Comments by the International Commission of Jurists

on the

proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC

A Briefing Paper

1. Introduction

The Digital Services Act aims to harmonise rules on online intermediary services providers, in particular in relation to their substantive and procedural obligations when acting as intermediaries in the provision of services online, including, among other things, communication networks, social media or cloud computing.[1]

This proposed Regulation represents a laudable endeavour to provide a supranational legal framework for entities facilitating flows of information online, whose impact on human rights cannot be understated. The proposed Regulation, if amended to be fully human rights compliant, would therefore be a welcome step towards the fulfilment of the EU and Member States' obligations to secure human rights online as well as offline. The ICJ, however, has identified a set of concerning elements in the draft Regulation that, if left unamended, risk leading to situations not in line with human rights law. For the sake of brevity, this briefing paper will focus on these concerns and will not address other positive elements of the Regulation.

2. Applicable international and EU human rights law

In order to comply with EU law, and in particular the Charter of Fundamental Rights of the EU, the Regulation must accord with the provisions of the Charter.

The wide variety of human activities made possible by online intermediary services, such as social media, cloud services and internet providers, have the potential to affect the enjoyment and exercise of all human rights to varying extents. While measures undertaken online may affect all rights, including the prohibition of torture or other cruel, inhuman or degrading treatment, the right to a fair trial and the right to life, this paper will focus in particular to the potential impact of the Regulation on the rights to freedom of opinion and expression and the rights to privacy and data protection, under articles 7, 8 and 11 of the EU Charter, articles 8 and 10 of the European Convention on Human Rights (ECHR) and articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR). The principles applying to these rights are generally applicable also to the rights to freedom of assembly and association and freedom of religion and belief, which may also be affected by the proposed Regulation.

Under international and EU human rights law, any interference with rights to privacy or freedom of opinion and expression, including the right to impart and receive information, can only be justified

- if it is in accordance with the law,
- pursues one of the legitimate aims contemplated by the abovementioned articles,
- is necessary to achieve any such aim,

[1] See, definition under article 2: "'intermediary service' means one of the following services:
–a 'mere conduit' service that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;
–a 'caching' service that consists of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;
–a 'hosting' service that consists of the storage of information provided by, and at the request of, a recipient of the service;"

- is proportionate, in that it is the least intrusive measure necessary to achieve the legitimate aim at hand and do not imperil the essence of the right,[2]
- and is not discriminatory.[3]

As further stated in article 52 of the EU Charter, any restriction must be authorised by a judicial or other independent adjudicatory authority and effective remedies, including redress, must be available against violations of these rights.

With regard to the requirement of prescription by law, the European Court of Human Rights has held that the domestic law authorising the restriction "must also be compatible with the rule of law[,] be accessible to the person concerned and foreseeable as to its effects."[4] The law must be "formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[5]

The Special Rapporteur on freedom of opinion and expression has equally affirmed that "[r]estrictions must meet the standards of legality, meaning that they are publicly provided by a law that meets standards of clarity and precision and are interpreted by independent judicial authorities.[6]

3. Implementation of orders by the authorities

The Regulation would introduce a general civil law liability exemption regime for intermediary services, that is predicated on the obligation to institute a 'notify-and-take-down-system' (see next section) as well as to implement orders of national authorities to take down "illegal content" and provide information.

According to articles 8 and 9 of the draft Regulation, providers of intermediary services must implement orders by national judicial or administrative authorities, when issued on the basis of the applicable Union or national law, in conformity with Union law, to act against specific items of illegal content or to provide a specific item of information.

Illegal content is defined, in article 2.g, as "any information, which, in itself or by its reference to an activity, including the sale of products or provision of services, is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law."

---

[2] *Big Brother Watch and Others v UK*, ECtHR, GC, Applications Nos. 58170/13, 62332/14 and 24960/15, 25 May 2021, para. 332. See, *Roman Zakharov v. Russia*, ECtHR, GC, Application No. 47143/06, 4 December 2015, para. 227; *Kennedy v. UK*, ECtHR, Application No. 26839/05, 18 May 2010, para. 130. See also, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the General Assembly,* UN Doc. A/74/486, 9 October 2019, para. 34; *Annual Report to the General Assembly*, Un Doc. A/73/348, para. 28. See also, among others, Judgment of 9 November 2010 (Grand Chamber), *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662) 11, para. 65.

