AMNESTY INTERNATIONAL

Amnesty International is a worldwide organisation committed to protecting human rights, including in the digital space. In our 2019 report "*Surveillance Giants: How the business model of Google and Facebook threatens human rights*", we set out an analysis of the concentration of power in dominant online platforms and the impact of their surveillance-based business model on the exercise of human rights online.[1]

AMNESTY INTERNATIONAL POSITION ON THE PROPOSALS FOR A DIGITAL SERVICES ACT AND A DIGITAL MARKETS ACT

March 2021

Amnesty International welcomes the European Commission putting forward legislative proposals to regulate digital services[2] and digital markets.[3] These measures have been eagerly awaited as there is a pressing need for a safer and more transparent online environment, where human rights are effectively protected, in particular in view of a few tech giants dominating and controlling the sphere. Given the two initiatives are intrinsically linked, this paper aims to address both.

KEY RECOMMENDATIONS

Amnesty International welcomes that the **Digital Services Act (DSA)** increases accountability of providers of online services, improves transparency of platforms' practices and establishes clearer rules for content moderation. The fact that the DSA upholds the conditional liability exemptions and the prohibition of a general monitoring obligation to find illegal activity is equally welcome. Amnesty also supports the imposition of risk assessment and mitigation measures on very large online platforms to manage systemic risks.

However, Amnesty believes the proposed DSA does not go far enough in protecting people's human rights and that it should be more ambitious to effectively protect them. In particular:

- The DSA should not delegate responsibility to companies as adjudicators of the substantive legality of content and consequently, intermediaries should not bear liability for failure to remove content of which they are not aware and which they have not modified absent a judicial order[4]. The DSA's provisions on **notice and action mechanisms** should clearly reflect this principle.
- Amnesty considers that the DSA should impose stricter limits on the **targeting of online advertising** based on the processing of personal data and urges the co-legislators to

[1] Amnesty International, Surveillance Giants: How the business model of Google and Facebook threatens human rights, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

[3] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.

[4] Note that this sentence has been amended post-publication for further clarification.

consider restrictions on targeted advertising on the basis of invasive tracking practices, such as cross-site tracking and tracking based on sensitive data or other personal data that could lead to discriminatory outcomes.

- Amnesty welcomes the obligations imposed on very large online platforms (VLOPs) to address **systemic risks** stemming from the functioning and use made of their services but these obligations must go further and extend to compulsory and effective human rights due diligence in line with international human rights standards including the UN Guiding Principles on Business and Human Rights. VLOPs need to be required to take appropriate action not only to identify and mitigate, but also to cease and prevent any human rights abuses linked to their operations and underlying business model and be transparent about their efforts in this regard.
- To protect people's privacy and to give them real choice and control, a profiling-free recommender system should not be an option but the norm. Therefore, **algorithmic recommender systems** used by online platforms shall not be based on profiling by default and must require an opt-in instead of an opt-out, with the consent for opting in meeting the requirements of the General Data Protection Regulation (GDPR) of being freely given, specific, informed and unambiguous.

With regard to the **Digital Markets Act (DMA)**, Amnesty welcomes its focus on levelling the playing field and addressing the dominant role of gatekeepers over the online environment.

However, the DMA should put more focus on end-users and be more ambitious to allow competitors to the gatekeepers to emerge that offer more choice and better conditions to end-users. In particular:

- The DMA should affirm the principle that access to and use of essential digital services and infrastructure cannot be made conditional on **ubiquitous surveillance and profiling**. Gatekeepers must be prevented from making access to their service conditional on individuals "consenting" to the processing of their personal data for marketing or advertising purposes.
- The DMA should furthermore include obligations for **cross-platform interoperability** that would allow people to connect and communicate across core services and platforms without the need to sign up to the gatekeeper services, which would give a true chance for competitors to emerge with more human rights respecting and privacy-friendly terms compared to current gatekeepers.

BACKGROUND

The rise of social media and other online platforms has brought unprecedented global connectivity. Despite the real value of online platforms in enabling human rights online, the services come at a serious human rights cost[5]. The increasing power of online platforms has led to a systemic erosion of the right to privacy in the digital space, and corresponding impacts on a range of other rights including non-discrimination, freedom of expression and opinion, and freedom of thought. It has become virtually impossible for users to engage in the digital world without being subject to ubiquitous corporate surveillance and intrusive profiling. Such practices are only increasing in breadth and depth in parallel with the erosion of any meaningful alternatives. As with all systems of surveillance, this has disproportionate impacts on marginalised groups, and exacerbates existing structural inequalities.[6]

The impacts on human rights go hand in hand with the concentration of platform power generated and entrenched, among others, by network and lock-in effects, increased entry barriers, leveraging dominance in one sector to increase dominance in another, downranking the services offered by would-be competitors, and buying-off competitors. These corporate practices are characteristic of the gatekeeper platforms, such as Google and Facebook.[7]

