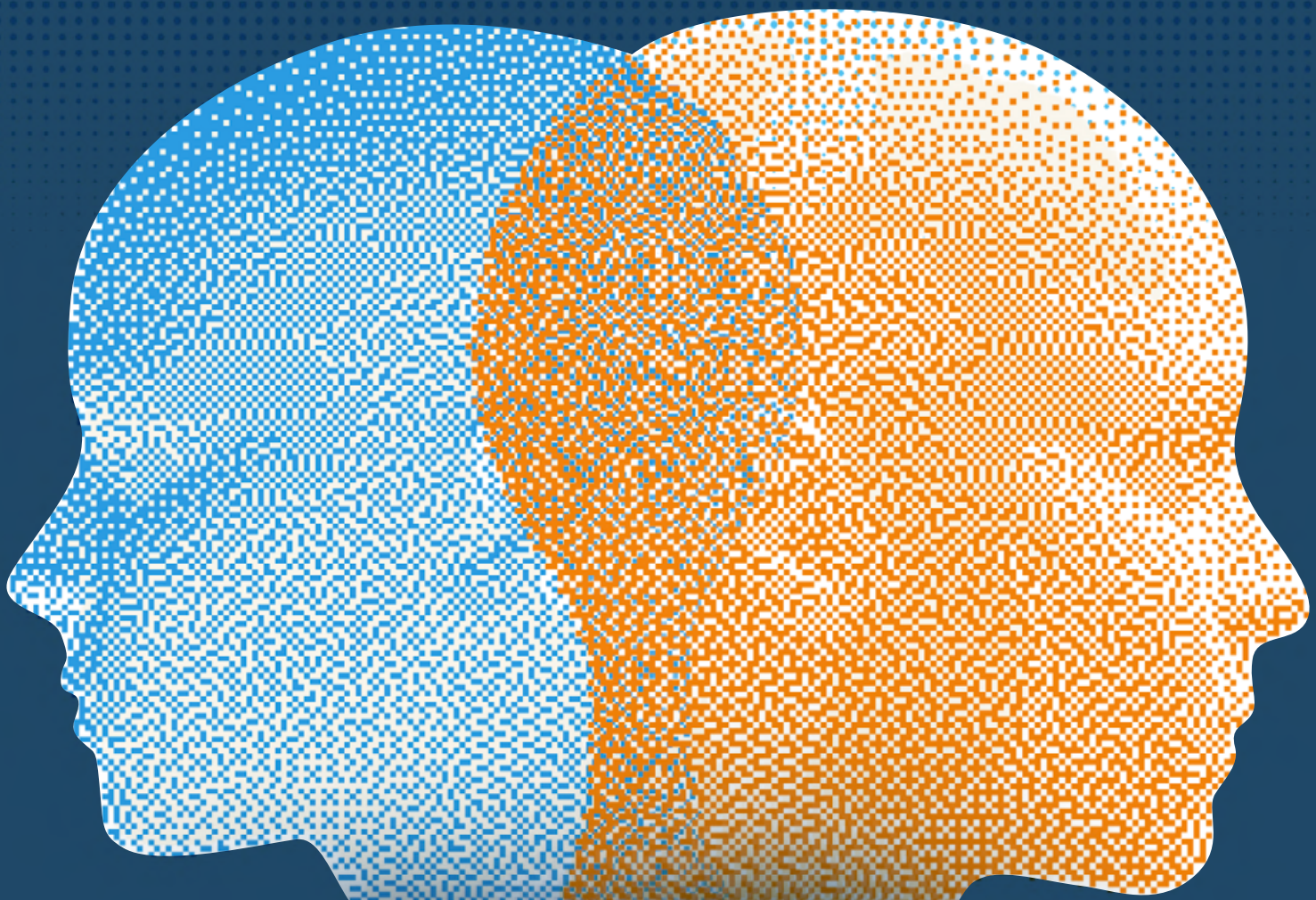
ISBN 978-9934-619-64-9



The Doppelganger case

Assessment of Platform Regulation on the EU Disinformation Environment

PREPARED AND PUBLISHED BY THE
NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

ISBN: 978-9934-619-64-9

Authors: Maria Giovanna Sessa, Raquel Miguel
Project Manager: Mārtiņš Pundors
Design: Una Grants

Riga, May 2024

NATO STRATCOM COE
11b Kalnciema iela,
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

The Doppelganger case

Assessment of Platform Regulation on the EU Disinformation Environment

Contents

Executive summary

In September 2022, EU DisinfoLab, with the support of Qurium, exposed a Russia-based influence operation network operating in Europe since at least May 2022. The campaign, dubbed "Doppelganger", replicated and impersonated authentic media by spoofing domain names and creating content falsely attributed to reputable news websites. Despite Meta's acknowledgement of the operation and legal prosecutions by affected media in France and Germany, recent findings from June 2023 confirm that the campaign is ongoing on multiple platforms, and even expanding. Public institutions such as ministries in France and Germany were recently impacted. In August 2023, Graphika's latest investigation on the campaign and Meta's Adversarial Threat Report Q2 2023 confirm that NATO has been a direct target of Doppelganger, in the context of last July's Vilnius summit.

