EU Policy News Bulletin

ICT

April 2019

AT A GLANCE: EU MEMBER STATES TO DISCUSS COMMON POSITION AHEAD OF G20 - DEVELOPMENTS ON THE EU CYBERSECURITY ACT AND THE EU COMPETENCE CENTRE PROPOSALS - COMMISSION RECOMMENDATION ON THE CYBERSECURITY OF 5G NETWORKS - ARTIFICIAL INTELLIGENCE ETHICS GUIDELINES - LAUNCH OF THE INTERNATIONAL ASSOCIATION FOR TRUSTED BLOCKCHAIN APPLICATIONS - REPORT ON THE IMPACT OF DIGITAL TRANSFORMATION ON THE EU LABOUR MARKETS

Edition Content

GLOSSARY

AI HLEG: European Commission led High-Level Expert Group on Artificial Intelligence composed of 52 experts from industry, academia, and civil society, with the aim to support the implementation of the European initiative on artificial intelligence.

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

ECOFIN: Economic and Financial Affairs Council configuration. Part of the Council of the EU, this configuration is responsible for EU policy in three main areas: economic policy, taxation issues and the regulation of financial services.

ENISA: The European Cybersecurity Agency is the centre of expertise for cyber security in Europe and is located in Athens, Greece.

G20: An international forum for the governments and central bank governors from 19 countries and the European Union.

G7: A group consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, comprising the seven largest IMF-described advanced economies in the world, represent 58% of the global net wealth.

INATBA: International Association for Trusted Blockchain Applications, which aims at encouraging the global governance and development of blockchain technology.

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

STEM: Science, technology, engineering and mathematics.

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

DIGITAL TAX

EU Member States to discuss common position ahead of G20

©Shutterstock

The Economic and Financial Affairs Council configuration (ECOFIN) meeting in May will discuss a common EU position on the digital tax, with the aim of having a clear view for the international debate, ahead of the G20 finance ministers and central bank governors meeting in Osaka in late June. Since smaller EU Member States voiced concerns about being left outside the international discussions, the Commission offered to step in and represent the bloc as a whole to address these concerns.

At the preparatory informal ECOFIN meeting in Bucharest in early April 2019, French Finance Minister Bruno Le Maire outlined a three-step approach on taxation reforms, which would entail the taxation of Internet companies based on turnover by 2020; the introduction of a minimum corporate tax rate; and the definition of goods taxed on the basis of production or consumer location. France is expected to lead the push for talks at the international level, when it hosts the G7 meeting at the end of August 2019.

Meanwhile, a number of EU Member States have introduced or are planning to introduce their own version of the digital tax. These include France, Germany, Spain, the UK, Italy, Austria and the Czech Republic.

Elsewhere, Competition Commissioner Margrethe Vestager offered her support for national digital tax measures, commenting that "the inconvenience of a fragmented digital taxation" is a step forward and, although a solution at the international level is preferable, this is nevertheless one way to ensure action in a reasonable timeframe.

(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

CYBERSECURITY

Developments on the EU Cybersecurity Act and the EU Competence Centre proposals

© ShutterStock

Following the formal endorsement of the **provisional agreement** on the EU Cybersecurity Act on 12 March by the European Parliament, all EU political groups welcomed it as an essential component for the protection of European interests and citizens. The legislation will strengthen the mandate of the European Cybersecurity Agency (ENISA) and will create a European certification scheme, operating on a voluntary basis.

The Council of the EU must now approve the agreement on the Cybersecurity Act before it is published in the Official Journal of the European Union. It will enter into force on the twentieth day after its publication.

The attention is therefore shifting to the implementation of the Act, as ENISA is taking forward the work on creating certification schemes, with cloud and 5G as immediate priorities. However, there is some industry concern that the first schemes on cloud and 5G will be rushed out. Meanwhile, ENISA Executive Director Udo Helmbrecht will be replaced, possibly over the summer.

With regards to the EU Competence Centre and the Network of National Coordination Centres proposal, both the European Parliament and the Council of the EU reached their respective positions on 13 March.

Representatives from the European Parliament, the Council of the EU and the European Commission already entered into trilogue negotiations. Overall, there is great support for this proposal, as the Competence Centre aims at enhancing the coordination of research and innovation in the field of cybersecurity and becoming the EU's main instrument to pool investment in cybersecurity research, technology and industrial development, while the National Coordination Centres should provide the technical expertise in cybersecurity.

Nevertheless, there is still quite a difference in perspective on issues such as the tasks of the Competence Centre, its financing and decision-making. There also appears to be a complex interaction with the Digital Europe and Horizon Europe

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

programmes. A number of Members of Parliament (MEP) and national attachés believe that more clarification is needed on the contribution by Member States.

Therefore, on 17 April 2019 the European Parliament voted to close the first reading of the file with 480 votes in favour, 70 against and 60 abstentions. This was a procedural vote to ensure the Parliament's position is endorsed by the Plenary. Trilogue negotiations on this file will be resumed under the new Parliament, with a new file Rapporteur, since MEP Julia Reda (Greens/Germany) is not running for the next parliamentary term.

