حملة - المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

Palestinian Digital Rights and the Extraterritorial Impact of the European Union's Digital Services Act

7amleh - The Arab Center for the Advancement of Social Media
April 2024

Position Paper on Palestinian Digital Rights and the Extraterritorial Impact of the European Union's Digital Services Act (DSA)

Author: Itxaso Domínguez de Olazábal
Revised and Edited by: Jalal Abukhater and Eric Sype
Design: Majd Shurbaji

Contact us:
Email: info@7amleh.org
Website: www.7amleh.org
Telephone: +972 (0) 7740 20670
Find us on social media: **7amleh**

Table of Content

Acronyms

- CSO – Civil Society Organisation
- DOI - Dangerous Individuals and Organisations
- DSA – Digital Services Act
- DSC - Digital Services Coordinator
- EBDS - European Board for Digital Services
- EC – European Commission
- EU – European Union
- IHRA WDA - International Holocaust Remembrance Alliance Working Definition of Antisemitism
- IRU – Internet Referral Unit
- MS – Member State
- TERREG - Regulation To Address The Dissemination Of Terrorist Content Online
- UNGPs - UN Guiding Principles on Business and Human Rights
- VLOPs - Very Large Online Platforms
- VLOSEs - Very Large Online Search Engines

Executive Summary

This study delves into the intricate intersection of European Union (EU) legislation, particularly the Digital Services Act (DSA) and Palestinian digital rights, shedding light on the adverse extraterritorial impact of the DSA, notably regarding contexts of conflict and crisis, extending its influence globally and affecting platforms' operations beyond EU borders. The findings, with a particular focus on the context post-7th October, underscore alarming indications that the enforcement of the DSA contributes to the violation of Palestinian digital rights. In a landscape marked by the politicisation of EU institutions, there is a risk that the DSA could inadvertently compromise the very rights it aims to protect, posing challenges to free expression, access to information, and safety both within and beyond the EU.

Introduction

This study, a culmination of 7amleh-The Arab Center for the Advancement of Social Media's extensive efforts, investigates the intricate relationship between the Israel/Palestine context and European Union (EU) legislation, particularly the Digital Services Act (DSA). While recognised as a positive step for addressing illegal and harmful content and fortifying digital rights in the EU, concerns have arisen about its unintended repercussions on Palestinian digital rights[1]. Initially, apprehensions focused on the potential replication of laws empowering illiberal regimes (and this might be true regarding Israel's now frozen so-called 'Facebook Bill') and the risk of diminished big tech investments in content moderation resources in 'the rest of the world', but this study shows that the focus should be also put elsewhere, notably when it comes to contexts of conflicts and crises.

This study casts light on the DSA's adverse extraterritorial impact stemming from content moderation decisions taken regarding content produced within the EU that extend their influence far beyond that territory, affecting platforms' operations on a global scale. While primarily centred on the Palestinian context, the findings and insights hold valuable potential for application in various communities worldwide, particularly in the Global South, considering recent instances of DSA enforcement raising similar concerns about restrictions on legitimate expression.

Examining the specific landscape of Palestinian digital rights post-7th October, marked by a spectrum of transgressions, the study addresses discrimination and censorship concerns, as well as the violation of other rights, within the EU, affecting both Palestinians and global advocates for Palestinian human rights. The subsequent sections provide an overview of the DSA, its components, and implications, followed by an exploration of its relevance and impact on Palestinian digital rights. Examining violations post-7th October, the study concludes with actionable recommendations to mitigate challenges and safeguard digital rights in the Palestinian context, but also across other contexts.

1. This expression encapsulates the infringement upon digital rights, viewed through the lens of human rights, affecting not only Palestinian individuals but also extending to non-Palestinian rights-holders who champion Palestinian human rights across various platforms and in diverse contexts globally.

Objectives and Methodology

- The study is guided by a number of research questions:
- How does the way the DSA addresses (and differentiates between) hate speech and harmful content impact Palestinian digital rights on major online platforms?
- What does the online experience post-7th October tell us about the potential advantages and dangers of DSA enforcement for Palestinian digital rights?
- To what extent might the politicisation of the DSA by the EU affect its application and relevance to Palestinian digital rights?
- What are the potential benefits and limitations of the mechanisms devised by the DSA in improving the Palestinian online experience?

The study employs various methodologies, including a literature review, desk research, and legal analysis. It also includes an in-depth study of relevant reports from 7or - The Palestinian Observatory of Digital Rights Violations, along with similar material obtained through interviews formally and informally[2]. This approach examines both the quantitative and qualitative dimensions of the study phenomena.

