Contextualisation over Replication

Tomiwa Ilori 2022-11-03T10:18:37

Today, at the centre of the debate on online content regulation are questions on how online platforms and governments wield disproportionate powers. It is therefore unsurprising that both online platforms and governments have attempted to consolidate these powers. However, while their attempts have been questionable and sometimes useful, there seems to be a global consensus that online harms, which are legitimate bases for content regulation, threaten human rights and democracies. This consensus is gradually gaining momentum and so are regulatory solutions towards combating these harms. An example of such a solution is the European Union's (EU) Digital Services Act (DSA).

The EU is notorious for using regulatory solutions like the DSA to dominate and pre-empt global digital standards. Often, the major conversations on the international impacts of EU laws have oscillated between capture and actually providing normative leadership on thorny aspects of digital regulation. Even though evidence of such capture is yet to be seen with the DSA, the DSA has shown some regulatory clarity towards regulating online harms, which should be treated with cautious optimism. This contribution discusses this cautious optimism especially as it concerns the DSA's potential impacts in African contexts, if African countries choose to take inspiration from it. This contribution concludes that African countries should develop their own content regulation rules by paying more attention to their contexts and consider aspects of the DSA only where they will improve such local rules.

The ‚Brussels Effect' in African Countries: Like the GDPR, Like the DSA?

Modernising the primary law on intermediary regulation in the EU, the E-Commerce-Directive 2000/31/EC, the DSA is currently the most elaborate and comprehensive body of regional rules on content regulation. The DSA aims to ensure "a safe, predictable and *trustworthy* online environment" (Article 1(1) DSA, emphasis added), and balance the regulation of illegal content with the protection of fundamental rights.

Like the General Data Protection Regulation (GDPR), even though the DSA directly applies to all 27 EU member states (Article 2(1) DSA), the „Brussels Effect„, which is the impact of EU laws in non-EU contexts, may cause some (un)intended effects such as de facto and de jure effects.

Using the GDPR as an example, the EU was able to set some data protection standards globally. Companies operating in the EU had to conform with the GDPR. As a result, a company's compliance measure meant for the EU could consequently become a measure applied across the globe, i.e., separate compliance measures are not developed for Europeans, rather, the measures are applied globally. This is a *de facto* impact of the GDPR. On the other hand, *de jure* effects involve the adoption

of some aspects of the GDPR as data protection standards in non-EU countries, including in African countries. These effects are majorly motivated by economic and trade interests.

Given this background, a possible international impact of the DSA is its normative clarity on how to combat online harms while protecting fundamental rights. For example, the DSA offers inspiration for African countries on protracted regulatory issues in the area of online content moderation, through provisions on intermediary liability (Article 1(2)(a) and Chapter II), due diligence obligations for different types of services (Article 1(2)(b) and Chapter III), and a framework for oversight and enforcement (Article 1(2)(c) and Chapter IV).

The DSA provides for specific responsibilities for platforms with respect to ensuring more transparency and accountability. Articles 14 – 20, 24, 26, 27, 28, 39 DSA and many others provide for various aspects of transparency obligations of online platforms. Articles 41, 49, 50, 51, 61 and 63 DSA also relate to platform obligations, accountability and oversight, provision for Digital Services Coordinators (DSCs) and their powers, the European Board (Board) for Digital Services and their powers respectively. Under the DSA, DSCs are national supervisors of intermediary service providers and they make up the Board to jointly administer the DSA.

While doing business in the EU, platforms now have to pay attention to the DSA's provisions. As seen with the GDPR, in the course of complying with these provisions, platforms might internationalise the DSA. Such compliance might encourage platforms to become accountable in non-EU contexts. A *de jure* impact that could reduce platforms' disregard for non-EU contexts may be that law- and policy-makers in non-EU contexts begin to pass these principles as laws. For example, data protection regulations in Egypt, Nigeria and South Africa bear similarities with the GDPR.

It is unclear whether the DSA will have the same international effect as the GDPR in African countries. In fact, if we think of the GDPR beyond handing down fines to platforms and include other core aspects a data protection law needs to excel at such as putting data subjects at the centre of data control, the GDPR still has a long way to go.

The DSA, Cautious Optimism and Need for Contextualization in African Countries

While African countries may choose to take inspiration from EU laws, there is a need to pay careful attention to local needs before blindly applying foreign rules like the DSA. Rather than replicating the DSA in the African context, African stakeholders, including governments, are encouraged to look more closely at the problems of online harms before they contextualise solutions. Even with its novel and bold moves at content regulation, the DSA has its rough edges and if transplanted without caution into African contexts, it might roll back the gains of human rights protection online in African countries.

To move towards contextualisation of online harms regulation that does not replicate errors but builds on useful aspects of existing regulation, African stakeholders will need to pay attention to a number of issues, such as old and new criminal measures on online harms, the role of African governments including Uganda, Democratic Republic of Congo and Eritrea in spreading online harms and complicating content regulation, in addition to the inherent shortcomings in the DSA itself.

