ERASMUS+ YOUTH EXCHANGE / CZECH REPUBLIC

DEMOCRACY 2.0

YOUTH VOICES IN THE DIGITAL WORLD

POLICY PROPOSALS

Six youth-led perspectives on the future of European digital democracy

26 OCTOBER – 4 NOVEMBER 2026

OCHOZ U BRNA, CZECHIA

Co-funded by the European Union

THE PROJECT / 01

Young voices.

Democracy in the digital age.

Democracy 2.0: Youth Voices in the Digital World was an Erasmus+ youth exchange coordinated by Cesta rozvoje, z.s. The mobility brought together 30 young people and group leaders from six countries to explore how digital technology is transforming civic participation, democratic values and the ability of young people to shape public life.

30	06	10
PARTICIPANTS AND GROUP LEADERS	PARTNER COUNTRIES	DAYS OF INTERNATIONAL EXCHANGE

HOW THE PROPOSALS WERE DEVELOPED

Through non-formal education, workshops, debate, intercultural exchange and a simulation of a multi-stakeholder conference, participants explored competing responsibilities across European institutions, national governments, technology companies, civil society and the media. Each thematic group developed its own recommendations, possible compromises and indicators for evaluating progress.

REPRESENTED COUNTRIES

Czechia · France · Italy · Poland · Slovakia · Spain

Why this booklet exists. These six working papers are shared as contributions to discussion with young people, youth organisations and policymakers — not as adopted EU policies.

YOUR GUIDE TO THE BOOKLET

Six proposals.

Six connected questions about safety, rights, participation and trust in the online public sphere.

01	Data privacy for minors	4
02	Disinformation and fake news	7
03	E-voting and inclusion	11
04	Responsible use of AI	14
05	Freedom of speech and online hate	17
06	Cybersecurity and democracy	20

The proposals are presented in thematic order. All targets, measures and indicators represent the participants' ideas and remain open to discussion and refinement.

POLICY AREA / 01 OF 06

Data privacy for minors

01

DATA PRIVACY POLICY PROPOSAL:

This proposal aims to protect the online information of the youth, through the creation of software by tech companies. This can be achieved by limiting the amount of information collected in the first place through cookies. The software won't be forced upon the population, because the responsibility to decide what information is collected falls on their parents.

PROBLEM.

In recent years, with the growth and increasing usage of AI, people's personal data have become less secure and more prone to being stolen through cyberattacks or sold by companies to third parties. This especially endangers the underage population, which we aim to protect.

EVIDENCE.

In the documentary by Carles Tamayo, "It Has Gotten Out of Hand," he infiltrates data broker companies (extremely opaque companies dedicated to collecting, buying, and selling personal information) to discover how our data is obtained, how it is traded, and to what extent all this information can escape the advertising circuit.

In a social experiment, he offered free gasoline in exchange for highly personal information, securing interviews during which people didn't seem to mind sharing such private details. After all, what could possibly be done with them? Carles then used a few of these individuals in his documentary to teach them a lesson: for instance, by approaching them on the street and revealing a wealth of information about them (despite them never having met him) or even by printing one person's face on a T-shirt and putting it up for sale.

GOAL.

The goal of this proposal is to create a safer environment for minors. This goal can be achieved by guiding tech companies to create software that limits the collection of private information through cookies. By restricting websites to collecting only necessary cookies instead of all types (analytical, technical, etc.), we provide minors with another layer of protection against online threats (identity theft, data leaks, and misuse of private information), as their information will not be collected in the first place. The responsibility for implementing this software falls to the parents, who will have to assign their children to their “family group”. Within this group, they can select whether their children are considered minors.

Reduction in the number of cookies collected.
Obligation to allow users to reject all unnecessary cookies.
Reduction in the amount of time websites retain users' information.

MEASURES.

The European Union should discuss this topic within a few weeks and then take action to research statistics on the dangers faced by underage people. It should then take a stand on the protection of minors and collaborate with IT companies that can begin the process of integrating this software into their websites.

The process outlined in this proposal should be completed by the end of 2027.

Following the acceptance of this proposal by the European Parliament, we expect to

EXPECTED IMPACT.

Tech companies are expected to gain a better reputation.

Civil society should take a clear stand in support of this proposal and defend minors who cannot fight for their personal rights.

National governments (the European Council) are expected to help with the implementation of this proposal by supporting or disagreeing with it, thereby raising public awareness about the software.

