Dr. Anna Zanathy

One's right to image on online platforms,

or whether the European platform regulation would have protected Hillary Clinton from the #Pizzagate story

Thesis Book

Supervisor:

Dr. Gergely Gosztonyi

habilitated associate professor

Eötvös Loránd University

Doctoral School of Law

Budapest, 2025

1 OBJECTIVES OF THE DOCTORAL DISSERTATION AND METHODOLOGY

The aim of this thesis is to assess whether the current (European) regulatory framework governing the internet and digital services provides effective protection in practice for individuals whose right to their image is infringed. In order to answer this main research question, the following sub-questions are examined in detail in my thesis:

a) What is the current legal approach to regulating the internet and the digital services provided over it?

b) Did the fake picture of Hillary Clinton circulated as part of the #PizzaGate conspiracy theory violate the former Secretary of State's right to be photographed?

c) Does the DSA provide effective protection for Hillary Clinton, whose right to image has been infringed, either by holding the platforms that stored and disseminated the fake image to the public liable or by imposing due diligence obligations on these platforms?

1.1 The #PizzaGate conspiracy theory

The #PizzaGate conspiracy theory started to spread in autumn 2016, after the FBI announced it was reopening its investigation into Hillary Clinton's emails. The investigation uncovered data and emails from Anthony Weiner's mobile phone that originated from Clinton's private server. A few days later, an anonymous tweet claimed that Clinton and her close associates were involved in a paedophile ring. These false allegations went viral on social media (Twitter, Reddit, 4chan) at lightning speed. At the centre of the theory was a Washington, DC pizzeria, Comet Ping Pong, which the Clinton campaign had previously used for fundraising.

On the forums of Reddit and 4chan, pizza and the term "cheese pizza" have been identified as child pornography, as the English abbreviation ("c.p.") refers to "child pornography". The owner of the Comet Ping Pong pizzeria, James Alefantis, and several Democratic politicians have been accused of running a satanic paedophile network out of the restaurant's basement, where children are held and ritual abuse takes place.

The lies escalated to the point that on 4 December 2016, American Edgar Maddison Welch, armed with a rifle, walked into the Comet Ping Pong, pointed his gun at employees and shot

several times into a closed door. A police investigation revealed that the gunman was motivated by the #Pizzagate hoax and wanted to investigate alleged child trafficking .[1] Welch personally admitted that he found no evidence of illegal activity.

Nevertheless, the theory lived on. In 2017, protests took place outside the White House demanding an investigation into PizzaGate, and in 2019 a young man set fire to the pizzeria.

In August 2020, a digitally altered (in this case, doctored) photo of Hillary Clinton began circulating on Facebook and other social networking sites.[2] In the picture, Hillary Clinton is shown wearing a tracking anklet on her ankle while walking her dog on the beach (Figure 1). The fake picture of the former US Secretary of State has been linked to the #PizzaGate conspiracy theory, suggesting that she is under house arrest on child trafficking charges.[3]

Figure 1: Digitally altered image of Hillary Clinton to support #Pizzagate[4]

[1] N/A: Washington gunman motivated by fake news 'Pizzagate' conspiracy. The Guardian, 5 December 2016, https://www.theguardian.com/us-news/2016/dec/05/gunman-detained-at-comet-pizza-restaurant-was-self-investigating-fake-news-reports

[2] N/A: Fact check: Altered photo shows ankle monitor on Hillary Clinton. Reuters, 17 August 2020, https://www.reuters.com/article/idUSKCN25D1UW

[3] Ibid.

[4] https://www.facebook.com/photo?fbid=3007323229329585&set=a.1237089659686293

The original photograph (Figure 2) of Hillary Clinton walking her dog without a tracker on the beach in Amagansett, New York, with Bill Clinton and a Secret Service agent, was taken by Matt Agudo for INFphoto.com in 2014. The original photo was digitally altered (manipulated) to include a tracking device.

Figure 2: The original photo of Hillary Clinton[5]

Although it's been nearly 10 years since the #Pizzagate conspiracy theory first appeared online, it hasn't disappeared from social media. On the contrary. With the proliferation of several - recently released - technologies or apps that allow users to create any kind of content (fake or not) using artificial intelligence technology, the fictional stories around #Pizzagate have become increasingly crazy and the supporting "evidence" more and more

[5] https://i.dailymail.co.uk/i/pix/2014/08/08/article-2720212-205E771500000578-434_634x762.jpg

realistic. For example, in November 2023, a video generated by artificial intelligence was circulating on TikTok in which a man talked about US President Donald Trump's designation of Guantanamo Bay, Guam and Tierra del Fuego for military trials of Hillary Clinton and John Podesta, among others.[6]

Despite the above, based on publicly available information, it appears that Hillary Clinton has never taken legal action for defamation against the creator of the fake image, those who distributed it, or the online platforms on which it was shared.

