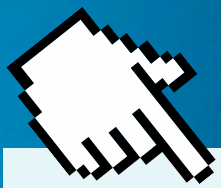
Liberal solutions for a Digital Europe

EUROPEAN LIBERAL YOUTH
LYMEC

elf



"Published by the European Liberal Forum in cooperation with The European Liberal Youth (LYMEC). Co-funded by the European Parliament. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum."

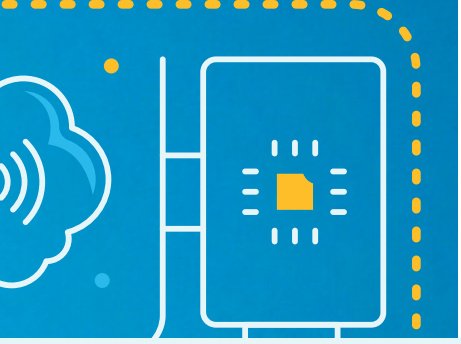
Table of Contents

Introduction

The concept of hackathons can be traced back to software engineering, where the ultimate goal is to create a functioning product through sprint-like designs by the end of a short period, usually 24 to 48 hours. In the case of the **ELF Event 'Liberal Hack 2022'**, held in Vienna from 28 to 30 October 2022, the aim was to come up with concrete liberal policies which would benefit the digitalisation of the European Union as a whole.

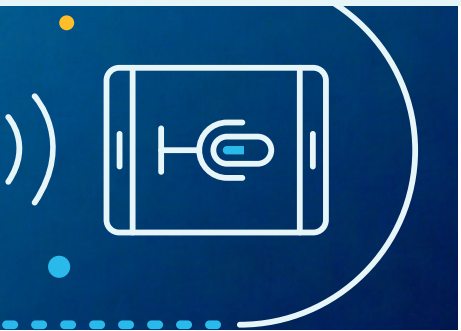
The Liberal Hack 2022 aims to challenge the young liberal participants to explore how the EU can become a global leader in a fair and democratic digitalisation process, while being competitive and developing cutting-edge technology. A hackathon with four teams of young liberals from all over Europe discussed proposals for a safe, liberal and digitised environment in Europe, focusing on four key technologies that will potentially bring a significant social transformation: **Artificial Intelligence** (AI), **Augmented Reality** (AR), **Blockchain**, and the **Internet of Things** (IoT). They focused on one specific technology and challenge to find an actionable policy solution.

The Liberal Hack was organised by the **European Liberal Forum (ELF)** with the support of **LYMEC (European Liberal Youth)** and their Austrian partner **NEOS Lab**. The aim was to challenge the hackathon's participants to take an active part as young liberals in shaping Europe's future in digital politics, a topic that is of special relevance and interest to the young generation and the Liberal stakeholders in Europe.



Each team had two hours of **"hacking time"** on the first day of the event, to start their policy proposals off from scratch. After several hacking sessions, the young liberals who took part in the event were finally ready to present their policy-oriented solutions to the jury. The jury consisted of LYMEC Vice-President **Ines Holzegger**, ELF Research and Policy Officer **Francesco Cappelletti,** and NEOS Lab Policy Coordinator **Dieter Feierabend**. Each team gave their best in presenting their ideas. Consequently, the points awarded were extremely close, but **the winning team was the Augmented Reality Group**. They presented solutions on how to make AR better regulated and safer for users in the EU. All the groups succeeded in following the guidelines and correctly answering the aim of the hackathon by designing an actionable, coherent, innovative and liberal policy to tackle their chosen challenge. It was overall a competitive but thus successful hackathon.

In the following pages, you will find all the detailed policy solutions the Hacking Groups came up with. Aside from the Augmented Reality proposal, winner of the Hackathon, the other outstanding ideas were: the "ballot chain", which proposes a European blockchain technology for safe elections presented by the Blockchain group; the clear and concrete path which the Artificial Intelligence (AI) group put forward as they proposed a way to use AI to our advantage, and not letting it become a threat to us; and the Internet of Things (IoT) group, which advanced the implementation of EU-wide tax reliefs for investments in European IoT start-up and scale-up companies, as well as crowdfunding platforms supported by the EU.