The European Parliament is expected to protect national security while respecting citizens’ privacy through clear laws and responsible data use.

The media is expected to publish articles, thereby bringing more public attention to the topic.

TRADE-OFF WE ACCEPTED.

Civil society did not need to compromise and accepted every statement in the proposal.

Tech companies compromised by agreeing to implement the measures negotiated in Parliament.

National governments agreed to compromise on the collection of information about their citizens in order to help protect children.

The media partly traded off their ability to understand their audiences' preferences.

The European Parliament compromised by accepting that the statistics they work with would not be as accurate as they were before.

HOW WE WILL KNOW IT WORKED.

Asking family members to complete questionnaires and comparing the results with previous years to evaluate how well the measures are being implemented.

Comparing the number of views on online sites with previous years to determine whether there are more views from “minor” accounts.

RISKS AND OPPOSITION

One of the biggest problems with this proposal is its implementation. Although it depends on the responsibility of parents, we believe that most parents will gladly cooperate. At the same time, the European Union can provide more educational courses to inform its citizens about online safety and the importance of using this software.

It is important to mention that the software does not replace any digital IDs. Furthermore, its misuse by adults is irrelevant, as it will only limit the amount of content they have access to.

Tech companies may object because they would lose data and money, but perhaps we can convince them by highlighting the benefits of gaining a better reputation.

WHERE WE USED AI.

AI was used to correct grammar and improve the structure to make the proposal clearer.

POLICY AREA / 02 OF 06

Disinformation and fake news

02

Policy Proposal: Disinformation and fake news

By: Artem DOBRENKYI, Filip VILAGI, Chiara TURETTA, Hosam MAHMOD, Corina BOHACOVA

1: PROBLEM – WHO IS AFFECTED, HOW, WHERE

Disinformation is defined as false or manipulated information that is deliberately created and spread with the intent to deceive or cause harm.

It affects mainly society (civil society), but also all parties concerned could be affected by disinformation, depending on the objective of the entity spreading the false information.

Fake news have the effect of boosting polarization in the public, disrupting public coercion, manipulation the public opinion of the masses.

Disinformation and fake news occur mainly on the internet, both on social media and through search engines.

2: TWO SENTENCES

Vaccines are not safe, and they are used by governments to inject us with unknown substances. Source: Medical parties who have their own agenda.

The propaganda related to the start of the Russian invasion of Ukraine, claiming that Kyiv is falling within a matter of hours. Source: Russian government

3: GOAL

By 2030, the EU should have an established unified system of journalistic accreditation, measured by the number of accredited fact-checks, online and on social media.

4: MEASURES

National governments;

Recommend, initiate, and pass certain projects to the next legislative procedure to finally form an act or a new law concerning the topic.

Prepare internal prerequisites for the application of the accreditation system.

MEPs;

Recommend, initiate, and pass certain projects to the next legislative procedure to finally form an act or a new law concerning the topic.

The authority to negotiate with the tech companies and state their terms regarding the new legislation.

Formulate the new law project.

TECH;

Platforms used for journalism and information sharing must enhance their fact-checking algorithms to instantly detect AI-generated content.

They have to add a feature for accredited journalists to fact-check the content on their platforms.

CIVIL SOCIETY;

They should work as watchdogs to point out widely spread false information affecting their organisations and societies.

Supporting the new accreditation system, with the resources of their societies and organizations, like media literacy workshops or any other form.

MEDIA;

Offering protection to the freedom of journalists, while simultaneously de-promoting the spread of misinformation.

Validate the new system of accreditation, and help with the testing of it.

P5: EXPECTED IMPACT

National governments;

National governments will be held accountable for their actions, while the level of public trust in them will increase.

MEPs;

Limiting distorted propaganda and false information will result in better representation in the parliament.

TECH;

Gaining better rates of public trust, while getting a better-organized market with investments directed to the right places; Although, they will bear a big share of the burden from the new system.

CIVIL SOCIETY;

They will gain the most positive effects, with access to better quality of news and the ability to distinguish false information.

MEDIA;

They will have the biggest responsibility for both protecting journalism and attacking misinformation, while gaining higher public credibility.

6: ACCEPTED TRADE-OFFs

As mentioned before, the two entities taking the most burdens were media and tech; they accepted the deal in which the unified system of accreditation gives them more credibility.

They will also accept the deal because of the EU's negotiating power.

