008] ECR I-271 make clear, the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.
>
> 48 Moreover, the effects of that injunction would not be limited to the hosting service provider, as the contested filtering system may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.
>
> 49 Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified (see, by analogy, Scarlet Extended, paragraph 51).
>
> 50 Moreover, that injunction could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned (see, by analogy, Scarlet Extended, paragraph 52).“[35]

Hence, any kind of monitoring obligation has to be construed in a restrictive manner – as required by a fair balance of fundamental rights and taking into account the multilateral effects not only on providers of social networks rather than all users affected.

Nevertheless, the German government invokes Recital 48 which reads:

> „(48) This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply which can reasonably be expected from and which are specified by national law, in order to detect and prevent certain types of illegal activities.“

However, this recital is difficult to bring in line with the prohibition of general monitoring obligations laid down in Art. 15 E-Commerce-Directive. Literally taken, recital 48 states the opposite of Art. 15, requiring host providers according to national law to take action in order to detect and prevent certain types of illegal activities. As Art. 15 E-Commerce-Directive is part of the legal obliging section of the E-commerce-Directive, any contradiction has to be resolved in

favour of the mandatory provisions of the legal obliging section. Hence, Recital 48 has to be read as an exception which can only take place if other requirements of the E-commerce-Directive has being met, such as the liability privileges of Art. 14. Thus, host providers may be required to take detecting measures etc. only after having obtained knowledge. Recital 48 may not be invoked in order to bypass mandatory provisions of Art. 14 (1) E-Commerce-Directive. The result – that providers have to remove or block access to information which is just being stored by a specific user - may not be a politically desired outcome today; however, it is one of the basic decisions enshrined in the E-Commerce-Directive.

### B. Notion of „copy“

Moreover, the notion of „copy“ remains unclear. If fake news or defamations are cited by other users, for instance in order to defend themselves or to correct the „faked news“, should it then be treated as a „copy“ or a statement on its own? Even it the illicit content is not cited, would it be a copy if another user just shares it with others? If every copy has to be removed threads of discussions would become incomprehensible, even scientific debates could not be any more followed such as discussions about the satiric quality of poems defaming political leaders etc.

These intrigue questions demonstrate that the approach of Art. 13, 14 E-Commerce-Directive to distinguish between information stored by a recipient and mirroring (and/or citing) information by others is clearly preferable.

### C. Summary

In sum, the obligation to delete or block access to all copies of an infringed content contravenes the prohibition of monitoring obligations in Art. 15 E-Commerce-Directive. It is also not covered by Art. 14 (1) E-Commerce-Directive which refers to information stored by the recipient – and not to all copies of the information regardless who has stored or mirrored the information.

## VII. Scope of application – legal insecurity

### A. The planned Act

According to the reasoning of the German Government the act should be restricted „to the operators of large, influential social networks, instead of to all service providers as set out in the Telemedia Act [Telemediengesetz – TMG]“.[36] Moreover,

> „the draft does not cover media platforms that publish their own journalistic and editorial content. The definition of a social network includes both the exchange of content between

[35] CJEU 16.2.2012 – C-360/10 SABAM v. Netlog.
[36] Notification of the Act.

> users in a closed or 'gated' community, and the public distribution of content. A minimum size is provided for relatively small companies (start-ups)."

Thus, the planned act defines social networks in Sec. 1(1) as those information society providers

> „...who operate platforms in the Internet with an intention to make profit which enable users to share any kind of content mit other users or to make the content publicly available"[37]

Only platforms with less than 2 Mio users in Germany are exempted (Sec. 1(2) of the planned act).

### B. Compatibility with the E-Commerce-Directive

This broad definition raises concerns about legal certainty for information society providers and is not in line with the notion of information society providers which host information according to Art. 14 E-commerce-Directive. The definition of the planned act aims at social networks such as Facebook or Twitter but could be applied to any kind of service which enable users to exchange content. Hence, even E-Mail-services would be concerned as well as any kind of cloud computing platform. It would be sufficient that a user just shares his content outside the platform with other users by sharing a hyperlink or by just enabling them access to the platform – the definition unspecifically just requires an „enabling" of sharing content which could be done by any means of uploading content and then sharing it. For example, services such as dropbox would be affected as well as other sharing platforms – which do not have any effect upon public discussions etc.