What is the aim of this booklet?

The aim is to creatively discuss ways to implement **A Europe fit for the Digital Age**, presented by **Margrethe Vestager** (Executive Vice President of the European Commission), from a variety of angles. We want to challenge our young liberal participants to explore **how the EU can become a global leader in a fair and democratic digitalisation process**, while being competitive and developing cutting-edge technology, and how it can be implemented at all policy levels (local up to European). The overall goal is to make the EU a truly global cyber-power that brings a positive perspective on global digitalisation, so that we avoid ending up with a technological Cold War between two non-communicating systems, namely the American and Chinese ones.

As the voice of young liberals in Europe, LYMEC wants to take an active part in **shaping Europe's future in the sphere of digital politics,** a topic that is of special relevance and interest to our generation. With the rapid spread of **disruptive technologies**, such as new communication technologies (5G and 6G), Artificial Intelligence applications, quantum and cloud computing, we have to come up with an inclusive and innovative strategy that leaves no one behind, protects our data and privacy, while preserving global communication. **We want to create a roadmap** for this strategy with the final goal of having the EU as a global digital power.

In this framework, LYMEC aims to develop **a set of policies focusing on digitalisation**, with liberal principles and values at its core. The conclusions of this booklet are distributed and advertised, among the network, to have an impact on the broad audience of LYMEC with the aim of creating a general understanding on digitalisation.

The booklet provides **insights about the four technologies tackled during the event**, their effects on the digital gap, as well as tips and advice on how to be better prepared for the future and how to acquire the relevant digital skills needed to excel.

Artificial Intelligence

Group members

- **Ari Habeshian** (NEODEPA, Cyprus)
- **Valerija Kozikaitė** (Lithuanian Liberal Youth, Lithuania)
- **Andrei Taga** (USR Tineret, Romania)

The Internet and Social Media platforms have become more and more fundamental in our lives. We spend a significant part of our time on our devices and often receive lots of news that is unfortunately not filtered. Young liberals believe that **every individual should be aware of the difference between real and fake news**. For instance, 40% of Europeans accidentally shared fake news last year and only 1 out of 4 declared that they can easily recognize fake news. As we all know, social media is lately being used as a propaganda tool by Russia, China and even Belarus to spread misleading information. This kind of news turns out to be extremely dangerous to everybody, especially to the elderly and the young audience. Furthermore, it brings mistrust to journalists and news outlets by creating unnecessary stress and anxiety to the society as a whole.

What is fake news?

Fake news **intensifies social conflict** and **creates division** in the society between the ones who blindly believe what is given to them by the media and the ones who think twice before trusting any article or media outlet. Also, it **creates mistrust to journalists and news informers**. In addition, sometimes governments use fake news to distract people from important issues so that these issues remain unresolved. Finally it generates stress, anxiety, worrying about the future and, in extreme cases, isolation.

How can we tackle fake news?

In light of this brief introduction, young liberals see the **Fake News Detector** as a possible solution to this major issue. The Fake News Detector is a **software update** for all computers and mobile phones **that will highlight the misleading information on a browser** using the principles of Artificial Intelligence, thus showing the **percentage of fake information** contained by a specific article. Through a **fact-checking AI process**, the software would simply check if the information on the webpage of the article corresponds to real facts.

How does it work?

The key liberal feature of this software is that **people can freely choose whether they wish to receive the update on their devices or not.** Moreover, once the software and correlated updates are installed in the device, people can still choose whether they want to rely on the outcome or not. They are totally free to use the information as they prefer. The European values represented by this tool are **democracy** (anti-propaganda tool, free choice), **human rights** (the right to be informed), **equality** (equal information for everybody) to achieve a well-informed public who is capable of distinguishing reliable sources on one side, and more responsible journalists on the other side.

We envisage four stages of implementation:

1. **Exploration:** identifying the need according to the existing data. The team working on this policy solution already did that and found out, based on the surveys conducted in the EU on fake news, a tool like this would come in handy.

