Digital EU: the Good, the Bad — and the Ugly
‘Digital EU’: the Good, the Bad — and the Ugly

By Shada Islam

The European Union has impressive digital ambitions and an equally impressive array of initiatives, proposals, directives and regulations, all designed to make the bloc ‘fit for the digital age’.

And there’s much to recommend in the EU plans. As the bloc underlines, the digital transition should certainly work for all, put people first, and open up new opportunities for business.

Artificial Intelligence (AI) must be developed in ways that respect people’s rights and also earn their trust. Online platforms must act in a responsible manner.

Digital solutions are also key to fighting climate change, achieving a green transition and they can help to foster a ‘digital democracy’. As illustrated by the expansion of the EU’s GDPR directive (which stands for General Data Protection Regulation), there’s also much to commend in the EU’s bid to become a global trendsetter for online norms, and a global role-model for the digital economy.

By-and-large, countries in the Global South welcome EU support for their efforts to go digital and develop global standards.

That is the good side of digital Europe. It reflects ways in which the EU has a positive impact on both domestic digital developments and on the wider technological transformations taking place across the world.

Walking the EU’s good talk can be a challenge, however. And that’s where dangers lurk.

The contributions in this magazine are not intended to provide a fully comprehensive, objective guide to help readers navigate the ups and downs of digital Europe. Because that’s the job of EU institutions themselves.

Our publication does provide important insights into the EU’s ‘digital jungle’, and there is a handy dictionary of key tech jargon and acronyms, to help us find our way without getting lost among the trees.

In a frank behind-the-scenes interview, European Union Commission vice-president Margrethe Vestager tells us that in addition to battling the world’s digital giants, she also worries about a future where technology takes even more control of our lives.

We look at the pros and cons of the ways in which Artificial Intelligence is taking over our lives — and the big battles ahead on regulating (at least some) aspects of AI.

There’s an attempt also to define the real focus of the EU’s quest for so-called ‘digital strategic autonomy’.

As editor, I am keen on exploring some of the untold stories of just how this rapidly transforming digital world is impacting on EU values, on migration policy, and how many of the EU’s partners look at digital Europe.

Here too, there is bad news and good news. The EU is trampling on its own values and peoples’ right to privacy and data protection as it expands its collection of data in areas such as migration, according to the EU’s own data-protection advisor.

Our article on ‘Digital Africa’ points out that despite all the talk of building an “equal” EU-African partnership, the EU’s colonial mindset prevents it from understanding — and investing in — Africa’s ongoing impressive digital transformation.

Still, despite their own remarkable digital achievements, African states, plus China, and countries in the Association of Southeast Asian Nations (ASEAN) are hoping to forge stronger digital partnerships with the EU.

As one of our authors points out, it is now up to the EU to respond to such initiatives by going beyond ‘digital tribalism’ and work to expand relations with both like-minded and “unlike-minded” states.

Our digital world is expanding our horizons every day, while we strive to strike the right balance between being online and offline, and reflect on the ‘correct’ social platform to use to communicate with friends and family and our new ‘digital friends’: the networks we have built with people who share – or don’t share – our concerns across the globe.

Technology helped us to live and work even as the pandemic forced us to stay home. It is now helping us find a better ‘work-life balance’ between working from the office and working from home.

Yet we are also spied on, manipulated and bullied online. Misinformation and disinformation thrive in the amorphous digital ‘cloud’, impacting on elections and trying to spread hate. The EU is right to try and bring some order into the digital world. But while doing so it must not forget its values.
## In this issue

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Vestager: ‘Technology must not steal our time’</td>
</tr>
<tr>
<td>10</td>
<td>Europe’s push to reform the ‘digital jungle’</td>
</tr>
<tr>
<td>12</td>
<td>Civil society calls for a rights-respecting Artificial Intelligence Act</td>
</tr>
<tr>
<td>14</td>
<td>AI — forecasting and profiling, or bias and discrimination?</td>
</tr>
<tr>
<td>18</td>
<td>How does ‘Digital Strategic Autonomy’ really work?</td>
</tr>
<tr>
<td>22</td>
<td>Expansion of data collection is eroding EU values and rights</td>
</tr>
<tr>
<td>26</td>
<td>Gearing up for tomorrow: Enhancing Europe’s tech competitiveness</td>
</tr>
<tr>
<td>28</td>
<td>Spyware scandals in Europe are ‘much worse than Watergate’</td>
</tr>
<tr>
<td>30</td>
<td>The outdated myths and exciting reality of ‘Digital Africa’</td>
</tr>
<tr>
<td>32</td>
<td>EU and ASEAN must step up digital connectivity amid rising geopolitical tensions</td>
</tr>
<tr>
<td>36</td>
<td>Chinese EU digital cooperation is possible – but needs political will</td>
</tr>
<tr>
<td>40</td>
<td>Worse than ‘deep fakes’ – disinfo’s new and more powerful apps</td>
</tr>
<tr>
<td>44</td>
<td>A European ‘right to repair’: The EU Commission needs to clear way for a circular economy revolution</td>
</tr>
<tr>
<td>46</td>
<td>To lead in cyberspace, the EU needs to avoid ‘digital tribalism’</td>
</tr>
<tr>
<td>50</td>
<td>An A-Z glossary of digital and tech jargon</td>
</tr>
</tbody>
</table>

---

**TABLE OF CONTENTS**

To lead in cyberspace, the EU needs to avoid ‘digital tribalism’
Margrethe Vestager, widely-regarded as one of Europe’s most powerful women, may spend most of her professional life trying to make the continent “fit for the digital age” (her official job title as EU commissioner) — yet she is adamant that technology must not control our entire lives.

“My main worry is that all of a sudden we forget just to look each other in the eye, and have a normal dinner without the phone on the table, to talk, or take a walk in the forest without registering every step,” she says in an interview for EUobserver magazine.

Technological transformation must work for people, warns the Danish former economy and home affairs minister. “We have chosen to do our best to make sure that technology actually serves the societies that we live in, and who we are as citizens, consumers, and voters,” she stresses.

The EU commissioner has her work cut out. One of her many tasks is to make sure the EU stays a step ahead in the fierce geopolitical competition for global tech leadership.

The European approach of ‘rules and regulations’, in order to promote a competitive model but one which is also values-based, is being challenged by China’s no-copyright ‘free-for-all’ method, and the US ‘move-fast-and-break-it’ model. Whether there is room for three such markedly-different approaches is still an open question, she acknowledges.

Certainly, the EU is making its own mark. The Digital Service Act (DSA) and the Digital Market Act (DMA) — two landmark pieces of digital legislation agreed upon in record time under the French EU Council presidency in the first half of 2022 — are the first salvos in Europe’s effort to bring an end to the so-called ‘Wild West’ elements of Big Tech.

These rules are deemed a new era in tech regulation, aiming to set worldwide standards beyond Europe’s borders — but it still remains to be seen whether national authorities or the EU bodies will have enough teeth to ensure their enforcement.

The DSA is expected to give control back to users, prohibit illegal content online, and make online platforms more transparent.

The DMA will complement the bloc’s competition policy, prohibiting anti-competitive behaviour by internet giants which act as ‘gatekeepers’.

Given their significant and entrenched market power, turnover and user numbers, US tech firms, Google, Amazon, Facebook, Apple and Microsoft, all fall under this category.

“With the Digital Market Act, the rules of the game are changing”, says Vestager. “Those who have market power, also have obligations and prohibitions that the others do not have — and that of course is rebalancing the market power”, she says, referring to the ways in which new rules will prohibit such gatekeepers from engaging in unfair business practices.

Google, for example, was fined €2.4bn in 2017 for promoting its service called “Google Shopping” over similar such services from competitors. But new rules will prohibit such behaviour a priori.

The commission, Vestager says, is already working with companies on what to do — and how to do it. Tech platforms presumed to be gatekeepers will have to share data about their average user numbers in the EU. These reports will help the commission designate very large companies in a list, which will be public and regularly updated.

Data boom
One may think that Europe lost the first battle for technological leadership to the US and China and their Big Tech behemoths such as Facebook, Amazon or Huawei. But has the EU lost the war?

The commissioner says a new phase of digitalisation is taking off — bringing a
The AI Act, a key piece of legislation to regulate AI applications dependent on the risks they pose to citizens’ rights or safety, is currently being discussed by EU member states and MEPs.

Once approved, it will become the first legislation of its kind worldwide. Like the EU’s data protection rules (GDPR) in 2018, the AI Act also aspires to become a global standard.

Risky for democracy

Disruptive technologies, meanwhile, have proven to be hard to regulate. The use of surveillance technologies such as the smartphone spyware, Pegasus, against anti-regime activists, journalists, and political leaders in several countries illustrates the risks that new technologies can pose to democracy and civil rights.

In 2021, an investigation by 17 media outlets (coordinated by Amnesty International and Forbidden Stories) revealed how the spyware tool of Israeli company NSO Group had been used against human-rights defenders, journalists, lawyers, and politicians.