In November 2022, the Digital Services Act (DSA) came into force, introducing sweeping changes to the EU online environment toward internet safety and accountability. As its enforcement is ongoing, we decided to take the

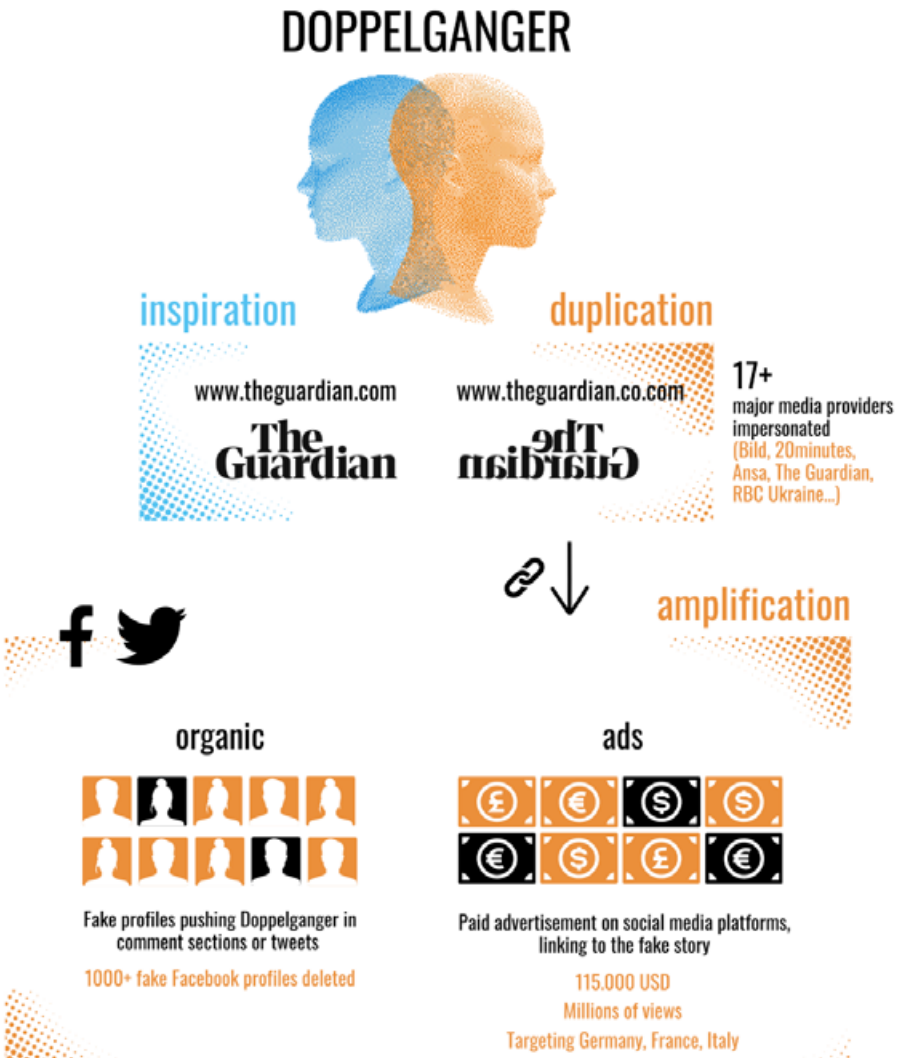


Figure 1 – A visual representation of the Doppelganger campaign's modus operandi

Figure 2 – Spot the difference: fake content on a cloned The Guardian page and article

Doppelganger operation as a case study to test the avenues for mitigation under this groundbreaking regulation.

The report considers infringements in the national legislation of three affected countries (France, Germany, and Italy) to understand the context in which the European law package will be implemented. Then, the analysis selects the appropriate DSA articles and corroborates them with concrete examples from the disinformation campaign to demonstrate the breach, distinguishing between illegal and harmful content. Moreover, we identify the relevant stakeholders, the mutual actions they can take within the DSA framework, and the consequent impact, ideally leading to a best-case scenario.

A composite reality emerges where actors are intertwined, and potential initiatives and avenues for mitigation inform one another. Final considerations voice preoccupations with the ongoing violation despite awareness and prohibition and hope for the exciting opportunities brought by the proper implementation of the legislative package.

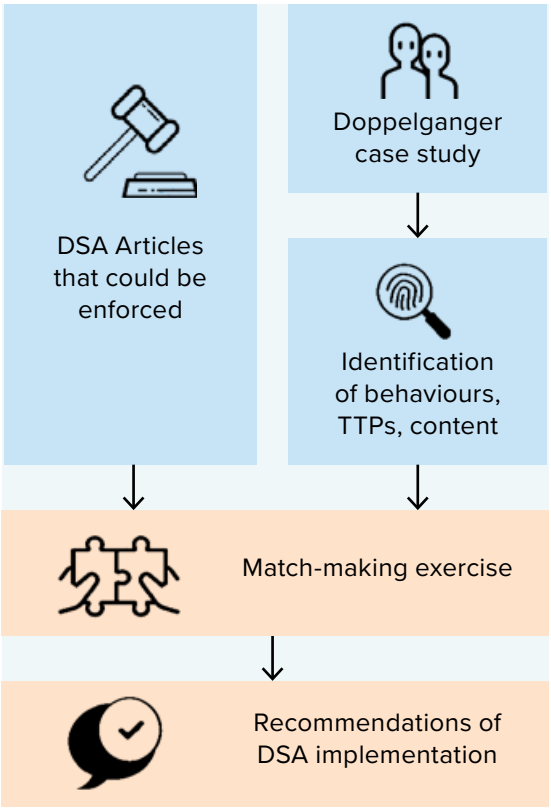


Figure 3 – An overview of our report

Avenues against disinformation in the DSA: The Doppelganger case

The Doppelganger case is based on distributing disinformative content through fake websites impersonating media outlets – and institutions at a later stage. The campaign relies on multiple clones of authentic media and targets users with counterfeit articles, doctored videos, and made-up polls. This was accomplished by buying dozens of Internet domain names that resembled the ones of actual media (e.g., theguardian.co.com mimicking theguardian.com) and copying their design. More than 17 media providers from different countries were impersonated, promoting Kremlin narratives depicting Ukraine as a Nazi state and European states as hurt by their own sanctions against Russia. Similar content is translated into different languages and published under the false pretence, redirecting and geo-blocking users based on location.