1.2 Methodology

In order to answer the first research question, the thesis primarily employs historical-descriptive and analytical methodology. Subsequently, to examine the second and third sub-questions, the thesis uses a hypothetical case study method: it examines the legal implications of the dissemination of a fake image of Hillary Clinton within the framework of the #PizzaGate conspiracy theory, as if it had taken place in Europe, and specifically in Hungary.

The #PizzaGate conspiracy theory was selected as the case study forming the basis of the thesis on the following grounds:

a) despite the fact that the #PizzaGate conspiracy theory is clearly absurd and untrue, it is still subject of public debate in the U.S. and has a significant number of followers;

b) the #PizzaGate conspiracy theory is one of the few pieces of fake news that has had serious consequences in real life;

c) the #PizzaGate conspiracy theory can be examined as one of the most documented fake news;

d) numerous deepfake videos have been produced to support the #PizzaGate conspiracy theory.

[6] N/A: Fact Check: Hillary Clinton, Podesta were not tried by US military at Guantanamo. Reuters, December 6, 2023, https://www.reuters.com/fact-check/hillary-clinton-podesta-were-not-tried-by-us-military-guantanamo-2023-12-06

1.2.1 Methods of data collection

For this thesis, two major data sets were needed:

a) Factual background to the #Pizzagate conspiracy theory. As the original content shared under the #Pizzagate conspiracy theory is no longer available online, it was necessary to establish the factual background on the basis of newspaper articles.

b) Data on the technical background of the platforms. This information was gathered from (i) explanatory and educational videos of the platforms; (ii) a personal interview with Robert van Eijk, Chief Supervisor of the Dutch Data Protection Authority; (iii) my personal observations of the use of the platforms concerned; and (iv) my experience as a lawyer in the Netherlands with respect to privacy collective action initiated against large social media sites.

1.2.2 Analysis and interpretation

In my legal analysis of the distribution of the manipulated photo of Hillary Clinton within the context of the #PizzaGate conspiracy theory, I followed the following logical steps:

a) I identified the applicable legislation that regulates the legal issue in question at the European and Hungarian level (e.g. international treaties, directives, regulations, laws).

b) If the provisions of the identified legislation were not clear or sufficient, I also looked at the case law interpreting it (e.g. the case law of the ECtHR, the CJEU, the Hungarian courts and the AB).

c) If the interpretation of the law was still not clear, I relied on secondary sources (e.g. academic literature, books, case studies, commentaries) to find the answer to the legal question.

2 SECTION OF THE DOCTORAL THESIS

The doctoral thesis addresses the research questions in the following structure:

a) Chapter 1 outlines the thesis's objectives and methodology, as well as presenting the #PizzaGate conspiracy theory in detail.

b) Chapter 2 provides a brief summary of the creation and development of the internet to provide context for the analysis.

c) Chapters 3 and 4 address the first research sub-question. Chapter three presents competing theories of internet governance and their respective advantages and disadvantages. Chapter four details the history of platform regulation and the main issues and challenges.

d) Chapters 5 and 6 aim to answer the second research sub-question. Chapter 6 summarizes the place of the right to image in the legal system, its material and personal scope, how this right can be infringed, and what are its typical limits (e.g. individual consent, public figures and public pictures). Chapter 7 seeks to answer the question of how, or indeed whether, the right to image prevails on the internet. To answer this question, Chapter 7 examines (i) the lack of consent required for uploading and distributing photos on social media; and (ii) deepfakes from the perspective of the right to image.

e) Chapter 7 examines the liability of hosting service providers for unlawful content they host, based on the previous EU legislation, Directive 2000/31/EC Directive on electronic commerce (E-Commerce Directive). The chapter specifically discusses the case law of the Court of Justice of the European Union (CJEU) adopted under the E-Commerce Directive. Chapter 7 also explains the reasons why the E-Commerce Directive has become obsolete and why a need has arisen to adopt a new law, the 2022/2065 EC Regulation on the Digital Services Act (DSA).

f) The aim of Chapter 8 is to examine whether platforms can be held liable for hosting and disseminating unlawful content under the DSA and if so, how this fits with the framework of freedom of expression. This chapter addresses the following: (i) the purposes of the DSA; (ii) the definition of platforms under the DSA; (iii) the general conditions for intermediary service providers to be exempt from liability; (iv) the rules for platforms to be exempt from liability under the DSA; (v) the conditions

under which platforms' freedom of expression may be lawfully restricted under the European Court of Human Rights' case law.

g) Chapter 9 discusses the due diligence obligations imposed by the DSA on platforms that are most relevant to the Hillary Clinton case at hand, namely: due diligence obligations adopted with respect to platforms' content moderation and use of recommender systems. I n Chapter 9, I provide a detailed discussion of the steps involved in content moderation and the concept of recommender systems. I also address the requirement for transparency regarding recommender systems (Article 27 of the DSA) and the right to opt out of profiling-based recommender systems (Article 38 DSA).

h) Chapter 10 addresses the question of whether the liability of platforms under the DSA, and the due diligence obligations adopted in relation to recommender systems, would have offered Hillary Clinton effective protection against the dissemination of her manipulated image and the spread of the #Pizzagate conspiracy theory.

i) Finally, in the last chapter, I summarised the main findings of my thesis. I concluded that the current method of internet regulation is inadequate for ensuring the right to image online, effectively protecting individuals whose right to image is violated and remedying the negative consequences of the echo chambers created by recommender systems. In the final chapter, I address the question of what alternative means of internet regulation would allow these objectives to be achieved.

