MEDIERÅDET
FOR BØRN & UNGE

Input on recurrent and prominent systemic risks in the EU and measures on their mitigation

By The Media Council for Children and Young People, Denmark

This is a response from the Danish Media Council for Children & Young People to the DSA team of the European Commission, regarding the invitation to provide input on articles 34 and 35 of the Digital Services Act (DSA).

The Media Council for Children and Young People is an independent council, formed by the Danish Minister of culture. Its' core tasks include raising awareness and giving guidance on children and young people's media literacy, including their safety, well-being and rights. Furthermore, The Media Council also functions as coordinator and awareness center in Safer Internet Center Denmark (SIC DK), along with Save the Children Denmark (hotline) and Center for Digital Youth Care (Helpline).

Systemic risks and risk factors

This comment responds to question 1 and 3 regarding systemic risks and risk factors. The understanding of systemic risks in this paper is the negative consequences that digital services have, directly or indirectly, on individuals and societies. The understanding of risk factors in this comment is the functions/design/features that enables the negative consequences and risks that are posed. Both systemic risks and risk factors deal with broader themes than just the well-being of children and young people, but in this response, the Media Council will focus solely on this target group.

There will be overlap between the response to question one and three, since it is, in many cases difficult to explain a systemic risk, without including corresponding risk factor(s). For example, it is difficult to explain the systemic risk of Danish children's lack of quality sleep without also addressing the risk factor of user retention on online platforms.

While some systemic risks and risk factors are easy to substantiate with research or other documentation, others are, to a higher degree, value-based and normative. This latter type of risk is also relevant, because it addresses an ideal of how society should protect vulnerable groups such as children and young people. In the physical space, societies and democratic institutions regulate the rules and secure children's safety. In the digital space the same protection and regulation by democratic institutions to safeguard children's rights and keep them safe from harm is of high need.

The comment is structured through the answering of question 1 first, with a total of 6 headlines, then the answer to question 3 with a total of 6 slightly different, but similar headlines, to relate the systemic risks and the risk factors.

Content

**MEDIERÅDET
FOR BØRN & UNGE**

Question 1: Recurring and prominent systemic risks

1. Children's best interests are not prioritized

Children are considered a vulnerable group, and the UN convention of the Child along with the General Comment 25 addresses their rights in the digital environment.

Children deserve and are entitled to having their rights cared for, putting their best interest first.[1] Many digital services that children encounter do not put children's rights first. That leads to children interacting with and on services designed for adults leaving them exposed to many risks – recurring, serious and right infringing. Thus, children are subject to an immense amount of harmful, abusive, offensive content, design and communication, when digital services, that let them onto their service, do not verify age and create age appropriate, rights-based environments suitable for their minor users.

Children participating in digital spaces suitable for adults has an array of possible systemic risks, which can be connected to a general decrease in well-being

Children exposed on adult services
Children participating in digital spaces created for adult expose them for inappropriate, risky and potentially harmful content and experiences. 71 pct. of Danish children aged 12-17 have lied about their age to access a digital service, not meant for children their age.[2]

Harmful and age-inappropriate digital experiences
Children want the positives of e.g. connecting with friends through these services, and many feel that they need to tolerate the negatives of that participation, since the services do not uphold their responsibility for their users' safe experiences. This can lead to de-sensibility and many harmful experiences for children at a very young age, such as access to abusive and offensive content or manipulating designs.

Time stolen
Further, children and adults are increasingly spending time online and on social media that actively work towards retaining their active engagement on their service, leaving less time for and engagement in (and displacing) other activities, that would help increase well-being. Many Danish children say that they spend time they do not want to or even regret, on these services.[3]

---

[1] Livingstone et al. 2024: The best interest of the child in the digital environment, https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf

[2] The Media Council for Children and Young People 2025: Young People's use of Digital Media

[3] Danish Consumer Authority 2025: Young Consumers and Social Media

According to the same report 31 pct. Of Danish teenage girls experience moderate to severe symptoms of addiction.

