EJLT European Journal of Law and Technology

Persisting penumbra in EU digital law: from the GDPR to the AI Act

Editorial

Edoardo Celeste and Abhilash Nair

Those who work in the field of digital law certainly appreciate what we could call the 'archaeological' nature of our discipline. Digital technology has disrupted many aspects of our society, generating multiple issues that the law often struggles to address. The legal scholar must thus retrace the rationale of legal rules, their origin – their ἀρχή (*archè*) – in order to reinterpret them in light of the challenges of the digital revolution. Legal sociologist Gunther Teubner speaks of a process of 'generalisation' and 're-specification'.[1] An interpretative task that is far from linear, often leading to conflicting views on the same issue. Yet, a necessary undertaking if we want to guarantee internal coherence between the existing legal framework and the developing digital law.

The digital law archaeologist studies the 'old' and the 'new', the 'material' and the 'immaterial', the 'visible' and the 'invisible'. When it comes to assessing the adoption of new pieces of legislation or judicial decisions in the field of digital law, such a critical, historical, lens is decisive. We cannot judge our present and discuss the options related to our future if we do not have a clear idea of where we come from and how we decided to regulate our society so far. The digital law archaeologist is thus often called to shed light on legal 'penumbra' - areas of law that are not fully illuminated by existing normative solutions, but that are nevertheless not completely immersed in darkness. Our task is to decipher the quintessence of technological changes, retrace applicable legal principles, interpret them critically, and propose innovations.

[1] See Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press 2012); see also Edoardo Celeste, 'Internet Bills of Rights: Generalisation and Re-Specification Towards a Digital Constitution' [2023] Indiana Journal of Global Legal Studies.

The last EJLT issue of 2024 contributes to this task. We present five research articles that explore legal penumbra of EU digital law. These papers critically assess the use of concepts that are shaping the development of digital technology, examine the limitations of existing digital rights when it comes to new data processing trends, clarify the boundaries between existing digital law frameworks regulating overlapping social activities, explore new solutions to longstanding societal issues that are exacerbated by the use of digital technology, reconstruct normative puzzles regulating developing technologies. In this way, these authors bridge the past and the present, constantly looking at the future. They aim to ensure coherence in the EU legal context, which is increasingly stratified in the area of digital law. They seek to make sense of the exponential 'act-ification' of the EU digital field,[2] especially when legal penumbra seems to be persisting, creeping from older analogue or digital pieces of legislation, whose profound rationale may have faded over time.

The first article, titled **'Risk, Harm and Damage as Preset Rational Categories in AI Literature: Do We See or Think the Problem?',** by Cristina Cocito, Thomas Marquenie and Paul De Hert, reflects on the adequacy of established concepts of EU law to capture the issues that AI is generating. The article focuses on the triad 'risk, harm and damage', three value-laden notions in legal studies that play a significant role in the context of the GDPR as well in the recently approved AI Act. They are considered as conceptual 'paradigms' or 'lenses' through which the negative implications of AI systems are framed. Drawing on Dewey and Bergson, the authors adopt a pragmatist methodology of problem inquiry, arguing that the concepts of risk, harm and damage risk to miss the 'problem' generated by AI systems. In particular, these notions would fail to capture other elements, such as feelings and concerns, which might be generated by the use of AI.

In **'The Right to Rectification and Inferred Personal Data',** Andreas Häuselmann and Bart Custers explore so-called 'inferred data', pieces of information that are derived from other elements in possession to the data controller. In particular, the paper looks at predictions and emotional status, analysing the limitations of the right to rectification as enshrined in the GDPR in relation to these two categories of data. Data subjects struggle to exercise their right to rectification as they might not be aware that the controller is in possession of this information and that the latter is not accurate. Moreover, the accuracy of inferred data is hardly verifiable, thus making the main burden of proof for the data subject who seeks to exercise their right to rectification challenging to meet.

In **'Between GDPR and Law Enforcement Directive in Security Research: The Use of Personal Data by Law Enforcement Authorities'**, Stergios Aidinlis, David Barnard-Wills, Leanne Cochrane, Krzysztof Garstka, Agata Gurzawska and Joshua Hughes charter the boundaries between the GDPR and the Law Enforcement Directive in a specific and unexplored setting, that of research carried out by enforcement

[2] See Vagelis Papakonstantinou and Paul De Hert, 'The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of "Act-Ification", "GDPR Mimesis" and "EU Law Brutality"' [2022] Technology and Regulation 48.

authorities. Over the past few decades, the fight against organised crime and human trafficking have greatly benefitted from the use of digital technologies. These advancements were possible thanks to significant investments in the field of security research. Law enforcement authorities process daily significant amount of personal data, whose protection is guaranteed by the Law Enforcement Directive. However, when they start using data to carry out research, the GDPR discipline applies. The paper illustrates that this demarcation, despite being apparently straightforward in theory, it is not crystal clear when it comes to reality, with the risk of making law enforcement authorities either disapply the GDPR or desist from engaging in research.

The article '**When Organised Crime Turns to Cryptocurrency: the Compatibility of Italian Patrimonial Preventive Measures with Cryptocurrency**' by Gaia Cavagnoli Micali examines the challenges that cryptocurrencies are generating in the context of the fight against organized crime. One of the main innovations of Italian law in contrasting the Mafia in the 1980's was the introduction of measures offering the possibility to freeze assets preventively, in case of concrete social danger. These instruments represented a paradigm change as they affected directly the financial assets of organized criminal organizations. After more than forty years, the effectivity of a similar remedy seems to fade when facing the immateriality and decentralised nature of new forms of investments, such as cryptocurrencies. The paper analyses the main points of incompatibility between this new technology and the Italian system, illustrating a series of potential solutions that might benefit in the future a broader European approach in the contrast of organized crime.

Our final article of this issue, **'The Renewed EU Legal Framework for Medical AI'**, by Sofia Palmieri examines the EU legislative framework applicable to medical AI. By this expression the author does not intend to focus exclusively on the use of AI systems in the clinical context, but to encompass more broadly the application of AI in the healthcare sector, for example also including healthcare management solutions. Palmieri points out that, as technologies evolve, the legal framework applicable to medical AI has become increasingly complex and stratified. If, indeed, the Medical Device Regulation still represents the cornerstone of this system, a series of other EU legal instruments now apply to this field. The paper then maps this intricate scenario particularly focusing on the contribution given by the AI Act, exploring how its requirements interact with the Medical Device Regulation and the other applicable legal instruments.

As 2024 is now coming to end, we would like to thank everyone who is involved in running the EJLT. Starting from our editorial board, our invaluable peer reviewers, our copyeditor Vicki Hillyard, all our contributors and readers: sincere thanks for dedicating your time to EJLT and supporting its mission. We wish you a peaceful (and restful) end of the year and we look forward to engaging with you in 2025!

Edoardo Celeste
Abhilash Nair