Position Paper

Making digitalisation work for young people
Introduction

Digitalisation, a phenomenon accelerated by the COVID-19 pandemic, can be understood as the ongoing integration of digital technologies into our daily lives. It has shown its value in bringing together young people from across the continent, amplifying their voices towards peers, towards society at large and towards public institutions. It has allowed young people to connect in new and faster ways, and has brought the sum of the world’s knowledge to their fingertips. Moving towards digital also brings many improvements to young people’s lives, in the form of access to information, new job opportunities, increased convenience and accessible entertainment.

Yet the online world is not without its dangers. Young people today are the first generation to have most of their lives reflected in online data. This raises privacy concerns, including how technology companies gather and use our data, converting our clicks into paradigms of economic and political targeting. It also raises safety concerns, including the extent to which young people are exposed to online harms such as hate speech, cyberbullying, deepfakes or the sharing of unwanted images, such as revenge porn. Similarly, digitalisation raises well-being concerns, including digital fatigue, digital stress, and the difficulty to disconnect.

Whilst young people are the biggest user group of the internet, it should not be assumed this means they have an inherent knowledge of how to navigate it safely. Digital literacy and digital skills are taking their rightful place in European education programmes, but there is a disparity in the level of young people’s digital skills across countries in Europe, especially between urban and rural areas, which risks leaving some young people behind. This is especially true for young people from disadvantaged backgrounds. Being digital today, especially for young people, is no longer really a choice. Without access to the digital world, young people miss out on essential elements of their lives, including most jobs.

The values that underpin the development of the digital world are political; they can and should be deliberately chosen. Currently it can seem that technology companies are steering the key decisions while policymakers and citizens catch up. Europe’s leaders need to decide - together with young people - which values they would like to have reflected in the digital world and work towards achieving them. Legislation at EU level such as the Digital Services Act (DSA), Digital Markets Act (DMA) and Artificial Intelligence Act are first steps in that direction, and the next steps that Europe chooses to take will shape the digital world for today’s young people and future generations.

This position paper details the key challenges surrounding digitalisation for young people in Europe and highlights the demands of the European Youth Forum to address them. We must ensure that young people’s rights are protected, and that we are choosing the digital Europe that young people want.

---


1. **Youth engagement online**

1. a. **Access**

With more and more of young people’s lives shifting to the digital realm, access to ICT tools and high-speed internet is the first necessity for ensuring young people’s digital rights and participation. Some young people in Europe, particularly rural youth, youth with migration and other disadvantaged backgrounds, still do not have proper access to computing equipment or affordable and robust high-speed internet.4

Therefore,

- Governments at all levels should ensure that all young people, regardless of their background or place of residence, have full access to information and communications technologies, affordable high quality internet and should invest in digital infrastructure, such as optical fibre and mobile connection, to ensure their young people are not left behind.

- Education providers must acknowledge varying levels of access to ICT hardware and software, and provide equipment to young people where needed to ensure their full participation.

1. b. **Online civic space**

The digital realm has created a huge range of opportunities for young people to share and amplify their political and societal messages, and for youth organisations to attract members and activists. Compared to other age groups, young people are leading in the use of digital systems to engage in political discussions and have been able to mobilise and organise like never before.5 However, some governments have sought to tighten online civic space through heightened surveillance, abuse of data for judiciary procedures, arbitrary shutdowns or partial constraints on communication. Additionally, a range of political actors are taking steps to limit freedom of speech in the online sphere, either by limiting or promoting particular content moderation decisions.

Equally, when young people are shown a repetition of idealised, heavily airbrushed or disturbing images, this can be damaging for self esteem. Algorithmic spirals can mean that young people see ever more of the harmful content in what has been dubbed “the Instagram effect”.7

Therefore,

- Very Large Online Platforms (VLOPs) must be mindful of the mental well-being of young people, and empower young people to decide how they wish to interact with apps and websites, for example through prompter systems that signal a certain amount of daily use.

- Creators of content should label images of people that have been excessively airbrushed.

4 Serban et al. Social inclusion, digitalisation and young people: Research study.
1. d. Right to disconnect

Whilst all young people should be encouraged to fully access the benefits of the online environment, too much time spent online can lead to digital fatigue and young people feeling like they cannot disconnect. This applies both in the workplace and in educational establishments. In addition, the COVID-19 pandemic period has shown that young people, like all demographics, struggled to stay engaged exclusively online over an extended period of time, which highlights that online activities should not systematically replace face-to-face meetings.

Therefore,

- The EU and national governments should adopt policies ensuring that all young people have the right to disconnect from their workplace and educational establishments outside of working hours and must ensure that this is fully enforced, to safeguard their wellbeing.