Hence, taken literally there would be in the end no difference between host providers as referred to in Art. 14(1) E-Commerce-Directive and the planned German Act. Even though a provider probably could not have any knowledge of sharing activities of the users the planned German Act could apply – for instance, a cloud provider who stores content for his users would be faced to comply with the obligations of the planned German Act as the content stored in the cloud may be shared with other users.

Only if the notion of „enabling" in the planned German act can be construed in such a way that the platform itself has to offer sharing tools so that any „external" sharing activities are not concerned the definition will not cover all host providers of Art. 14(1) E-Commerce-Directive.

### C. Inequal treatment

However, even though the German act may be specified by a restrictive interpretation it is highly questionable why these platforms (with internal sharing tools) should be treated differently from

[37] Translation by the author.

other host providers. As the cases in copyright law have shown sharing activities could be done by a variety of business models, such as placing links to content stored on other servers (such as rapidshare).

Moreover, Art. 14(1) E-commerce-Directive does not distinguish between small and big enterprises. A distinction between small and big information society providers may be justified on grounds of defending public security and interests as platforms with a lot of users are more likely to affect the public discussion – as the US-elections and the debate about „fake news" etc. have shown. However, the German Act refers to a variety of criminal offenses which cover not only offenses against public interest or security rather than also more individual legally protected interests such as defamation. Hence, it is hard to justify a different treatment of small platforms which also endanger individual interests (as in cases of defamation etc.).[38] Thus, Art. 14(1) E-Commerce-Directive does not distinguish between offenses against public interests and individual interests (only between damages based upon civil law and other offenses). Moreover, Art. 14(1) E-Commerce-Directive applies to any kind of information society provider without regard to numbers of users or capital etc.

#### D. Summary

In sum, the definition in the envisaged Sec. 1 of the German Act deviates from Art. 14 E-Commerce-Directive and the notion of providers of information services. The E-Commerce-Directive treats small and big providers in the same way – in contrast to the planned act. Moreover, the privileges and also obligations of Art 14 E-Commerce-Directive apply to all kind of offenses and illegal activities – in contrast to the planned act.

## VIII. Data protection issues

### A. Disclosure of identity and other personal data in case of violation of „absolute rights"

#### 1. Range of disclosure

The proposed German act intends also to give victims of defamation a right to claim for a disclosure of the personal data, in particular data about the identity, of the defamer. The envisaged amendment in Sec. 14 (2) Telemediengesetz (Telemediaact) will allow providers to disclose these data (Bestandsdaten) to the victim, thus giving providers a justification to transfer personal data. Moreover, as sec. 15 (5) sentence 4 Telemediaact refers to Sec. 14 (2) Telemediaact a provider could also disclose all personal data which is related to traffic of the

[38] Same result in *Wimmers/Heymann*, Archiv für Presserecht (Journal = AfP) 2017, 93, 96

user to a third party. Neither Sec. 14(2) Telemediaact nor Sec. 15 (5) Telemediaact provide for certain procedures to comply with before data is being disclosed.

However, in contrast to the reasoning of the government the envisaged amendment embraces all kind of so-called „absolute rights“ without specifying them. Thus, according to German doctrine in tort law (to which the reasoning evidently refers, sec. 823 (1) German Civil Code (Bürgerliches Gesetzbuch) every violation of an „absolute right“ would justify then the disclosure and transfer of personal data of the presumed tort feasor. Hence, not only personality rights are covered by this provision rather than all kind of absolute rights, such as the so-called „Right to an established and functioning business“ (Recht am eingerichteten und ausgeübten Gewerbebetrieb) which has been developed by German courts on the base of Sec. 823(1) German Civil Code.[39] Moreover, any violation of property rights etc. would then be covered by the new clause justifying the provider to disclose personal data of the tortfeasor to the victim. Thus, the amendment reaches far wider than the envisaged improvement for defamed persons.

This wide range raises concerns with regard to data protection, in particular if such a disclosure of personal data for violation of any absolute right is still covered and justified by data protection rules such as the ePrivacy Directive (in future ePrivacy Regulation), the General Data Protection Regulation,[40] and European fundamental rights (proportionality test).

