# Aiding and abetting liability for social media platforms in relation to 'image-based sexual abuse'

*a way around Article 14 (1) of EU Directive 2000/31?*

Sluiter, G.

**Publication date**
2021

**Document Version**
Final published version

Criminal law 17.12.2021 Göran Sluiter

# Aiding and abetting liability for social media platforms in relation to 'image-based sexual abuse' – a way around Article 14 (1) of EU Directive 2000/31?

Image-based sexual abuse (I-BSA), also known as 'revenge pornography', has a grave impact on its victims and can lead to feelings of fear, shame, humiliation, anger, sadness and depression, and in some cases even to suicide. There is thus every reason to have a robust investigative and prosecutorial policy in place to effectively deal with such cases. In the Netherlands, a new provision in the Dutch Penal Code, Article 139h, was inserted quite recently to better encapsulate the conduct of I-BSA, justified by the need for a focused penal provision on I-BSA on the basis of a need for a uniform framework, to do justice to victims and to send a strong signal to potential wrongdoers. Could social media platforms be held liable for aiding and abetting I-BSA?

**Introduction**

Image-based sexual abuse (I-BSA) can be described as the non-consensual disclosure of sexualized private images or videos. It is also known as 'revenge pornography', although this term is too restricted and based only on motive (revenge). Therefore, I-BSA appears to be the preferable terminology.

Sadly, I-BSA is a more and more frequent phenomenon, in which the internet, particularly a variety of social media platforms, such as Facebook, YouTube, Instagram or WhatsApp, play an essential role.[1] It can be safely said that in the non-digital age, this type of criminality hardly existed at all.

I-BSA has a grave impact on its victims.[2] It leads to feelings of fear, shame, humiliation, anger, sadness and depression; victims might even contemplate and in some cases commit suicide.[3] There is thus every reason to have a robust investigative and prosecutorial policy in place to effectively deal with cases of I-BSA. This requires, first of all, adequate penal provisions. In the Netherlands, a new provision in the Dutch Penal Code, Article 139h, was inserted quite recently to better encapsulate the conduct of I-BSA. Prior to this focused penal provision, other crimes were used to prosecute situations of I-BSA, such as defamation (Article 261 of the Dutch Penal Code) or fabrication and spreading of child pornography (in the case of minors, as penalized in Article 240b).[4] But these provisions fall short of addressing all instances of I-BSA.[5] The Dutch government justified the need for a focused penal provision on I-BSA on the basis of a need for a uniform framework, to do justice to victims and to send a strong signal to potential wrongdoers.[6]

Interestingly, in the legislative process very limited attention was payed to the role, and criminal liability, of social media platforms in cases of I-BSA.[7] This appears quite remarkable in today's modern day and age of digitalization, where the focus on legal responsibilities incumbent upon social media platforms is increasing.

This apparent lack of attention has much to do with a -relatively- old EU Directive on E-commerce (No. 2000/31), which excludes liability for an 'information society service' – a provider for information stored at the request of a recipient of the service, on condition that a. the provider does not have actual knowledge of illegal information, and b. the provider, upon obtaining such knowledge, acts expeditiously to remove the information.

In this blog post, I will offer a few thoughts on whether the mode of liability of aiding and abetting for social media platforms in the context of I-BSA could be considered to fall outside the scope of the immunity clause. Thereby, it could offer a pathway to criminal liability for social media platforms, for as long as the E-commerce Directive remains unrevised.

