Journal of Law, Market & Innovation

ISSUE 3/2024

Journal of Law, Market & Innovation

3/2024

Editors: ***Riccardo de Caria – Cristina Poncibò - Piotr Tereszkiewicz***

Journal of Law, Market & Innovation
Vol. 3 - Issue 3 - 2024
ISSN 2785-7867
Journal of Law, Market & Innovation

The Journal of Law, Market & Innovation is indexed in DOAJ, Scopus and ERIH+.
It is also classified as a "scientific" journal of Law (Area 12) by the Italian National Agency for the Evaluation of Universities and Research Institutes (ANVUR).

TABLE OF CONTENTS

Riccardo de Caria - Lorenza Mola - Cristina Poncibò

ACKNOWLEDGEMENT

The Editors-in-Chief, on behalf of the whole JLMI community, would like to deeply congratulate Professor Mateja Durovic, member of our Advisory Board, on being elected Judge of the European Court of Human Rights.

We are delighted to know that the Court will benefit from the unparalleled expertise of such an exceptional jurist.

Warmest wishes

R.d.C., L.M., C.P.

Riccardo de Caria - Cristina Poncibò - Piotr Tereszkiewicz

FOREWORD TO ISSUE 3/2024

The present issue of the Journal of Law, Market & Innovation covers, from a comparative perspective, different topics exploring the legal regime of contracts of adhesion in the platform economy.

From a European Union law perspective, the recent 30th anniversary of the Council Directive 93/13/EEC on unfair terms in consumer contracts (UCTD) justifies an inquiry into whether statutory regulations on unfair contract terms, such as the UCTD are suitable as a regulatory framework applicable to transactions in the digital environment shaped by platform operators. As is commonly known, the UCTD has given rise to a substantial jurisprudence of the Court of Justice of the European Union (CJUE). The Court laid down interpretations and guidance, among other issues, on the concept of 'consumer', the requirements of 'transparency' and 'fairness' of standard contract terms and the legal consequences of breaching these requirements.

While the UCTD applies to business-to-consumer contracts, the much more recent EU Platform to Business Regulation 2019/1150 addresses issues of fairness in contracts of adhesion between digital platform operators and business users. It significantly extends the EU regulatory framework regarding contractual fairness, explicitly focusing on the platform economy.

Beyond contract law, one must emphasise the development of the EU Digital Acquis, i.e., the Digital Services Act, the Digital Markets Act, the AI Act, and the EU legal framework on data and personal data protection, i.e. the Data Act and the General Data Protection Regulation (GDPR). These overlapping legal regimes may create inconsistencies and gaps in achieving the goal of protecting digital platform users. They may also result in uncertainty for digital platforms, making it challenging for platform operators to navigate and comply with the regulatory landscape effectively. Further regulatory layers include sector-specific regulation of goods and services (e.g., financial services) and competition law.

The articles in this issue of the Journal of Law, Market & Innovation paint a rich and nuanced picture of the legal regime applicable to contracting in the digital environment in the EU and beyond.

R.d.C., C.P., P.T.

Pietro Ghirlanda *

INNOVATION LETTER

HOW PLATFORM COOPERATIVES CAN REDRESS ABUSES OF AUTHORITY WITHIN DIGITAL MARKETS

Abstract

After their advent, digital platforms were hailed as innovative institutional solutions capable of reducing transaction costs for a wide group of stakeholders by removing traditional intermediaries and facilitating the match of demand and supply through digital means. However, a group of big investor-owned platforms from Silicon Valley soon imposed themselves as monopolistic actors within digital markets, leveraging their strong bargaining position to abuse their authority and extract undue rents. Different legal strategies have been assessed in the last few years to limit this unilateral rule-setting power, particularly at the EU level. Nevertheless, little consideration has been given to alternative forms of platform organising, aimed at including the relevant stakeholders in the governance of platforms to redress power abuses. This article presents the case of platform cooperatives, which are platforms owned and governed by their workers and users. Moreover, the article considers the institutional complementarities that could help platform co-ops overcome challenges and compete with capitalist platforms on fair legal and political bases.

JEL CLASSIFICATION: D23, D26, J54, L22, L38, O35, P13

SUMMARY

1 Abuses of Authority within Digital Markets

In the last two decades, the platform business model has profoundly transformed modern societies and assumed an increasing centrality in the academic debate. According to the OECD, the term 'online platform' describes 'a range of services available on the Internet including marketplaces, search engines, social media, creative content outlets, app stores, communication services, payment systems, services comprising the so-called "collaborative" or "gig" economy, and much more.'[1] Despite obvious differences, what

* Department of Political and Social Sciences, University of Pavia.

[1] OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (OECD Publishing 2019) 20.

DOI 1.13135/2785-7867/11340

associates all these platforms is that they facilitate on-demand exchanges of goods and services (including labour) through digital means. In this way, digital platforms were originally supposed to reduce transaction costs for all their stakeholders and more democratically distribute value amongst them. The promise was that algorithmic management systems would have helped to build reciprocal trust between users without making it necessary to resort to vertically integrated hierarchies to organise transactions.