 (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

Commission recommendation on the cybersecurity of 5G networks

©Shutterstock

On 26 March, the European Commission **published** a Recommendation on the Cybersecurity of 5G networks. The document is an attempt to address concerns raised over Huawei's involvement in the roll out of 5G networks in Europe, but without going for a full ban (along the lines of US rhetoric). The main line to take is that a risk assessment needs to be undertaken and follow-up action taken up depending on the results of this assessment. Supply chain and the legal and policy framework of suppliers will feature into the risk assessment, highlighting the importance of the political environment, especially from third countries.

During the presentation of the recommendation, the Vice-President of the Commission, Andrus Ansip, noted that "we have some concerns with some producers", naming China and Huawei. However, he noted that the Commission was "not asking for a ban on any suppliers" but "by the time we have enough evidence allowing us to go public, it will be too late. We have to undertake our risk assessment now".

The Commissioner for the Security Union, Julian King, was keen to stress that the risk assessment envisaged in the recommendation was something that would have to be undertaken anyway and was not targeted at any one company, or dictated by any other country. While Ansip added that, according to Chinese law, Chinese companies need to collaborate with security services, King commented that "legal and policy frameworks governing potential third country suppliers" would have to be taken into account in the risk assessment.

The first step suggested by the Recommendation is that, by June 2019, Member States would have to undertake a risk assessment to identify risks and look at how to mitigate them. They should look at supply chain diversity, technical factors, legal and policy frameworks governing potential third country suppliers. On this basis, Member States should update existing security requirements for network providers and include conditions for ensuring the security of public networks, especially when granting rights of use for radio frequencies in 5G bands. It is worth noting that EU Member States have the right to exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework.

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

Then, by October 2019, the individual national risk assessments should be woven together into a European review of 5G network security. These should prioritise the most sensitive and vulnerable aspects. Therefore, Member States will agree on a set of mitigating measures that can be used at national level. These can include certification requirements, tests, controls, as well as the identification of products or suppliers that are considered potentially nonsecure.

Finally, by the end of 2019, a toolbox of measures will be presented for both at national and European level to mitigate security threats and develop common minimum standards for cybersecurity of 5G networks across the EU. The toolbox will include an inventory of the types of security risks that can affect the cybersecurity of 5G networks; and a set of possible mitigating measures. Member States and the Commission will also develop specific security requirements in the context of public procurement for 5G, which should include mandatory requirements to implement cybersecurity certification schemes in public procurement.

(Source: European Commission)

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

ARTIFICIAL INTELLIGENCE

Artificial Intelligence Ethics Guidelines

©Shutterstock

The final **Artificial Intelligence Ethics Guidelines** were published on 8 April 2019, by the **High-Level Expert Group** on Artificial Intelligence (AI HLEG), composed of 52 experts from industry, academia, and civil society.

Following the publication of the **draft AI ethics guidelines** in December 2018, to which more than 500 comments were received, the expert group agreed on a series of ethical requirements for AI, in order to make AI "trustworthy" based on a human-centric approach. The industry is invited to test these requirements in an upcoming pilot phase in Q3 and Q4 of 2019.

These guidelines are part of the Commission's three-step approach of setting out the key requirements for trustworthy AI, launching a large scale pilot phase for feedback from stakeholders, and working on international consensus building for human-centric AI.

Human agency and oversight is the first of the seven essential requirements for achieving trustworthy AI. Indeed, AI systems should enable equitable societies by supporting human agency and fundamental rights, and not decrease, limit or misguide human autonomy.

Robustness and safety are the second requirement. Trustworthy AI requires algorithms to be secure, reliable and robust enough to deal with errors or inconsistencies during all life cycle phases of AI systems.

Thirdly, privacy and data governance are essential. Citizens should have full control over their own data, while data concerning them will not be used to harm or discriminate against them. With regards to access to data, it is recommended that, in any given organisation that handles individuals' data, protocols governing data access should be put in place to outline who can access data and under which circumstances.

The fourth requirement is transparency. Since the traceability of AI systems is essential, data sets and algorithms, should be ensured and any decision made by an algorithm should be verifiable and explained.

Edition Content

Diversity, non-discrimination and fairness is the fifth requirement. AI systems should consider the whole range of human abilities, skills and requirements, and ensure accessibility, especially during the algorithms' programming. Oversight processes to analyse and address the system's purpose, constraints, requirements and decisions might be put in place.

Societal and environmental well-being is the sixth requirement. AI systems should be used to enhance positive social change and enhance sustainability and ecological responsibility.

Finally accountability is essential as mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes.

In May 2019, the AI HLEG should publish its second deliverable on "Policy and Investment Recommendations", which in turn will take a more policymaking angle in looking at how to boost European investment in AI and how much regulation is needed.