“When the Pegasus scandal erupted, the commission found that this was absolutely non-acceptable because everyone has a right to privacy and journalists, in particular, have a right to protect their sources,” Vestager insists.

But this will probably not be the last spying scandal, she concedes. “Unfortunately, in the world we live in, if there is a buyer for something very often there’s also a supply... What is important is that people can protect themselves and that those who produce such technology know what obligations they have.”

When asked about the most significant dangers that technology may bring in the future, Vestager warned against allowing technology to dominate our lives. Globally, it is estimated that European citizens spend nearly seven hours per day using the internet across all devices — with an average of 2.5 hours on social media alone. “If we allow technology to steal our time, we are not in control anymore,” Vestager warned.

The EU competition chief’s battle against global tech giants has made her admired — but also hated by many, mainly in the US.

But she is not too worried and differentiates between two types of criticism: the one where someone interested thinks that there is a better solution and the one that tries to silence certain ideas.

Many women are exposed to the latter, she points out. Europe is backsliding in gender equality and women in power and politics because “a lot of efforts are made to scare people off,” she says, adding: “It’s not acceptable to bully other people, no matter the age, no matter the gender. And, here, I think we’re too timid.”

Elena Sánchez Nicolás

Elena joined EUobserver in 2019. She covers climate change and tech policy. Before joining EUobserver, she worked on European affairs at the Brussels-based think tank VoteWatch Europe and the Spanish news agency EFE. Elena is a graduate of Vrije Universiteit Brussel (VUB), where she completed a master in New Media and Society in Europe. She previously studied journalism in Spain, and was part of an exchange programme with the Thomas More Hogeschool, where she focussed on cross-media production.
Europe's push to reform the 'digital jungle'

Upcoming rules for online platforms, data-sharing and artificial intelligence will play a key role in the digital transformation of the EU and member states.

By ELENA SANCHEZ NICOLAS

Europe's digital transformation has been one of the key priorities of the European Commission as new technologies are deemed critical for societal and economic progress. European policymakers have long pledged to strengthen Europe's digital sovereignty, especially where dependencies are linked to security, but economic interdependencies remain.

The overall strategy is to improve digital infrastructure and connectivity across the bloc to boost Europe's competitiveness and green transition.

As regards competitive digital markets, the EU has given special importance to the roll-out of connectivity infrastructure (including 5G) and emerging technologies (such as artificial intelligence (AI), quantum technologies and blockchain). Improving digital skills and cybersecurity has also become a priority.

Europe does not boast Big Tech giants like the US (Google, Facebook or Amazon) and China (Baidu, Alibaba or Xiaomi), and whether the EU will be part of the next wave of digitalisation of machine-to-machine interactions still remains to be seen. In today’s data-driven economy, AI and machine learning (ML) are essential to enable the digital transformation of many industries in the bloc.

Building on previous legislation such as the data-privacy rulebook, the EU wants to become a champion of setting online standards for the digital age. The new AI Act, for example, aims to shape global standards and norms for AI technologies. But there are many other key initiatives for the EU's digital future.

The EU recently adopted two landmark pieces of legislation that set legal obligations for digital platforms. And, for the first time, big tech companies will have to comply with a series of obligations which aim to ensure competitiveness, plurality and transparency.

Other initiatives include new civil liability obligations, the open data directive, the e-Privacy regulation, a new consumer agenda, and rules to ensure secure cross-border transactions.

EU's Digital targets for 2030

- 5G everywhere. Double EU share in semiconductors global production
- 80% of citizens using digital ID
- 100% of citizens having access to medical records
- 75% of EU firms using Cloud/AI/Big Data
- Grow scale-ups & increase finance to double EU unicorns
- 20 million ICT specialists.
- 80% population with basic digital skills

Facts & Figures

**Funds**

Around 20% of the €723.8bn EU recovery funds are dedicated to digital objectives, supporting digital public services, digitalisation of businesses, connectivity or education.

**Cybersecurity**

It is estimated that every 11 seconds there is a ransomware attack targeting an organisation across the globe—a criminal business with an estimated cost of €20bn in 2021. Overall, cybercrime had a global cost of €5.5 trillion in 2021. Cyberattacks targeting EU bodies have increased more than tenfold during the last four years.

**AI investment**

The estimated annual investment of the EU in AI is €11bn, compared to €1.1bn invested annually by the US and €6.8bn by China. The investment gap in AI and blockchain is estimated to be €10bn.

The EU wants to mobilise funding to invest €20bn per year in AI during the next decade to reduce the investment gap between the US and China.

**Data economy**

The value of the data economy of EU-27 was almost €525bn in 2019 (representing 2.6% of GDP) but it is expected to increase to over €550bn by 2025 (4% of GDP).

**5G**

Just one-quarter of EU citizens can access a 5G network. 5G is expected to add up to over €1 trillion to EU GDP by 2025.

**Skills & workforce**

More than 40% of Europeans lack basic digital skills and sometimes it is difficult for companies to find the ICT talent. In 2021, about nine million people worked as ICT specialists in the EU, with the highest number in Germany and France.

**Business using IoT technologies in 2021**

**Business using AI technologies in 2021**

* All enterprises, excluding financial sector (10 or more employees and self-employed persons)
As part of a collective of 123 civil society organisations, European Digital Rights (EDRi), an association of civil and human rights organisations from across Europe, has been calling for an Artificial Intelligence Act that foregrounds fundamental rights.

We specifically recognise that Artificial Intelligence systems exacerbate structural imbalances of power, with harms often falling on the most marginalised in society.

As such, we urge members of the European Parliament to be bold in building the AI Act to safeguard the rights of people and ensure that AI development and deployment fully respect fundamental rights and democracy.

The AI Act takes a risk-based approach to regulating the use of AI systems. The intention is to introduce appropriate safeguards and obligations on providers (developers) and users (deployers) of AI systems that pose a risk to “the health and safety or fundamental rights of persons.”

Prohibited practices
The AI act recognises that some uses of AI are ‘unacceptable’ and must be prohibited. However, currently, the list of prohibitions, such as the prohibition on the use of facial recognition in public spaces, contains too many loopholes and exemptions.

MEPs must expand the list of ‘prohibited AI practices’ to cover all systems that are proven to pose an unacceptable risk to fundamental rights, including predictive policing, emotion recognition, the use of remote biometric identification in publicly accessible spaces by all actors, and AI uses in the migration context.

Accountability for users
The AIA predominantly imposes obligations on providers (developers) rather than on users (deployers) of high-risk AI. While some of the risk posed by the systems listed in the AIA come from how they are designed, significant risks actually stem from how they are used.

Providers cannot comprehensively assess the full, potential, impact of a high-risk AI system during the conformity assessment, and therefore that users must have obligations to uphold fundamental rights as well.

MEPs must include a duty to conduct and publish a fundamental rights impact assessment for all high risk AI systems, to ensure accountability and transparency to the public.

Empowering people affected by AI systems
The AIA currently does not confer individual rights to people impacted by AI systems, nor does it include any provision for individual or collective redress, or a mechanism by which people or civil society can participate in the investigatory process of high-risk AI systems.

The AIA should include a right for people affected to seek an explanation for how they are affected by AI systems, and ways to challenge non-compliant AI systems with national authorities. The AIA should also include horizontal, and mainstreamed, accessibility requirements for AI systems including for AI-related information and instruction manuals, consistent with the European Accessibility Act.

To guarantee the AIA works for everyone MEPs must widen the list of prohibitions, include accountability measures, and routes to challenge and seek remedies for harmful AI systems.

The AIA negotiations are a key moment to ask ourselves what society we want to live in: technological tools promoting a healthy and accountable digital future, or dystopian and discriminatory ones.

Civil society calls for a rights-respecting Artificial Intelligence Act

MEPs and representatives of EU member states governments must deliver an Artificial Intelligence Act (AIA) that centers people impacted by this technology.
AI — forecasting and profiling, or bias and discrimination?

A showdown is likely among MEPs and governments over the EU Commission’s proposal on Artificial Intelligence and fundamental rights. The legislation, likely to be agreed next year, will be key in fighting discrimination in the virtual and real world.

By ESZTER ZALAN
Artificial Intelligence has already brought down one government in Europe. In 2019, the Dutch tax authority used self-learning algorithms to create risk profiles in an attempt to spot fraud involving child-care benefits. As it became clear that the families, mainly from ethnic-minority communities, had been identified on suspicion of fraud and then penalised because of algorithm-generated profiles, a massive political scandal brought down the government of Dutch prime minister Mark Rutte. Rutte survived. But thousands of ordinary lives were ruined.

As Artificial Intelligence becomes an essential, albeit invisible, feature of our daily interactions, brace yourselves for even more EU-wide political wrangles centring on European Commission proposals to regulate the sector.

The proposals, made in 2019, are now making their way through the European Parliament – where political groups have tabled over 3,000 amendments – and are expected to receive the Council green-light in December. The EU’s AI Act will then be agreed next year, after intra-institutional negotiations.