The DSA in a nutshell

One of the goals of the EU's Digital Agenda was to rein in the power of Big Tech companies, but also to address the dangerous threats of online harms. One of the 'jewels of the crown' was the Digital Services Act, whose final text was adopted on 19th October 2022. It became effective for Very Large Online Platforms (**VLOPs**) on 25th August 2023 and became fully applicable across the EU for all entities in its scope on 17th February 2024. The goal was to set harmonised and clear rules on intermediary services online, all hosting services and online platforms providing services within the EU, thus regulating the interactions between users and providers concerning content moderation and other sensitive areas, ensuring fundamental rights are protected through meaningful safeguards. The DSA applies to all online intermediary service providers, as long as their users have their place of establishment or residence in the EU. Specific obligations and more stringent regulations are set up to rein in the power of VLOPs and VLOSEs **(Very Large Online Search Engines**).

2. Five interviews were conducted with EU users affected by content moderation decisions, spanning various platforms. To ensure security, their names cannot be disclosed. Additionally, an interview was held on March 6, 2024, with Deborah Brown, acting associate director in the Technology and Human Rights division, and Rasha Younes, acting deputy director in the Lesbian, Gay, Bisexual, and Transgender (LGBT) Rights program at Human Rights Watch. They are the researchers and authors behind Human Rights Watch's report titled 'Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook.'

The European Commission (**EC**) has the role of supervision, investigation, enforcement and monitoring of VLOPs and VLOSEs. Each Member State (**MS**) will appoint a Digital Services Coordinator (**DSC**) responsible for overseeing smaller platforms and enforcing the legislation in other means. A European Board for Digital Services (**EBDS**) will be created. An essential feature of the DSA is that failure to comply with its rules may result in fines, which can go up to 6% of VLOPs' global turnover.

• Illegal and harmful content

The DSA focuses on the central concept of 'illegal content,' and the platforms' primary obligation is to act rapidly to delete illegal content. The DSA also addresses the urgency of harmful content and dis- and misinformation. Whereas the text speaks of 'otherwise harmful content and activities online,' it does not contain any definition of what 'harmful content' is, reflecting the difficulties of reconciling this notion with the fundamental right to freedom of expression. When it comes to disinformation, the 2022 Code of Practice on Disinformation defines the term as 'false or misleading content that is disseminated with the intention to deceive or achieve economic or political gain and that may cause public harm.'

• Content moderation rules

While the rule before was a self-regulatory paradigm and a limited liability framework, the DSA imposes on platforms a conditional liability regime and a mandatory 'notice-and-action' system. One of the most important victories for CSOs was a ban on general content monitoring: platforms don't have to monitor content systematically and, under a conditional model of intermediary liability, they just have to be able to clearly identify the illegality of the content without a detailed legal examination, thus establishing a -tricky- distinction between scanning everything to identify illegal content on one hand and being or becoming aware of specific illegal content on the other. This is where the 'Procedure Before Substance' approach to content moderation comes in: the text guarantees people can reclaim action and accountability in cases of alleged online harm through the codification of the notice and takedown and complaint mechanisms. Platforms can act or not upon the notices, when those are precise and substantiated. Additionally, platforms must provide a statement of reasons and explicitly mention whether they use automated means. They also need to inform both the notifiers and the concerned users of their decision without undue delay.

There will be different **ways for platforms to know about the presence of illegal content:**

- First, we have 'Orders to act against illegal content', according to which MS' judicial or administrative authorities will be priority informants. Platforms are also obliged to respond to MS' Orders to provide information.
- In line with their conditional liability, platforms have to conduct monitoring for content that has been proven or is manifestly illegal.
- Notices can also be submitted by individuals or entities using the respective Notice and action mechanisms.

The DSA also introduces **complaint and redress mechanisms**. The possibility of appeal includes a three-tiered grievance mechanism: internal complaint, out-of-court dispute settlements, and even court challenges. The efficacy of addressing online harm and abuse will continue to rely on the platform's adherence to DSA requirements and the specific procedural laws of each nation more broadly.

• Transparency Obligations

The DSA introduces transparency obligations for different actors: the EC, platforms, DSCs, and Trusted Flaggers. Notably, platforms will produce annual reports detailing, amongst others, the number of takedown requests and users' complaints. Additionally, transparency reports must refer to automation and disclose accuracy and possible error rates. The first round of reports was published in the Autumn of 2023. The EC also introduced a DSA Transparency Database in August 2023, enabling scrutiny of content moderation decisions.

When it comes to transparency, it is also critical to mention that the DSA also stresses the need for platforms to provide access to data for researchers, which might in principle include CSOs. Vetted researchers would possess the capability to access platform data for investigating relevant harms and dynamics related to platform operations. However, providers may be able to cite trade secrets as a reason to withhold data access from researchers. Up until the moment the study was published, the process has proven to be exceptionally challenging for both individual and collective researchers who have sought to utilise the system.