**Recent penalization of I-BSA – Article 139h of the Dutch Penal Code**

Article 139h of the Dutch Penal Code entered into force on 1 January 2020 and reads as follows:

*1. The following shall be punished by a term of imprisonment not exceeding one year or a fine of the fourth category:*

*a. he who intentionally and unlawfully creates an image of a person of a sexual nature;*

*b. he who has access to an image as referred to under a, while he knows or should reasonably suspect that it was obtained through or as a result of an act made punishable under a.*

*2. The following shall be punished by a term of imprisonment not exceeding two years or a fine of the fourth category:*

*a. he who makes public an image as referred to in the first paragraph, under a, while he knows or should reasonably suspect that it was obtained through or as a result of an act made punishable in the first paragraph, under a;*

*b. he who discloses an image of a person of a sexual nature, knowing that such disclosure may be detrimental to that person.*[8]

The provision penalizes the fabrication and possession of (or access to) sexual images, as well as making such images public. As follows from section 2 of the provision, making public carries double the penalty (2 years imprisonment) compared to fabrication and possession (1 year imprisonment). This makes sense, in light of the much graver harm to the victim in instances of making the images public.

Generally speaking, this new provision has been welcomed, and other Dutch publications offer a detailed analysis of the provision's content and scope.[9] Article 139h was also acclaimed from an international and comparative perspective, although it was argued that further improvements need to be made.[10]

Focusing on the role that social media platforms play in the dissemination of I-BSA, it would seem that under section 2 (a) of Article 139h, they are very much targeted to incur criminal liability. In fact, a social media platform is making a sexual image just as public as the individual who posts it. On top of that, the social media platform makes the image public, while it knows or should reasonably suspect that the image was created or obtained unlawfully.

Bearing in mind that the Netherlands provides for criminal liability for legal persons (Article 51 of the Penal Code)[11], one might expect to witness a strong focus on social media platforms in Dutch investigative and prosecutorial policy related to Article 139h (2) (a). But this is not yet the case.

In response to questions from members of Dutch parliament, addressing the issue of criminal liability of porn sites for I-BSA, the Minister of Justice referenced the E-commerce Directive as the reason hosting services cannot be held liable for content; the Minister hastened to add that hosting services have, however, a *moral* responsibility to keep their platform 'clean'.[12]

The question arises whether it would be correct to state that criminal liability for hosting services is prohibited under all circumstances.

**The 'immunity'-clause in article 14 (1) of EU Directive 2000/31 - is there a way around it?**

The E-Commerce Directive's immunity clause had a very important precedent in US Section 230 of the Communications Decency Act (1996).[13] Article 14 of the EU's Commerce Directive of 2000 offers a similar liability-protection.[14] Concerning hosted (illegal) material, it is afforded to 'providers of an interactive computer service' (US) or an 'information society service provider' (EU). Leaving the issue of precise definitional scope and reach aside, for the purpose of this blog post it suffices to mention that all social media platforms, as well as internet porn sites, fall within both definitions, and thus enjoy protection against liability for unlawful content they host and make public, in both the US and all EU countries.[15]

Section 230 and the E-Commerce Directive can be seen as the cornerstone of what is traditionally referred to as the 'freedom of the internet'.[16] This becomes especially clear in the introductory parts of the E-Commerce Directive, where reference is being made to the importance of freedom of expression and the various benefits of the internet. It will supposedly stimulate economic growth and investment in innovation by European companies, which in turn can enhance the competitiveness of European industry, provided that everyone has access to the Internet.[17] The benefits of 'the Internet' were also praised in the US context when adopting Section 230: 'The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity', and: 'The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.'[18]

After more than 20 years of worldwide internet practice and experience, we can conclude in hindsight that this lack of attention to the negative and criminal aspects of internet use seems quite naïve.[19] Together with the role of big technical companies ('Big Tech'),[20] which make huge profits with social media platforms, but take no or very little responsibility for their content, this has resulted in more and more criticism of both the E-Commerce Directive and Section 230.[21]

In the ongoing debate, the attention is not yet so much on criminal liability for 'Big Tech' when making unlawful content public, but rather on improving monitoring, i.e. ensuring that unlawful content can rapidly be taken down, and improving cooperation in the criminal prosecution of those individuals who have posted criminal content.[22]

It seems to me, however, that this focus is too limited. There is every reason to take steps in some scenarios to hold social media platforms criminally liable, such as for making I-BSA public. Especially when -new- penal provisions, such as Article 139h of the Dutch Penal Code, provide a very solid basis for this, and essentially find their origin in posting criminal content online.[23] After having enacted such a provision, it would be hard to explain as to why social media platforms/Big Tech should (continue to) enjoy any immunity from prosecution.