Expect a showdown between the parliament and the council, however. MEPs are expected to push for stricter regulation and better protection of rights, while governments will likely argue for fewer rules, citing the need for competitiveness and security concerns.

“The success of the text will lie in the balance we find between the need to protect the interests and rights of our citizens, and the interest to stimulate innovation and encourage the uptake and development of AI,” Romanian liberal MEP Dragos Tudorache, one of the European lawmakers in charge of the file, said recently. “The real political discussions are yet to come.”

Bulgarian socialist MEP Petar Vitanov, one of the negotiators on the file, says the focus must be on ensuring that “fundamental rights and freedoms are safeguarded, there can be no innovation without fundamental rights.”

Key issues include the governance of the act, and the legislation’s definition of risk.

Lawmakers want to give the commission the power to extend the list of so-called “high-risk areas”, and to raise fines for non-compliance to €40m or seven per cent of annual turnover.

Some EU governments are seeking exemptions for the use of AI by migration authorities and law enforcement, which could lead to more control over communities, including ethnic communities, which are already more policed than others.

While some critics, such as the United Nations’ former human rights chief, Michelle Bachlet, say governments should put a moratorium on the safe and use of AI systems until the “negative, even catastrophic” risks they pose can be addressed.

Exceptions are allowed in the case of a search for victims of kidnapping, the identification of a perpetrator or suspect of a criminal offence, or for the prevention of imminent threats such as a terrorist attack.

Digital-rights activists warn, however, that there are “loopholes” that allow mass surveillance.

Any exemption given to governments and companies for use of an AI system which is “purely accessory” and used in a minor matter could, in fact, “undermine the entire act”, warns Sarah Chander, who leads the policy work on Artificial Intelligence for European Digital Rights (EDRi), a network of non-profit organisations working to defend digital rights in the EU.

High risk

The Commission proposal focuses on so-called “high-risk” AI systems which may jeopardise people’s safety or fundamental rights, such as education (for example, scoring of exams), employment (like CV-filtering software for recruitment), or public services (for instance, credit-scoring to deny people the opportunity to obtain a loan).

Companies who want to compete using AI systems in this “high-risk” category, would have to meet EU requirements, such as explainability, risk-assessment, and human oversight.

Some worry, however, that these requirements could discourage start-ups and businesses from investing in Europe in such AI systems, giving the competitive advantage to the US or China.

Companies that fail to comply with the legislation could face fines of up to €15m per year, or six percent of their global turnover.

Chander highlighted that some of the biggest harm from AI systems could come in the delivery of public services, such as social services, policing (where predictive-policing based on mass surveillance is a major concern), and migration.

AI-based social decisions are dangerous because AI systems make assumptions seem like facts.

Chander says the commission’s proposal does not go far enough on restricting the use of facial recognition. Her organisation also wants to ban the use of AI for predictive policing and migration as well as for predicting emotions.

Rights-defenders argue that companies should be obliged to make fundamental rights impact-assessments, and provide information on where and how an AI system would be used and its impact on individuals.

They also want clear information provided to the public, and say citizens should be able to seek explanations from public authorities or companies. Citizens should also be able to claim remedies if a company or an authority has violated the AI Act, or an individual has been impacted by a banned system.

Chander said there is a common misunderstanding that AI systems can be “perfect”, and pecky-makers often ask her how to make these systems better, less prone to bias. But that is the wrong question, she argues because the problem is that AI systems are replicating an already discriminatory system.

“Some systems cannot be made better,” she says, adding: “We don’t want to make a perfect predictive-policing system, or perfect lie detector”.
How does ‘Digital Strategic Autonomy’ really work?

Buzzwords like ‘strategic’ and ‘autonomy’ have long been heard among Brussels’ policy-makers, think-tankers, and academics. However, the concept has only become a real priority as a result of recent events, bringing the geopolitical role of the EU to the top of the agenda.

By DR ANTONIOS NESTORAS AND FRANCESCO CAPPELLETTI

Strategic autonomy today is no longer just about security. Many domains are now thought of to be ‘strategic’: economy and industry, manufacturing and critical infrastructure, sustainability, energy security and the electricity revolution, plus also, of course, security and defence.

But the real game for the future is undoubtedly now being played out in the field of new technologies and, even more so, in the digitalisation of societies.

Although it is now clear that autonomy cannot mean protectionism, in times of crisis, it might mean ‘pragmatism’. In this context, a solid and adaptable industrial base is essential to ensure the capacity to act with autonomy.

On the one hand, finding like-minded partners is now more necessary than ever. On the other hand, member states and the EU must create a dialogue with strategic and even systemic rivals. As the world itself functions on interdependencies, openness will secure the goals and needs of a digital, sustainable, and future-proof European transition.

Yet rebalancing the nature of such relations towards an assertive stance may be necessary in the long-term strategy — ensuring that no compromises in terms of core values will be ever accepted.

Critical technologies must be considered instruments of digital strategic autonomy.
Dimensions of 'Strategic Autonomy Europe' and sources of power

Like a computer, it is time for the EU to seek updates — perhaps even rebooting its operating system — reassessing its strategic priorities, strengthening relations with like-minded partners, and reconsidering those with strategic rivals.

Microchips, together with new telecommunication technologies such as 5G and 6G, artificial intelligence, quantum computing, and cybersecurity tools, as well as electronic and digital ID, are only a few of the key enablers within the different segments of this digital transition.

Shortages in the supply chain and know-how in these domains (as experienced during the pandemic) have underlined how diversification and even rethinking of strategic prerogatives must be at the centre of the EU’s political agendas.

Therefore, finding the right partners to cooperate with is a significant part of a prosperous strategic Europe. Partners are defined as like-minded, market-oriented democracies towards which openness is essential.

Transatlantic cooperation with both Americas, meaningful relations for trade and investment with democracies in Africa, as well as a close cooperation with countries like Taiwan or Japan must be fostered.

Trade and technology councils, and digital diplomacy sound good, but they miss meat on the bone. Additionally, as interests may vary over time and circumstances, it is crucial for the EU to explore new market-based relations under common standards, creating a systemic dialogue and reciprocal information-sharing mechanisms.

To this end, a solid foundation of data-governance and privacy rules is crucial. In fact, data can be defined as the ‘oil’ of a digital economy. With its recent effort in defining the Digital Services Act and the Digital Market Act, the Data Governance Act and Data Act, European institutions have taken significant steps toward the way European companies store, use, and process data and deal with privacy.

The European data economy itself, however, is still far from reaching its full potential, undermining its strategic digital autonomy.

Ahead of the 2024 European Parliament elections, the discussion on how data is processed for political advertising becomes increasingly important — to ensure transparency, protect citizens’ rights, while fighting disinformation and interference.

The protection of citizens’ rights online is at the heart of the future digital Europe. With the rise of Chinese imperialism and following the Russian aggression against Ukraine, malicious activities in the digital domain have intensified.

There is a need for the EU to be resilient in cyberspace. Cybersecurity vulnerabilities threaten the functioning of our economies, the internal market across the EU and represent a transversal danger to our societies. Being resilient in cyberspace requires strategic, proactive, integrated, and future-proof policy advancements.

Resilience can neither be built by force nor can it be regulated into existence without a comprehensive strategy that listens to industry. This strategy must be future-proof and long-term, let the free market work, let the digital industry produce and avoid over-regulation. It may not be a miracle cure but it represents a liberal best practice to ensure policies that are truly ‘smart’.

And the EU must facilitate such a strategy ‘yesterday’ if it wants to secure its ‘Fit for Digital Future’ plan — and bring digital strategic autonomy to reality. Like a computer, it is time for the EU to seek updates — perhaps even rebooting its operating system — reassessing its strategic priorities, strengthening relations with like-minded partners, and reconsidering those with strategic rivals.

About Dr. Antonios Nestoras
Interim executive director at the European Liberal Forum (ELF) and Francesco Cappelletti, policy and research officer at the ELF.
Expansion of data-collection is eroding EU values and rights

The EU is trampling on its own values and peoples’ rights to privacy and data-protection as it expands its collection of data in areas such as migration, the EU’s data protection advisor tells Nikolaj Nielsen.

By NIKOLAJ NIELSEN

Wojciech Wiewiórowski is a 51-year old Polish national whose job as the EU’s data protection supervisor (EDPS) is to ensure that European institutions and bodies respect peoples’ right to privacy and data-protection. Yet those rights are regularly denied to thousands of people seeking asylum in the EU, he warns.

Wiewiórowski, who heads the independent, Brussels-based, EDPS, says the EU has “two extreme approaches,” when it comes to the collection of and processing of people’s data crossing a border of the European Union.

The first is value-based and one where everyone is treated fairly regardless of origin. The second is security focussed and one where people have to give up all their data, irrespective of privacy rights. “The second approach is not convincing for us,” he says.

Wiewiórowski warns that people who arrive at the borders seeking international protection are forced into divulging all their personal data in order to gain access to the EU. That data is fed into large EU databases, some of which were set up to crack down on criminals.