Any laws governing online content pose high risks of undermining freedom of opinion and expression and must be carefully crafted and implemented in line with human rights law and standards.[8] It is therefore vital that the Digital Services Act Package addresses not only online content itself but also the root causes of the spread of disinformation and other harmful content – namely the dominance of Big Tech and their business models predicated on intrusive surveillance, profiling and manipulation at scale.[9]

I. THE DIGITAL SERVICES ACT (DSA)

Amnesty welcomes that the DSA increases accountability of providers of online services, improves transparency of platforms' practices and establishes clearer rules for content moderation. The fact that the DSA upholds the conditional liability exemptions and the prohibition of a general monitoring obligation to find illegal activity is equally welcome. Amnesty also supports the imposition of risk assessment and mitigation measures on very large online platforms to manage systemic risks. However, Amnesty believes the proposed DSA does not go far enough in protecting people's human rights and that it should be more ambitious to effectively protect them.

---

[5] Amnesty International, *Surveillance Giants*.

[6] See for example Pratyusha Kalluri, co-creator of the Radical AI Network, *Don't ask if artificial intelligence is good or fair, ask how it shifts power*, in Nature, July 2020, https://www.nature.com/articles/d41586-020-02003-2; Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, 2019.

[7] Amnesty International, *Surveillance Giants.*

[8] UN Special Rapporteur on freedom of opinion and expression, *Online content regulation*, Report to the Human Rights Council, April 2018, A/HRC/38/35.

[9] Ranking Digital Rights, *It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy*, 2020, https://rankingdigitalrights.org/its-the-business-model/.

1. Content moderation

Why is this a human rights issue?

People rely on social media platforms to access information, interact and organise. These private actors are increasingly the arbiters of speech, regulating what is acceptable content on their platforms and deciding on content take-downs, suspension of accounts or on the banning of users from their platforms. Removing or disabling access to third-party content by providers of hosting services risks leading to undue restrictions of the right to freedom of expression with additional implications on other rights, such as the right to freedom of association. Even where complaint and redress mechanisms exist, these are accessible only after the content has been removed, which means the harm is already done and which imposes a burden on the user to remedy this harm.

Public actors can also unlawfully restrict content online, for instance by issuing removal orders in the name of combatting terrorism, extremism or hate speech, or simply defending traditional values, leading to further violations to free expression. Certain EU governments like Hungary, Poland, Romania and France, in the course of 2020, further pursued limitations to freedom of expression, mostly as a response to the COVID19 pandemic,[10] but even when this was not strictly required by the pandemic itself.[11] This is a worrying sign of increasing authoritarian trends in Europe, which the EU institutions have struggled to effectively counter.

Furthermore, the size and scale of online platforms has fuelled amplification of abusive and hateful content, particularly targeting women, people of colour, LGBTI people and other groups. Amnesty's work on online violence and abuse against women highlights how such conduct – and the failure of companies to address it –has the effect of silencing people, or driving them offline, rendering the enjoyment of the right to freedom of expression unequal in practice.[12]

The particular risks for vulnerable or marginalised communities have also been highlighted by the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, who has raised concerns that company policies on hate, harassment and abuse, and on content that promotes terrorist acts or that incites to violence, are often vague and result in inconsistent policy enforcement that penalizes minorities while reinforcing the status of dominant or powerful groups.

The Special Rapporteur has also called for greater transparency and accountability in content moderation decisions and a commitment to remedy, so that individuals' ability to use online

---

[10] France: Thousands of protesters wrongly punished under draconian laws in pre and post COVID-19 crackdown | Amnesty International, https://www.amnesty.org/en/latest/news/2020/09/france-thousands-of-protesters-wrongly-punished-under-draconian-laws-in-pre-and-post-covid19-crackdown/

[11] https://www.amnesty.org/en/latest/news/2020/11/poland-charges-against-women-for-lgbti-virgin-mary-posters-must-be-dropped/

[12] Amnesty International, Toxic Twitter - A Toxic Place For Women, March 2018 https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

platforms as forums for free expression, access to information and engagement in public life can be protected.[13]

What does the DSA propose?

Article 12 requires providers of intermediary services to include in their terms and conditions information on any restrictions that they impose in relation to the use of their service in respect of information provided by users of the service. This must include information on content moderation policies, procedures, measures and tools, including algorithmic decision-making and human review. Providers of intermediary services are required to act in a diligent, objective and proportionate manner in applying and enforcing the restrictions, taking into account fundamental rights.

Article 14 sets out rules on notice and action mechanisms. These require hosting service providers to put in place mechanisms to allow individuals or entities to notify them of the presence of content on their services that they consider to be illegal. These mechanisms need to facilitate sufficiently precise and adequately substantiated notices that allow a diligent economic operator to identify the illegality of the content in question. The notices furthermore need to contain certain elements such as an explanation of the reasons why the content is considered illegal, an indication of the electronic location of the content and information on the individual or entity submitting the notice.