3 RESULTS OF THE DOCTORAL THESIS

3.1 Mass violations of the right to image on the internet

In my thesis, I have demonstrated through several examples how the right to privacy cannot prevail on the internet.

I demonstrated that, despite 14 billion images being shared daily via social media, social media sites' attitude towards individuals' rights over their own images is fundamentally flawed. My conclusion is based on the following findings.

a) Firstly, I found that the tagging feature on social media sites such as Facebook, YouTube, Instagram and TikTok means that the audience for a shared photo depends primarily on the settings of the person who created the post. Therefore, if the user has set the photo to be public, meaning it can be viewed by anyone, the tagged person cannot reduce the audience. The autonomy of the person who has been tagged extends only to the extent of public access to the photo in question on their own profile page. Moreover, on Facebook, this autonomy is limited: the person sharing the content can restrict the audience of the uploaded image to their friends only, potentially overriding the tagged person's decision to share the content on their profile. Social media sites therefore primarily place the decision on how the image is used (i.e. shared) in the hands of the sharer. However, this approach contrasts sharply with the essence of the right to image, whereby the data subject has the right to determine how their image is used. [7] Under the two-way protection of the right to image, no one can be forced to allow their image to be disclosed to a public other than the one they wish.[8]

b) Secondly, I found that the right to image is massively violated by the practice of sharing photos of individuals without consent on social media sites such as Facebook, YouTube, Instagram and TikTok. As a general rule, anyone can upload a photo of anyone, regardless of whether they are a user or not, or whether they are a friend or not. None of these require the consent of the person concerned, and anyone can be tagged.

[7] Lenkovics Barnabás – Székely László: Magyar polgári jog. A személyi jog vázlata. Budapest, 2001, p. 126.
[8] Törő Károly: Személyiségvédelem a polgári jogban, Budapest, 1979, p. 520.

On the other hand, deepfakes, which are another typical case of infringement of the right to image, were also examined in part. Deepfakes are fake videos, images or sound recordings created using deep learning and artificial neural networks to create a convincing false impression that the fake content has actually taken place[9]). In this context, I came to the following conclusions in my thesis:

a) Although there is currently no case law that explicitly states that content produced using deepfake technology is covered by the right to image, it can reasonably be argued by analogy with existing case law that such content is covered by this right. Indeed, there are several judgements in which the court has analysed the legal consequences of facial reproduction. For example, in its judgment no. Pfv.21.267/2018/17, the Curia sought to answer the question of whether the plaintiff's right to image had been infringed by the defendant mounting the plaintiff's face on a nude female body performing a sexual act without her consent.[10] Similarly, in its decision no. Pf.21.277/2008/3, the Budapest Court of Appeal analysed a case in which a woman's face had been copied onto a man's body. In both cases, the court ruled that the right to image extended to include forged photographs and found an infringement of this right.

b) There are two types of infringement of the right to image by deepfake: (i) using an existing image to create a deepfake, and (ii) tampering with the original image. An example of the former is using any photograph of Hillary Clinton to create a portrait of a middle-aged, blonde, Caucasian woman. The latter category includes the image of Hillary Clinton examined in detail in this paper, for example.

c) It follows from the Hungarian case law[11] that the unauthorised use of existing photographs of individuals for the purpose of creating a deepfake (e.g.: analysis by artificial intelligence for the purpose of creating similar photographs or copying of uploaded photographs by artificial intelligence) constitutes an infringement of the right to image under Article 2:48 (1) of the Civil Code. The requirement of "purpose limitation" of the use of a photograph (i.e. that a photograph lawfully taken and used for a specific purpose may be used only for another purpose compatible with that

[9] Mráz Attila: Deepfake, demokrácia, kampány, szólásszabadság. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Budapest: Ludovika Egyetemi Kiadó, 2022, p. 249.
[10] Pfv. 21.267/2018/17.
[11] BH 1995/632 and Pfv. 20.801/2007/7, Pfv. 20.801/2007/7, BDT 2015.3312 (Pfv. 20.092./2013/2).