However, soon, this ideal left space for reality and a group of big investor-owned platforms from Silicon Valley ended up monopolising digital markets; Uber is an emblematic example. Investor-owned platforms, thanks to network effects, have in fact become infrastructural actors in our daily lives providing increasingly essential services and often representing the only viable options in the labour market for vulnerable people who lack other alternatives. At the same time, these platforms have the unilateral power of setting and updating the rules of the game through their terms and conditions. Consequently, many scholars argue that they can't be intended anymore just as the neutral multi-sided market-matching systems they claim to be. They are instead gatekeepers of digital markets who embrace, evolve and extend some of the control features typical of traditional corporations. Namely, they exploit their algorithms and their unequal bargaining position to dictate the behaviour, take unfair advantages and extract rents from non-financial stakeholders who depend on them at different levels but are not formally integrated into the firm.[2] That is particularly evident in labour-based gig platforms—both 'geographically tethered' and 'cloudwork' centred—which externalise tasks to precarious independent contractors not guaranteed with standard employment protections.[3]

From the perspective of New Institutional Economics (NIE), we could say that digital platforms exacerbate one of the defining features of traditional capitalism: the unilateral allocation of residual control rights.[4] Due to contract incompleteness, residual control rights give their holders, who are usually the ones who own the physical assets of the firm, the right to make decisions about whatever is *ex-ante* left outside of contracts when unforeseeable contingencies happen. However, such an allocation, originally thought to protect the actor supposed to undertake the costliest investment from the hold-up risk, overlooks other important investments: especially in human capital. Therefore, it can create the conditions for an 'abuse of authority': the residual owner may unilaterally renegotiate contracts *ex-post* and expropriate in turn other stakeholders from their

[2] Martin Kenney and John Zysman, 'The Rise of the Platform Economy' (2016) 32(3) Issues in Science and Technology; K Sabeel Rahman and Kathleen Thelen, 'The Rise of the Platform Business Model and the Transformation of Twenty-First Century Capitalism' (2019) 47(2) Politics & Society 177; Mariana Mazzucato, Josh Ryan-Collins and Giorgos Gouzoulis, 'Theorising and Mapping Modern Economic Rents' (2020) 13 UCL Institute for Innovation and Public Purpose Working Paper; David Stark and Ivana Pais, 'Algorithmic Management in the Platform Economy' (2020) 14(3) Sociologica 47; Koen Frenken and Lea Fuenfschilling, 'The Rise of Online Platforms and the Triumph of the Corporation' (2020) 14(3) Sociologica 101.

[3] Jamie Woodcock and Mark Graham, *The Gig Economy: A Critical Introduction* (Polity Press 2020).

[4] Oliver Hart, 'Incomplete Contracts and Control' (2017) 107(7) American Economic Review 1731.

specific investments.[5] Moreover, it can also reduce firm efficiency in the long run since, fearing the risk of expropriation, the latter will likely start to underinvest. This dynamic is even worse for platform stakeholders—not only workers but also customers and service providers.

Indeed, as I have anticipated, the organisational model of platform capitalism is founded almost entirely on the externalisation of the entrepreneurial risk.[6] The only real asset platforms own are their algorithms and no protections are granted to other actors who are not integrated into digital companies that just claim for themselves the role of market-matching systems. As a consequence, platform stakeholders do not have any bargaining power in negotiating the rules to which they are subjected and can only accept terms and conditions on a take-it-or-leave-it basis, knowing that these rules can even be unilaterally renegotiated from one moment to the next. Therefore, some scholars are currently referring to this business model as 'neoliberalism on steroids'[7] and advocating for the necessity of alternative institutional solutions to tackle the increasing precarity of working conditions, the unilateral extraction of users' value (including data), the extensive adoption of unaccountable surveillance practices through algorithmic management systems, the platforms' anti-competitive behaviours and their role of gatekeepers concerning essential infrastructures of our daily lives.

So far, the main strategy considered, at least at the EU level, for protecting stakeholders' rights while preserving the possibility for healthy innovation is to regulate the sector from the top to level the playing field and force all platforms to guarantee minimum protections in order to create a fair terrain for competition. At the same time, it is contested the extent to which legal instruments such as the Council Directive 93/13/EEC on unfair terms in consumer contracts (UCTD), the EU Platform to Business Regulation 2019/1150 (the P2B Regulation), the Digital Markets Act (EU Regulation 2022/1925), the Digital Services Act (EU Regulation 2022/2065) or the new Platform Work Directive can capture all the specificities of the platform economy and solve the problems posed on the demand and supply sides by the unilateral adoption of contracts of adhesion in this sector. In the same way, it is under debate to what extent national governments are bound to implement and enforce EU rules. Accordingly, this article presents the idea that fixing minimum standards for protecting stakeholders' interests within digital markets could be just a part of the answer. A complementary strategy that would deserve attention is to actively sustain more democratic and equitable bottom-up initiatives that can thrive in an enabling and more certain legal context. In particular, the article focuses

[5] Lorenzo Sacconi, 'Codes of Ethics as Contractarian Constraints on the Abuse of Authority Within Hierarchies: A Perspective from the Theory of the Firm' (1999) 21 Journal of Business Ethics 189.
[6] Nick Srnicek, *Platform Capitalism* (Polity Press 2017).
[7] David Murillo, Heloise Buckland and Esther Val, 'When the Sharing Economy Becomes Neoliberalism on Steroids: Unravelling the Controversies' (2017) 125 Technological Forecasting and Social Change 66.

on one of the most promising alternatives recently proposed: the organisational model known as platform cooperativism.

2 The Platform Cooperativism Alternative

The concept of platform cooperativism was coined by the New School professor and digital activist Trebor Scholz in 2014 through its first influential article on the topic: *Platform Cooperativism vs. the Sharing Economy*.[8] Subsequently, Scholz founded the Platform Cooperativism Consortium (PCC): 'an organisation dedicated to fostering the growth of platform co-ops and related projects' that actively supports cooperative developers in the most disparate contexts and sectors through advocacy activities, community building, education and co-design.[9] Moreover, in 2019, he also founded the Institute for the Cooperative Digital Economy, the research arm of the PCC at the New School. Each year this institute launches a non-residential fellowship programme to convene young scholars from all over the world to conduct frontier research on platform co-ops. Amongst the most interesting projects that have emerged until today, we can recall: CoopCycle, a French-born federation of food-delivery cooperatives that share the software infrastructure and is rapidly expanding in different countries across the globe to compete with Deliveroo, Glovo and similar other companies; Fairbnb, an ethical alternative to Airbnb born in Italy and aiming to redistribute value to local communities; and the Drivers Cooperative, a New York City-based driver-owned cooperative challenging Uber and Lyft.