• Risk assessment and mitigation

The DSA emphasises duty-of-care obligations and accountability alongside procedural obligations. This includes requiring VLOPs to conduct and publish annual reports on risk assessments, providing information to the EC and DSCs upon request. Risk assessments will inform content moderation adjustments, with platforms mandated to mitigate identified risks, especially concerning fundamental rights. Fundamental Rights Impact Assessments will be conducted annually and when significant functional changes occur. VLOPs must undergo annual independent audits of their algorithms' impact on democracy and human rights, complemented by EC scrutiny.

The DSA lacks provisions for a particular delegated act or guidelines that would establish standardised rules for risk assessments and, furthermore, does not provide a precise definition for a crucial element like risk. For a risk to be relevant, it must meet the threshold to be considered a 'systemic' risk. Importantly for Palestinian digital rights, extraterritorial aspects concerning risks may pertain to either the origin or the impact of these risks. The DSA text does not indicate any exclusion of risks originating from outside the EU in a risk assessment, as long as these risks can be connected to individuals located within the EU.

• The Role of Civil Society

Another victory for CSOs was the reference to stakeholder engagement, albeit again characterised by the absence of precise definitions. This indefiniteness opened the door for civil society to be major actors in the implementation and enforcement of the text. A key responsibility involves ensuring the efficacy of DSA provisions by actively participating in the formulation of delegated acts and guidelines overseen by the EC during the drafting process.

The relevance of DSA for Palestinian digital rights

Despite platforms being theoretically encouraged not to excessively police online speech due to the conditional liability regime and the emphasis on freedom of expression as a fundamental right in the EU and the DSA, practical implications suggest an invitation to do so. This is particularly evident in the case of Palestinian digital rights, resulting from interconnected phenomena related to the behaviour of both platforms and institutions at various levels described below.

• Politicisation and biased framing at the hands of institutions

Despite the DSA's aim to prevent fragmentation, its implementation depends a lot on the actions of MS' judicial, administrative, and regulatory bodies and, with that, on the political context in each MS, and of the EU as a whole. Particularly, the EC is supposed to be an independent regulator and enforcer. However, at the end of the day, it is a political entity, specifically the main executive body of the EU, with the power to influence the tensions between the DSA's different policy objectives, notably when it comes to battling online content on one hand and ensuring the protection of fundamental rights on the other. Add to that the EC's interests beyond DSA, mainly the goals of the different Commissioners, the EU's own objectives, and even the goals of relevant EU leaders and governments. Threatened with an investigation under DSA rules, platforms might be pushed to over-enforcement so as to limit their liability instead of prioritising contextual analysis and caring for freedom of expression, leading to over-moderation of pro-Palestinian content. The pressure is also exerted -directly or indirectly- on other relevant actors at the supranational or national level, for instance, Trusted Flaggers.
The definition of 'illegal content' refers to *'any information, which, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State, irrespective of the precise subject matter or nature of that law'*. The legislators thus opted for an open definition of the term: it was to depend on what the applicable law or the relevant rules would render illegal, in regard to information, irrespective of its form and illegal activities. The text provides specific examples of what could be 'illegal content', namely 'illegal hate speech or terrorist content and unlawful discriminatory content'.

• Potential instrumentalisation of the Working Definition of Antisemitism adopted by the International Holocaust Remembrance Alliance (IHRA WDA)

One of the pillars of the DSA's critical concept of 'illegal content' is 'illegal hate speech': it has to be defined by member states, with considerable discrepancies in regard to what constitutes hate speech in different MS. Antisemitism rightly falls under that concept in many member states. However, the struggle against antisemitic content has become one of the primary avenues for politicisation, as a consequence of the IHRA WDA. This definition is being employed by public actors across the EU as if it were a legal mandate, despite being officially labelled as 'non-legally binding.' The instrumentalisation is associated with the definition's 'contemporary examples of antisemitism,' which are characterised by conflating antisemitism with legitimate criticism of Israel. This conflation is often utilised to restrict the freedom of expression for advocates of Palestinian human rights.

Indeed, there have been a considerable number of attempts by pro-Israel advocates to interfere with the process of DSA drafting and enforcement so that it explicitly encompasses the IHRA WDA. A worrying precedent is Germany's 2017 NetzDG: section 46 was amended by a bill referencing the IHRA WDA regarding hate crimes, and even though it did not make it into the law, law enforcement authorities can use it to request content takedowns. In June 2020, Katharina von Schnurbein, the EC's Coordinator on combating antisemitism, agreed to discuss the DSA with B'nai B'rith, which led to the presentation of conclusions in the online event 'Digital Governance: A Jewish Perspective' on October 21st, 2020, with Věra Jourová (EC's Vice President For Values And Transparency and a staunch supporter of Israel) and some platforms, and in which one of the central messages was that the DSA ought to offer direction and incentive for platforms to embrace and implement the IHRA WDA definition. A definitive evidence of instrumentalisation was the 14th EU – Israel High-Level Seminar On Combating Racism, Xenophobia And Antisemitism held in Jerusalem on June 12th, 2023. In the joint press release, Israeli FM Eli Cohen stated that 'we need to encourage states, organisations and tech companies to adopt the IHRA WDA and embrace tools it provides'.