I realize there are also critics of increasing the liability of social media platforms, as it will inevitably interfere with freedom of speech and carries the risk that a handful of major players will effectively determine what can still be said, seen and heard online.[24] But I am not persuaded by their arguments, or rather: I find that their arguments are being outweighed by the current risks and harm occasioned by the position and role of social media platforms.

Let us start by taking a step back and consider the position and role of social media platforms within society. Compared to traditional media, such as newspapers, it is the speed and widespread nature of individual postings that may have triggered different perceptions on liability, apparently necessitating, at the time, this immunity. Clearly, any traditional newspaper *deciding* to publish I-BSA, or similar clearly unlawful content, can be subjected to criminal liability. It is interesting to pause on the matter as to why *not deciding* on publishing postings should reduce, or avoid all together, liability. In the distribution of risks and harms between victim, main perpetrator and social media company, it seems hard to justify that criminal liability would be limited to the individual posting criminal content, whereas the role of the platform is clearly essential in making the content public. It is even more difficult to continue to support immunity from prosecution of 'Big Tech', knowing that a. they have deliberately created a model of unfettered postings without proper monitoring and supervision; b. this business model has generated enormous profits, at times at the expense of victims of crime, such as hate-speech, or I-SBA. There is thus good reason to reconsider the immunity clause in the E-commerce Directive, as well as in Section 230.

A very recent judgement of the Texas Supreme Court against Facebook in a civil suit brought by victims of human trafficking, in the victimization of whom Facebook played a role, offers further support for the above views.[25] The Court held (by majority) that in the context of human trafficking, Section 230 does not "'create a lawless no-man's-land on the Internet' in which states are powerless to impose liability on websites that knowingly or intentionally participate in the evil of online human trafficking;" and that " [h]olding internet platforms accountable for the words or actions of their users is one thing, and the federal precedent uniformly dictates that Section 230 does not allow it,", but "[h]olding internet platforms accountable for their own misdeeds is quite another thing. This is particularly the case for human trafficking."[26]

In spite of recent trends to gradually erode liability from immunity, such as the Texas Judgement of June 2021, any development in abolishing or substantively restricting the immunity clause is likely to take time. Until then, one may wonder whether aiding and abetting liability could be imposed without violating the E-commerce Directive's immunity clause. The argument in favor of using aiding and abetting liability would be that this form of accessory liability should be distinguished from principal liability for the main crime, which pertains to an individual disclosing, online, unlawful information or images. The social media platform can be considered to have *facilitated* the element of the crime of I-SBA, as defined in Article 139h of the Dutch Penal Code, of *making* sexual images *public*. Thus, social media platforms make the difference between disclosing I-SBA to a few individuals, and making this public for an audience of hundreds to millions of individuals. Looking at the wording of Section 14 (1) of the E-Commerce Directive, which provides for immunity in respect of liability for *storage of information*, one could subsequently argue that the social media platform is, as an aider and abettor, not held criminally liable for storing illegal information as such, but for assisting someone in making such information public by providing its services. The liability-paradigm would thus shift from *storage*, to *assistance in making public*, and could arguably be used in Dutch prosecution of Article 139h without violating Section 14 (1) of the E-Commerce Directive.

On the one hand, this paradigm-shift in liability may appear artificial, because liability can still be traced back to exactly the same content, an instance of I-SBA. On the other hand, it is something worth exploring, because a. it conceptually resonates with aiding and abetting-liability as having its own position, including own time and place of commission in substantive Dutch criminal law;[27] b. it would fill the long overdue liability gap for social media platforms; c. especially the crime of I-SBA, as punished by Article 139h, is by and large triggered by the role social media play in the dissemination of sexual images. It is in this respect worth mentioning that the abovementioned Texan Supreme Court Judgement also makes a carve-out of the immunity clause in respect of a social media platform's own acts/misdeeds, which further supports making the distinction between the acts of the principal perpetrator and the role of social media as accomplice, through aiding and abetting.