Thus, there are direct negative effects of children's engagement with services not adjusted to their rights and needs, and there are the negative effects due to the retention causing overuse, which is stealing time from other activities better for general well-being.

Reports show that Danish girls experience lower well-being related to their digital use and feeling retained.[3]

According to a report from 2022, every fourth Danish child between 11-19 years of age have exclusively contact with friends through digital media on an average week, which is worrying in terms of physical, social skills and relationships necessary for them to thrive.[4]

Research also shows that Danish children sleep and move less than earlier, which may be linked to the use of screens and increase in sedentary time with digital media, though this is not scientifically proven.[5]

2. Commercialization of children's digital lives

Children are exposed to commercial content to a huge extent on digital services. This applies to commercial content that we protect children from elsewhere, e.g. unhealthy foods and gambling, commercial content that appears as non-commercial content, e.g. influencer recommendations, and commercial content regarding products that promote inappropriate messages to children, e.g. about wrinkle cream or makeup.

Digital childhood on market terms
The commercialization of children's lives is connected to profit being prioritized over the best interest of children, which is a violation of their rights. It is also a violation of proper conditions for what is considered a good childhood, according to how we in a democratic society protects children in the physical space. In society we have certain values, we build childhood upon, e.g. children are protected against certain risks and harms – through regulation of marketing, age restrictions on certain commodities and distributors held accountable for it, a system for when we notify social services regarding concerns about children's well-being and safety etc. These child-protecting and rights-based systems have yet to be formulated and implemented sufficiently in the digital arenas.

Influencing children's habits in an unhealthy way
A recent count from the Danish Cancer Society shows that children aged 12-17 are exposed to

---

[4] VIVE, 2022: Children and Young People in Denmark, Welfare and Well-being

[5] SDU 2020: The Relationship between Screen Time and Physical Activity and Sedentary Time among Children – A Systematic Literature Review

commercial content promoting unhealthy foods, such as foods high in fat, sugar or salt (HFSS) 26 times a day. Along other health and children's organizations, the Danish Cancer Society stress that the excessive amount of commercial content on digital services influence children's choices, preferences and consumption, which may lead to unhealthy eating habits and increase the risk of overweight. This influences well-being and risk of diseases such as type 2-diabetes, cancer and cardiovascular disease.[6] This trajectory is mirrored in many other areas, such as when children are exposed to content, commercial and non-commercial, promoting unreal body ideals, makeup products and makeup habits, multi-level and network marketing and so forth. These are things, children are exposed to and especially susceptible to, and which can have similar negative consequences.

3. Tracking, manipulation and lack of autonomy

Prediction and manipulation of behavior
Many digital services track users' every move and preference and predict user behavior – e.g. through their communication with others, what they pay attention to and likes, their friends, family and other factors all at once – to make a comprehensive characteristic of users to use in a way that supports their commercial interests.

This means that digital services design includes exploitation of the human psyche via behavioral design. For example, the prediction of one's behavior based on previous behavior is easy to use for influencing people's information during elections or pandemic etc., as well as on a smaller, everyday basis. Based on that the services can predict user-behavior and present users with information and messages that they are highly susceptible to.

Polarization and trajectories of increasingly extreme content
Another way to take advantage of that, is the uses of content recommendation systems and autoplay, which automatically display increasingly extreme content based on user data, at the expense of the user's informed, free choice, time consumption and protection against unwanted and potentially harmful content. Such methods can have harmful effects on individuals and society, as misinformation, disinformation, propaganda and extremist content are pushed forward and can polarize, radicalize and spread socially harmful practices.

No autonomy-by design
This threatens people's possibility to act freely in the digital space and to think and act critically. The power that these digital companies have over people's behavior, opinions, exposure to certain content, political opinion, commercial influence etc. is non-democratic and is a risk for democracies as well as populations and individual rights, health and well-being.