7: SUCCESS INDICATORS

Collected statistics from the new system will show how well the system works, while independent agencies or organizations collect their own data and publish their own charts.

Surveys about public trust and credibility in the media are also a good indicator of how the system is doing.

8: RISKS & OPPOSITION

Media;

Institutions might not want to cooperate with the new system for the reason of not adding more burden and responsibilities. Solution: Media needs incentives like retribution or penalties to make media adhere to this project.

National governments;

They might not want to give the media this much freedom and power. - By convincing the voting forces, they will take care of it. Solution: By using disinformation against them.

Tech;

They might lobby their way out of the new regulations by relieving the legislatures, or making the formulation of law less binding. Solution: By limiting the effect of lobbies on decision-making.

9: AI USAGE

This proposal was done solely by the group members, and AI was not used in any form during writing this proposal or formulating the ideas.

POLICY AREA / 03 OF 06

E-voting and inclusion

03

E-VOTING PROPOSAL

Introduction:

Allowing young citizens to vote online creates a key opportunity to raise youth participation and simplify voting across EU borders. However, replacing paper ballots with online voting requires clear legal security, strong digital safeguards, and broad public trust. This proposal brings together governments, European representatives, technology providers, civil society, and media to build a secure and fair online voting system.

National Governments

As the European Council, we support introducing online voting in the European Union, but we believe it should be done gradually and responsibly.

We propose starting with pilot projects in several EU member states, focusing on local elections and young voters aged 18 to 25. Online voting should be voluntary, while traditional paper voting must remain available. Our main priority is security. We need strong identity verification, data encryption and independent cybersecurity checks to protect every vote and prevent electoral fraud.

We also believe that online voting could make elections more accessible, especially for young people studying or living abroad.

MEPs

We propose introducing common EU standards for electronic voting to make elections more accessible, secure and inclusive across Member States. A key priority should be facilitating cross-border voting, allowing EU citizens living, studying or working in another Member State. This could initially be tested through pilot programmes involving selected Member States and specific groups, such as EU citizens. MEPs should also encourage innovations such as secure digital voter registration, multilingual voting platforms and accessible applications for people with disabilities. However, these developments must be accompanied by strong safeguards, including independent cybersecurity audits. Particular attention must be paid to protecting ballot secrecy and preventing intimidation, coercion, vote-buying and external pressure.

Tech companies

To keep the system safe, voters are identified securely through the national e-ID, which prevents fake accounts and double voting. The system uses end-to-end encryption and open-source code that independent experts can test. The vote stays secret, and voters can change it before election day, so nobody can pressure them. We also need regular hacking tests, independent audits, transparent recounts and a clear plan if something goes wrong.

To build trust, governments explain how the system works and publish audit results, and the media explain online voting and report on hacking and fake news. The app will be simple, with a few clear steps, large text, several EU languages and accessibility for people with disabilities. Help points and paper voting will always stay available.

Civil society

It's crucial to ensure everyone can participate in the e-voting system, regardless of age, technical skills, or whether they have a phone. That's why we, as civil society, propose creating a network of offline voting centres to ensure equal access for everyone.

These centres would provide computers, internet access, and trained volunteers who could help people understand the voting process without influencing their decisions. But accessibility alone isn't enough; people need to trust the system. That's why we propose three additional measures:

Firstly, transparency. Independent organisations should be able to monitor the voting process and verify that votes are counted correctly without revealing who voted for whom.

Secondly, education. Before introducing e-voting, we should launch public awareness campaigns explaining how the system works, how personal data is protected, and how people can recognise misinformation.

Lastly, protection against pressure. Every person must be able to vote privately and without interference. Voting centres should provide private booths, and no volunteer, official, or third party should be allowed to observe or influence someone's choice.

Media

As Media, our responsibility is to explain to the public how e-voting works while actively watching for manipulation and disinformation.

When we look at youth participation, particularly in Italy, millions of off-site university students and citizens abroad face massive bureaucracy to exercise their right to vote. Digital voting offers a solution, but technology alone cannot guarantee democratic success. Deepfakes, conspiracy theories, and online misinformation campaigns create confusion.

To solve this, our proposal targets a controlled pilot group: university students in representative elections and off-site voters in municipal trials. Identity verification relies on secure systems like Italy's SPID and Electronic Identity Card.

