European Digital Democracy: Sovereignty, Rights and Online Safety

Digital and data technologies such as artificial intelligence are transforming our societies. Over 90% of European data is stored on servers controlled by non-EU companies such as Google, Amazon or Microsoft, while five global giants dominate more than 70% of the EU digital market. This dependence threatens Europe's sovereignty, sustainable economic competitiveness, security and democracy. The European Greens call for strong rights-based regulation in order to obtain a digital future based on sovereignty, ethics and fairness, with effective protections for all.

1. A strong need for European digital sovereignty and transparency.

Europe's digital infrastructures and social platforms are dominated by foreign companies such as Google, Apple, Meta, Amazon, Microsoft and TikTok. Moreover, AI systems from both the US and China operate on business models based on surveillance and censorship, putting the EU at risk. With 90% of European data processed abroad, this dependence undermines our sovereignty, economy security and democracy.

Generative AI systems rely on massive data sets that they obtain by the opaque scraping of online data often under violation of copyright. This endangers not just the authors' work but also the protection of personal data and fundamental rights. Even household devices have started collecting personal data, storing and then selling them to third parties without consent. These practices magnify Big Tech's power and further diminish their accountability. The European Greens have championed ground-breaking EU digital legislation such as the GDPR, the Digital Services Act, the Digital Markets Act, the Artificial Intelligence Act and rules on political advertising. These democratic protections are Europe's answer to the power of Big Tech and they must be enforced.

To regain control, the EU and its Member States must act not only through regulation but also through its market power and research and business competence. Public procurement should be used as a lever to support the adoption and scaling of open and interoperable European alternatives to Big Tech. Strengthening open and interoperable technologies can create fairer conditions and allow Europe to develop sovereign digital solutions. By investing in resilient, secure infrastructure and transparent governance, as well as consistently enforcing EU digital legislation, we can create a level playing field, reduce the power of dominant digital platforms, drive innovation and contribute to a more democratic future. The era of untransparent algorithms must end in order for users to regain power. Therefore, we must break big tech's monopolies in the social media infrastructure. Their dominance is based on algorithms that are constantly tracking behaviour, clicks and interactions and that prefer disinformation, polarizing and hateful content over factual posts and pluralism. Finally, Big Tech lobbying must be strongly supervised and entirely transparent, with an obligation to disclose which political parties or political actors are targeting citizens with paid content on their platforms as already the case under the Regulation on transparency and targeting of political ads.

2. Understanding the impact on people´s lives

Digital technologies and social platforms have a profound impact on people's lives. They shape what individuals see, feel and believe, often in ways that are neither transparent nor easily **regulated**.

Vulnerable groups are particularly exposed. Behavioural profiling, targeted advertising and opaque recommender systems amplify risks for people who already face **violence,** discrimination or social and economic insecurity.

Children and young people are especially at risk. European teenagers spend around three hours per day on social media, **where they are served addictive feeds through recommender systems, which** increase**s** their exposure to harmful, explicit and deceptive content. Amnesty International found that TikTok's algorithms can push self-harm and depressive content to teenage accounts within minutes.

Users are also shown this kind of content through chatbots and other generative AI tools. Conversations with chatbots are even less visible to parents and peers than content shown on social media, and users are at risk of emotional dependence on the tool.

AI-driven manipulation has direct consequences on people's lives. Women face a disproportionate threat through deepfake abuse. Around 96 percent of deepfakes are pornographic, with more than 90 percent targeting women. This fuels harassment, blackmail and lasting psychological **and physical** harm.

This shows that the threat is not only who owns the platforms, but how the systems operate and how they exploit emotions, vulnerabilities and even mental health for profit. This is why we need higher fines for multiple violations of the GDPR, AI Act, Digital Markets Act and Digital Services Act to such a level that the fines cannot be factored in as a business risk.

3. Ongoing social and environmental risks

Digital technologies have a heavy ecological footprint. Data centres already consume around 3% of EU electricity and could reach 10% by 2030 (EEA). Especially the production and operation of AI systems demand vast water and energy resources for chip manufacturing and data centre cooling. Chip production by major firms furthermore relies on rare earth minerals, whose extraction causes severe environmental harm. Training large AI models and expanding cloud infrastructures will further increase emissions unless smaller, task specific models are encouraged over larger, general models. Water and energy consumption should be transparently monitored and further energy and water saving regulation considered. A sovereign digital transition must also be a sustainable one, aligned with the Green Deal and the 1.5°C pathway. The development of AI also plays a role in exploiting the labour force. Generative AI models need to be trained in order to eliminate graphic content. This work is often outsourced to click workers, human trainers who are constantly exposed to this content, for extremely low wages. This can severely damage their mental health, leading to post-traumatic stress disorder, depression and diminished empathy.

At the same time, the EU must address the global dimension of behavioural analysis technologies. From mass surveillance in authoritarian regimes to political manipulation from social media platforms and exploitative mining of rare materials, Europe's choices have global consequences. Sovereignty cannot mean isolation: it must mean responsibility. The AI Act needs to be fully enforced, not weakened, in the EU and candidate countries in order to prevent biometric surveillance and AI-driven monitoring of private communication which could endanger privacy and democratic rights in times of an already shrinking civic space. A Green Europe must set standards that protect democracy, human rights and the environment worldwide. Very large data centres operated by non-European hyper-scalers lead to excessive energy and water consumption, driving up utility costs for citizens and local businesses. While this creates only minimal local employment, the massive revenues are transferred abroad. European data infrastructure should contribute instead to the local economy, creating jobs, and ensuring taxes are paid within Europe.