[3] See, among other sources, CCPR, General Comment No. 34, UN Doc. CCPR/C/GC/34; CCPR, General Comment No. 37, UN Doc. CCPR/C/GC/37, and the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights at https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf .

[4] *Big Brother Watch and Others v UK*, *op.cit.,* para. 332. See also, Heglas v. the Czech Republic, ECtHR, Application No. 5935/02, 1 March 2007, para. 74; *Roman Zakharov v Russia*, *op. cit.*, § 228; *Delfi AS v. Estonia*, ECtHR, GC, Application No. 64569/09, 16 June 2015, para. 120.

[5] *Delfi AS v. Estonia*, *op. cit.*, para. 121; *Ahmet Yildrim v. Turkey*, ECtHR, Application No. 3111/10, 18 December 2012 , para. 57.

[6] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the General Assembly,* A/73/348, para. 28.

In this regard, recital 12 states that "the concept of 'illegal content' should be defined broadly and also covers information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that relates to activities that are illegal, such as the sharing of images depicting child sexual abuse, unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the non-authorised use of copyright protected material or activities involving infringements of consumer protection law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is consistent with Union law and what the precise nature or subject matter is of the law in question."

The order to the provider would have to contain a statement of reasons, and information of the redress available to the provider and the recipient of the service. However, in case of request of information by public authorities, the statement of reasons could be omitted if it "cannot be provided for reasons related to the prevention, investigation, detection and prosecution of criminal offences."[7]

These articles would effectively introduce a regime of forced compliance by intermediate service providers, such as for example Facebook or a cloud service, with surveillance or wiretapping by authorities, i.e. "the specific item of information", or with activities that restrict the availability of information online.

In this regard, they constitute clear interferences with the rights to privacy, data protection and to freedom of expression, including freedom to impart and receive information, protected by articles 17 and 19 ICCPR, 8 and 10 ECHR, and 7,8 and 11 of the EU Charter. The ICJ is concerned that some of these interferences may be arbitrary or otherwise unlawful and that the draft Regulation proposed by the Commission is therefore not in compliance with obligations under international human rights law and the Charter.

The UN Special Rapporteur on freedom of opinion and expression has repeatedly warned that laws compelling social media platforms or other internet intermediaries to remove content that they deem illegal entail the risk that these actors will err on the side of caution and over-censorship. The Special Rapporteur has pointed to the unfortunate "trend that sees States delegating to online platforms "speech police" functions that traditionally belong to the courts."[8] The Special Rapporteur last July warned that "determinations on the legality of content under national laws … should be done by the courts".[9]

The *Council of Europe Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities* affirm, inline with the ECHR and ICCPR that "[a]ny request, demand or other action by public authorities addressed to internet intermediaries to restrict access (including blocking or removal of content), or any other measure that could lead to a restriction of the right to freedom

[7] Article 9.2.
[8] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Council,* UN Doc. A/HRC/47/25, para. 58.
[9] *Ibid.*, para. 90. See also, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Council,* UN Doc. A/HRC/17/27, para. 47. See also, para. 75-76.

of expression, shall be prescribed by law, pursue one of the legitimate aims foreseen in Article 10 of the Convention, be necessary in a democratic society and be proportionate to the aim pursued. State authorities should carefully evaluate the possible impact, including unintended, of any restrictions before and after applying them, while seeking to apply the least intrusive measure necessary to meet the policy objective. [Furthermore,] State authorities should obtain an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content."[10]

When considering the question of wiretapping of communications in criminal investigations and situations of national security and their compliance with the ECHR, the European Court has set minimum requirements for what should be set out in law, in order to ensure that any interference with private life rights meets standards of prescription by law, necessity and proportionality. These require that the law should set out: "(i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed."[11]

When dealing with secret surveillance, the Court has affirmed the importance of judicial review. It has held that, while "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge, [in] a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, … it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[12] Once surveillance is terminated, notification to the individual is of the essence to ensure effective access to justice against any potential violation.[13]

In relation to the position of intermediaries of services that face orders by authorities to block access or take down content, the European Court of Human Rights has held that a system of prior restraint is only acceptable where it is governed by a legal framework that ensures "both tight control over the scope of bans and effective judicial review to prevent any abuse of power."[14] The Court has further stressed that "the judicial review of such a measure, based on a weighing-up of the competing interests at stake and designed to strike a balance between them, is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression."[15]