Social media platforms, especially Facebook, were crucial in the amplification chain, granting public visibility to the campaign. Paid advertisements on Facebook for at least 115.000 USD boosted the content's organic amplification (through tweets or comments). Fake profiles shared the fake articles, reaching millions of views in Germany, France, and Italy, thus violating Meta's community standards for not disclosing the advertiser's identity. Nonetheless, we detected that the fake content circulated on other platforms, such as X (formerly Twitter) or Telegram, our investigation focused on Facebook as the main amplifier of the campaign. Besides, in September 2022, Meta announced a takedown of a Russian network engaged in coordinated inauthentic behaviour, referring to the same campaign. The limitations in data access made it unfeasible to pursue the research on other platforms. However, new cloned media assets have recently been re-circulated on platforms such as X, emphasising the need to access data across platforms.

Besides voluntary and self-defined rules defined by the platforms, the DSA introduces binding provisions for online service providers. The legislation offers critical tools to design a more coherent and robust system of platform accountability and digital safety, allowing avenues for tackling disinformation when it coincides with illegal – and to some extent harmful – content.

For example, the DSA empowers users to challenge excessive or insufficient content moderation by the platforms through the novel internal complaint handling system (Article 20), while it was previously up to the platform's discretion to act on a user's content report. Platforms must now report meticulously and transparently on all actions designed and taken to assess and mitigate systemic risks of spreading illegal and harmful content. Therefore, the Doppelganger case is a lens to evaluate shortcomings in Very Large Online Platforms' (VLOPs) behaviour and the opportunities presented by the new legal package.

The DSA stimulates European and cross-national cooperation, as relevant authorities can demand that platforms provide specific information or act. On this note, actions can be taken if the disseminated content is considered illegal, which is each country's prerogative to assess. While disinformation can be considered a criminal offence in France, unlike in Germany or Italy, other trademark violations and identity theft are transnationally criminalised, contributing to eradicating deceptive practices.

In short, the DSA enforces a circular mechanism of platform accountability and digital safety. It facilitates access to information by national authorities, vetted researchers, and users. This data is important to assess the content's illegal or harmful nature and evaluate the platforms' terms and conditions and systemic risks. Based on this assessment, specific actions on the examined content can be demanded and taken. Finally, these actions are aimed at achieving a certain impact to mitigate the disruptive content and, ideally, avoid its repetition. The cycle continues as actions and mitigation mechanisms raise situational awareness, which feeds on new information.

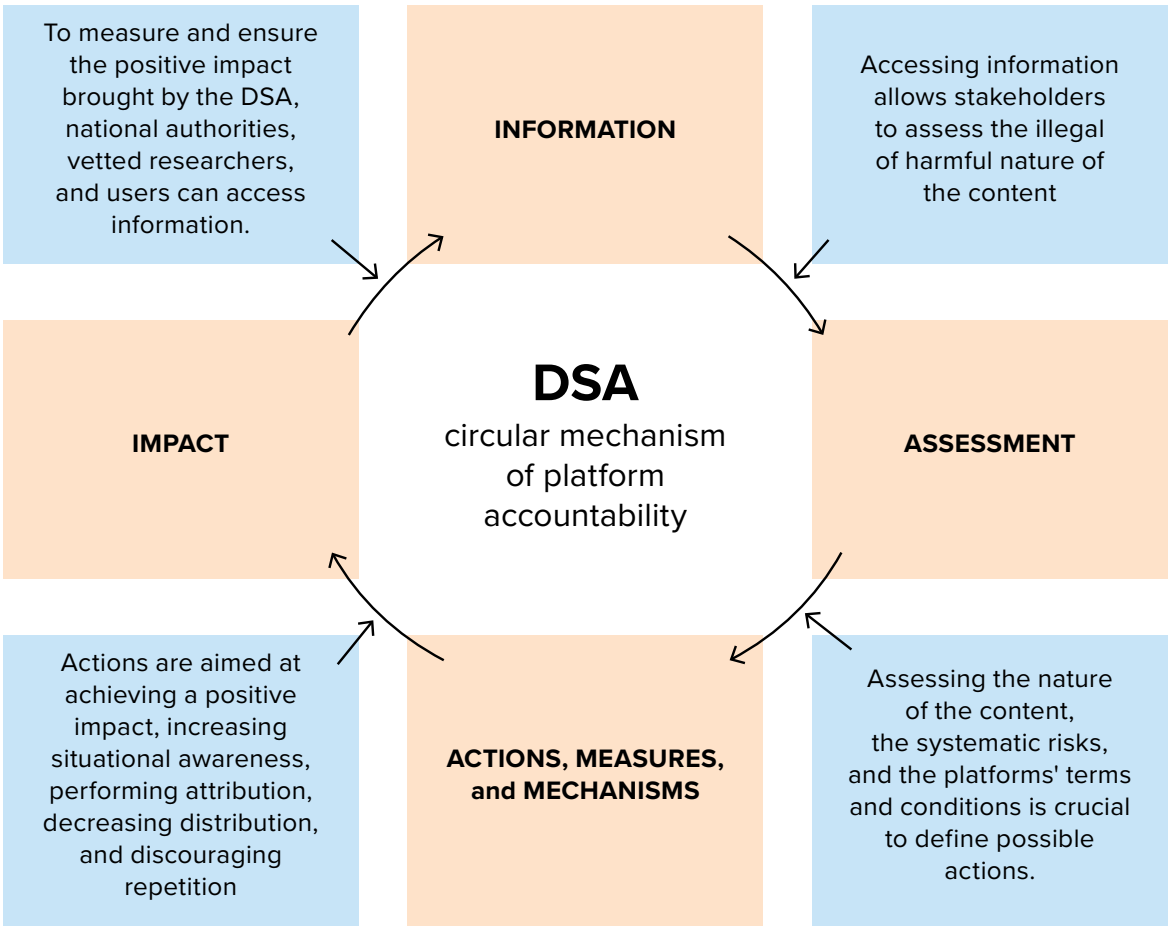


Figure 4 – The circular mechanism of platform accountability triggered by the DSA

ACTIONS, MEASURES, and MECHANISMS		
illegal content		**harmful content**
x	access to data	x
x	ads transparency	
x	appeal, report and complain	x
x	content moderation	x
x	denial of service	
x	liability & accountability	x
x	reporting of actions taken	x
x	risk assessment and mitigation	x
x	sanctions on platform	

Figure 5 – Matching actions, measures, and mechanisms to illegal and harmful content

Prosecution in Member States: National legislations and judicial cases

The DSA can be activated in the presence of illegal content that "is not in compliance with Union law or the law of any Member State", as Article 3(h) recites. As said, the Doppelganger operation also infringes various national legislation provisions. Considering three countries that were (and in some cases are still) targeted by the campaign – namely France, Germany, and Italy – the next section delves into infringements of their legal frameworks and the actions taken against these violations. Although by no means exhaustive, this overview wishes to convey the similarities and differences between EU Member States when dealing with illegal and harmful content, which will affect the activation of the DSA.

