EU Policy News Bulletin

ICT

March 2019

AT A GLANCE: EU MEMBER STATES PLACE DIGITAL SERVICES TAX ON HOLD - DEVELOPMENTS ON THE EU CYBERSECURITY ACT AND THE EU COMPETENCE CENTRE PROPOSALS - EUROPEAN COURT OF AUDITORS SAYS THERE ARE MULTIPLE CHALLENGES IN EU CYBERSECURITY - ETHICAL CONCERNS OF ARTIFICIAL INTELLIGENCE - EUROPEAN PARLIAMENT RESEARCH CENTRE STUDY ON ALGORITHMIC DECISION-MAKING

Edition Content

GLOSSARY

COMMITTEE: Members of the European Parliament are divided up among 20 specialized standing committees. These committees instruct proposals through the adoption of reports, propose amendments to Plenary and appoint a negotiation team to conduct negotiations with the Council on EU legislation.

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.

EPRC: The European Parliament Research Centre is the European Parliament's in-house research service and think tank.

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

OECD: Organisation for Economic Co-operation and Development. It is an intergovernmental economic organisation based in Paris, France, with 36 member countries, founded in 1961 to stimulate economic progress and world trade.

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 place digital services tax on hold

©Shutterstock

The Economic and Financial Affairs Council configuration (ECOFIN) confirmed on 12 March that the proposal for an EU-wide digital services tax will be placed "on ice", after four Member States (Ireland, Denmark, Sweden and Finland) maintained their "fundamental" opposition to the proposal.

The attention now turns to the work of the Organisation for Economic Co-operation and Development (OECD), which is working towards a global solution to the taxation of the digital economy. Commenting on the part of the European Commission, Commissioner Pierre Moscovici, responsible for Economic and Financial Affairs, Taxation and Customs, stated that negotiations could be relaunched, if talks at the international level become gridlocked. The Romanian Presidency of the Council of the EU commented that it would work to ensure a common position in the context of the OECD's work and "revert" to the proposal, if "by the end of 2020 it appears that an agreement at OECD is bound to take more time".

On 13 and 14 March, the OECD hosted a debate on "Addressing the Tax Challenges of the Digitalisation of the Economy". As explained by Brian Jenn, US Department of Treasury and Co-Chair of the Task Force on the Digital Economy, the aim of the debate was to get an overview of the stakeholders' input to the public consultation **document**, which the OECD published on 13 February as part of its ongoing work on the Inclusive Framework on Base Erosion and Profit Shifting and its Task Force on the Digital Economy. The public consultation fed the work of the OECD on this matter, in order to develop a work programme to be presented to the Inclusive Framework at the end of May, to the G20 Finance Ministers at the beginning of June, and, lastly, to the G20 leaders at the end of June.

(Source: Interel + OECD)

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

The **provisional agreement** on the EU Cybersecurity Act was formally endorsed by the European Parliament with a very large majority in the plenary session of 12 March.

All political groups welcomed the Cybersecurity Act 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. Some MEPs regretted the lack of ambition in the text, as they had hoped mandatory certification for critical infrastructure would be included. The Council is expected to formally approve the Cybersecurity Act shortly as well, so that the regulation can enter into force 20 days after it is published in the Official Journal of the EU.

Moreover, 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 a their respective positions on 13 March.

Representatives from the European Parliament, the Council of the EU and the European Commission already entered into negotiations in order to agree on a common text before the European elections in May 2019. 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. The most contentious issue between the European Parliament and the Council of the EU is on how much of an institution this Cybersecurity Centre should become, as the former thinks it is important that the Competence Centre is executing a common European strategy for cybersecurity rather than only distributing funding for national projects.

(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

European Court of Auditors believes there are multiple challenges in EU cybersecurity

According to a new **Briefing Paper** from the European Court of Auditors on the EU cybersecurity policy, multiple challenges in strengthening EU cybersecurity remain despite progress made. As the risk of falling victim to cybercrime or a cyberattack increases, they say it is essential to build resilience through strengthening governance, raising skills and awareness, and improving coordination. They also highlight the importance of meaningful accountability and evaluation to help the EU achieve its aim of becoming the world's safest digital environment.

The authors consider the challenges facing cyber policy under four main headings: the policy and legislative framework; funding and spending; building cyber-resilience; and responding effectively to cyber incidents.

Firstly, the policy and legislative framework on cybersecurity is complex and multi-layered, according to the paper. Trying to forge all parts together into a comprehensive, strategic, coherent and coordinated way is a key challenge. Developing action aligned to EU cybersecurity strategy is a challenge in the absence of measurable objectives and scarce, reliable data. Outcomes are rarely measured and few policy areas have been evaluated, including the state of EU cybersecurity and readiness. The challenge is therefore to shift towards a performance culture with embedded evaluation practices.