purpose) is also applicable to photographs of public figures according to the case law.[12]

d) Another example of infringing the right to the image through deepfakes is falsifying an existing image. While there are no judgements analysing deepfake videos or images from the perspective of an individual's right to reproduction, several judgements have analysed the distortion, montage or falsification of original photographs under Article 2:42 and 2:48 of the Civil Code. For example, in its decision no. PJD 2019.18 (Pfv. 20.955/2017/9), the Curia ruled that publishing an image of an individual in a way that distorts or misleads the viewer violates Article 2:48 of the Civil Code.[13] While the facts of this case show that the defendant did not modify the image in question using technical means, merely cutting it from an existing video to support an inference that could not be drawn from the original recording, this approach can still be applied to the legal analysis of deepfakes. Therefore, any deepfake that falsifies the original image infringes the right to image. This approach is generally applied by the judiciary to the falsification of images of public figures. For instance, the District Court of Budapest ruled that the right to image of a performer's family members had been infringed because the defendant had placed their faces on the bodies of others without consent and published the images in a newspaper. Recognising the applicants' status as public figures, the court stated in its judgment that the applicants had agreed to have their images published in various newspapers in their capacity as public figures. However, the Court also held that the applicants had not consented to being ridiculed or humiliated simply by appearing on or promoting a programme.[14] Nevertheless, the right of public figures to be portrayed is not absolute, and in certain cases, their portrayal may be altered, distorted, or falsified. Several court judgements have also addressed this issue.[15] For instance, the Budapest Court of Appeal ruled that the right to be photographed of a public figure whose face was incorporated into a photomontage bearing the caption 'Together on the Liberal Mafia' had not been violated. In that decision, the court focused particularly on the relationship between the text and images on the

[12] PJD 2016.21. (1.Pfv. 21.458/2015/4/II.) BH 2006.282 (Pfv. IV. 21.553/2004) BDT 2020.4222 (Pfv.III.20.010/2020) BH 2006. 282 (Pfv. IV. 21.553/2004).
[13] PJD. 2019.18 (Pfv. 20.955/2017/9) See also: BH.1994.127 (Pfv. IV. 21 327/1993) and BH 1997.578 (Pfv. IV. 20.118/1996).
[14] Pf. 21.277/2008/3; P. 20.239/2008/3.
[15] Pf. 20.750/2021/15 and Pf. 20.537/2014/3.

photomontage, which both parties considered to be legitimate expressions of opinion.[16] In the same case, the Curia added that 'the grouping of the photographs in the montage was made in the context of the specific public activities of the individuals in a particular government term, which, together with the captions, constituted a specific form of expression of opinion'.[17] Therefore, despite the negative content of the montage, the first applicant, a former minister, and the second applicant, a former member of parliament, were obliged to tolerate it.[18]

e) In my thesis, I recognised that the fact that deepfakes are inherently fake does not necessarily mean that they are all unlawful or not protected by freedom of expression. Indeed, a deepfake can only be constitutionally protected if it is an opinion based on false information, rather than a false statement of fact. However, as many authors have pointed out, deepfakes fall somewhere between a statement of fact and an expression of opinion. According to the above definition of a deepfake — a falsified video, image or sound recording that creates the false impression that the content has actually taken place — it is a false statement of fact. On the other hand, as we have seen in the cases discussed in previous chapters, distorted photographs are often used as a means of expression. In my thesis, I argue that, in light of the Constitutional Court's case law, deepfakes are generally false statements of fact. By its very nature, a deepfake is a convincing way of creating the impression that the falsified content has in fact been fabricated. For example, research conducted by Nightingale and Farid in 2022 showed that participants could only identify real persons with 48% accuracy and that persons 'created' by AI had an 8% higher confidence index.[19]) However, it also follows from the ability of deepfakes to imitate authenticity to such a high degree that the average recipient will interpret them as literal statements of fact rather than opinions. However, deepfakes' ability to imitate authenticity so convincingly means that the average recipient will interpret them as literal statements of fact rather than opinions. Accordingly, in view of the provisions of AB Decision 3107/2018 (9 April 2018), deepfakes are a statement of fact in these cases This does not, of course, exclude the possibility that, depending on the circumstances and context of the

[16] Pf. 20.537/2014/3.
[17] Pfv. 21.245/2015/4.
[18] Pf. 20.537/2014/3.
[19] Mezriczky Marcell: Ne higgy a szemének! A deepfake online sajtóreprezentációja 2018 és 2022 között. In: Aczél Petra – Veszelszki Ágnes (szerk.): Deepfake: A valótlan valóság. Budapest, Gondolat Kiadó, 2023, p. 44.

communication, some deepfake content may be interpreted as an opinion in certain cases. For instance, if the falsity of the recording is evident from the visual material itself, or if it can be proven beyond doubt from the communication's context that the manipulated image solely illustrates the communicator's opinion, the deepfake may be considered an expression of opinion.