The threat of instrumentalisation of the IHRA WDA is also symbolised by the 2016 EU Code of Conduct for Countering Hate Speech Online, a voluntary code agreed upon between the EC and several tech companies, now VLOPs, which has been condemned for its negative human rights impact. Amongst others, United Nations experts have criticised it for undermining the Rule of Law and potentially encouraging censorship.

One of the most worrying aspects was that, encouraged to resort to their own terms of service, the companies implementing the Code were neither required to verify whether the content they were removing was illegal or not, nor asked to meaningfully protect freedom of expression. The Code is still in force and is considered fundamental for correctly enforcing the DSA. There are rumours in Brussels saying that it will be reformed, even become official (thus not voluntary any longer) in 2024. The periodic evaluations of the Code (the EC released the seventh assessment in November 2022) are accompanied by Information provided by the companies about measures taken to counter hate speech. Even if there is no way to check in which proportion the IHRA WDA is applied, there is room to believe that might be the case, and that is because of the Code's own Trusted Flaggers, some of which embrace the IHRA WDA, for instance, CEJI – A Jewish Contribution to an Inclusive Europe and LICRA.

• The potential instrumentalisation of the fight against terrorism

Another avenue for politicisation of the DSA with a harmful impact on Palestinian digital rights is the instrumentalisation of the fight against terrorism, one of the most common framings of the context in Israel/Palestine across the EU. This is particularly the case with the potential conflation of DSA and the 2022 Regulation on addressing the dissemination of terrorist content online (TERREG), a legislation which came into force on 7th June 2022 and is considered lex specialis to the DSA and with which it shared as main features the centralisation of enforcement powers and the framework for addressing illegal content online. Digital rights organisations repeatedly showed concern over TERREG, particularly regarding the incentives to over-enforce content moderation policies. TERREG introduces more specific rules as regards the fight against a particular form of illegal content, constraining all hosting service providers offering services in the EU to remove within an hour any content reported as 'terrorist,' following receipt of a removal order issued by Member States' law enforcement authorities. Additionally, platforms need to take proactive measures in locating and deleting content.

There is a danger that the decisions implemented in TERREG's context could also be used to comply with DSA-related obligations. In the case of both texts, if platforms check the flagged content against their terms of reference, the most probable consequence would be the deletion of lawful content that is considered 'sensitive' as a consequence of their problematic Dangerous Individuals and Organisations (DOI) policies. The danger is even higher in the case of automated tools, which cannot differentiate between terrorist content, educational and news materials, or documentation of human rights violations.

There are even instances in which both kinds of politicisation have been used together. For instance, the EC explicitly includes references to terrorism when evaluating 'Actions on combating antisemitism in different policy fields.' Additionally, pro-Israel advocates also link the two: 'Antisemitism must be addressed in all areas of digital policy, such as, illegal terrorist or violent content.' The EC-commissioned study 'Approaches to addressing antisemitism in European P/CVE' openly accepts IHRA WDA and recommends linking online radicalisation with a focus on antisemitism.

• Member States' Orders to act against illegal content

A consensus amongst CSOs working on digital rights is that the DSA should have introduced stronger safeguards against government abuse. Even though the text includes references to fundamental rights, it still risks creating new powers that facilitate carving out the genuine space for freedom of expression and other human rights. The text, indeed, gives too much power to government agencies to flag allegedly illegal content, for Orders can be issued by administrative authorities, even if they do not refer to the prior issuance of a decision of illegality by a competent authority. A clear threat in that regard is how Israel's Ministry of Justice can reach out, as a result of links nourished throughout the years, to EU national bodies requesting they ask for content removal.

• Terms and conditions first

As confirmed by some of the Transparency Reports submitted by VLOPs in November 2023 and the DSA Transparency Database, platforms have developed the habit of first checking the requests received, even if it's through official DSA (or others) channels, against their own terms of reference. This has the danger of leading to global takedown orders and, thus, over-removal, particularly when it comes to the proven insufficiencies of platforms' terms and conditions when dealing with Palestinian content, or content advocating for Palestinian human rights (as demonstrated in, amongst others, a human rights due diligence report commissioned by Meta and carried out by the network Business for Social Responsibility), as it happens with many other under-represented contexts across the Global South.

As indicated by the presence of still confidential -but still problematic- DOI lists, platforms are urged to customise their terms of reference to conform with counter-terrorism strategies. These obligations may necessitate significant, government-mandated alterations to how they currently enforce their terms and conditions.

