Protecting democracy in the EU digital space

Addressing Disinformation through the DSA and CPD

Thesis Semester

Dr. Ossewaarde

Dr. Freise

MSc European Studies & MA Comparative Public Governance

Cairán Seán Hennessy

532852

1st of July, 2023

Executive Summary

The EU has launched the DSA and an amendment to the CPD in 2022, with the DSA poised to come into effect in the first month of 2024. In practice, the DSA functions as both the legitimizer of the CPD as well as the regulation that allows the ECM to enforce compliance to both, with the caveat that the DSA is of a procedural yet sweeping nature and the CPD is specialized in combating disinformation especially within the dominion of VLOPs and VLOSEs. Structurally, both are exceptionally well constructed and draw legitimacy from law, public and private norms, and include revision mechanisms that make them future-proof. In addition, definitions of what is being addressed are flexible enough to allow action on the basis of all three, with ultimate operational enforcement being delegated to the actors that have technical competence to monitor and moderate, being internet intermediaries, whereas a combination of public and private establish the norms and practices on the basis of which this happens. The ECM is tasked with the supervision thereof, and can only start guiding the process from 2024 onwards. As a consequence, the established results of CPD18 and the in-effect CPD prove to be somewhat lackluster, with the baseline reports of 2023 being inconsistently filled out, as well as companies using one document to discuss multiple subsidiaries and Twitter outright refusing to reiterate information, they have available elsewhere. Nonetheless the CPD has attracted a significant amount of third-parties that will help further insights through the provision of information, and the way things are arranged it seems the CPD and DSA compliance will only improve. In conclusion, this paper finds that the potential effectivity of the combination of the DSA and CPD in materializing the intents of the EDAP cannot be understated, but that the CPDs current unenforced nature inhibits progress and subsequently any information garnered through it, which for now prohibits well-informed action concerning disinformation. This may be alleviated as the DSA and CPD pick up pace, however this could be sped up by good faith proactivity on behalf of the signatories. From the case study within this thesis, it is clear that the DSA and CPD should allow addressing of illiberal developments within the digital sphere, as well as allow the enforcers to engage with disinformation that escapes illegality while nonetheless adhering to obligations on fundamental and human rights. On the other hand, it can be concluded on the first wave of baseline reports that the in-effect CPD suffers from many of the same shortcomings that the CPD18 did, emphasizing how important the role of the ECM is going to be in getting involved once it receives enforcement capabilities.

List of Abbreviations

AIA	AI Act
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CPD	Code of Practice on Disinformation that is in effect
CPD18	Code of Practice on Disinformation that is no longer in effect
DMA	Digital Markets Act
DSA	Digital Services Act
DSC	Digital Services Coordinator
EBDS	European Board of Digital Services
EC	European Communities
ECHR	European Convention on Human Rights
ECM	European Commission
e-CM	European e-Commerce Directive
ECN	European Council
EDAP	European Democracy Action Plan
EP	European Parliament
ERGA	European Regulators Group for Audiovisual Media Services
ESCS	European Steel and Coal Community
EU	European Union
GDPR	General Data Protection Regulation
IM	Internet Intermediary
IMH	Internet Intermediaries [host]
IMS	Internet Intermediaries [marketplace]
LPS	Legal Representatives
MS	Member-States
OPs	Online Platforms
TEU	Treaty on European Union
TFEU	Treaty on Functioning of European Union
ToS	Terms of Service
UN	United Nations
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine

Contents

1. Introduction

A swift glimpse at the Democracy Index, which is annually reported by the Economist, shows that Democratic Health has been experiencing gradual decline globally since 2017. Furthermore, this trend seems to be accelerating yearly, with the European Union [EU] being the only positive outlier that has managed to return to pre-pandemic levels of Democratic Health (The Economist, 2018; The Economist, 2023). Much has already been written on the necessity and difficulties associated with Democratic Consolidation. Andreas Schedler, a researcher that has been active in the field of Democratic Health since the early 1980s, already warned in 2010 that misinformation and disinformation would likely form a core tenet of authoritarian attempts to hijack or obfuscate public narratives, disempowering the ability of the populace to make informed electoral choices and thus impairing fair elections within democratic systems (Schelder, 2010, 74). On top of this, he noted that upholding the functioning of democracies is highly contingent with the principle of reciprocity, in other words compliance with its norms, and that an increase in political polarization and retaliation invariably would usher in incremental forms of "*erosion, backsliding or subversion*" (Schelder, 2021, 263). In short, respect of the normative basis upon which democracies are founded is essential to ensuring Democratic Health and upholding its institutions, and this is being threatened on the internet.

The EU has inter alia formalized its intent to protect Democratic Health and the functioning of democratic institutions under its member states through Article 2 of the Treaty on European Union [TEU] which states the bloc must uphold "*human dignity, freedom, democracy, equality, the rule of law and respect for human rights*" (European Commission, 2012 -a, 3).As of writing this, the EU still finds itself in the process of accession to the European Convention on Human Rights [ECHR] despite its ratification through the 2009 Treaty of Lisbon, resulting in a situation in which all 27 EU member states are signatories, but not the institutions of the EU itself, meaning that the latter cannot be liable to ECHR transgressions while the former can (Council of Europe, 2022). Despite norms being enshrined in the TEU, the EU finds itself relatively limited in its power to influence many activities that negatively impact the Democratic Health of its member states. One of such activities is the malignant spreading of disinformation, which is a phenomenon that the EU has now started taking tentative action against, launching the Digital Services Act [DSA] and the Code of Practice on Disinformation [CPD] as part of the European Democracy Action Plan [EDAP] to combat the presence of harmful and manipulative information. As these are part of a new initiative, their absolute effectivity in current form cannot yet be measured, but its attempts to balance stakeholder interests and incentives may already be assessed. As such, this thesis is written to answer the following research question:

> "How does the EU fight digital disinformation under the Digital Services Act and Code of Practice on Disinformation, in accordance with the European Democracy Action Plan? "

This research is set to contribute to the existing academic discussions concerning disinformation, its harmful effects and how governments, and the EU, gauging the results and structural integrity of the DSA and CPD, as well as balancing its respect for freedom of speech for which the internet has long been a stronghold. Concerning academic discussions on disinformation, a distinction is commonly made between misinformation and disinformation, with the former indicating no foul intent whereas the latter is targeted, intentional and subject to various aims (Schutz and Godson, 1984; Jowett and O'Donnell, 2005; Saurwein and Spencer-Smith, 2020; Pennycook and Rand, 2021). This paper tests the capacity of the DSA and CPD to address malinformation, as coined by Derakshan (2017), which is technically legal and correct information that is nonetheless incomplete for purposes of manipulation (Derakshan, 2017). Furthermore, this research is positioned in a manner that is actual to contemporary discussions on European Integration and Disintegration, as well as fitting into the larger ongoing discussion on Democratic Backsliding and Democratic Health, assessing how the modern liberalist and constitutionalist democracies of the EU are to be equipped to combat the degenerative effects of various forms of disinformation through these two EU initiatives. The early warning by Schelder (2010) seems to have come to fruition, and while the effects on the actual proliferation of disinformation cannot be accurately deduced at this time, the harmonizing effects of the DSA and CPD can already be subject to explorative research when taking into consideration the binding obligations and law within these documents (Schelder, 2010). This is significant, as digital law entertaining explicit values is a relatively new reality, especially at the behest of a liberalist EU.

Mapping the musts, mays and intents of these documents should allow extrapolation of areas in which in which the EU attempts to actively prevent disintegration, which may also shine light on areas in which this is not the case and further research is warranted. Furthermore, it will allow a degree of assessment and a preliminary conclusion on whether the DSA and CPD are equipped to tackle the issues that the EDAP identifies, and where they might fall short. Thirdly, this thesis fits into the ongoing discussions on the merits of harmonization of law in digital spaces as well ongoing discussions about what democracy itself entails. Liberalism as a conceptual category has become increasingly contested, with the plethora of adjectives of democracies having significant impact on their normative foundations (Pappas, 2019; Bell, 2014). Constitutionalism itself furthermore has also become an assumed factor, that ought to be adhered to, which has proven to not necessarily be true in the case of Hungary and other democracies, where governments have undertaken actions to *ex post* legalize decisions that were illegal when they were ratified (Scheppele, 2018; Ginsburg, 2022). Lastly, it engages with the academic understanding that freedom of expression is both a core tenet and increasingly a weakness to democracies within the as of yet unregulated and increasingly compartmentalized digital spaces of the open internet (Persily and Tucker, 2020; Jackson, 2019).

1.1 Research Questions

In essence, this thesis is written to exhume how the EU can or cannot address disinformation, including that which might escape technical illegality, yet nonetheless debase Democratic Health by impairing constituents' capacity to access unmanipulated information and thus inhibit Democratic Functioning. As mentioned earlier, the main research question holds:

> "How does the EU fight digital disinformation under the Digital Services Act and Code of Practice on Disinformation, in accordance with the European Democracy Action Plan? "

The EDAP, being a non-legal document, is assumed to provide the normative basis upon which the DSA and CPD are based. The delegated competences within the latter two documents allow division of responsibilities to be framed within the intent to combat forms of disinformation. To establish a valid foundation to draw conclusions in order to answer this question, three sub-questions are answered, which range from top-down to bottom-up focus; (1) In what ways does the organization of the DSA and CPD prevent or give rise to digital policy fragmentation, subversion or EU disintegration; (2) What forms of disinformation are addressed by the CPD and DSA; (3) How is responsibility and accountability delegated within the DSA and CPD, for the moderation of 'unhealthy' content?

The first sub-question of this thesis looks at the accumulative effects of the DSA and CPD on the degree of harmonization within EU digital spaces, as EU initiatives that go further than economic integration and cooperation remain relatively scarce. Attention here is paid to how these initiatives promote integration and how the ECM has arranged the DSA and CPD in a manner that incentivizes both policy harmony and functionality, as one is co-regulatory and the other is self-regulatory. This question approaches the DSA and CPD from a top-down angle. The second sub-question is intended to assess the forms of disinformation that the DSA and CPD tackle, and how these are operationalized and enforcement is measured. Herein lies the potential conflict with 'freedom of expression', allowing preliminary conclusions to be drawn on the capabilities and obligations that the two documents actually bestow. Here the interpretative powers of the two documents are discussed. The third sub-question looks specifically at the attribution of accountability within the two documents, disseminating how obligations and makes an attempt at gauging engagement with the strengthened CPD so far. This will allow conclusions to be drawn upon both the feasibility of measuring the combating of disinformation through these two documents, as well as discuss the effects the delegation of responsibilities might have on the dichotomy between freedom of speech and harmful speech if this proves to be relevant. This question regards the bottom-up outcomes of the documents, illuminating possible strengths or weaknesses in the organization of the documents at the operational level.

1.2 Research Approach

As this thesis focuses on the DSA and CPD, both of these documents will be subject to systemic analysis. Furthermore, to allow contextualization of the current shape of the CPD, its first round of signatory reports will be examined in full, requiring an analysis that contains two separate steps. As the DSA and CPD are explicitly analyzed to assess their capacity to deal with disinformation, the EDAP is mentioned exclusively to underline the normative push of the EU in reiterating its liberalist and constitutionalist values, linking this thesis to the EDAP and making the research of interpretative nature. As the DSA and CPD are both text-based initiatives that are both officiated in the form of documents provided by the European Commission [ECM], this thesis also extensively utilizes textual analysis. Due to this, both inductive and deductive reasoning is used. For the testing of easily empirically measurable factors such as delegation of competences, assignment of roles [e.g., enforcer or monitor], deductive data collection is used to draw structured conclusions on the frequency of attribution of obligations within both documents. This is done because these factors can be aggregated without losing important contextual context, which is also practical for assessing their mentions within the evaluation reports of the signatories of the CPD. For the inductive section, all 26 reports that are published by the signatories of the CPD are systematically examined to *inter alia* extrapolate recurring patterns in terms of implementations, compliance and qualitatively determined shortcomings. This is done because the examination of these reports, and the measuring of the current iteration of the CPD is of an explorative nature since this has not yet been done, meaning that it presents the only way of assessing its tentative effects at this point in time, and could result in a proverbial treasure trove of information upon which future research can be based.

The first step of the analysis thus allows drawing empirically established conclusions without risking the invalidation of results due to contextual obfuscation, and while it will form a major element of this thesis as it is extensively used to underline points in the argumentative analysis section, still other scholars might be able to deduce more complicated matters from the results that escape the scope of this thesis. This step of the case study is conducted at the hand of the coding scheme found in chapter 2, with processed results recorded in *appendix 1*. The second step forms the main argumentative content of the analysis section and refers to the data from the first step as a basis to illustrate conclusions on findings, placing these findings in academic discussions and contemporary developments to allow answering of the sub-questions in their respective order, which is given in section 1.1. This order is adhered to, as it allows the thesis to discuss material transitioning from the top-down EU level effects, to the individual stakeholder accountabilities bestowed by the horizontal legislative nature of this act. The next chapter provides the relevant theoretical background to this endeavor.

2. Theory

Much has already been written on the EU's functioning at all three strategical levels that were mentioned in the previous section. As the guiding research question of this thesis seeks to explore the manner in which the DSA and CPD combat disinformation, this chapter is written to underline how important this initiative is to the EU by drawing from academic discussions on Democratic functioning, disinformation and regulatory governance. Similar to the sub-questions, these three topics are discussed in that particular order due to their affects, with subsequent topics building on what was dealt with in the former, allowing the theory to be discussed while moving from the abstract level to the more tangible and identifiable regulatory level. In the first section of the chapter, writings on democratic functioning and its importance to the EU are examined.

2.1 EU member-states ought to be liberalist constitutionalist democracies

The EU has traditionally been composed of member states that in practice all adhere to the same mutual respect for democratic values and human rights, and has officiated these values through the introduction of Article 2 TEU (European Commission, 2012 -a, 3). The EU itself is a conductor of governance through regulations, and as such the constitutionalist side of the apparatus speaks for itself, however the normative underpinnings of the EU being present in its initiatives is a relatively recent phenomenon. Early liberalist scholar Rawls (1971) argued that under a liberalist system, personal freedoms should beget absolute primacy, and externalities such as economic considerations should be given a subordinate position, and that to uphold these freedoms it is paramount that procedures should be established, respected and upheld (Rawls, 1971, 82-90). Despite this early argument that upholding liberalist values necessitates constitutionalism, Hittinger (1994) noted that this definition of liberalism failed to account for conflict arising within liberalist governments exactly due to the nature of externalities, and that not accounting for externalities will lead to exacerbated political difficulties even in cases of 'reasonable' pluralism (Hittinger, 1994, 600-602). At this point in time, most liberalist constitutionalist democracies are signatories to international legal treaties that further underline their dedication to the protection of fundamental freedoms and human rights, and in the case of the EU this has led to all EU member-states being signatories to the ECHR (Council of Europe, 1950). In other words, even when a government departs from liberalist values, and they may, there are treaties in place to secure adherence to the most basic of fundamental and human rights.

The ongoing changes to the global democratic composition have led to a rapidly growing body of studies that focus on illiberalism, examining its origins and mechanisms in a bid to examine how it is possible that consolidated democracies have started to succumb to illiberal influences (Daly, 2019, 16-18). Modern indexes that assess democratic health have adjusted their categorization accordingly, the Economist's intelligence unit discerning between (i) Full democracies, (ii) Flawed democracies, (iii)

Hybrid regimes and (iv) Authoritarian regimes, in their annually published 'Democracy Index' (The Economist, 2023, 3). V-DEM on the other hand discerns between (i) Liberal democracies, (ii) Electoral democracies, (iii) Electoral autocracies and (iv) Closed autocracies for the same purpose (Herre, 2021). It has become clear both in academia and in the investigatory fields that intersect with it that democracy is not a one-way street, but rather it is located on a sphere and governments can under certain constraints move along the axes without necessarily losing their adjectives. While much may be said on regime types, the forms of a reduction in democratic health have been conceptualized in a variety of manners, which are given below.

Democratic backsliding, entailing gradual deconstruction of democratic backstops to allow impediment to democratic functioning or openly authoritarian political actors (Levitsky and Ziblatt, 2018, 15 and 146); democratic deconsolidation, meaning the weakening of democratic institutions under certain systems of governance, particularly under presidential systems due to bipartisan demands (Linz, 1990, 51-52); democratic decline, illustrating the susceptibility of weak democratic institutions during the fledgling days of a new democracy, with Venezuela being a case in point (Levine, 2002, 250). Nonetheless, illiberalism scholar Scheppele (2018) argues that it is only respect for the rule-of-law that can save a democracy, and that if a democracy respects its constitution, it should be entrenched enough to withstand illiberal attacks (Scheppele, 2018, 557-580). On this, Daly (2019) argues that modern writing on democracies have come to intricately link liberalism, constitutionalism and democracy, and argues that a functional democracy requires all three, given that other adjectives often largely explain their de facto functioning and direction of development instead (Daly, 2019, 6). Furthermore, on the assessment of Scheppele he finds that it is exactly this normative reliance on respect for rule-of-law as only backstop that makes democracies susceptible illiberalism (*Idem.,* 7-8). The question then becomes how successfully exploits and disempowers democratic mechanisms.

Levitsky and Ziblatt (2018) consider that there are four major indicators that show the presence of political authoritarian tendencies, indicative of a form of democratic decay, that one can account for: (i) rejection of democratic values, (ii) delegitimization of the political opposition, (iii) indifference or worse to violence and (iv) willingness to scorn liberal values (Levitsky and Ziblatt, 2018, 14-15). These can easily be juxtaposed to the functional foundations of a liberalist democracy: (a) recognizing society necessarily contains cleavages, (b) requiring political moderation and building political consensus and (c) necessitating sticking to the rule-of-law (Pappas, 2016, 41-48 and 265-266). The former indicators may be strengthened whenever one of the latter three functions of liberalist democracies fail to meet its constituencies' expectations, with Papas (2016) concluding that "*populism stands as an alternative type of democracy*" whenever liberalism goes into crisis (*Idem.,* 51). He concludes that this issue is further exacerbated by the fact that if the failing system functions as a toolkit to control and reprimand,

illiberalism necessarily delegitimizes it to pursue popular mandate (*Idem.,* 55). The absence of such checks and controls would turn a governmental system into populist democracy (Riker, 1982, 181-200). In other words, a direct opposite to the idea of Rawls (1971), populism foregoes liberalist externalities in favor of the functioning of democratic self-determinism. Vormann and Weinman (2020) consider that the ongoing conflict between liberalism and illiberalism, at least within liberalist and constitutionalist democracies, are caused by the inherent conflict between social equality and popular rule as well as protection of minorities in the face of possible tyranny of the majority (Vormann and Weinman, 2020, 65-66). Fukuyama (2022) argues that "*liberal ideas being stretched to the point of breaking*" lies at the root of such illiberal ideology, and that such freedoms were not meant to be absolute unconditional rights (Fukuyama, 2022, 68). In conclusion, the normative clash between illiberal thought, here presented interchangeably with populism, and liberalism lies in majoritarianism, which in turn is dealt with by democracies through the institution of rules with normative underpinnings.