“We are forgetting for which reasons we were collecting the data,” he says. This poses a slew of data-protection problems, spanning concepts like “purpose limitation” and “data minimisation.” Both are spelled out in the EU’s general data protection regulation (GDPR), as well as its directive on law enforcement.

It means authorities are only supposed to collect data for specific purposes. But Wiewiórowski says there is a push to collect everything possible. This is fed into a maze of EU and national security databases that then ‘talk’ to one another. “I feel a little bit puzzled,” he acknowledges.

The European system is based on humane values, he says. But at the same time people are being denied their rights. Wiewiórowski says he partly understands the approach by EU states, the border authorities, and Frontex when it comes to migration. But he is also bound by rights entrenched in the EU treaties.

Earlier this year he ordered Europol to erase data on people with no established link to a criminal activity. The Hague-based agency had hoovered up four petabytes of sensitive data, including from asylum seekers with no criminal records.

And in October, his staff carried out an audit of Frontex’s processing of personal data of migrants at their headquarters in Warsaw. The probe is looking at how Frontex and Europol are sharing data through the Processing of Personal Data for Risk Analysis, known as PeDRA.

“Fabrice Leggeri, when he was still executive director at Frontex, had proposed expanding PeDRA to allow border guards to collect sensitive data on asylum seekers, including their sexual orientation.

Wiewiórowski’s task and that of national data-protection authorities is only likely to get more difficult as tech-based solutions to security issues push privacy rights on the back burner. Over the years, the EU has dramatically increased its security budgets to shore up its external borders.

The EU’s Internal Security Fund shot up by 90 percent to €1.9bn, when compared to the EU’s previous seven-year budget cycle. The fund is intended to reinforce police powers, including the exchange of data. It helped finance to the tune of some €50m the expansion of Greece’s automated border surveillance system,
which aims to track down migrants attempting to enter through Turkey. It is operated by the Hellenic Police.

Greek authorities describe it as an all-seeing system that can provide real-time and accurate information. Now Athens is testing EU-funded drones with artificial intelligence to track people seeking refuge.

Another big budget boost went to the EU’s Integrated Border Management Fund, which increased to €7.3bn. One of its goals is to detect irregular migration crossings, including by setting up large scale IT systems for border management.

Behind those figures lies a wider malaise over migration, coupled with EU-wide policy initiatives tying asylum to geopolitical tensions. None of the money, for example, will go towards helping search and rescue in the Mediterranean Sea.

Instead, the clampdown on the borders in places like Greece, Hungary, Lithuania, Latvia, Poland and elsewhere is most visibly manifested by walls and fences aimed at keeping people out. Border guards, for instance in Latvia, used force to push people back into Belarus last year, according to Amnesty International.

The focus may be on these physical barriers. But while tech surveillance systems, artificial intelligence technologies, and security databases used by EU and national authorities to gauge a person’s intent, background, and origin may be less visible, they are very much part and parcel of ‘Fortress Europe’.

“Fundamental rights are definitely right now under stress,” Wiewiórowski warns.

About Nikolaj Nielsen

Nikolaj was born in Denmark but spent a better part of his life in Belgium, France and the United States. He joined EUobserver in 2012, where he primarily covers migration, human rights and transparency issues. His reporting for EUobserver has taken him to Algeria, Belarus, Egypt, Lebanon, Moldova, Russia, Transnistria, Turkey, Uganda, Ukraine and off the Libyan coast.

Familiar sight?

*Yes* | European consumers are increasingly using digital tools to get information on food and drinks!

8 in 10

are used to scanning QR codes

75%

have scanned a QR code on a food or drink product

95%

find QR codes useful to get detailed product information

DID YOU KNOW?

EU law already allows wines & aromatised wines to communicate their ingredients and nutrition declaration through the use of QR-codes and e-labels.

**IN THE UPCOMING REVISION OF EU FOOD LABELLING RULES, THE EU SHOULD:**

Allow & regulate the use of e-labels on all food & drink products (as is already the case for wine).

Let’s support the digital transition & make EU rules on food information fit for the 21st century!

U-LABEL is a unique digital platform that enables consumers to access product specific information about wines & spirits, anytime, anywhere, in their own language.

SCAN THIS QR CODE TO SEE THE WIDTH OF INFORMATION AVAILABLE

U-LABEL

is a unique digital platform that enables consumers to access product specific information about wines & spirits, anytime, anywhere, in their own language.

#YesWeScan
Europe recognizes the importance of digital technology, which is evident in numerous studies that aim to boost and regulate the sector. However, Europe too slow to react and adapt to new conditions.

By SILVIO KUTIĆ

The ‘Old Continent’ is on the right track, but it must speed up its efforts to avoid being left behind in new technological opportunities this time.

The question arises - where does Europe stand on this global map of tech power?

The McKinsey Global Institute points out that overcoming the technology gap will be crucial to reduce Europe’s exposure across various sectors. Technology is one of the key drivers of growth, and even though Europe has many high-performing companies, they typically grow slower, generate lower returns, and invest less in R&D compared to their US counterparts. Although Europe arguably missed the first boat in the previous technology revolution, many boats are still in the harbor, ready to be boarded by the new leaders of developing technologies.

Despite the fact that we live in uncertain times, we must think in terms of the future where interactions and communication between the physical and virtual realities will play a major role. What connects all new technologies is the need for communication. Online solutions are the new drivers of growth.

One of the areas that could unleash an entire set of new values is the communication and data industry. In the context of Europe, these areas can offer space for specialisation and new expertise required for the jobs of the future while protecting the democratisation of data and inclusion so that no one is left out in the new wave of growth.

How long Europe will endure the technology gap in the face of the burgeoning digital ecosystem in global markets also depends on the focus it puts on competitiveness development. We see concrete examples of overcoming challenges in EU funding in the IPCEI (Important Projects of Common European Interest) instrument, comparable to what DARPA (Defense Advanced Research Projects Agency) is doing in the US.

Europe recognizes the importance of digital technology, which is evident in numerous studies that aim to boost and regulate the sector. However, Europe too slow to react and adapt to new conditions.

Infobip is using its cloud platform to open and democratise global communication and digital interactions. As a leader in its field, Infobip helps navigate the new wave of tech companies that have power to position Europe at the forefront of upcoming digital technologies.

About Silvio Kutić

Silvio Kutić, CEO of Infobip a global cloud communications platform established in 2006 and the first Croatian unicorn.

The platform has the capacity to reach over seven billion mobile devices and ‘things’ on 6 continents with direct connections to more than 700 mobile network operators in over 190 countries worldwide. Infobip’s mission has always been to provide affordable and innovative global communications technology.

Our vision for the future is a cloud-based communication continuum that gives more power to users and enables seamless interaction between businesses and people around the world.
Spyware scandals in Europe are ‘much worse than Watergate’

The illicit use of spyware in Europe is worse than the Watergate scandal which brought down US president Richard Nixon — yet EU authorities are ignoring the danger, MEP Sophie in ‘t Veld tells Wester van Gaal.

By WESTER VAN GAAL

Electronic spying on citizens isn’t the preserve of autocratic states alone. Journalists and politicians are also being spied on by several European governments, including Spain, Greece, Hungary and Poland, according to Sophie in ‘t Veld MEP, rapporteur of the European Parliament’s PEGA-committee.

“The European Commission is very strict regarding threats to democracy elsewhere in the world, but when it comes to its members, it prefers to remain quiet,” says the Dutch MEP, who is parliament’s lead investigator on the use of spyware in Europe.

The illicit use of spyware in Europe is comparable to the Watergate scandal which brought down US president Richard Nixon — yet EU authorities are ignoring the danger, MEP Sophie in ‘t Veld tells Wester van Gaal.

In ‘t Veld’s report, presented in November and to be finalised next year, points to the Polish government’s use of material extracted from telephones for smear campaigns against journalists. The Hungarian government used spyware on at least 300 telephones belonging to NGOs and individuals connected to American-Hungarian businessman George Soros.

Top-level politicians in Greece have used spyware to cover up corruption, and the Spanish government has used spyware on 65 Catalans, supposedly in connection with the independence movement. The Hun- garian government used spyware on at least 300 telephones belonging to NGOs and individuals connected to American-Hungarian businessman George Soros.

Not all member states use spyware illicitly, but “all member states have spyware at their disposal, whether they admit it or not,” in ‘t Veld warns.

Governments operate alongside “an impenetrable maze of persons, locations, connections, ownership structures, letterbox companies, ever-changing corporate names” and purchase spyware, often through middlemen, “from criminals or quasi-criminals,” she adds.

Israeli spyware companies dominate the sector and have spread their operations across Europe, taking advantage of lax export enforcement, and favourable tax arrangements in Ireland and other countries.

Electronic spying on citizens isn’t the preserve of autocratic states alone. Journalists and politicians are also being spied on by several European governments, including Spain, Greece, Hungary and Poland, according to Sophie in ‘t Veld MEP, rapporteur of the European Parliament’s PEGA-committee.

“It’s not a matter of a few isolated incidents where some governments have crossed the line. It’s a widespread system that centres around Europe.”

