Articles

Future-proof Regulation and Enforcement for the Digitalised Age

edited by Gavin Robinson, Sybe de Vries *and* Bram Duivenvoorde

Introduction: Future-proof Regulation and Enforcement for the Digitalised Age

This *Special Section* in *European Papers* is devoted to assessing whether core areas and core values of European law are future-proof (and how they could or should be made future-proof) in light of developments in terms of digitalisation and technological innovation.

Digital technologies create various challenges, in many cases associated with the use of algorithms, the massive collection of personal data and the possibilities (and difficulties) of access to digital content. All these challenges require careful consideration, and regulation and enforcement arrangements which protect and balance the possibly conflicting values that we deem important in our societies, including innovation and technological development and protection of fundamental rights. Yet, it is exactly the continuous and fast-paced technological developments that make it difficult to regulate in these areas. In the European Union, this response is predominantly shaped and guided within the multi-level legal order, whereby the EU legislature has gained a growing role in shaping the regulatory response to technological developments and in shaping our digital societies: through policy, through soft-law instruments, through regulations, directives, and other legal instruments. Add the crucial contributions of the EU judiciary to the interpretation and development of regulation and enforcement through the growing body of CJEU jurisprudence, and the great extent to which the European Union is shaping our digital futures becomes clear.

This *Special Section* is the result of a joint project of researchers at the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE) at Utrecht University.[1] The project brought together researchers with expertise in different fields of EU law, who are all focusing on the impact of digitalisation on their respective fields of law. The different fields of expertise include EU internal market law, consumer protection law, data protection law, competition law, financial law, intellectual property law and criminal law. This *Special Section* follows

[1] More specifically, the project took place within the 'Digitalisation & Technological Innovation in Europe' Building Block, essentially a sub-group within RENFORCE focusing on the impact of digitalisation and technology on EU law.

European Papers
Vol. 8, 2023, No 2, pp. 579-582
www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/676

a joint workshop organised in Utrecht on 4 November 2022, in which each of the authors – after an inspiring keynote by Sofia Ranchordas (Tilburg University and LUISS, Rome) on future-proofing EU regulation – presented and discussed their preliminary findings.

What stands out in the seven contributions in this *Special Section* is that despite the impressive legislative output at EU level, more – or rather, different or "out of the box" thinking – is needed to tackle the digital challenges now and in the future.

The first contribution in this *Special Section* is written by Sybe De Vries, Olia Kanevskaia and Rik De Jager, who discuss the future-proofness of the proposed AI Act from three perspectives: *i)* the internal market; *ii)* protection of fundamental rights and *iii)* democratic legitimacy in the EU decision-making processes. Ultimately, their contribution offers a broader reflection on the policy and legal implications of AI and proposes a number of recommendations on how to increase the fitness of the future AI Act, bearing in mind the balance between the economic and fundamental rights goals of the AI Regulation.

Secondly, Alessia D'Amico offers an *Article* rooted in a matter of perennial importance for legal research and for citizens more broadly: consent in data protection law, and more specifically the credibility of the notion of both "informed" and freely-given consent in today's Big Tech-dominated world. The piece focuses on the recent proceedings in Case C-252/21 *Meta vs Bundeskartellamt* before the CJEU, including the novel proposal from the Advocate General to include dominance as a factor in the assessment of customers' freedom of consent to data processing. Competition law thus meets data protection law on both the theoretical and practical levels, with the author sharing a critical and constructive discussion of how such an interplay between competition authorities and data protection authorities may contribute to better protection of individuals' rights over their data into the future.

The third contribution is from Bram Duivenvoorde, who discusses whether EU consumer law is future-proof in terms of protecting consumers against harmful personalised advertising. After explaining that personalised marketing can exploit consumer vulnerabilities, he shows that the current EU legal framework is unfit to effectively protect consumers against these harms. Duivenvoorde argues that recent EU laws and proposals address this problem only to a limited extent. He therefore draws the conclusion that EU marketing law should be redesigned in order to better protect consumers, both in terms of regulation and enforcement.

The next contribution is written by Catalina Goanta, with the title "Digital Detectives: A Research Agenda for Consumer Forensics". Goanta argues that effective enforcement on digital markets is one of the key challenges of contemporary consumer law and policy, and that public authorities need to arm themselves with the means necessary to detect digital violations. In her *Article*, Goanta proposes a new field of research focused on the investigation and enforcement of consumer violations on digital markets in the form of "consumer forensics", and argues that consumer forensics is the way forward in making consumer enforcement future-proof. She offers insights on how this could be achieved,

focusing on the potential of consumer forensics in response to consumer protection violations in the context of influencer marketing.

Goanta's *Article* is followed by the contribution of Nikita Divissenko, which analyses the EU's recent Markets in Crypto-Assets (MiCA) Regulation, sitting within the Digital Finance Package (DFP), from the perspective of financial innovation. The legislative desire to foster said digital financial innovation whilst ensuring adequate protection of European consumers is the key balancing act explored in the *Article*. Divissenko highlights two main points of vulnerability that tend to undermine future-proofness in this field – the scope of the new MiCA Regulation and its capacity to incorporate future innovation, and the responsiveness of the regulatory and supervisory framework to as-yet-unknown risks – before discussing potential solutions in the shape of (greater use of) regulatory sandboxes and technological regulation.

Next is the *Article* by Vicky Breemen, who discusses the difficult position of libraries in the digital society under EU copyright law. She explains that despite modernisation efforts in the past decades, the "library privilege" (i.e. the provisions regulating library functions) still persistently focuses on physicality. Breemen finds that the most recent addition to the EU copyright acquis, the Digital Single Market Directive (2019), does offer some openings in this regard. Looking at the future, Breemen argues that copyright law should move away from the library privilege's focus on physicality, facilitating remote access at least to some extent.

Lastly, Gavin Robinson discusses the collection and preservation by private companies, for the public purposes of preventing, investigating and prosecuting criminal offences, of EU citizens' communications metadata (for instance, records of mobile telephone calls or emails) – a practice more widely known as "data retention". Nearly ten years on from the CJEU's seminal decision in Case C-293/12 *Digital Rights Ireland,* the *Article* tackles the prospect that will not go away – that of a fresh EU-level data retention law – both in terms of its compatibility with the body of CJEU case law today and its viability into the future, also in light of technological evolution in the very kinds of data it may be technologically possible for private actors to retain. The *Article* looks at the first attempts at the national level to square the circle presented by the CJEU as its favoured middle ground – "targeted" data retention – and discusses the need for the effectiveness of any such scheme to be credibly demonstrated over time.

A key challenge for any collective effort seeking to tackle disparate fields within the realm of EU law, alongside ensuring a common focus on its animating theme (the future-proofness of EU law today) together with a shared constructive approach (how EU law can be more future-proof tomorrow), is that of ensuring the *Articles* all tackle recent or ongoing legal developments – or in other words, that they are all up-to-date. We are therefore most grateful to everyone at *European Papers* and to our colleagues at Utrecht for their commitment to ensuring the topicality as well as the quality of all parts making up this whole. We hope that the contributions provide food for thought, useful insights

and inspiration for the process of making regulation and enforcement in the EU (more) future-proof for digitalisation – both within the specific fields of expertise and beyond.

Gavin Robinson[*], Bram Duivenvoorde[**] and Sybe de Vries[***]

[*] Assistant professor, Utrecht University, g.l.robinson@uu.nl.
[**] Associate professor, Utrecht University, b.b.duivenvoorde@uu.nl.
[***] Professor of Public Economic Law, Utrecht University, s.a.devries@uu.nl.