The ICJ is concerned that the intentionally wide definition of "illegal content" in Article 2.g of the proposed regulation is overbroad does not satisfy the requirement of foreseeability under the principle of legality and prescription

[10] Appendix to Recommendation CM/Rec(2018)2, Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities, paras. 1.3.1 – 1.3.2.
[11] *Big Brother Watch and Others v UK*, *op.cit.,* para. 335. See also, *Roman Zakharov v. Russia*, *op. cit.*, para. 231.
[12] *Ibid.*, para. 336
[13] *Ibid.*, para. 337.
[14] *Ahmet Yildrim v. Turkey*, *op. cit.,* para. 64; *Vladimir Kharitonov v. Russia*, ECtHR, Application No. 10795/14, 23 June 2020, para. 43; *Association Ekin v. France*, ECtHR, Application No. 39288/98, para. 58; *Cengiz and Others v. Turkey*, ECtHR, Applications Nos. 48226/10 and 14027/11, 1 December 2015, para. 62.
[15] *Ahmet Yildrim v. Turkey*, *op. cit.,* para. 64.

by law. The application of this overbroad definition to obligations on intermediary providers to take down or provide information to the authorities, and thereby interfering with freedom of expression, is also unlikely to satisfy the principles of necessity and proportionality. There is no limitation of such obligations to serious criminal offences, including for example for measures which intermediary providers would be required to take that effectively correspond to internet wiretapping. The system of request of information effectively allows an extension of wiretapping systems far beyond the remits of criminal law, when, offline, this is usually restricted to serious offences only. **The draft regulation further fails to specify which legitimate aims, if any, any of the orders would pursue, since it mixes up aims of crime control with others of protection of copyright without clearly stating any of them.**

It is also a matter of concern that the Regulation does not require that the statement of reasons includes documentation and analytical reasoning in respect of an assessment of necessity and proportionality of the interference as required by human rights law.

The ICJ is further concerned that such orders may be issued not only by judicial authorities but also by "administrative authorities" that are not requested to satisfy any requirement of independence nor to be of judicial nature. This is a serious shortcoming in relation to the EU and Member State's obligations under international and EU human rights law, which requires wiretapping and taking down of content by order of public authorities to be solely authorised by judicial authorities.[16] The absence of judicial authorisation is particularly problematic in situations of prevention, investigation, detection and prosecution of criminal offences in which the Regulation allows Member States to dispense with the requirement of providing a statement of reasons is not provided and the only safeguard for human rights protection is the authorisation by a judicial authority.

4. Notice-and-take-down-system

The Regulation also establishes the obligation to introduce notice and content moderation systems.

Providers will have the obligation to set up mechanisms for private persons or entities to flag information they consider to be "illegal content" by providing information and their contact details.[17] It also allows for the establishment of "trusted flaggers" for such notifications. Based on this information or by their own initiative, providers would be able to decide to "remove or disable access to specific items of information." When doing so, they would need to inform the recipient promptly with a statement of reasons that include the explanation of why the content was deemed illegal or incompatible with the terms of service, as well as with information on remedies and redress against the decision.[18]

According to the Regulation, providers would need to make available to these recipients information on how to access an internal complaint-handling system. The

[16] See article 52 EU Charter and *Big Brother Watch and Others v UK*, *op.cit.,* para. 337.
[17] Article 14.
[18] Article 16.

time limit to apply under this system will be six months from the notification of the decision to remove or disable access, or to suspend or terminate, wholly or partly, the provision of the service or the recipient's account. The decisions issued by these complaint mechanisms should also provide information about out of court dispute settlement procedures available and other redress possibilities.[19]

Article 18 of the Regulation regulates these "out of court dispute settlements", that are effectively arbitration mechanisms certified by the Digital Service Coordinator (see section 6). The resort to the arbitration mechanism is without prejudice to redress before courts but "in accordance with the applicable law."[20] To certify the arbitration mechanism, the DSC must be satisfied that they are "impartial and independent of online platforms and recipients of the service" and "have the necessary expertise".[21] Article 18 does not specify what sort of redress the arbitration mechanism is empowered to provide or what are the requirements as to enforcement mechanisms for their decisions, besides the fact that under this same article online platforms are bound by the body's decision, which presumably will trigger competence of national courts for enforcement.