Notices containing the required elements are considered to give rise to actual knowledge or awareness under Article 5, meaning the provider may lose their liability exemption unless they act expeditiously to remove or disable access to the illegal content.

What is Amnesty calling for?

Notice and action mechanisms like those in the DSA represent a shift from the traditional adjudication of free expression and censorship questions from the judiciary to private companies. While this reflects an acknowledgment of the practical difficulties in managing the high number of cases within national courts, it nonetheless carries serious implications for human rights. It remains questionable whether private companies are the best placed to decide on the legal or illegal nature of online content. This doubt is reinforced by the fact that illegal content is not defined in the DSA and captures any content that is illegal under EU or national law, ranging from terrorist content, child sexual abuse material, hate speech to intellectual property rights and consumer protection infringements.

As called for by the former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, States "should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users".[14] In this regard, the DSA must uphold the principle that

[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/38/35, 6 April 2018, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.

[14] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/38/35, 6 April 2018, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35.

intermediaries should not be required to substantively evaluate the legality of third-party content, in line with the Manila Principles on Intermediary Liability.[15]

Furthermore, the fact that a notice gives rise to actual knowledge or awareness and thus risks taking away the liability exemption means that platforms are likely to act in a precautionary way to over-remove content, so as not to incur liability and to avoid being held accountable. Intermediaries should not bear liability for failure to remove content of which they are not aware and which they have not modified absent a judicial order and the provisions of the DSA on notice and action mechanisms should clearly reflect this principle[16].

Finally, the DSA's content moderation provisions must keep human rights at their centre and include rules for intermediaries to more closely engage with digital rights organizations, further supporting transparency and accountability.

2. Online advertising

Why is this a human rights issue?

Amnesty International considers current targeted advertising practices that rely on indiscriminate corporate surveillance and profiling to be inherently incompatible with human rights and data protection principles established in the General Data Protection Regulation (GDPR) and the Charter of Fundamental Rights of the European Union. One of the main purposes of the GDPR is to give people control over their personal data, but the current online advertising ecosystem does exactly the opposite, taking people's control away. And once control is lost, it cannot easily be regained, and people have essentially been forced to sign away their fundamental rights.

Many of the big tech companies make the vast majority of their revenue through digital advertising, which comes at the price of enormous privacy invasions. Indeed, the way today's online ecosystem works incentivises collections of vast amounts of personal data and gives those who hold the most data a competitive advantage. But it should not be forgotten that our personal data is not a tradeable commodity that can be exchanged like money or other goods.[17] The only way to de-incentivise such abusive data collection is to set clear regulatory limits on it. Power over personal data cannot be a unique selling proposition for any commercial actor.

The surveillance-based business model of big tech companies like Google and Facebook needs our attention to survive and competes for it fiercely. In fact, this attention-grabbing machinery, fuelled by the business model, is at the source of many of the problems today's internet faces. Any engagement online means more eyeballs, which in turn means more advertising revenue. Therefore, these companies are incentivised to use any means to increase views, clicks, likes and shares, which leads to the amplification of online disinformation, polarisation and advocacy of hatred, given that sensationalist and extreme content is the fastest way to success in the form

[15] https://manilaprinciples.org/ .

[16] Note that this sentence has been amended post-publication for further clarification.

[17] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, 8 October 2019.

of advertising revenue.[18]The role of social media platforms' business model, based on micro-targeted advertising, in the spread and amplification of hate speech and radicalisation has also been recognized by the European Parliament in its resolution on strengthening media freedom.[19]

What does the DSA propose?

Article 24 imposes advertising transparency obligations on online platforms. In particular, the platforms need to enable users to identify ads as such as well as the natural or legal person on whose behalf the advertising is displayed. Furthermore, platforms are required to provide "meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed". Additionally, Article 36 provides for the possibility to draw up codes of conduct at EU level between online platforms and other relevant service providers to contribute to further transparency in online advertising.

Despite calls from the European Parliament,[20] the DSA does not include rules to regulate more strictly the targeting of ads based on the processing of personal data.

What is Amnesty calling for?

The internet needs to become a healthier place where human rights and dignity are fully preserved and that does not allow harmful content to flourish. There should no longer be an incentive to collect such vast amounts of personal data.

Amnesty International considers that the DSA should impose stricter limits on the targeting of online advertising and not restrict itself to increased transparency requirements. It is an illusion to believe the digital economy would not work without the current model of ads being targeted based on aggressive data harvesting and profiling. In fact, evidence indicates that contextual advertising can be more profitable for publishers and at the same time perform better than ads driven by personal data.[21]

---

[18] Amnesty International, *Surveillance Giants;* UK House of Commons, *Disinformation and 'fake news': Final Report*, 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf; and Cohan Peter, *"Does Facebook Generate Over Half of Its Ad Revenue From Fake News?",* Forbes, November 25 2016, https://www.forbes.com/sites/petercohan/2016/11/25/does-facebook-generate-over-half-its-revenue-from-fake-news/#e633dda375f5.