- Youth workers and other stakeholders working with young people should consider when physical activities and programmes would be more beneficial and appropriate than online activities.

2. Privacy and safety

2. a. Right to Privacy

As per article 7 of the EU Charter of Fundamental Rights, everyone has “the right to respect for his or her private and family life, home and communications”. Despite advances since the implementation of the General Data Protection Regulation (GDPR), young people continue to see their privacy impacted by excessive data collection, behaviour surveillance, and malicious spyware techniques used in the online world. Some of these aspects are inherent in the business models of tech companies, while some are practised by states. In an age of rising authoritarianism, governments are placing increased restrictions on the civic space available for citizens to enjoy their rights online.

Therefore,

- The implementation of the DSA by VLOPs, search engines, email carriers and browsers should be monitored and supervised properly through the assigned Digital Services Coordinator, bearing in mind the previous implementation issues of the GDPR.

- The highest privacy settings should be readily accessible and transparently available to all users of platforms, browsers, email carriers and search engines, ensuring easy and available opt-out mechanisms for data sharing and content recommendation.

- End-to-end encryption for private messaging services should be the default. Governments at all levels should not allow generalised restrictions to end-to-end encryption technologies for criminal prevention or justice concerns.

- Users must be clearly informed when facial recognition algorithms are being used, and for what purpose, with clear options to withdraw consent.

2. b. Youth-friendly privacy information

Privacy settings on online platforms, search engines and browsers are often presented in an overcomplicated way, spread out over multiple menu categories or difficult to navigate and understand. In some cases this is a deliberate overcomplication (also known as deceptive design), and can extend to the choice of colour, layout, positioning and wording being used to deliberately steer users into accepting settings, or purchases, that they did not want to agree to. Young people deserve to be able to make sound choices in their online lives that ensure their digital safety and enhance their digital wellbeing.

Therefore,

- Technology companies should present privacy settings in a clear and simple way, for example, using videos or graphics, or via in-app support features, so that all young people understand the consequences of their choices online.

---

• Governments should regulate against overt deceptive design features, such as disguised buttons, misdirection and trick questions, in the presentation of privacy choices.

2. c. Content moderation

When it comes to content moderation on websites and social media platforms, young people feel that breaches to community standards are not dealt with fast enough or taken seriously enough. Whilst online posts containing illegal content (incitement to commit a crime, or to violence, sexual exploitation) have clearer rules for being detected and removed quickly, “objectionable” content continues to circulate widely on social media platforms. This applies notably to hate speech, bullying and harassment.

The diversity of content moderation teams is essential, particularly as these teams inform the algorithms sweeping online posts. Notably, the quality of content moderation in languages other than English is lacking. This goes beyond the linguistic element, as knowledge of the local context and social situation is key.

Therefore,

• Technology companies must ensure consistent and accessible methods for user reporting of illegal content; and must provide sufficient capacity for review and for appeal.

• VLOPs must ensure that content moderators are not only English-speakers but are equipped to handle moderation in other languages and cultures. Community standards should be regularly updated to reflect real societal and political developments.

• When the case for content removal is difficult to ascertain, platforms and websites should turn to demotion, demonetisation and flagging in order to protect freedom of speech.

• Users of social media platforms should be empowered to choose if there are certain types of content that they find objectionable and would not like to see on their feeds.

• Platforms should include trigger warnings for sensitive content (e.g. self-harm or eating disorders) to protect vulnerable youth.

3. Collection and use of data

3. a. Minimising data collection

As the age group with the largest amount of personal data circulating online, young people are particularly vulnerable to exploitative data harvesting practices. Young people are not sufficiently knowledgeable about the extent of information held by technology companies that reveals their ethnicity, sexual orientation, political affiliation or religion. Many technology companies are not just using “provided” data but are extracting broader behavioural data from users known as “observed” data and creating profiles on this, known as “inferred” data. This includes information coming from websites external to the application, search engine or platform.

Therefore,

• Use of inferred data extracted from third-party websites should only be used when users actively search for something and must require explicit consent;

• Governments should ensure a strong enforcement of the GDPR and ePrivacy provisions, especially regarding the use of sensitive personal data.

3. b. Commercial advertising

Current practices of behaviour-based advertising rely on inferred data to create user profiles. These profiles, supplemented by information about what friends or similar users interacted with, determine which ads are recommended. As well as being

---


shown emotive content which can heighten desires and contribute to over-consumption, this method can also result in traumatic content being shown to young people.