If the Dutch prosecution service were to pay more attention to social media in the investigation of violations of Article 139h, and assuming this would be consistent with the E-Commerce Directive, the question arises under what circumstances social media should attract aiding and abetting-liability under Dutch criminal law for assistance in making I-BSA available to the wider public.

The answer to this question depends first of all on the fulfilment of the criteria for criminal liability for legal persons, as they have been developed in Dutch case law, generally known as the '*Drijfmest*'-criteria (the assigned name to the landmark Supreme Court decision on this issue).[28] These criteria in essence come down to a system of reasonable attribution of acts to a company, based on a number of factors such as whether or not the act was part of the ordinary business operation or whether the company had control over the act or has accepted the act.[29] Second, it needs to be determined how knowledge -under Dutch law: actual knowledge or a should have known-standard- should be construed in this unique context of a social media platform assisting in the commission of the crime of making I-SBA public.

It seems to me that in respect of both the '*Drijfmest*'-criteria and the construction of a company's knowledge of its assistance in the crime of making I-BSA public, a number of factors will be relevant. In this regard, one can think of having strict user's conditions in place prohibiting posting criminal content, especially I-BSA; the existence of adequate monitoring systems in respect of I-BSA;[30] the existence of effective mechanisms to remove criminal content rapidly; and the availability of adequate cooperation mechanisms with the police and judicial authorities more broadly in fighting unlawful content. These due diligence-factors should, arguably, even be more stringent in case of platforms with a significantly higher risk of making I-BSA public, such as porn sites.

If a social media platform were to perform very poorly on various aspects of due diligence in preventing and/or addressing postings containing I-BSA, there is a compelling argument to be made that a. the assistance in commission of Article 139h (2) can be reasonably attributed to the social media company concerned; b. this assistance has been provided while the company should have known they were thus contributing to the commission of the crime as provided for in Article 139h (2).

It will need to be established through case law to what degree the due diligence mechanisms that are presently in place at social media platforms will be sufficient to avoid criminal liability for aiding and abetting I-SBA crimes. Looking, for example, at Facebook's relevant policies, it can be noticed that they 'default to removing sexual imagery to prevent the sharing of non-consensual or underage content.'[31] However, there is nothing to suggest that Facebook prevents I-BSA from being posted to begin with. In addition, it is unclear how rapid and effective the policy of removing sexual imagery is in practice. Therefore, I am not persuaded that in light of Facebook's present policies and due diligence practices, it would fall short of meeting the threshold of aider and abettor to Article 139h crimes.

In many respects, the new crime of Article 139h offers an excellent starting point to hold social media platforms criminally accountable for their assistance in the commission of I-BSA. As said earlier, this new crime was developed especially to respond to I-BSA divulged via social media platforms. This type of criminality also entails immediate and significant harm to individual victims, which is exacerbated with any minute the content continues to be available online. The harm can even become irreparable, when I-BSA is copied and reproduced elsewhere, and the images continue to be available somewhere online for many years.[32] In my view, there is no reason for an unconditional and continuing application of the immunity clause, as provided for in the EU's E-Commerce Directive and Section 230, in respect of social media platforms' role in facilitating I-BSA.

My suggestion would be for the Dutch prosecution service to start with a suitable test-case involving a social media platform's role in facilitating I-BSA. In case of doubts as to whether aiding and abetting-liability would be consistent with the EU E-Commerce Directive, a preliminary reference can be submitted to the European Court of Justice (CJEU), to resolve interpretation of EU law, pursuant to article 267 of the TFEU.

