CENL
Foundation Conference of European National Librarians

Marina Kaljurand:

EU digital agenda and responsibilities of big tech companies

Annual General Meeting 2022
19 - 21 June 2022
National Library of Türkiye, Ankara

The Digital Agenda and Responsibilities of Big Tech Companies

Marina Kaljurand

Member of European Parliament, Estonia

Ladies and Gentlemen

First of all, I would like to thank you for giving me the opportunity to address you on the topic of digitalisation and also share my personal experience.

I come from e-Estonia and digitalisation is very close to my heart. Estonia has had the luxury of experiencing the benefits of ICTs, we call it – e-lifestyle – for more than 30 years. It started with recognizing and having digital agenda and cyber security high on political agenda. Then came paperless e-Government, digital signature that saves annually up to 2% of GDP, then came Skype, online voting and more thousand of other online services.

Digital lifestyle means also digital dependency, digital vulnerability, facing digital challenges and taking very seriously cyber security. In 2004 Estonia acceded to the EU and NATO and tried to raise digital topics but our partners and allies were not ready to discuss it seriously. In 2007 Estonia was the first country in the world to fall under cyberattacks supported by another state. I was then Estonian Ambassador to Russia. That way cybersecurity came into my professional life and stays with me since then. The attacks of 2007 were primitive D-DOS attacks that disrupted some online services and took down some websites. They were also a wake-up call for other nations and since then digital topics have gained more and more political attention. In other words – digital topics have moved step by step from the basements where IT geeks work to the upper floors of CEOs and political decisionmakers. COVID pandemic showed very clearly how much we depend on ICT solutions and how important it is to have digitalisation as a political priority.

Digital transformation has gone global, and I am proud that Europe plays a leading role in the process. I can witness this as an European and as a Member of the European Parliament.

The **EU Digital Agenda** represents an ambitious programme of reform to not only tackle online harms, but also to foster technological development, boost a more sustainable economy, and enable European citizens to secure their fundamental rights.

Established in 2010, the first **Digital Agenda for Europe** identified not only the challenges but also the key enabling role of ICTs in reaching Europe's goals. The **Digital Single Market Strategy** in 2015 developed these ideas further and set

out specific provisions to secure a fair, open, and secure digital environment - for example by providing better access for consumers and businesses to digital goods and services, better conditions for digital networks and services, and maximising the growth potential of the digital economy.

More recently, the second five-year digital strategy - **Shaping Europe's Digital Future** - was established in 2020. It focuses on three objectives:

- technology that works for people,

- a fair and competitive economy, and

- an open, democratic and sustainable society.

This is complemented by the 10-year **Digital Compass**, which sets out the EU's digital goals for 2030 in more concrete terms. I would like to mention some examples:

- 80% of adults to have basic digital skills,
- there should be 20 million ICT specialists in the EU, and more ICT jobs for women,
- 75% of companies should use cloud computing services, big data and AI
- all EU households to have gigabit connectivity, and
- all key EU public services should be available online.

My work in the European Parliament in the **Civil Liberties, Justice and Home Affairs or LIBE Committee** has focussed on the protection of citizens in telecommunications by supporting legislation on the fundamental rights to data protection and privacy. The most noteworthy example of this is the **General Data Protection Regulation, known as the GDPR,** which was adopted in 2016. During my time in the Parliament, other important acts have been adopted such as the **Digital Services Act** and **Digital Markets Act**, which will strengthen users' fundamental rights and establish a level playing field for businesses.

Further important Regulations are in the pipeline, such as the **AI Act,** which will set out a risk-based approach for AI systems. I will address these proposals in more detail later.

By setting out a policy agenda to regulate the extensive development of digital service platforms and new technologies like artificial intelligence, the EU is setting standards that impact the development of the technology sector, in particular the handful of companies that have developed monopolies in the sector - otherwise known as Big Tech.