A central player has been the Israeli company NSO Group, which has sold Pe-gatus and other products to 22 end-users in 14 member states, including Poland, Hungary, Spain, the Netherlands and Belgium.

The US has blacklisted the group and is developing new spyware legislation. Victims have filed legal complaints. Tech giants like Microsoft and Apple have launched legal challenges against spyware companies, the latter describing the NSO Group as “amoral 21st-century mercenaries” who “target, attack, and harm... for their own commercial gain.”

But the European response has been muted. The European Council has yet to respond and the European Commission, which was itself hacked, has “absolutely no interest” in pursuing the question, in ‘t Veld says.

Europol, the EU’s law enforcement agency, has so far declined to investigate the matter, claiming it is an exclusively national matter. But EU governments have “stonewalled” in ‘t Veld’s efforts, citing “national security reasons.”

Those victims who have mounted legal challenges find that judges and prosecutors refuse to investigate and put the burden of proof on the victims. This leaves victims defenceless against state power. All vital checks and balances of a democratic society are disabled.

“Democracy isn’t about elections. Russia has elections. Democracy is about countervailing power,” in ‘t Veld says. “Once it’s gone, democracy ends.”

Out of all the EU’s 27 governments that she has sent questions to, only Austria, Cyprus, and Poland have responded, and then only “in the most evasive terms.”

Partly because of this, there is a lack of hard evidence.

Modern spyware can be used to take complete control of a mobile phone with hardly a trace, and even if it is detected, it is nearly impossible to prove who was responsible for the attack.

“The list of victims of spyware tells the real story,” she underlines. “If you have nine hundred pieces of a puzzle of a thousand, you have a good idea of the whole picture.”

Those victims who have mounted legal challenges find that judges and prosecutors refuse to investigate and put the burden of proof on the victims. This leaves victims defenceless against state power. All vital checks and balances of a democratic society are disabled.

“The list of victims of spyware tells the real story,” she underlines. “If you have nine hundred pieces of a puzzle of a thousand, you have a good idea of the whole picture.”

Out of all the EU’s 27 governments that she has sent questions to, only Austria, Cyprus, and Poland have responded, and then only “in the most evasive terms.”

Partly because of this, there is a lack of hard evidence.

Modern spyware can be used to take complete control of a mobile phone with hardly a trace, and even if it is detected, it is nearly impossible to prove who was responsible for the attack.

“The list of victims of spyware tells the real story,” she underlines. “If you have nine hundred pieces of a puzzle of a thousand, you have a good idea of the whole picture.”

Those victims who have mounted legal challenges find that judges and prosecutors refuse to investigate and put the burden of proof on the victims. This leaves victims defenceless against state power. All vital checks and balances of a democratic society are disabled.

“Democracy isn’t about elections. Russia has elections. Democracy is about countervailing power,” in ‘t Veld says. “Once it’s gone, democracy ends.”

About
Wester van Gaal

Wester is a journalist from the Netherlands with a focus on the green economy. He joined EUobserver in September 2021. Previously he was editor-in-chief of Vice, Motherboard, a science-based website, and climate economy journalist for The Correspondent.
The outdated myths and exciting reality of ‘Digital Africa’

A look at the history of the digital transformation taking place in Africa proves that the continent is certainly not backward. Africa has always been progressive and is currently in the midst of an exciting and disruptive digital revolution.

By Dr. ADEYINKA ADEWALE

Africa is in the midst of an ongoing digital revolution which is exciting, different and disruptive. It is different because the change is happening in a unique context with unique nuances; it is disruptive because it demands that Africans and the rest of the world adopt new ways of thinking and doing things.

A look at the history of the digital transformation taking place in Africa proves that the continent is certainly not backward. Africa has always been progressive, a fact proven by accurate rather than false narratives about her pre-colonial past.

More recently, African countries have been among the early adopters of the internet. The 1990s marked the beginning of the first era of digital revolution on the continent, which can be dubbed the ‘infrastructure era’. Internet service providers got licensed in many African nations and the internet became publicly accessible.

Between 2000 and 2010, the ‘knowledge era’ unfolded, powered by the proliferation of internet cafes, a popular business venture. This period opened up new horizons for young entrepreneurs who began to dare to do things in new ways.

This soon ushered in the ‘skills era’. As the number of tech businesses soared on the continent, gaps in the requisite digital skills needed to power these businesses became obvious – and remain an ongoing challenge.

These eras are not mutually exclusive and have become more sophisticated over time. The internet is now more mobile than it has ever been, with 570 million internet users across the continent in 2021, representing about half of Africa’s population. Projections suggest a 25-percent increase by 2030.

Online education has made the knowledge era more refined, with young Africans producing their own content whilst also consuming material from other parts of the globe. The digital skills challenge has also birthed tech hubs, training academies and other multi-stakeholder interventions.

Each era has often attracted massive investment opportunities — despite the challenges on the continent. The jump in venture capital investment in Africa from $500m (€481m) in 2016 to $2.2bn in 2021 is not a mere coincidence, it has been brewing for years. As far back as 2012, Foreign Direct Investment (FDI) had eclipsed Official Development Assistance (ODA) in 17 African countries. By 2014, FDI flow into Africa was double ODA flow.

The message is clear: Africa is no longer the beggarly, needy continent, dependent on aid. The continent is ready for trade and investment. Approaching the continent with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

A look at the history of the digital transformation taking place in Africa proves that the continent is certainly not backward. Africa has always been progressive and is currently in the midst of an exciting and disruptive digital revolution.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.

Venture capital inflow into Africa is one sign that investors are willing to take a risk on a continent that offers about a 2.7-percent return on investments. This may be low relative to other contexts but this will improve with time not because of sheer optimism but because of encouraging and positive emerging trends.

African youths are harnessing the opportunities afforded by the digital revolution to engage in high-impact entrepreneurial activities and are creating digital services and solutions tailored to address myriad challenges on the continent. This has driven an unusually high volume of entrepreneurship activities across Africa.

Technology is seen as a ‘silver bullet’, with almost every major sector having a sub-sector under the tech appendage – Fintech, Edtech, Medtech, Civictech and the like. The challenge is translating this quantity into quality.
EU and ASEAN must step up digital connectivity ties amid rising geopolitical tensions

The digital sphere is particularly complex with a diverse range of actors and stakeholders. Working closely with each other and other like-minded partners in the Indo-Pacific, the EU and ASEAN can be voices of moderation.

BY Dr. YEO LAY HWEE
The recent signature of an air-connectivity agreement between the EU and the Association of Southeast Asian Nations (ASEAN) provides some good news in challenging geopolitical times.

The EU-ASEAN Comprehensive Air Transport Agreement (CATA), signed in October during an ASEAN transport ministers meeting, is the result of years of tough negotiations. It is expected to provide greater opportunities for ASEAN and EU airlines to operate passenger and cargo services between and beyond both regions, helping to bolster the recovery of air connectivity between the two regions following the Covid-19 pandemic.

But CATA also has ramifications beyond immediate benefits of increased inter-regional connectivity, by signalling the increased importance of regional blocs like the 27-member EU and the 10-member ASEAN and their ability to exercise more agency and leadership.

And the next area that the EU and ASEAN need to focus on is digital connectivity.

Both EU and ASEAN face economic headwinds caused by the war in Ukraine, and geopolitical tensions arising from challenges to the current world order. While the global security order remains dominated by the US, increasingly, the world is becoming more multi-polar and multi-stakeholder-driven.

The EU needs to strengthen its autonomy and ASEAN needs to regain its centrality as different powers and stakeholders jostle to shape the global or regional economic order and influence the climate and digital agendas.

The digital sphere is particularly complex, with a diverse range of actors and stakeholders. Working closely with each other and other like-minded partners in the Indo-Pacific, the EU and ASEAN can converge.

Instead of allowing any single issue to dominate the global agenda, EU and ASEAN can work pragmatically to exercise joint leadership in functional areas where their interests and priorities converge.

The EU-ASEAN Comprehensive Air Transport Agreement have just been launched. As a trusted strategic partner of ASEAN, the EU is in a good position to work with the region to increase digital connectivity and build interoperable and standards-based systems.

The digital sphere is one of these areas.

Southeast Asia’s digital economy has reached a whopping $282bn ($272bn) in 2022. With a population of 680 million comprising an expanding middle class eager to participate in the digital economy, the region’s digital economy is projected to reach $1 trillion by 2030.

ASEAN has made a collective commitment towards the development of an integrated ASEAN digital economy. The ASEAN Digital Masterplan 2025 further envisions ASEAN as a leading digital community and economic bloc powered by secure and transformative digital services, technologies and ecosystem.

Digital transformation has been on ASEAN’s radar for some time now. Covid-19 has accelerated the pace of digitalisation in ASEAN and the region has evolved into one of the fastest-growing digital markets in the world. Negotiations towards an ASEAN Digital Economy Framework Agreement have just been launched.

As a trusted strategic partner of ASEAN, the EU is in a good position to work with the region to increase digital connectivity and build interoperable and standards-based systems.

The digital sphere is one of these areas.