---

[6] Article brought in Altinget the 25th of March 2025: https://www.altinget.dk/sundhed/artikel/syv-boerne-og-sundhedsorganisationer-boern-bombarderes-med-usund-mad-vi-har-brug-for-en-staerkere-markedsfoeringslov

4. Attention based economy, retention and addictive design

Obtaining attention is a type of wealth in the attention economy, where attention is scarce. This is why retention techniques are so widespread – they retain attention, which creates profit. This systemic risk is thus, in addition to the already mentioned above, related to human well-being and time (not) spent on other activities necessary and more supporting for people's well-being and health. Many reports have shown how users spend a lot of time on digital services, also time that they did not necessarily want to spend with that and even regret spending on digital services.[7]

At the same time there is correlating systemic risks posed to national public health, e.g. lack of quality sleep[8], increase in consumption of unhealthy foods[9], increase in sedentary activity / less physical exercise[3]. For children, these risks are also present, and current research shows that overuse of social media is not just related to the individual's capacities. It is related to the media and design as well:

"…the tendency to over-use was far more prevalent among individuals who use social media mainly for viewing content (e.g., TikTok and Instagram) than among those who use social media mainly for chatting (e.g., Messenger and Discord)."[3]

This shows how the design affects user autonomy and how content-focused social media services are designed against the user's best interest and autonomy in their effort to maintain users on their services. The business model many social media are based on rely on the retention of their users, also when they're children. This is why regulation of the functions and design is highly needed, as well as age verification and mandatory age-appropriate design.

5. Discrimination and hate

Minorities and vulnerable groups are more at risk
Digital services can be a catalyzing environment of known harms and targeting certain groups, leaving them more vulnerable and exposed to harms. Minority groups are at higher risk than others of being exposed to discrimination, bullying or hate speech.

In depicting this as a systemic and on-going risk, it is important to notice that minority groups are not a uniform and cannot be reduced to a single group. The diversity amongst minority groups should be a prioritized focus area in assessing and depicting systematic risks.

---

[7] Danish Competition and Consumer Authority, 2025: Young Consumers and Social Media.

[8] National Institute of Public Health 2021: The health and morbidity survey

[9] Danish Cancer Society, 2025: Når skærmen frister /"The temptations on screen"

Minority groups experience more online hate and lower levels of well-being level
A large part of hate speech online consists of hateful rhetoric's regarding ethnicity, sexual or gendered identity markers[10]. A recent study from the Danish research institute Analysis and Numbers maps the tone of voice in the public online debate. It concludes that the majority of hateful comments are aimed at ethnicity or gender-expression.

Other studies have displayed how children and young people in Denmark can be exposed to hate speech, discrimination, racism or bullying. One study published by the Danish Institute for Human Rights and Children's Welfare[11], concludes that over 56 pct. of Danish children has experienced bullying based on their race, nationality, religion or culture in either the physical or digital space.

Other relevant studies concerning discrimination or hate speech in a Danish context includes 'Experience with racism in Denmark' from the Danish Institute for Human Rights[12] or 'Online antisemitism in Denmark' by the analysis institute Analysis and Numbers[13]. A report published by LGBT+ Denmark displays the well-being of LGBTQ+ - children in the Danish public schools[14]. This shows the general well-being of LGBTQ+- children is low in comparison to the average and with many reporting experiences with discrimination in their everyday life.

6. Promotion of risky/harmful behavior and communities

The digital space offers a variety of different communities based on shared interests and self-expression. However, some of these communities can be risky and harmful for children and lead them or groom them towards extremist opinion/behavior and potential radicalization. In relation to this, two systematic risks can be identified. Firstly, the risk of accessing communities and content promoting self-harm[15][16]. In this context, it has been established that current content moderation is not sufficient[17], which puts young females - in particular - at risk for being exposed to self-harm content, and this may lead to the practicing of self-harm. Related to digital self-harm is content, which can lead to distorted and unhealthy body images for children and young people[18]. This can potentially harm children's self-worth, confidence and positive development.