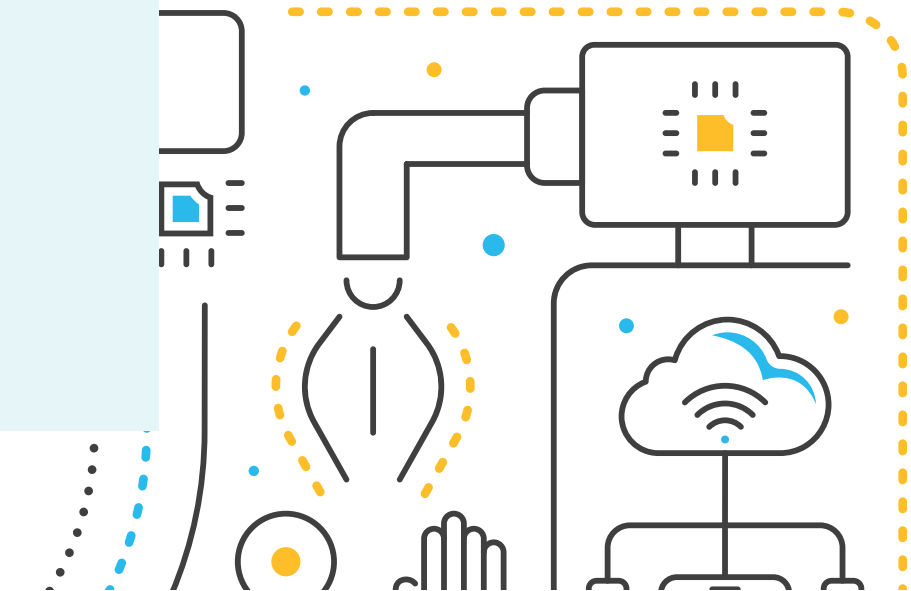
2. **Installation:** gathering IT specialists, creating the actual software and testing it out.

3. **Initial implementation:** planning the steps for the full implementation and check if there's room for improvement. Moneywise, the official EU digital budget for 2021-2027 is 7.6 billion EUR, therefore in this context, we would estimate the cost of this project at 250 million EUR with a possibility for additional funding from relevant NGOs or businesses in the IT sector.

4. **Full implementation:** implementing the software at the broader EU level. We imagine this to become in the years to come a common European feature, proposed to all EU citizens, not forcing states to implement this by law.

Result

To conclude, the **Fake News Detector software** could tackle most of the problems that we are used to experiencing on a daily basis when it comes to fake news, making it clear which media sources promote fake news and in which percentage. It also gives the chance to the citizens to **think critically**. The general audience will be more aware and think twice before trusting news on social media.



Internet of Things

Group members

- **Toine Schouteten** (LYMEC Individual Member, The Netherlands)
- **Maciej Witek** (Nowoczesna Youth, Poland)
- **Kyra van Rossum** (JOVD, The Netherlands)

What is it?

The **Internet of Things** (IoT) refers to a "distributed network connecting physical objects that are capable of sensing or acting on their environment and able to communicate with each other, other machines or computers". Basically, it refers to what we can call 'smart objects' (European Parliament, 2015).[1] Examples of objects that you can think about are smart home appliances that you can turn on and off on your phone, like smart lamps, blinds, washing machines etc. Other than that, IoT is also used in the context of city management (for example regarding traffic lights and public transport).

The IoT market

When looking at the major players in IoT, the **European IoT market** is currently almost entirely **supplied by non-European parties**, namely **American and Chinese companies** (for example Apple and Huawei). The European IoT market has no major European participants yet. The challenge that we are therefore facing within Europe has to do with geopolitical instability (CBI, 2022),[2] in the case of the USA and China personified by Donald Trump and Xi Jinping respectively. According to young liberals, **the EU should reassess the structuring of its current and future IoT market**. Therefore, we are presenting an innovative policy solution for the future.

Liberal measures

We propose three measures in this area: **EU crowdfunding** platforms should be founded, preferably supported and partially financed by European financial institutions such as banks. Said platforms are almost entirely focused on their own national market. **Cross-border investments** through EU crowdfunding platforms will benefit the European IoT market. We also propose an implementation of an **EU wide tax relief scheme**, and we suggest that European policy should focus on storing all data at the lowest possible level through the subsidiarity principle. European data should not leave Europe in general, but ideally it should not even leave the country of its origin or the local network.