3.2 The DSA is inadequate to provide effective protection for individuals whose right to image has been infringed, while ensuring adequate protection of freedom of expression

In the second half of my thesis, I concluded that there is no effective legal protection for someone whose right to an image on the internet has been infringed.

Holding authors (the one who shares the content that infringes another's right to image) liable is not a realistic alternative for a number of reasons. Indeed, before the victim can bring any substantive legal claim against the author, he or she must at least overcome the following obstacles: (i) the problem of identifying the defendant (anonymity); (ii) the existence of multiple potential authors/ infringers; (iii) the conflict of jurisdiction of several countries and the problem of conflict of laws; and (iv) the challenge that once illegal content is on the Internet, it is almost impossible to remove it permanently.[20]

However, the DSA, which inter alia regulates the liability of platforms for unlawful content they store and disseminate to the public, also does not provide an effective remedy for the person whose right to image is infringed. My conclusions are based on following findings of mine:

a) The concept of a 'platform' is, in many ways, misleading and self-contradictory, and does not reflect the true capabilities of the underlying technology. For example, a key element of the platform definition is that service providers not only store information, but also make it available to a wide and indefinite audience. However, this would mean that Facebook's private groups and Reddit's private pages ('subreddits') would not qualify as platforms, since (i) they are only accessible to a limited number of users, and (ii) access is at the discretion of the group's host or organiser. Nevertheless,

[20] Laidlaw, Emily: Are we asking too much from defamation law? Reputation systems, ADR, Industry Regulation and other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age. Ontario, Law Commission of Ontario, 2017, pp. 17–18. https://doi.org/10.2139/ssrn.3059954

Facebook was one of the first platforms to be classified as a very-large-online-platfrom (VLOP) by the European Commission.

b) Furthermore, the DSA does not clarify which liability provisions apply to intermediary service providers offering multiple types of intermediary service simultaneously. For example, Facebook hosts user-generated content, making it a hosting service provider. However, Facebook Messenger, which is integrated into Facebook, is merely a conduit service, facilitating access to the communication network for users. In my opinion, and in line with the academic literature,[21] such hybrid intermediaries should be evaluated according to their functionality. Therefore, if a legal practitioner is asked whether Facebook can be held liable for unlawful content shared by a user on its timeline, they must refer to Article 6 of the DSA.[22] Conversely, where liability arises in relation to infringing content sent via Facebook Messenger, the enforcer must determine Facebook's liability on the basis of Article 4 of the DSA. However, it also follows that hybrid services cannot fall exclusively within a single sub-category of intermediary service providers. In contrast, the Commission's decision to designate Facebook as a VLOP ignored features that do not constitute 'public distribution' (e.g. sharing content in private groups) or fall outside the scope of hosting services (e.g. Facebook Messenger). Two alternative conclusions can be drawn from this: (i) the DSA has abandoned the approach whereby the liability of a hybrid service provider is determined based on which of its functions are involved in the dispute, or (ii) the European Commission has begun to interpret the definition of 'platform' under the DSA more broadly, including not only intermediary service providers that offer hosting services exclusively, but also those that offer only partial hosting services, provided the hosting service is not a minor, ancillary element of another service or a minor function of the main service.

c) The DSA has completely misunderstood the role of social media sites in content distribution. Platforms are defined as having a passive role in storing and distributing content to the public. This approach is based on the CJEU's erroneous assumption in

[21] Wilman, Folkert – Kalėda, Saulius Lukas – Loewenthal, Paul-John: The EU Digital Services Act. Oxford, Oxford University Press, 2024. https://doi.org/10.1093/law/9780198892847.001.0001
[22] Hofmann, Franz - Raue, Benjamin (eds.): Digital Services Act. Article-by-Article Commentary. Baden-Baden, Nomos, 2025, p. 160.

the Google France and Google[23] and YouTube cases[24] that the automated handling of the content in question and the general application of the algorithm implies a neutral role for the hosting provider. In reality, the effect of an algorithm applied automatically to all user-generated content is not necessarily neutral. For example, algorithms used for content moderation reflect the values encoded by the platforms, meaning each post examined by such an algorithm reflects the platform's approval or disapproval.[25] Furthermore, platforms have a financial interest in having their algorithms select and recommend content that matches users' interests and is popular with other users, thus increasing the number of views, user attention, and inevitably, advertising revenue for social networks. The higher the number of views of the content, the higher the amount of money that can be demanded for the sale of the associated advertising space in an ad auction. However, fake news is among the most widely shared content on social media, so platforms have a significant financial interest in distributing it.[26] In my opinion, the concept of neutral platforms is more of a myth, as they act as 'advocates' of collective creativity. They invite and encourage their users to participate in creating content, thereby setting the conditions for its production. As Tarleton Gillespie puts it, "These conditions are practical, technical, economic and legal, and far removed from the neutrality implied by the platform's rhetoric".[27]

d) Due to the legal gap between the DSA's provisions on content moderation (particularly the notification and action mechanism) and its rules on platform liability, platforms tend to remove potentionally unlawful content to avoid potential legal or reputational consequences. This is because Article 16(3) of the DSA states that a notification gives the platform actual knowledge of unlawful content, which makes the platform liable. However, the notification must contain enough information for the platform to decide that the content is unlawful without a detailed