Disinformation

To explore the opportunities offered by the DSA in disinformation operations, the first crucial aspect regards whether the Member State criminalises disinformation. This means that it can be considered illegal content, which the European regulation tackles. In detail:

- The French law No. 2018-1202, dated 22 December 2018, for the fight against "fake news" imposes on platforms (with over 5 million monthly unique visitors) certain obligations to fight inaccurate or misleading information that can alter voting integrity. Violations can lead to one year of imprisonment and a €75.000 fine. The law builds upon the 1881 law on the freedom of the press that outlawed the dissemination of "false news" and was later amended to target "manipulation of information".
- Germany does not criminalise disinformation per se but since 2017 has a law against hate speech since 2017 titled "Netzwerkdurchsetzungsgesetz" (NetzDG), which forces online platforms (with over 2 million members) to remove "obviously illegal" posts within 24 hours or risk fines of up to €50.000.000.
- Italy is missing a clear legal framework regarding disinformation. The dissemination of false news is a crime only when there is a causal link between the piece of disinformation and specific effects envisaged by law, such as slander or disturbance of public order.

Other illegal activities

Apart from the criminalisation of disinformation or ethical considerations related to truthful information, the Doppelganger operation committed criminal actions that are recognised by all legislative systems. Spoofing domain names and copying logos violates intellectual property provisions relating to registered and unregistered (de facto) trademarks. Impersonating journalists – using their names and photos – constitutes identity theft. Other violations might include unfair advertisement – given the use of ads – and slander, as the media and journalists impersonated were attributed false positions.

Trademark law violations

- In France, Intellectual Code Article L. 716-4-7 prosecutes trademark counterfeiting, which occurs when an unauthorised person exploits a brand without the owner's permission by reproducing, imitating, or affixing the disputed logo.
- According to Sections 143, 143a, 112, and 124 of the German Trade Mark Act, infringing a German national trademark, an international trademark registered for Germany, or an EU trademark intentionally is a criminal offence.
- Article 473 of the Italian Criminal Code disciplines the offence of counterfeiting, altering, or using a registered trademark, although it has been applied to include also the criminal protection of the unregistered trademark.

Identity theft

- In France, the act of usurping a third party's identity or using one or more data of any kind to identify, disturb, or undermine said party is a publishable offence, according to Criminal Code Article 226-4-1.

- The German Criminal code punished various forms of identity theft depending on how the offender obtains access to the data. In particular, Section 263 criminalises fraud, and Section 263a publishes computer fraud, i.e., the use of such identity data for fraudulent purposes.

- In Italy, Article 494 of the Criminal Code punished "impersonation", i.e., the action made by those who steal or use someone's identity for personal benefit or to cause damage. The introduction of Article 640-ter of the Criminal Code includes digital identity theft, i.e., the theft or improper use of digital identity to the detriment of one or more people.

Judicial cases in affected Member States

On the basis of the illegality of these activities, some of the targeted media filed lawsuits in court against their impersonation. For instance, Der Spiegel reports that the German newspaper Süddeutsche Zeitung filed criminal charges. In its reports, the German daily denounced that "unknown persons misused the trademark of the Süddeutsche Zeitung for pro-Russian propaganda". In France, Le Parisien also went to court to condemn the campaign. At the same time, to the best of our knowledge as of 28 August 2023, in Italy, no legal action has been initiated despite national news agency ANSA's awareness of being an operation target. Despite the scale of the operation, EU DisinfoLab is not aware of any further court cases, although this may be due to the confidentiality with which they are being conducted.

Regarding other potential actions initiated by the stakeholders impersonated in France and Germany, the German Ministry of Interior (BMI) admitted having been aware of the fake website since 1 June 2023, as Der Spiegel magazine reports. The Federal Office for Information Security notified the relevant internet service providers and requested the deactivation of the content.

DSA applicability: The Doppelganger operation case study

Illegal v. harmful content	Stakeholders involved	Potential actions	Relevant DSA articles	Application in the Doppelganger case	Impact
Illegal content	Platforms	Liability and accountability	**Article 6** exempts platforms from being liable for the content they host unless they have actual knowledge of the illegal activity or illegal content.	Meta was notified via email by EU DisinfoLab. In September 2022, the platform was already working on the case study with DFRLab. Therefore, it had actual knowledge of these illegal activities as established by Article 6.1(a) but did not act expeditiously to remove or restrict access to the illegal content, violating Article 6.1(b). On the contrary, we currently have no way of proving that X received specific notifications about the campaign circulating on the platform. However, due to the public attention received by this campaign, appropriated preventive measures could have been taken.	Less distribution of illegal content
Illegal content	National judicial or administrative authorities Platforms	Content moderation Liability and accountability Reporting on actions taken	According to **Article 9**, if the relevant national judicial or adminaistrative authorities had issued an order to act against specific items of illegal content (e.g., in countries where impersonation is a punishable offence), the platform should have informed the authorities of any effect given to the order.	For instance, the Italian national authorities could have ordered the removal of a Facebook post or tweet engaging in media impersonation, referencing the violated law (Article 473 of the Italian Criminal Code), the reason why (i.e., counterfeiting a registered trademark), and the exact URL, as defined by Article 9.2(a). As a result, the platform would have been obliged to report on the action(s) taken in response to that order.	Less distribution of illegal content More situational awareness
Illegal content	National judicial or administrative authorities Platforms	Access to data Liability and accountability Reporting on actions taken	Following the previous point, **Article 10** states that if the relevant national judicial or administrative authorities had issued an order to provide specific information about specific service recipients' illegal content, the platform should have informed the authorities of receiving and giving effect to the order.	This provision is crucial for attribution in the Doppelganger case. Authorities can request information about providers of deceiving URLs or ads published on Facebook or X, for example. However, authorities are required to have research capacities as the order has to contain "account names or unique identifiers" (Article 2(a.iii)). The process requires one of the direct targets – e.g., Le Parisien in France – to establish illegality with the French national authority. At the same time, the platform is obliged to report on the action(s) taken in response to that order.	More situational awareness More attribution opportunities