Whereas liberalism and democracies are under various types of attack by undemocratic pressures and actors, constitutionalism has been less examined as rule-of-law has simply been bypassed by illiberal governments. Both Bozóki (2015) and Bánkuti *et al.* (2015) have found that in the case of Hungary and Poland, illiberal governments have illicit actions or decisions to gain control over the judiciary, making short work legalizing their past deeds through amendments to the constitution or other legal changes to prevent judiciary atonement (Bozóki, 2015, 18; Bánkuti *et al.*, 2015, 38). One case of such aforementioned social and governmental Illiberalist developments can be found in a public speech by Hungarian prime minister Orbán, where he openly stated that his government strives to pursue self-determinism and majoritarianism, a fair democracy under the flag of Christianity, alleging that the latter is an "*illiberal concept*" itself (Plattner, 2019, 10-11). So far, liberalism, illiberalism and constitutionalism have been discussed to picture the harmful normative and political developments that have been taking place globally, but also within the EU, establishing why it is necessary to counteract illiberal developments. The next section will discuss how the EU is organized and how it may affect or be affected by illiberal developments.

2.2 Illiberalism threatens all levels of EU cooperation

The EU itself is constructed upon the premise that its member-states are full-fledged democracies that adhere to liberalist, constitutionalist, pluralist and democratic principles; in other words, that they are fully functional liberal democracies. This sets a basic premise for how it is able to conduct governance, which is the means through which it seeks to achieve greater integration amongst its member-states, predominantly for strengthening its single market but recently also for the protection of its normative underpinnings.

To bring justice to the value of governance a brief glimpse needs to be given to what might incentivize a sovereign government to delegate aspects of its self-determination through in international engagement. Early neo-functionalist scholar Haas (1958) is generally hailed as the first of his school, and argued that cooperation at the intergovernmental level arises from practical considerations and incrementally diversifies due to functional spill-over, leading to an increase in political will (Haas, 1958, 313-317). Moravcsik (2018), a contemporary intergovernmentalism scholar, instead argues that governments to not delegate their decision-making capacity to any degree as they remain not ideological but strategic actor (Moravcsik, 2018, 1649). And indeed, governance in many ways escapes the possibility of direct coercion or enforcement. Czempiel and Rosenau (1992) coined governance to describe how power can be projected outside of areas within which governments are traditionally the decision-makers, regulatory mechanisms missing formal authority, or "*routinized arrangements*" despite the absence of "*some overarching governmental authority*" (Czempiel and Rosenau, 1992, 4 and 7). The EU largely makes use of regulations, directives and acts to achieve similar purposes, which in theory sets it apart from governance due to the latter being reserved for areas in which the issuing authority has no competence. Nonetheless, argues Savin (2019), one ought to speak of governance when dealing with a "*multitude of actors and authority structures*", concluding that regardless of competences bestowed upon the EU, it is not a government and possesses a lack of enforcement mechanisms which makes it wholly reliant on that very concept (Savin, 2019, 29-31). The EU possesses very few executive enforcement mechanisms, but boasts a relatively large amount of legitimacy and competences to conduct governance, which it predominantly utilizes to bring its member-states closer together.

The EU has not coined the idea of European integration, and as such it should be clear that it has received a mandate to govern before its inception. The idea of European integration has been around since the 19th century, realizing itself two years after the Schuman declaration of 1950 which established the European Coal and Steel Community [ESCS] (European Commission, 1950). Over time this multilateral cooperation with particular focus would grow and be supplemented by inter alia the European Communities [EC], ultimately culminating in the 1992 'Treaty of Maastricht', known as the TEU, which established institutions as known today: the European Commission [ECM]; European Parliament [EP]; European Council [ECN]; Court of Justice of the European Union [CJEU]; Court of Auditors [CoA] (European Commission, 1992 -a). This degree of integration was further solidified through the 2017 'Treaty of Lisbon' which revised the TEU, introducing common norms and values, and introduces the Treaty on the Functioning of the European Union [TFEU], which both came into effect in 2009 (European Commission, 2012 -b). Dougan (2000) argues that to foster cooperation between the EU member-states, the EU enjoys a vast preference for legislative initiatives that seek

"*minimal harmonization*" by establishing a legal backdrop that minimally infringes upon member-state legal sovereignty, ensuring standards through "*values which merely interface with rather than serve the economic demands of the single market*" (Dougan, 2000, 860). To ensure that its capabilities are limited, the EU is subject to several principles enshrined in the treaties, however it also undertakes public normative action to ensure that member-states know that the EU is exclusively pluralist.

The ECM maintains a 'Single Market Scoreboard' which contains data on its conduct and member-states' regulatory frameworks to offer transparency in its engagement to uphold its own four freedoms of; [i] goods; [ii] capital; [iii] services; [iv] people (European Commission, 2023 -c; European Commission, 1997). Despite proactive efforts on behalf of the ECM to offer transparency to its member-states and promote cooperation and mutual reciprocity, it is also possible for disintegration, or an increase in distance between the regulatory framework and practices of member-states and the EU, to occur. Many discussions on the causation thereof have already been had, with post-functionalists arguing that ideological politicization of governance and its liberal values is a major driver of both positive and negative effects on integration, while historical institutionalists interpret negative effects on integration as a symptom of logical feedback due to prior decisions (Moravcsik, 2018, 1949). Moravcsik (2018) himself however argues that a modern neo-functionalist interpretation on integration constitutes oversimplification due to its reducing of multilateral engagements to normative political choices, while historical institutionalists fail to account for institutional change since the signing of the Schuman declaration: instead, current cooperation can be explained best through liberalist institutionalism which accords for the normative foundations of the institutions gaining in importance, and thus coming to the forefront more at the behest of, and within, the member-states (*Idem.,* 1668). Accounting for the normative push exerted by institutions, one must re-examine how it is possible that governments that are part of the pluralist EU are able to become illiberal despite being deeply entangled and benefitting from it at large.

As the EU and contemporary multilateral engagements are of a highly complex nature, Vollaard (2014) warns that conceptualizing disintegration as a simple return to "*national states*" would be a gross and faulty simplification (Vollaard, 2014, 1144-1145). Furthermore, disintegration of the EU does not mean that a member-state moves away from the EU, but it can also happen due to EU decisions. Schimmelfennig (2018) considers this a form of "*differentiated disintegration*", a fully negotiated process under which "*EU policies and competences are transferred back to … member-states*" (Schimmelfennig, 2018, 1165-1166). Disintegration of the bloc as such can follow the course of the infamous Brexit decision, but it can also be present on the mere basis of democratic decisions of the member-states' representatives. Ginsberg (2021) warns that international organizations are not merely a liberalist normative force, and can also be used for more nefarious purposes, citing how the

United Nation's [UN] "*Cooperation in Combating Cybercrime*" was utilized by illiberal states to promote non-interference (Ginsberg, 2021, 229). It is safe to conclude that an organized illiberal presence at the EU level could have profound effects on the normative direction and capacity of the EU. Albert (2017) has, due to the susceptibility of democracies and institutionalist systems, argued that member-states and the EU might benefit from a toolkit "*of reasons to invalidate constitutional changes in order to protect the foundation of constitutional democracy*" (Albert, 2017, 197-198).

This section has discussed how the EU stands to be exploited by illiberalism, touching upon the various risks it brings, making clear why it is important that illiberal developments, and any harmful symptoms thereof, should be dealt with for as far as competences and law allows. It has also underlined why it is important to be proactive in identifying indicators, and how certain developments that might not immediately invoke scrutiny could warrant investigation to prevent materialization of illiberal threats or challenges. The next section discusses and problematizes the prevalence of disinformation within EU digital spaces., underlining that illiberalism does not only pose risks at the state-level.

2.3 Disinformation affects member-state constituencies

Disinformation is a phenomenon that is as old, if not older, than democracy. Fallas (2009) mentions that the "*Platonic definition*", coined by Plato, still holds true: "*That is, if something is knowledge, then it is justified, true, and believed (the necessity condition). Also, if something is justified, true, and believed, then it is knowledge (the sufficiency condition)." (*Fallas, 2009, 2). In other words, whether something is actually true hinges fully on whether something actually is true, and can be inferred to be the case if knowledge is shared from one individual to another under the implicit pretense that it ought to be true, leading to the false belief that something is true. Disinformation might be disseminated exactly to impair society's capacity to assess.

One can make a distinction between a plethora of different modes of manipulative information provision, such as inter alia: Propaganda" (Doob, 1948; Jowett and O'Donnell, 2005, 4); "Fake News" (Pennycook and Rand, 2021, 390); "Fabricated Content, Manipulated Content, Imposter Content, Misleading Content, False Context, Satire and Parody, False Connections, Sponsored Content […] and Error." (UNHCR, 2021, 231); "Information influence operation" and "Foreign interference in the Information space" (European Commission, 2020 -a, 17-18). On top of disinformation coming in various shapes, forms and techniques, a distinction can also be made on the basis of the intent. Wardle and Derakshan (2017) make a distinction between disinformation, misinformation and malinformation, being intentional and targeted, unintentionally incorrect and intentional and correct albeit incomplete, respectively (Wardle and Derakshan, 2017, 20). And then there is of course discussion on what disinformation itself entails: as being "false, incomplete, or misleading information that is passed, fed,

or confirmed to a target individual, group, or country" (Schutz and Godson, 1984, 41); as "forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit." (Saurwein and Spencer-Smith, 2020, 821); as "is deliberate and includes propaganda and malicious content, such as hoaxes and phishing" (UNHCR, 2021, 231); or as "creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public" (European Court of Auditors, 2020, 2). The same holds true for misinformation: as "merely misguided or erroneous information" (Jowett and O'Donnell, 2005, 22); as fully accidental, or "yellow journalism" which is poorly researched and sensationalist news, akin to tabloid journalism (Pennycook and Rand, 2021, 390); as "false or inaccurate information, spread accidentally" and "by people not meaning to deceive" (UNHCR, 2021, 128-129). Disinformation and misinformation are both separately mentioned in the DSA and CPD, however the next paragraph contains a term that is not explicitly mentioned, yet will have to be dealt with.

The term "*malinformation*" is accredited to Akshan (2017), who conceptualizes it in an attempt to make explicit the intentional removal of key parts of information to cause harm (Derakshan, 2017, 21). Disinformation does not necessarily have to be inaccurate, but it does have to be misleading, meaning that the presentation of limited facts surrounding a technically correct report can become disinformation as well (Fallas, 2009, 6). As such, for something to be disinformation, it is not being false but being manipulative, that is a necessity. Disinformation scholar Doob (1989) at the end of his career already made an argument against an essentialized definition, stating that societal behavior, culture and time are not static (Doob, 1989; Jowett and O'Donnell, 2015, 4). It is to be noted that the prior definition that the EU has used on disinformation, specifically the requirement of disinformation being "verifiably false", has been removed, de facto meaning that the falsehood no longer needs to be proven before action can be undertaken (European Commission, 2020 -a, 18). The EU has clearly removed the absolute necessity of requirement of proof from the shoulders of whomever combats disinformation, which should be considered a positive step for the regulative acts that are to be examined. Nonetheless, context must be provided for why disinformation and manipulative comments are such a problem within the EU digital space.

In recent times, "*fake news*" has received an incredible amount of attention due to the prevalence of fabrication, manipulation and propaganda and its respective inherent degenerative effect on democratic health (Saurwein and Spencer-Smith, 2020, 821). Populists have seized this tactic to establish frames that exacerbate existing democratic issues, making for "*fertile grounds for such resentment when the core value expectations of social justice, economic equality, and political inclusion are either in jeopardy or altogether thwarted*" (Pappas, 2016, 113). Ophir and Jamieson (2021) find that besides fake news and populist framing, recurring framing in which key details are left out can

invigorate media skepticism, finding that when this is done on matters that concern science the entire scientific method can lose legitimacy (Ophir and Jamieson, 2021, 10-13). Huq (2022) finds that liberal democracies are particularly vulnerable to disinformation, identifying a rise of foreign actors investing "*in misinformation for their own geopolitical ends*" (Huq, 2022, 120). On the other hand, there are internet mechanisms that incentivize sensationalism due to how it generates financial benefits, and some actors conduct business purely for monetary gain (Saurwein and Spencer-Smith, 2020, 825).

Framing as such stands central to the spread of disinformation to delegitimize, hijack, defame, or otherwise impair the normal functioning of the media. It is only recently that a bridling academic body of research into the policy response to the proliferation of disinformation has occured (Saurwein and Spencer-Smith, 2020, 822). This is extremely necessary, as media changes are leading to the disempowerment of traditional media and its coherent journalistic standards, and the internet creates a very different environment for information exchange (Guess and Lyons, 2020, 17). The changes on the internet warrant putting the logistical organization of the systems that are utilized to spread disinformation today, and this also forms a focal point of this thesis as the DSA and CPD directly engage and try to regulate the owners thereof. The next section discusses how the internet and actors thereof so far have been both intentionally and unintentionally complicit to the dissemination of harmful disinformation.

2.4 An unregulated internet is a hotbed for harmful disinformation

The internet offers an extreme degree of 'freedom to expression', and most forms of policing beyond self-regulated terms of service is established in a predominantly reactive manner. One can swiftly think about how illegal content had been freely accessible on the internet before the advent of the new millennium, and in many cases up until the mid-2000s. In due time however, it is not possessions but information that has become a new commodity in digital spaces, culminating in exploits that require the EU to institute the sweeping DSA and CPD to introduce a minimum of rules that all actors that wish to utilize the space should adhere to.

Huntington (1991) already predicted in the early 90s that Russia would pose a threat to Eastern European democracies through spreading disinformation to ex-Soviet states (Huntington, 1991, 19). While he did not speak on the mechanisms that made this possible, Bakir and McStay (2018) have concluded that digital platforms play a pivotal role in the rise to prevalence of disinformation due to the altered media landscape and weakened journalistic standards (Bakir and McStay, 2018, 170-171). The internet has long been devoid of sweeping legislation, with social media adhering to a minimum of self-regulation to reflect their users' norms and prevent government regulation (Zurth, 2021, 1121-1122). Huq (2022) on this note argues that for a long time, such platforms have considered themselves "*digital Switzerlands*" due to their neutrality and independence from greater blocs (Huq, 2022, 123).

Despite their formal neutral disposition, Woolley and Howard (2018) have found that there is ample proof that in-place algorithms, that exist to maximize financial gains, can be exploited through "*computational propaganda*" to effectively disseminate disinformation, and that this has already been done by Russia to attack the West, and by China to reach its own populace (Woolley and Howard, 2018, 212) Besides the mechanisms that recommend potentially interesting content or algorithms that help spread your content further, the behaviors of users, which might vary from platform to platform, can also be an enabling factor. Saurwein and Spencer-Smith (2020) find that the users of social media serve a double role, namely as the recipients and consumers of disinformation, but at times also as the distributors (Saurwein and Spencer-Smith, 2020, 825). It is thus clear that the mechanisms that are currently in-place may well be exploited, and some measure of regulation and harmonization are in order, however the question remains what this should look like.

Regulating the internet is also not without potential issues, as Fallas (2009) argues a geographical map might include elements that are not actually physically present. The creator of the map is aware, and knows that someone will believe that those elements are actually there, but has no intent to willfully deceive (Fallas, 2009, 5). Concerning data and data protection, another likely factor in why the internet could function as a hotbed for disinformation, many types of actors might choose to utilize automated programs to scour the internet for data, and not all of these are nefarious. These are, amongst others, used by "corporate lobbyists, content management firms, civic activists, defense contractors, and political campaigns" (Woolley and Howard, 2016, 4885). In addition, Murthy *et al.* (2016) have found that for automated bot networks to be effective in disseminating information in order to sway political opinions, a considerable amount of cultural, economic and social capital formed a prerequisite (Murphy *et al.*, 2016, 4966-4967). Some groundwork must be laid that goes further than the mechanical functioning of whichever platform might be exploited to gain meaningful control over digital spaces, Huq (2022) proposes that governments impose *ex ante*, preventive, and *ex post*, reactive, penalties on digital actors to slow the spread of illegal content online (Huq, 2022, 127). EU internet has for a long-time escaped sweeping and stringent legislation, however the EU and its member states have started introducing law in response to several key events since the mid-2010s, and academics have called for such.

Woolley and Howard (2016) argue for the importance of proactively regulating internet communications, stating that (i) internet access and use will only grow, (ii) internet penetration is and will continue rising, meaning "*virtually everybody can connect to everybody else*" and (iii) in a decade everyone will be a "*digital native"*, that is fully-immersed in a world affected and affecting the internet, including a shift from seeing majority use in democratic countries to one in non-democratic states (Woolley and Howard, 2016, 4884). In addition, despite American internet being based upon

essentializing "*free speech*" rather than the EU "*liberal freedoms*", internet regulation seems to globally be itching closer to a form of regulated *"healthy speech*", rather than retaining its old focus on unrestricted "*open speech*", coinciding with the approach spearheaded by European regulatory initiatives (Zurth, 2021, 1098). Herein the EU has gradually shifted from a focus of establishing and letting the market grow through liberal market-based policies, to a more constitutional-based strategy that prerequires respect for liberal values such as the rule-of-law (De Gregorio and Dunn, 2022, 478 and 490). This section has discussed how changes of the media landscape and actions by actors utilize the digital space for potentially nefarious aims, as well as changes in the digital landscape that were brought about as a consequence. The following section discusses the other factors within which the EU requires competences factor into the issue that disinformation poses to EU democratic health.

2.5 The EU is and ought to be increasingly stringent in regulating its digital spaces

The normative standards of the EU are slowly but surely penetrating the semi-unregulated web, despite power on the internet slowly accumulating in the hands of a few strong 'gatekeepers', players so big that they are able to brute force out smaller competitors. These have in turn positioned their social media platforms to become "*critical elements of the public sphere*", with Huq (2022) arguing that so inconsistently regulated that they cannot prevent "*deliberately engineered falsehoods being intentionally disseminated*" (Huq, 2022, 117). He continues to state that this has been a long-established staple to US politics, and that only third parties getting involved is a more recent trend (*Idem.,* 120-121). The question is however, what sets the digital spaces apart from the real world that make them so dangerous to democratic functioning.