Southeast Asia’s digital economy has reached a whopping $282bn ($272bn) in 2022. With a population of 680 million comprising an expanding middle class eager to participate in the digital economy, the region’s digital economy is projected to reach $1 trillion by 2030.

ASEAN has made a collective commitment towards the development of an integrated ASEAN digital economy. The ASEAN Digital Masterplan 2025 further envisions ASEAN as a leading digital community and economic bloc powered by secure and transformative digital services, technologies and ecosystem.

Digital transformation has been on ASEAN’s radar for some time now. Covid-19 has accelerated the pace of digitalisation in ASEAN and the region has evolved into one of the fastest-growing digital markets in the world. Negotiations towards an ASEAN Digital Economy Framework Agreement have just been launched.

As a trusted strategic partner of ASEAN, the EU is in a good position to work with the region to increase digital connectivity and build interoperable and standards-based systems.

The EU and Singapore have already launched discussions on a comprehensive and forward-looking digital partnership, a deal which aims to provide an overarching framework to strengthen digital connectivity and interoperability of digital markets and policy frameworks and facilitate digital trade between the EU and Singapore.

That agreement can be a pathfinder and template for a wider bloc-to-bloc EU-ASEAN digital agreement, which in turn could contribute to the development of a global architecture of interoperable standards. Shaping the future digital order with an open and inclusive approach towards multi-stakeholders is increasingly important in the light of Sino-American tensions and the danger of technological bifurcation.

The EU’s determination to promote a sustainable, people-centric vision for digital transformation is in line with ASEAN’s vision for a digitally-inclusive economy and society.

More investments would be needed to reach this vision, not only in hardware – high-speed broadband and fibre-optic networks – but also in designing regulatory regimes with proper incentive structures and governance.

There is also a lot to be gained if ASEAN and the EU step up cooperation to build digital literacy and skills of their people needed to benefit from digitalisation. In-stilling the mindset of lifelong learning is also important given the exponential pace of technological change.

With that in mind, more EU-ASEAN exchanges among institutions of higher learning, as well as vocational institutes and those dedicated to lifelong learning, should be stepped up.

Last but not least, the EU and ASEAN should truly collaborate in rule-setting for digital connectivity. This is how a EU-ASEAN strategic partnership can be truly meaningful and contribute to a more inclusive rules-based order that can underpin sustainable peace and development.
Chinese–EU digital cooperation is possible — but needs political will

The EU and China have their differences but should reinvigorate their high-level digital dialogue and work together on building a better and more connected digital world.

By YAN SHAOHUA & YAO XU
As other countries step up their efforts to promote digital innovation and rule-making, China has put forward the Digital Silk Road (DSR) as an integral part of the Belt and Road Initiative (BRI), in a bid to try to improve digital infrastructure and narrow the digital gaps in countries which are part of the BRI.

While the digital world is widely-perceived to be dominated by the US and China, the EU is also seen by China as a global digital power with unique advantages. The EU’s pursuit of “digital sovereignty” means more competition for China but it also presents opportunities for cooperation in areas where there are complementarities between China and the EU.

To tap the potential for cooperation, China and the EU have established a high-level digital dialogue, which provides a valuable platform for discussions between Brussels and Beijing on their respective approaches to digital transformation.

Despite the differences between China and the EU when it comes to terms like reciprocity, fairness and values, digitalisation remains one of the most promising areas for bilateral cooperation. It is thus necessary to identify priorities and new channels to move China-EU digital cooperation to the next level.

Digital innovation stands out as an area where China-EU cooperation could bring benefits to both sides. It is not only closely-related to investment in — and research of — a specific field, but also has a huge influence on the related high-tech industrial chains.

There is room for cooperation on digital rules and regulations.

Digital cooperation is also changing business models and market perceptions in China and Europe as online fashion houses expand their business. Meanwhile, New Energy Vehicles (NEV) play a central role in both digitalisation and decarbonisation that have topped the agenda in China and Europe over the past few years.

Despite growing competition, there has been excellent cooperation on NEV between China and the EU. China is now the world’s largest NEV market, accounting for more than 60 percent of global sales volume. For European NEV companies and the related industrial chains, the Chinese market is key to their expansion. During the past decades, Chinese-EU cooperation in the automobile industry is largely a story of success, and this story should be continued in NEV industry.

There is also room for cooperation on digital rules and regulations. The EU is a leader in trans-border data flows and data protection. The GDPR adopted by the EU in 2016 has set a series of global standards for trans-border data flows, which also provide an example for China in creating and updating its regulatory frameworks in the digital world. Cooperation in digital rules and regulations would greatly benefit Chinese and Europe digital companies by connecting resources and markets on both sides.

In regulating cutting-edge technologies like AI, China and the EU face common challenges: of striking the right balance between civil rights, socio-economic development and national security. It is important that China and the EU could jointly develop the best practice in this regard.

The digital economy will continue to be a driver for global economic recovery and growth. It is therefore the right time for China and the EU to restart the next round of their recently-launched digital dialogue in order to open new avenues for cooperation.

Volkswagen and ‘automatic driving’

For instance, Volkswagen recently announced a €2.4bn investment to take a 60 percent stake in a joint venture with Horizon Robotics, a Chinese startup specializing in automatic driving and AI. Incorporating the AI technologies of AI, deep-learning and perception-control, automatic driving represents a future trend of the automobile industry and provides a broad stage for China-EU cooperation in digital innovation.

Digital cooperation is also changing business models and market perceptions in China and Europe as online fashion houses expand their business. Mean-while, New Energy Vehicles (NEV) play a central role in both digitalisation and decarbonisation that have topped the agenda in China and Europe over the past few years.

Despite growing competition, there has been excellent cooperation on NEV between China and the EU. China is now the world’s largest NEV market, accounting for more than 60 percent of global sales volume. For European NEV companies and the related industrial chains, the Chinese market is key to their expansion. During the past decades, Chinese-EU cooperation in the automobile industry is largely a story of success, and this story should be continued in NEV industry.

There is also room for cooperation on digital rules and regulations. The EU is a leader in trans-border data flows and data protection. The GDPR adopted by the EU in 2016 has set a series of global standards for trans-border data flows, which also provide an example for China in creating and updating its regulatory frameworks in the digital world. Cooperation in digital rules and regulations would greatly benefit Chinese and Europe digital companies by connecting resources and markets on both sides.

In regulating cutting-edge technologies like AI, China and the EU face common challenges: of striking the right balance between civil rights, socio-economic development and national security. It is important that China and the EU could jointly develop the best practice in this regard.

The digital economy will continue to be a driver for global economic recovery and growth. It is therefore the right time for China and the EU to restart the next round of their recently-launched digital dialogue in order to open new avenues for cooperation.

There is room for cooperation on digital rules and regulations.

As other countries step up their efforts to promote digital innovation and rule-making, China has put forward the Digital Silk Road (DSR) as an integral part of the Belt and Road Initiative (BRI), in a bid to try to improve digital infrastructure and narrow the digital gaps in countries which are part of the BRI.

While the digital world is widely-perceived to be dominated by the US and China, the EU is also seen by China as a global digital power with unique advantages. The EU’s pursuit of “digital sovereignty” means more competition for China but it also presents opportunities for cooperation in areas where there are complementarities between China and the EU.

To tap the potential for cooperation, China and the EU have established a high-level digital dialogue, which provides a valuable platform for discussions between Brussels and Beijing on their respective approaches to digital transformation.

Despite the differences between China and the EU when it comes to terms like reciprocity, fairness and values, digitalisation remains one of the most promising areas for bilateral cooperation. It is thus necessary to identify priorities and new channels to move China-EU digital cooperation to the next level.

Digital innovation stands out as an area where China-EU cooperation could bring benefits to both sides. It is not only closely-related to investment in — and research of — a specific field, but also has a huge influence on the related high-tech industrial chains.
Worse than ‘deep fakes’ — disinfo’s new and more-powerful apps

Forget “old-fashioned” deep fakes, the challenge to democracy posed by “fully-synthetic media” which can be created seemingly out of thin air is much greater.

By HEATHER DANNYELLE THOMPSON
On 24 June 2022, Berlin’s mayor Franziska Giffey had a ‘completely normal video-conversation’ with Kyiv’s mayor Vitali Klitschko. Or so she thought. She started to become suspicious when the supposed mayor asked her to support a gay pride parade in the middle of war-torn Kyiv.

It was not Klitschko, it turned out, but an impostor. Giffey’s office later said the person was probably using deepfake technology to trick Berlin’s mayor (though the tech behind it has remained unclear).

A year or two ago, few were familiar with deepfakes; today most people are. Its popularity is in large part due to its prominence on popular apps, such as face-swaps or AI-powered lip-syncing tech on TikTok.

Once merely a tool for entertainment, disinformation actors have begun to leverage them. This year, 2022, alone saw multiple similar high-profile stunts, from those that were, relatively speaking, less harmful – such as the scam on JK Rowling – to potentially dangerous ones, like the deepfake imitating Ukrainian president Volodymyr Zelensky instructing his citizens to lay down their arms.