Illegal v. harmful content	Stakeholders involved	Potential actions	Relevant DSA articles	Application in the Doppelganger case	Impact
Ilegal and harmful content	National judicial or administrative authorities Platforms	Liability and accountability Reporting on actions taken	**Articles 15, 24, and 42** on transparency reporting obligations will bind platforms to report on their activities in response to receiving notices, for instance, on how many notices were submitted by national authorities (Article 15.1(a)), trusted flaggers (Article 15.1(b)), or through the internal complaint-handing system (Article 15.1(d)). **Article 37** mandates that VLOPs should be subject to independent audits to assess compliance with the Codes of Conduct (Articles 45 and 46) and crisis protocols (Article 48).	The Meta Quarterly Adversarial Threat Report Q4 2022 mentioned the Doppelganger network. However, the report does not clarify whether the company took the necessary actions to stop the campaign. In this regard, Doppelganger should be a case study for an independent auditor to assess Meta's general compliance with Article 15 of the DSA, as foreseen by Article 37. At present, X has left the European Code of Practice on disinformation. As a consequence, there were no public reports on threats, in general, or the Doppelganger operation, in particular. However, the DSA binds X to new transparency reporting obligations. We will be on the lookout for whether it reports about this campaign.	Deter illegal and harmful content More situational awareness
Illegal content	Platforms Users	Content moderation Liability and accountability Report content	**Article 16** on notice and action mechanisms applies as platforms allow individuals to report illegal content.	Platform users, including the operation's targets (such as the impersonated media), can notify the platforms about the illegal content. For instance, Süddeutsche Zeitung can notify Meta or X about the content circulating on the platforms violating its trademark, which should act against this illicit content.	Less distribution of illegal content
Illegal and harmful content	Platforms Users	Appeal decisions Content moderation Liability and accountability	The internal complaint handling system introduced by **Article 20** empowers users to appeal to a platform's over- and under-moderation, the latter being a tool for victims to challenge a platform's inaction. Similarly, **Article 21** introduces an out-of-court dispute settlement. We have no information on whether Meta or X have implemented these two provisions at this stage.	On the one hand, the victims of the Doppelganger campaign can appeal the platform's decision not to remove their content (under-moderation). On the other hand, although less likely to occur, the actors behind the operation could potentially appeal the platform's decision to remove their content (over-moderation) and seek an out-of-court dispute settlement.	Less distribution of illegal and harmful content
Illegal content	Platforms Users	Content moderation Denial of service	**Article 23** on measures and protection against misuse allows a platform to suspend its services to recipients that frequently provide manifestly illegal content for a reasonable period. We have no information on whether Meta or X have implemented these two provisions at this stage.	Meta reportedly enforced takedowns and "blocked hundreds" of spoofed domains. Contrarily, X did not report on its action regarding Doppelganger.	Less distribution of illegal content

Illegal v. harmful content	Stakeholders involved	Potential actions	Relevant DSA articles	Application in the Doppelganger case	Impact
Illegal and harmful content	Platforms	Ads transparency Content moderation	Facebook failed to disclose to its users the real identity of those who paid for the advertisement, violating **Article 26** on online advertising transparency. **Article 39** foresees additional online advertising transparency for VLOPs, including a searchable repository of ads.	Facebook ads used in the campaign relied on fake personas. Thus, they did not include the natural or legal person "on whose behalf the advertisement is presented" (Article 26.1(b)) and "who paid for the advertisement" (Article 26.1(c)). During the investigation, retrieving the ads related to the campaign was very difficult, as only issue- or political-based ads are currently archived in the Meta Ad Library. Nonetheless, ad-related information is even less accessible for other VLOPs, such as X, hindering research and attribution. In 2023, X relaunched Ads Transparency to comply with the DSA, creating an Ad Repository for ads served in the EU. However, the latter proves not to be activable as it requires searching campaigns per advertiser and not by keywords, leaving researchers with no data available if they have no idea who's advertising a campaign.	More situational awareness More attribution opportunities
Illegal and harmful content	Platforms	Content moderation Liability and accountability Reporting of actions taken Risk assessment and mitigation	The risk assessment envisioned by **Article 34** is fundamental. Social media platforms should consider the risks caused by the Doppelganger operation as a systemic risk through their services, given the severity of its potential impact on victims, its impact on a potentially unlimited amount of people, the irreversibility of financial damage, and the likelihood of reoccurrence (see Recital 79). Risk assessment might include drawing up codes of conduct and a regular reporting framework on any measures taken and their outcomes, as written in **Article 45**. **Article 35** on risk mitigation considers the measures that platforms should take to mitigate the risks posed by the campaign. They should assess to what extent their algorithmic structure and advertising system can be changed to prevent operations like this from happening in the future, for instance, by ensuring a better authentication system for advertisers.	The provision is especially relevant in countries like Belgium or Germany, which do not consider disinformation *per se* as illegal content. Still, it might refer to the impersonation and violation of trademark laws undergone by media outlets or journalists. The second phase of the Doppelganger operation – ongoing despite Meta's awareness and criminal charges being filed by Le Parisien and Süddeutsche Zeitung – shows that systemic risks are not being properly addressed. The operation is also ongoing on X, as another evidence that systemic risks were not tackled adequately. For instance, both platforms should assess to what extent its terms and conditions (Article 14 and 35.1(b)), content moderation processes (Article 35.1(c)), or advertising system (Article 35.1(e)) need to be altered to prevent operations like this from reoccurring.	Less distribution of illegal and harmful content Deter illegal and harmful content