Such a case, including a possible reference to the CJEU, may be seen as cumbersome and time-consuming, but victims of I-BSA deserve a robust prosecutorial policy in respect of this new crime in the Dutch criminal justice system. Without inclusion of social media platforms in the investigation and prosecution of Article 139h, the provision will be deprived of much of its effect and potential.

**Conclusion**

The Netherlands has recently taken a laudable step in fighting I-BSA, through adoption of Article 139h, which focuses on its penalization. Both the definition of the crime and the timing of and reason for its enactment make clear that the provision is, to a large degree, a response to the role of social media platforms in making I-BSA available to -potentially- hundreds of millions of users worldwide.

Bearing in mind the content, as well as the object and purpose of Article 139h, this blog post has addressed the question how social media platforms can be held criminally liable for their role in making public I-BSA.

My position on this matter is, first of all, that the main obstacle to prosecution of social media platforms for violations of Article 139h, the EU E-Commerce Directive's immunity clause, is outdated and should be revised.

As long as such a revision has not taken place, aiding and abetting-liability under Dutch criminal law for social media platforms could be a way around the immunity clause, and could serve to fill a long overdue liability gap. Focusing on aiding and abetting liability would shift the liability-paradigm from *storage* (to which the immunity clause in the E-Commerce Directive applies) to *assistance in making* I-BSA *public*, and could arguably be acceptable from a EU-perspective.

Under Dutch criminal law, aiding and abetting liability for social media platforms which facilitate individual perpetrators in making I-BSA public can be reasonably attributed when social media platforms do poorly on various aspects of due diligence.

In order to materialize such liability in practice, it is suggested that the Dutch prosecution service initiates a first (test-)case against a social media platform, even if this would entail submitting a preliminary reference to the CJEU to obtain clarity on EU law. The bottom line is that victims of I-BSA deserve a broader investigative focus, including social media platforms, and that the new provision, Article 139h, loses much of its effect when social media platforms remain untouched.

*The author would like to express his gratitude to Georgina Howe for -additional- research, comments and editing.

[1] In addition to being published on social media platforms, the focus of the present blog post, I-SBA also can be made public via pornsites. Illegal material being published on these sites has already resulted in a reaction from credit card companies, see https://www.cbc.ca/news/canada/montreal/mastercard-ends-card-use-on-pornhub-1.5836289.

[2] See M. Goudsmit, 'Criminalising Image-Based Sexual Abuase: An Analysis of the Dutch Bill against 'Revenge Pornography', *Ars Aequi*, June 2019, p. 443.

[3] Ibid.

[4] See, for example, Court of Appeals of Amsterdam, 20 June 2020, ECLI:NL:GHAMS:2020:1951; Supreme Court, 3 December 2013, ECLI:NL:HR:2013:1556.

[5] See, in more detail, S. Ourahma, ''Wraakporno' in het strafrecht: een analyse van rechtspraak en recente wetgeving over ongewenste publicatie van seksueel beeldmateriaal', *Delikt en Delinkwent*, 2021/35.

[6] Explanatory Memorandum, 2018–2019, 35 080, nr. 3, p. 4, available at https://www.tweedekamer.nl/download s/document?id=12264179-6eb7-4492-afd9-6b974974c1bd&title=Memorie%20van%20toelichting.pdf.

[7] The exception in this regard is the Dutch Bar Association (DBA) in its advise on the proposed penal provision. The DBA found there was a lack of attention to criminal accountability for 'Internet Service Providers' in the legislative process, and raised a few scenarios in which it alluded to potential criminal liability for Facebook and Whatsapp; see Advice of 11 June 2018, pp. 9-10, available at https://www.tweedekamer.nl/downloads/document ?id=666eae 22-ea36-46d0-a3c8 9dcfa73c2a4e&title=Advies%20Nederlandse%20Orde%20van%20Advocaten. pdf.

[8] Own translation, because to my knowledge, there is not yet an official translation of this quite recent addition to the Dutch Penal Code.