However, technical safeguards only work if the public trusts them. Media can help people by showing simple videos on TikTok, Instagram, and RAI, Italy's national public service broadcaster, so everyone can see that their vote is safe. In addition, to watch for manipulation, independent journalists and fact-checkers must be granted direct access to security audit logs and algorithm data.

Closing:

National governments will establish legal validity and cost efficiency, while Members of the European Parliament set common rules across all EU countries. Tech companies will build simple, secure applications designed to prevent hacking, fraud, and fake accounts. Civil society will make sure no one is left out due to lack of skills or devices, ensuring transparency for all voters. Finally, the media will explain to the public how the online system works and monitor for any digital manipulation. Together, they will launch small pilots for young voters first, protect the system against pressure or abuse, and guarantee an inclusive process.

POLICY AREA / 04 OF 06

Responsible use of AI

04

PROBLEM

Everybody, no matter social status or age, is affected by the abusive use of AI. It affects critical thinking and also the autonomy of people around the world.

EVIDENCE

According to Eurostat data extracted in March 2026, In 2025, a third of people surveyed in the EU had used generative AI tools in the previous 3 months; the highest rates were in Denmark (48%), Estonia and Malta (both 47%), and Finland (46%). Younger people reported using generative AI more than older people; those aged 16 to 24 were the biggest users of AI (64%), while only 7% of respondents aged 65 to 74 had used it.

GOAL

By 2030, the goal is to reduce in a 30% the abusive use of AI among the population. This can be possible with the cooperation of the Tech Companies and the Governments of all EU countries. Annual reports of all AI apps and developers will be the indicator that the measures are working by using samples extracted from the users.

MEASURES

We propose a restriction of the generation and promotion of certain AI content through social media.

Forbid AI promotion in ads, apps, etc.

Make it mandatory for apps and tech to have an option of turning off AI content and research.

Forbid the appropriation of AI content and get it all marked.

More budget and job/university places for people - this way the need of AI is lower because enough human intellection is available.

EXPECT IMPACT

Tech Companies: Reduction of the digital gap between the population and increment of the productivity between the workers and companies.

Media: Increase of the audience's confidence in the media and reduction of fake news.

Civil Society: Use of AI as a tool and not as a second mind. (critical thinking)

MEP's: Emphasis on approvement of budget for AI education, development of digital skills around EU citizens.

European Council: Development of the current measures.

TRADE-OFF WE ACCEPTED

Tech companies can compromise themselves to the application of the following restrictions. The EU council can compromise with the proposition and tracking of the laws. Media compromises on transparency with news and information promoted, also with the sources.

HOW WILL WE KNOW IT WORKED

The indicators will be a reduction of the implementation of AI tools in applications like whatsapp and Instagram, also a more compromised society with the ethical use of AI. Detection tools on algorithms about AI generated text. Improvement in the detection tools on algorithms about AI generated text and pictures.

RISKS AND OPPOSITION

There's no guarantee that society may compromise to these laws - after accepting the laws compromises can be made to accommodate more amount of people. Introduction of the law is the first step, the improvement of the law comes later

Big Tech Companies can be in disagreement with the implementations - they don't have to accommodate whole world, we just agree on their product use and compromise in EU.

The media may oppose it because of the lack of economical resources - budget can be accommodated to media needs - bigger salaries and more job places for human intelligence.

WHERE WE USED AI

Google, it generates answers. We used to research actual non-generational information.

POLICY AREA / 05 OF 06

Freedom of speech and online hate

05

Policy Proposal: Committee 3 – Censorship and Freedom of Speech

Members: Anna Marharyta, Ema, Tamara, Uliana

Your Profile, Your Rights: Stopping Online Hate Together

1. PROBLEM

Online extremist groups actively spread hate speech that leads to real-life physical attacks on minorities. Current content moderation tools cannot catch coded language or private chat groups where people get radicalized. This allows hate speech to hide behind free speech, creating a real threat to human life.

Real story: In October 2022, a radicalized gunman inspired by extremist online rhetoric opened fire outside a known LGBT+ bar in Bratislava, Slovakia, killing 2 innocent people. Investigations revealed that the perpetrator was deeply involved in online hate groups and chat rooms that systematically normalized violence and dehumanized minorities without platform intervention.

2. EVIDENCE

Following the 2022 Bratislava attack, security analysts confirmed that the perpetrator's radicalization was heavily fueled by manifestos, hate speech, and ideological echo chambers hosted on unmoderated digital platforms (Source: EU Terrorism Situation and Trend Report / Police Investigation).