[23] Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08), ECLI:EU:C:2010:159.
[24] Joined Cases C-682/18 and C-683/18, Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG, ECLI:EU:C:2021:503.
[25] Gillespie, Tarleton: Custodians of the Internet. Platforms, Content Moderation and the Hidden Decision that Shape Social Media. New Haven, Yale University Press, 2018, pp. 210–211. https://doi.org/10.12987/9780300235029
[26] Ghosh, Dipayan – Scott, Ben: #Digitaldeceit. The Technologies Behind Precision Propaganda on the Internet, Washington, New America, 2018, p. 25.
[27] Gillespie, 2018, p. 188.

legal assessment. However, Article 16(3) of the DSA lays down requirements for the content of notifications rather than imposing a substantive obligation to prove the clear illegality of the content in question. Therefore, the DSA does not require the illegality of the content to be immediately apparent; rather, it requires the notifier to provide sufficiently detailed information to enable the hosting provider to establish it. However, there are cases where the content is not clearly illegal, and even a sufficiently detailed notification cannot remedy this. A perfect example of this is the present case involving a photo of Hillary Clinton "wearing a tracking device". There is no doubt that the photo was fake. However, just because a picture is fake does not automatically mean that it is unlawful, nor does it mean that it is unquestionably unlawful. Since the DSA is unclear as to whether a notification in such cases establishes the platform's actual knowledge and thus liability, platforms are more likely to remove the notified content than risk being found legally liable. (For example, the Future of Free Speech 2024 report showed that 88–98% of comments removed from Facebook and YouTube in France, Germany, and Sweden were in fact legally protected expressions.[28])

3.3 DSA does not provide effective protection against information bubbles and echo chambers created by platforms' recommender systems

My thesis has also shown that the optimisation of content by platforms, driven by financial incentives, results in so-called information bubbles. Take fake news, for example, which is one of the most widely shared types of content and therefore appears repeatedly at the top of users' news feeds. When a user interacts with such content — by clicking on a link, for example — the algorithm favours similar content in future, regardless of the user's actual interests or original intent. This is because the platform's ranking mechanism considers such content to be both popular and relevant due to the user's repeated engagement. This inevitably triggers a self-perpetuating process that gradually isolates the user, trapping them in an information bubble without their realising it.

However, platforms' recommendation systems not only trap users in an information bubble, they also constantly reinforce the ideas on which the bubble was originally built. This is

[28] Vigen Smolarz, August – Vinther-Jensen, Eske: Preventing "Torrents of Hate" or Stifling Free Expression Online? Nashville, Vanderbilt University, 2024, p. 41.

because users are not naturally encouraged to seek out all the facts, especially those that contradict their beliefs. Echo chambers can develop as a result of people shutting themselves off from opinions and information that challenge their belief systems.[29] These echo chambers are essentially parallel but separate universes that coexist without knowing of each other's existence.

These filtering bubbles and echo chambers lead to ideological segregation, which poses a direct threat to freedom of expression — specifically, the freedom of the individual to seek, receive and impart information and ideas of all kinds, whether orally, in writing, in print, in the form of art or through any other medium of their choice.

Although the existence of information bubbles created by recommender systems and their negative social impact were already widely known at the time the DSA was adopted, the DSA makes no reference to them.[30] In my view, the DSA seeks to address information bubbles indirectly through the due diligence obligations adopted in the context of recommender systems. However, I conclude in my thesis that these due diligence obligations do not effectively protect against information bubbles and echo chambers:

a) Article 27 of the DSA imposes a dual transparency obligation. Platforms must explain: (i) the key parameters used in their recommender system; and (ii) how these key parameters can be modified or influenced.[31] However, the DSA does not specify what these key parameters are exactly.[32] The purpose of Article 27 is therefore not to restrict or prohibit recommender systems, but to promote transparency and enable users to understand the impact of such systems on the presentation of information. However, as I discuss in my thesis, the content and scope of this obligation are unclear.

b) In addition to the requirements set out in Article 27, Article 38 imposes an obligation on online platforms to provide an alternative to recommender systems that does not

[29] Seargeant, Philip – Tagg, Caroline: Social media and the future of open debate: A user-oriented approach to Facebook's filter bubble conundrum. Discourse, Context & Media, 2019/3, p. 42. https://doi.org/10.1016/j.dcm.2018.03.005

[30] Papp János Tamás: Recontextualizing the Role of Social Media in the Formation of Filter Bubbles. Hungarian Yearbook of International Law and European Law, 2023/1., p. 146. http://www.doi.org/10.5553/HYIEL/266627012023011001012