The European Green Party calls for:

1. A European strategy for digital sovereignty and transparency, safeguarding open standards, internet neutrality, ethical AI, radical transparent, effective limits on Big Tech Lobbying at EU level, and strict regulation of dominant platforms.
2. A strong regulation of platform interoperability on social network infrastructure, so that users can access third-party applications and creating genuine transparency about how decisions and recommendations are made, and consent is given. Open source should be promoted and established as EU standard. Create good conditions to support new models of independent and open social networks, based on business models without exploitative data profiling, problematic algorithms, and not controlled by billionaires. The European Commission must fully utilise the powers granted by the Digital Services Act to require changes to platform algorithms whenever systemic risks to public discourse, elections, or media and opinion pluralism are identified.
3. Regulate the concentration of computing power in corporate hands as well as individual and consumer rights with a Digital Fairness Act, the firm protection of net neutrality, and the rejection of chat control technologies.
4. A safe and democratic digital environments as the norm, by switching off engagement-based and hyper personalisation recommender systems by default as required by the Digital Services Act, by banning behavioural profiling of minors, AI-systems facilitating gender-based violence, addictive designs and enforcing algorithmic transparency to safeguard pluralism.
5. Member parties to uphold the current GDPR framework and ensure that data processing is understandable for users and maximally optional.
6. Reject the 'digital omnibus' as presented by the European Commission after heavy lobbying of the tech industry and the Trump administration. This deregulation in the name of "simplification" or "cutting red tape" would weaken citizens' rights and safeguards in the AI

Act, the GDPR and other important pieces of legislation. Instead, implementation, guidelines and handbooks have to be prioritized.

7. Using part of the funds of the European Commission's programme InvestAI meant to mobilize investment in AI gigafactories and the deployment of AI in key economic sectors for developing sustainable, trustworthy~~, open source~~ and sovereign artificial intelligence**, favouring open-source methods.**
8. Support secure EU-wide management and messaging systems for public services, safeguarding critical infrastructure from external interference. Guarantee the right to end-to-end-encrypted communications in the EU.
9. A clear digital signature, ensuring easy identification and traceability for generative AI content
10. Implement protocols preventing the creation of content that encourages emotional dependence, suicidal thoughts or self-harm and referring users to crisis services where necessary. Users always need to know that content is AI-generated when talking to a chat bot or generative AI.
11. Promote a fair and sustainable digital transition by ensuring interoperability between systems and platforms, preventing technological lock-in and guaranteeing users’ freedom of choice through open standards, data portability switching off Generative AI features in search engines by default and security.
12. Ensure human understandable output for large AI systems.
13. Ensure fair taxation and European sovereignty funding, making Big Tech pay what they owe, and guaranteeing that part of these revenues finances the EU digital strategy to strengthen Europe’s sovereignty. Advocate for an EU-wide corporate tax framework, aiming for global adoption through the UN to ensure fair taxation of tech giants.
14. Continue to fight for fair remuneration for artists in Copyright Law. Developments in AI are a risk for the cultural sector; We will examine its impact particularly with regard to fair working conditions and remuneration, personal rights, data protection requirements and copyright law. We want to ensure that authors can enforce their rights and remuneration claims in the future, for example through licensing or levy models.

Background

- 90% of EU data is stored outside the EU — European Commission, European Data Strategy (2023).
- GAFAM control over 70% of the EU digital market — BEUC, Big Tech Market Dominance Report (2022).
- TikTok processes data from 125 million EU users — European Commission, Digital Services Act Factsheet (2023).

- Chinese AI systems (Baidu ERNIE Bot, iFlytek Spark) operate under state-supervised censorship — Reuters, China expands AI rollout under state supervision (2024).
- 96% of deepfakes are pornographic, with over 90% targeting women — Sensity AI, State of Deepfakes Report (2021).
- Amnesty International (2023) found that within 3–20 minutes on TikTok, teenage test accounts were shown self-harm, depression or suicide-related content — Amnesty International, TikTok risks pushing children towards harmful content (2023).
- Meta fined €390 million by the Irish Data Protection Commission (2023) for behavioural advertising without consent, and €1.2 billion by the European Data Protection Board (2023) for illegal data transfers to the US — AP News / EDPB.
- Meta and Google investigated in 2024 for a secret ad partnership targeting 13–17 year olds on YouTube — Reuters, Brussels probes Google–Meta ad deal (2024).
- 73% of European Facebook users classified under sensitive categories (health, religion, orientation) for ad targeting — University of Carlos III of Madrid, ArXiv (2018).
- Over 75% of European voice-scam victims reported financial losses — McAfee, Voice Cloning Report (2023); Europol, IOCTA (2023).
- EU teenagers spend an average of 3 hours per day on social media — EU Kids Online Survey (2022), LSE.
- Data centres account for 3% of EU electricity use today, projected to reach 10% by 2030 — European Environment Agency, Digitalisation and Environment (2022).
- Interoperability, open standards and data portability identified as key to prevent technological lock-in — European Commission, Interoperable Europe Act (2023).