The Digital Services Act (DSA) requires very large online platforms to assess and mitigate systemic risks, including coordinated disinformation, while respecting fundamental rights (Source: European Commission – Digital Services Act).

3. GOAL

By 2027, implement an AI-assisted detection framework across major EU platforms to identify violent hate speech and radicalization networks, significantly reducing response times while protecting freedom of speech through human verification and transparent appeals.

4. MEASURES

National Governments and MEPs: Introduce clear rules to identify manipulated images, videos, and fake information. Require social media and traditional media to check their sources and clearly state when content is misleading. Protect freedom of speech by allowing users to appeal unfair content removals and ensuring that real opinions are not censored.

Technology Companies: Use AI tools to detect manipulated content and fake accounts, introduce verified labels and privacy-preserving age verification for 18+ content, and ensure human review and appeal options for moderation decisions.

Civil Society: Watch over tech platforms to make sure they follow EU safety rules, help targeted individuals and minority groups quickly appeal unfair online decisions, and run community training to help everyday citizens spot manipulated media without resorting to censorship.

Media: The independent research institute will establish editorial guidelines to prevent political interference, with independent media associations reviewing them annually. Journalists will publish explanations of disinformation campaigns and teach audiences how to recognize manipulated images, videos, and misleading headlines.

5. EXPECTED IMPACT

National Governments and MEPs: Stronger platform accountability and better protection of freedom of expression across Member States.

Technology Companies: Clearer moderation guidelines, leading to safer digital spaces and reduced legal risks.

Civil Society: Greater protection for vulnerable groups against online hate speech alongside user-friendly appeal pathways.

Media: Increased public trust, better reporting accuracy, higher awareness of disinformation, and stronger journalistic independence.

6. TRADE-OFF WE ACCEPTED

Civil society agreed to allow strict automatic filtering for violent extremist content and online hate, while tech companies and governments agreed to give independent civil society groups final oversight on user appeals so that peaceful speech, student activism, and minority rights are never wrongly censored.

7. HOW WE WILL KNOW IT WORKED

The aim is to set up an independent institute to conduct research into the prevalence of hate speech online and on social media amongst young people, and to examine the nature of this hate speech (gender, race, nationality, sexual orientation, etc.). An AI tool will be created to effectively analyze large volumes of data. With this institution and the data collected, it will be possible to monitor the effectiveness of our proposals. Furthermore, following an analysis of the data, this institute will be able to produce monthly reports, on the basis of which the working group will be able to analyze the dynamics – identifying what is working and what is not – and provide recommendations on what can be implemented and improved.

8. RISKS AND OPPOSITION

Digital rights advocates and civil society groups may object due to fears that automated moderation tools could accidentally censor peaceful speech or legitimate political debate. We answer this by guaranteeing that all content removals can be appealed to independent civil society panels, ensuring human oversight and protecting freedom of expression.

9. WHERE WE USED AI

We used AI to make our sentences accurate grammatically and lexically. All the ideas above were provided by our team.

POLICY AREA / 06 OF 06

Cybersecurity and democracy

06

A European Shield for Cybersecurity and Democracy

Committee: Cyber Attacks Sector

PROBLEM

Cyberattacks threaten European elections, public services, democratic institutions and the personal accounts of young people across all EU Member States. Attacks such as phishing, ransomware, data theft and coordinated digital disruption can undermine public trust, expose personal information and interfere with democratic participation.

Since cyber threats cross national borders, individual countries cannot address them effectively without European cooperation. The European Union needs a coordinated approach involving European institutions, national governments, technology companies, media organisations and civil society to protect democracy, citizens and public infrastructure.

Real stories:

Public services

The example of the Binance cyberattack on 29 October 2026 can be presented. The hackers stole approximately $6.3 billion in cryptocurrency from the world's largest cryptocurrency exchange. They reportedly exploited compromised company infrastructure to authorise unauthorised withdrawals across multiple blockchain networks. The FBI later attributed the attack to the North Korean-linked hacking group TraderTraitor. This incident demonstrates how cyberattacks can undermine the security of digital financial services, compromise public trust and put people's financial assets at risk.

Personal accounts

Another example is the “Vote for my relative” scam, which spread through WhatsApp. People received messages from friends or family asking them to vote for someone's daughter or another relative in an online competition. The link led to a fake website where they were asked to enter their phone number or login details. Once they did this, hackers could steal their WhatsApp accounts and access their private information.