Recently, the risks related to the common use of digital services and radicalization and extremism has been analyzed in Center countering Terrorism Analysis and PET report (2025)

---

[10] Analysis and Numbers 2025: Angreb-og-had-i-den-offentlige-debat-paa-Facebook.pdf
[11] Children's Welfare and Institute of Human Rights, 2024: 2024_05_29_Etnicitet-og-mobbedynamikker_DK_04-1.pdf
[12] Institute of Human Rights 2023: Oplevet etnisk diskrimination i Danmark.pdf
[13] Analysis and Numbers et al 2023: Online-antisemitisme-i-Danmark_2023_endelig.pdf
[14] LGBT Denmark, 2021: Stop-diskrimination-i-skolen-2021.pdf
[15] Digital Responsibility, 2023: Digital-vold-i-Danmark_første-del.pdf - Google Drev
[16] Union against Eating Disorders and Self-harm, 2024: Auto-trolling hos unge - et studie af digital selvskade blandt elever på stx og hf WEB_0.pdf
[17] Digital Responsibility 2024, : Digitalt_Ansvar_InstaHARM.pdf - Google Drev
[18] Sex and Society, 2024: Sex&Samfund_UgeSex 2024_Web FINAL.pdf

'Online platforms and extremist environments in Denmark'[19]. They put forward the following risks – both systemic and factors. The report highlights how the online communication offers anonymity and communication, which is not regulated by physical presence or by criteria's such as, "as geographical distance, age, gender and ethnicity." This can potentially increase the exploitation of minors' and access to international extremist environments. The increased access to these extremist environments should also be seen in relation to technical possibilities, which increases the speed of dissemination and the amount of extremist content. This means that the average users are more at risk of being exposed to unwanted extremist material. The above-mentioned risk factors cannot be separated from the fact that some online communities can function as echo chambers, that can potentially push the ethical and social boundaries of participants, where extremist content, statements and behavior may be perceived by users as normal.

Question 3: Risk factors

This section focuses on question 3 and the factors that enables the systemic risks and potential harms to people and their rights. Thus, this section is focused on concrete elements on online platforms that can be considered risk factors, as well as potential solutions.

7. Not verifying and adjusting to the user's age

Digital services must document how their service is free of significant risks for children and other users in their risk assessment and mitigation measures.

The lack of proper age verification on online platforms is a risk factor. Services must have an age limit that relates to for whom the service is age-appropriate or not age-appropriate, which must be justified in accordance with children's rights and communicated publicly. To enforce the age limits, privacy-protecting, effective age verification is necessary. Furthermore, children of different ages have different needs, in relation to maturity, cognitive development, etc. Therefore, age adjustment, including better content moderation that build on these needs, is required.

The Commission should develop a framework for what is and is not age-appropriate for different age groups, which the services should use as a basis for their age adjustment. To this end, ongoing dialogue between the services and the Commission, national authorities, Safer Internet Centers, etc. is necessary.

---

[19]Center countering Terrorism Analysis and PET report, 2025: Online platforms and extremist environments in Denmark'

Age adjustment will, in some respects, be culturally determined, which is why member states must have a say, for example in decisions about children's exposure to nudity and sexual depictions. In addition, the aforementioned forums can also support decisions about national and cultural contexts and age adjustment to support democratic rights and values supported by the majority of EU member states.

We, the EU and member states, must demand that children's best interest is put first, and the bare minimum, and starting point for this is mandatory privacy protecting age verification systems along with age adjustment.

Risk factors listed: no effective age verification, recommender systems – promoting certain content (e.g. emotion provoking), personalized feed, lack of privacy by default, lack of safety by default, lack of age appropriate design, activity-based notifications such as 'read' or 'typing' notifications, visible social metrics such as likes, autoplay, infinity scroll, AI chatbots acting as friends, beauty filters, rewards for a certain activity that forces users to increased use e.g. streaks or bonuses, fake social notifications, playing by appointment, recapture notifications, time fog, casino pull-to-refresh, grinding, disguised ads, guilty pleasure recommendations etc.

