EU Policy News Bulletin

ICT

September 2019

AT A GLANCE: NEW COMMISSIONER PORTFOLIOS - LEAKED DG CNECT ADVICE FOR INCOMING COMMISSIONERS - DISCUSSION WITH THE EUROPEAN COMMISSION ON THE EU DIGITAL ECONOMY - DEBATE ON THE FUTURE ARTIFICIAL INTELLIGENCE LEGISLATIVE FRAMEWORK - HOW CAN BLOCKCHAIN CHANGE THE FUTURE?

Edition Content

GLOSSARY

AI: Artificial Intelligence, the simulation of human intelligence processes by machines, especially computer systems.

COUNCIL OF THE EU: Co-legislator, made up of representatives from Member State Governments. Has a six-month rotating presidency, currently held by Finland until the end of December 2019.

DG: European Commission Directorate-Generals. Department in charge of a certain EU policy area.

DG CNECT: The European Commission Directorate General for Communications Networks, Content and Technology. Directorate General responsible for digital policy.

DG FISMA: The European Commission Directorate-General for Financial Stability, Financial Services and Capital Markets Union.

E-PRIVACY: Proposal by the European Commission for a Regulation on Privacy and Electronic Communications aimed at increasing privacy for individuals and entities, and reinforcing trust and security in the Digital Single Market, by updating the legal framework on ePrivacy.

EP: European Parliament, institutions of the European Union constituted of 751 Members of Parliament directly elected by European citizens.

GDPR: General Data Protection Regulation, it replaces the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy and reshape the way organizations across the region approach data privacy.

MEP: Member of the European Parliament, a co-legislator within the EU that is made up of representatives from political parties throughout Member States.

Edition Content

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

EU ELECTIONS

New Commissioner portfolios

©Shutterstock

At the beginning of September, European Commission President-elect Ursula von der Leyen announced the composition of her Commission.

The new structure will see three Executive Vice-Presidents (European Green Deal, Europe Fit for Digital Age and An Economy That Works for People), and five Vice-Presidents. The difference is that Executive Vice-Presidents will have access to staff from Commission Directorates-General (DGs) and directly manage a wide range of policy initiatives, while also overseeing wider thematic areas. This makes them very powerful. The other five "non-executive" Vice-Presidents will be overseeing thematic objectives, but not leading a DG directly.

Of interest for IEEE, different aspects of digital policy are split between a number of Commissioners. The most relevant is French Commissioner **Sylvie Goulard**, responsible for the Single Market, whose portfolio includes blockchain, algorithms, 5G and cybersecurity (certification, implementing rules on network and information system security etc). She will also be responsible for building the joint Cyber Unit that was announced by von der Leyen as part of her priorities.

Sylvie Goulard's role appears to be extremely influential, as she takes the lead on number of key issues, while overseen by Executive Vice-President **Margrethe Vestager**, who has responsibility for competition policy. Partnering the French and Danish Commissioners could result in a delicate balance between the traditionally more protectionist French approach and the more liberal Danish one. It also must be noted that Goulard will play a key role in the EU's recent assertiveness and attempt to move towards digital independence by creating its own companies and technologies in order to reduce dependence on the US and China.

Other aspects of digital policy are included in the portfolios of Belgium's **Didier Reynders** (Justice, covering GDPR), Bulgaria's Mariya Gabriel (Innovation and Youth, covering investment in innovation), and Czech Republic's **Vera Jourova** (Values and Transparency, covering illegal content online, disinformation etc.

(Source: European Commission & Interel)

Edition Content

If you have any suggestions for
content, or would like to know
more about IEEE's European Public
Policy activities, please contact
eppc@ieee.org. Thank you

EU DIGITAL POLICY PRIORITIES

Leaked DG CNECT advice for incoming Commissioners

©ShutterStock

A leaked version of a **document** from the European Commission Directorate General for Communications Networks, Content and Technology (DG CNECT) for Commissioners Margrethe Vestager (Executive Vice-President-designate for a Europe fit for the Digital Age and responsible for competition policy) and Sylvie Goulard (Commissioner-designate for Internal Market) was published in the media on 24 September.

The document provides advice on topics the Commissioners should focus on, emphasising in particular artificial intelligence, the Digital Services Act, greening technology and enhancing Europe's technological sovereignty as immediate priorities. It stresses the need to find "A European way of doing digital policy that is human-centric and founded on respect for fundamental rights and European values, distinct from a laissez-faire approach (privately-ruled digital economy and society), and a top-down controlled model".

DG CNECT proposes actions along four broad policy areas: A Europe fit for the digital age; Digital for a European Green New Deal; Digital for European Democracy; A stronger Europe in the digital world. Therefore, it is suggested that the following short-term actions be adopted:

- Artificial Intelligence (AI) regulatory framework within the first 100 days of the new Commission;
- Digital Services Act and Greening ICT by the end of 2020;
- Enhancing Europe's technological sovereignty, as part of a broader industrial strategy.