Additionally, a phenomenon associated with TERREG is that governmental authorities, notably Internet Referral Units (IRUs), as well as other actors, can opt to still request content removal based on breaches of company content policies and not through the legal avenue explicitly established for that purpose for content allegedly violating local laws. In both cases, the biggest threat has to do with platforms' lack of accountability, for transparency obligations do not explicitly include such notices (at the time of writing, the corresponding proposed qualitative and quantitative reporting templates from the EC had not been disclosed to the public).

• Automation, proactive censorship and discriminatory over-compliance

One of the most serious consequences of the DSA regarding Palestinian digital rights is the potential for reduced accuracy in identifying illegal content, along with a rise in unjustified content removals. Even though the text seemingly imposes limits on automated decision-making and platforms are obliged to take a neutral position in relation to their users' content, there are instances in which platforms might inevitably resort to automated mechanisms of content moderation (such as upload filters), sometimes even in higher proportions than it would normally do. This, as we know, exacerbates the risk of censorship and discrimination. As demonstrated in the context of Palestinian digital rights in 7amleh's position paper on AI Technologies Impact on Palestinian Lives and Narratives, algorithms often lack a sufficient understanding of context and magnify existing biases.

To avoid liability for illegal content under the DSA, platforms are mandated to promptly remove or disable access to such content. Even though no specific time limit is specified, this could inevitably lead to further utilisation of automated tools for content moderation. Furthermore, the DSA also adds that conditional liability should not prevent EU or national law, and thus authorities who could potentially fall prey to politicisation, from obliging the platforms to conduct specific monitoring for content that has been proven or is manifestly illegal. When it comes to Palestinian digital rights, resorting to IHRA WDA or pressure from institutions in moments of crisis, the dangers of automation in terms of over-removals are clear.

Over-compliance might also occur without automation, in the case of hate speech. Whereas the deletion of the content should in principle be limited to the country where the content is, indeed, illegal, companies might opt for over-cautiousness and delete the

piece of content across the EU, and even globally. In addition to that, content moderators prepared to deal with situations within the EU might not have enough knowledge of the specifics of the context (or languages) in Israel/Palestine.

• Notices submitted by Trusted Flaggers

In principle, any user can flag illegal content under the notice-and-action mechanism. However, the DSA establishes a specific category of sources: notices submitted by 'Trusted Flaggers' must be processed and decided upon with priority and expeditiously, something that might lead to less comprehensive assessments of the content flagged as illegal.

Trusted Flaggers are entities appointed by and accountable to DSCs, and their status can also be suspended. They are entities which must fulfil a number of criteria. The EC will maintain and regularly update a publicly accessible database that features Trusted Flaggers, and flaggers will need to submit yearly reports on submitted notices. According to the DSA, Trusted Flaggers can be non-governmental organisations. In this regard and related to the instrumentalisation of the IHRA WDA, one of the main dangers is that the problematic CSOs already collaborating with the Code of Conduct for Countering Hate Speech Online (see above)are automatically awarded that status.

Furthermore, the DSA specifies that national or European enforcement authorities might become trusted flaggers. The text expressly refers to the possibility of these authorities becoming Trusted Flaggers 'for terrorist content'. This points to the possibility of enforcement overreach as a consequence of the intervention of MS' or Europol's IRUs. It's important to stress that online platforms are 'inherently biased in favour of the government's favoured positions', and thus they are likely to be compelled to moderate content that they would not have otherwise intervened in. In the case of Palestinian digital rights, there is, therefore, a twofold danger: on the one hand, that Israel's IRU -the so-called 'Cyber Unit'- summons some of those authorities to flag content in line with their narrative and, on the other, that these authorities are influenced by the framing imposed by their national and supranational institutions (see above).

Case Study: the aftermath of the events of 7th October

• Worrying signs of politicisation

A number of events worryingly point to the DSA having been applied with bias, with examples of all the issues identified in the previous section. Much of the issues stem from politicisation: a few days into the invasion of Gaza, European Commissioner Thierry Breton emphasised the global impact of the DSA, albeit without explicit reference to Palestinians. The primary issue lay in the framing of the situation, which aligned closely with a biased mainstream narrative that neglects the Palestinian perspective and ongoing human rights violations by Israel. This narrow focus perpetuates a one-sided narrative that overlooks the complexities and nuances essential in understanding the situation's full scope, undermining efforts to address Palestinian human rights issues. These interventions do not just avoid mentioning how online platforms may be used to incite violence against Palestinians and infringe on other fundamental rights of both Palestinians and Palestinians who support human rights. They also shed light on avenues to coerce the platforms into over-complying and discriminating content moderation practices mentioned above. It's important to emphasise that the censorship of Palestinian and pro-Palestinian content in the EU is a consequence of both the DSA-related dynamics identified in this study and the results of the platforms' content moderation policies and practices on a global scale.