What do we mean when we say Big Tech? Yes, the Big Five come to mind: Google, Apple, Facebook, Amazon and Microsoft have undoubtedly achieved an unprecedented dominance in the field of digital technology over the past 30 years. But monopolies have also been created in other parts of the digital economy. This is why the digital agenda should not be limited to regulating only the biggest tech players today. We need to be more aware of the speed of change and anticipate who the Googles and Amazons of the future will be to avoid repeating the mistakes of the past.

The open Internet has provided incredible benefits to all of us, new economic opportunities, increased possibilities for education and access to information online. At the same time, it has become clear that Big Tech companies - often dubbed gatekeepers - have assumed unprecedented control over our commerce, content, and communications. Better regulation is needed to keep pace with the influence of Big Tech, and to ensure fairness and competition online.

However, while we may expect that the EU's goals of regulating digital technology via the Digital Agenda would often come into conflict with the aims of Big Tech, this is not always the case. We must ensure that EU regulation serves EU citizens. But that does not mean that the interests of Big Tech and citizens are always opposed, nor that we cannot learn from the experience of those working in the tech industry.

In the case of the takedown of terrorist content for example, when there has been political pressure to adopt laws to ensure that content would be taken down within an hour, service providers warned that such strict rules would have an impact on free speech online, as such rules would mean that legal content could also be taken down. Rules on intermediary liability are another example of where caution is needed, as by regulating Big Tech we do not want to undermine the principles of freedom of information that the Internet was founded upon.

It is in cases like these that we must be aware of the sensitivities of regulating new and fast-changing industries, and not be afraid to call on the expertise of industry, academia and civil society when needed. In other words – inclusiveness, public-private-partnership and/or multistakeholderism – should develop from politically correct slogans to reality.

In my remarks I would also like to discuss the challenges we face as a society, both long-term and new, from profiling and COVID, to foreign interference and disinformation. I will then address how this relates to the EU agenda and the European Parliament, both in terms of ongoing legislation and what is expected in the pipeline.

The threat posed by the collection of citizens' data and the power of those who hold this information has become increasingly apparent. The revelations involving **Cambridge Analytica and Facebook in 2018**, for example, showed the extent of this problem. By manipulating the Presidential elections in the US, as well as the Brexit - UK referendum on leaving the European Union, it was clear that the issue had reached the point of threatening our core values, the principle of fair elections and democracy itself.

The practice of gathering and selling our information is not an isolated case. Other companies are carrying out the same practice in order to create algorithms for targeted advertising. This difference is that now we can see that this data gathering has implications not just for conventional economic advertising but that it can also be used for social or political manipulation.

I would argue that in terms of data protection and privacy rights in the EU, we have made progress - privacy is a fundamental right of the EU Charter and is upheld by the recent case law of the European Court of Justice and the European Court of Human Rights. EU citizens have a modern, robust, and advanced level of protection for individuals, which is arguably the strongest in the world and sets a global example.

I am proud that the European Parliament helped to develop these protections. The LIBE Committee in particular has extensive experience in examining this issue. We have kept a track of the failings of Big Tech companies, and, particularly since the Snowden revelations, of the mass surveillance activities of Governments, particularly the United States.

Linked to Government's use of mass surveillance is of course the rise in the use of **Pegasus technology**. The scandal showed that, rather than only being carried out by a limited number of state actors, advanced surveillance technology is now available to any client of the unregulated global spyware industry.

While Pegasus is produced by an arms company, not Big Tech, it is nevertheless demonstrative of the new technologies that the EU must regulate. This spyware, and others like it, is capable of extracting all the information from our mobile phones - reading text messages, tracking calls, collecting passwords, tracking locations, accessing cameras and microphones, and harvesting information from apps. This means that it poses a new and unprecedented threat to leading opposition politicians, human rights activists, journalists, and other political dissidents around the world.

While the technology cannot be rolled back, we can take steps to regulate this surveillance industry. In April 2022, the European Parliament launched an inquiry Committee to examine the use of Pegasus and equivalent software.

Given the real threats posed by this technology, we need to consider ambitious measures such as a global moratorium if we are to protect activists from repressive regimes and to safeguard citizens and companies from unlawful hacking.