Bendiek (2021) warns that recent developments have led to highly frequented public spaces falling under the dominion of digital oligopolies which forms an impediment to democratic processes, as unlike within the nation-state, where participation is tied to citizenship status, the digital spaces can be utilized by anyone that possesses enough capital (Bendiek, 2021, 3). Saurwein and Spencer-Smith (2020) furthermore find that besides human and human-targeted technological processes, "non-human technological actants, such as interface design and news feed algorithms, play a key role in *"the fake news process"*" (Saurwein and Spencer-Smith, 2020, 824). Almost fifty percent of all traffic on the internet is generated through the use of automated bots, and e.g. Twitter has over 30 million 'active users' that are actually bots, mimicking human activity "*and produce copious information*" (Woolley and Howard, 2016, 4885). In short, everyone can create content which is then automatically disseminated throughout the system in order to maximize reach for financial benefit, with automated programs factoring in and potentially exacerbating the issue through providing or collecting large quantities of data. Non-regulation has also played right into the hand of the consolidation of big players

on the market. A now bygone example is the introduction of the spam filter, on behalf of private enterprises, which to the consolidation "*of a handful of global email providers*", leading them to dominate the market (Sullivan, 2019, 215-216).

These mechanisms are not only passively complicit in the dissemination of harmful disinformation, but can also be exploited for unhealthy deeds by individuals. As an example of individual misuse, live-stream come video material recorded by the terrorist that killed 50 at a shooting at a Christchurch Mosque was uploaded to Facebook an astonishing 1.5 million times, of which 1.2 million were automatically blocked by a preventative anti-spam Facebook algorithm, with this mechanism only coming about due to an EU initiative to combat illegal online hate speech (Gorwa *et al*., 2020, 2). Had this filter not existed, one can only imagine the reach this hate-filled content might have had, however to some degree this result can also be seen as a success story due to it having prevented 80% of the uploads, with the other 20% having been engineered to circumvent the similarly automated checks (*Ibid).* Due to the susceptibility of the digital spaces to exploitation, digital regulations and cybersecurity have been a point on the ECN agenda since 2008 (Pellegrino and Stang, 2016, 14). Since then, de Gregorio and Dunn (2022) consider that the EU has slowly been building and expanding regulatory framework that constitutes a de facto "*digital constitution*", consisting of the General Data Protection Regulation [GDPR], AI Act [AIA] and DSA (De Gregorio and Dunn, 2022, 490). These regulations have already done much to limit the potential for exploitation that digital spaces have, however all of these regulations nonetheless must adhere to some limiting dimensions at the behest of TEU obligations.

Bendiek (2021) finds that due to full adherence to the self-regulatory nature, as well as proportionality and subsidiarity principles, the original 2018 iteration of the CPD has proven its inefficiency in halting disinformation calling for violence on the 2021 US Election Day, as well as the 2019 Twitter data-leak in which a user released German politicians' compromised data in a bid to hurt their credibility (Bendiek, 2021, 4). The CPD has since been strengthened by doing away with the "*verifiably false"* requirement to identify disinformation, as well as introducing numerous transparency clauses for future revision and evaluation (European Commission, 2022 -b). Accompanying this, the EU has launched the DSA and Digital Markets Act [DMA], of which all clauses will be in effect on latest 12 February 2024 (European Commission, 2022 -a; European Commission, 2022 -c). These supplement the supposed digital constitution of the EU, and seek to strike a "*proportionate balance between risks and costs of regulation*" when it comes to their reach, implementation and enforcement (De Gregorio and Dunn, 2022, 475). Saurwein and Spencer-Smith (2020) find that the DSA adheres to a risk-based approach, predominantly serving to provide the EU with information to examine and adapt their approach (Saurwein and Spencer-Smith, 2020, 823). To refer back to the previous sections of this

chapter, the EU thus consolidates their approach to be human-centered, incorporating economic interests while maintaining the liberalist mantra to uphold and strengthen "*individual fundamental rights and democratic values*" while taking action against all dimensions that empower disinformation (*Idem.,* 491). However, the DSA and CPD are also unique in that they are procedural, assigning considerably more obligations to Very Large Online Platforms [VLOPs] and Very Large Online Search Engines [VLOSEs], and obligations to the former fall under the jurisdiction of the CJEU (*Idem.,* 492; European Commission, 2022 -b).

This section has made specific the historical effects of a lack of regulation, as well as shown the positive outcome of a relatively recent regulation on an unfortunate and coordinated attempt at abusing the mechanisms of a social media platform. In addition, it has briefly outlined relevant in-effect legislative material to show how the EU is precautious by introducing highly specialized law to address select excesses within digital spaces. So far illiberalism, disinformation and regulations have been discussed. The next section is relatively brief, synthesizing the relevant literature that will be drawn upon to answer the research questions as given in Chapter 1.2.

2.6 Summarizing the approach to assessing the DSA and CPD

This section is organized at the hand of the order of the research questions that can be found in chapter 1.2. The overall intent of this thesis is to produce insights into how the EU has constructed the DSA and CPD to combat disinformation within its digital spaces in accordance with its ambitions as derived from the EDAP. Three sub-questions are fielded and answered which ultimately contributes to an overarching answer to the aforementioned question, and these are; [1] how does the organization of the DSA and CPD impact EU integration; [2] what forms of disinformation are addressed by the DSA and CPD; [3] how is responsibility and accountability to moderate delegated within the DSA and CPD? To this end, this section is divided in three, each drawing from relevant literature that was discussed in the other five sections of this chapter as well as theory that is specifically applicable to the analysis of the data from the case study.

The first question concerns itself with the top-down implications of the DSA and CPD, examining which effects can be expected due to the nature and organization of the relevant regulation. The context here is EU democracies and integration, and the approach of this thesis towards assessment of the harmonizing or disharmonizing capabilities of the DSA and CPD can be assessed at the hand of scholars that were mentioned in chapters 2.1 and 2.2. To see whether the DSA and CPD seek to escape what was coined as "*minimum harmonization*" by Dougan (2000), the analysis section of this thesis will discuss the positive and negative obligations, seeking to conclude on whether the documents lean more on what actors should do than what they should not do (Dougan, 2000, 860). In addition, both documents are contextualized to how the ECM pursues compliance and legitimacy itself

by checking for obligations to provide information and transparency. In addition, it will be examined to what degree action is mandated on the basis of the four authoritarian indicators as outlined by Levitsky and Ziblatt (2018), which are [i] rejection of democratic values, [ii] delegitimization of political opposition, [iii] indifference to violence or worse and [iv] willingness to scorn liberal values (Levitsky and Ziblatt, 2018, 14-15).

The second sub-question, on what type of disinformation begets what sort of response, can draw quite directly from the existing literature on disinformation already. The three definitions of Derakshan (2017) are utilized: [i] Disinformation, [ii] Misinformation and [iii] Malinformation. In doing so, the DSA and CPD can be analyzed to differentiate between [i and ii] false information that is, intentionally or not, incorrect and [iii] correct but deceptive information for commercial or political purposes (Derakshan, 2017, 20). This distinction is essential since on the internet it can become incredibly difficult to locate the source of content, and in most definitions attribution of blame falls on the content creator rather than the internet intermediary, however since the ratification of the DSA this will change, and both could be found non-compliant in separate acts (Husover and Laguna, 2023, 1 and 12); The research by Ophir and Jamieson (2021) additionally shows that the effects of disinformation, misinformation and malinformation are equally harmful albeit they might require a different method to be dealt with (Ophir and Jamieson, 2021, 13-16). This paper sweeps the three under the moniker 'unhealthy' content for purposes of analysis, and will at times set them apart where limitations occur. These are furthermore juxtaposed to the EU statement on its own values: "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*", to examine whether any of the normative factors herein are also mentioned within obligations within the documents, i.e., whether sexism is now subject to moderation (European Commission, 2012 -a).

Thirdly, to examine the practical divisions that are to occur under the DSA and CPD, a closer glimpse will be given to how the division of roles within the DSA and CPD are organized. To organize this, two different theoretical frameworks are be brought in and synthesized; firstly, the three factors that Howard and Parks (2012) consider 'make up' social media are used: [a] infrastructure to distribute individual contents that contain shared values, [b] content that takes form as "*personal messages, news, ideas, that become cultural products*" and [c] the users, "*people, organizations, and industries*" that produce and consume both the infrastructure and its contents (Howard and Parks, 2012, 362); Secondly, Sartor's (2013) liability paradigm warns that allocation of accountability can have chilling effects on the ability of users to utilize their right to expression, or cause over-censoring on behalf of

the providers. The relevant responsibilities are divided in three roles: [1] controllers, [2] enablers and [3] monitors (Sartor, 2013, 44). This thesis will synthesize both frameworks: [a] can be linked to [2], for internet intermediaries can enable internet access, but they might not be liable for its consequences of misuse of service; [b] is linked to the main responsibility of the [3] monitor due to content monitoring being focal points of the DSA and CPD; and finally, [c] the various stakeholders are often both [1] controllers, e.g. social media through infrastructure and end-users through reporting tools, and consumers (Saurwein and Spencer-Smith, 2020, 825).

Having established mechanisms to measure [a] how normative values are embedded and protected throughout the regulations, [b] how disinformation and manipulative behavior may be addressed and [c] how accountability is distributed amongst categorized stakeholders, the theoretical chapter is concluded. The following chapter explains the methods that are utilized for purposes of analysis during the case study of this paper.

3. Methods

This chapter forms the backbone of the analysis that is conducted in order to gauge how the DSA and CPD are poised to impact the dissemination of disinformation in accordance with the EU ambitions as laid out in the EDAP. Accordingly, this chapter starts out by explaining the case study chosen for this thesis. Secondly, the method of data collection is discussed and data selection and gathering is discussed. In the final section of this selected method of data analysis is examined, followed by a short conclusion that reiterates the exact method of approach. While much has been said in the previous chapters on matters of regulation and the necessity thereof, the case of the DSA and CPD are ongoing and will be given below.

3.1 Case Description

Outright direct engagement with disinformation as basis is a relatively new phenomenon to the EU, with the original iteration of the Code of Practice on Disinformation from 2018 [CPD18] serving as its first attempt to usher in a form of regulation that pre-empted the launch of the DSA and the strengthened CPD. The former as such implemented the first attempt at regulating digital spaces in terms of what can and cannot be said when it comes to the provision of information that escapes illegality, and the DSA is set to not only support it but increasingly legitimize the prevalence and adherence of the CPD due to its incorporation of its 35th article, which stipulates that the ECM and European Board of Digital Services [EBDS] may choose to invite internet intermediaries upon the constatation that their current mode of conduct presents a systemic risk (European Commission, 2022 -b, 64-65). In other words, while the self-regulatory initiatives to bring about harmonization amongst private enterprises within the EU digital spaces are voluntary, it can occur that the ECM or EBDS establishes joining one of such initiatives as a prerequisite to increase compliance with adherence to other regulations, such as the DSA. This means that the CPD as it exists today interacts with the DSA as the latter legitimizes it and also empowers it, creating a constellation in which illegalities are clearly outlined within regulations that concern digital environments, but disinformation as non-illegal phenomenon must and can also be addressed.

Due to their nature as policy documents, text is the main source by which the EU can officiate and communicate their strategies and frameworks. While there are many interlinking acts within the digital sphere, the two documents that make up the DSA and CPD are of a different nature, with the former being a sweeping and horizontal integration backstop that bestows binding positive and negative obligations, and the CPD being procedural and multi-purpose that is specially tailored towards compliance of VLOPs and VLOSs. Both of these documents were doctored by the ECM, albeit the CPD has incorporated feedback from the evaluation of its predecessor, CPD18, and as such falls under the executive review mechanisms as bestowed by the DSA which introduces the obligation to conduct a

thorough review of the functioning of the regulation every 5 years (European Commission, 2022 -b, 100-101). The first wave of reviews is similarly based in text, following a template distributed by the ECM which is filled in by signatories to the CPD. These documents were included to assess the practicalities of the CPD, inter alia the subscription to the CPD as every commitment is on a voluntary basis, which allows an early assessment to be made from the data gathered.

The case study that is chosen naturally presents several limitations, as the immaturity of the review mechanism, including the template distributed by the EU for signatories to fill-in, may contain shortcomings or lead to disharmonized results. In addition, the effects of the DSA and to a lesser extent the CPD may reach well beyond its potential implications on the prevalence of disinformation, however such influences are disregarded for purposes of clarity when analyzing the case study and locating it in the ongoing academic discussions. Given that it is the first wave of obligations to report on the CPD, it is well possible that future rounds attract a much greater number of signatories, which may make the results of this case study less significant or indicative. In addition, this study cannot realistically engage with the tangible efficacy of the DSA and CPD due to them both still being ratified, and as a consequence it focuses on the supposed effects that can be inferred from their organization and the limited feedback available.

3.2 Method of Data Collection

In this section, the manner in which data has been collected for the purposes of this thesis will be explained and justified. Thereafter the process of gathering as well as the results thereof are touched upon, after which these are similarly explained and justified. All of this data is collected to allow for an answer to the guiding research question and sub-questions that draws both upon primary documents and secondary documents in the form of the selected and analyzed documents and the research surrounding the thesis.

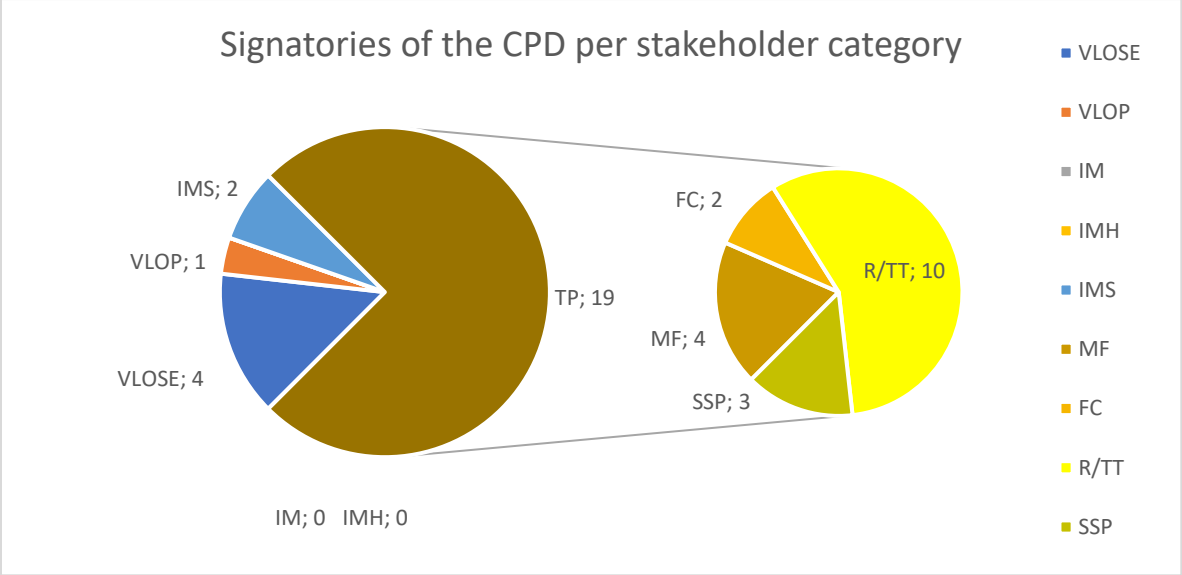
The data from which the analysis is set to draw conclusions is considered the most viable and official sources from which regulatory makeup and the supporting normative underpinnings can be deduced in terms of EU engagement with disinformation. Given that the nature of regulatory frameworks is relatively static, it can thus be assumed that the results that ebb forth from this are subject to *instrumental* interpretation, the interaction between the DSA being an example of the phenomenon on how it ushers in integration with codes of conduct (Stake, 1995). For the second part of analysis that pertains the reports by signatories of the CPD, a combination of 'within-case sampling', to establish linkage to the DSA and CPD, and *collective* interpretation is used to allow aggrandization of text into palpable percentiles that are interpretative of broader trends concerning subscriptions and compliance (Stake, 1995; Mills et al., 2010). The units of analysis that are sequenced are paragraphs, with the overarching tone and intent of the paragraph determining what tag it begets, especially in the

case of obligations, which are split between ‘INFO’ and ‘ACT’ depending on whether they concern provision of information to another party, or whether they oblige to undertake an action. Very rarely does a paragraph contain a high amount of both, and will it receive both obligation tags.

The legal documents that are utilized throughout the analysis chapter both hail from a website that officially belongs to the EU, however the DSA is extracted from EUR-lex, which is a website that functions as the legal repository of the EU, with the CPD being accessed via the main website of the ECM, which also holds the timeline of the CPD and the EUs complete initiative against disinformation. The information of the DSA can also be accessed through the website of the European Parliament [EP], however EUR-lex was chosen due to the document being available in PDF-format, which aligns with all other collected documents. Furthermore, the evaluation reports on the CPD were accessed through the transparency centre, which is a website established by CPD signatories as a consequence of obligations within the CPD, functioning as the official database on the CPD, where researchers should be able to access data. The two legal documents were chosen due to their legislative and normative foundation, and them being part of the EDAP, whereas the latter reports were incorporated to asses how self-regulation functions and what its future prospects are.

In total this means that 28 documents are analyzed, of which two are the aforementioned legal documents, and the latter 26 being comprised of signatory reports, with the signatories being rather varied, ranging from inter alia fact-checking organizations to VLOPs. Both legal documents were ratified in 2022 meaning that they are binding at the point of writing, while the 26 reports were uploaded in January of 2023, representing the first wave of ‘baseline reports’ for which the template was established through cooperation between the ECM and European Regulators Group for Audiovisual Media Services [ERGA], which contains 152 reporting elements (European Commission, 2023 -a). The two legal documents account for 150 pages, and the 26 stakeholder reports contain another 1493, meaning that in totality 1643 pages are analyzed. As the two legal documents hail from the same origin, no questions remain on engagement, however for the CPD this differs significantly. It may well be that the reader at this point has already attained some skepticism concerning the self-regulatory and voluntary nature of the CPD. The graph below illustrates how relatively monogamous the signatories to the CPD so far actually are when it comes to the intended reach of the EU, with both the highest number of signatories and variety therein being visible under the voluntary signatories.

Figure 1



The overwhelming majority of signatories of the CPD are third-party. For information on the abbreviations, please see the footnotes (Hennessy, Appendix 2).[1] TP is third-party signatories.

As can be deduced from the graph above, 21 out of 26 signatories that filed their reports under obligation to the CPD do not belong to the group of actors that it is most likely seeking to reach, as they do not possess the technical capacities to directly address the proliferation of disinformation. Nonetheless, one can also infer that while the CPD has not yet managed to attain sizable signatory status of the owners of the biggest internet intermediaries, some success has already been booked; the five VLOP/VLOSEs accumulatively possess and thus report on 11 of the 19, totaling 57% of the identified very large online intermediaries by the ECM in April of 2023[2] (European Commission, 2023 - b). Thus, at least half of the targeted enterprises have already signed onto the CPD before it became mandatory, with another 8 reports likely joining the fray in the upcoming renditions of the evaluation reports.