But what’s scarier is that deepfakes are themselves rapidly becoming an ‘old-fashioned’ way to create fake video content.

The new kid on the block this year is text-to-image software. Unlike deepfakes, which are partially synthetic and graft the image of one person’s face onto the body of another’s in an existing video, fully synthetic media can be created seemingly out of thin air. This year saw the rise of text-to-image software that seemingly out of thin air. This year saw fully synthetic media can be created from a user’s prompt and — hey presto! — out comes the image. The most popular programs are Partially Synthetic and their text descriptions.

This points to troubling potential: these tools are a dream for a disinformation actor who need only to be able to imagine the ‘evidence’ they need to support their narrative, and then create it.

These technologies are already starting to penetrate social media and images are only the beginning.

Just recently in September, Meta released ‘Make-A-Video’ that enables users to create ‘brief, high-quality video clips’ from a text prompt. Experts warn that synthetic video is even more troubling than synthetic images, given that today’s social media landscape already favours fast and clipped videos, over text or images.

Entertainment aside, the penetration of synthetic media onto an app like TikTok is particularly troubling. TikTok is centered on user-generated content, encouraging people to take existing media, add their own edits, and re-upload — an operating model not too different from deepfake creation.

Recent research by the Associated Press has shown that one-in-five videos on TikTok are misinformation and that young people increasingly use the app as a search engine on important issues like Covid-19, climate change, or Russia’s invasion of Ukraine. It is also significantly harder to audit than other apps like Twitter.

In short, the TikTok app is a perfect incubator for such new tactics, which then commonly spread across the web through cross-platform sharing.

Most disinformation is still created using commonplace tactics like video and sound-editing software. Altering videos by splicing, changing the speed, replacing the audio, or simply taking the video out of context, disinformation actors can already easily sow discord.

Yet, the danger of text-to-image is already real and present. One does not have to expend too much creative energy to imagine the not-too-distant future when untraceable synthetic media appears en masse on our phones and laptops. As trust in institutions and reliable media is already tenuous, the potential impact on our democracies is terrifying to contemplate.

For many of us, seeing is still believing”

Heather Dannyelle Thompson

The sheer density of news today is a compounding part of the problem. Each of us only has a finite capacity to consume news – let alone fact-check it. We know that debunking is a slow and ineffective solution. For many of us, seeing is still believing.

We need to provide an easy and widespread solution to empower users to identify and understand false images or videos immediately. Solutions that do not empower users — and journalists — to identify fake news faster, easier, and more independently will always be a step behind.

Currently, the most promising solutions focus on provenance: technology which embeds media with a transparent and visible watermark at the point of creation, as proposed by Adobe’s Content Au-
A European ‘right-to-repair’: The EU Commission needs to clear way for a circular-economy revolution

The right-to-repair could lead to more green jobs, less waste, better consumer protection and ultimately contribute to saving our planet. However, the European Commission has dragged its feet by repeatedly postponing its proposal on the Right to Repair.

By SARA MATTHIEU, a Belgian MEP and city councillor in Ghent for the Greens.

In the EU and globally, waste from electrical and electronic equipment (known by the acronym, WEEE) has become one of the fastest-growing waste streams, with more than 55m tonnes discarded in 2019.

Although the information and communication technology sector accounts for only a small part of the growing demand for critical raw materials, the sector remains highly dependent on these non-renewable resources.

Materials like lithium copper and rare-earth elements are often extracted and processed in poor environmental and working conditions. The increasingly high demand for these resources, as well as various crises including the ongoing Russian invasion in Ukraine, is posing a serious threat to the supply of these resources. Meanwhile, the recycling rates of many critical raw materials remains abysmal.

It’s clear that our extractive and linear industrial production system and our throw-away culture affects the planet and impacts workers’ conditions. We need to transition to a more circular economy.

In 2018, the International Labour Organisation published a study showing that “a just transition to a more sustainable economy offers much potential for job creation and the promotion of decent work”. To date, labour markets, education and training systems remain inadequately equipped to support the transition to the circular economy. For instance, for every 10,000 tonnes of waste processed per year in the EU, incineration generates just two jobs. Recycling generates 115 jobs, but repair creates up to 404 jobs, according to available data.

We need to improve and accelerate skills, training, and certification, in particular in the repair, reuse and recycling sectors both in the context of the European skills agenda and the recovery plans. EU investment programmes and national recovery plans must work hand-in-hand to boost circular skills and good working conditions. That will allow us to seize the full employment potential of the right-to-repair.

Good for the economy, great for consumers

Moving towards a circular economy can also benefit our consumers and businesses. The shift to a circular economy could help companies to better match their customers’ expectations and societal trends. In fact, 77 percent of consumers in the EU would rather repair their broken devices than buy new ones, according to Eurobarometer.

We can strengthen second-hand markets by requiring consumer-friendly designs that aim at empowering citizens.

Consumers should have the right to receive more information about the repairability of a product. For example, products could feature a repair score with information on the estimated service life, repair services, the duration of availability of software updates and the price of spare parts. We can then do more to make repair more attractive to consumers, for example by reducing the VAT for spare parts at member-state level.

Consumers could also be offered vouchers to partly cover the repair of a defective device, as about a third of consumers decide against a repair due to high costs. The Greens/EFA Group in the European Parliament have repeatedly brought the importance of making repair easy and affordable to consumers to the commission’s attention, like with our “Fix it - Make repairing affordable” action.

We need the right-to-repair now

The right-to-repair will work hand-in-hand with other bold and ambitious policies, such as the Sustainable Product Initiative which introduces circular product design, a digital product passport, mandatory recycled material content in products and more. This entire legislative package must become the leading example of how high consumer protection standards and climate protection work together. Ultimately, the European Union has to seize this opportunity to keep valuable materials and circular jobs within the EU economy.

Systemic change in value creation is fundamental. The industrial revolution saw a tenfold increase in humanity’s mechanical and energy capacity, but since then, the people and the planet have had to pay a steep price. A circular economy is the next revolution that will bring about equally fundamental changes, providing a chance for us to improve livelihoods and safeguard the earth, all at the same time.

Let’s not wait any longer. European Commission, publish the right-to-repair initiative now.
To lead in cyberspace, the EU needs to avoid 'digital tribalism'

To avoid 'digital tribalism' the EU needs a strategy to better engage with the Global South, including the emerging digital powers such as Brazil, Egypt, Ghana, India, Indonesia, Jamaica, Kenya, Mexico, Singapore, South Africa, and Senegal.

By PATRYK PAWLAK

The European Union’s view of digital diplomacy as articulated in July 2022 centres on working closely with ‘like-minded partners’.

Whilst this may be a good starting point, if the EU wants to build broad support and strengthen its position as a norm-setter in the existing and emerging digital technology areas, it needs to remain fully committed to multilateralism as being globally inclusive rather than coalition exclusive.

EU policymakers in Brussels must therefore resist the temptation to form “digital tribes” of the so-called like-minded countries or other values-driven technological alliances.

The EU has established itself as a leader of digital transformation. But as decisions about the future of cyberspace increasingly become part of the geopolitical balancing act, the EU needs to build partnerships that are future-proof and reflect the key trends of the digital world.

Over the past 10 years, at least 70 countries – including Iran, Thailand, Botswana, Ghana, Egypt, Saudi Arabia, and Indonesia – have registered an increase of about 25 percent in their internet pen-
With 2.7 billion people still offline, according to the International Telecommunication Union’s 2022 data, the biggest rise in online population in the coming decades will come from Africa, Asia Pacific, and Latin America. As this happens, these regions are expected to pay increasing attention to digital and cyber policies, including the regional agenda for digital transformation by the Organisation of American States, the ASEAN Digital Masterplan (2021-2025) or the African Union’s Digital Transformation Strategy for Africa (2020-2030). The EU needs to prioritise engagement with those regions to demonstrate the universality of the values it promotes, lead the way in ensuring common standards for the internet, secure market access, and secure their support in multilateral fora.

Currently, the dominant view in the EU is that if it wants to speak the language of digital power, it also needs diplomats who can speak that language. First, to avoid ‘digital tribalism’ the EU needs a strategy to better engage with the Global South, including the emerging digital powers such as Brazil, Egypt, Ghana, India, Indonesia, Jamaica, Kenya, Mexico, Singapore, South Africa, and Senegal, countries which are expanding their influence in cyberspace but are not necessarily part of the like-minded formations.

Second, to set norms and standards globally, the EU should regularly assess how its laws and policies – such as the recently announced cyber defence policy, the NIS II Directive or the ethical principles for AI – may impact other parts of the world. The external effects and unintended consequences for the global, free and open nature of cyberspace need to be anticipated. A proper external impact assessment and genuine consultations with international partners regarding the EU’s planned technology regulation would be a valuable tool.