With regards to the new AI regulatory framework, the EU wants legislation to protect, though enhanced transparency, safety and robustness, and to empower, through the use of data and EU cooperation on AI development. The general assessment is that the GDPR does not address the entire spectrum of risks associated with the use of AI in various applications. The lack of clarity can lead to regulatory fragmentation and there are also concerns with risk posed for fundamental rights.

Moreover, data access is seen as a perquisite for the competitiveness of EU businesses. As part of the AI framework, issues related to quality, transparency

Edition Content

and interoperability of data, as well as further barriers to data reuse in specific sectors (e.g. health, energy, manufacturing) should be tackled. This should create common data spaces in specific sectors. Access to data is particularly needed to ensure effective competition, especially when data are key to market dominance. For instance, the EU will ensure that Internet of Things data can be exploited and does not lead to market foreclosure (e.g. in aftersales or repairs markets). It will also ensure that public sector bodies are provided with access to private sector data for specific tasks at preferential market conditions.

Finally, the document outlines the EU's strategy to ensure increased cyber resilience of critical infrastructures, and cybersecurity by design of ICT products and services. The EU has three priorities in this area: cooperation and information sharing should follow the spirit of "need to share" rather than ":need to know"; critical infrastructure and other users should be able to use cybersecure ICT products and services; cybersecurity governance at the EU level needs to be strengthened, allowing for a collective response to serious threats and incidents.

A review of the NIS Directive is suggested to "bring its pillars to the next level" (national capabilities, EU cooperation and risk management for key companies). In addition, the cybersecurity of products and services needs to be covered in a horizontal way (currently not the case with the Cybersecurity Act). It is proposed that a "cybersecurity by design" approach is considered by establishing common cybersecurity requirements for products and services to be placed in the EU market. This could be achieved via a co-regulatory approach with the industry or via specific legislation.

Work on certifications due to the cybersecurity act will continue, together with more investment in "made in the EU' cybersecurity solutions and the creation of a Joint Cybersecurity Unit to allow for a structured and coordinated mutual assistance mechanism at EU level in response to serious incidents.

(Source: European Commission & Interel)

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Edition Content

If you have any suggestions for content, or would like to know more about IEEE's European Public Policy activities, please contact eppc@ieee.org. Thank you

Discussion with the European Commission on the EU digital economy

©Shutterstock

On 20 September, Interel attended a meeting on the digital economy at the American Chamber of Commerce to the EU. The guest speaker was Renate Nicolay, Head of Cabinet of Commissioner Jourova, currently responsible for Justice and Consumers, and chosen to be responsible for democracy and rule of law issues in the new Commission.

Future challenges are to make the EU fit for a digital age, and in particular boosting Artificial Intelligence (AI) and EU technological sovereignty, while marrying these goals with privacy.

Of particular interest for IEEE is the latest intelligence on the upcoming AI legislation, which will be a transparency-focused legislative act, perhaps accompanied by a non-binding document on undertaking impact assessments. A definition of AI will be included and this is only the first legislation on the topic, with more initiatives expected.

Artificial Intelligence: The first piece of legislation ("first 100 days") will probably be a horizontal legislative proposal on transparency, accompanied by something non-binding on undertaking impact assessments. It will probably not contain anything on liability, but likely include a definition of AI. Not much planned on the liability question at the moment. Ms Nicolay believes we need a balanced regulatory approach to AI and that there is a clear link to industrial strategy, therefore, we need to do it in a privacy-conscious way. The challenge is to give a European touch to the next step of regulating AI. This will be very different from the Chinese and US approach. The work on the first 100 days will not be final. This will be a principles-based legislation, but more will follow.

GDPR implementation: According to the Commission, gold-plating should be avoided and a harmonised approach maintained. The upcoming review is an opportunity to fix a few things, but a total re-write should be avoided. On the international side, data transfers must be kept intact. There is a good relationship on the privacy shield and a report on that can hopefully be published before the end of the mandate. However, the Schrems case, although focussing on standard contractual clauses, can affect the privacy shield too. Adequacy decisions need to be updated and data access for national security or the public need to be made compatible with the GDPR.

Edition Content

New portfolios: Commissioner Jourova will be involved in digital policy. The new organigram does not follow the "institutionalised" mentality, but is shaped around societal issues. This is new and breaking out of the "silo mentality". The new structure will keep elements of the old, for example Vice Presidents will oversee project teams. Collegial debates are necessary and there will be an effort to not keep this as a closed shop.

Digital sovereignty: A balance will have to be found between a constructive and critical debate. The main line seems to be that Europe must not "disconnect itself" by imposing restrictions to US and other companies in procurement. Some of the policy goals are legitimate, but we need to be careful that levelling the playing field does not come back to bite us (e.g. the US has restrictions, which could be replicated here). A lot of the measures are geared towards China.

