EJLT European Journal of Law and Technology

BILETA Special Issue: Editorial

Aysem Diker Vanberg and James Griffin

It is with great pleasure that we introduce this special issue of the EJLT further to the 2024 BILETA Conference at Dublin City University. The conference featured numerous outstanding presentations, followed by thought-provoking discussions, and the papers included in this special issue stem from those sessions.

The conference was based around the question of 'Digital and Green: Twin Transitions.' Of course, one of the most contemporary issues has simply been the power consumption of AI models, especially the systems required to compute them. However, there has also been a trend, led by companies such as Nvidia, to also respond to this and show how AI can be used for a green future, e.g. in assisting with weather modelling and production processes.

Phulu, in 'Advancing Symbiosis: The Confluence of Green AI and Labour Rights in Paving the Way for a Sustainable Future' focuses on the intersection of green Artificial Intelligence and labour and suggests that this represents a significant step toward global sustainability. Phulu argues that as AI technology has evolved, many advancements focus on energy efficiency and eco-friendly practices. However, these AI advancements also bring up important concerns about labour rights, such as job loss and changing work conditions. Phulu postulates that companies should collaborate with academic institutions to foster research on green AI; meanwhile, that governments have a responsibility of encouraging such collaborations in research and development of sustainable technologies through provision of incentives. Phulu argues these incentives could involve grants for financial support of particular research, the development of particular products, or tax exemptions. In this way, governments could foster innovation, promote investment into technologies for increased energy efficiency and apply a link between research and practical implementation.

The debate concerning AI and its relationship to copyright has become a topic of considerable international debate, both within IP law and beyond. In the paper 'New Frontiers and The Impact of Artificial Intelligence and the Digital Revolution on the Future of Intellectual Property Laws,' **Naim** focuses on the IP aspect, and argues that it is necessary to distinguish between AI assisted and AI generated works, in order to consider the future direction of AI development vis-à-vis IP law. The article considers the EU's legislative measures, approaches of the US and the UK, and China. Naim

argues that current laws and regulations on copyright law need to be overhauled to reflect the impact of AI systems. She recommends the creation of a task force led by WIPO to offer additional provisions that supplement existing TRIPS standards. She argues that the EU can lead on model laws for AI and IP, alongside the taskforce.

The impact of AI on patent criteria has also garnered attention in both academic and legal circles. In her paper 'Safeguarding a Human-Centric Patent System: The Case of the Inventive Step Test', which won the Professor Diane Rowland Postgraduate prize at the conference, **Kahwaji** addresses the gap in understanding how AI tools affect the inventive step test and disclosure requirements. Kahwaji focuses on the disclosure requirement and the inventive step test, arguing that the patent system needs to be reassessed as AI tools become more common in the inventive process. Kahwaji highlights that if AI-generated insights and tools are not disclosed in patent applications, the standard used to assess the hypothetical Person Skilled in the Art (PSITA) may no longer reflect the actual technological abilities needed for the evaluation, which could make the test less effective. Hence, she calls for more transparency in patent disclosures, ensuring that the use of AI tools and access to them are properly documented and available to the PSITA. Kahwaji concludes that a human-centric patent framework is essential not only for preserving the core principles of patent law but also for creating a system that balances patent protection with the need for clear knowledge sharing.

Tzimas, in 'Legal anthropocentrism at crossroads: International legal principles ahead of transhumanism and post- anthropocentrism' looks at transhumanism and post-anthropocentrism, and how they have entered the forefront of philosophical and legal discourse. He argues that "whether we are talking about the evolution of Artificial Intelligence (AI) itself to higher forms of intelligence and autonomy, or about the synergy of human and artificial intelligence, the self-evident to this day anthropocentrism of our societies and law enters a phase of transformation with the prospect of post- anthropocentrism looming." The paper distinguishes between transhumanism and techno- ontological post- anthropocentrism – and importantly, seeks to identify the legal principles that should guide us in order to preserve legal anthropocentrism. It is proposed that we must be able to distinguish between human enhancement and post- anthropocentrism. The article argues for a distinction between permissible "human enhancement in anthropocentrism" – a form of transhumanism at the initial stages - and practices of transition to post-anthropocentrism, which should be outlawed. Tzimas argues that the basis for such distinction is the prevalence of natural selection with modifications only for the avoidance of diseases, the binary relationship between human and "other- than-human" and the maintenance of the dominion of human, legal personality.

The Online Safety Act 2023, which came into force on October 2023, with key duties coming into force on March 17, 2025, has faced criticism both in the UK and internationally for issues like potential overreach on free speech and concerns about privacy and encryption. In this timely paper, 'Differentiating between harm to users and third parties in the UK's Online Safety Regulations', **Colegate** highlights a critical

blind spot in the Online Safety Act: its failure to adequately address harms to third parties. While the Online Safety Act concentrates on protecting individual viewing users consuming and interacting with harmful content, Colegate argues that the Act overlooks situations where online material incites offline action that harms other (third) parties—economically, physically, or socially. Drawing on recent UK case studies, including viral content on TikTok that led to public disorder and consequential harm to third parties, the paper categorises and evidences these third-party harms. Colegate calls for clearer definitions and the reform of the Online Safety Act and subsidiary codes including the formal recognition of third-party harm and greater scrutiny of algorithmic recommendation systems that can amplify such content.

In *'*Data Protection's Function in Society: A Search for the Limits of a Non-Absolute Right', **Nolan** offers an incisive exploration of the under-examined concept of data protection's "function in society," as articulated in Recital 4 of the GDPR and recurrently referenced by the CJEU. Tracing the evolution of this notion across EU case law, Nolan argues that the CJEU employs it as a rhetorical device to justify limitations on the right to data protection, without giving it substantial independent meaning. The article situates this trend within broader debates around proportionality, judicial balancing, and the challenges of defining the scope and limits of data protection in the EU legal order. Nolan calls for a re-engagement with the limits of data protection, suggesting that greater use of jurisprudence from the ECtHR and Member State constitutional traditions could bring needed coherence and constraint to the CJEU's interpretation of the right. In doing so, Nolan contributes to ongoing scholarly debate about the expansive reach of EU data protection law and its implications for both regulatory clarity and fundamental rights jurisprudence.

Finally, **Vellinga and Mulder** in 'Under Attack: The Discrepancy between Cybersecurity Regulation and Vehicle Regulation' argue that potential cyberattacks are increasing as products are increasingly more connected, for instance with regard to the Internet of Things. They note that this issue has been acknowledged by the European Commission. The proposed Cyber Resilience Act sets minimum cybersecurity requirements for products with digital elements. The Act, for example, requires regular tests, and the dissemination of free security updates in case of a cybersecurity breach. However, as they note, some products, such as vehicles, are not subject to the Act. The authors argue that this seems counter intuitive, as vehicles are becoming ever more connected to the push towards full automation. This has meant that attacks such as disengaging brakes, taking over the steering and killing the engine of a car while driving have proven to be possible. Nevertheless, the regulation of cybersecurity in vehicles is left to the forum regulating traditional vehicle safety – not exactly adequate. They argue that the legislator should remain vigilant to avoid vulnerabilities that could ultimately compromise the right to life - and also the right to privacy.