By definition, a 'platform cooperative' is a 'project or business that *primarily* uses a website, mobile app, or protocol to sell goods (e.g., data) or services, and relies on democratic decision-making and shared community ownership of the platform by workers and users.'[10] Hence, Scholz's idea can be summarised as follows: involving platform stakeholders in the governance and ownership structures of digital companies to solve the issues mentioned in the previous section. Similarly, the other founding father of the movement, the American academic and activist Nathan Schneider, stresses how, 'under the banner of "platform cooperativism," an emerging network of cooperative developers, entrepreneurs, labour organisers and scholars is developing an economic ecosystem that seeks to align the ownership and governance of enterprises with the people whose lives are most affected by them.'[11] In this sense, at least four possible membership types have

[8] Trebor Scholz, 'Platform Cooperativism vs. the Sharing Economy' (*Medium*, 5 December 2014) <https://medium.com/@trebors/platform-cooperativism-vs-the-sharing-economy-2ea737f1b5ad> accessed 10 September 2024.
[9] Trebor Scholz, *Own This: How Platform Cooperatives Help Workers Build a Democratic Internet* (Verso 2023) 18.
[10] ibid 8.
[11] Nathan Schneider, 'An Internet of Ownership: Democratic Design for the Online Economy' (2018) 66/2 The Sociological Review Monographs 320. For the different stakeholders that can be involved in an ideal-typical platform cooperative and the role they can respectively play in an extended governance structure, see Pietro Ghirlanda and Vassil Kirov, 'An

been recognised: multi-stakeholder/community platforms, producer-led platforms, consortia/worker platforms and data consortia platforms.[12] Focusing on the centrality of digital workers for all these membership types, Scholz has also proposed ten further defining principles of platform cooperativism: (collective) ownership, decent pay and income security, transparency and data portability, appreciation and acknowledgement for workers, co-determined work, (the need for) a protective legal framework, portable worker protections and benefits, protection against arbitrary behaviour, rejection of excessive workplace surveillance and the right to log off from platforms.[13]

We have already seen how the organisational model of capitalist platforms has quickly proved to be extremely asymmetric and prone to power abuses, despite the original promises of transaction cost reduction and economic democratisation. The entrepreneurial network characterising investor-owned platforms is in fact composed of a central hub represented by platform owners and venture capitalists who keep residual control rights for themselves and can extract monopolistic rents from other stakeholders. On the contrary, the organisational model of platform cooperatives is more horizontal and decentralised, with the different stakeholders that are democratically involved in the value creation process, appropriately rewarded for their specific investments and that, in this way, contribute to increasing the relational capital of the firm.[14] As a consequence, platform co-ops can boost efficiency in the long run because of stakeholders' lower incentive to underinvest and because of the superadditivity of joint human capital investments characterising the digital environment. Therefore, platform cooperatives seem to re-actualise the project of a polycentric digital economy based on 'commons-based peer-production' that the Internet's theorist Yochai Benkler had described as a third mode of production and distribution of value alternative to markets and hierarchies.[15] A model that was betrayed by the monopolisation of digital markets by the hands of capitalist platforms, but which is now gaining a renewed attention to preserve Internet's public nature.

Of course, while platform co-ops have considerable potential, we cannot expect them to be equally successful in all sectors. With an often-dispersed pool of stakeholders who may be connected only by digital means, they risk exacerbating the governance challenges that economists traditionally oppose to cooperatives: the high cost of making decisions and the free-riding problem. Moreover, other challenges related to digital markets are financial, technological and growth challenges. Namely, co-ops lack access to the

Alternative Organizational Model for a More Democratic and Equitable Digital Economy: A Systematic Literature Review on Platform Cooperativism through the Lens of Stakeholder Theory. Competitive Advantages and Challenges' (2024) 95 Annals of Public and Cooperative Economics 1197.

[12] Simon Borkin, 'Platform Co-operatives — Solving the Capital Conundrum' (2019) Nesta and Co-operatives UK Report, February.

[13] Trebor Scholz, *Uberworked and Underpaid: How Workers are Disrupting the Digital Economy* (Polity Press 2017) 180, 184.

[14] Ghirlanda and Kirov (n 11).

[15] Yochai Benkler, 'Coase's Penguin, or, Linux and The Nature of the Firm' (2002) 112(3) The Yale Law Journal 369.

financing channels of venture-capital-backed platforms yet still require huge early-stage investments to build the technological infrastructure and develop the network of users. Consequently, they must find alternative scaling strategies to the traditional 'growth-before-profits' business models of their competitors.[16] Therefore, in the case of global marketplaces, search engines or social media platforms, other institutional arrangements, such as a stronger regulatory role for public institutions, may be more effective in constraining monopolistic tendencies. In contrast, the cooperative solution seems more viable for labour-based platforms, which are those where platform capitalism produces some of its most negative outcomes, because of the more homogenous stakeholders' interests that can reduce governance costs.[17] That is especially true for geographically tethered platforms like ride-hailing or food-delivery, since most of the services, even if managed online, are provided in the real world by people who can more easily meet and organise. At the local level, platform cooperatives may indeed prove greater efficiency, because of the deeper social embeddedness and the even lower costs of making decisions, and higher productivity, due to the lower peer-monitoring effort that is required locally—where there is also less need to build a highly sophisticated platform.[18] At the same time, an alternative scaling strategy to the development of big monopolistic giants is represented by the option of pooling the technological investment and sharing the same infrastructure within a network of federated but autonomous local cooperatives to reduce the entry barrier represented by the cost of the platform, similar to the model of CoopCycle.[19]