Article 20 gives the power to online platforms to suspend services to recipients that "frequently provide manifestly illegal content" as well as to individuals and entities that "frequently submit notices or complaints that are manifestly unfounded."[22] In the first case prior warning is sufficient while in the second the exhaustion of all previous mechanisms is necessary.

Finally, article 21 creates an obligation on online platforms to report to law enforcement and judicial authorities whenever they become "aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place."[23]

a) *International standards and jurisprudence*

International human rights law provides that individuals must be able to access effective remedies and redress for their human rights violations occurring both online and offline.[24]

As the UN Special Rapporteur on freedom of opinion and expression has outlined, "[r]emedies must be known by and accessible to anyone who has had their rights violated; must involve prompt, thorough and impartial investigation of alleged violations; and must be capable of ending ongoing violations … ."[25] The Special Rapporteur had previously recommended that "[a]ny determination on what content

[19] Article 17.
[20] Article 18.1.
[21] Article 18.2
[22] Article 20.1-2
[23] Article 21.1
[24] Article 47 EU Charter, article 2.3 ICCPR and article 13 ECHR. A thorough analysis of the right to a remedy is to be found in, ICJ, Practitioners' Guide No. 2, available at https://www.icj.org/wp-content/uploads/2018/11/Universal-Right-to-a-Remedy-Publications-Reports-Practitioners-Guides-2018-ENG.pdf. See, SR FOAA A/HRC/41/41, para. 15.
[25] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the General Assembly,* UN Doc. A/73/348, para. 39. See also, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Council,* UN Doc. A/HRC/39/29, para. 50, stressing in particular that whatever authority providing a remedy must be independent.

should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences."[26]

Furthermore, the UN Guiding Principles on Business and Human Rights, in their explanatory notes, make clear that "States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. They should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users."[27]

The *Council of Europe Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities* state that "[a]ny interference by intermediaries with the free and open flow of information and ideas, be it by automated means or not, should be based on clear and transparent policies and be limited to specific legitimate purposes, such as restricting access to illegal content, as determined either by law or by a judicial authority or other independent administrative authority whose decisions are subject to judicial review, or in accordance with their own content-restriction policies or codes of ethics, which may include flagging mechanisms."[28]

In cases of responsibility of intermediary platforms for the content they host, the European Court has made a distinction between media platforms or platforms publishing content and allowing for interaction with it on the one hand, and more general platforms such as social media, hosting services and ISSP providers, on the other. For these more general platforms, the position is that they "should not be held responsible for content emanating from third parties unless they failed to act expeditiously in removing or disabling access to it once they became aware of its illegality."[29]

In the case of the former, the obligation on the company to remove content from its website will be considered a proportionate interference with freedom of expression where the "company must be considered to have exercised a substantial degree of control over the comments published on its portal" and the content to be removed includes content such as "comments that amounted to hate speech and incitements to violence, and were thus clearly unlawful on their face."[30] The resort to filtering mechanisms for comments amounting to hate speech or speech entailing an incitement to violence was not considered by the Court as equating to "private censorship."[31] This was the case also for "notice-and-take-down" systems. However, these positions referred to the specific and defined situation of comments amounting to hate speech or incitement to violence.[32]

---

[26] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Council,* UN Doc. A/HRC/17/27, para. 70.
[27] UN Guiding Principles on Business and Human Rights with commentaries, para. 68.
[28] Appendix to Recommendation CM/Rec(2018)2, Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities, para. 2.1.3. See also, para. 2.3.6: "In cases where content is restricted by intermediaries in line with their own content-restriction policies because it contains an indication of a serious crime, restriction should be accompanied by adequate measures to ensure that evidence is retained for effective criminal law investigations. If intermediaries have specific knowledge of such restricted content, they should report this to a law-enforcement authority without undue delay."
[29] *Tamiz v. UK*, ECtHR, Application No. 3877/14, Decision of 19 September 2017, para. 84.
[30] *Delfi AS v. Estonia*, *op. cit.*, para. 153
[31] *Ibid.*, para. 157
[32] *Ibid.*, para. 159; *Magyar Tartalomszolgaltatok Egyesülete and Index.hu zrt v. Hungary*, ECtHR, Application No. 22947/13, 2 February 2016, para. 91.

b) ICJ assessment

The ICJ is concerned that the articles 14 to 21 of the draft Regulation, taken together, create a privatised system of policing and adjudication of human rights violations online. Considering the increasing and central role of intermediary platforms in the enjoyment of human rights online, in particular for what the Regulation defines as "very large platforms", restrictions on capacity to post information or make use of online services may lead to violations of the rights of freedom of expression, association, privacy, data protection, education, property, amongst others.