[19] European Parliament resolution of 25 November 2020 on strengthening media freedom: the protection of journalists in Europe, hate speech, disinformation and the role of platforms (2020/2009(INI)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0320_EN.html.

[20] European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))", https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html. and European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, (2020/2018(INL))" https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html.

[21] Panoptykon, *To track or not to track? Towards privacy-friendly and sustainable online advertising*, 25 November 2020, https://en.panoptykon.org/privacy-friendly-advertising.

In this context, Amnesty welcomes the calls from the European Parliament[22] and the European Data Protection Supervisor[23] to regulate advertising "more strictly in favour of less intrusive forms of advertising that do not require any tracking of user interaction with content" and urges the co-legislators to consider restrictions on targeted advertising on the basis of invasive tracking. At a minimum, such restrictions should end the use of cross-site tracking, prohibit the use for ad targeting of special categories of data listed under Article 9 of the GDPR and prohibit further uses of personal data that could expose people to discrimination (e.g. data inferring a person's social or financial situation or mood). The DSA should also put in place greater limitations on the use of data for targeted advertising by the very large online platforms (VLOPs), given these platforms have control over large troves of data and data infrastructure with corresponding high risks of human rights harms. Ideally, the information ad targeting relies on should shift towards more general parameters, such as the user's current device language, approximate geographic area, and the context in which an ad is shown.

Furthermore, Amnesty International regrets that the DSA's advertising transparency provisions do not go much further than existing rules established in EU legislation, which already require ads to be identifiable as such and to disclose the person behind those ads.[24] Additionally, the requirement to provide "meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed" does not give sufficient insight to individuals to determine and fully understand why they have been targeted by a certain ad. For this purpose, detailed parameters need to be disclosed, such as online interactions relied upon (clicks, likes, shares, posts etc.), interests deducted and the specific information that was processed to reach these deductions. Even though, as a primary and preferred goal, targeting possibilities should be strictly limited, at the very least, Amnesty calls for the obligatory disclosure by all online platforms of detailed targeting parameters to ensure full transparency and truly meaningful information to people on the use that has been made of their personal data.

3. Obligations imposed on very large online platforms (VLOPs)

a) Systemic risks

Why is this a human rights issue?

The technology companies behind the very large online platforms (VLOPs) have acquired an unprecedented degree of concentrated power over modern societies and economies, driven by

[22] European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))", https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html. and European Parliament, "European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, (2020/2018(INL))" https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html.

[23] European Data Protection Supervisor, Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021.

[24] See for instance Article 6 of Directive 2000/31/EC and Article 9 of Directive 2010/13/EU.

their ability to leverage their dominant control over data infrastructure.[25] Indeed, a few very large platforms act as gatekeepers to information online, facilitate public debate, contribute to shaping public opinion, but also drive content that can fuel polarization, extremism, and online disinformation, enabled by recommender algorithms and ad-driven business models. In particular two companies have established near total control over the primary channels that most people rely on to engage with the digital world and the global "public square", a position that was largely facilitated by their surveillance-based business model.

The size and scale of the platforms and their dominance over our lives greatly heightens the risk of harms linked to their operations and underlying business model, and as such the VLOPs pose systemic risks to human rights. These risks such as the amplification and spread of hateful content and disinformation prevent people from fully enjoying and exercising their human rights, such as the rights to freedom of expression and freedom of thought. The surveillance-based business model of some of the VLOPs has also fundamentally undermined the right to privacy, with a range of knock on effects on other rights. The awareness and fear of being constantly tracked creates chilling effects that impede people from expressing themselves freely and alters their behaviour. The risks are further aggravated when data are accessed by third parties, such as insurers, employers or even governments. People belonging to racial or ethnic minorities or anyone else who belongs to a "different" group from those in positions of privilege or power (e.g. LGBTI) are particularly affected and at risk.

What does the DSA propose?

Article 25 defines very large online platforms (VLOPs) as those which provide their services to at least 45 million average monthly active recipients of the service in the EU. Article 26 requires these VLOPs to identify, analyse and assess any significant systemic risks arising from the "functioning and use made of their services", including:

> the dissemination of illegal content through their services;
>
> any negative effects on fundamental rights to private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child;
>
> intentional manipulation of their service, such as by inauthentic use or automated exploitation, with negative effects on public health, minors, civic discourse, electoral processes and public security;

These risk assessments shall take into account how content moderation, recommender systems and advertising practices influence these risks.