How does it work?

Thanks to the **EU wide tax relief scheme**, individual Europeans can invest in IoT companies and subtract their investment as costs from their national taxable income. This will make sure that the "average European" can take part in the new drive for European IoT champions. Examples of this that already exist are the UK relief schemes[3] and the Belgian tax shelter.[4] When it comes to **storing all data at the lowest possible level**, we aim at achieving that through **network encapsulation**. We propose to demotivate the movement of data between the following layers by **taxing per byte**, whereas movement of data within the layers should be allowed 1) within a company; 2) between companies within Europe; 3) between companies, of which one is outside Europe.

Result

The growth of **future European IoT key players** should be boosted in a European liberal way, the latter meaning that the market should be allowed to function with government interference playing a minimal role.

Augmented Reality

Group members

- **Andrei Dan Olaru** (USR Tineret, Romania)
- **Livia Ilse Maria Schorno** (JOVD, The Netherlands)
- **Makar Navitski** (Estonian Center Party Youth, Estonia)

What is AR?

Augmented reality describes technological products that **combine the real world and computer-generated content**. The content can span multiple sensory modalities, including visual, auditory, haptic, somatosensory, and olfactory. AR incorporates three basics features:

1. A combination of real and virtual worlds;
2. Real-time integration;
3. Accurate 3D registration of virtual and real objects.

The overlaid sensory information can be **constructive** (additive to the natural environment), or **destructive** (masking the natural environment).

The primary value proposition of augmented reality is the way components of the digital world blend into a person's perception of the real world, not as a simple display of data, but through the integration of immersive sensations, which are perceived as natural parts of an environment.

Major Challenges

- **Hardware issues:** AR headsets have bulky hardware that may also be too expensive for the general public;

- **Lack of regulations:** currently, there are no regulations to govern the usage of augmented reality.

- **Privacy and data protection:** AR devices capture the real-world scene, analyse it, and then overlay additional visual information to augment reality. Therefore, data collection is an integral part of how AR works.

- **Hacker attacks and security**: despite its many advantages, AR technology is vulnerable to security threats and various types of cyberattacks. For example, hackers could misdirect a vehicle using an AR-enabled navigation system and use it to cause an accident.

- **Increased cognitive load:** AR is perceived as cognitively demanding and can lead to poorer performance (Buchner et al, (2021).[5]

To dive deeper into the lack of regulations and privacy, there are no guidelines for AR developers to secure users' privacy yet. AR devices collect similar data as other consumer technologies, but raise new privacy issues regarding the variety of technologies involved and the sensitivity of the information. It also collects extensive biometric data, which can identify and infer additional information. This data can create better immersive experiences, but also exacerbate privacy risks. The immersive nature of AR makes it difficult to mitigate risks by applying existing privacy policies and practices from other digital media. It requires innovative new approaches to transparency, choice and security.

As regards the increase of cognitive load, a majority of studies reported positive effects of AR use on mental workload and task performances when compared against conventional methods. AR helps to reduce extraneous cognitive load and increases germane cognitive load. Germane load refers to the mental resources devoted to acquiring and automating schemata in long-term memory. For example, companies could influence the germane load and eventually the long-term memory of users by selecting which information is shown on the smart-glasses.

The biggest risk arises at the intersection of a lack of regulation on privacy and cognitive load. With vast amounts of data about us and the ability to direct our focus as they please, companies can exploit our mental health vulnerabilities, guide our belief system and construct in time our entire mindscape, all to suit their short term and long term profit-making interest.

What is the solution?

The liberal solution focuses on regulating the burgeoning market of smart-glasses in particular. Whilst these regulatory elements fail at solving the whole problem, they do minimise it significantly and constitute a good first step in the uphill battle against corporate control over citizens' minds and their privacy.

These regulations have been chosen to:

- Have little to no administrative footprint - it is hard for institutions to fail at implementing them;
- Offer little to no room for loophole exploitation. They are simple, to the point, clear and robust.
- Slow down innovation as little as possible.

How does it work?