This shows how cyberattacks could affect ordinary people, especially young people, by taking advantage of their trust in friends and family. Scammers could also use stolen accounts to send the same messages to more victims.

Democratic institutions

In 2022, just hours after the European Parliament declared Russia a state sponsor of terrorism, the official website of European Parliament was aggressively knocked offline by a pro-Kremlin DDoS attack. This proved that hacktivists target democratic institutions in real-time during critical political voting.

EVIDENCE

According to ENISA, 586 publicly reported cyber incidents targeted public administration in the EU during 2024, with DDoS attacks accounting for nearly two-thirds of these incidents.

Furthermore, ENISA’s 2024 Threat Landscape identified public administration as the most targeted sector, representing 19% of reported incidents across the sectors analysed.

GOAL

By 2030, all 27 EU Member States should participate in a stronger and more coordinated European cybersecurity framework. The European Council should encourage common political commitments to improve cooperation during cyberattacks, protect elections and democratic institutions, and strengthen digital literacy among young people.

The framework should also ensure that technology companies take greater responsibility for cybersecurity, that media organisations can provide reliable information during digital crises, and that civil society participates in monitoring the protection of citizens’ rights.

MEASURES

First, the European Council should promote a European Cyber Crisis Coordination Mechanism. The European Council should encourage all 27 Member States to strengthen cooperation and establish common procedures for sharing information and providing mutual assistance during major cyberattacks. The European Commission should coordinate the implementation of this framework with national cybersecurity authorities and existing European cybersecurity structures. National governments and their cybersecurity response teams should remain responsible for operational responses within their territories while cooperating with other Member States. The framework should be politically agreed upon by 2027, with annual European cybersecurity exercises beginning in 2028.

Second, the European Parliament and European Commission should support a European Election Protection Programme. National governments and electoral authorities should conduct regular cybersecurity risk assessments to protect electoral infrastructure against hacking, foreign interference and digital manipulation. The European Parliament should strengthen democratic oversight and encourage common minimum security standards, while the European Commission should provide technical support and coordinate cooperation between Member States. The first coordinated European election-security exercise should take place by 2028, while respecting the different electoral systems and national responsibilities of each Member State.

Third, national governments should introduce a Youth Digital Safety Initiative. Governments should work with educational institutions, civil society organisations, youth organisations and media organisations to provide accessible digital literacy education. These programmes should teach young people how to recognise phishing attempts, protect their personal accounts, identify identity theft, recognise AI-generated scams and respond to online manipulation. The European Commission should facilitate cooperation and provide educational resources, while the European Parliament should support awareness initiatives and funding. The programme should begin in 2027 and be evaluated annually.

Fourth, the European Commission and European Parliament should strengthen Corporate Accountability.

They should work with the Council of the EU and relevant national regulators to ensure that technology companies take responsibility for protecting their platforms and users. Companies should be expected to improve data security, report serious security breaches within applicable legal deadlines, cooperate with cybersecurity authorities and provide transparent information about major security incidents. Independent technical audits and regulatory supervision should help ensure compliance. Existing European legislation should be reviewed by 2027, with any necessary improvements to regulatory requirements introduced during 2028–2029.

Fifth, European institutions should establish a Media and Democratic Resilience Programme. The European Commission and European Parliament should encourage cooperation between public and private media organisations, independent journalists and fact-checking organisations to improve public awareness of cyber threats and coordinated disinformation campaigns. Media organisations should provide accurate and responsible information during cyber incidents without compromising their editorial independence. Training programmes and public awareness campaigns should begin in 2027, with annual evaluations of their impact.

Finally, the European Parliament and national governments should strengthen the participation of Civil Society in cybersecurity policies. Civil society organisations, digital rights groups and independent experts should be invited to participate in public consultations and monitor the effects of cybersecurity measures on privacy, freedom of expression and other fundamental rights. The European Commission should facilitate these consultations, while the European Parliament should provide democratic oversight. A common consultation framework should be established by 2027, followed by the first independent public assessment in 2028.

EXPECTED IMPACT

The European Council and national leaders should benefit from stronger political cooperation, shared responsibility and more coordinated responses to major cyber crises. The European Parliament should be able to strengthen democratic oversight and ensure that European cybersecurity policies remain accountable and transparent. The European Commission should improve the implementation and monitoring of common European policies.