Article 27 requires VLOPs to put in place reasonable, proportionate and effective risk mitigation measures, such as adapting content moderation or recommender systems, limiting the display

[25] Paul Nemitz, Principal Adviser in the European Commission (writing in his personal capacity), Constitutional democracy and technology in the age of artificial intelligence, October 2018. The analysis refers to the power of Google, Facebook, Microsoft, Apple and Amazon.

of ads, initiating or adjusting cooperation with trusted flaggers or with other online platforms through codes of conduct and crisis protocols.

The European Board for Digital Services shall publish yearly reports on the identification and assessment of the most prominent and recurrent systemic risks and include best practices to mitigate the risks identified.

What is Amnesty calling for?

Amnesty welcomes the greater obligations imposed on VLOPs to address systemic risks stemming from the functioning and use made of their services, and in particular the need to assess and mitigate any negative effects on fundamental rights to respect for privacy, freedom of expression, non-discrimination and the right of the child.

However, these obligations must go further and extend to compulsory and effective human rights due diligence requiring the VLOPs' to identify, cease, prevent, mitigate, monitor and account for their impacts on any human rights, in line with international standards including the UN Guiding Principles on Business and Human Rights. The introduction of rules for mandatory corporate environmental and human rights due diligence is also what the European Commission has committed to, as part of a Sustainable Corporate Governance initiative, and which has recently been supported by the European Parliament.[26]

As part of due diligence, VLOPs need to be required to take appropriate action not only to mitigate, but also to cease and prevent any human rights abuses linked to their operations and underlying business model, and be transparent about their efforts in this regard. Unfortunately, given the size, reach and dominance of the VLOPs, the mitigation measures currently indicated in the proposal will be insufficient to address the depth and scale of their human rights impacts. In particular, the proposal should make clear that where VLOPs' core data-driven operations inherently undermine human rights, the companies must curtail these practices and find ways to transition to a rights-respecting business model.

VLOPs must also put in place measures to ensure that during the development and deployment of algorithmic systems, the algorithms do not disproportionately undermine the rights of any group in society, particularly marginalised communities. For this purpose, VLOPs need to consult with relevant stakeholders in an inclusive manner, including affected groups, organizations that work on human rights, equality and discrimination, as well as independent human rights and machine learning experts.[27]

Finally, remedies need to be in place in case breaches occur, which, where appropriate, could include operational-level grievance mechanisms that are accessible directly to individuals and

---

[26] European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability (2020/2129(INL)), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0073_EN.html ; Civil society statement on the adoption of European Parliament Due Diligence & Corporate Accountability Legislative Report, 11 March 2021, https://www.business-humanrights.org/en/latest-news/cso-statement-strong-signal-from-european-parliament-but-the-commission-will-have-to-go-further/

[27] Amnesty International and Access Now, The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems, May 2018, https://www.torontodeclaration.org/.

communities who are adversely impacted. In this context, remedies should be carved out more clearly with an out-of-court dispute settlement available for any topics falling under the scope of the Regulation (e.g. online advertising, recommender systems, intentional manipulation of services). The scope of remedies should also account for the inherently collective nature of algorithmic harms linked to the VLOPs that impact large groups of people at scale.

b) Audits

Why is this a human rights issue?

Companies need to be held liable for human rights harms linked to their algorithmic systems or if they fail to carry out meaningful due diligence and regulators must have powers to oversee their practices, including the application and impact of algorithmic systems. Independent third-party audits will help bring clarity and transparency into the opacity of platforms' systems and algorithmic processes and hold companies accountable for human rights abuses.

What does the DSA propose?

Article 28 requires VLOPs to be subject, at their own expense, to a yearly audit to assess compliance with their due diligence obligations under the DSA and with any commitments undertaken pursuant to codes of conduct and crisis protocols. This audit shall be performed by an organisation that is independent from the VLOP, with proven expertise in the area of risk management, technical competence and capabilities as well as proven objectivity and professional ethics.

What is Amnesty calling for?

Amnesty welcomes the obligation for VLOPs to be subject to a yearly audit by an organisation that is independent from the VLOP, with proven expertise in the area of risk management, technical competence as well as proven objectivity and professional ethics.

However, the mentioned criteria are not enough to ensure the auditor is truly independent as the VLOP still has a large margin to choose the auditor to their liking, which raises serious questions as to their true objectivity and independence. For an auditor to be actually independent, the choice cannot be left to the platform, but should instead be designated or certified by a third party, e.g. the Digital Services Coordinator.

c) Recommender systems

Why is this a human rights issue?

Algorithmic recommender systems facilitate access to information while ranking, prioritising and amplifying certain messages. They are responsible for what kind of content people see in their social media feeds, they stimulate public discourse and impact people's ability to retrieve and interact with information online.