[31] Decarolis, Francesco – Li, Muxin: Regulating online search in the EU: From the android case to the Digital Markets Act and Digital Services Act. International Journal of Industrial Organization, 2023/90, p. 6. https://doi.org/10.1016/j.ijindorg.2023.102983

[32] DSA, Article 27 (1).

rely on user profiling.[33] Article 38 therefore allows users to opt out of profiling-based recommendation systems. Nevertheless, the DSA does not oblige VLOPs to use the non-profiling alternative as the default setting, nor to refrain from using profiling-based recommendation systems for certain content. Moreover, the duty of care imposed by Article 38 of the DSA could easily become counterproductive. The alternative solutions preferred by giant platforms (e.g. chronological or alphabetical layout) may result in an impractical or difficult-to-navigate interface, which could discourage users from choosing non-personalised recommendations.

3.4 Summary and alternative proposal for internet regulation

In conclusion, I found that the current regulation of the internet is inadequate for ensuring the proper enforcement of the right to image, effectively protecting individuals whose right has been violated and counteracting echo chambers created by referral systems. In the final chapter, I therefore sought to answer the question of what alternative means of internet regulation would enable these objectives to be achieved. In doing so, I made the following suggestions, among others:

a) In order to ensure that the individual whose right to be represented is violated is effectively protected without unnecessary and disproportionate restrictions on the right of others to express their views, believe that, instead of the current command-and-control regulatory approach, a model of co-regulation should be introduced. This model would see the state take a principles-based regulatory approach and self-regulation achieved through the adoption of codes of conduct. This regulatory approach would enable (i) legislation to keep pace with the constantly and rapidly changing technological developments; (ii) detailed regulation of conduct to remain in the hands of those who understand and have detailed knowledge of the technology; and (iii) compliance with the legislation to reflect the organisation's own operations, structure and service, thus facilitating compliance by global firms.

b) In order to limit the role of platforms in enforcing users' rights to freedom of expression and other fundamental rights, I believe it would be worthwhile to establish

[33] Papp János Tamás: Ajánlórendszerek. In: Koltay András – Lapsánszky András – Szikora Tamás – Tóth András (szerk.): DSA rendelet nagykommentár. Nagykommentár a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló, az Európai Parlament és a Tanács 2022. október 19-i (EU) 2022/2065 rendelethez (digitális szolgáltatásokról szóló rendelet). Budapest, Wolters Kluwer, 2024, p. 137.

an authority (or give limited authority to the out-of-court dispute resolution forums already established by the DSA[34]) that would act as a complaints platform. Users could report illegal content to this platform.[35]

c) Recognizing that the emergence of echo chambers and the failure to enforce individuals' rights to privacy can be traced back to the 'physical environment' created by the platforms, I conclude by arguing that the internet should be regulated primarily through other means, such as code, rather than legislation, according to Lawrence Lessig's model. [36] However, as there is no such thing as neutral architecture (i.e. a physical environment that does not influence user behaviour and decisions)[37] legislators should consider what values the internet should be built on when regulating it. With regard to eliminating information bubbles, for example, this would mean legislators obliging platforms to promote diversity. Platforms should therefore design their interfaces to promote diversity of viewpoints, while remaining transparent and preserving users' freedom. For example, recommender systems should first identify topics of interest to the user, such as climate change, foreign policy or the economy, and then display information that matches the user's interests, followed by information that conflicts with them.

[34] DSA, Article 21.
[35] Rozgonyi Krisztina: A hálózati médiumok szabályozásának néhány lehetséges szempontja. In: Enyedi Nagy Mihály – Polyák Gábor – Sarkady Ildikó (szerk.): Magyarország médiakönyve 2003. Budapest, ENAMIKÉ, 2003, p. 641.
[36] Lessig, Lawrence: Code 2.0. New York, Basic Book, 2006, pp. 122–123.
[37] Thaler, Richard – Sunstein, Cass R.: Nudge. Improving Decisions about Health, Wealth and Happiness. New Haven, Penguin Books, 2009, p. 3.

4 BIBLIOGRAPHY OF THE THESIS BOOK

Decarolis, Francesco – Li, Muxin: Regulating online search in the EU: From the android case to the Digital Markets Act and Digital Services Act. International Journal of Industrial Organization, 2023/90.