In addition to adapting to the threats posed by new technology, the Digital Agenda must also adapt to respond to challenges posed by the societal changes brought about by the COVID pandemic. In this case, new technology provided many solutions to the dislocation created by global lockdowns and travel bans, enabling many individuals to continue working from home and to conduct business and commerce online.

New rules were introduced at the EU level at great speed to respond to these challenges. One example is the **EU Digital Covid Certificate**, which was adopted to ensure that citizens could continue to benefit from free movement throughout the EU. These rules ensured that there was one standard acceptance period throughout the EU, and people who had either been vaccinated, tested, or had recovered from COVID would not face additional restrictions, such as tests or quarantine.

An additional challenge was the need for increased connectivity as an unprecedented level business and entertainment (such as streaming services) moved online. This has required increased vigilance at the EU level, such as the special reporting mechanism established by the Body of European Regulators of Electronic Communications, to ensure that Member States are able to respond to capacity issues.

Increased online activity in the wake of COVID raised the threat of many pre-existing challenges such as disinformation and online safety**.** Many of the existing measures such as codes of practice, information pages, and annual reporting from the Commission are insufficient to address these issues. Making sure that the legislative proposals of the Digital Agenda, such as the Digital Services Act and the Digital Markets Act, are as ambitious as possible is therefore more important than ever.

Further to this, widespread electoral interference continues to be a major issue in many of our Member States and the measures that have been introduced are insufficient to counter the assault on our democracy.

The continuing impact of disinformation, including from foreign actors, is recognised by the Commission. Russia's aggression in Ukraine of course provides the most recent example, with regular attempts to undermine accurate reporting of the war. This active interference is nothing new however and was taking place even during the last European elections in 2019. The Commission

concluded in its report on disinformation following the elections that Russia had engaged in a "continued and sustained" misinformation campaign similar to those carried out in the US, France and other countries.

European elections are only as strong as the weakest Member State. The truth is that some Member States are better prepared than others for future elections, and it would only take a single successful act of disruption on one Member State to cast doubt on the composition of the next European Parliament. If we allow the use of bots and fake accounts to continue unabated, it will leave us in the European Parliament and other democratic institutions vulnerable to attempts to influence us.

The EU Digital Agenda represents a number of positive solutions to these challenges. And the European Parliament has played an important role in scrutinising and amending the new laws, often strengthening them in support of users' fundamental rights.

In response to the foreign interference and disinformation, for example, the Parliament established the **Special Committee on Foreign Interference in Democratic Processes in the European Union, including Disinformation.** The final Report concluded that malicious actors can, without fear of consequence, influence elections, carry out cyber-attacks, recruit former politicians and advance polarisation in public debate.

This interference and manipulation, largely carried out by Russia and China, is exacerbated by loopholes in legislation and a lack of coordination between Member States. We see information being weaponised in Russian aggression against Ukraine, as Russia spreads disinformation of an unparalleled magnitude to deceive both its own citizens and the international community.

In order to enable governments and tech companies to respond to this disinformation, we called for

- a common strategy to tackle disinformation,
- to involve civil society organisations in raising public awareness and
- for more public funding for pluralistic, independent media, journalists, fact checkers and researchers.

We also called for the licences of foreign state propaganda to be revoked (as has been successfully achieved with the EU-wide ban on Russian propaganda outlets such as Sputnik TV and RT.)

These ambitious calls for reform will feed into the future work of the Commission, but as Parliamentarians, we also have a direct impact on many of the laws that make up the Digital Agenda.

One of the most publicised and impactful examples of the direct impact of the European Parliament was of course the GDPR itself.

Adopted in 2016 as part of a package alongside the **Law Enforcement Directive**, these new rules represented a significant improvement on existing data protection legislation, which had gone unchanged since 1995. The European Parliament negotiated with the Council for four years to grant citizens control over their own personal data and achieve the right balance between safeguarding fundamental rights and enhancing police cooperation and the exchange of law enforcement data.