This concern is exacerbated by the fact that private entities exercising these functions will have to rely on the same vague concepts of "illegal content" described above that will very likely be prone to abuse and give rise to unnecessary, disproportionate and/or discriminatory restrictions.

The articles of the draft regulation on moderation of content provide a legal ground for web providers to delete information upon notification without resort to judicial proceedings. Private entities will *de iure* and *de facto* be the first instance remedy for human rights violations likely to occur online. For these reasons, **the statement of reasons should also explain the human rights grounds and implications of the decision.**

With regard to **the complaint mechanism**, it is unclear why its competence should be limited only to three kinds of decisions (decisions to remove or disable access to the information; decisions to suspend or terminate the provision of the service, in whole or in part; decisions to suspend or terminate the recipients' account) since previous articles do not define or restrict the powers of action by providers to these three types of decisions. They **should have competence on all decisions of providers interfering with the rights of recipients**. Furthermore, **it is of concern that these complaint mechanisms are not required to be independent of the provider and the recipient**, as is the case for out of court mechanisms under article 18, **nor from executive or legislative bodies**. **It is insufficient that the only power of the complaint mechanism is to reverse the decision and it does not hold any power to order reparation, including compensation, satisfaction or guarantees of non-repetition as required pursuant to the right to an effective remedy under international human rights law.**

While it is positive that their decision should provide information on further mechanisms and remedies, **the ICJ is concerned that there is too much emphasis on out of court mechanisms even for further redress than on judicial proceedings**. In terms of national law, the resort to arbitration mechanisms will often have as a consequence that, irrespective of whether afterwards those affected are able to access national courts, these mechanisms will be able only to assess the respect of minimal procedural safeguards and due process and not necessarily the merits of the dispute. It is also not clear what principles and standard of international law they will be able to apply when making their decisions. It is furthermore not clear what powers the arbitration mechanism has in terms of reparation. Finally, **the ICJ is concerned that the requirement of independence of the arbitration mechanism is only towards the platform and not State executive and legislative bodies.**

With regard to the power on intermediary services, under article 20, to suspend services to recipients that "frequently provide manifestly illegal content" as well as to individuals and entities that "frequently submit notices or complaints that are manifestly unfounded.", recipients should be clearly informed of the possibility and the means to appeal against the order in court. **The ICJ also considers that the ground for suspension of "manifest unfoundedness" of the notice is incorrect**. In the experience of human rights litigation, manifest unfoundedness is not necessarily a signal of abusiveness of the complaint. **It is** therefore **suggested to use the more established concept of "abusive".**

Finally, **the ICJ is concerned at the obligation on providers under Article 21 to report serous criminal offences that are likely to take place.** This may allow authorities to require platforms to set up predictability systems to be able to pre-empt commission of crimes. More traditionally, **obligations of prevention refer to obligation to report crimes that "are about to occur" or where there is the imminence of a risk to life or safety of persons. This article should be revised accordingly.**

5. Very large platforms

The Regulation correctly imposes accrued obligations on very large platforms compared to other operators in consideration of their systemic impact on human rights and the power imbalance they create. Some of these obligations oblige these platforms to provide risk assessments and undergo independent audits.

The ICJ is however concerned that these tools are not sufficiently focused on the human rights impact of the activities of these very large platforms. Under the regulation, their risk assessment must focus on risk for "illegal content" and specific rights, such as the right to private and family life, the right to freedom of expression and information, the prohibition of discrimination and the rights of the child. While this latter focus is welcome, it remains insufficient in light of the impact that actions on these platforms may have on a wide range of human rights. For this reason, **the risk assessment under article 26 should encompass all rights enshrined in the EU Charter of Fundamental Rights.**

The same may be said for the requirement of **independent audits** under article 28 that reflects current traditional audits. These **should include in addition a human rights impact focus.**

6. The Digital Service Coordinator

The draft Regulation would institute Digital Service Coordinators as the key oversight system of the Regulation. Designated by the Member State, they would be "responsible for all matters relating to application and enforcement of th[e] Regulation in that Member State, unless the Member State concerned has assigned certain specific tasks or sectors to other competent authorities. The Digital Services Coordinator would in any event be responsible for ensuring coordination at national level in respect of those matters and for contributing to the effective and consistent application and enforcement of th[e] Regulation throughout the Union."[33]

[33] Article 38.1.