Furthermore, the DSA, CPD and 26 reports will be subjected to a qualitative textual analysis at the hand of a coding scheme which will be provided in the next section. This examination will result in empirical data that can be aggregated without losing important context, and shall be embedded within literature and secondary literature throughout chapter 4.

[1] VLOSE; Very Large Online Search Engine, VLOP; Very Large Online Platform, IM; Internet Intermediary, IMH; Internet Intermediary [host], IMS; Internet Intermediary [marketplace], TP; Third-parties, MF; Marketing Firm, FC; Fact Checker, R/TT; Research or Think-Tank, SSP; Standardizing certifier.
[2] All 19: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing and Google Search. Under report of the measured VLOSE/VLOPS: Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, TikTok, Twitter, YouTube, Bing and Google Search.

3.3 Method of Data Analysis

This section of the chapter explains the final dimension of the method that is applied to the case study, seeking to produce results that synthesize well with the theories selected throughout the theory chapter. Due to the nature of the case study, the method most applicable becomes qualitative content analysis. This is conducted on two separate occasions, for different illustrative purposes.

As a first step, the DSA and CPD are both subjected to a coding matrix that will be given at a later point within this section. Herein, the teachings of Mayring (2019) are followed, who argues that through the utilization of a coding scheme the processing of "*larger amounts of text to be able to go beyond a purely case-by-case exploratory research strategy"* is allowed (Mayring, 2019, 2). This is important to the current case study, as the DSA and CPD are constructed to come together under a single initiative to further the ambitions of combating disinformation on proverbial EU soil. In addition, this approach lends itself for data generalization in analysis that concerns itself with more than a few documents, which make it applicable to the analysis of the 26 stakeholder reports of the CPD. Berg and Lune (2017) furthermore determine that data collection and organization function as advance planning, through the creation of categories, which is paramount to representativeness, validity and reproducibility, concluding that "*the raw data require some sort of organizing and processing before they can actually be analyzed*" (Berg and Lune, 2017, 40). This in turn makes the analysis of interpretative nature.

For the second step of the analysis, qualitative interpretation is necessary to allow juxtaposition of the empirical findings that have been produced through the aforementioned application of the coding scheme. This is what Miles and Huberman (1994) describe as interpretative qualitative data analysis, as it allows research to "*uncover patterns of […] action, and meaning*." (*Idem.,* 182-183). This will allow wide interpretation of the stakeholders' decisions to engage with certain sections of the CPD on a wholly or partially self-regulatory basis, depending on stakeholder categorization, and thus forms a method through which "*generalizations*" can be established which have the ultimate purpose of allowing the establishment of how the reporting template is utilized and what can be gauged on the basis thereof (Neuendorf, 2002, 12 and 14-16). Whereas the data to be examined has already been explained in the previous two sections of this chapter, the coding scheme has to still be elaborated on, and this will happen in the following section of this chapter.

Concerning the validity and reproducibility of research conducted in such manners, Berg (2004) underlines that empirically measuring the occurrence of text elements can serve as an intermediate step of understanding, allowing "*identifying, organizing, indexing and retrieving data*" (Mayring, 2020; Berg, 2004). Such categorical aggregation makes use of markers that allow reduction to number of instances without losing context, allowing both in-depth close reading as well as empirical inference

(Stake, 1995, 74-75). Mayring (2014) remarks that in such cases, the best way of establishing the codes to be measured is through engaging with the material at the hand of 'anchoring examples' which can be refined once the researcher applying it has gone through a certain percentage of the total material, in order to account for what has been omitted, as well as allowing the incorporation of interesting categories that might have otherwise been missed (Mayring, 2014, 40-42). To come to a coding scheme that is functionally appropriate as well as a valid and consistent, the advice by Mayring (2014) was followed and the DSA and CPD were subjected to a pilot study which led to the priorly envisioned two coding schemes being reduced to a single, more robust coding scheme (*Ibid.,* 41). In short, the coding scheme is used to empirically measure the frequency of the terms as outlined in the coding matrix, solidifying the interpretative factor of the qualitative content analysis.

3.3.1 The Coding Matrix

As becomes clear from section 3.3, the methodological composition of this thesis leans heavily on qualitative methods as envisioned, critiqued and refined by Mayring throughout his many years as a research methodologist. He argues that while the aggregation of much data into few integers amongst many things requires the establishment of a category system to identify the elements of text that are measured in frequency, for these to acquire a conceptualized definition, determination of the unit of analysis, formalization of a reproducible coding scheme and the computation and ultimately interpretation (*Ibid*, 25). As the original pilot study upon which the anchors are based will be omitted from this thesis due to size constraints, the coding matrix will be given on the next page, and its contents will be elucidated subsequently.

Figure 2

Variable	Category	ID	Codes	Definition	Implication
Procedure	Positive	INFO	Inform; Publish; Report; Provide […]; Notify; Make Public; Draw up; May […]	Provide information in written-form, for purposes of transparency	This tag indicates a positive obligation to provide information being bestowed
		ACT	Put; Create; Certify; Establish; Conduct; Convey; Act; Mandate; Designate; Shall […]; Be; Take; Process; Provide; Suspend; May […]	Conduct an action, for respective purpose related to its clause	This tag indicates a positive obligation to conduct an action being bestowed
	Negative	NO	Shall not; Will not; May not; Can not; … [not];	Assigned action is disallowed	The mention hereof implies that the actor is obliged to, can choose to, or ought to NOT undertake a certain action
Procedure	Origin	BI	[Mechanical]; Start […]; May […]; Will […];	This tag is applied to purely mechanical paragraphs, invalidating any other tags assigned to it	This indicates assignments of purely mechanical nature, in respect to already labeled tasks
	Accountability	PERS	ECM; VLOPs; VLOSs; OPs; OPsS; EBDS; MS; EC; EP; PPL; DSC; AUDI; CJEU; LRP; IMs; CofC; HIMS	Abbreviations stand for an actor either derived from priority 1 or 2 documents	Allows attribution of obligations to relevant actors
Regulative	Specific	CR	[Mention of EU regulation]; [Mention of EU directive]	Tag is applied to cross-references EU legislation to discern interactions	This tag allows extrapolation of relevant documents in their relation to others, technically allows mapping of intersecting frameworks
	Broad	CR(g)	[Mention of EU initiative that is not a document under CR]	Tag is applied to cross-references EU initiatives to position and justify	This tag allows extrapolation of relevant documents in their relation to others, technically allows mapping of normative push

3.3.2 The Codes

The utilized codes within the coding scheme can be interpreted as being organized to allow the systematic answering of the sub-questions as given in Chapter 1.1 of this document, building on one another as the sub-questions progress in number respectively. Positive and negative law, the first two categories, containing the codes INFO, ACT and NO, imply obligations to act through provision of information, undertaking action, or prevent action through a negative obligation. These codes directly relate to sub-question 1 that concerns itself with how the DSA and CPD function as an attempt to prevent policy fragmentation and standardize conduct by measuring the established protocols that actors should comply to, allowing inference of what actions are heavily regulated as well as how, in addition to which specific actors they are attributed to, directly allowing assessment of "*minimum standardization*" as coined by Dougan (2000) as well as assessing when action is warranted, measuring capacity to act against the four authoritarian indicators as coined by Levitsky and Ziblatt (Dougan, 2000, 860; Levitsky and Ziblatt, 2018, 14-15).

Secondly, BI and PERS are measured to assess which actors are attributed responsibility and where freedom to act is given, allowing measuring of how much freedom or obligation to act is bestowed upon the relevant actors throughout the documents, as well as when clear fault is attributed. These findings in turn further compound the answer to sub-question 1, while also allowing insight into how disinformation or the will of actors may trigger, or alter, subsequent protocols, which falls within the area of interest for sub-question 2. As these codes represent actions that may be undertaken as well as assign responsibility, these five codes cumulatively allow tackling whether the conceptualization of disinformation also allows interaction with "*malinformation*" as coined by Derakshan (2017) which remains relevant since, as Ophir and Jamieson (2021) find, the effects of unhealthy information and any form of disinformation are equally severe (Derakshan, 2017, 20; Ophir and Jamieson, 2021, 13-16).

Thirdly, the codes CR and CR(g) are measured to represent instances of cross-legislative references. Much like the previous two codes, this compounds the answers to both sub-question 1 and 2, however since such cross references can also function as referrals and demarcate limitations of the reach of the two documents that are being analyzed, they offer valuable context to assess the integration of the push against disinformation at the European policy level, contextualizing the applicability of the conceptualization of disinformation and its protocols, while also finalizing the boundaries of competences and obligations on behalf of the involved actors. Building on the answers to sub-question 1 and 2, the theories of Howard and Parks (2012) and Sartor (2013) can be utilized together to establish how the responsibilities and risks of delegation of risk are utilized throughout the DSA and CPD, allowing an academic measurement thereof while also keeping in mind the potential chilling effects that these might have, as well as the warnings of Saurwein and Spencer-

Smith (2020) that these might cause conflicts of interest (Howard and Parks, 2012, 362; Saurwein and Spencer-Smith, 2020, 825; Sartor, 2013, 44).

3.4 Conclusion

The research for this thesis is of interpretive nature drawing heavily from qualitative content analysis. The codes utilized throughout the coding matrix, which is utilized to establish empirical knowledge upon which the conclusions to answer the sub-questions and answer the final research question are based. These codes are embedded in their respective theories and form three groups, of which each pair establishes a foundation for the subsequent sub-question to be answered, synthesizing all theories as mentioned Chapter 2.6. This coding scheme is then applied to the DSA, measuring the frequency of the codes within the document to allow the theoretical assessment of the DSA on its own; this is also done for the 26 CPD reports of which the results are accumulatively assessed, before they are combined together to establish complete insight as to their functioning in tandem, given that the ECM has communicated that the CPD is to become an official supporting document of the DSA. From these empirical results, conclusions will be drawn to answer the relevant sub-questions which allows the positioning of this thesis vis-à-vis the contemporary literature that has already been written on disinformation, censorship, digital moderation and the degenerative effects of the proliferation of all the aforementioned.

4. Analysis

The DSA and CPD were examined at the hand of the coding scheme as presented in Chapter 3.3. As a second step, the first wave of evaluative signatory reports as well as the aforementioned two documents were subjected to qualitative document analysis to provide context and insights to make use of this data and place it into the greater academic discussion surrounding the DSA and CPD as well as to form a basis upon which the guiding research question is to be answered. As the size of this thesis does not allow for extensive elaboration of the results or tracking of the process, please see appendix 1 and 2 for codified results of the two sets of documents analyzed. This section follows the same order as the sub-questions: [4.1] function, [4.2] disinformation and [4.3] accountability, to allow the dissemination of information to follow the same gradual shift from top-down to bottom-up, which is in-line with the research questions. In the next subsection, the function of the DSA and CPD will be discussed and juxtaposed to the tangible results of the first wave of reports, to allow positioning of the outcome into the greater strategy against disinformation of the EU.

4.1 Organization of the DSA and CPD

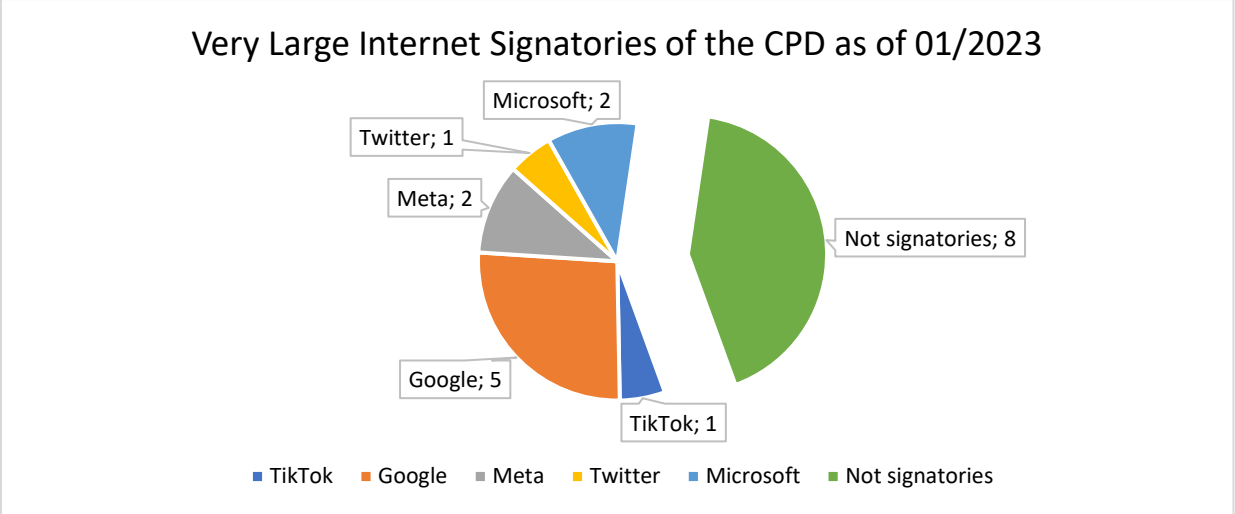
The function of the DSA and the CPD are manifold. The DSA is a regulation that introduces horizontal obligations for purposes of harmonizing the digital spaces of internet intermediaries that are frequented by significant portions of the EU population, augmenting data transparency and consumer rights, as well as offering positive incentives for very large online platforms and search engines to engage in self-regulatory codes of conduct (European Commission, 2022 -d, 3, 63, 88 and 21). The strengthened CPD is poised to form one of these 'codes of conduct', targeting disinformation and preventative action against manipulation of information and digital mechanisms, allowing voluntary procedural subscription to its commitments and measures while simultaneously functioning as framework that can be utilized for VLOPs and VLOSs to get their obligations in order to smoothen the coming-into-entry of the full list of obligations of the DSA (European Commission, 2022 -a, 2). Both documents augment each other through the legal power of the DSA which specifically recognizes the CPD as being one of the instruments that might be necessary for big internet intermediaries to effectively address systemic threats, of which disinformation is one.

This is contextualized through the EDAP, where the EU has upgraded and officiated its intent to combat the presence of disinformation through three means: actively expanding (i) its toolbox for "*imposing costs on the perpetrators*", (ii) "*overhaul … the Code of Practice on Disinformation into a co-regulatory framework*" and (iii) establishing a more "*robust framework for monitoring [the CPDs] implementation*" (European Commission, 2020 -b). This could be interpreted as the EU doing exactly what Albert (2017) argued member-state democracies should do, establishing a toolkit to deal with undemocratic practices (Albert, 2017, 197-198). Via the DSA, the EU has introduced procedural

mechanisms functioning as a negative incentive to *inter alia* not create or disseminate illegal and harmful disinformation, and strengthened the CPD (European Commission, 2022 -a, 1-3). The CPD takes on a similar procedural nature, attributing various levels of obligations to categories that are determined via the documents on the basis of reach and type as well as other in-effect legislation (Husovec and Laguna, 2023, 9). Three definitions reiterated within the DSA are based on a 2015 regulation: "*Mere conduit", "Caching" and "Hosting'* (European Commission, 2022 -d, 2). In the latter definition, it additionally defines a sub-category, "*online platforms*" (*Idem*., 5) and furthermore the ECM also assigns platforms with a reach of over 45 million active users the moniker 'Very Large Online Platform' [VLOP] or 'Very Large Online Search Engine' [VLOSE] which bestows additional obligations upon the company (*Idem.,* 21). For a list of these, please see Chapter 3.2.

The role of the CPD can be located in relation to how it interacts with the DSA. While the original CPD was launched in 2018, the strengthened CPD came into effect in 2022 as an element that belongs to the DSA by functioning as a 'code of conduct' [European Commission, 2022 -a, 2]. This is significant due to the DSA stipulating that "adherence to and compliance with a given code of conduct" by a VLOP "may be considered as an appropriate risk mitigation measure." (European Commission, 2022 -d, 29). As such, the DSA can be seen as the regulatory backstop, whereas its function and incentivization of signing on to the CPD can be seen as a step towards it also functioning as a "*co-regulatory backstop*" (Shattock, 2021, 3). Shattock (2021) himself concluded hereon that in its CPD18 state, the CPD lacks enforcement capacity and the DSA fails to address disinformation that escapes technical illegality (*Idem.,* 5-6). As the CPD has received an update since then and the DSA is in the final stages of being ratified however, it seems that the ECM is actively working on further ensuring that the EU is establishing viable means to combat disinformation, with a focus on delegation of responsibilities. It can be safe to say that, as far as the voluntary nature of the CPD is concerned, the DSA and its enforcement will gradually seek to enforce adherence to the CPD by at least the 19 major internet intermediaries that conduct business within the EU. Furthermore, the voluntary nature does not seem to result in such negative outcomes, as 11 of 19 VLOSEs and VLOPs are already signatories to the CPD, due to them being owned by 4 signatories, as is visible in *Figure 3* below.

Figure 3



Over half of the VLOPs and VLOSE were signatories to the CPD and thus at least normatively have accepted the obligations of proactively combating the proliferation of disinformation to the extent their technical capabilities allow (Hennessy, *Appendix 2*).

On this it has to be noted that Twitter has officially withdrawn from its commitments to the DSA (Broersma, 2023). This reduces current membership to 10 out of 19, or 52%, meaning the regulation is nonetheless still reaching over half of its intended audience with increased enrollment to the CPD being likely. The future will have to tell what the implications thereof are as the internal market commissioner Breton (2023) in response to this choice stated "*Obligations remain. You can run but you can't hide"* (*Idem.*) Under any circumstances, it is likely safe to say that the Achilles heel of the CPD, if it possesses one, most likely does not exclusively lie within its voluntary nature. This matter does however warrant a look at how the DSA, being the regulation that has enforcement capabilities, is constructed to be able to achieve its intended aims. The DSA functions not as a framework to indicate when an internet intermediary can explicitly be held liable, instead it heavily focuses on reiterating the conditions under which one cannot be held liable for the illegality of illegal content dissemination via the mechanisms of their service (European Commission, 2022 -a, 6). It does, however, demand that internet intermediaries extensively document their conduct.

Besides bestowing obligations to inform or act upon internet intermediaries in a procedural manner, the DSA and CPD should also be considered highly normative documents. The first 156 and 32 paragraphs of these respective documents establish the norms under which the regulations itself should be interpreted and enacted (Hennessy, *Appendix 1*). This implies that Dougan's (2000) assessment that EU policy tend to impose "*values which merely interface with rather than serve the economic demands of the single market*" does not uphold at least in the case of both the intent and

the functioning of the DSA and CPD, with compliance enforcement of the former falling under the legal interpretative role of the CJEU in cases that the ECM cannot enforce compliance (European Commission, 2022 -a, *38*). Furthermore, this allows the embedded norms to intersect with the four indicators of authoritarian presence as established by Levitsky and Ziblatt (2018), which will be discussed in greater detail in the second section of this chapter. The DSA and CPD as such are embedded heavily within the EU regulatory frameworks, attributing executive power to the ECM and in worst case relying on the CJEU for interpretative case law to legitimize the decisions of the ECM or even of those that challenge their interpretations, but also allowing the presence of a normative dimension that creates greater leeway of action against abuse or noncompliance to both documents.