## 2. European legal framework

### *a) General Data Protection Regulation and ePrivacy Directive*

Any disclosure of personal data by a provider is considered by the GDPR as well as the ePrivacy Directive as a data processing action, Art. 4 (2) GDPR (disclosure by transmission). The CJEU also upheld for the former Data Protection Directive and the ePrivacy Directive that „communication of information which is stored by Telefónica constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46.“[41]

Hence, any disclosure has to be justified according to the principles of the GDPR as laid down in Art. 5 (1) and Art. 6. Thus, a disclosure of personal data of an injurer may be justified in particular according to Art. 6 (1) f) GDPR as third party interests are concerned. However, as Art. 6 (1) f) GDPR clearly states, a balance of interests between the third party and the data

---

[39] See for instance German High Federal Court (Bundesgerichtshof), 24.01.2006 - XI ZR 384/03, BGHZ 166, 84 (110) = NJW 2006, 830 Rn. 91; more references cf. Beckscher Online Großkommentar BGB/Spindler, § 823 Rn. 134 and following.

[40] As the GDPR will soon enter into force (2018) the Data Protection Directive is considered here only with reference to former decisions of the CJEU (ECJ).

subject has to be stricken („overriden by the interests“). Further, a provision justifying data disclosure has to take into account the fact that the data subject is a child.

Moreover, Art. 23 of the GDPR allows Member States to restrict Art. 5 GDPR and related rights and obligations in Art. 12 and 22 GDPR, in particular regarding „the prevention, investigation, detection or prosecution of criminal offences“ (Art. 23(1) d)) and (j) the enforcement of civil law claims. However, Art. 23 GDPR provides several limits to these national restrictions, first in Art. 23 (1) GDPR the respect of „the essence of the fundamental rights and freedoms“, flanked by a proportionality test. In addition, Art. 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“.

### *b) Influence of European Fundamental Rights*

These restrictions set up by the GDRP are underpinned by the European Fundamental Rights enshrined in Art. 7, 8 and 11 of the EU Charter of Fundamental Rights and as interpreted by the CJEU, in particular with regard to data retention and disclosure of personal data.

The case which is closest to the issue of disclosing personal data by host providers is the Promusica Case decided in 2008.[42] The court had to decide if European provisions require a disclosure of personal data by a telecommunication provider in order to enforce intellectual property rights. The court held that Art. 15(1) ePrivacy Directive and Art. 13 (1) of the Data Protection Directive as exceptions for Member States have to interpreted in the light of conflicting fundamental rights, in particular Art. 7 (right to respect for private life ) and 8 (right to protection of personal data) of the EU-Charta,[43] what the Court confirmed in later decisions as well, especially concerning social networks.[44] The Court explicitly required a proportionality test regarding disclosure of personal data.

Important are also the decisions of the CJEU regarding data retention, even though they are not directly related to disclosure of personal data rather than to data retention in general (on the national level); however, they lay emphasis on provisions that safeguard the interests of data subjects and clarifies the importance of fundamental rights in interpreting the ePrivacy Directive

---

[41] CJEU 29.1.2008 - C-275/06 – Promusicae Paragraph 45.
[42] CJEU 29.1.2008 - C-275/06 – Promusicae.
[43] CJEU 29.1.2008 - C-275/06 – Promusicae Paragraph 63 - 65..
[44] See also CJEU 16.2.2012 – C-360/10 SABAM v. Netlog.

as wall as the Data Protection Directive.[45] The Court once again stressed the need to interpret Art. 15(1) of the ePrivacy Directive (2002/58) in the light of fundamental principles of the ePrivacy Directive and fundamental rights and freedoms granted by the EU-charter.[46] The CJEU explicitly refers not only to data protection but also to the freedom of expression.[47] Limitations on these rights are only justified „with due regard to the principle of proportionality" and „only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others".[48] The Court stresses the interference of data retention with Art. 7, 8 of the EU-Charter as „very far-reaching" and „particularly serious" – if it „is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance".[49] In order to guarantee the data subject`s fundamental rights the CJEU establishes a set of criteria that has to be met by the legislation of the Member State.[50]

Of special interest for the envisaged German act and regarding the safeguards for individuals the Court insisted on a prior judicial control of data retention and access to this data.[51]

### 3. Data protection rules and Disclosure of personal data in the planned act

Thus, Germany may in principle entitle provider to disclose personal data to third parties such as the injured (defamed) victim in order to enable the enforcement of civil law claims, following Art. 15 (1) ePrivacy Directive as well as the restrictions provided by Art. 23 GDPR (which are alike to those of the Data Protection Directive (Art. 13) still in force).