Despite the clear oversight role of the DSC, however, the draft Regulation does not require that they be independent but only that they "perform their task under this Regulation in an impartial, transparent and timely manner",[34] to "act with complete independence" when carrying out their tasks and exercising their powers and to "remain free from any external influence, whether direct or indirect, and shall neither seek nor take instructions from any other public authority or any private party."[35]

The DSC will have the investigation powers (requesting information from providers, carrying out on-site inspection of any premises and interrogate staff members and representatives of the providers) and enforcement powers (including ordering the cessation of infringements, impose remedies aimed at reparation and cessation, impose fines and adopt interim measures).[36]

When all these powers have been used and the infringement persists and causes serious harm, DSCs can request an action plan from the providers' management body to terminate the infringement and follow up on its implementation and, if that does not work, "request the competent judicial authority of that Member State to order the temporary restriction of access of recipients of the service concerned by the infringement" or even to the online interface.[37]

The Regulation provides for the possibility of the targets of these measures to present their views and mandates Member States to "ensure that any exercise of the powers pursuant to paragraphs 1, 2 and 3 is subject to adequate safeguards laid down in the applicable national law in conformity with the Charter and with the general principles of Union law. In particular, those measures shall only be taken in accordance with the right to respect for private life and the rights of defence, including the rights to be heard and of access to the file, and subject to the right to an effective judicial remedy of all affected parties."[38]

The ICJ is concerned that an institution with such a key oversight mandate and intrusive investigative and enforcement powers has no requirement of institutional independence.

The UN Special Rapporteur on freedom of opinion and expression has recommended that the independence of oversight bodies or regulators must be assured and scrupulously respected.[39] The Special Rapporteur underscored that "State regulation of social media should focus on enforcing transparency, due process rights for users and due diligence on human rights by companies, and on ensuring that the independence and remit of the regulators are clearly defined, guaranteed and limited by law."[40]

The Court of Justice of the EU has ruled that "supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an

[34] Article 39.1
[35] Article 39.2
[36] Article 41.1-2
[37] Article 41.3.
[38] Article 41.6
[39] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Committee,* A/HRC/47/25, para. 59, 60.
[40] *Ibid.*, para. 91.

independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task of establishing a fair balance between the protection of the right to private life and the free movement of personal data. The mere risk that the scrutinising authorities could exercise a political influence over the decisions of the competent supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks."[41]

Considering the impact of their actions on human rights and the holding of certain powers that would require judicial authorisation, such as the power to search and interrogate, Digital Service Coordinators should be guaranteed structural and functional independence as a minimum standard.

7. The European Board for Digital Services

Articles 47 and 48 of the draft Regulation establish an independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services named 'European Board for Digital Services', tasked with an advisory role for the Commission and the DSCs.

The ICJ is concerned that the European Board has a merely advisory role and leaves all supervisory power in the hands of the European Commission, i.e. an executive body. **Article 57 should make clear that the Board shall be independent of Member States, any executive authority and the European Commission and Council.** It is problematic that the European Commission, an executive body, chairs the Board. While it is welcome that observers may be invited, the potential impact of this Regulation on human rights is so significant that more expertise in the field should be guaranteed. For that reason, **the ICJ considers that the FRA should be a member of the Board and with provision for full and meaningful participation by civil society.**

[41] Judgment of 9 March 2010 (Grand Chamber), *Commission v Germany* (C-518/07, EU:C:2010:125) 5. See also, Judgment of 16 October 2012 (Grand Chamber), *Commission v Austria* (C-614/10, EU:C:2012:631): "The fact that such an authority has functional independence in so far as its members are independent and are not bound by instructions of any kind in the performance of their duties is not by itself sufficient to protect that supervisory authority from all external influence. The independence required in that connection is intended to preclude not only direct influence, in the form of instructions, but also any indirect influence which is liable to have an effect on the supervisory authority's decisions."