For a scientific source on Attention Capture Damaging Patterns (ACDP) the Media Council refers to the paper by Roffarello et al. 2023: Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces.

8. Commercialisation of children's digital lives

The commercialization of children's digital lives is driven by digital services that target and allow children onto their service. The business-model is often the ad-based one, relying on commercial content and logics to secure revenue. This results in retention techniques (addictive by design), privacy breaches and manipulation of user behavior to maximize use of the service. That is a risk factor since so many minors are using these digital services, also before the age-limits allow it.

In Denmark a report by Children's Welfare (2024) concludes that 48 pct. Danish of children have at least one profile on a social media service before the age of ten[20].

Commercial content today is many things, such as paid partnerships and recommendations by influencers, who children see as trusted role models, competitions and challenges making a game out of a commercial advertisement, advertorials and paid for articles to mention some of the commercial content, that is hard to decipher – especially for children.

---

[20] Børns Vilkår, 2024: Børns liv med sociale medier / "Children's use of Social Media"

Children are entitled to better digital spaces, that support their right to play and participate in the digital environment on their terms, which include minimizing the commercialization and moderating content according to children's needs and well-being.

Risk factors listed: Ads-based business models, lack of age-appropriate design, in-transparency of Advertisement, algorithms recommending popular content, influencers targeting children with advertisements.

9. Harvesting of data, tracking and personalization

The immense harvesting of user-data and lack of choice and impact on what data is collected and how the data is used and shared is a risk factor. The harvesting of data is detrimental to the right to privacy.

A fight on the widespread manipulation is required to ensure the best interests of the child and fundamental rights. The design compromises the users' possibility to choose and act freely – users are not free from hidden commercial agendas. The design influence one's every possible move in the digital space. The existing business models of the very large online platforms (VLOPs) covered by the DSA widely use manipulation and push users' behavior in directions based on the interest of the service, which can violate users' fundamental rights. The users are unable to see the manipulation of them since it depends on the massive and hidden harvest of their data and manipulative design.

It is manipulative when the service provider collects data and adapts the behavioral design to user profiles and behavior without users' knowledge and without the possibility, or for children's sake the default setting, of opting out.

A solution to this would be a better protection of privacy and minor's data and a neutral standard setting, where recommendations and social metrics etc. are switched off by default. Where children and adults have different options to opt into some of these personalized settings. For more on how children's best interest could be default settings by digital services see The Media Council for Children and Young People's ethical guidelines for digital service providers.[21]

Users are unaware of the amount of information services collect and utilize, and how it impacts them – and users can seldom choose freely if and how they agree to any amount of data collection. The data is used commercially in an un-transparent matter for targeting ads, messages and digital surfaces that serves the service's agenda, rather than the users.

---

[21] The Media Council for Children and Young People's Ethical Guidelines for Digital Service Providers, 2023: https://digitaletik.dk/Media/638632882835361423/The%20ethical%20guidelines.pdf

Risk factors listed: Ads-based business models, manipulative design / dark patterns, algorithmic based feeds based on user data and behavior, in-transparency regarding digital design and functions, digital design that manipulate user behavior (retention techniques), algorithmic based recommender systems pushing certain content, insufficient content moderation.

10. Retention at every cost

The business models of many digital services are based on advertising, and this model is not always ethical, as it is based on logics that often conflict with the rights of the child and the users, as mentioned previously. This happens when the business is based on retention, time (and attention) consumption and advertising, and we have seen how this has led to a massive spread of (unethical) methods for retaining users.

For example, the use of content recommendation systems and autoplay, which automatically display increasingly extreme content, which is at the expense of the user's informed, free choice, time consumption and protection against unwanted and potentially harmful content.

The use of social media for children exposes them to the prominent and recurring risk in terms of potential harmful content that affects their wellbeing, life satisfaction and self-worth

Services' content moderation needs to be strengthened, and services need to be held accountable for the protection of children and their encounter with age-inappropriate content.