Breton warned X, Meta and TikTok of their obligations under the text. 7amleh, in conjunction with other civil society organisations dedicated to upholding digital rights, voiced concerns regarding this portrayal of the context and with it about the EC's role in enforcing the text. Even more tellingly, on 18th October, the EC reaffirmed its position by proposing a temporary 'incident response mechanism' until the DSA is enforced. The framework urged MS to expedite DSA governance to coordinate efforts in addressing the 'spread and amplification of illegal content,' highlighting a 'serious threat to public security.' The same day, the European Parliament held a debate titled 'Fighting Disinformation and the Spread of Illegal Content in the Context of the Digital Services Act during Times of Conflict,' in which Vice President of the EC, Věra Jourová, referred to 'online platforms becoming a tool for terrorists and the spread of antisemitic and violent illegal content'.

• Instrumentalisation of the fights against terrorism and antisemitism

In alignment with the problematic framing mentioned earlier, particularly concerning the instrumentalisation of terrorism, the EC's Recommendation referred to 'the terrorist attacks by Hamas in Israel' and the war in Ukraine. The accompanying press release focused solely on the Middle East, with the EC's President addressing an 'online assault of heinous, illegal content promoting hatred and terror.' The EC's specifically suggested utilising TERREG and other counterterrorism structures to combat illegal content. Aligned with this perspective, a leaked document from December 2023 by the NGO Statewatch, specialised in surveilling, scrutinising, and unveiling governmental actions that jeopardise civil liberties, revealed a plan formulated by France, Germany, and Italy. This plan, characterised by ambiguous language and a broad scope, outlines strategies to counter Hamas activities. It includes a section on monitoring and enforcing obligations on online platforms, raising concerns that various governments might exploit the online space for further actions against Palestinian digital rights. This is exacerbated by the fact that platforms consistently engage in arbitrary and erroneous over-enforcement of anti-terrorism policies, often falling short of meeting due process criteria.

The EC's framing also pointed to an instrumentalisation of the IHRA WDA. The Recommendation expressed concern about 'a clear risk of intimidating groups of the population,' possibly alluding to antisemitic content. The proposed response mechanism encouraged member states discussing 'good practices and methodologies' and regularly reporting and exchanging information collected at the national level, and that despite variations in the definition of illegal hate speech across countries.

• Enforcement overreach

The post-7th October context has also shed light on the threat of enforcement overreach. Referring to the imperative to 'anticipate threats of waves of illegal hate speech before content has gone viral online' and highlighting the expectation for signatory platforms to remove such content 'within the majority of cases within 24 hours,' the EC underscored the revision of the Code of Conduct on Countering Hate Speech Online mentioned hereinabove. This revision would indirectly promote swift removals, potentially resulting in false positives, as well as the removal of content that might be subject to the conflation of antisemitism and criticism of Israel. As we know from an array of

studios, the prioritisation of speed over due diligence in content removal results in the unjust removal of legitimate content, breaching DSA provisions in a context where nuanced contextual understanding is crucial. The zeal to combat illegal content at any cost exerts significant pressure on VLOPs to act swiftly and decisively, even if it means relying on imperfect and opaque algorithmic tools to avoid liability and public scrutiny. Additionally, regarding over-enforcement, the EC's Recommendation reminded that orders could be issued on a cross-border basis. In practice, as specified, most of the time, these lead to global takedown orders, leaving EU users without explanations for the reasons for the content removal.

• Conflation with disinformation

Another worrisome aspect of the current framing is the conflation in the DSA's treatment of illegal content and disinformation. The text establishes distinct regulatory approaches for these content types. VLOPs are tasked with assessing the risks their systems pose to society and taking actions to mitigate these risks, encompassing the need to address disinformation while also considering threats to freedom of expression. This balance is crucial for Palestinian digital rights. However, due to the problematic framing of the context, there is a risk that the labelling of legitimate content as 'disinformation' may further suppress Palestinian narratives and accounts of the reality on the ground.

• Quantitative and qualitative evidence

Instead of adhering to the principle that any restriction on freedom of expression must be necessary and proportionate, the post-7th October implementation of the DSA paints a picture of unjust and disproportionate removal of lawful content produced by users advocating for Palestinian human rights in the EU. The evidence obtained through 7or-The Palestinian Observatory for Digital Rights Violations - 127 reported cases of violations in the period from 7th October to Late January 2024[3] - points to the fact that online platforms have removed Palestinian-related lawful content and suspended Palestinian-related accounts within the EU. This evidence is corroborated by data collected by Human Rights Watch during the preparation of their report, 'Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook.' The report highlights over 100 cases of violations on Meta's platforms in 16 EU Member States (out of 1,049 cases of content takedowns or suppression of content) between October and November 2023. Additionally, incitement to violence from within the EU

3. An important caveat is that the option for users to report violations to 7or, indicating that they are located in Europe, was not introduced until the first week of October 2023. Additionally, the reported cases represent only instances disclosed by individuals familiar with the platform, and therefore may not precisely reflect the comprehensive landscape of censorship.

against Palestinians -often accompanied by disinformation- persists as a grave issue. Despite efforts to report the latter kind of content as illegal under the DSA, these actions have not resulted in satisfactory responses.