3 Institutional Complementarities for Supporting Platform Co-Ops

Building on the previous section, the reduced risk of abusive behaviours, which is a defining feature of platform cooperatives, can be thus read as one of their main competitive advantages (distributed between all the relevant platform stakeholders and not appropriated by a small oligopoly). Nevertheless, we have seen that platform co-ops experience several difficulties in becoming a credible alternative to capitalist platforms. Moreover, by externalising entrepreneurial costs on precarious and low-paid workers, capitalist platforms can further outcompete platform co-ops through price dumping strategies.[20]

[16] Borkin (n 12); Ghirlanda and Kirov (n 11).
[17] Henry Hansmann, *The Ownership of Enterprise* (Belknap Press 1996).
[18] Richard Spear, 'The Co-Operative Advantage' (2000) 71(4) Annals of Public and Cooperative Economics 507; Koen Frenken, 'Political Economies and Environmental Futures for the Sharing Economy' (2017) 375(2095) Philosophical Transactions of the Royal Society A 20160367; Damion J. Bunders and others, 'The Feasibility of Platform Cooperatives in the Gig Economy' (2022) 10(1) Journal of Co-operative Organization and Management 100167; James Muldoon, *Platform Socialism* (Pluto Press 2022); Ghirlanda and Kirov (n 11).
[19] Morshed Mannan and Nathan Schneider, 'Exit to Community: Strategies for Multi-Stakeholder Ownership in the Platform Economy' 5(1) Georgetown Law Technology Review 1; Scholz (n 9); Ghirlanda and Kirov (n 11).
[20] Scholz (n 9).

For these reasons, beyond identifying the sectors where the cooperative solution is feasible, the success of platform cooperatives also depends on the socio-political compromises that modern societies can decide to adopt for pushing digital companies to produce and distribute public value instead of appropriating undue rents. Such socio-political compromises are usually referred to as 'institutional complementarities,' a concept that stresses how institutions belonging to different domains can reinforce each other to stabilise a socio-political system.[21] In this sense, different varieties of capitalism can be analysed through the interdependences between certain corporate governance models and certain other political and regulatory choices. For example, the path characterised by the financialisation of the economy and by the increasing precarity of labour markets that culminated in the current platform capitalism has been facilitated by the conducive legal environment and business sector of the U.S.[22] That is the core of what Anu Bradford defines the American market-driven regulatory model: the 'U.S. digital empire.' On the contrary, the 'European digital empire' is characterised by a rights-driven model that prioritises the protection of the fundamental rights of EU citizens over radical innovation.[23] Accordingly, a more human-centric governmental approach may serve as an institutional complement to the platform cooperative movement.

I have already mentioned the regulatory role that supranational and national governments can play in levelling the playing field to create a fair terrain for platform competition, pushing capitalist platforms to internalise the costs that they often externalise on other stakeholders and that grant them unfair advantages over platform cooperatives. In this sense, the UCTD, DSA, DMA, P2B Regulation and Platform Work Directive do not directly mandate co-ownership of platforms. Still, despite the problems of implementation they face in regulating businesses that structurally exploit legal grey zones, they seek to reallocate entitlements within the EU digital economy. This reallocation can favour more equitable and democratic governance models that naturally align with these rules. For example, the UCTD (together with the GDPR) can be implemented to protect consumers from the unfair terms and conditions unilaterally set by platforms, often leading to data extraction, while platform co-ops already leave users in control of their data. Similarly, the P2B Regulation shields small businesses and traders on online platforms from the latter's exploitation of information asymmetries, promoting a transparent and predictable digital environment that extends to individual entrepreneurs. The aim of the Platform Work Directive is instead to capture the case of fake independent contractors and limit the use of algorithmic management systems in the workplace, introducing a presumption of employment to force platforms to guarantee

[21] Masahiko Aoki, *Toward a Comparative Institutional Analysis* (The MIT Press 2001); Ugo Pagano and Massimiliano Vatiero, 'Costly Institutions as Substitutes: Novelty and Limits of the Coasian Approach' (2015) 11(2) Journal of Institutional Economics 265; Bruno Amable, 'Institutional Complementarities in the Dynamic Comparative Analysis of Capitalism' (2016) 12(1) Journal of Institutional Economics 79.
[22] Rahman and Thelen (n 2).
[23] Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).

their workers with standard protections when material facts indicate control and direction. This would increase the costs for capitalist platforms and foster the competitiveness of worker-owned alternatives. Finally, the DSA and the DMA, preventing illegal activities on large online platforms and regulating their role as gatekeepers, can benefit platform co-ops not only as competitors but, more importantly, as business users of these services.

At the same time, there are more direct strategies that public institutions may decide to undertake. As a direction for future research, I thus want to conclude this innovation letter by mentioning a policy paper jointly produced by the Platform Cooperativism Consortium and the Berggruen Institute about *Policies for Cooperative Ownership in the Digital Economy*.[24] In this paper, the authors discuss several strategies that local and regional governments may adopt for actively supporting platform co-ops and other ethical forms of platform organising by taking inspiration from prominent case studies. For example, they extensively refer to the work on the digital urban commons done in Barcelona by Francesca Bria, former Chief Technology and Digital Innovation Officer of the city under Ada Colau's administration. Among these strategies, it is worth recalling: the development of sustainable public procurement initiatives friendly to platform co-ops, the implementation of loan/funding programs targeted for solidarity-oriented platforms, the public participation in multi-stakeholder platform cooperatives, investments in university research to identify and overcome legal, technological and economic barriers, and the provision of public spaces that platform co-ops can use for free or at a low cost. Accordingly, the interesting idea of this policy paper is that, apart from regulation, public institutions have a whole set of policy solutions they can implement to incentivise the development of socially innovative forms of platform organising and redress abuses of authority within digital markets. If the aim is shaping a more democratic and just digital transition, there is a need for multi-level, multi-sectorial and comprehensive approaches that acknowledge the importance of community-driven alternatives as one piece of the puzzle.