Illegal v. harmful content	Stakeholders involved	Potential actions	Relevant DSA articles	Application in the Doppelganger case	Impact
Illegal and harmful content	Platforms	Content moderation	**Article 14** on terms and conditions does not apply *per se*, but platforms can specify that their terms and conditions prohibit impersonating third parties.	In that case, impersonation in Doppelganger would violate Meta's policy on Inauthentic_Behaviour. However, the policy must be more explicit to cover the case study. Moreover, X also prohibits impersonation and deceptive identities.	Less distribution of illegal and harmful content
Illegal and harmful content	Vetted researchers	Access to data Ads transparency Content moderation Liability and accountability Reporting on actions taken Risk assessment and mitigation	**Article 40** defines data access and scrutiny by vetted researchers for research purposes. It is worth noting that the General Data Protection Regulation's (GDPR) principles are safeguarded.	Regarding the present case study, a data access request could have been focused on the following points: **Amplification loop** – Understanding how the sharing mechanisms of fake links worked (e.g., through ads, posts, or accounts amplifying the content) to map the spread of the campaign on platforms and whether the same domains or assets were used in other ongoing operations. – Knowing if, why, and how a piece of content has been recommended per Article 27 about recommender system transparency. – Reducing restrictions for researchers regarding general public access to data, as defined by Article 40(12), for instance, reproducing for multiple platforms tools such as CrowdTangle would allow to understand better the operation's cross-platform diffusion besides Meta. In fact, a similar tool for X would be very useful for facilitating data access, especially after X's decision to limit its API and search functions. Archiving data – Creating a repository of takedowns, removed ads, and any relevant harmful content linked to disinformation campaigns would enable researchers to access it for future investigations, implementing Recital 97. In the Doppelganger operation, only a small portion of the ads were qualified as issue-based or political and thus archived in Meta's Ad Library. The lack of a repository for ads on X and other platforms hindered the possibility of mapping the campaign elsewhere.	More situational awareness More attribution opportunities

Illegal v. harmful content	Stakeholders involved	Potential actions	Relevant DSA articles	Application in the Doppelganger case	Impact
				– Accessing a strike history archive that does not expire would help identify repeated offenders and better understand the working of Article 23's measures and protection against misuse. – Shedding light on content moderation practices, such as accessing information about the overall number of Doppelganger-related content reported that was not moderated and why. This would help researchers understand how a platform manages complaints and the rationale for applying their policies, increasing accountability for platform action and inaction in line with the DSA's complaint-handling system established by Article 20. **Threat entity** – In the Adversarial Threat Report Q1 2023, Meta published clear threat indicators – e.g., URLs, domains, or other clear indicators used in harmful campaigns. The publication of similar information by other platforms involved, such as X, would help further the investigation and apply standardisation-oriented models such as the Kill Chain or the DISARM framework.	
Illegal and harmful content	Platforms User	Liability and accountability Appeal decisions	According to **Article 53**, the recipients of the service have the right to lodge a complaint against a platform's lack of adequate response to their notices or violation of other provisions. **Article 54** adds that, per EU and national law, service recipients shall have the right to seek compensation from platforms for infringing their obligations.	The provision allows a broad understanding of recipients, including the mimicked media, targeted journalists, organisations like EU DisinfoLab, and regular users. A necessary disclaimer is that service recipients must prove how the platform's shortcomings damaged them to obtain compensation.	Less distribution of illegal content Deter illegal and harmful content

Who, what, and why: The stakeholders, actions, and expected impact behind the DSA implementation

Cooperation and obligation: Interactions between stakeholders

The DSA paves a two-way street between the stakeholders that populate the digital space. Platforms are always on the receiving hand in this interaction, as their responsibilities are regulated. In order to deepen the understanding of these dynamics, we present a visual representation of some salient articles and discuss them briefly.

- **Platforms and national judicial or administrative authorities (Articles 9 and 10)**

National judicial and administrative authorities act as gatekeepers of platform liability and accountability in the presence of illegal content. Member States' authorities can access data following an order to provide information (Article 10) and demand action in terms of content moderation with an order to act (Article 9). In return, platforms have to report to the authorities receiving the order and taking action, which can consist of moderating illegal content.

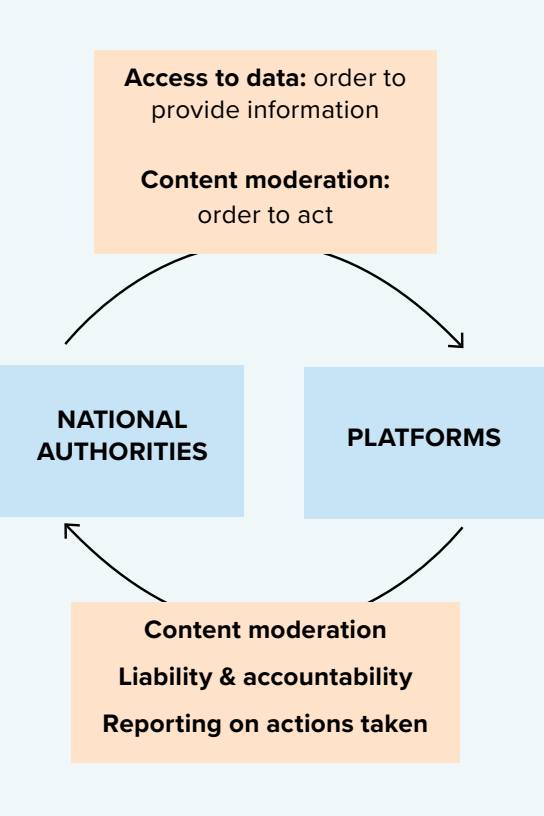


Figure 6 – A visual representation of Articles 9 and 10

- **Platforms and users (Articles 16, 20, 21, and 23)**

Under the DSA, users can report illegal content to platforms (Article 16), which is a means to activate the platform's content moderation policies as well as their liability. Moreover, users can also appeal to the platform's content moderation decisions (Articles 20 and 21), holding them accountable for their

actions or inaction. As the relation goes both ways, platforms can also deny their service to users who frequently and manifestly share illegal content for a period they see fit (Article 23).