Cognitive Overload Awareness Training

The first time a user starts using a new visor or smart-glasses device, the setup process will contain **training created by educational professionals** together with **neuroscientists** and **psychologists**. The training will ensure that users are aware of the real dangers of cognitive overload.

Content Toggles

Every notification source and content source will be by default off. Users will be asked if they wish to receive content or notifications from that source one time only or all the time. The UI will have to be developed so that any notification or content source can be toggled off at any point in no more than 3 actions (ex: enter settings, select source, hit toggle). The purpose of this particular regulation is to allow users to **exercise the awareness** developed through the training they received towards customising their AR experience to suit their mind and desires.

Data Manipulation Regulations

- **Forbidding the storing of personal data** (location, facial expressions, environmental sounds, recordings of what is in the person's field of view, movement patterns etc.);
- **Prohibiting any form of cloud processing of data:** even real time language translation needs to be processed on device;
- **Banning any form of transmitting unencrypted data:** if you are in a virtual meeting with a colleague, data transmitted (sound, facial expressions, movement etc.) will be encrypted and only accessible by your colleague.

This restricts the ability of companies to collect data about us, infringing our **right to privacy** and then instrumentalising their insight towards manipulation. Second, by banning off-device processing of displayed content, we further make sure users' data cannot be aggregated. Finally, this also limits companies' ability to push context and the economic exploitation.

Signal what is not real

With technological development, 3D items rendered by AR glasses will become more and more photo-realistic. To prevent a future in which accidents happen from people confusing real objects from virtual ones, and a future in which kids' brains are affected in their formative years, every virtual item will have to be signalled as virtual through a clear outline or a clear symbol.

Field of Vision Protection Regulations

As a result of neurological and psychological studies, the field of view will be restricted to the maximum deemed as healthy, even in case of long term exposure. This will further restrict the ability of companies to damage citizens' mental health by overloading their cognitive space.

Result

To sum up, by forbidding the transfer of non-encrypted data, we make sure that even when it's in the user's interest to send data (ex: a remote meeting in which speech, facial expressions and physical positioning need to be sent to other meeting members), that data reaches only the people they want it to reach and only to the extent the user intends to.

Blockchain

Group members

- **Brit Maria Villand** (Estonian Reform Party Youth, Estonia)
- **Nima Hairy** (Jeunes MR, Belgium)
- **Felix Barenthien** (Junge Liberale, Germany)
- **Akim Kibonovskyi** (Liberal Democratic League of Ukraine, Ukraine)

Finding EU solutions and Ideas in the Area of Blockchain is a hard task: since we are so early in the development of this technology, a lot is yet to be paved.

What's wrong with the Blockchain?

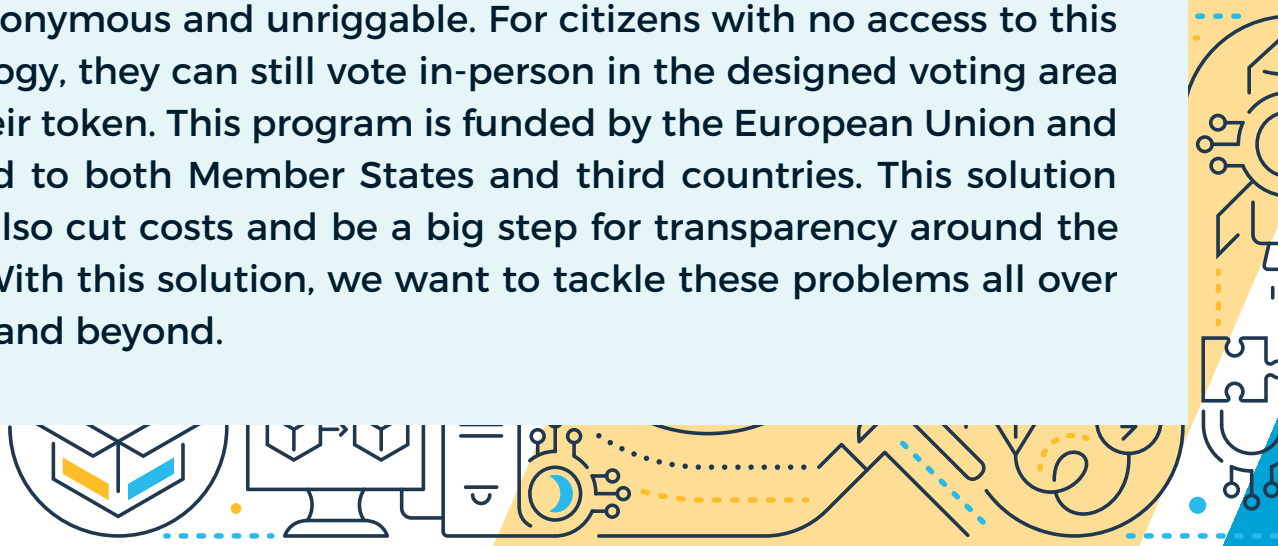
Blockchain and cryptocurrencies in the public sector are often deceived of being risky and not trustworthy enough. In this group, we looked for solutions on how the European Union can work on projects that can expand blockchains' full potential, as well as raising the trustworthiness towards Technology.