[24] Trebor Scholz and others, 'Policies for Cooperative Ownership in the Digital Economy' (2021) Platform Cooperativism Consortium and Berggruen Institute Policy Paper, December.

Sabrina Akram Ibrahim El Sabi[*]

SPECIAL SECTION

PLATFORM ECONOMY AND ITS IMPACT ON VULNERABLE DIGITAL CONSUMERS

RETHINKING THE EFFECTIVENESS OF UCTD

Abstract

The rapid proliferation of digitisation processes has exponentially increased the number of international online transactions, including business-to-business (B2B), business-to-consumer (B2C), platform-to-business (P2B) and platform-to-consumer (P2C) relationships. The unlimited economic potential of the Internet for commerce, enables the aggregation and globalisation of markets by offering new opportunities, while also requiring new forms of regulation of the digitised landscape. In such scenarios, in recent years it is fundamental to define a regulatory framework and to ensure a greater protection to vulnerable digital consumers. On this point, the digital revolution, which has overwhelmed the European market, trying also to protect the 'weak' party of digital contracts: the consumer-user. The use of digital platforms in contracting, governed at European level by the P2B Regulation, requires the rethinking of the traditional civil law profiles and the promotion of fair and transparent contractual practices.

Moreover, the digital transformation is also reshaping standard contract terms, their application and functionality. Indeed, with the emergence of online platforms, supported by algorithmic data analysis and self-enforcing technologies, platform terms and conditions are becoming increasingly common. The digitisation of standard terms poses challenges to the existing regulatory model of Unfair Contracts Terms Directive – recently amended by the '*Omnibus*' Directive – in several aspects: it needs updating to address the challenges posed by digital services.

In light of an analysis of the rapid evolution of the digital landscape, the work, starting from the vulnerable digital consumer, intended to examine the impact of the platform economy on the latter, the (in)adequacy of the UCTD in the digital world and, finally, how the '*Omnibus*' Directive addresses unfair digital contract terms.

JEL CLASSIFICATION: K12, K15

[*] Research fellow in Private Comparative Law at the University of Bari Aldo Moro. Email: sabrina.elsabi@uniba.it

DOI 10.13135/2785-7867/11332

SUMMARY

1 Introduction

The unstoppable technological development[1] has strongly influenced (and continues to influence) the traditional consumer's role.

Information technology and telematics have profoundly crossed the legal phenomenon causing radical transformations[2] in the way of organising thought, working, educating and even purchasing[3]. Moreover, the purchase of digital goods and services with the simple action of a click, has exponentially increased the number of international online transactions, including business-to-business (B2B), business-to-consumer (B2C), platform-to-business (P2B) and platform-to-consumer relationships (P2C)[4].

Thus, the unlimited economic potential of the Internet for trade enables the aggregation and globalisation of markets by offering new opportunities[5] and, at the same time, presupposes new forms of regulation of the digital landscape.

As well known, the attention given today to the phenomenon of digitisation makes it possible to identify the close relationship between law and technology: law is called upon

[1] Rumana Bukht and Richard Heeks, 'Defining, Conceptualising and Measuring the Digital Economy' (2017) 68 Development Informatics Working Paper Series 4.

[2] See Oreste Pollicino and others, *Diritti e libertà in Internet* (Le Monnier Università 2017).

[3] Eurostat's Digital Economy and Society Statistics - Households and Individuals (September 2020) <https://ec.europa.eu/eurostat/statisticsexplained/ index.php?title=Digital_economy_and_society_statistics_ _households_and_individuals/en> accessed 25 October 2024, on Internet access, which has gained a wide spread in the European Union: 'in 2007 it reached 55% of the population, rising to 75% in 2012, 85% in 2014, 89% in 2018 and finally 90% in 2020. See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Identifying and tackling barriers to the single market" COM (2020)93/F1 (10 March 2020), which states that between 2012 and 2018, despite the sharp increase in online shopping, the lack of confidence in cross-border online shopping compared to domestic online shopping has not diminished but, on the contrary, the percentage of consumers shopping online within the EU has almost doubled.'

[4] Cf A de Streel, 'Online Intermediation Platforms and Fairness: An Assessment of the Recent Commission Proposal' [2018] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248723> accessed 25 October 2024.

[5] Consider, in this regard, the pandemic crisis, which, following the imposition of social distancing and quarantine measures by states, led to an increase in online shopping, the use of online entertainment and online tools for professional purposes. See MC Causarano, 'Le piattaforme online e la tutela degli utenti digitali al tempo della pandemia' (2020) 4 Persona e Mercato 467. See also O Dumitru and AV Tomescu, 'European Consumer Law in the Digital Single Market' (2020) 10(2) Juridical Tribune 223.

to regulate technologies, while at the same time using the innovations made available to mankind to pursue its own ends and determine the creation of new rules[6].

This leads (erroneously) to the assumption that the law-technology relationship is characteristic of more recent epochs, thus ending up by not giving so much prominence to the fact that law has always been related to technologies[7]. It is often the case, however, that technology evolves so rapidly that law cannot adapt or renew itself[8].

In this context, it is necessary to dwell on another relationship: the one between technology, law and vulnerability[9].

"The concept of vulnerability holds an important, yet often overlooked role. It is precisely in a digital era where technologies grow enormously and transactions are predominantly online that vulnerability becomes the breeding ground for exploitation techniques"[10].