A portion of content generated by Palestinians has been removed by online platforms in response to requests from Israel's 'Cyber Unit.' At the global level, these removal requests have seen in the past a high rate of acceptance, with Meta and TikTok responding affirmatively to 90% and 85% of these requests, respectively, according to one report from October 2023. Importantly, VLOPs have also reportedly received takedown demands from EU law enforcement authorities (for instance, according to the EC's report on the implementation of TERREG made public on 14 February 2024, Germany's Federal Criminal Police Office issued 249 removal orders from 7th October to 31st December 2023), a situation that raises valid concerns about the potential involvement of law enforcement agencies as Trusted Flaggers. This intricate relationship is intrinsically connected to the substantial political pressures exerted on online platforms from various fronts.

• Human rights impacts

Concerning the concrete human rights implications of implementing the DSA under the described circumstances, it is vital to mention that the selective pressure to remove only portions of inflammatory content, and not the hate and violent speech targeting Palestinians, leads to discrimination and harm, something particularly concerning given that such content can incite real-life harm on Palestinians in the occupied territory and other marginalised communities across the EU territory. This is particularly concerning in the context of Palestine, as there has been a well documented correlation between harmful content online, and on the ground violence. In early 2023, Israeli settlers organized on X (formerly twitter) to incite a pogrom against the Palestinian village of Huwara, and in the wake of October 7th, top Israeli officials used social media accounts to justify collective punishment for all Palestinians.

In addition to that, the foremost infringed right pertains to freedom of expression. This transgression manifests directly through the stifling of voices and the resultant chilling effect. Another facet of this encroachment on freedom of expression relates to compromised access to information, a consequence exacerbated since 7th October. This compromise is particularly alarming given the current criticality of freedom of expression and access to information regarding the Israel/Palestine context. This urgency arises not only due to the prevalence of biased narratives disseminated by

mainstream media and official institutions but also because of the significant risks faced by Palestinian journalists and human rights advocates reporting on the ground, compounded by frequent blackouts and internet shutdowns. Together with other cases of discrimination throughout the globe, particularly regarding global majority countries, the identified dynamics distort vital information necessary for global understanding and monitoring of human rights abuses.

A second fundamental right systematically violated is the freedom of peaceful assembly and association, especially concerning activists and civil society organisations advocating for Palestinian human rights within the EU. It is crucial to recognize that these breaches impact EU residents, including both long-standing advocates for the Israel/Palestine situation and individuals who previously refrained from engaging in discourse on the matter. The latter group may be more susceptible to the chilling effect, amplifying the detrimental consequences of these restrictions.

Furthermore, the human rights ramifications extend to the freedom to choose a profession. Within this context, residents of the EU affected by these dynamics include not only journalists and human rights defenders but also ordinary citizens. The pervasive atmosphere of fear within platforms such as Instagram and LinkedIn, resulting from disproportionate censorship, has led individuals to curtail expressing their views online. This self-censorship stems from concerns that openly expressing opinions could adversely impact their professional careers and opportunities.

• Adding fuel to the fire

This scenario, coupled with biased contextual framing and the prevailing power imbalances in the region, highlights the encroachment of EU actors into the digital sphere. It paints a picture of the digital space evolving into a battleground where EU governments might feel free to seek to limit free expression. The motives driving content removal often remain ambiguous, owing to a troubling lack of transparency in these activities despite compliance requirements outlined by the DSA that emphasise the need for greater transparency and accountability. Furthermore, the policies implemented by online platforms frequently surpass the limitations allowed under international human rights standards, further contributing to the already prevalent over-enforcement of decisions against Palestinian and pro-Palestinian content.

Conclusion, Recommendations and Potential Action Points

This study has dissected the implications of the DSA within the realm of Palestinian digital rights, particularly in the aftermath of events on 7th October. The findings point to alarming indications that the enforcement of the DSA, whose wording allows for significant interpretation, may, and seemingly has, contributed to the violation of Palestinian digital rights. In an environment characterised by the hyper-politicisation of some EU institutions and leaders, there is a discernible risk that the application of the DSA might inadvertently compromise the very rights it aims to protect. As such, the multifaceted impact of these dynamics poses significant challenges to the principles of free expression, access to information, and the ability to freely choose one's profession and to the right to safety within, but also beyond, the EU.