Recommender systems play an important role in the ad-driven business model of today's main online platforms, aiming at keeping people's attention fixed on the platform for as long as possible so that they can be shown more ads and thus generate more revenue. These algorithms feed on people's personal data and online behaviour over time, profiling and manipulating them

by presenting people content as being the most "relevant", while being determined to maximise revenues.[28]

As algorithmic recommender systems are designed to maximise ad revenues, they promote divisive and scandalising content that is more likely to attract users' attention and keep them engaged, fuelling online disinformation, incitement to violence and racial discrimination.

As demonstrated, these practices are harmful to a myriad of human rights, such as the rights to privacy, non-discrimination, freedom of expression and freedom of thought, particularly when applied at the scale of the VLOPs.

What does the DSA propose?

Article 29 requires VLOPs to clearly set out in their terms and conditions the main parameters used in their recommender systems "as well as any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling".

What is Amnesty calling for?

Amnesty supports more transparency, choice and control for users of online platforms with regard to opaque recommender systems. Transparency is a core element of human rights due diligence, ensuring that companies "know and show" that they respect human rights, where showing "involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."[29]

However, the obligation to have at least one option which is not based on profiling does little to go beyond requirements already well-established in the GDPR. To protect people's privacy and to give them real choice and control, a profiling-free recommender system should not be an option but the norm. Therefore, recommender systems shall not be based on profiling by default and must require an opt-in instead of an opt-out, with the consent for opting meeting the requirements of the GDPR of being freely given, specific, informed and unambiguous.

Furthermore, the proposed transparency obligations on recommender systems are too vague, limiting themselves to the requirement to disclose the "main parameters used" in the platforms' terms and conditions. The latter tend to be lengthy and legalistic documents, which makes it difficult for people to find and understand the relevant information buried therein. Transparency requirements need to be strengthened to disclose detailed parameters for the public to understand how information is presented and prioritised, and how their data is used to drive these systems. These parameters need to be made available to users in an easily comprehensible and accessible manner, which requires these to be made available in a place separate to the terms and conditions.

d) Advertising repositories

[28] European Data Protection Supervisor, Opinion 1/2021 on the Proposal for a Digital Services Act, 10 February 2021; European Data Protection Supervisor, "Opinion 3/2018 EDPS Opinion on online manipulation and personal data", 19 March 2018.

[29] UNGPs, Commentary to Principle 21.

Why is this a human rights issue?

The topic of online advertising was discussed in section 2, where the human rights harms linked to the advertising-driven business model that some of the big tech companies rely on were elaborated in detail. While Amnesty maintains that current online advertising practices based on pervasive tracking are inherently incompatible with human rights, increasing transparency is a first step to shedding light into opaque algorithmic systems and profiling techniques and to eventually give people more choice and control over the content (including advertised content) they are confronted with online.

What does the DSA propose?

Article 30 sets out the obligation for VLOPs to compile and make publicly available through APIs their ads in repositories until one year after the ad was displayed for the last time. The repositories have to contain information i) on the content of the ad; ii) the natural or legal person on whose behalf it was displayed; iii) the period during which it ran; iv) whether the ad was intended to be displayed specifically to one or more particular groups of people and if so, the main targeting parameters used for that purpose; and v) the total number of people reached and aggregate numbers for the group of people to whom the ad was targeted specifically.

What is Amnesty calling for?

Amnesty welcomes any efforts to provide people with more transparency about the content, including advertised content, presented to them online, however regrets the lack of ambition of the proposal with regard to advertising repositories. The proposal obliges VLOPs to compile and make publicly available their ads in repositories with information such as the content of the ad, on whose behalf it was displayed, the period it ran and the main targeting parameters. More detailed targeting criteria must be made available to ensure meaningful information is provided that enables an understanding of how people were targeted. Additionally, exclusion criteria must be disclosed in order to detect discriminatory practices, i.e. whether one or more particular groups were excluded from the advertisement.

e) Access to data

Why is this a human rights issue?

Transparency entails not only providing adequate information to individuals who use the services of the VLOPs, but also enabling third parties to scrutinise and assess the functioning of the platforms and their underlying algorithmic systems.[30] On the one hand, providing regulators and researchers access to platform data contributes to shedding light into opaque algorithmic black boxes and to holding platforms more accountable. A better understanding of the systemic risks can also help alter the course and prevent and halt future harms. On the other hand, such access to data can raise risks to the right to privacy, as the Cambridge Analytica scandal demonstrated,

[30] Kaminski, Margot E., Understanding Transparency in Algorithmic Accountability, June 2020, available at: https://ssrn.com/abstract=3622657

where personal data of 87 million Facebook users was misused, relying on data initially collected for academic research.[31]

What does the DSA propose?