Indeed, the evolution of the European market pushes the legislator to prepare new regulatory initiatives aimed at realising and, at the same time, innovating the Digital

[6] See CB Picker, 'A View from 40,000 Feet: International Law and the Invisible Hand of Technology' (2001) 23 Cardozo Law Review 149; J Babikian, 'Justice in Flux: Evolving Legal Paradigms in Response to Technological Advancements' (2023) 1(1) Journal for Social Science Studies 1, 16 <https://journalofsocialscience.com/index.php/Journal/article/view/18> accessed 25 October 2024; V Dudchenko, Y Tsurkan-Saifulina and K Vitman, 'Legal Tech: Unravelling the Nature and Purpose of Modern Law in the Digital Era' (2023) 6(3) Social & Legal Studios 24, 31; M Burri, 'The Impact of Digitalization on Global Trade Law' (2023) 24(3) German Law Journal 551, 573; V Zeno Zencovich and S Grumbach, 'A Painful Divorce: Law vs Digital Technologies' (2024) 1 European Journal of Comparative Law and Governance 1-22.

[7] See G Pascuzzi, *Il diritto dell'era digitale* (5th edition, il Mulino 2020) 26; A Manganelli and A Nicita, *Regulating Digital Markets – The European Approach* (illustrated edition, Springer International Publishing 2022) passim.

[8] G Giannone Codiglione *Internet e tutele di diritto civile: dati – persona – mercato: un'analisi comparata* (Giappichelli 2020) *passim*. An example comes from the issues raised on the subject of online standard contracts and digital platforms, where the need to adopt more modern rules and to update the list of unfair terms has recently been highlighted.

[9] With reference to the relationship between vulnerability and law: some scholars argue that the relationship between vulnerability and law has shown the presence of three elements that capture the essence of vulnerability: exposure to a risk, which is amplified for the vulnerable subject; lack of resilience: the vulnerable subject does not have the resources to avoid the risk that may cause the harm; the vulnerable subject is unable to respond adequately to the harm when the risk has materialised. The vulnerable subject's greater exposure to risk determines the need to construct preventive protective measures, aimed at reducing the probability that such risks may materialise; and to provide for subsequent remedial measures, should the injury have occurred. On this point, see J Herring, *Vulnerable Adults and the Law* (Oxford 2016) 1; J Alwang, P Siegel and SL Jorgensen, 'Vulnerability: a View from Different Disciplines' [2001] Social Protection Discussion Papers and Notes 1; MA Fineman, 'Introducing Vulnerability' in MA Fineman and J Fineman (eds), *Vulnerability and the Legal Organization of Work* (first edition, Routledge 2017) *passim*.

[10] See G Guerra, *Redesigning Protection for Consumer Autonomy - The case-study of dark patterns in European private law* (Franco Angeli 2023) 169; C Lanza, 'Vulnerability and AI-based technologies: European protection of vulnerable consumers in the digital market' (Master thesis, Faculté de droit et de criminologie, Université catholique de Louvain 2023) <http://hdl.handle.net/2078.1/thesis:42369> accessed 25 October 2024; OECD, 'Consumer vulnerability in the digital age' [2023] 355 OECD Digital Economy Papers <https://doi.org/10.1787/4d013cc5-en> accessed 25 October 2024.

Single Market[11] (henceforth, DSM)[12] with specific regard to the area of European online contract law and to digital platforms, with the goal of guaranteeing protection to that 'weak' party of the digital contracting: the user-consumer[13].

The research is structured to examine the notion of vulnerability, especially the concept of vulnerable consumer in the digital economy[14], to ascertain what are the differences between the traditional consumer and the digital one (section 2).

Furthermore, the study also evaluates the impact of the platform economy on vulnerable consumers – whether digital technologies may exacerbate pre-existing vulnerabilities or create new ones – and some of the recent issues on digital contracts (para 2.3), discussing in which point the economy platform could make digital consumers even more vulnerable.

In conclusion, the work analyses common terms in contracts of digital services providers (DSPs), trying to understand whether this type of terms differs from traditional standard terms in various aspects, and whether the existing provisions against the Unfair Contract Terms Directive (UCTD) are still adequate for digital contracts (section 3).

1.1 The Ascent and the Rapid Evolution of the Digital Market

In order to better understand the evolution of the digital consumer and the subsequent impact of the platform economy on it, it is fundamental to focus on the DSM.

The European Union has recently issued a large number of directives and regulations to keep pace with the high rate of innovation of the DSM. European consumer law has started

[11] G Alpa, 'Towards the Completion of the Digital Single Market: The Proposal of a Regulation on a Common European Sales Law' (2015) 26(3) European Business Law Review 347.

[12] In this sense, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Strategy for a Digital Single Market in Europe', COM (2015) 192 <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52015DC0192&from=EN> accessed 25 October 2024.

[13] See J Ouyang, '"Embedded Consumer": Towards a Constitutional Reframing of the Legal Image of Consumers in EU Law' (2024) Journal of Consumer Policy 2, 4.

[14] N Helberger and others, 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45 Journal of Consumer Policy 175. The paper focuses on the notion of consumer vulnerability for the digital economy. "The idea of the 'average consumer' permeates large parts of European consumer law and has been pivotal in building a narrative of consumer empowerment and enabling consumers to protect themselves through active and well-informed choices in the marketplace. This is contrasted by the 'vulnerable consumer'- a concept that singles out certain groups of consumers that are more susceptible to unfair commercial practices than others, and less able to protect themselves. It is argued that, in digital markets, consumer vulnerability is not simply a vantage point from which to assess some consumers' lack of ability to activate their awareness of persuasion".

from a minimum harmonisation approach[15] to arrive at new acts that seek to harmonise[16] the sector completely in order to achieve a functional and uniform internal market (a Single Market, precisely), increasingly driven by the technological revolution and digitisation processes to change perspective, as users interact with commerce in different ways than in the past, with digital content becoming the main product or service to be provided.