The GDPR gives all EU citizens new positive rights including the ability to know when your data has been hacked, the use of plain language in requests for personal data, the appointment of data protection officers in firms handling large amounts of data, and fines of up to 4% of annual turnover for companies that do not respect the rules.

The main challenge for the EU data protection package, however, was not the texts themselves, but ensuring that they are enforced by the Member States. Four years after the implementation of the GDPR in 2018, the enforcement by Member States has been described as nothing but hot air as Data Protection Authorities have been found to be suffering from insufficient financial resources and staffing leading to substantial discrepancies in enforcement.

For higher standards of personal data in the EU, it is also necessary to ensure it is safe when transferred overseas, particularly as many tech companies that use this data are based in the United States. Under the GDPR, the European Commission is responsible for judging whether our data is safe in foreign jurisdictions.

As you can imagine, given the different standards of privacy afforded in different countries, this process has been far from straightforward. And, as we know, both of the data transfer agreements with the US (**the Safe Harbor and Privacy Shield agreements)** have been invalidated by the European Court of Justice for failing to uphold an equivalent level of protection for the fundamental rights of EU citizens.

The European Parliament has worked to ensure that future agreements do not suffer the same fate, so that businesses can be sure that there are stable agreements for transfers between the US and EU, and at the same time that EU citizens data is protected when it is transferred abroad.

One of the European Parliament Resolutions was the **Resolution on the Schrems II judgement**, in which we have called on the Commission to monitor the use of mass surveillance in the US and other third countries, and to not adopt a new adequacy decision until meaningful safeguards are introduced.

The Digital Services Act, is another step in the EU's approach to regulating Big Tech. This Act specifically tackles illegal online content, and provide stronger protection of users' privacy, like ensuring that consent was required before profiling could take place and providing greater choice in terms of recommender systems on social media feeds.

An agreement has recently been reached between the Parliament and the Council on the Act, which sets out clear responsibility and accountability rules for providers of intermediary services and, in particular, online platforms, such as social media and marketplaces.

LIBEs Committee of the European Parliament focused in particular on issues related to digital privacy, targeted advertising, and content moderation to put citizens' rights at the centre of the framework.

On targeted advertising, we supported measures to ensure greater transparency to tackle interference in elections and limit the spread of disinformation. Further to this, we also won support for a ban on profiling using sensitive data for targeted ads, and a specific ban on the targeting of minors, which is applicable to all online platforms.

Increasing the choice and transparency of recommender algorithms may seem obscure, but this is the system that decides what you see in your social media feed. More transparency on how this information is decided is crucial to reduce disinformation and empower citizens to control the information they are receiving. Platforms currently amplify sensationalist news at the expense of quality news, media diversity, and the mental health of users.

We won support for greater transparency of these algorithms, and **"Very Large Online Platforms"** will now be required to offer an alternative recommender system that is not based on profiling.

We also ensured that there was no change in liability to ensure the free exchange of lawful information and media content online. Internet providers should not be called upon to police the Internet or arbitrarily supress legal content. As long as it is compatible with the purpose of the service, content that is legal online should be allowed online.

The steps we take with the DSA will not just be felt in Europe, but around the world. As the GDPR demonstrated, the EU can set global standards for the regulation of technology.

The Digital Markets Act complements the DSA by targeting large companies providing services that are most prone to unfair business practices, such as social networks or search engines. In March, agreement was reached on this much-

needed proposal, which will introduce new standards for Big Tech companies encouraging fair competition and innovation on the Internet.

DMA would target companies with a market capitalisation of at least 75 billion Euros or an annual turnover of 7.5 billion. To be designated as "gatekeepers", these companies must also provide browsers, messaging, or social media services, which have at least 45 million monthly users in the EU and 10 thousand annual business users. This means that the Regulation will target Big Tech, without penalising small businesses or app developers.

In addition, users will be able to choose their browser, virtual assistants, or search engines. These rules are backed up by fines of up to 10% of companies' total worldwide turnover, even higher than the maximum levels of 4% imposed by the GDPR.

Despite these achievements, the EU Digital Agenda is far from complete and there are many reforms that are still needed.