Ghosh, Dipayan – Scott, Ben: #Digitaldeceit. The Technologies Behind Precision Propaganda on the Internet. Washington, New America, 2018

Gillespie, Tarleton: Custodians of the Internet. Platforms, Content Moderation and the Hidden Decision that Shape Social Media. New Haven, Yale University Press, 2018

Hofmann, Franz – Raue, Benjamin (szerk.): Digital Services Act. Article-by-Article Commentary. Baden-Baden, Nomos, 2025

szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló, az Európai Parlament és a Tanács 2022. október 19-i (EU) 2022/2065 rendelethez (digitális szolgáltatásokról szóló rendelet). Budapest, Wolters Kluwer, 2024

Laidlaw, Emily: Are we asking too much from defamation law? Reputation systems, ADR, Industry Regulation and other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age. Proposal for Reform. Ontario, Law Commission of Ontario, 2017

Lenkovics Barnabás – Székely László: Magyar polgári jog. A személyi jog vázlata. Budapest, Eötvös József Könyvkiadó, 2001

Lessig, Lawrence: Code 2.0. New York, Basic Books, 2006

Mezriczky Marcell: Ne higgy a szemének! A deepfake online sajtóreprezentációja 2018 és 2022 között. In: Aczél Petra – Veszelszki Ágnes (szerk.): Deepfake: A valótlan valóság. Budapest, Gondolat Kiadó, 2023

Mráz Attila: Deepfake, demokrácia, kampány, szólásszabadság. In: Török Bernát – Ződi Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Budapest: Ludovika Egyetemi Kiadó, 2022

Papp János Tamás: Ajánlórendszerek és szűrőbuborékok. In: Koltay András – Szikora Tamás – Lapsánszky András (szerk.): A vadnyugat vége? Tanulmányok az Európai Unió platform szabályozásáról. Budapest, ORAC Kiadó, 2024

Papp János Tamás: Recontextualizing the Role of Social Media in the Formation of Filter Bubbles. Hungarian Yearbook of International Law and European Law, 2023/1.

Rozgonyi Krisztina: A hálózati médiumok szabályozásának néhány lehetséges szempontja. In: Enyedi Nagy Mihály – Polyák Gábor – Sarkady Ildikó (szerk.): Magyarország médiakönyve 2003. Budapest, ENAMIKÉ, 2003

Seargeant, Philip – Tagg, Caroline: Social media and the future of open debate: A user-oriented approach to Facebook's filter bubble conundrum. Discourse, Context & Media, 2019/3.

Thaler, Richard – Sunstein, Cass R.: Nudge. Improving Decisions about Health, Wealth and Happiness. New Haven, Penguin Books, 2009

Törő Károly: Személyiségvédelem a polgári jogban, Budapest, Közgazdasági és Jogi Könyvkiadó, 1979

Vigen Smolarz, August – Vinther-Jensen, Eske: Preventing "Torrents of Hate" or Stifling Free Expression Online? Nashville, Vanderbilt University, 2024

Wilman, Folkert – Kalėda, Saulius Lukas – Loewenthal, Paul-John: The EU Digital Services Act. Oxford, Oxford University Press, 2024

5 LIST OF PUBLICATIONS IN THE FIELD OF THE DOCTORAL DISSERTATION

1. Gosztonyi Gergely – Zanathy Anna: Az internet szabályozására vonatkozó korai elméletek. *Jogelméleti Szemle*, 2025/3. *(közlésre befogadva, megjelenés alatt)*
2. Zanathy Anna: A képmáshoz való jog magyarországi érvényesülése a deepfake világában. *ELTE Law Working Papers*, 2025/4., 1–21. o. https://m2.mtmt.hu/api/publication/36281896
3. Zanathy Anna: A DSA által előírt gondossági kötelezettségek az online platformok ajánlórendszereivel összefüggésben a P2B függvényében. *Pázmány Law Working Papers*, 2025/4., 1–15. o. https://m2.mtmt.hu/api/publication/36229135
4. Zanathy Anna: A DSA által az online platformokkal szemben előírt kellő gondossági kötelezettségek a tartalommoderálással összefüggésben. *MTA Law Working Papers*, 2025/6., 1–10. o. https://m2.mtmt.hu/api/publication/36176156
5. Zanathy Anna: A közösségi média platformok jogi meghatározásának nehézségei a DSA előtt és alatt. *Themis*, 2025/2., 184–203. o. https://m2.mtmt.hu/api/publication/35666407
6. Zanathy Anna: Burst the Bubble. How to defend freedom of expression from algorithmic personalization. *International Journal of Scientific and Research Publication*, 2021/7., 95–99. o. https://m2.mtmt.hu/api/publication/32109710
7. Zanathy Anna: Platforms, Delivery Men of "Fake Advertisement": The paradox of regulation regarding platforms' liability for hosting "fake news" that amounts to be unfair commercial practice. *International Journal of Scientific and Research Publication*, 2021/6., 798–803. o. https://m2.mtmt.hu/api/publication/32109709
8. Zanathy Anna: "Kiberjog" vagy Netikett: Az internet szabályozására vonatkozó jogtörténeti elméletek. *Joghistória*, 2021/1–2., 44–52. o. https://m2.mtmt.hu/api/publication/32109684
9. Zanathy Anna: A képmáshoz való jog az interneten. *Joghistória*, 2015/4., 11–17. o. https://m2.mtmt.hu/api/publication/32109687