Secondly, funding and spending in the EU on cybersecurity has been low and fragmented. The EU and its Member States need to know how much is being invested collectively to know which gaps to close. There is no dedicated EU budget to fund the cybersecurity strategy or a clear picture of what money goes where. The European Commission is working to overcome fragmentation in the cybersecurity research field, but to date results from investment in research are often not well patented, commercialised or scaled up, holding back the EU's resilience, competitiveness and autonomy.

Thirdly, the absence of a coherent, international cybersecurity governance framework impairs the EU's ability to respond to and prevent cyberattacks. Weaknesses in cybersecurity governance abound in the public and private sectors across the EU. This poses a challenge to a coherent EU-wide approach to cybersecurity. In addition, given the growing global cybersecurity skills shortfall, raising skills and awareness across all sectors and levels of society is essential.

Lastly, digital systems have become so complex that preventing every attack is impossible. The challenge is therefore on rapid detection and response. Cybersecurity is not yet fully integrated into existing EU-level crisis response coordination mechanisms, potentially limiting the EU's capacity to respond to large-scale, cross-border cyber incidents. The potential interference in electoral processes and disinformation campaigns is also a critical challenge, especially in view of the European Parliamentary elections in May 2019.

(Source: European Court of Auditors)

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

Ethical concerns for Artificial Intelligence

On 19 March, the European Parliament organised a seminar on ethical concerns for Artificial Intelligence (AI) gathering a wider variety of speakers from different

©Shutterstock

sectors. The positions expressed during the discussion gravitated around the main theme of maintaining the human person at the centre of AI development in order to avoid its possible negative ramifications, ranging from monopolies of technological giants and 'surveillance capitalism' to geopolitical ramifications with regards to Big Data and AI based on the values and principles of different regions of the world. Discussions continued on what essentially constitutes the difference between human and machine and the consequences this has for the development of AI.

Furthermore, a Member of the European Commission's High-Level Experts Group on Artificial Intelligence, Thomas Metzinger, Professor of Theoretical Philosophy, Johannes Gutenberg University, gave an exclusive preview of the ethical guidelines that will be published on 10 April, underlining that it will be the most advance ethical guidance document on AI in the world. In his view, the strong industry majority of the High-Level Experts Group on AI, is reflected in the guidelines, as the private sector has an interest in cultivating ethical debates in order to delay, postpone, or deter policymaking or regulation. According to Mr Metzinger, the major goal of the industry is to avoid the enforcement of concrete legislation. He added that for the private sector, ethical guidelines are a declaration for an investment strategy, with the danger that too strong regulation would mean that research funding will go to other parts of the world. One positive proposal for him is to take 12.5% of the investment, namely €20 billion a year for the next 10 years, to create a European Ethics Hub, a research centre for ethics and education network across all European universities in all Member States. In this respect, he noted that Massachusetts Institute of Technology in the U.S. invested $1 billion in this kind of centre for AI.

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

ALGORITHMS

European Parliament Research Centre study on algorithmic decision-making

©Shutterstock

The European Parliament Research Centre (EPRC), the in-house research department and think tank of the European Parliament, released a **study** looking into the challenges and opportunities posed by algorithmic decision-making.

The study is aimed at assisting Members of the European Parliament (MEPs) and parliamentary committees in providing them with independent and objective analysis to feed into the European Parliament's reflection on the transparency and accountability of algorithms. Authors warn that the expected benefits of algorithm decision systems may be offset by the variety of risks for individuals (discrimination, unfair practices, loss of autonomy, etc.), the economy (unfair practices, limited access to markets, etc) and society as a whole (manipulation, threat to democracy, etc). It therefore presents several options to reduce the risks related to algorithm decision systems and sketches some recommendations to benefit from them, while limiting the risks related to their use.

Moreover, the study warns against hasty legislation that could end up creating more problems than solutions but stresses, nevertheless, that oversight agencies should be entitled to sanction operators of non-compliant algorithm decision systems in a similar fashion as data protection authorities for non-compliance with the General Data Protection Regulation (GDPR). Additionally, it recommends that the deployment of these systems be made conditional to prior algorithmic impact assessment and that their certification be made mandatory in certain sectors.

The study puts forward five complementary types of options to overcome challenges posed by algorithm decision systems, including to: develop and disseminate knowledge about algorithm decision systems; launch a public debate about their benefits and risks; adapt legislation to enhance their accountability; develop tools to enhance their accountability; and put in place effective validation and monitoring measures.

The European Commission has also **commissioned** a study to look into the challenges and opportunities of algorithmic decisions, following the proposal of the European Parliament for a **pilot project** on the topic. The study is due to be released by October 2019 and will inform the next Commission's digital agenda in the area of AI and algorithms.

(Source: EPRC)