EU quiet on internet shutdowns

Third, the EU needs to expand the use of the Cyber Diplomacy Toolbox to promote the EU’s vision for a “digital future” globally. Part of that vision is the EU’s commitment to human rights online. But the EU has kept its explicit criticism of practices such as internet shutdowns or the sales of surveillance technology to authoritarian regimes rather quiet. Adopting a more coherent approach and a comprehensive use of all EU tools and instruments, including human rights and political dialogues with third countries, is important.

Finally, the EU’s diplomatic service needs to become fluent in framing and reframing cyber and digital issues to better navigate and exploit the existing international regimes (i.e. trade, human rights, crime). This requires significant investment in strengthening skills and knowledge among the EU’s diplomats, starting from the very top. Only then the EU will be able to achieve its foreign and security policy goals within the existing (or new) international organisations.

With some countries questioning the universality of the EU-promoted norms and values, re-stating their importance and building barricades to defend them will simply not work. Instead, to steer digital transformation globally and shape the future of cyberspace, the EU needs to opt for an ambitious and inclusive network diplomacy that demonstrates why the solutions, standards, and norms it promotes benefit everybody.

In the age of geostrategic competition, leadership is demonstrated not by flexed muscles but by rolled-up sleeves and a willingness to cooperate globally.

Developing regional or country-specific cyber and digital roadmaps might provide a way forward.

First, to avoid ‘digital tribalism’ the EU needs a strategy to better engage with the Global South, including the emerging digital powers such as Brazil, Egypt, Ghana, India, Indonesia, Jamaica, Kenya, Mexico, Singapore, South Africa, and Senegal, countries which are expanding their influence in cyberspace but are not necessarily part of the like-minded formations.

Second, to set norms and standards globally, the EU should regularly assess how its laws and policies – such as the recently announced cyber defence policy, the NIS II Directive or the ethical principles for AI – may impact other parts of the world. The external effects and unintended consequences for the global, free and open nature of cyberspace need to be anticipated. A proper external impact assessment and genuine consultations with international partners regarding the EU’s planned technology regulation would be a valuable tool.

EU quiet on internet shutdowns

Third, the EU needs to expand the use of the Cyber Diplomacy Toolbox to promote the EU’s vision for a “digital future” globally. Part of that vision is the EU’s commitment to human rights online. But the EU has kept its explicit criticism of practices such as internet shutdowns or the sales of surveillance technology to authoritarian regimes rather quiet. Adopting a more coherent approach and a comprehensive use of all EU tools and instruments, including human rights and political dialogues with third countries, is important.

Finally, the EU’s diplomatic service needs to become fluent in framing and reframing cyber and digital issues to better navigate and exploit the existing international regimes (i.e. trade, human rights, crime). This requires significant investment in strengthening skills and knowledge among the EU’s diplomats, starting from the very top. Only then the EU will be able to achieve its foreign and security policy goals within the existing (or new) international organisations.

With some countries questioning the universality of the EU-promoted norms and values, re-stating their importance and building barricades to defend them will simply not work. Instead, to steer digital transformation globally and shape the future of cyberspace, the EU needs to opt for an ambitious and inclusive network diplomacy that demonstrates why the solutions, standards, and norms it promotes benefit everybody.

In the age of geostrategic competition, leadership is demonstrated not by flexed muscles but by rolled-up sleeves and a willingness to cooperate globally.

Patryk Pawlak: ‘The EU has kept its explicit criticism of practices such as internet shutdowns or the sales of surveillance technology to authoritarian regimes rather quiet’

About Patryk Pawlak

Patryk Pawlak leads the work of the European Union Institute for Security Studies on cyber and digital issues. He is project director for the EU Cyber-Direct European Cyber Diplomacy Initiative, and co-editor of the Directions Blog on cyber, digital and tech issues.
Technology

ARTIFICIAL INTELLIGENCE (AI): The field of computer science devoted to designing and building computerised systems or machines capable of performing tasks and making decisions, often using real-time data.

BLOCKCHAIN: A de-centralised, distributed and public digital system that is used to record transactions on multiple computers in a way that makes the verification and traceability of the information very easy.

CRYPTOCURRENCIES: Digital and encrypted currencies, such as Bitcoin and Etheruem, that run without the need for a central authority. There are already more than 18,000 different types of cryptocurrencies in existence.

EDGE COMPUTING: This type of technology refers to capturing, storing, processing and analyzing data near the user, where the data is generated. This is key, for example, for optimizing IoT devices and web applications.

INTERNET OF THINGS (IOT): Network of connected smart devices and often household or domestic objects, from fridges to cars, that transmit and exchange data with other systems over the internet.

MACHINE LEARNING: A discipline of artificial intelligence which focuses on the use of data and algorithms to provide machines with the ability to automatically learn and gradually improve from experience — without being re-programmed.

METAVERSE: A virtual-reality space where humans, as programmable avatars, interact with each other and a computerised environment.

QUANTUM COMPUTERS: Technologies that use the properties of quantum physics to store data and perform computations. Quantum computers, for example, will be particularly transformational for artificial intelligence and machine learning. Big technology companies like IBM, Google and Microsoft are leading the way.

Society

DIGITAL AUTONOMY: The term refers to self-determined choices and decisions in the digital space. When a firm has digital authority, it means they have full control of its IT and data.

DIGITAL DIVIDE: The broad range of social differences regarding the access or use of digital technology and online services. Digital divides exist, for example, between developed and developing countries, urban and rural populations, the elderly and younger generations.

DIGITAL HEALTHCARE: The use of technologies by healthcare professionals in order to deliver diagnoses, treat illnesses, manage health risks or promote wellness. Wearable devices such as Google’s Fitbit or Apple Watch and teletherapy are some examples.

DIGITAL INCLUSION: The political and societal efforts that aim to ensure that information and technology are available to the whole population, including for educational activities, social services, healthcare, and community participation.

DIGITAL SOVEREIGNTY: This phrase has become an important concept for European policymakers in recent years as it refers to Europe’s ability to act independently in the digital world, ensuring that tech European companies can manage production processes (mostly) autonomously.

Other key terms

5G: The fifth generation of mobile network, designed to increase transmission speed and responsiveness of wireless technologies.

ALGORITHM: A set of instructions, step-by-step method, or formula, designed to fulfil a task or solve a problem. Technically, computer and computer-like systems use algorithms to list detailed instructions needed to carry out a specific task.

CLOUD SERVICES: Also known as cloud solutions or cloud computing, these deliver different services through the internet, including data storage, servers, and databases.

GATEKEEPER: In EU legislation, it refers to very large tech companies which have significant and entrenched market power, turnover, and user threshold.

RANSOMWARE: A type of malicious software that threatens to publish or permanently block access to a computer system until a sum of money is paid. Phishing attacks are one of the most common forms of ransomware.

SMART CITIES: An urban area that uses different types of smart devices and sensors to collect specific data to improve citizens’ quality of life and make certain activities more energy efficient. For example, smart mobility applications can ease road congestion.

SURVEILLANCE TECHNOLOGIES: Electronic devices, hardware or software, which allow the monitoring of people or groups’ online behaviour and activities, collecting, capturing, and recording information often in a surreptitious manner.

CONTRIBUTORS

Shada Islam is the editor of EUobserver magazine, columnist for EUobserver, and visiting professor at the College of Europe.

Matt Tempost is comment editor at EUobserver, and a former political correspondent for The Guardian in London, and news editor at AFP in Paris.

Elena Sanchez Nieto is the climate and tech reporter at EUobserver, also responsible for infographics.

Nikolaj Nilsen is migration correspondent at EUobserver.

Easter Zalm is democracy and rule-of-law reporter at EUobserver, focusing on central and eastern Europe.

Wester van Gaal is green economy reporter with EUobserver.

Lukeh Kirk is the founder of EUobserver.

Tomas Lako is sales and marketing director at EUobserver.

Henner Song is sales and marketing manager at EUobserver.

Faridha Salihu-Lukman is an EUObserver intern and a masters student at the VUB Brussels School of Governance.

Dr Antonios Nestoras is intern executive director at the European Liberal Forum.

Francesco Cappelletti is policy and research officer at the European Liberal Forum.

Dr Adenike Adewale is associate professor of leadership ethics and entrepreneurship, and deputy director of studies at Henley Business School.

Dr You Lay Htoe is director of the EU Centre in Singapore.

Yan Shaohua is a research associate professor at the Institute of International Studies, Fudan University.

Yao Xi is a research associate professor at Fudan Development Institute, Fudan University.

Patrik Pawlik leads the work of the European Union Institute for Security Studies on cyber and digital issues.

Heather Dannylee Thompson is manager of Digital Democracy at Democracy Reporting International, the Brussels-based NGO watchdog on elections and democracy.

CREATIVE DIRECTION

Studio Limbo - www.studiolimbo.be

PRINTED BY

Designpress GmbH

ADDRESS

EUobserver

Résidence Palace - International Press Centre

Boulevard de la Loui XV - 1050 Brussels - Belgium

CONTRACT

contact@euobserver.com
THE CIRCULAR ECONOMY REVOLUTION
GOOD FOR PEOPLE AND THE PLANET

The European Commission needs to clear the way for the Right to Repair now. Learn more.