Young people enjoy spending time on the internet for the opportunities it opens up for them. They should be able to choose what they see on the internet, to enjoy a fruitful and enriching experience there, without being shown unwanted, unnecessary or triggering adverts.11

Therefore,

• Governments should prohibit targeted advertising based on involuntary tracking, personal profiling and inferred data. Contextual advertising, which relies on data provided by people voluntarily and specifically for that purpose, should be preferred.

• Individual users should be able to review and edit what information technology companies are using to select ads and content shown to them.

• The EU and national governments should explore the possibility of third-party recommender systems, which would be interoperable with VLOPs, to allow a decentralised system whereby users are empowered to select which types of content they wish to see and can separate user-generated content from curated content.

3. c. Political advertising

Phenomena such as the Cambridge Analytica scandals have shown the extent to which sponsored political content can have an impact on voting behaviour.12 Micro-targeting certain profiles with certain political content uses data not consented to for that purpose and can limit agency. Young people who are refining their political opinions and voting for the first time in their lives need access to diverse and unbiased information. At the broader democratic level, undue foreign interference through non-transparent funding of political adverts is also a concern for European democracies and election cycles. Nevertheless, civil society actors and youth organisations must be able to share paid content online in order to reach out to new members and supporters, without risking repercussions from governments. Labelling online speech as ‘political’ can pose a risk to civic space, notably freedom of speech, and requirements to publicly display information can risk endangering human rights defenders and youth activists.

Therefore,

• EU legislation should ensure that political advertisements can only target users based on broad profiles and provided data, not using inferred or sensitive personal data.

• Any requirement to label online posts as ‘political’ must be approached by the EU with caution. Clear and robust definitions are needed to avoid an unwanted chilling effect on youth organisations who are trying to promote youth engagement in political and societal spaces, especially when their positions can be critical of governments in power.

• Any requirements to publicly display information about political advertisements must ensure the protection of young human rights defenders and youth organisations.

4. Ethical AI

4. a. Avoiding bias in AI

Artificial intelligence, machine learning and deep learning are bringing huge advancements in pattern detection and statistical reasoning, saving our societies huge amounts of time and facilitating communication and access to information for young people. Yet AI remains weak at decisions relying on common sense or value judgements. There are numerous examples of AI processes resulting in discrimination,


whether based on skin-colour, gender or sexual orientation.\textsuperscript{13} This must be avoided to ensure that young people have equality of opportunity.

Therefore,

\textbullet{} National governments and the EU must ensure that young people have access to the right to explanation, building on the basis already provided by the GDPR. For example, when young people apply for a job, mortgage or benefits via a system that uses AI, they should receive an explanation detailing which parts of the process were subject to automated decisions.

\textbullet{} Technology companies need to be accountable for the algorithms they are using. Non-disclosure to protect business secrets should only be granted in exceptional circumstances.

\textbullet{} Governments, universities and foundations need to dedicate more funds to research on AI in Europe, to refine machine-learning processes to remove bias and - more broadly - to make sure that new AI innovations are fully in line with the values laid down in Article 2 of the TEU.

4. b. Human involvement in critical decisions

Whilst speeding up many processes that would otherwise be arduous for humans, AI is still largely an arbitrary gatekeeper. Too many AI conclusions are based on correlation and not causation.\textsuperscript{14} The so-called “digitisation of judgement”\textsuperscript{15} should not have free reign, especially when this relates to sensitive areas central to young people’s wellbeing. In employment, AI-based systems have sometimes engendered employee surveillance that is too intensive and oppressive, such as 24/7 location monitoring, and tracking of all phone data, under the guise of anti-fraud laws.\textsuperscript{16} When decisions about job allocation, contract termination and appeal are taken by AI, young people’s rights can be negatively impacted.

Therefore,

\textbullet{} Decisions relating to young people’s access to education, employment and housing, need to be classified by the EU as “high risk”, and therefore subject to human monitoring.

\textbullet{} EU and national governments should set guidelines for how and when human oversight of AI processes must be guaranteed. However, recognising that human monitoring of AI systems can be slow and ineffective,\textsuperscript{17} proper checks must be introduced to determine whether automation of certain procedures is suitable, legally compliant, and ethical.

5. Strong digital societies

5. a. Digital skills

With more and more jobs requiring digital aptitude, Europe’s education and training programmes need to equip young people with skills, knowledge and competences that will serve them throughout their lives. With the fast-paced evolution of technology, neither educators nor pupils will be able to keep up with all new developments, which is why complex problem-solving skills should complement digital skills education.

Therefore,

\textbullet{} National and local governments must ensure that the curricula of schools, universities and training institutes across Europe include digital skills and
competences from an early age, moving towards progressively advanced skills.