- **Platforms and vetted researchers (Article 40)**

The DSA also envisions data access and scrutiny for vetted researchers. According to Article 40(8), vetted researchers must fulfil several conditions. They must be affiliated with a research organisation, be independent of commercial interests, disclose the research funding, and be capable of fulfilling the specific data security and confidentiality requirements (including GDPR). Besides, they must duly justify the necessity and proportionality of their request and agree to make the results of their investigation public. At EU DisinfoLab, we advocate for a larger understanding of vetted researchers, comprising non-academic researchers, CSO experts, and journalists.

In brief, the process envisaged by Article 40(4) entails that researchers go to a regulator (see the paragraph about Digital Services Coordinators in Section 4) with a research proposal, specifying why the requested data is necessary and proportional to answer their researcher question, what is the ideal data access formats, and which data protection safeguards they will put in place. The regulator will approve or reject the application based on several criteria, and if the request is approved, platforms must provide the data within 15 days. As discussed earlier when suggesting what a data access request would look like in the Doppelganger case, this provision would favour greater transparency on ads and content moderation practices, as well as a deeper understanding of the systematic actions taken and risks assessment and mitigation avenues pursued. Ultimately, data access would mean more in-platform and cross-platform liability and accountability.

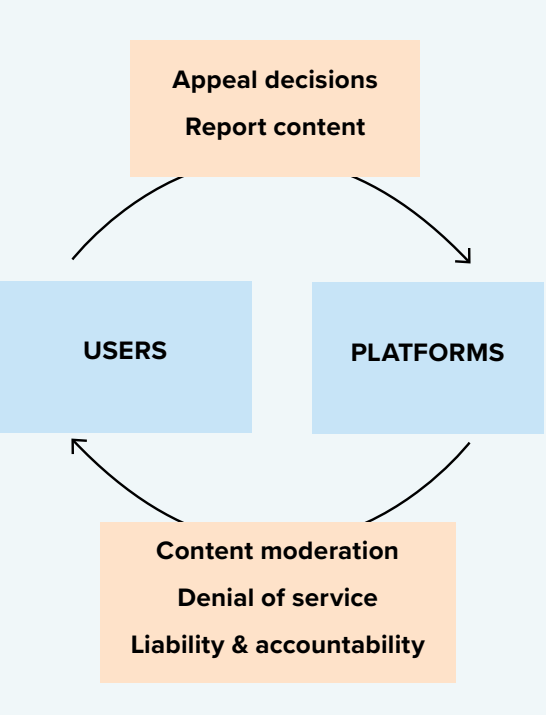


Figure 7 – A visual representation of Articles 16, 20, 21, and 23

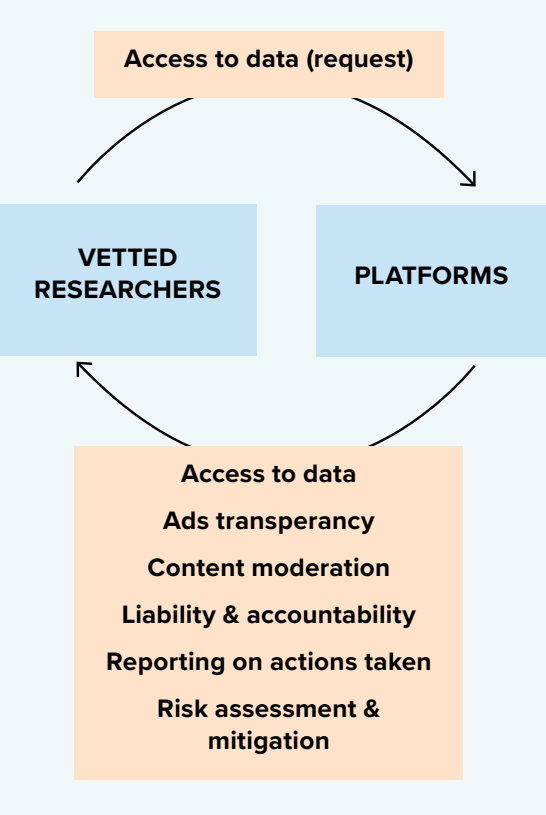


Figure 8 – A visual representation of Article 40

From action to impact: Drawing the best-case scenario

The previous section focused on the actions that various stakeholders can take in the context of the DSA. Of course, this simplifies a complex process, actions are not mutually exclusive but influence and enhance one another. For instance, we saw how access to data could elicit ad transparency, content moderation can lead to denial of service, and everything favours liability and accountability.

In addition, these actions seek to positively impact the digital space. Our analysis concluded that all these actions, as indicated by the various DSA provisions, have two overarching objectives:

- Understanding the mechanisms behind the proliferation of illegal and harmful content
- Creating a safer online environment free from illegal and harmful content

Again, these goals are intertwined: reducing the distribution of said content implies analysing it in depth and, if possible, identifying the actors behind it, which brings greater awareness and more resilience so that similar operations do not happen again. Another virtuous aspect is that this whole process enhances transparency and open-source knowledge-sharing.