This is also the point where the normative definitions as utilized by the ECM become important, as these are determinant in their ability to enforce cases of distinguishable noncompliance. In chapter 2.1 it has been explained that the EU is by large a multilateral institution of which the persistent functioning relies on the governments that make it up adhering to the principles of liberalism, constitutionalism and pluralism, and if these values are scorned then the democratic security of member-states and subsequently the EU are at risk. The necessity of these values is officiated through codification in article 2 of the TEU (European Commission, 2012 -a, 17). Within the DSA and CPD the importance moderating content that does not uphold these as well as other fundamental rights and freedoms are mentioned an additional 45 and 4 times, with 13 and 2 being in the regulative half of the respective documents (European Commission, 2022 -a; European Commission, 2022 -b). Furthermore, the introduction of a normative dimension should disempower exorbitant abuse of the framework for private purposes, and thus reduces the freedom that social media platforms or other internet intermediaries might be able to exert. In other words, the concerns of Bendiek (2021) that power has been increasingly accumulating in the hands of digital oligopolies is somewhat alleviated, allowing the ECM to infringe or demand explanations on removal of content or denial of service even when the accosted actor is in technical legal compliance with the two documents. Giving this power to the ECM and CJEU they should prove to enforce harmonization of both the normative and legal aspects amongst the actors that beget obligations under the DSA and CPD, indicating that this act goes further than “merely interfacing” with EU values.

Besides harmonization for application of the obligations under the norms of the EU, the EU also acknowledges that the norms as enshrined in the Terms of Service [ToS] of individual stakeholders should be harmonized to some degree. For purposes of clarity, consistency and procedural transparency the normative pages of the DSA and CPD refer to the necessity of ToS to be known and enforceable by end-users, as well as requiring information on how ToS are constructed to deal with the proliferation of disinformation (European Commission, 2022 -a, 49; European Commission, 2022 -

b, 20, 25 and 35). The demand for identified stakeholders to comply to the regulations and transparently report to both the ECM and communicate to the public hereon creates another safeguard as grounds on which end-users are protected to possible abuses of power on behalf of internet intermediaries. The DSA and CPD as such establish a complicated intertwined network of obligations that are constructed in a manner that through transparency all stakeholders should be empowered, ranging from information provision towards end-users by platforms to requiring moderation mechanisms to be accessible and challengeable by end-users, distributing the liability of actual enforcement of disinformation in a manner that alleviates Sartor's (2013) concerns on the possible "*Chilling*" express that moderation liabilities would bring about. This is predominantly due to the nature of the content of the DSA and CPD that address disinformation, which will be elaborated upon more in Section 4.2.

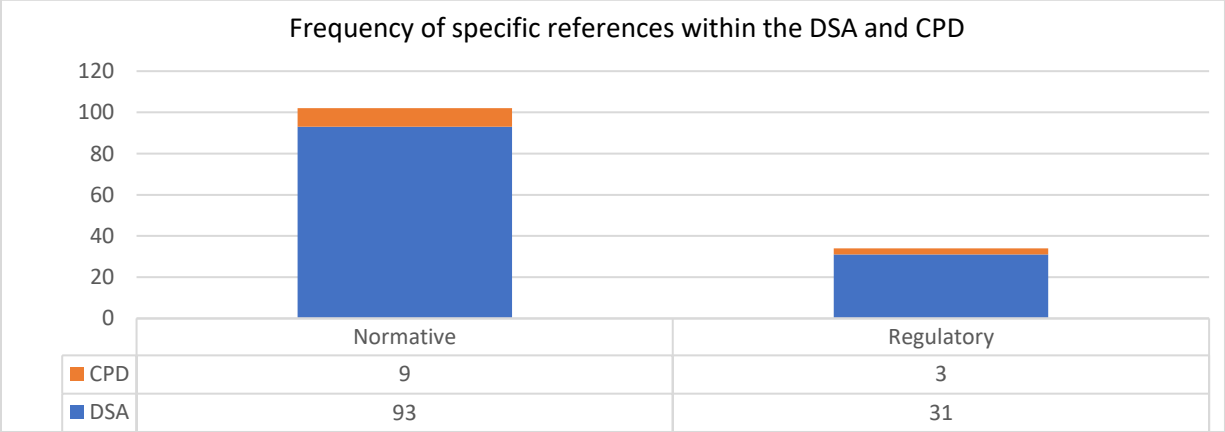
So far, the harmonizing effects of both regulations, as well as its technical internal interactions have been discussed, allowing a tentative argument to made for both the successes of the combined reach as well as the ability for the framework to pervasively strengthen EU norms, which are fully in line with the intents of the EDAP. A third variable that factors into the organizational makeup, and enforceability, of the obligations within the documents is the EU level legitimization that allows actors guideline their interpretation of the obligations contained within. The push for harmonization of service and mechanisms brought by the DSA can be interpreted as a level of democratization of the internet, in that checks and balances are redistributed amongst its stakeholders ranging from top-down to bottom-up, with ECM being able to enforce compliance and mechanisms that empower end-users to make informed decisions and judicially challenge decisions by internet intermediaries, with procedural reliability being paramount to democratic functioning and the latter being enshrined as a right in Article 47 of the Charter of Fundamental Rights of the European Union [CFREU] (Pappas, 2016, 265-266; European Commission, 2012 -c, 405). The recognition of the importance of public participation in establishing rules and norms on the internet is heavily embedded both in the normative nature of the EU as well as countless of its legal and normative undertakings.

Savin (2021) noted that the proposal of the DSA, in combination with the CPD18, left too much individual executive responsibility in determining what is illegal due to its reliance on international law of absolute negative obligations and conferral to domestic law for other grounds of content termination or restriction (*Idem.,* 15-16). While arguments for the inclusion of both normativity and legal aspects, as well as their interpretation, have already been made in this section, the current set-up also offers ample review mechanisms that the ECM shall utilize to ensure the harmonizing effect of the DSA and CPD. To translate the copious amounts of information that the DSA and CPD stand to extract, a 5-year review mechanism is introduced through Article 91 which obliges the ECM to report

to the EC and EP on the effectivity of the regulation, and the CPD obliges its signatories to publish a report on their work conducted in face of their obligations yearly (European Commission, 2022 -a, 101; European Commission, 2022 -b, 17).

This bides well for the ability of the ECM to improve harmonization and reduce pitfalls that might arise as a result of the DSA, which is the legal backstop. The CPD in this is considered a specialized supplement to the DSA, and this is also visible in the degree it refers to existing regulations. *Figure 4* and *Figure 5* display the number of references made to other regulative acts and other normative initiatives such as the EDAP, respectively. These are given to illustrate that both the CPD and EDAP are not meant to function without context, and seek intersection and engagement with other regulations throughout their functionality, making the push against disinformation as pluralist and procedural as the EU and constitutionalist democracies are.

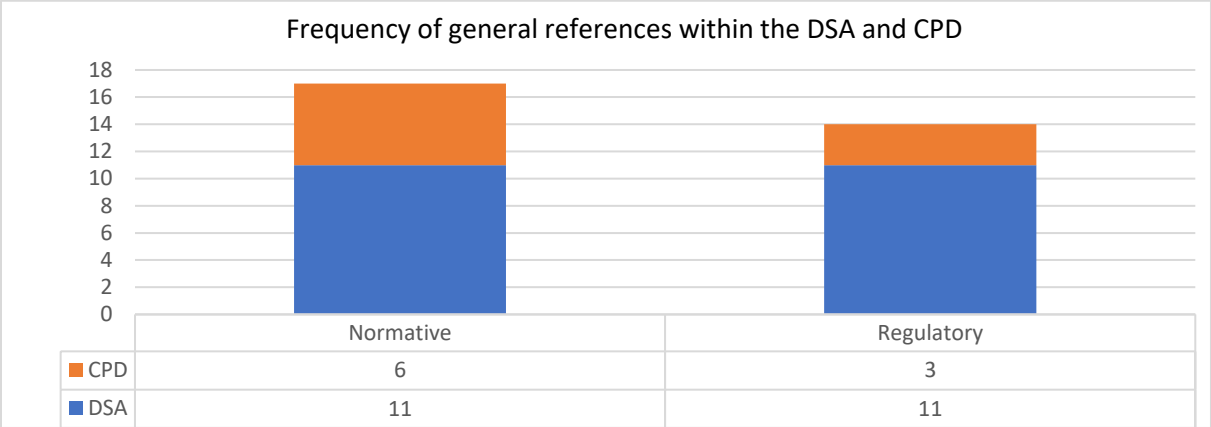
Figure 4



Slightly over 100 specific references are made to in-effect EU regulations on normative, as obligations of the DSA and CPD ought to supplement other initiatives (Hennessy, Appendix 1).

The specific references made to other in-effect EU regulations are extensively present in the normative sections of the DSA and CPD, indicating that the obligations within the two documents are above all intended not to take primacy over, or negatively impact, other legislative acts' functioning. These acts also extract definitions from other EU documents, reiterating that obligations to the DSA and CPD are also subject to compliance to other regulations, which is surprising given that the CPD itself is on voluntary basis, but nonetheless shows how the EU might be seeking to gradually integrate it further into the DSA and mandatory codes of practice within EU digital spaces.

Figure 5



*Featuring considerably lower numbers, general references are made somewhat consistently, locating both documents in the scope of ongoing initiatives that set out the normative direction (*Hennessy, *Appendix 1*)

In conclusion, the DSA and CPD are meticulously organized in a manner that prevents wrongful interpretation, extensively establishing foundations for both normative and legal enforcement. Having established the justifications, the next topic to be discussed is conceptualizations, intent of the obligations and how these manifest within the DSA and CPD.

4.2 Defining and dealing with disinformation

Having established how the EU is organized in a manner that ensures the harmonizing effects of the policies at the EU level, it is important to deduce how the DSA and CPD intend to operationalize action against the spread and presence of disinformation. Here it is important to briefly touch upon the fact that the DSA in part came about due to the "*diverging national laws negatively affect the internal market*" (European Commission, 2022 -a, 1). Thus, the EU, no longer able to guarantee its obligations concerning the healthy functioning of the internal market in accordance with Article 26 of the TFEU, the EU was forced to undertake action (*Ibid.*). This has led to the risky necessity of the EU having to define what exactly entails disinformation despite the fact that defining this has also escaped academia, which has managed to identify innumerable variants but failed to reach consensus on what is necessary and what is sufficient to qualify as disinformation. Nonetheless, besides introducing specialized clauses the DSA and CPD draw from definitions of disinformation and its variants in the EDAP, conceptualizing and demarcating a phenomenon that can be addressed (European Commission, 2022 -b, 7).

Herein it defines (i) misinformation, (ii) disinformation, (iii) information influence operations and (iv) foreign interference in the information space, with the former two being variants of disinformation whereas the latter two are phenomenon that may bring it about (*Ibid.)*. These

definitions are furthermore also linked to intent, with misinformation assuming or deducting that the information was unintentionally manipulative whereas the latter was clearly created or spread for nefarious purposes. Differentiating between these two establishes a rather obvious issue, as Husover and Laguna (2023) note, concluding that the source of the content may be hard to locate, even for internet intermediaries that may possess the technical capacity and information for as far as their place in the digital ecosystem allows (Husover and Laguna, 2023, 1). Malinformation, as coined by Akshan (2017) is not formally mentioned as being amongst one of the separately identified modes of disinformation that is utilized by the CPD, and thus the DSA (Akshan, 2017, 20). Nonetheless, the EU tackles manipulative behaviors as a separate phenomenon as well, meaning that while it is not swept up under the moniker disinformation, manipulatively including, editing or leaving out important contextual matters may still be identified and addressed through the DSA and CPD (European Commission, 2022 -a, 58 and 64-65; European Commission, 2022 -b, 15-18) Furthermore political advertising, one of the main drivers of disinformation in recent times, is addressed in general throughout the DSA and has special clauses for VLOPs and VLOSEs, and is subject to a harmonization of definition under the CPD, meaning that in this case the EU bypasses the potential shortcomings of their definitions and introduces measures to make its sources more recognizable (European Commission, 2022 -a, 59 and 69; European Commission, 2022 -b, 10-14).

This means that the relative difficulty of which the definitions that are subjective to intent of the original source of communication risks making the conceptual addressing of occurrences on that basis difficult or impossible without a constant fact-checking apparatus. Despite this, the DSA makes a strong case by including the prohibition of manipulation of the mechanisms of internet intermediaries, regardless of source, through requiring information provision towards end-users on the basis of the information's funder (European Commission, 2022 -a, 59). Thus, the DSA again establishes a way for end-users to discern whether the source of the advertisement or information is reputable, alleviating the absolute need for demarcations of trustworthiness as spreaders of potential disinformation or manipulative information become susceptible to reputational costs. The requirement for online environments to proactively display the source of content, as well as the requirement for internet intermediaries to identify and establish the trustworthiness of legal individuals that conduct business on their platform's interfaces well with the concerns of Ophir and Jamieson (Ophir and Jamieson, 2021, 13-16). The interpretation of the definitions as enshrined in the EDAP thus are not perfect, however the DSA and CPD seem to establish a wide toolkit with which end-users and ultimately constituencies should be more protected against the unhealthy effects of manipulative information, allowing both completely false and misleading information to be identified in an accumulative manner through the establishment of an online advertisement database conform with Article 30 of the DSA (European

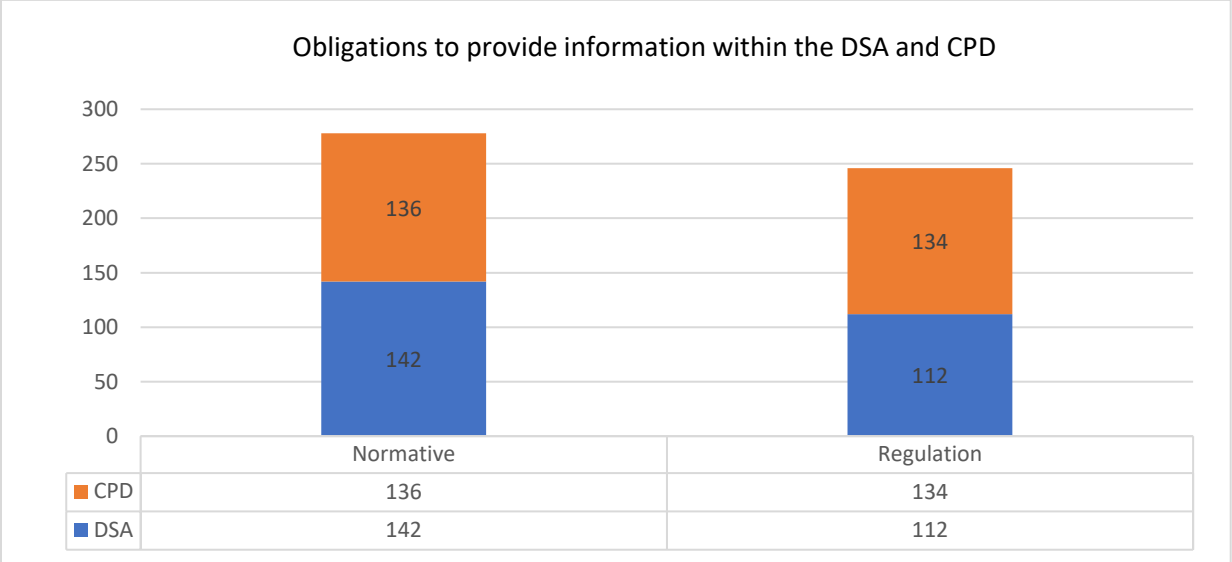
Commission, 2022 -a, 60-61). Malin formation, as defined by Akshan (2017), thus can also be traced back and addressed at the hand of this database, which bids well for researchers and internet intermediaries that wish to comply with their obligations to the DSA and CPD (Akshan, 2017, 20).

Rather than being stringent, the definitions are as such highly flexible and may intersect, making the basis of removal and procedural sides of the process more important than the conceptualization. This is taken into consideration throughout the construction of the frameworks of the DSA and CPD, and as a consequence they include clauses that necessitates preliminary notices and the proactive provision of information on procedures, law and terms and conditions (European Commission, 2022 -a, 12 and 84; European Commission, 2022 -b, 20, 25 and 35). Altogether this makes the DSA and CPD relatively extensive toolkits that allow removal of unhealthy content by private enterprises on various grounds, but also bestows both ex ante and ex post guarantees that allow end-users and the ECM to address misuse of the obligations to act. Whereas Savin (2021) argued that Article 12 to 15 being copied into "*Articles 3, 4, 5 and 7*" of the DSA will not lead to additional liability for platforms, and thus misses the point of bestowing due diligence obligations on them, the absence of enforced preliminary action prevents the chilling effect on freedom of expression that was warned for by Sartor (2013), implying that EU has taken a middle road which bestows limited liability but also fully accounts for the protection of the economic externality that is its obligations to the CFREU and ECHR (Savin, 2021, 5-6; Sartor, 2013, 44).

As explained in the previous paragraphs, action is thus warranted on various grounds and needs to be procedural and justified, citing relevant law or ToS that has not been complied with. As such the burden of proof wholly falls on the stakeholders, and while liabilities and exemptions thereon remain largely in-place, the DSA and CPD are organized in a manner that incentives both action and information. The DSA and CPD contain an incredible number of obligations on provision of information or obligations to act, most of which are directed at internet intermediaries in general, with few applying only to those offering specific services, citing chapter 4.1 these are "*Mere conduit"*, *"Caching*", *Hosts*" and "*Online Platforms*" as well as very large variants of the aforementioned, plus search engines. Given that disinformation is an issue that is hard to localize, much of the provisions within both documents seem to underline the importance of identification of the scope of the threat that disinformation poses through the services of internet intermediaries, which is achieved through data provision. This will ultimately allow the identification of any sort of systemic abuse of online services, as well as the perpetrator behind it, meaning that the warnings by Ginsberg (2021) on the risk of prolonged normative hijack of international organizations and spaces is alleviated by making good faith compliance a palpably identifiable metric (Ginsberg, 2021, 229). The number of arguments made in

favor of the necessity of information provision, as well as the actual obligations to do so, are illustrated in *Figure 6* which is below.