Extant laws that criminalise legally permissible content abound in many African countries. These laws, which have been used to regulate online communications, do not provide clear meaning of online harms and as a result, this leads to disproportionate measures that violate online rights. Many users have been harassed and arrested based on these laws. In addition, new cyber-regulatory laws also provide for the offences of insults, false information, criminal defamation and libel. These political offences are often conflated with online harms and are incompatible with international human rights standards. When online harms such as hate speech or harassment are actually provided for in laws, they tend to be overbroad and vague as seen in Nigeria, Kenya, Uganda, Ethiopia and other African countries.

Additionally, African governments are one of the biggest purveyors of online harms in the region. Governments' active complicity makes it difficult to meaningfully regulate them – it is more or less like having cattle make the rules on hay.

Concerning the DSA's shortcomings, if it were copied into the African context, the DSA may pose at least three challenges to content regulation in the region.

One, Article 16, which provides for notice and action mechanisms. Article 16(2) DSA requires a "sufficiently substantiated explanation" for why an individual or entity alleges an item of information to be illegal. This provision is problematic for two major reasons. One, it is not clear what must be considered for such an explanation to be sufficiently substantiated. Two, this creates more problems for human-rights protection, if such sufficiently substantiated explanation is based on one or more of the various problematic laws on content regulation in the African countries. This provision also adds to the challenge of over-removal of content by platforms.

Second, some of the DSA's provision, including ones that create significant new powers for the European Commission, if transplanted to an African context would create a lack of judicial oversight. For example, Article 40 DSA provides for data access and scrutiny by the DSCs and the Commission. As a result, it gives both the DSC and the Commission excessive powers with respect to demanding, accessing and using such data from platforms without concomitant judicial oversight. Adopting this provision in African countries will put data protection in grave danger, as there will be no means of ensuring that such access is legal, proportionate and necessary.

Third, currently, the initial financial cost of hiring outside staff for the EU at the regional level to enforce the DSA and the Digital Markets Act (DMA) is estimated at $26 million. This excludes other manifold costs required for building institutional capacities of national regulators and ensuring active monitoring and evaluation of compliance with the Act. These financial costs might dissuade African countries,

hoping to model their online harms regulations according to the DSA. However, Article 43 DSA allows the Commission to charge VLOPs and VLOSEs for supervisory fees in proportion to the monthly active users in the EU and it shall not exceed 0.05% of the annual turnover of a VLOP or VLOSEs. These supervisory fees could also be calculated and charged by African countries, as done in the DSA.

Recommendations

The adoption of the DSA in the EU has started generating necessary debates on its possible impacts in non-EU contexts. While the internationalisation of the DSA might be useful, considering how it has provided regulatory clarity in some aspects, its adoption in non-EU contexts must be treated with cautious optimism and be properly contextualised. One way of working towards such contextualisation for online harms regulation in Africa would be developing a regional normative document, led by the African Commission on Human and Peoples' Rights (African Commission), that elaborately articulates a rights-based approach to online harms regulation in Africa and this is possible given existing efforts in the region.

Adopted by the African Commission in 2019, the revised Declaration of Principles on Freedom of Expression and Access to Information offers a starting point for African governments looking towards such contextualisation. While the Declaration can be referred to as the closest and the most elaborate regional constitution on digital rights, it provides for specific aspects of content regulation that can be further developed by African governments.

For example, Principle 22 of the Declaration provides for review of criminal measures such as offences of sedition, insults, false information, criminal defamation and libel in line with international human rights standards. The repeal of these criminal measures addresses the problematic provisions of old extant laws highlighted above and it will go a long way in setting the tone for a foundational and ground-up development of a regional law on content regulation like the DSA in African countries.

Principle 39(4) of the Declaration also provides that governments shall not require removal of online content without considering five major safeguards. One of these safeguards as provided for under principle 39(4)(b) include ensuring that such a request must be imposed by an independent and impartial judicial authority. The only exception to such a request is that law enforcement agencies may make a request for removal to forestall imminent dangers to lives and properties which must also be subject to retroactive judicial review. This principle provides a useful backdrop for African governments to develop rules on notice and action which is one of the major shortcomings of the DSA.

In its implementation, and as a direct response to the challenge of limited ex ante judicial oversight under the DSA, the Declaration requires African governments to adopt judicial measures that give effect to its provisions. Therefore, the prior and retroactive judicial review of executive and legislative powers on regulation of online harms in African countries will be further strengthened.

Conclusion

Developing regulatory norms that seek to balance human rights protection and prevention of online harms in African countries like the DSA is difficult but not impossible. However, the major motivation for such development must involve the appreciation of the impacts of online harms on human rights and democracies, drive meaningful multi-stakeholderism to combat these harms, ensure victim-centred approaches towards regulatory policies and commit to dynamic enforcement and implementation strategies of these policies.