The Ballot chain

That's how we came up with the ballot chain.
The **ballot chain** is an **EU program and long term flagship project**, working on **decentralising and securing elections**. Trust in elections and in voting is sinking more and more in some countries. In other countries, instead, it's not even sure how long democracies will still be able to last. Implying democratic and secure standards can be a challenge in many countries, as they don't have the election infrastructure or the funds to perform the elections properly.

How does it work?

The idea is that every eligible voter owns a wallet. In this wallet, they receive tokens which they can use on the given election. The vote stays anonymous and unriggable. For citizens with no access to this technology, they can still vote in-person in the designed voting area with their token. This program is funded by the European Union and provided to both Member States and third countries. This solution would also cut costs and be a big step for transparency around the globe. With this solution, we want to tackle these problems all over Europe and beyond.



Conclusion

One of the main problems affecting the digitalisation of our European society is the digital gap. Without digital skills, no economic progress will be possible, especially among young people. The technology is there, but a youth-centred plan for its management is not. Young liberals call for ensuring appropriate digital education, in order to equip the young people of Europe with competitive skill sets of the 21st century.

Bibliography

1. European Parliament (2015), **'The Internet of Things - Opportunities and challenges'**, Briefing, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf
2. Centre for the Promotion of Imports from developing countries CBI (2022), **'Which trends offer opportunities or pose threats on the European outsourcing market?'**, Dutch Minsitry of Foreign Affairs, available at https://www.cbi.eu/market-information/outsourcing-itobpo/which-trends-offer-opportunities#geopolitical-instability-influences-the-selection-of-service-providers
3. TBAT Innovation, **'What is SEIS Tax Relief & EIS Tax Relief?',** available at https://tbat.co.uk/knowledge/what-is-seis-tax-relief-and-eis-tax-relief/
4. Spreds, **'What is the Tax Shelter?'**, available at https://www.spreds.com/en/tax-shelter
5. Buchner, J. et al. (2021), 'An Augmented Reality Learning Environment for Informal Geoinformatics Education', GI_Forum 2021, Issue 2, Page: 3 - 17.

Published by the **European Liberal Forum** (ELF)
in cooperation with **European Liberal Youth** (LYMEC)

Rue d'Idalie 11-13, boite 6
1050 Ixelles,
Brussels

Contact

Email: info@liberalforum.eu
Telephone: +32 266 91318
Web: www.liberalforum.eu

Email: office@lymec.eu
Telephone: +32 484 644068
Web: www.lymec.eu

ISBN: 978-2-39067-046-9

Author:
Francesco Cappelletti - fcappelletti@liberalforum.eu

Design:
Chiara Olga Liguori - chiara@lymec.eu

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 46 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard.

ELF was founded in 2017 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European.

We bring together a diverse network of national foundations, think tanks and other experts. At the same time, we are close to, but independent from, the ALDE Party and other Liberal actors in Europe. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of actors.

This publication was co-financed by the European Parliament. The European Parliament is not responsible for the content of this publication, or for any use that may be made of it.

ISBN 978-239067046-9

/europeanliberalforum
@eurliberalforum
#ELFevent

liberalforum.eu