E-privacy: The Finnish presidency has scheduled a number of meetings and Germany has released a position paper on the topic. A new text has been released following the 9 September meeting. This includes changes in the sexual abuse content provisions and on the wording on transmission. The Commission is looking at alternatives, possibly even a recast of the proposal. The official Finnish Presidency goal is for a General Approach in December, but that is unlikely. Industry groups are preparing a joint statement.

Data sharing: The Commission is preparing possible actions to facilitate data transfers and sharing, therefore, feedback is currently being gathered from stakeholders.

(Source: Interel)

Edition Content

If you have any suggestions for
content, or would like to know
more about IEEE's European Public
Policy activities, please contact
eppc@ieee.org. Thank you

Debate on the future Artificial Intelligence legislative framework

On 24 September; Interel attended a meeting on Artificial Intelligence (AI) at the American Chamber of Commerce to the EU. The guest speaker was the Director-General of the European Commission Directorate General for Communications Networks, Content and Technology (DG CNECT), Roberto Viola. His speech was preceded by a panel discussion with Pascal Rogard, Attaché at the French Permanent Representation; Dita Charanzova, Czech Liberal MEP and EP Vice-President; Andrea Renda from CEPS and the HLEG on AI; and Joan Val Loom from IBM Belgium-Luxembourg.

©Shutterstock

The discussion held reiterated the intelligence we have received so far about the upcoming legislative proposal on AI, namely that it will focus on transparency and be principles-based, rather than too prescriptive and limiting.

Panellists were particularly sceptical about the "100 day" commitment to introduce legislation, given Better Regulation procedures, the need for consultations, impact assessments etc. Pascal Rogard noted that France considers transparency and facial recognition as key aspects to be addressed. Dita Charanzova commented that the discussion has shifted from the Digital Single Market to a Single Market for AI, adding that consumer trust is a key issue. She stressed that the European Parliament also wants to look at product liability, while we would need to review existing legislation to determine whether it is fit for the 21st century.

Andrea Renda added that legislation will be based on the AI High-Level Expert Group's recommendations and he does not expect a heavy-handed legislation, except for "areas of critical concern", such as mass scoring, biometric data, facial recognition. No bans in the first instance, but transparency obligations as the first step. He was less pessimistic that the EU has missed the AI train, adding that this technology is still in its infancy and the new wave of AI is different to the previous one. The EU has a competitive advantage in a number of sectors and should focus

Edition Content

on those. Data is a key issue that will not be addressed under AI legislation, but as part of industrial policy. The data we have now is a drop in the ocean compared to the data to come so we have not yet missed the train. We will need to keep data as close as possible to where value is created.

Moreover, Joan Van Loon stressed the need for trust and transparency on AI, adding that many aspects are already regulated (liability, consumer protection). He cautioned against regulating AI too soon. He underlined the importance of business to business AI applications which are not the ones widely seen (compared to business to consumers). AI will be used in decision support, more "augmented intelligence" than artificial. Any system we build needs professionals to support it and this is where we have the question of skills. This starts at the school and university curriculum level, while reskilling is also an issue.

Finally, Director-General Robert Viola, in his keynote, reiterated that decisions on next steps are for the new Commission to make. He downplayed differences between the EU and the US, choosing to focus on the areas where cooperation is possible. He noted, however, that "our investment programmes are open and we expect the same from others". On EU-China relations, he repeated that the recent Commission communication showed the opportunities and limits in cooperation. He also stressed that the EU does not "name and shame", but has certain principles (rule of law) which are clear.

(Source: Interel)

If you have any suggestions for

content, or would like to know

more about IEEE's European Public

Policy activities, please contact

eppc@ieee.org. Thank you

Edition Content

If you have any suggestions for
content, or would like to know
more about IEEE's European Public
Policy activities, please contact
eppc@ieee.org. Thank you

BLOCKCHAIN

How can Blockchain change the future?

On 9 September, Interel attended an event on blockchain entitled "How can Blockchain change the future?", at the British Chambers of Commerce, with Peteris Zilgalvis, Head of Unit for Digital Innovation and Blockchain at the European Commission's (DG CNECT).

©Shutterstock

The main point to take is that the Commission is considering blockchain as a promising solution for cases where you have multiple actors who do not want to share a single database, also at Member State level. In the regulatory field, the Commission is looking at shaping legal clarity on blockchain. However, this decision is to be taken by the incoming Commission. The focus will be on smart contracts and tokenisation (utility tokens to run decentralized systems for investment products). The new rules will be housed under either e-commerce, investment legislation or consumer protection. In principle, there will not be a regulation on blockchain, in the same way there is not a regulation on servers. Work will most likely be led by the Commission's Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA) and DG CNECT's e-commerce team.

Mr Zilgalvis also described the work of the EU Blockchain Partnership and the Blockchain agreement. It is currently deploying infrastructure/public services by the end of 2019 and identifies use cases of blockchain where it can be useful. One example is regulatory reporting where there would be a legal requirement for Member States to share data. Based on a pilot, 80% savings could be made.

To conclude, the EU will only regulate Blockchain indirectly via other legislation tangentially linked to this technology.

(Source: Interel)