Figure 6



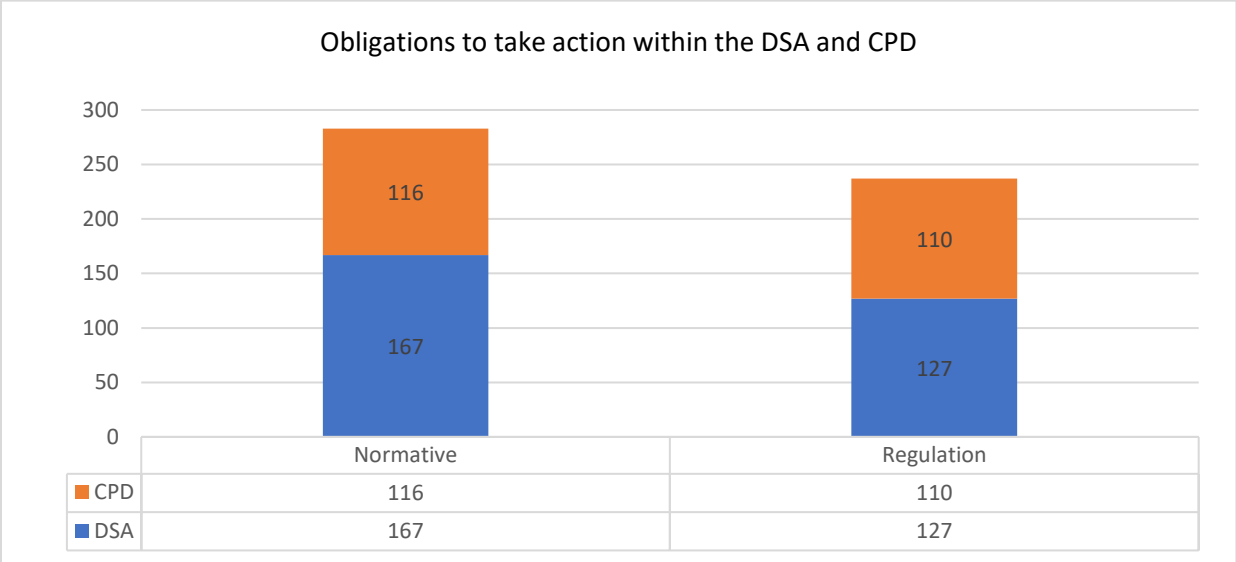
The number of obligations to provide information is high in both the DSA and CPD. Considering that the DSA is less than half as long as the DSA, this is especially true for the CPD (Hennessy, *Appendix 1*).

The sheer amount of information that should become available over time as both documents come into effect should allow the ECM, EBDS as well as all other stakeholders to make consistent decisions and furthermore serve to protect users against misuses of the powers bestowed hereby. This is also supported by the large number of involved stakeholders that are directly named within the documents, as seen under PERS in *Appendix 1*, which all function as a check within the process.

On the other end, there are also a large number of obligations to act incorporated into the DSA and CPD, which call upon those it addresses to undertake actions ranging from establishing the transparency centre, to complying with a wide range of due diligence obligations (European Commission, 2022 -b, 35-36; European Commission, 2022 -a, 48). Here, the mostly voluntary nature of conscription towards the CPD might become a point of contempt, however this quickly brings about the question to which degree non-very big players have the actual capacity to disseminate disinformation while completely avoiding the big platforms. As such, the obligations to undertake action bestowed upon the procedurally categorized internet intermediaries can be assumed to be at least as important as the provisions to provide information, as it is the information that provides foundation for the enforcement thereof, and the enforcement is the matter within most of the paragraphs that determine what actions to take at which point, underlined by their purpose in the normative sections. If social media consist of infrastructure, content and actors, as Howard and Parks

(2012) theorize, then the DSA and CPD do well to bestow the responsibility to act upon those that have the technical capacity and capabilities to moderate the content (Howard and Parks, 2012). Below, *Figure 7* is given that provides similar metrics on obligations to act.

Figure 7



The number of Obligations to act within both documents is slightly higher (Hennessy, *Appendix 1*).

Not all of these actions concern disinformation, as priorly mentioned some of them may contain preventative action and address political advertising, which may in turn have a positive effect on the presence of disinformation throughout the digital ecosystem. Information provision stands essential to the DSA and CPD, especially when it comes to disinformation, and the CPD herein functions as the vanguard that allows an extremely high amount of information thereon to become accessible to the EU even if only the VLOPs and VLOSEs were to become signatories. So far, in Chapter 4.1 the position and functioning of the DSA and CPD relative to each other and to the EU have been discussed, the incorporation of grounds of justification as being legal and on the basis of EU and stakeholder norms and terms of service, as well as how these can factor together to allow theoretical enforcement against disinformation. In chapter 4.2, so far, the given, utilized and functionally by-passed definitions have been explained that allow enforcement that foregoes stringent definition, followed by this chapter that discussed the frequency with which obligations to provide information, as well as obligations to conduct action, are present in the DSA and CPD, in combination with why the allocation of responsibilities as it is makes sense and should alleviate the academically identified risks, threats or shortcomings. The following and final section of this subchapter serves to illustrate the engagement of third-parties with these engagements, and why it might actually prove beneficial that the CPD, as

an element of the DSA, is accessible to actors that are not enabling or providing access to services online.

As was already indicated in Chapter 3, the majority of the actors that subscribed to the CPD and thus its obligations and commitments are not providers of online services, especially not to the height that regulation thereof might prove beneficial to the EUs EDAP commitments against disinformation. Instead, it is indicative that there is a degree of public demand or awareness of the threat that is posed by disinformation, especially when taking into consideration that of the 21 third party signatories, 2 are fact-checkers, 3 are organizations that standardize through certification and 12 are specialized research organizations and think-tanks (Hennessy, *Appendix 2)*. It is in practice, where the co-regulatory nature of the EU initiative to combat disinformation comes to fruition, allowing such actors to directly engage with the companies and mechanisms that are meant to both map the issue of disinformation and establish a toolkit to effectively deal with it. The normative basis upon which disinformation is identified as such should stand to become increasingly supplemented by insights and observations of highly specialized firms that conduct work in this area for private and public firms, incorporating the myriad of perspectives that disinformation and its many variants requires, given that it can manifest in so many ways it escapes simple definition. The fluidity of the DSA and CPDs definition of disinformation, misinformation, manipulative information through determination of discernible patterned intent to manipulate or mislead, heeds Doobs (1989) early warning that defining it would merely problematize its capture (1989; Jowett and O'Donell, 2015, 4). A better basis for enforcement, validating the obligations to act, thus becomes information. After all, as was argued by Jowet and O'Donell (2015) on establishing a dogmatic definition of propaganda, an interpretation that becomes value-laden can lead the enforcers too focus too much on any of the attributed factors, making research or action too narrow and constrained to be effective (Jowet and O'Donell, 2015, 2-6).

Much like chapter 4.1 concluded, the future-proofing of combating disinformation partially hinges on the wide applicability of the framework that it is embedded in. The review mechanism of the DSA bides well for future amendments and reorganizations of the regulatory side, whereas the sheer information provision that is provided by the CPD should multiply the information to assess effectiveness and compliance for the policymakers by multitudes. In practice this means that there is no single form of disinformation that cannot be addressed by the DSA in combination with the CPD, while it also has to be recognized that the DSA offers legal basis only for the removal of illegal content as conform with international treaties such as CFREU and ECHR, and domestic laws, the CPD provides and burdens internet intermediaries with legitimated grounds to undertake pressing action against the proliferation of harmful content within their technical dominion. In conclusion, the DSA and CPD provide a legal basis as well as a normative basis, which is then further complemented by the ToS of

platforms that function as house-rules; all three of these levels are subject to harmonization as a consequence. The next subchapter, 4.3, more closely examines the results of the analysis into the CPD reports to determine how the responsibility to moderate unhealthy content is delegated.

4.3 Accountability within the DSA and CPD

The previous two subsections discussed how the DSA and CPD are organized, and how disinformation is conceptualized and operationalized as well as how internet intermediaries are tasked with and empowered in combating it. This is the final subsection of the discussion chapter of the thesis and serves to illustrate, based upon the outcomes of the case study of this thesis, how the responsibilities of actually combating disinformation are divided within these two documents. As mentioned in subchapter 4.1, the DSA and CPD have received an update since Shattock's (2021) critiques and conclusion on the lack of enforcement within the framework (Shattock, 2021, 5-6). These have in practice at least equipped the monitors, both internet intermediaries and platforms, as well as the enforcers with an expanded toolkit that foregoes legal basis and removed CPD18 requirement of information being "*verifiably false*", allowing wider application albeit also demanding more reporting in-depth reporting on the application of moderation (European Commission, 2018, 1). Nonetheless, the enforcers have been equipped with a more extensive toolkit to combat disinformation, and the monitors have been given, at least in terms of guarantees, more access to information and more specific points where they can collect this, but the question of how the ECM is able to enforce compliance with the frameworks of the DSA and CPD are a wholly different matter.

The DSA and CPD are organized in a manner that pursues harmonization not through aggressive legislation, but rather introduces minimums from which actors in digital spaces cannot deviate. Dougan's (2000) claims that EU values tend to "*merely interface with economic considerations*", as such does not uphold completely, however it may partially explain the relative lack of enforcement mechanisms that are visible within the DSA and CPD. This also seemingly confirms Shattock's (2021) claim that the DSA to this degree functions as a "*co-regulatory backstop*". Nonetheless, as argued for in the previous two subchapters its function is limited to these things only when viewed from a reductionist angle, and it is clear that its implications and ambitions supersede these views. It is unlikely to assume that all stakeholders will engage with the regulation in bad faith, so some degree of harmonization should be achieved, especially since combating disinformation should go against no involved stakeholder's long-range interests. The main factors that might however function as sources of disinformation and manipulation are explicitly addressed in the documents, being politically motivated actors or foreign agents (European Commission, 2022 -a, 59 and 69; European Commission, 2022 -b, 7, 22 and 24). As the DSA and CPD are besides documents that bestow obligations also documents that establish procedures and mechanisms, with the DSA

focusing on more matters than just disinformation, the mentioning of disinformation in the normative section of the DSA largely legitimizes the existence of the specialized CPD, which may thus function as the grounds of attributing accountability to internet intermediaries, especially VLOPs and VLOSEs, which are being actively incentivized to sign up in order to comply with the normative demands of the DSA (European Commission, 2022 -a, 29 and 88). While the CPD is non-binding, the ECM monitors both compliance to the DSA and CPD, and as a consequence of non-compliance the ECM might directly request a company to subscribe to the CPD as being a code of conduct, meaning it does have the capacity of procedurally establishing [a lack of] good faith engagement with EU norms (European Commission, 2022 -a, 94-95). Accountability to the CPD is thus incentivized through the processes of the DSA, meaning that ultimately the ECM may be able to hold internet intermediaries accountable despite the CPDs voluntary nature.

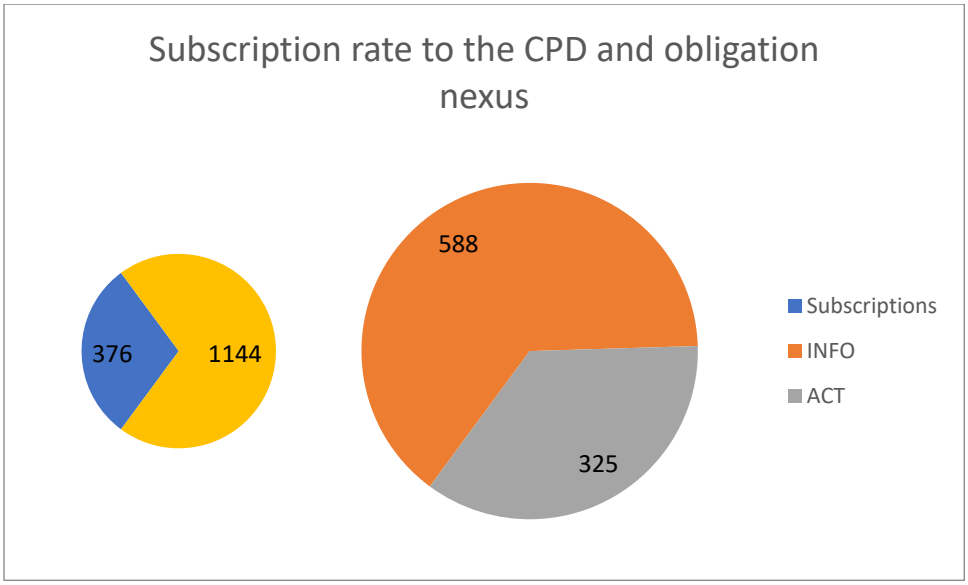
The CPD itself lacks any meaningful enforcement mechanisms, with all of its 44 commitments being on a per-subscription basis, meaning that a company could well sign up to the CPD but still attempt to outmaneuver the commitments by reporting that it has its own equivalents in place and thus is fully complying. Signatories are thus fully free to disregard point [f] of the normative underpinnings of the document, which states that companies should sign up for commitments and measures that are relevant to their services, and if not, report and justify this decision (European Commission, 2022 -b, 2). Twitter's 2023 evaluation report serves as a great case in point, as they have not only rescinded their status as signatory, but their report in early January answers only 7 of the 44 possible commitments despite their status as a VLOP, a categorization they were aware of would be assigned to them well before this actually was done by the ECM, and after months of reducing their compliance (Hennessy, *Appendix 2;* Villasenor, 2023). Furthermore, while compliance is mentioned 9 times throughout the document, it is only in commitment 44 which is specific to VLOPs and VLOSEs, that an obligation concerning compliance is bestowed, in this case being the funding of independent auditors to asses compliance with the DSA, the other eight times actually refer to how the CPD should be followed only where it is in full compliance with other regulations, thus establishing the potential of excusing noncompliance through country of origin issues, a phenomenon that supersedes the CPD or DSA (European Commission, 2022 -b, 40; Husovec and Laguna, 2023, 12).

The DSA, on the other hand, does have an enforcement mechanism that can be activated by several actors. Section 4, ranging from Article 64 to 83, bestows a large number of executive capabilities upon the ECM, and furthermore stipulates that the ECM can be requested to use these at the request of a formal request by the EBDS, member states or Digital Service Coordinators as well as other national authorities on the matter (*Ibid.*; European Commission, 2022 -a, 88-98). Article 74,

functions as the sharp edge of the regulation and is specialized towards VLOPs and VLOSEs, enabling the ECM and EBDS to fine the aforementioned a maximum of 6 percent of their "*worldwide annual turnover in the preceding final year*" when they are found in non-compliance in accordance with Article 76, or up to a maximum of 1 percent of the same when a company refuses to provide information upon request, which is an obligation as per Article 67 (*Ibid.,* 94). It is significant to note here that an internet intermediary that is found at fault can be penalized on a per-infringement basis, meaning that there is virtually no limit to the financial costs a company can incur as a consequence of enforcement (European Union, 2022 -d, 32). It is also this enforcement mechanism, including the competences of the ECM to infringe as well as protections that it bestows upon internet intermediaries that will also function as the backbone of the CPD, given that the DSA and CPD both contain separate clauses for VLOPs and VLOSEs, they both introduce separate obligations in their bodies of text, but since the normative sections of both documents cross reference each other obligations to the CPD in theory also fully fall under the jurisdiction of the enforcement capacities of the DSA. Thus, accountability under the CPD is as accountability under the DSA, with the difference that the enforcement thereof is more likely to be a creeping matter as, as Gregorio and Dunn (2022) determined, the EU generally adheres to "*proportionate balance between risks and costs of regulation*" and possibly giving time for a supportive body of literature to arise from the third-party signatories (De Gregorio and Dunn, 2022, 475).

For the purposes of examining how the CPD is currently functioning, analysis was conducted on the first wave of baseline reports that were published through the Transparency centre of the CPD, and while this is the first iteration, the results were shockingly disparate both in terms of consistency and quality. This has significant implications across the board as it complicates the assessment of the compliance with the CPD as far as the self-reporting template allows, as well as the patterns that may be deduced from the computation of the data contained therein. Despite this, it is not impossible to deduct the current compliance to the CPD. *Figure 8*, given below, shows the total quantity of subscriptions by signatories vis-à-vis the accumulative potential subscriptions, also making a distinction between subscriptions to obligations to inform versus obligations to act.

Figure 8



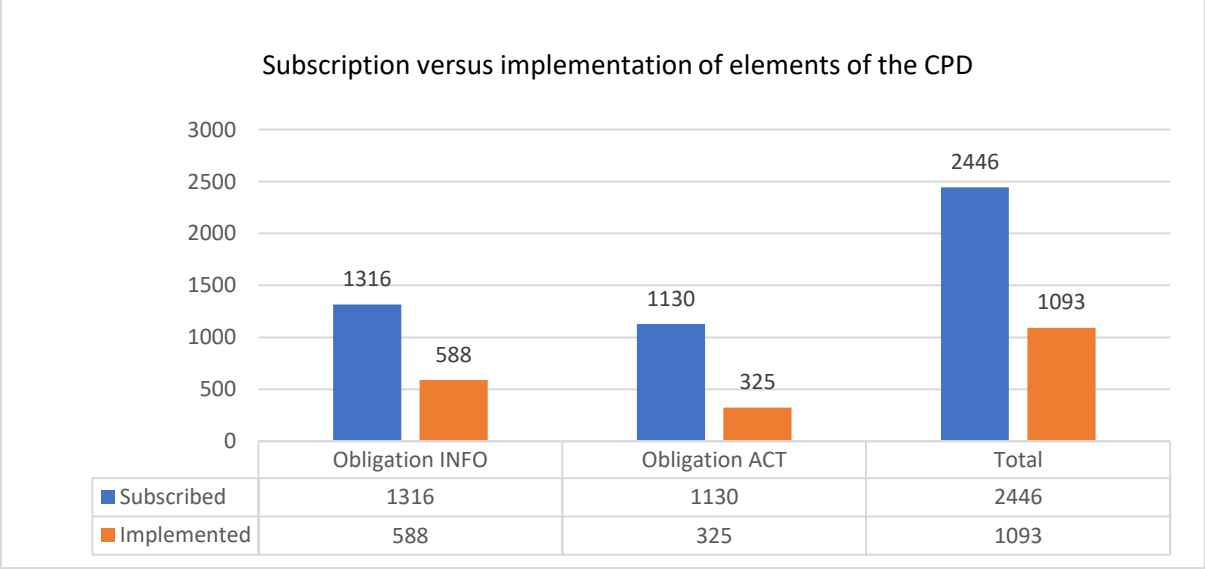
The total amount of possible commitments [yellow] versus the subscriptions thereto on the left, with division of subscribed elements on the right (Hennessy, *Appendix 2*).