As is well known, the strategy on the DSM[17] has been adapted to the 'digital age', precisely because of the recognised importance of digital technologies and the Internet.

Indeed, until then, the use of online tools and services severely limited both businesses and consumers, preventing not only citizens, but also governments, from fully benefiting from the advantages of the digitisation phenomenon.

The DSM strategy is nothing more than the European Commission's reaction to the latest online development to pursue a digital transformation for the benefit of the European community. The DSM envisaged the free movement of goods, persons, services and capital, a market where, irrespective of their citizenship or nationality or place of residence, individuals and businesses face no obstacles to accessing and conducting online activities[18], specifically aimed at preventing or removing unfair commercial practices and

[15] On the dichotomy between minimum and maximum harmonisation, compare also GA Benacchio, 'Pregi e difetti del modello europeo di tutela del consumatore' (2021) 11 Revista Universul Juridic 13 <http://revista.universuljuridic.ro/> accessed 25 October 2024; T Dalla Massara, 'L'imminente attuazione della Dir. UE 2019/771 e il problema del coordinamento con il codice civile: una proposta per il futuro art. 135 c. cons.' (2021) 38(10) Il Corriere giuridico 1278; E Bertelli, 'L'armonizzazione massima della direttiva 2019/771/UE e le sorti del principio di maggior tutela del consumatore' (2019) 4 Europa e diritto privato 953; F Galli, *Algorithmic Marketing and EU Law on Unfair Commercial Practices, Law, Governance and Technology* (Springer 2022) 181. See also, A Savin, 'Harmonising Private Law in Cyberspace: The New Directives in the Digital Single Market Context' [2019] Copenhagen Business School, CBS LAW Research Paper 19; S Weatherill, '10 Maximum versus Minimum Harmonization: Choosing between Unity and Diversity in the Search for the Soul of the Internal Market' in NN Shuibhne and L W Gormley (eds), *From Single Market to Economic Union: Essays in Memory of John A. Usher* (online edn, Oxford 2012) 175; S Weatherill, 'Models of Harmonisation: Maximum or Minimum', in S Weatherill (ed), *Contract Law of the Internal Market* (Intersentia 2016) 223; J Drexl, 'Continuing Contract Law Harmonisation under the White Paper of 1985? Between Minimum Harmonisation, Mutual Recognition, Conflict of Laws, and Uniform Law' in S Grundmann and J Stuyck (eds), *An Academic Green Paper to European Contract Law* (The Hague 2002) *passim*.

[16] See S Pagliantini, 'Armonizzazione massima, parziale e temperata della Direttiva UE 2019/771: una prima lettura' in the paper given at the Conference 'What is European in European Private Law' (Florence 13 September 2019) 44; G D'Amico and S Pagliantini, *L'armonizzazione degli ordinamenti dell'Unione europea tra principi e regole* (Giappichelli 2018) 117; H W Micklitz, 'The Targeted Full Harmonisation Approach: Looking Behind the Curtain' in G Howells and R Schulze (eds), *Modernising and Harmonising Consumer Contract Law* (Sellier European Law Publishers 2009) 47.

[17] Adopted by the European Commission Juncker on 6 May 2015 who decided to commit to innovating Europe's single market. See European Commission, Press Release, 'A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen' (6 May 2015) <https://ec.europa.eu/commission/presscorner/detail/en/ip_15_4919> accessed 25 October 2024.

[18] See C Ratcliff, B Martinello and V Litos, European Parliament, 'Ubiquità del mercato unico digitale, Note tematiche sull'Unione europea' <https://www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-delmercato-unico-digitale> accessed 25 October 2024.

better delineating the latest unfair terms[19], so as to ensure a high level of consumer and personal data protection[20].

In particular, as of 2015, a legislative initiative was announced with the aim of harmonising the online sale of goods and the provision of digital content and services within the platform economy[21].

[19] E Pedilarco, 'Il mercato unico digitale per l'integrazione europea. La prospettiva del Fin Tech' (2018) 3 MediaLaws <https://www.medialaws.eu/il-mercato-unico-digitale-per-lintegrazione-europea-la-prospettiva-del-fintech/> accessed 25 October 2024; J Pelkmans, 'What Strategy for a Genuine Single Market?' (2016) 126 CEPS 1-4 <https://www.ceps.eu/ceps-publications/what-strategy-genuine-single-market/> accessed 25 October 2024; S Montaldo, 'Internet Governance and the European Union: Between Net Neutrality and the Implementation of the Digital Single Market' (2015) 3 Diritto dell'economia 601.

[20] See European Parliament – Fact Sheets on the European Union, 'The Ubiquitous Digital Single Market' (2024) <https://www.europarl.europa.eu/factsheets/en/sheet/43/the-ubiquitous-digital-single-market> accessed 25 October 2024: The goals explicitly stated by the European Commission are fundamental for the achievement of the integration of the digital economy.