By the end of June 2019, the Commission will launch a pilot phase, which will be a practical implementation assessment of the AI ethics requirements. Through the European AI Alliance, industry, research institutes and public authorities are invited to test the detailed assessment list, which complements the guidelines. The results will be reviewed by the expert group in early 2020 and building on this, the Commission will evaluate the outcome, update the assessment list, and might move on to the legislative stage if deemed necessary.

Moreover, the Commission will by the autumn 2019 launch a set of networks of AI research excellence centres; begin setting up networks of digital innovation hubs; and together with Member States and stakeholders, start discussions to develop and implement a model for data sharing.

(Source: AI HLEG)

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 TECHNOLOGY

Launch of the International Association for Trusted Blockchain Applications
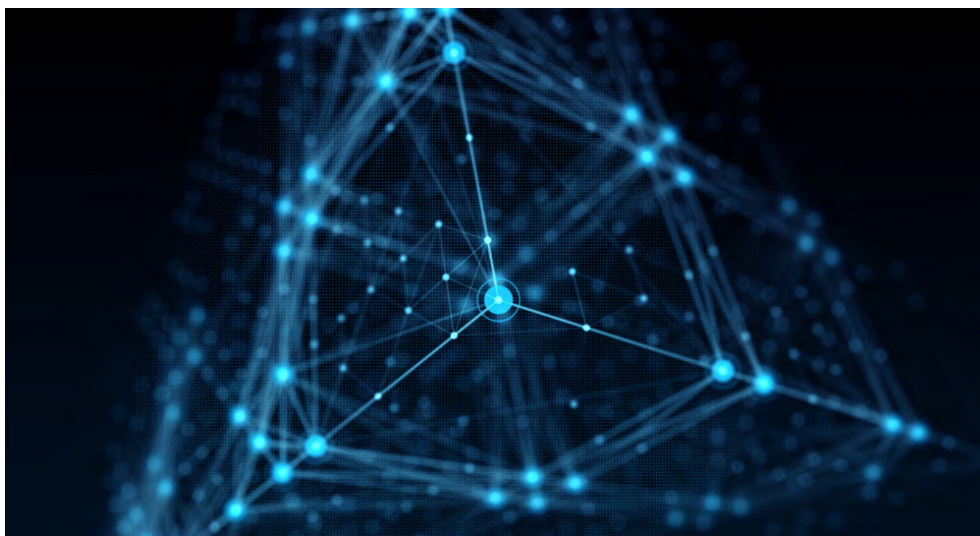
©Shutterstock

A new international association with the aim of encouraging the global governance and development of blockchain technology was launched on 3 April in Brussels.

The International Association for Trusted Blockchain Applications (INATBA) brings together industry, start-ups and SMEs, policy makers, international organisations, regulators, civil society organisations and standard setting bodies to support the roll-out of blockchain and distributed ledger technology across multiple sectors. It aims to develop a framework that promotes public and private sector collaboration, regulatory convergence, legal predictability and ensures the system's integrity and transparency.

Speaking ahead of her keynote speech to the inaugural meeting of the International Association for Trusted Blockchain Applications (INATBA), Mariya Gabriel, Commissioner for Digital Economy and Society praised the potential of blockchain technology to increase trust in the security and reliability of information and welcomed INATBA's "ambitious goals" of bringing together "a range of stakeholders on blockchain and distributed ledger technologies" to "develop a governance structure that works for everyone".

In 2018, the European Commission launched the **European Blockchain Partnership**, in order to develop a European Blockchain Services Infrastructure that will support the delivery of cross-border digital public services, with the highest standards of security and privacy, as well as the **EU Blockchain Observatory and Forum,** with the support of the European Parliament. Blockchain technology is also a key part of the **FinTech Action plan** as well as of the priorities for the **Digital Europe Programme**.

(Source: INATBA)

Edition Content

DIGITALISATION

Report on the impact of digital transformation on the EU labour markets

The European Commission-led High-Level Group on the impact of digital transformation on EU labour markets handed over its report on 10 April 2019 to Commissioner for Employment, Social Affairs, Skills and Labour Mobility, Marianne Thyssen, and Commissioner for Digital Economy and Society, Mariya Gabriel, unveiling its list of recommendations.

Commissioner Marianne Thyssen welcomed the **report on 'The impact of digital transformation on EU labour markets'** and committed to examine its recommendations and identify policy gaps where the Commission could act.

Among their recommendations, the experts called upon different actors on the labour market to reduce structural skill gaps, especially for women in science, technology, engineering and mathematics (STEM), workers at risk of automation and the low-skilled.

Personal learning trajectories should allow workers to acquire relevant skills throughout their careers in order to keep up with rapidly transforming, digital labour markets.

New labour relations should intensify and better organise dialogue of workers and social partners, especially in the platform economy.

Finally, social protection against unemployment, sickness and other life circumstances should be accessible independent of employment status.

(Source: European Commission)

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