[9] M. Berndsen, Een verbod op wraakporno. Het nieuwe artikel 139h Sr kritisch beschouwd, *Nederlands Tijdschrift voor Strafrecht* 2020/24 70-76; J.M. ten Voorde, Heimelijk of zonder toestemming? Op zoek naar de juiste grondslag van de nieuwe strafbaarstelling van misbruik van seksueel beeldmateriaal, *Delikt en Delinkwent* 2019/2 84-97; S. Ourahma, supra note 5.

[10] See https://www.secjure.nl/2021/01/04/criminalizing-revenge-pornography/.

[11] Art. 51 provides as follows:

1. Offences may be committed by natural persons and legal persons.
2. If an offence is committed by a legal person, criminal proceedings may be instituted and the punishments and other measures provided for by law may be implemented where appropriate:
3. against the legal person; or
4. against those who ordered the commission of the offence, and those who were in control of such unlawful behaviour; or
5. against the persons mentioned under (1) and (2) together.
6. For the purpose of the application of the above paragraphs legal persons shall be deemed to include a unincorporated company, a partnership and a special fund.

[12] Answers to Questions of Member of Parliament, 28 August 2020, p 4, available at https://www.google.com/ url?sa=t&rct =j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiwtbCV8MT0AhWRiv0HHarKDVUQFnoEC BQQAQ&url=https%3A%2F%2Fwww.rijksoverheid.nl%2Fbinaries%2Frijksoverheid%2Fdocumenten%2Fkamerstukken%2F2020%2F09%2F28%2Fantwoorde kamervragen-over-non.

[13] This provision reads, in relevant part, as follows:

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

[14] This provision reads as follows:

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or(b) the provider, upon obtaining such knowledge or aware- ness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

[15] For other countries, see https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability.

[16] See UNESCO Series on Internet Freedom, *Fostering Freedom online: the Role of Internet Intermediaries* (2014) at 40-43.

[17] Preambular paragraph 2 of the E-Commerce Directive.

[18] Findings 3 and 4 of Congress, Section 230 (1996).

[19] See also this statement in a very recent Texas Supreme Court Judgement, holding that Section 230 does not provide for full immunity in cases of human trafficking: 'The internet today looks nothing like it did in 1996, when Congress enacted section 230.', available at https://search.txcourts.gov/RetrieveDocument.aspx? DocId=8226&Index =%5c%5c10.20.4.7%5cTamesIndexes%5csc%5cOpinion)

[20] See Collin's definition of Big Tech, available at https://www.collinsdictionary.com/de/worterbuch/englisch /big-tech (last accessed on 29 November 2021).

[21] See as far as the debate in the US is concerned, e.g., https://www.cnbc.com/2020/02/19/what-is-section-230-and-why-do-some-people-want-to-change-it.html. and https://www.latimes.com/business/technology/story/2021-10-14/big-tech-faces-new-bills-on-liability-and-competition-in-the-u-s; In the EU context, see https://www.huffpost.com/entry/limited-liability-for-the-net-the-future-of-europesb58ecd2cfe4b0145a227cb846.

For current relevant developments in Australia, e.g. https://www.wsj.com/articles/australia-seeks-to-make-social-media-firms-liable-for-users-defamatory-comments-11638109003 and https://www.reuters.com/world/ asia-pacific/australia-introduce-new-laws-force-media-platforms-unmask-online-trolls-2021-11-28/,

[22] See e.g. https://www.atlanticcouncil.org/blogs/new-atlanticist/the-emerging-eu-regulatory-landscape-for-digital-platform-liability/; and https://blog.chavannes.net/2019/05/regulation-of-online-platforms-in-the-european-union-the-state-of-play/.

[23] See the Explanatory Memorandum (supra note 6), p. 3: 'The digitalization of society is accompanied by opportunities to produce and distribute visual material, including intimate sexual imagery, anywhere and at any time.' (own translation)

[24] See e.g. https://www.theparliamentmagazine.eu/news/article/a-losing-game-moderating-online-content-fuels-big-tech-power.

