The Rise of Standardization as a Regulatory Technique in the EU: NISD, CSA, AI Act Proposal, GDPR (21 April 2022)

Summary by Almira Akbay

On 21 April 2022, the Brussels Privacy Hub and dr. Irene Kamara from the Tilburg Institute of Law, Technology and Society (TILT), organized an event titled **"The rise of standardization as a regulatory technique in the EU: NISD, CSA, AI Act Proposal, GDPR".** The event was opened by **Prof. Paul De Hert** and hosted by **Dr. Irene Kamara**.

The event started with introductory remarks by **Prof. Paul de Hert** (professor Vrije Universiteit Brussel), who drew attention to the fact that standards, as a regulatory tool, were not treated with the "academic objectivity" that they deserved. He concluded his opening remarks by thanking **Dr. Irene Kamara** for bringing a multi-disciplinary composed panel.

Dr. Irene Kamara gave a brief introduction on the importance of standardization in different fields such as policy making, legal compliance and technical expertise and explained the meaning of technical standards and their role and limitations, in harmonization and regulatory compliance in the EU law.

The invited speakers were **Prof. Ian Walden** (Professor of Information and Communications Law and Director at the Centre for Commercial Law Studies at Queen Mary University of London), **Slawomir Górniak** (Senior Cybersecurity Expert at the European Union Agency for Cybersecurity (ENISA)), **Dr. Saharnaz Dilmaghani** (Artificial Intelligence and Data Science Consultant at PwC in Luxembourg) and **Dr. Annalisa Volpato** (Assistant professor in EU Administrative Law at Maastricht University in the Netherlands).

Prof. Ian Walden commenced his presentation from the point of cybersecurity as an example of how standards are being used as a regulation tool. The demand and need for cybersecurity has increased in the post pandemic era. He mentioned two regulatory responses to cybersecurity, namely; safeguarding obligations and transparency obligations. **Prof. Walden** elaborated on the Network and Information Security Directive ("NIS Directive")[1] as a response to concerns about critical nature of networks and information systems and the need to ensure the use of information network systems to provide the implementation of appropriate and proportionate security measures. This was the first time that EU law defined the notion of cloud computing and therefore, the obligation become enhanced as a consequence of its increased importance within the functioning of our society and our economies. In addition, **Prof. Walden** argued that more standards have been proposed under the proposal of NIS 2 Directive[2] and these standards would become not only part of the regulatory framework but when covered with certification, become hard regulatory tools; no longer soft regulatory tools. The last point which **Prof. Walden** referred to was regarding the issues of data localization that raises questions about data sovereignty and politicization of standardization.

Slawomir Górniak presented the policy perspective and latest developments as regards standardization and certification in the Cybersecurity Act[3] and other related laws such as eIDAS

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high-risk common level of security of network and information systems across the Union OJ L 194/1.

[2] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final.

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151.

Regulation version 2[4], NIS 2 Directive reform, and the AI Act[5]. **Mr. Górniak** provided ENISA's perspective about cybersecurity standardization and views about how to tackle this important matter with participants. He underlined the importance of standards in many areas such as improving efficiency and effectiveness, being able to compare different products, facilitating systems' integration and interoperability. **Mr. Górniak** emphasized that cybersecurity faces organizational challenges regarding the quantity of standards that are introduced, the companies' lack of interest in using standards when those companies already have a strong position in the market, as well as the lack of agility. ENISA's activities in the field of standardization have three pillars; (i) assessing standards in various areas of cybersecurity, (ii) collaborating with different stakeholders and (iii) providing guidelines to experts from standardization bodies. It has been noted that ENISA currently has been working on AI standards and digital identities standards.

Dr. Saharnaz Dilmaghani reflected on providing standardization for a trustable and ethically responsible AI framework. The AI Act is still under development but it raises a lot of questions for companies who deliver AI based solutions to their clients. She pointed out that the AI Act defines four levels of risk, each of which proposes requirements for users and providers, and that there are questions on how to comply with these requirements. **Dr. Dilmaghani** remarked that harmonized standardization to comply with the AI Act is necessary. She further highlighted that the most important level highlighted by the AI Act is the high-risk level; if there is an unacceptable risk for the AI system, such act is prohibited. It has been identified that a standardization is necessary to determine what kind of applications fall under the level of high-risk application. **Dr. Dilmaghani** concluded her speech by noting that providing more intense standardization activity in AI is crucial.

Dr. Annalisa Volpato talked about legitimacy issues in European standardization. **Dr. Volpato** discussed the evolution of standardization as a regulatory technique from the perspective of EU public law. **Dr. Volpato** stressed the growing important CJEU case law regarding standardization, such as *Fra.bo.* (Case C-171/11) which is the first case in which a national standard was considered by the CJEU as de facto binding; *James Elliott* (C-613/14); *Stichting Rookpreventie* (Case C-160/20) and the General Court case Public.Resource.Org (T-185/19). Furthermore, **Dr. Volpato** elaborated on the input, throughput and output legitimacy of standardisation. Within the legitimacy scholarship, questions are raised regarding the Meroni Doctrine conditions, transparency and legal certainty of the standards, as well as issues such as copyright, and access to standards. **Dr. Volpato** ended her remarks by saying that standardization is a well-established regulatory technique of EU law and it has been considered to have a strong output legitimacy for the efficiency and quality of a document while it remains problematic from a public law perspective because some questions on input legitimacy remain unsolved. It has been concluded that the more technical standardization is used for high profile initiatives, the more these issues will come before CJEU and require enhanced scholar attention.

[4] Proposal for a Regulation of the Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final.

[5] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final.