The table below shows how stakeholders' actions intersect with the avenues of mitigation. In particular:

1. Higher levels of situational awareness are ensured, for instance, by granting access to data, reporting on actions taken, or assessing and mitigating platforms' systemic risks. The result is to increase stakeholder resilience to illegal and harmful content.

2. More opportunities for attribution are permitted by having platforms report on the actions taken to combat illegal and harmful content or granting vetted researchers data access.

3. The lower distribution of illegal and harmful content on the platforms can be achieved, for example, through content moderation or access to data, which can also ensure cross-country and cross-platform solutions.

4. Deterrence, i.e., avoiding repetition, can be a virtuous effect of holding the platforms liable and accountable or an effective risk assessment and mitigation. Furthermore, sanctions have a tremendously valuable deterrence effect.

	IMPACT			
ACTION	**Deterrence**	**Less distribution**	**More attribution opportunities**	**More situational awareness**
Access to data			x	x
Ads transparency			x	x
Appeal, report, and complain	x	x		
Content moderation	x	x		x
Denial of service		x		
Liability and accountability	x	x		x
Reporting of actions taken	x	x	x	x
Risk assessment and mitigation	x	x	x	x
DSA sanctions on platforms	x			

Final considerations on DSA implementation

The report performed a match-making exercise between the Doppelganger operation identified by EU DisinfoLab and the potentially applicable articles of the Digital Services Act. At the time of the investigation, the DSA had not entered into force yet. However, the case study offers a good testing ground to reflect on the implementation of the regulation.

An ongoing campaign despite our best efforts

A few considerations emerge, especially given the ongoing nature of the operation in France and Germany, as reported in June 2023. An open question remains, wondering how the campaign may still be active despite the robust evidence produced by researchers, Meta's acknowledgement of its existence and undeniable effort to constraint it, and the legal consequences unleashed in the two countries.

NATO, a target itself of the Doppelganger campaign

According to a recent Graphika's report, NATO was impersonated through the domain nato[.]ws, registered on 5 July. The fake website was used to host two sets of counterfeit NATO press releases published in French, English, Russian, and Ukrainian in the context of last July's NATO summit in Vilnius. Based on behavioural indicators (mainly hosting data, behavioural fingerprints, and amplification patterns), Graphika researchers attribute the operation with medium confidence to Doppelganger. On 29 August 2023, Meta confirmed in its Adversarial Threat Report Q2 2023 the existence of new campaign assets impersonating NATO. This fact raises NATO's status itself to a Doppelganger target almost one year after the campaign was unveiled.

Compliance with the General Data Protection Regulation (GDPR)

The criteria defined by Article 40(8) to vet researchers interested in accessing data within the framework of the DSA includes fulfilling specific data security and confidentiality requirements, in line with GDPR. Similarly, data protection and privacy principles apply to the national authorities' orders to provide information established by Article 10. Moreover, specific exemptions allow data sharing for research and law enforcement. Therefore, GDPR poses some legitimate challenges in this scenario, but it should not be an excuse to slow down the DSA-mandated data access. The matter will be certainly addressed in the upcoming delegated acts focusing on data access, which will lay down technical conditions and purposes for data sharing.

The open role of the Digital Services Coordinators

As a new figure created by the DSA (Article 49), The Digital Services Coordinators (with the powers granted by Article 51) will play a role in platform accountability and digital security. However, since their appointment by the authorities is still pending, their role and potential impact remain unclear. Sharing information (Article 85) or promoting joint investigations (Article 60) emerge as two potential actionable areas, but the lack of precedents only permits speculation. In a merely imaginative exercise, we wonder whether and how their existence might have prevented or reduced the spread of the Doppelganger campaign in different countries. Referring to the system established by Article 85, which allows information sharing (i.e., regarding judicial or administrative authority's orders), we imagine that the DSC of the first country where the Doppelganger campaign was detected could have alerted the DSCs in other countries. Together, they could have monitored the actions of the platforms involved in their respective countries more closely, avoiding being caught unnoticed.

The best-case scenario to pave the way for DSA implementation

We outlined a best-case scenario where the distribution of illegal and harmful content online is contained, more information

is available about the actors and the whole situation, and additional cases are avoided. Yet, it is essential to acknowledge that some measures are easier to implement than others. Most DSA actions are aimed at decreasing the distribution of illegal content on platforms, which is accomplished mainly through content moderation and a structural re-evaluation of their distribution mechanisms. Yet, things become more complicated when addressing cross-border distribution, as the Member State-level prevails in the implementation. Instead, fewer actions lead to attribution, a challenge for many stakeholders and crucial for tackling disinformation. Another key aspect is to prevent similar cases from happening and to exert a deterrent effect, which can only be achieved if platforms are held accountable for distributing illegal and, in some circumstances, harmful content and ultimately sanctioned.

Getting an early start and hoping to get further

A potential drawback of this analysis lies in the fact that the DSA is in the middle of a very complex application process – and the capabilities of platforms and Member States to enforce the provisions are unclear. However, we firmly believe that researchers should continue to explore and test what the application of the DSA will look like. Hopefully, this report inspires the community to familiarise themselves with this exceptional tool and incentivises stakeholders to seize the opportunity and take action before the regulation is fully implemented.

Another future aspect to consider is that the **Code of Practice on Disinformation** aims to become a mitigation measure and a Code of Conduct for VLOPs recognised under the DSA. Article 45 and **Recital 106** allow implementing the Code of Practice on disinformation as a risk mitigation measure. However, at this stage, the Code of Practice is not the Code of Conduct and understanding its mobilisation within the DSA framework will require a legal assessment in the future. One thing is sure: the continuously evolving nature of the digital space, with its regulation, malign and benign actors populating it, reveals infinite potential for research. Further analysis is encouraged to assess the progress on DSA enforcement – which has limits and greatly depends on Member States' enforcement capabilities – evaluate new findings in view of an ongoing campaign and explore avenues for standardisation offered, for instance, by the DISARM framework.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org