• Schools, universities and training institutes should commit to imparting complex problem-solving skills, to help young people adapt to future technological advancements. They should also increase awareness of individual rights around personal data and safe use of the internet.

5. b. E-democracy and e-governance

Access to paper-based government processes can be difficult for young people, especially those who are already marginalised, living in rural settings or those with lower literacy levels. Furthermore, young people are amongst the most mobile societal groups, and may be studying abroad or away from their hometowns, making traditional registration and administration procedures difficult. This is also one factor that contributes to a lower voter turnout amongst youth. 18 Securing universal access to a high-speed internet connection, and widened access to digital devices, could open doors for a shift towards digital administration. Increased e-governance facilities, through secure apps and multi-factor authentication, would make such processes more efficient and allow broader access and participation for young people in democratic processes.

Therefore,

• Governments at all levels should examine e-voting systems to allow broader access to voting, learning from best practices within Europe, such as in Estonia and France.

• Governments at all levels should commit to making more public services and administrative procedures available online in the coming years, through secure apps and websites - and ensure public authorities are ready to use them.

5. c. Disinformation and misinformation

Disinformation is a phenomenon grounded in societal interactions, and amplified by the digital world. Social media have allowed the mass sharing of information - including false information - at the touch of a button. Some governments have already deliberately weaponised online disinformation to serve their political aims and to undermine their political opponents. With the advent of deepfake technology, some malevolent actors are creating false videos at a convincing level. Moreover, content recommender systems used by online platforms exacerbate the polarisation of opinions online and amplify sensational content, such as disinformation, to the forefront of young people’s timelines.

Therefore,

• Governments at all levels need to ensure that sound digital literacy and critical thinking skills are embedded in all educational curricula so that the first line of defence against misinformation is users’ recognition and rejection.

• VLOPs must ensure that fact-checkers are equipped to handle moderation of disinformation in other languages and cultures.

• National governments should invest in research into detection software to label deepfake videos.

6. Digitalisation and Sustainability

6. a. Mainstreaming sustainability

Digitalisation can provide many solutions to boosting sustainability, addressing climate change and protecting biodiversity. However, it carries a major carbon footprint itself. If ‘the Cloud’ were a country, it would be the 7th highest consumer of electricity in the world. As overconsumption is one of the main drivers of the current climate crisis, avoiding unnecessary digitalisation will also be an important consideration.

Therefore,

• EU institutions must reassess the logic of the ‘twin transition’; since sometimes being more green will mean being less digital. The carbon

and energy footprint of digitalisation should be mainstreamed into all future digital policies proposed by the European Commission.

- Technology companies must be mindful of their own carbon footprint and must take measures to reduce energy consumption of data centres to move towards climate-neutral data centres by 2030.

6. b. Right to repair

E-waste is the fastest growing waste stream in the world, with only 15-20% being recycled.19 The short lifespan of smartphones, computers, tablets and other electronic devices is a major contributing factor to this. The practice of 'planned obsolescence', when manufacturers deliberately limit the lifespan of devices, block removable parts, and stop providing software updates, pushes young people, like most consumers, to buy more devices than they actually need.

Therefore,

- The EU should legislate to extend the minimum operating life of digital devices, smartphones and other digital hardware to 7 years. During this period, spare parts, software updates and repair manuals must be readily available to customers throughout the EU.

- The EU should legislate to incentivise the design of durable products, which allow easy disassembly and replacement. The cost of repairing a device should not be more expensive than buying a new one.

Conclusion

An empowering digital world

Young people are keen to make the most of the digital world and in many cases are the main drivers of innovation in this area. They are also counting on policymakers to make the online world a safe, open, empowering and inspiring place for them to practise civic engagement, activism, learning and sharing. To do this, they need sound access to ICT equipment and robust internet, and they also need to feel safe and empowered when browsing online. Policymakers and technology companies alike should create a safe space for dialogue with young people and youth organisations to ensure that young people are pro-actively included in decision making processes about further digitalisation.

A responsible digital world

Recognising the influence that the online world has over the lives of young people, governments and technology companies must ensure that online spaces offer young people the choice to see the content that they want. Data extraction and harmful algorithmic practices need to be reigned in to ensure that young people's digital rights are protected. Particularly when it comes to new advancements such as the metaverse or increasingly powerful AI, young people should be consulted thoroughly to ensure that new technologies help to enhance their lives rather than compound concerns around surveillance and addiction. Going forward, responsible digitalisation will also mean that the environmental footprint of new technologies must also be considered, as young people demand responsible consumption in their online lives just as in their offline lives.