[25] Judgement of 25 June 2021, available at https://search.txcourts.gov/RetrieveDocument.aspx?DocId=8226&Index=%5c%5c10.20.4.7%5cTamesIndexes%5csc%5cOpinion.

[26] Ibid.

[27] Supreme Court, 15 March 1943, NJ 1943, 375.

[28] ECLI:NL:HR:2003:AF7938 (Drijfmest).

[29] Id., par. 3.4.

[30] I realise that such a factor may be regarded by some as inconsistent with another provision in the E-Commerce Directive, namely article 15, which stipulates the EU States may not impose a general obligation on internet service providers to monitor information from users they store or transmit. Leaving aside the issue that this provision appears quite outdated in light of the risks and perils of modern-day internet, one can argue that the monitoring obligation that can be a factor in attributing criminal liability is not one of a general nature, but restricted to monitoring, filtering, obvious criminal content.

[31] See https://transparency.fb.com/policies/community-standards/adult-nudity-sexual-activity/.

[32] On the slightly related issue of the 'right to be forgotten', i.e. to have information no longer be available online, see a series of ECtHR of cases, the most recent of them being *Biancardi v. Italy* (application no. 77419/16), 25 November 2021, available at https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22 document%22],%22 itemid%22:[%22001-213827%22]}.

Criminal law | Aiding and abetting | The Netherlands | Social Media

## Related articles

- Could companies in the Netherlands face criminal liability for 'facilitating' 8kun?
- Recent Domestic Developments on Corporate Criminal Assistance in Atrocity Crimes
- The Cases of Kouwenhoven and Poch and the Fine Line Between Guilt and Innocence for Assisting in the Commission of War Crimes
- Autonomous Weapons Systems and the Liability Gap, Part One: Introduction to Autonomous Weapons Systems and International Criminal Liability
- Are Social Media Algorithms "Passive Nonfeasance"? What Twitter v. Taamneh Got Wrong
- Secondary Liability and Terrorism – Spill-over to other international crimes?

## Tag cloud

accomplice liability 3 | Aiding and abetting 11 | Alien tort statute 3 | Arms export 9 | Autonomous Weapons 2 | banking and finances 1 | BNP Paribas 1 | Business and human rights 20 | bystander liability 1 | Canada 1 | Child slave labour 2 | China 2 | Civil law 9 | cobalt 1 | Command responsibility 1 | Consequentialism 1 | constructive knowlegde standard 1 | Corporate criminal liability 10 | crime of aggression 2 | Criminal law 25 | Criminal membership 2 | DARS 3 | Data Protection Act 1 | death penalty 1 | Democratic Republic of Congo 1 | Doctrine of adoption 1 | Domestic law 9 | DPA 1 | Dual-use 1 | Due diligence 11 | ECHR 4 | Ecocide 2 | ECtHR 5 | Europe 8 | export licencing 2 | Facebook 1 | France 3 | Gemmeker 1 | Germany 1 | Guiding principles 4 | Holocaust 1 | ICC 6 | ICTY 1 | International Humanitarian Law 4 | JCE 1 | Jurisdiction 5 | Kant 1 | MLA 1 | Mutual legal assistance 1 | Myanmar 1 | Netslé 1 | OECD guidelines 1 | Parent company liability 4 | participation in a venture 1 | police brutality 1 | Private international law 1 | Public scrutiny 1 | Russia 5 | Social Media 3 | Soering liability 1 | South America 1 | State responsibility 10 | State-owned enterprise 1 | Strict liability 1 | Sudan 1 | Supply chain 7 | Syria 5 | Technology 2 | Terrorism 2 | The Netherlands 4 | Tort law 8 | U.S. Supreme Court 2 | Ukraine 4 | UNGPs 1 | United States 5 | Westerbork 1 | World War II 1