Article 31 requires VLOPs to provide the Digital Services Coordinator or the European Commission upon their reasoned request access to data that are necessary to monitor and assess compliance with the DSA. Upon reasoned request by the Digital Services Coordinator or the European Commission, VLOPs also have to give access to vetted researchers to conduct research that contributes to the identification and understanding of systemic risks. To be vetted, researchers have to be affiliated with academic institutions, be independent from commercial interests, have proven expertise as well as commit and be in a capacity to preserve specific data security and confidentiality requirements.

The provisions of the DSA do not specify what kind of data VLOPs should give access to and could potentially also extend to personal data.

What is Amnesty calling for?

Amnesty supports enhanced access to platform data for regulators as well as for independent researchers, journalists, academics and civil society to conduct research into systemic risks. However, Amnesty urges caution that such access to data might lead to further privacy abuses. Any data access must fully ensure the respect of the right to privacy and the confidentiality of communications and be in line with users' legitimate expectations.

The DSA needs to clearly specify the types of data independent researchers can access. As a rule, data access shall be limited to non-personal and anonymised data. Access to personal data can only take place in exceptional circumstances and must be limited to the absolute necessary, given the high degree of intrusion into people's private lives and the potentially sensitive nature of the data. In this case, a data protection impact assessment needs to be mandated and the DSA must put in place appropriate safeguards.

4. Enforcement in the DSA

Why is this a human rights issue?

To be effective, the new responsibilities and obligations imposed on online intermediaries must be accompanied by a strong enforcement mechanism. As experience with the GDPR has shown, even if there is a robust legal framework in place, breaches of the rules will persist if these rules are not enforced and sanctioned.[32] Without proper enforcement and without effectively tackling and putting an end to infringements of the rules, harms to human rights that the DSA aims to prevent will continue to exist.

What does the DSA propose?

---

[31] Amnesty International, *Surveillance Giants*.

[32] See Brave, *Europe's governments are failing the GDPR*, April 2020, https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf; Access Now raises the alarm over weak enforcement of the EU GDPR on the two-year anniversary, 25 May 2020 https://www.accessnow.org/alarm-over-weak-enforcement-of-gdpr-on-two-year-anniversary/

Article 38 provides for a system of enforcement principally based on one or more competent authorities at national level with one of those authorities designated as Digital Services Coordinator. Article 39 requires the Digital Services Coordinators to perform their tasks in an impartial, transparent and timely manner and to act with complete independence. According to Article 40, jurisdiction lies with the member state in which the main establishment of the provider of intermediary services is located. For VLOPs, the DSA establishes a system of enhanced supervision in its Section 3 with the possibility for the European Commission to intervene in or initiate proceedings. In this regard, the Commission has a set of powers, such as to request information, conduct on-site inspections, order interim measures, adopt non-compliance decisions and impose fines on the VLOPs.

What is Amnesty calling for?

The Digital Services Coordinators must regularly engage in consultation and dialogue with relevant stakeholders, including civil society and representatives of marginalised groups[33] and be adequately resourced, independent and given enough authority to meaningfully hold powerful technology companies to account. Online platforms must be held liable, which includes the imposition of effective and dissuasive sanctions, when they have caused or contributed to human rights harms, or when they have failed to carry out human rights due diligence. Amnesty welcomes the possibility for the European Commission to step in as an enforcement and oversight body, which may help ensure the rules are effectively enforced and alleviate the problem of enforcement depending on a single national regulator, which might be overburdened with cases and under-resourced to tackle them.

II. THE DIGITAL MARKETS ACT (DMA)

Amnesty International welcomes the DMA's focus on levelling the playing field and addressing the dominant role of gatekeepers over the online environment. However, Amnesty believes the DMA should put more focus on end-users and be more ambitious to allow competitors to the gatekeepers to emerge that offer more choice and better conditions to end-users.

1. Combination of data and profiling

Why is this a human rights issue?

Companies such as Google and Facebook make their services conditional upon ubiquitous surveillance of their users, from search preferences to location tracking, which provides them extensive powers to exploit individual vulnerabilities.[34] This is achieved by creating lock-in effects, which discourage users from selecting privacy-friendly alternatives to surveillance-based business models.

The dominance of the gatekeeper platforms means in practice people have become reliant on their services to facilitate the enjoyment of rights such as freedom of expression, the rights of

[33] Council of Europe, *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, April 2020, Preamble para. 5.

[34] Amnesty International, *Surveillance Giants*.

peaceful assembly and association.[35] This has created a paradoxical situation where for people to exercise their rights in the digital age, they are forced to accede to a business model that inherently undermines their human rights. This false choice and its impact on people's rights was recognised by Germany's federal court in a ruling on Facebook and antitrust, in a case that has now been referred to the European Court of Justice.[36]

What does the DMA propose?

Article 5(a) prohibits gatekeepers from combining personal data from core platform services with other sources or from signing in end-users to different gatekeeper services in order to combine personal data, unless the end-user has been presented with the specific choice and consents.