While it is not a new proposal as such, one such reform is the **e-Privacy Regulation**, which has been blocked between the Parliament and Council for several years. The EU may have a strong data protection framework in place, but this Regulation would increase protections for citizens' communications data. Adoption of the file will mean that we will have clearer rules on how and under what circumstances communications data can be used and when the consent of the user may be required.

Parliament and Council negotiating teams continue to work on a compromise position on rules concerning cookies and the storage of personal data. An agreement on this important file will be pivotal for the effective protection of European citizens' data.

The Data Act, published by the Commission in late February this year, will regulate data access and use in a way that aims to give consumers and companies more control over what can be done with their data. Building on the Data Governance Act, which regulated how public sector data could be re-used by the private sector under specific conditions, the Data Act proposes to make greater use of industrial data, while ensuring that data protection rules are respected.

Specifically, the Act would allow users to make use of data generated by them on connected devices, which may currently only be available to manufacturers. This should lead to increased incentives for manufacturers to continue investing in high-quality data generation. It will also make data from the private sector available to the public sector, enabling services to respond more effectively to public emergencies such as floods or wildfires.

At the end of last year Commission tabled a proposal for the **Regulation of political advertising**. This measure will respond to the impact of the use of targeted advertising and profiling on social media to influence electoral outcomes. We will now discuss and debate the proposal in the European Parliament.

The proposal is a direct response to the manipulation of electoral processes that we saw during the Facebook and Cambridge Analytica scandal in 2018, and which has continued to affect our democratic processes ever since. It would require any political advert to be clearly labelled as such and include information such as who paid for it and how much.

The transparency measures for targeted advertising, which will be introduced by the DSA, are a step in the right direction, but, due to the sensitivity of political adverts, the measures outlined in this proposal are a necessary additional measure to ensure that new technologies are not used for the manipulation of our political processes.

One of the key reforms currently debated is the **Regulation on Artificial Intelligence.** This aims to establish harmonised European standards for AI, **known as trustworthy AI** - principles that will apply to both Big Tech and smaller AI developers. The proposal includes a legal framework for AI to address fundamental rights and safety risks. The approach is based on a risk assessment for AI systems based on four levels of risk from minimal to unacceptable risk.

We are currently debating the proposal in the European Parliament and one of the main concerns is the use AI for biometric mass surveillance. The use of technology such as facial recognition will have a major impact of society, potentially removing the possibility of anonymity in public spaces. It is therefore possible that the use of such biometric AI could be prohibited to protect individuals' fundamental rights.

Once we have reached agreement on the proposal, it will have the dual benefit of raising fundamental rights protections from high-risk AI while also provide increase confidence for developers to create trustworthy AI systems.

I would also like to mention the work on **EU digital identity.** I am convinced that we cannot have fully operational digital single market without trans-European digital ID. I admit that there are still several stereotypes and misperceptions surrounding digital ID. And this is where Estonian experience could shine. Every person residing in Estonia receives a unique identification number. Every child born in Estonia is given digital ID, even before name. E-ID has existed for more than 20 years and is the cornerstone of the e-state. E-ID and the ecosystem around it is part of any person's daily transactions in the public and private sectors.

People use e-ID to pay bills, to vote online, to sign contracts, access digital health system and e-School. I hope that the cartoon by Peter Steiner published in The New Yorker in 1993 - where a dog sitting in front of a computer tells another dog - that *on the Internet nobody knows you are a dog* remains in history.

To conclude, I would like to say that EU Digital Agenda is ambitious but not impossible. The COVID pandemic demonstrated in black and white the central role the digital technologies play in our economy and daily lives. It also showed the urgency with which we need to accelerate Europe's digital transformation. EU institutions should work together to achieve the ambitious goals of the Digital Agenda. I can't agree more to Commission President Ursula von der Leyen who said in her State of the Union speech that *if Europe is not ready to lead digitalization, we will forever have to follow the way of others, who are setting these standards for us.* It is time for EU to become e-EU. It is time for EU to lead global digitalization.

Thank you!