Out of 1144 possible commitments, the accumulative signatories of the CPD amounted for only 376 subscriptions to commitments, of which they implemented 588 measures that are obligations to provide information, and 325 are obligations to conduct some sort of action (Hennessy, *Appendix 2*). As dominance of obligations to provide information could logically be expected based upon the signatory profiles as visible in *Figure 1*, the vast majority of the subscriptions made by signatories were to establish information exchange and conduct annual reports as well as cooperate to spread best practices and provide access. Thus, these results are heavily skewed in favor of representation of third-parties, which are themselves relatively diverse. If one were to make a similar graph on the basis of the commitments and subscriptions, as well as compliance, of only the VLOSEs and VLOPs similar issues would arise, with Microsoft, Google and Meta using a single document to discuss subscriptions of three or more of their subsidiaries, gathering information on the actual implementation processes of these companies becomes a quagmire rife with false positives. Intentional noncompliance to the reporting standards such as in the case of Twitter only reinforces the messiness of the data that is produced by the CPD reporting mechanism (Hennessy, Appendix 2; Twitter, 2023). Twitter, in this case, reported on their initiatives within the first two pages of the template which give space for an executive summary, with the rest of the document serving for in-depth elaboration, which they refused to give, referring to what had already been said in the summary (*Ibid.*). *Figure 8* is corrected for false positives in terms of

commitments, as visible in *Appendix 2*, determining the number of commitments that were truthfully subscribed and implemented to in cases the form has been misapplied.

As such, the current quality of information attainable through the transparency centre that was establishes specifically for that reason is dubious at best, with the quality of content varying wildly amongst stakeholders, as one signatory simply reporting that they have not been approached for cooperation in bigger initiatives and other signatories not even removing the placeholder text, some even removing page numbers (Vimeo, 2023, 6-7; The Bright App, 2023, e.g. 4; DoubleVerify, 2023). These discrepancies are indicative of an essential element of the CPD, and through it the DSA, not yet functioning as intended, and might be a consequence of the coming-in-effect of both, or it might serve as a preliminary indicator that despite the richness in obligations to provide information, will or clarity is lacking, or the obligations to adequately document and inform are not taken serious enough. The lackluster quality of the reports seems to strengthen the concerns that arose when the CPD18 was still in-effect, with Shattock (2021) stating that after 2 years of the CPD the ECM commended the work of third-parties, while critiquing the actions of the platforms in actually implementing their commitments and obligations (Shattock, 2021, 2). *Figure 9* consists of a single graph, showing three comparisons: subscription versus implementation of obligations to provide information, the same for obligations to act and finally the total difference in subscription to implementation rates.

Figure 9



While subscription rates to both are similar, there is a tangible difference in the reported actions that have been conducted to materialize signatories' obligation to undertake action, resulting in an implementation rate of less than 50% (Hennessy, *Appendix 2*).

Notwithstanding the shortcomings of the template or how it is filled in by the signatories, the data that can be derived from it also does not shine a great light upon the current state of affairs concerning the CPD's implementation. While responsibility to act on disinformation, both ex post and ex ante, is delegated towards the signatories, less than half of the accumulative obligations to provide information have materialized and for responsibilities this reaches a low of almost one third. So far, this subchapter has examined how the DSA and CPD are constructed to cooperate and have been given more leeway to remain functional, yet the CPD in particular is hampered by procedural issues and stagnation of initiative on behalf of its signatories, which is ironic given that it is established exactly to create continuous and predictable procedures concerning dealing with disinformation. The data in *Figure 8* and *Figure 9* furthermore show that options to choose are in some manner resulting in a lot of decisions being made for information provision, which is in no doubt explained in part due to signatory composition, but can also be indicative of a lack of leadership being taken amongst signatories when it comes to spearheading the obligations to act. More worryingly perhaps, the possibility of low implementations here can be due to pre-existing similar initiatives by the VLOPs or VLOSEs, who see no need to wholesale replace their own established initiatives with new constructs derived from the CPD, with Twitter being yet another case in point here (Twitter, 2023).

Having discussed the difficulties of the CPD gaining traction, it thus becomes clear that while the DSA and CPD offer a remarkably flexible and sturdy network that allows increasingly effective dealings with disinformation, akin to case law, the first wave of baseline reports seems to be a major disappointment. The capacity of the ECM to enforce under the DSA has already been discussed, and will officially come into effect on February 17th, 2024, meaning that is within possibility that the ECM will immediately pull in the reins on the internet giants that it accosted of being too complacent in their implementation (Shattock, 2021, 2). Nonetheless the CPD with the DSA as a backdrop establishes a basis for harmonization of enforcement amongst member-states and private enterprises alike, allowing it to avoid the predictions of Bendiek (2021) that any degree of subsidiarity to domestic law might cause enforcement differences (Bendiek, 2021, 11). The CPD will function unpredictably at first, but should stabilize as the proportionality of actions becomes more clear, and it also incentivizes internet intermediaries to make similar changes to their terms of service, meaning that issues might get streamlined before reaching domestic courts in the first place.

For now, it can in large lines be concluded that Shattock's (2021) observation still retains some truth, and the EU seems to have made little progress when it comes to incentivizing digital giants to pick up the "*speed and scope*" of the implementation, let alone the prescribed definitions of the CPD allowing opt-outs until the enforcing effect of the DSA comes into effect. Before exiting the

CPD, in January of 2023 Twitter even rolled-back its ban on political and issue-based advertisements (Piper, 2023). The success of the CPD cannot be assessed, but its failure to operate without a clear enforcement mechanism as such can be determined pretty obviously. Nonetheless, once the CPD becomes an official supplement to the DSA the extensive procedural structure of the document might prove of more effect, and may as a consequence allow the intent of the EDAP to proactively combat disinformation to gain more traction. After all, the DSA and CPD are also concerned with creating a new infrastructure for researchers and policy makers alike to access data that can clearly allude to the presence, spread and origin of disinformation.

Yet, simply due to the structuring of the DSA and CPD and how they are meant to integrate seamlessly into EU and domestic law, the subtle optimism Shattock (2021) on the direction of EU regulation on disinformation has to be shared: the CPD in its current shape is not the panacea to disinformation, but it most definitely sets the stage to address it. The CPD is wholly non-binding, but takes on a more stringent character for the big digital players from the moment the DSA comes into full effect, at which point the DSCs and EBDS as well as ECM and national authorities receive support in enforcing compliance from the EU level. In the private sphere, non-VLOPs and VLOSEs are empower through being provided access to reports on combating disinformation, which should allow them to copy best practices, as well as contribute to the material in case they belong to a relevant third-party. For end-users, additional protections are bestowed which implicitly reduces susceptibility to information-based manipulation. Final accountability thus still lies with the decisions of the ECM as finding an internet intermediary in non-compliance, but the capacity and ability of combating disinformation is divided between the private sphere and the public sphere via the CPD.

4.4 Conclusion

In the previous three subchapters the three research questions have been answered at length. For sub-question 1, on the integration or disintegration caused by the DSA and CPD, it was found that most targeted VLOPs and VLOSEs willfully subjected themselves to the CPD in preparation of its officiation. While the DSA functions as a legal backstop, the CPD functions as a harmonizing self-regulation tool that also serves as the vanguard of a database for information provision, enjoying a relatively high degree of harmonization despite being in its fledgling stages. The second sub-question on the conceptualization shows that the conceptualization is ‘open’ enough to allow addressing various issues that are deemed suspect to either the enforcer or the ECM. Here information provision is extensive as well, indicating that if the operationalization is not successful unto itself, the ECM might be able to refine it more explicitly at the hand of identified problem areas. For sub-question 3, the results are less positive, indicating a massive discrepancy between subscription and implementation rates, indicating both reporting issues and continued lagging in implementation.

5. Conclusion

The analysis has systematically sketched a picture of how the EU and its member states might utilize the Digital Services Act and Code of Practice on Disinformation to combat the proliferation of disinformation as intended under the European Democracy Action Plan. Most importantly, it is found that the DSA predominantly functions as a legislative backdrop establishing protocols and delegating both limitations and competences without in itself explicitly enabling actors to undertake actions against disinformation. The latter competence is instead subject to the ECM's capacity to request and advise actors, in this case internet intermediaries, to enroll in voluntary 'codes of conduct', which are legitimized by the DSA as being initiatives that serve as proof of good will to compliance with the legislation of the DSA and other EU initiatives such as the TEU and TFEU, simultaneously functioning as a system that allows the ECM to identify companies that have ulterior motives. This is non-binding, and "optional" at the behest of the ECM at this point of the legislation, and as such it seems the DSA and CPD are approached carefully and in a non-sweeping, tentative manner.

The organization and interactions of the DSA and CPD allow platforms, member states and in the worst-case the ECM itself to undertake actions against the proliferation of disinformation and establishes precedent for further interaction within the digital sphere; it acknowledges in the importance of regulating digital platforms (Bakir and McStay, 2018; Bendiek, 2021; Huq, 2022) and the harmonization thereof (Vollaard, 2014; Schimmelfennig, 2018), it identifies potentially harmful algorithms and machine developments (Woolley and Howard, 2018; Saurwein and Spencer-Smith, 2020), it addresses the source of what might take advantage of digital infrastructure (*Idem.;* Sullivan, 2019), it introduces *ex ante* responsibilities (Huq, 2022; De Gregorio and Dunn, 2022); simultaneously it also prevents potential issues such as copyright (Fallas, 2009) through proportional horizontal integration with other EU regulations, it prevents the risk of loss of access as identified by Woolley and Howard (2016) by promoting machine-readability throughout the CPD and DSA consistently, and it prioritizes liberal freedoms over unrestricted open speech which confirms what Zurth (2021) has found within other EU regulatory initiatives.

On the other hand, the findings also tentatively show that the risk of continued polarization (Schelder, 2021), ultimately leading to negative effects for democracy, for as far as these are influenced by the free proliferation of unhealthy information within the biggest digital platforms that operate within the EU, can now be legitimately and consistently tackled across platforms. The issue therein naturally does not disappear overnight; however, the EU has in the DSA and CPD established a toolkit that allows progressively exerting financial pressures, or in worst-case limiting service, of actors that are shown to not comply in good faith with the dimension of European values that are actively scorned

through the spread of disinformation. Still, it remains impossible to draw stronger conclusions hereon given the relatively little information on the functioning of the strengthened CPD which is available, with the available reports wildly varying in quality and value. Nonetheless, the way the regulation and code of conduct interact implies a degree of future-proofing, in that the relatively new definition of "*malinformation"* by Derakshan (2017), as well as sensationalist news as coined by Pennycook and Rand (2021) both fall within the conceptualization of disinformation of the CPD and DSA, meaning that action can, and possibly one day must, be undertaken against slightly manipulated information in the future as well; this is also true for the push for harmonization of "terms of use", which falls outside of the scope of this thesis but nonetheless follows the same principle.

The DSA and CPD as such, in their current forms are not a panacea to the pervasive issues of manipulated information within the EU, but they do set the tone for expansion of the EU institutions' capacity to engage and limit the reach thereof, which in turn has implications for all of the post 2010 literature mentioned in the theory chapter; most significantly, the EU does away with "digital switzerlands" (Huq, 2022; Zurth, 2021) and establishes law in a new domain that far supersedes geographic bounds, officiating a digital version of the *Brussels Effect*. Of course, all is well in theory, but practice has yet to show, and future scholars might choose to delve into whether *Malinformation* is actually tackled in practice; whether member states do not consider the open conceptualization of disinformation stringent enough and still opt to launch their own legislation; whether self-regulation, even as legitimized by the DSA, under codes of conduct actually works; the inevitable political discourse these regulations are subject to. The DSA and CPD seem to have incorporated many academic qualms and advices, and the true question remains which aspects of their approach will actually perform well. Further research into tangible enforcement is warranted.

The open character of the CPD, being the sharp edge of the DSA's attempt to at least bring the big platform in line suffers from the same issues that the open conceptualization of disinformation does. If *ex ante* obligations are introduced but the conceptualization remains too open, or too few explicit circumstances are mentioned, then perhaps the CPD is reduced to merely a somewhat narrower backstop which complements the DSA. Monitoring of compliance seems to heavily rely on compliance officers, which are onboarded by companies and domestic DSCs. It would most likely do the EDAP initiative to combat disinformation well if at least the DSCs, possibly also the compliance officers, had direct obligations towards EU institutions. If the 5-year revision periods of the DSA are not prioritized, the openness of the pressure points of the CPD under the DSA, may well exactly result in Dougan's (2000) "*Minimum Harmonization*" and in effect not differ much from "*verifiably false*".

Appendix 1

Here the quantified and computed results of the analysis over the DSA and CPD are visible. Please note that the actors that belong to the code PERS have been elaborated upon further, to identify how often an obligation or act or inform, was specifically bestowed upon specifically named actors. For readability a legend has been added.

	INFO		ACT		NO		BI		PERS			
Normative or Regulation	N	R	N	R	N	R	N	R	ECM	98	MS	23
DSA	142	112	167	116	76	66	96	77	VLOPs	36	EC	1
CPD	136	134	127	110	3	1	45	46	VLOSEs	36	EP	1
Total	278	**246**	294	**226**	79	**67**	141	**123**	OPs	18	Cs	6
	CR		CR(g)		Conferral		Prejudice		IMs	22	DSCs	33
Document or Regulation	N	R	N	R	N	R	N	R	IMSs	24	As	7
DSA	93	31	22	11	10	4	45	13	HIMs	12	CJEU	2
CPD	9	3	19	11	0	0	1	1	EBDS	12	LRPs	1
Total	102	**34**	41	**22**	10	**4**	47	**2**	Total mentions			332

Legend					
ECM	European Commission	HIMs	Internet Intermediaries [host]	DSCs	Digital Service Coordinators
VLOPs	Very Large Online Platforms	EBDS	European Board of Digital Services	As	Auditors
VLOSEs	Very Large Online Search Engines	MS	Member-States	CJEU	Court of Justice of the European Union
OPs	Online Platforms	EC	European Council	LRPs	Legal Representatives
Ims	Internet Intermediaries	EP	European Parliament		
IMSs	Internet Intermediaries [marketplace]	Cs	End-Users		

Appendix 2

Here the quantified and computed results of the analysis over the reports of the CPD are visible. Please note that in the cases that seemed unrealistic, such as 100% commitments or compliance rates, extra calculations have been ran to discern more plausible rates as these original rates likely are due to shortcomings of the reporting templates, utilized coding scheme or cherry-picking on behalf of the stakeholder that wrote the report.

	INFO	**ACT**	**Commitments**
	Filled-in/Empty [vs. ACT]	Filled-in/Empty [vs. INFO]	Relative to total [44]
[3][2]	13/13 [26] – 25%/25% [50%]	2/24 [26] – 3.85%/46.15% [50%]	11 [25%]
[4][2]	6/1 [7] – 37.5%/6.25% [43.75%]	0/9 [9] – 0%/56.25% [56.25%]	4 [9.09%]
[5][2]	8/0 [8] – 53.33%/0% [53.33%]	5/2 [7] – 33.33%/13.33% [46.67%]	2 [4.55%]
[6][2]	13/0 [13] – 48.15/0% [48.15%]	14/0 – 51.85%/0% [51.85%]	11 [25%]
[7][2]	6/125 [131] – 2.53%/52.74% [55.27%]	5/101 [106] – 2.11%/42.62% [44.7%]	44 [2] [100%] [4.55%]
[8][2]	8/16 [24] – 15.28%/30.77%]46.15%]	7/21 [28] – 13.46%/40.38% [53.85%]	13 [29.54%]
[9][2]	1/0 [1] – 7.14%/0% [7.14%]	13/0 [13] – 92.86%/0% [92.86%]	10 [22.73%]
[10][1]	110/0 [110] – 54.73%/0% [54.73%]	91/0 [91] – 45.27%/0% [45.27%]	39 [88.64%0]
[11][2]	6/6 [12] – 21.43%/21.43% [42.86%]	0/16 [16] – 0%/57.14% [47.14%]	16 [36.36%]
[12][2]	16/12 [28] – 28.57%/21.43% [50%]	0/28 [28] – 0%/50% [50%]	15 [34.09%]
[13][2]	4/10 [14] – 17.39%/43.48% [60.87%]	0/9 [9] – 0%/39.13% [39.13%]	10 [22.73%]
[14][2]	33/7 [40] – 46.48%/9.86% [56.34%]	3/28 [31] – 4.23%/39.44% [43.67%]	13 [29.55%]
[15][1]	104/0 [104] – 54.74%/0% [54.74%]	86/0 [86] – 45.26%/0% [45.26%]	41 [93.18%]

[3] Adobe
[4] Avaaz
[5] Crisp
[6] Demagog
[7] DoubleVerify
[8] Faktograf
[9] Globsec
[10] Google
[11] IAB Europe
[12] Logically
[13] Maldita-es
[14] MediaMath
[15] Meta

[16][1]	94/0 [94] – 53.11%/0% [53.11%]	83/0 [83] – 46.89%/0% [46.89%]	33 [75%]
[17][2]	15/0 [15] – 71.43%/0% [71.43%]	6/0 [6] – 28.57%/0% [28.57%]	9 [20.45%]
[18][2]	45/0 [45] – 52.33%/0% [52.33%]	41/0 [41] – 47.67%/0% [47.67%]	20 [45.45%]
[19][2]	3/124 [127] – 1.28%/52.99% [54.27%]	0/104 [104] – 0%/44.44% [44.44%]	44 [3] [100%] [6.82%]
[20][2]	4/8 [12] – 15.38%/30.77% [46.15%]	0/14 [14] – 0%/53.85% [53.85]	10 [22.73%]
[21][2]	10/10 [20] – 23.81%/23.81% [47.62%]	1/21 [22] – 2.38%/50% [52.38%[	13 [29.55%]
[22][2]	5/125 [130] – 2.11%/52.74% [54.85%]	5/102 [107] – 2.11%/43.04% [45.15%]	44 [2] [100%] [4.55%]
[23][1]	71/14 [85] – 42.51%/8.38% [50.90%]	3/79 [82] – 1.8%/47.31% [49.1%]	31 [70.45%]
[24][6]	27/8 [35] – 37.5%/11.11% [48.61%]	6/31 [37] – 8.33%/43.06% [51.39%]	19 [43.18%]
[25][1]	5/129 [134] – 2.04%/52.65 [54.69%]	2/109 [111] – 0.82%/44.49% [45.31%]	44 [7] [100%] [15.91%]
[26][2]	9/9 [18] – 25%/25% [50%]	11/7 [18] – 30.56%/19.44 [50%]	11 [25%]
[27][6]	32/2 [34] – 45.71%/2.86% [48.57%]	26/10 [36] – 37.14%/14.29% [51.43%]	18 [40.91%]
[28][2]	34/15 [49] – 36.17%/15.96% [52.15%]]	1/44 [45] – 1.06%/46.81% [47.87%]	24 [54.55%]

Glossary:

[1] VLOPs and VLOPS [2] TP: FC/MF/SSP/R-TTs [3] Online Platforms

[4] Internet Intermediaries [general] [5] Internet Intermediaries [host] [6] Internet Intermediaries [reseller]