User-generated content can be a challenge for effective age-appropriateness. One way to give services this responsibility could be to give them editorial responsibility for the content distributed via their services.

The gaps for interpretation need to be filled by the Commission, Safer Internet Centers, child rights organizations and the like, so the services have as small a gap for interpretation as possible. The DSA entails many concepts that are abstract, where definitions by the Commission would help secure children's best interest in the best way. It must be the Commission that sets the standards for child protection and safety, and that evaluates if the necessary risks are mitigated and dealt with appropriately.

Risk factors listed: Pull-to-refresh, autoplay, recommender systems targeting the individual based on data, push of extreme/ engaging content that brings out emotion to maximize engagement.

11. Underlining hateful behavior and harmful communities

The way services' algorithms promote engaging and emotion-provoking content leads the way to how some certain groups are more exposed to hate and discrimination in digital spaces. People may always be categorizing, and some may always lack empathy and tolerance for others, but algorithms should not promote aggressive, angry or hateful content because it

engages people, which is the case today. Design shouldn't reward a certain hateful, polarizing and excluding behavior with exposure. Services must document how their algorithm supports a safe digital environment for all.

GenAI

GenAI and Large Language Models scrape the internet for information and producing content, which is replicating and spreading bias and discrimination, disinformation, misinformation, propaganda and promoting harmful behavior. Therefore, they are considered a risk factor.

Harmful communities

Harmful communities cover users being exposed to hateful content, such as discrimination, racism, hate speech or bullying or content such as self-harm or radicalization.
These systemic risks are influenced by similar risk factors.

The current level of content moderation on many large platforms is insufficient, in that vulnerable groups risk being exposed to the above-listed systemic risks. Therefore, the content moderations systems of online platforms can be considered a risk factor. Likewise, the terms and conditions of a platform can be considered a risk factor. The terms and conditions might be designed in such a way that they allow for discrimination, racism, etc. to occur, or the platform may by unable to properly moderate in accordance with them (insufficient content moderation), so that user will be exposed to this systemic risk.

Furthermore, recommender systems and the platforms push of extreme content to maximize engagement are risk factors that influence how users might be exposed content that intends to promote, for example, self-harm or radicalization.

 Risk factors listed: Faceless communication, algorithmic spread and promotion of extremist content, anonymity, non-moderated or -regulated toxic communities, recommender systems building on maximizing engagement, spread of disinformation, LLM's spreading untrue and harmful information, AI chatbots acting as friends, insufficient content moderation, recommender systems, push of extreme/ engaging content that brings out emotion to maximize engagement, terms and condition

12. Annex 1: List of the risk factors mentioned in this document

List of risk factors mentioned in this comment
1. no effective age verification
recommender systems -promoting certain, e.g. emotion-provoking, content
2. lack of privacy by default
3. lack of safety by default
4. lack of age-appropriate design
5. activity-based notifications such as read notifications
6. visible social metrics such as likes
7. autoplay
8. infinity scroll
9. AI chatbots acting as friends
10. beauty filters
11. rewards for a certain activity that forces users to increased use e.g. streaks or bonuses
12. fake social notifications
13. playing by appointment
14. recapture notifications
15. time fog
16. casino pull-to-refresh
17. grinding
18. disguised ads

19. guilty pleasure recommendations
20. Ads-based business models
21. algorithmic based and personalized feeds based on user data and behavior
22. in-transparency regarding digital design and functions
23. insufficient content moderation
24. push of extreme/ engaging content that brings out emotion to maximise engagement
25. promoting self-harm
26. faceless communication
27. algorithmic spread and promotion of extremist content
28. anonymity
29. non-moderated or -regulated toxic communities
30. spread of disinformation
31. LLMs spreading biased, untrue, harmful information
32. Manipulative design / dark patterns

For more risks we also refer to Stoilova and Livingstone, 2021: The 4C's: Classifying online risks to Children