Article 13 obliges gatekeepers to annually submit to the Commission "an independently audited description of any techniques for profiling of consumers that the gatekeeper applies to or across its core platform services".

What is Amnesty calling for?

The prohibition to combine personal data from different sources or to sign in users to different gatekeeper services unless the user has provided consent raises strong doubts as to whether such consent will truly meet the GDPR's requirements of being freely given, specific, informed and unambiguous. Current practice has shown that breaches of basic GDPR obligations are common and difficult to rectify once they occur with lengthy legal proceedings.[37]

With regard to the DMA's provision on an audit of profiling[38] techniques, Amnesty opposes intrusive profiling that relies on ubiquitous surveillance as such practices are inherently incompatible with a range of human rights (such as privacy and data protection, non-discrimination, freedom of expression and thought).

The DMA should affirm the principle that access to and use of essential digital services and infrastructure cannot be made conditional on ubiquitous surveillance and profiling. Gatekeepers must be prevented from making access to their service conditional on individuals "consenting" to the processing of their data for marketing or advertising purposes. Such practices are already contrary to requirements set out in the GDPR, and subject to ongoing legal challenge.[39] Even

---

[35] "In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms." Clément Nyaletsossi Voule, Special Rapporteur on the rights to freedom of peaceful assembly and of association.

[36] Natasha Lomas, TechCrunch, *Antitrust case against Facebook's 'super profiling' back on track after German federal court ruling*, 23 June 2020, https://techcrunch.com/2020/06/23/antitrust-case-against-facebooks-super-profiling-back-on-track-after-german-federal-court-ruling/; Matthias Inverardi, Reuters, *German court turns to top European judges for help on Facebook data case*, 24 March 2021, https://www.reuters.com/article/idUSKBN2BG1PF.

[37] noyb, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*, May 2018.

[38] The term "profiling" under the DMA should have the same meaning as "profiling" defined in Article 4(4) of the GDPR and a specific reference in this regard should be added to the proposal.

[39] noyb, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*, May 2018.

though Amnesty favours strict limitations to profiling practices, at the very least, the audited description of profiling practices should be further specified and include the data which was relied on to create the profile, the purpose(s) and uses of the profiling and specify how data protection principles were complied with including which safeguards were applied.

2. Interoperability

Why is this a human rights issue?

The fact that a few companies dominate the market and act as gatekeepers to the internet and to information allows these companies to impose any, including detrimental, terms of service upon their users. If people want to make use of digital services and exercise their human rights online, such as the right to freedom of expression and freedom of association, they effectively have no choice but to agree to being surveilled, controlled and manipulated by tech companies, thereby signing away their human rights, above all, the right to privacy.

Mandatory requirements for interoperability imposed on gatekeepers are crucial to limit the risks of user lock-in and the network effects that tie users to one dominant platform. Such requirements would allow the development of a more open and pluralistic environment and the emergence of alternative platforms with more user-friendly terms.

What does the DMA propose?

The DMA includes in its Articles 5 and 6 a list of positive obligations and prohibited practices for gatekeepers. The majority of these obligations are focussed on creating better conditions for competition at the business users' level, rather than on creating better conditions for alternative platforms to emerge that give end-users more choice between platforms.

With regard to interoperability requirements, Article 6 prohibits gatekeepers from technically restricting the ability of end-users to switch between and subscribe to different software applications and services to be accessed using the operating system of the gatekeeper. It furthermore obliges gatekeepers to allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware of software features that are available or used in the provision by the gatekeeper of any ancillary services. There is also an obligation to provide effective portability of data generated through the activity of a business user or end-user. However, there is no interoperability obligation that would enable platforms to interoperate with gatekeeper's core services, allowing for communication across platforms.

What is Amnesty calling for?

Amnesty regrets the DMA does not include obligations for cross-platform interoperability that would allow people to connect and communicate across core services and platforms without the need to sign up to the gatekeeper services[40]. Interoperability implemented at the EU-level would

[40] Amnesty International, *Surveillance Giants*; La Quadrature du Net, *For the interoperability of the Web's Giants: An Open Letter from 70 organisations,* 14 June 2019, https://www.laquadrature.net/en/2019/06/14/for-the-interoperability-of-the-webs-giants-an-open-letter-from-70-organisations/; and EDRi, *Open letter demands interoperability of the big online platforms,* 03 July 2019, https://edri.org/open-letter-demands-interoperability-of-the-big-online-platforms/.

ensure that users can move between platforms while upholding their ability to communicate with members of their networks. Strong interoperability requirements would give a true chance for competitors to gatekeepers to emerge, which would enable users to benefit from increased competition and give them a genuine choice between different core platform services. Such competing platforms could distinguish themselves from gatekeepers by providing users with alternatives to surveillance, by offering privacy-friendly terms and better protection of their rights.