[16] Microsoft
[17] NewsGuard
[18] NewsBack
[19] PagellaPolitica
[20] RSF
[21] ScienceFeedback
[22] The Bright App
[23] TikTok
[24] Twitch
[25] Twitter
[26] VOST Europe
[27] Vimeo
[28] Who Targets Me

Adobe, in its self-ascribed CPD obligations:	15/52	28.85% in-effect; 71.15% pending
Avaaz, in its self-ascribed CPD obligations:	6/16	37.50% in-effect; 62.50% pending
Crisp, in its self-ascribed CPD obligations:	13/15	86.67% in-effect; 13.33% pending
Demagog, in its self-ascribed CPD obligations:	27/27	100% in-effect; 0% pending
DoubleVerify, in its self-ascribed CPD obligations:	11/237	4.64% in-effect; 95.36% pending
Faktograf, in its self-ascribed CPD obligations:	15/37	28.85% in-effect; 71.15% pending
Globsec, in its self-ascribed CPD obligations:	14/14	100% in-effect; 0% pending
Google, in its self-ascribed CPD obligations:	201/201	100% in-effect; 0% pending
IAB Europe, in its self-ascribed CPD obligations:	6/28	21.43% in-effect; 78.57% pending
Logically, in its self-ascribed CPD obligations:	16/56	28.57% in-effect; 71.43% pending
Maldita-es, in its self-ascribed CPD obligations:	4/23	17.39% in-effect; 83.61% pending
MediaMath, in its self-ascribed CPD obligations:	36/71	50.7% in-effect; 49.3% pending
Meta, in its self-ascribed CPD obligations:	190/190	100% in-effect; 0% pending
Microsoft, in its self-ascribed CPD obligations:	177/177	100% in-effect; 0% pending
NewsGuard, in its self-ascribed CPD obligations:	21/21	100% in-effect; 0% pending
NewsBack, in its self-ascribed CPD obligations:	86/86	100% in-effect; 0% pending
PagellaPolitica, in its self-ascribed CPD obligations:	3/237	1.27% in-effect; 98.73% pending
RSF, in its self-ascribed CPD obligations:	4/26	15.38% in-effect; 84.62% pending
ScienceFeedback, in its self-ascribed CPD obligations:	11/42	26.19% in-effect; 73.81% pendings
The Bright App, in its self-ascribed CPD obligations:	10/237	4.22% in-effect; 95.78% pending
TikTok, in its self-ascribed CPD obligations:	74/167	44.31%% in-effect; 55.69% pending
Twitch, in its self-ascribed CPD obligations:	33/72	45.83% in-effect; 54.17% pending
Twitter, in its self-ascribed CPD obligations:	7/245	2.78% in-effect; 97.22% pending
VOST Europe, in its self-ascribed CPD obligations:	18/36	50% in-effect; 50% pending
Vimeo, in its self-ascribed CPD obligations:	58/70	82.86% in-effect; 17.14% pending
Who Targets Me, in its self-ascribed CPD obligations:	35/94	37.23% in-effect; 62.77% pending

Bibliography

Albert, R. (2017). "Four Unconstitutional Constitutions and their Democratic Foundations." *Cornell International Law Journal* 50(2), 169-198. Doi: 10.31228/osf.io/v9tz4

Bánkuti, M., Halmai, G. and Scheppele, K. (2015). *Hungary's Illiberal Turn: Disabling the Constitution.* In Krasztev, P. and Van Til, J. (2015). *The Hungarian Patient*. Budapest: Central European University Press. https://www.researchgate.net/publication/290454553_The_hungarian_patient_Social_opposition_to_an_illiberal_democracy

Bendiek, A. (2021). "*The Impact of the Digital Service Act (DSA) and Digital Markets Act (DMA) on European Integration Policy*." Working Paper. Accessed May 12th, 2023, via https://www.swp-berlin.org/publications/products/arbeitspapiere/WP0121_Bendiek_Digital_Service_Act_and_Digital_Markets_Act.pdf

Berg, B. (2004). *Qualitative research methods for the social sciences* (8). Boston: Pearson. Published November 2011. Accessed June 7th, 2023, via http://law.gtu.ge/wp-content/uploads/2017/02/Berg-B.-Lune-H.-2012.-Qualitative-Research-Methods-for-the-Social-Sciences.pdf

Boffey, D. (2020). "*EU faces crisis as Hungary and Poland veto seven-year budget."* The Guardian. Published November 16th, 2020. Accessed June 3rd, 2023, via https://www.theguardian.com/world/2020/nov/16/eu-hungary-veto-budget-viktor-orban

Bozóki, A. (2015). "Broken Democracy, Predatory State, and Nationalist Populism." *Hungary's Illiberal Turn: Disabling the Constitution.* In Krasztev, P. and Van Til, J. (2015). *The Hungarian Patient*. Budapest: Central European University Press. https://www.researchgate.net/publication/290454553_The_hungarian_patient_Social_opposition_to_an_illiberal_democracy

Broersma, M. (2023). *"Twitter Quits EU Code Of Practice On Disinformation."* Silicon, technology powering business. Accessed May 31st, 2023, via https://www.silicon.co.uk/e-marketing/socialmedia/twitter-eu-code-514018

Czempiel, E. and Rosenau, J. (1992). *Governance Without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press. Doi: 10.1017/CBO9780511521775.003

Daly, T. (2019). "*Democratic Decay: Conceptualizing an Emerging Research Field*." Hague J Rule Law 11(1), 9-36. Doi: 10.1007/s40803-019-00086-2

De Gregorio, G. and Dunn, P. (2022). "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age." *Common Market Law Review* 59(2), 473-500. Doi: 10.2139/ssrn.4071437

Dougan, M. (2000). "Minimum Harmonization and the Internal Market." *Common Market Law Review* 37(1), 853-885. Doi: 10.54648/272669

Ginsberg, T. (2021). "*Democracies and International Law*." Cambridge: Cambridge University Press. Doi: 10.1017/9781108914871

Gorwa, R., Binns, R. and Katzenbach, C. (2020). "Algorithmic content moderation: Technical and political challenges in the automation of platform governance." *Big Data & Society* 7(1), 1-15. 10.1177/2053951719897945

Guess, A. and Lyons, B. (2020). *Misinformation, Disinformation and Online Propaganda*. In Persily, N. and Tucker, J. (2020). *Social Media and Democracy*. New York: Cambridge University Press. ISBN 9781108890960

Haas, E. (1958). "*The Uniting of Europe*." Indiana: University of Notre Dame Press. ISBN 0-268-04346-9

Herre, B. (2021). "The 'Regimes of the World' data: how do researchers measure democracy?" *Our World in Data*. Published December 2nd, 2021. Accessed June 11th, 2023, via https://ourworldindata.org/regimes-of-the-world-data

Howard, P. and Parks, M. (2012). "Social Media and Political Change: Capacity, Constraint, and Consequence." *Journal of Communication* 62(2), 359-362. Doi: 10.1111/j.1460-2466.2012.01626.x

Huntington, S. (1991). "Democracy's Third Wave." *Journal of Democracy* 2(2), 12-34. https://www.ned.org/docs/Samuel-P-Huntington-Democracy-Third-Wave.pdf

Huq, A. (2022). "International Institutions and Platform-Mediated Misinformation." *Chicago Journal of International Law* 23(1), 116-129. https://chicagounbound.uchicago.edu/cjil/vol23/iss1/8/

Husovec, M. and Laguna, I. (2023). "Digital Services Act: A Short Primer." 1-13. in Husovec, M. and Laguna, I. (Forthcoming, 2023). *Principles of the Digital Services Act*. Oxford: Oxford University Press. Accessed May 30th, 2023, via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4153796

Jowett, G. and O'Donnell, V. (2005). *Readings in Propaganda and Persuasion: New and Classic Essays*. New York: Sage Publications. ISBN 1412909007

Levine, D. (2002). "The Decline and Fall of Democracy in Venezuela: Ten Theses." *Bulletin of Latin American Research* 21(2), 248-269. Doi: 10.1111/1470-9856.00042

Levitsky, S. and Ziblatt, D. (2018). *How Democracies Die*. New York: Crown Publishing Group. ISBN 1524762938

Linz, J. (1990). "The Perils of Presidentialism." *Journal of Democracy* 1(1), 51-69. https://muse.jhu.edu/article/225694/pdf

Mayring, P. (2014). *Qualitative content analysis: theoretical foundation, basic procedures and software solution.* Social Science Open Access Repository. Published 2014. Accessed June 29th, 2023, via https://www.ssoar.info/ssoar/bitstream/handle/document/39517/ssoar-2014-mayring-Qualitative_content_analysis_theoretical_foundation.pdf

Mayring, P. (2019). "Qualitative Content Analysis: Demarcation, Varieties, Developments." *Forum: Qualitative Social Research* 20(3), 1-14. Doi: 10.17169/fqs-20.3.3343

Mayring, P. (2020). *Qualitative Content Analysis: Demarcation, Varieties, Developments*. Forum Qualitative Sozialforschung 20(3), Art. 16. Published September 2019. Accessed June 1st 2023, via http://dx.doi.org/10.17169/fqs-20.3.3343.

Miles, M. and Huberman, A. (1994). "*Qualitative Data Analysis.*" Newbury Park: Sage Publishing. ISBN 9780803955400

Mills, A., Durepos, G. and Wiebe, E. (2010). *Encyclopedia of Case Study Research, Volumes I and II.* California: Sage Publishing. ISBN 9781506320274.

Moravcsik, A. (2018). "Preferences, Power and Institutions in 21st-century Europe." *Journal of Common Market Studies* 56(7), 1648-1674. Doi: 10.1111/jcms.12804

Murphy, D., Powell, A., Tinati, R., Anstead, N., Carr, L., Halford, S. and Weal, M. (2016). "Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital." *International Journal of Communication* 10(1), 4952-4971. Doi: 1932–8036/20160005

N.d. (1950). "*European Convention on Human Rights."* Council of Europe. Published November 1950. Accessed June 1st, 2023, via https://www.echr.coe.int/documents/convention_eng.pdf

N.d. (1950). "*The Schuman Declaration*" European Commission. Published May 9th, 1950. Accessed April 24th, 2023, via https://op.europa.eu/en/publication-detail/-/publication/2fa0afe0-9f7c-426d-9933-fca909c50983

N.d. (1997). "Treaty of Amsterdam amending the Treaty on European Union, the treaties establishing the European Community and certain related acts." *Official Journal of the European Union* C340, 1-144. Published November 10th, 1997. Accessed May 13th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:11997D/TXT

N.d. (2012 -a). "The treaty on European Union." *Official Journal of the European Union* C326, 13-45. Published October 26th, 2012. Accessed Jun 1st, 2023, via https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

N.d. (2012 -b) "Treaty on the Functioning of the European Union." *Official Journal of the European Union* C326, 47-390. Published October 10th, 2012. Accessed April 10th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

N.d. (2012 -c) "Charter of Fundamental Rights of the European Union." *Official Journal of the European Union* C326, 391-407. Published October 26th, 2012. Accessed Jun 30th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

N.d. (2018). "Democracy continues its disturbing retreat." *The Economist*. Published January 31st, 2018. Accessed May 31st, 2023, via https://www.economist.com/graphic-detail/2018/01/31/democracy-continues-its-disturbing-retreat

N.d. (2018). "EU Code of Practice on Disinformation." *European Commission*. Accessed April 24th, 2023, via https://ec.europa.eu/newsroom/dae/redirection/document/87534

N.d. (2020 -a). "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan." *Document 52020DC0790*. Published December 3rd, 2020. Accessed May 21st, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:790:FIN

N.d. (2020 -b). "*European Democracy Action Plan*". European Commission. Published December 2020. Accessed June 19th, 2023, via https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

N.d. (2020 -d). “Regulation EU 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)”. *Official Journal of the European Union* L 277, 1-102. Published October 27th, 2022. Accessed April 29th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

N.d. (2020). *EU action plan against disinformation*. European Court of Auditors. Published March 2020. Accessed May 29th, 2023, via https://www.eca.europa.eu/Lists/ECADocuments/AP20_04/AP_Disinformation_EN.pdf

N.d. (2022 -a). *The Strengthened Code of Practice on Disinformation 2022*. European Commission. Published June 16th, 2022. Accessed March 9th, 2023, via https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

N.d. (2022 -b) “Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).” *Official Journal of the European Union* L277, 1-102. Published October 27th, 2022. Accessed April 8th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

N.d. (2022 -c) “Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).” *Official Journal of the European Union* L265, 1-66. Published October 12th, 2022. Accessed April 15th, 2023, via https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

N.d. (2022). “*Implementing ECHR judgments: Latest decisions from the Committee of Ministers*.” Council of Europe. Published September 22nd, 2022. Accessed April 29th, 2023, via https://www.coe.int/en/web/portal/-/implementing-echr-judgments-latest-decisions- from-the-committee-of-ministe-4

N.d. (2023 -a). “*Signatories of the Code of Practice on Disinformation deliver their first baseline reports in the Transparency Centre.*” European Commission. Published February 9th, 2023. Accessed June 24th, 2023, via https://digital-strategy.ec.europa.eu/en/news/signatories-code-practice-disinformation-deliver-their-first-baseline-reports-transparency-centre

N.d. (2023 -b). “*Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*.” European Commission. Published April 25th, 2023. Accessed June 27th, 2023, via https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

N.d. (2023 -c). "*The Single Market Scoreboard*." European Commission. Published 2023. Accessed Jun 11th, 2023, via https://single-market-scoreboard.ec.europa.eu/

N.d. (2023). *"Code of Practice on Disinformation – Report of Twitter for the period H2 2022".* Twitter. Published January 2023. Accessed June 26th, 2023, via https://disinfocode.eu/reports-archive/?years=2023

N.d. (2023). *"Code of Practice on Disinformation – Report of Twitter for the period H2 2022".* Vimeo. Published January 2023. Accessed June 26th, 2023, via https://disinfocode.eu/reports-archive/?years=2023

N.d. (2023). *"Code of Practice on Disinformation – Report of Twitter for the period H2 2022".* Tiktok. Published January 2023. Accessed June 26th, 2023, via https://disinfocode.eu/reports-archive/?years=2023

N.d. (2023). "*Democracy index 2022: Frontline democracy and the battle for Ukrain*e." The Economist. Published February 7th, 2023. Accessed May 18th, 2023, via https://pages.eiu.com/rs/753-RIQ-438/images/DI-final-version-report.pdf

Neuendorf, K. (2002). *The Content Analysis Guidebook.* London: Sage Publications. https://www.daneshnamehicsa.ir/userfiles/files/1/9-%20The%20Content%20Analysis%20Guidebook.pdf

Ophir, Y. and Jamieson, K. (2021). "The effects of media narratives about failures and discoveries in science on beliefs about and support for science." *Public Understand of Science* 30(8), 1-16. Doi: 10.1177/09636625211012630

Pappas, T. (2016). *Populism and Liberal Democracy*. Oxford: Oxford University Press. ISBN 978–0–19–883788–6

Pellegrino, M. and Stang, G. (2016). "*Space Security for Europe*." EU Institute for Security Studies, 29(1), 5-99. https://aerospace.org/sites/default/files/policy_archives/Space%20Security%20for%20Europe%20Jul16.pdf

Pennycook, G. and Rand, D. (2021). "The Psychology of Fake News." *Trends in Cognitive Sciences* 25(5), 388-402. Doi: 10.1016/j.tics.2021.02.007

Piper, J. (2023). "*Elon Musk reopened Twitter for political ad business. But is it too late?"* Politico. Published March 3rd, 2023. Accessed June 23rd, 2023, via https://www.politico.com/news/2023/03/03/elon-musk-twitter-political-ad-business-00085183

Plattner, M. (2019). “Illiberal Democracy and the Struggle on the Right.” *Journal of Democracy* 30(1), 5-19. Doi: 10.1353/jod.2019.0000

Rawls, J. (1972). “*A Theory of Justice: Original Edition*.” New York: Harvard University Press. Doi: 10.2307/j.ctvjf9z6v

Sartor, G. (2013). “Providers’ liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms?” *International Data Privacy Law* 3(1), 3-12. Doi: 10.1093/idpl/ips0200234

Saurwein, F. and Spencer-Smith, C. (2020). “Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe.” *Digital Journalism* 8(6), 820-841. Doi: 10.1080/21670811.2020.1765401

Savin, A. (2019). “Rule Making in the Digital Economy: Overcoming Functional Equivalence as a Regulatory Principle in the EU.” *Journal of Internet Law* 22(8), 1-31. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3340886

Schelder, A. (2010). “Authoritarianism’s Last Line of Defense.” *Journal of Democracy* 21(1), 69-80. Doi: 10.1353/jod.0.0137

Schelder, A. (2021). “Democratic Reciprocity.” *The Journal of Political Philosophy* 29(2), 252-278. Doi: 10.1111/jopp.12232

Scheppele, K. (2018). “Autocratic Legalism.” *The University of Chicago Law Review* 85(2), 545-584. Doi: 10.2307/26455917

Schimmelfennig, F. (2018). “Brexit: differentiated disintegration in the European Union.” *Journal of European Public Policy* 25(8), 1154-1173. Doi: 10.1080/13501763.2018.1467954

Shattock, E. (2021). “Self-regulation 2:0? A critical reflection of the European fight against disinformation.” *Harvard Kennedy School Misinformation Review* 2(3), 1-8. Doi: 10.37016/mr-2020-73

Stake, R. (1995). *The art of case study research*. California: Sage Publishing. ISBN 080395767X.

Sullivan, J. (2019). “Reviewed Work(s): Computational Propaganda: Political Parties, Politicians and Political Manipulation on Social Media by Samuel C. Wooley and Philip N. Howard.” *St Antony’s International Review* 15(1), 213-217. https://www.jstor.org/stable/10.2307/27027766

Villasenor, J. (2023). *"Twitter, the EU, and self-regulation of disinformation."* Brookings Institute. Published January 18th, 2023. Accessed June 28th, 2023, via https://www.brookings.edu/articles/twitter-the-eu-and-self-regulation-of-disinformation/

Vollaard, H. (2014). "Explaining European Disintegration." *Journal of Common Market Studies* 52(5), 1142-1159. Doi: 10.1111/jcms.12132

Wardle, C. and Derakshan, H. (2017). "I*nformation Disorder: Toward an interdisciplinary framework for research and policy making*." Council of Europe. Published September 27th, 2017. Accessed May 30th, 2023, via https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

Woolley, S. and Howard, P. (2016). "Political Communication, Computational Propaganda, and Autonomous Agents." *International Journal of Communication* 10(1), 4882-4890. https://par.nsf.gov/servlets/purl/10021331

Woolley, S. and Howard, P. (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press. Doi: 10.1093/oso/9780190931407.001.0001

Zurth, P. (2021). "The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability." *Fordham Intellectual Property, Media and Entertainment Law Journal* 31(4), 1084-1153. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1782&context=iplj