National governments should become better prepared to prevent and respond to cyberattacks, while technology companies should adopt stronger security standards and become more accountable for protecting users' data. Media organisations should be better equipped to provide reliable information and resist coordinated disinformation campaigns. Civil society should have greater opportunities to participate in policymaking and independently monitor the protection of citizens' rights. Finally, young people and other European citizens should become more aware of digital risks and better protected against online threats.

TRADE-OFF WE ACCEPTED

We accept that stronger cybersecurity requirements may increase financial and administrative costs for national governments and technology companies. We also recognise that greater European coordination may raise concerns about national sovereignty and the distribution of responsibilities between European and national institutions.

However, we believe that collective security and democratic stability justify proportionate investments and stronger cooperation. At the same time, cybersecurity measures must not become a justification for mass surveillance, censorship or restrictions on freedom of expression. All policies should respect privacy, transparency, proportionality and fundamental rights.

HOW WE WILL KNOW IT WORKED

We will evaluate the success of this proposal through measurable indicators. We should monitor whether successful cyberattacks against public institutions and election infrastructure decrease and whether governments become faster at detecting, reporting and responding to major incidents.

We should also measure whether all 27 Member States participate in regular joint cybersecurity exercises and whether national electoral authorities conduct regular security assessments. The effectiveness of youth education programmes should be evaluated by measuring participation and improvements in young people's cybersecurity knowledge.

Furthermore, we should monitor technology companies' compliance with European cybersecurity requirements, the participation of media organisations in digital literacy initiatives and the involvement of civil society in independent monitoring and public consultations. A progress report should be published annually, followed by a comprehensive evaluation in 2030.

RISKS AND OPPOSITION

Some national governments may oppose additional financial commitments or stronger European coordination because of concerns about national sovereignty. Political disagreements may also arise between European institutions regarding the balance between security, democratic oversight and national responsibilities.

Technology companies may resist additional regulatory obligations because of increased compliance costs. Media organisations may be concerned about political interference and threats to editorial independence, while civil society organisations may raise concerns about surveillance, censorship and the misuse of cybersecurity policies.

To address these concerns, the European institutions should promote transparent decision-making, proportionate regulations, independent oversight and regular consultations with national governments, technology companies, media organisations and civil society.

WHERE WE USED AI

AI was used to help identify possible cybersecurity measures, and improve the clarity of the text. The final recommendations and policy priorities were reviewed by the committee members.

BEYOND THE YOUTH EXCHANGE

From debate to dialogue.

The purpose of these proposals is to open conversations — about which digital protections young people need, which opportunities technology can create and where rights must shape public policy.

PUBLICATION AND EDITORIAL NOTE

This edition keeps the participants' policy texts in their original wording. Headings, chapter titles and layout are editorial. The proposals, targets, examples and claims represent participants' ideas and have not been independently fact-checked or adopted as EU policies.

THE SIX THEMES

PRIVACY · DISINFORMATION · E-VOTING · AI · FREEDOM OF EXPRESSION · CYBERSECURITY

PROJECT COORDINATION

Cesta rozvoje, z.s.

Ochoz u Brna, Czechia | 26 October – 4 November 2026

Co-funded by the European Union

The people behind the proposals.

The policy papers in this booklet were developed through the collaboration, debate and creativity of young people taking part in Democracy 2.0: Youth Voices in the Digital World. We acknowledge the following contributors, as provided by the project team.

Corina Bohac, Daryna Khomechko, Uliana Shkurkina, Milla Yakymenko, Kateryna Omelchenko, Cecilia Maria Collu, Erica Barbieri, Letizia Canosa, Chiara Turetta, Anna Sparaco, Ewelina Cudinowicz, Marharyta Kamianetska, Filip Lisowski, Artem Dobrenkyi, Matvii Matviienko, Mykhailo Hriaznov, Renata Koneva, Ingrid Hlavandová, Tereza Filipovičová, Ema Zimermanová, Tamara Polláková, Filip Világi, Martin Drdák, Fatemeh Sanaatian, Gwendoline Martínez Ble, Paula Canalda Sorribas, Alexia Gabriela Radu, Carla Mercé Escura, Oleksandra Balaban, Vladyslav Khahai.

These are collective credits; the booklet does not attribute individual contributions to a specific committee.

EU FUNDING DISCLAIMER

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Czech National Agency for International Education and Research. Neither the European Union nor the granting authority can be held responsible for them.