However, as the CJEU clearly stated in the Promusicae-case these exceptions have to be balanced with the conflicting fundamental rights of affected users, taking in particular chilling effects on fundamental rights such as the freedom of expression carefully into account. Notwithstanding the fact that a disclosure of identity is not the same as a constant surveillance of behaviour of users it has to be acknowledged that if users constantly have to reckon with a disclosure of their identity to third parties only upon grounds of a complaint they might be severely deterred from participating in discussions, be it any subject. Moreover, as the German act does not distinguish between different rights even commercial rights such as giving marks to

[45] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige
[46] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 89, 93.
[47] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 92.
[48] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 94 with reference to CJEU 15.2.2016, N., C-601/15 PPU, EU:C:2016:84, Paragraph 50.
[49] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 100
[50] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 109 - 118.
[51] CJEU 21.12.2016 - C-203/15 and C-698/15 – Tele2 Sverige Paragraph 120 with reference to ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, §§ 77 and 80

the service or product of an enterprise may be invoked in order to disclose the identity of a consumer.

Moreover, according to the planned Sec. 14 (2) Telemediaact the disclosure of identity is being covered by a wide range of rights of third parties – which do not share all the same importance with regard to fundamental rights. For instance, commercial reputation is not closely related to human dignity as for individuals affected by defamation. Given this wide range of rights mentioned by the German Act it is highly questionable if this simple justification to disclose the identity of users (as provided in the planned Sec. 14(2) Telemedia Act) meets the criteria established in the data retention decision of the CJEU. Safeguards for the fundamental freedoms and rights have to be established by the national law, even more if we take into account the incentives for providers to comply too swiftly with claims for disclosure in order to avoid claims for damages or even fines.[52]

Hence, a clear cut set of criteria when personal data has to be revealed is necessary - and more important a mandatory prior judicial control before disclosing identity of persons.[53]

As a blue print for such a prior judicial may serve the provision of Sec. 101 (9) of the German Copyright Act which requires for any disclosure of personal data a prior judicial consent. On the European level Art. 8 (1, 3) of the Enforcement Directive[54] provides that any information on the origin and distribution of goods or services which infringe an intellectual property is provided upon judicial order, provided that these provisions apply without prejudice to other statutory provisions which „(e) govern the protection of confidentiality of information sources or the processing of personal data.“ Moreover, recitals 2 and 15 of the Enforcement Directive clearly state that freedom of expression and protection of personal data have to be respected.

Why disclosure of personal data by telecommuncation provider should be handled in a different (i.e. more protected) way in contrast to social networks can not be justified. Freedom of expression is concerned in a far reaching manner in both cases so that a judicial control prior to any disclosure is even more important than in cases of infringing intellectual property rights.

Thus, the crucial point refers to the establishment of safeguards in order to establish the balance of fundamental rights, hence, a prior judicial control. Thus, it should not be left to providers to decide to disclose personal data as – for instance – they may be „incentivized“ to disclose too

---

[52] See above V.B.2.
[53] See also *Feldmann* Kommunikation und Recht (Journal = K&R) 2017, 292, 294
[54] Directive 2004/48/EC of the European Parliament and of the Council of 29.4.2004 on the enforcement of intellectual property rights, OJ L 157 of 30.4.2004, corrigendum OJ L 16 of 2.6.2004.

rapidly identities of users as they could face damage claims of victims, in particular in cases of alleged violoation of commercial reputation.

#### 4. Summary

Given the chilling effects to communication by disclosure of personal data to third parties it is mandatory according to Art. 23 (1, 2) GDPR as well as EU Fundamental Rights (Art. 7, 8, 11 of the EU Charter) to introduce a prior judicial control bringing into balance concurring fundamental rights.

### B. Obligation to store data

Furthermore, Sec. 3(2) Nr. 4 of the envisaged German act obliges the provider to store the relevant illicit content for 10 weeks in Germany after its removal.

This obligation is – once again – in conflict with Art. 3 (2) of the E-Commerce-Directive as providers from other EU-member states have to operate servers etc. in Germany in order to comply with this obligation. Given the guarantees by the GDPR and the free movement of data inside the EU it is hard to conceive a justification for the obligation to store the relevant content in Germany. Such an obligation would clearly counter the efforts of the EU to remove data location requirements.[55] Moreover, the obligation to identify a responsible representative in Germany according to Sec. 5 of the envisaged act would suffice in order to inspect the relevant data.

[55] Cf. explicitly Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions „ Building a European Data Economy“, vom 10.1.2017 COM(2017) 9 final, here p. 5 and following