The study underscores the need for vigilance and proactive measures to address the challenges identified, as the politicised landscape may inadvertently perpetuate an environment where digital rights are not only compromised but also manipulated to serve political agendas. The EC has initiated formal proceedings against X under the DSA, a framework where many of the company's DSA obligations are under scrutiny, some of them notably when it comes to the post-7th October context. The outcome of this process could provide insights into some of the concerns addressed in this study and studied by 7amleh more generally. As the DSA aspires to be a global standard for digital regulation, it is imperative to critically examine its impact on specific contexts, especially those marred by geopolitical complexities. The recommendations provided hereunder, in line with the 'respect, protect, remedy' framework set out under the UN Guiding Principles on Business and Human Rights (**UNGPs**), could serve as a roadmap for stakeholders to navigate the potential pitfalls and to uphold the principles of human rights protection in the context of Palestinian digital rights, as well as other contexts. Only through a vigilant and adaptive approach can the DSA fulfil its intended purpose without inadvertently becoming a tool for the violation of fundamental rights in the EU and beyond.

• Responsibilities of EU institutions regarding the DSA's extraterritorial impact

- The European Commission's DSA enforcement team at DG CONNECT, and other entities responsible for the enforcement and oversight of the text, ought to give increased consideration to the DSA's extraterritorial impact.
- DSA risk assessments must encompass the effects of products and services on individuals and groups who do not directly use the services. Transparency, due diligence, and an unwavering focus on human rights are indispensable in crisis situations to safeguard the rights of all users and rights holders, particularly those from vulnerable communities.
- In line with what BSR calls 'conflict sensitivity', potential spillover from conflict contexts like the one in Israel/Palestine should be included as a systemic risk underscoring the human rights implications of these situations in the EU, taking into account the specifics of the context and avoiding politicisation and instrumentalisation at all times, to avoid discrimination and further fundamental rights violations ultimately. This approach should adopt an intersectional methodology to ensure that mitigation measures and access to remedies encompass the essential mechanisms required for those most severely affected by rights violations.
- Given the DSA's provision of a more significant role for civil society actors, the European Commission (if needed, through the European External Action Service) should engage with digital rights defenders beyond the EU, particularly in the Global South. These CSOs and individuals, both civil society from the concerned territory and EU civil society with expertise in the context, should be involved in a meaningful multistakeholder process. This involvement should take the form of periodic consultation, not just occur in moments of crises.
- EU Member States' Digital Services Coordinators should be mindful of the potential instrumentalisation of the IHRA WDA or the fight against terrorism when appointing Trusted Flaggers, be it CSOs or law enforcement authorities.
- Digital Services Coordinators should establish meaningful relationships with civil society. In the case of Palestinian digital rights, CSOs with a robust understanding of the context should be taken into consideration when appointing Trusted Flaggers.
- Digital Services Coordinators should also investigate the behaviour and potential human rights violations of Trusted Flaggers when these entities are accused of actions resulting in online censorship.

• How Civil Society can Utilise the DSA to protect digital rights concerning Palestine and beyond.

- Civil society and individuals affected by the violations outlined in this study could leverage the complaints mechanism established by the DSA concerning services located or established in a Member State [there is no requirement for EU nationality to file a complaint, and users may be represented by entities outside the EU].
- Civil society and individuals impacted by the violations identified in this study should advocate for the enforcement of clearly defined and publicly documented moderation policies and processes on content flagged by Trusted Flaggers.
- Civil society, particularly digital rights organisations, should have full or meaningful access to the VLOPs' systemic risks self-assessments. Platforms should engage in consultations with affected groups, independent experts, and, particularly in cases of severe human rights violations with significant on-the-ground impacts. In encouraging VLOPs and regulators to address specific risks in their assessments, CSOs should actively provide evidence based on their expertise and deep knowledge of specific contexts.
- CSOs should seize the opportunity to become approved researchers, and shed light on the restrictions imposed upon them in that regard.

• Online platforms: be transparent and go beyond what DSA states

- Because the DSA follows an approach whereby problems will be addressed only where they materialise, platforms should stick to the UNGPs and apply four core elements in their own human rights due diligences: 'assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed'.
- Platforms should refrain from invoking trade secrets as a reason to withhold data access from researchers, and meaningfully facilitate the process of access to data.
- Given that VLOPs' design decisions significantly contribute to 'systemic risks,' particularly through their recommender systems, and considering that platforms implemented changes to these systems post-7th October, it is essential for these platforms to transparently incorporate information about these systems into their risk assessments. This aspect should be a focal point for subsequent independent audits and investigations led by DG CONNECT.
- Include voluntary governmental IRU's requests in their transparency reports.

Contact us:
info@7amleh.org | www.7amleh.org
Find us on social media: **7amleh**