[21] This initiative took the form of targeted legislation that was the springboard for the Directive on the Provision of Digital Content and Digital Services (EU Directive 770/2019 - DCD), the Directive on the Online Sale of Goods (EU Directive 771/2019 - SGD), the Digital Services Act (Regulation EU 2022/2065 - DSA), the Digital Market Act (Regulation EU 2022/1925 - DMA), the P2B Regulation (EU 1150/2019). See E Battelli, 'Questioni aperte in materia di contrattazione nelle piattaforme online' (2022) 5 I Contratti 563, 575; On digital platforms see also P D'Elia, *Commercio elettronico e nuove frontiere dell'autonomia privata - Contrattazione online e tutele dell'utente nelle esperienze europee e statunitense* (Giappichelli 2022); E Battelli, 'Il contratto di accesso a Internet' (2021) 1 MediaLaws <https://www.medialaws.eu/rivista/il-contratto-di-accesso-ad-internet/> accessed 25 October 2024, "The use of digital platforms in contracting requires a reconsideration of the purely civil law profiles that seemed to be exhausted in the study of the telematic contract and the consumer protection of the online contracting party. For this reason, one may ask oneself whether the most recent contracting in the virtual dimension of the Internet requires to be declined in a new way, in order to better adapt to the role of online platforms". L Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Raffaello Cortina Editore 2017) 5. The Regulation (EU) 2019/1150 (see Regulation (EU) 2019/1150 of the European Parliament and of the Council (20 June 2019) Eur Lex, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R1150> accessed 25 October 2024, whose main purpose is to promote fairness and transparency for business users of online intermediation services in the different areas of digital markets, is of importance. For more on this topic, see C Ogriseg, 'Il mercato unico digitale e il nuovo assetto di tutele che attende il consumatore' (2022) 2 Ciberspazio e diritto 346; E Bargelli and V Calderai, *A Contract Law for the Age of Digital Platform?* (Pacini 2021) 38; L Guffanti Pesenti, 'Some Considerations about Digital Platforms and Consumer Protection' (2021) 2 European Journal of Privacy Law & Technologies 76; G Smorto, 'La tutela del contraente debole nella platform economy dopo il Regolamento UE 2019/1150 e la Direttiva UE 2019/2161 (c.d. Omnibus)' in V Falce (ed), *Fairness e innovazione nel mercato digitale* (Giappichelli 2020) 64; S Martinelli, 'Contratto e mercato ai tempi dell'algoritmo: reputational feedback system e ranking nella platform economy' Final report of the 15th S.I.S.Di.C. Conference - Naples, 14, 15, 16 May – Rapporti civilistici e intelligenze artificiali: attività e responsabilità (ESI 2020) 2; A D'Alessio, 'Online Platforms: New Vulnerabilities to be Addressed in the European Legal Framework. Platform to Business User Relations' (2020) 2 European Journal of Privacy Law & Technologies 38. This legal framework has been supplemented by the very recent '*Omnibus*' Directive (EU Directive 2161/2019), the preliminary regulatory intervention of which is part of the package of measures presented by the EU Commission on 11 April 2018, under the name 'New Deal for Consumers. See Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, A New Deal for Consumers, COM (2018) 183 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0183> accessed 25 October 2024.

The "New Deal for Consumers" initiative, aimed at strengthening enforcement of EU consumer law in light of a growing risk of EU-wide infringements and at modernising EU consumer protection rules in view of digital market developments[22].

Its primary aim is to strengthen the enforcement of EU consumer law in the light of the increasing risk of infringements at EU level and to modernise the rules for better enforcement in view of market developments[23].

This project shed light on the digital consumer, the consumer-user who buys (digital) goods and services on online marketplaces[24].

With the '*Omnibus*' directive, the European legislator focused particularly on the consumer acting in the DSM. In particular, the transposition of the directive in question in the various member States aimed to implement a real modernisation of the consumer code, through a greater openness to digitisation, thanks also to the inclusion of new notions, such as, for instance: 'online marketplace', 'digital services', 'digital content' and 'online search'. The main innovations brought about by the directive concern transparency in the online marketplaces, unfair terms, increased penalties, online reviews, price reductions, and the role of the consumer even in cases where the purchase of a digital product or service takes place through the payment of personal data[25].

The main purpose of the directive is to require online shop providers to fulfil specific information obligations in order to close information gaps that may, in some way, influence the consumer's decision-making capacity and, thus, prevent unfair commercial practices or the introduction of new unfair terms.

The purpose of the 'Package' seems particularly clear: to offer legal certainty and protection to European consumers and to facilitate transactions of digital content and

[22] See Ouyang (n 13). About the New Deal see also M Grochowski, 'European Consumer Law after the New Deal: A Tryptich' (2020) 39 Yearbook of European Law 387 <https://academic.oup.com/yel/article/doi/10.1093/yel/yeaa016/6204745#302918654> accessed 25 October 2024 "Particularly, the New Deal put considerable emphasis on online commerce. As part of this package, it primarily seeks to provide a better framing not only for the new ways of concluding agreements and the novel types of tradeable objects (including consumer data as a counter-performance), but also to address the evolving structure of the market as such (in an attempt to tackle the new modes of concluding and executing agreements online)".

[23] I Speziale, 'La Dir. 2019/2161/UE tra protezione dei consumatori e promozione della competitività sul mercato unico' (2020) 4 Il Corriere giuridico 441.

[24] L Ammannati, 'Il paradigma del consumatore nell'era digitale Consumatore digitale o digitalizzazione del consumatore?' (2019) 1 Rivista trimestrale di diritto dell'economia 8; F Foltran, 'Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri negoziali' (2019) 3 MediaLaws 162 <https://www.medialaws.eu/rivista/professionisti-consumatori-e-piattaforme-online-la-tutela-delle-parti-deboli-nei-nuovi-equilibri-negoziali/> accessed 25 October 2024; G Sartor, *New Aspect and Challenges in Consumer Protection - Digital Services and Artificial Intelligence* (Strasburgo: European Parliament 2020) 9 <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)648790> accessed 25 October 2024.

[25] VSZ Bonamini Pepoli, 'L'evoluzione del consumatore nell'era del digitale' (2023) 10 Federalismi.it 243 <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=48719> accessed 25 October 2024; C Cauffman, 'New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' (2019) 26(4) Maastricht Journal of European and Comparative Law 469.

goods, all specifically at cross-border level, demonstrating the persistent discrepancies in the field of user-consumer protection[26].

On the basis of these considerations, it should be noted that the technological revolution does not only bring about (undoubtedly) positive effects, but also appears to produce numerous challenges and high risks, influencing the way traditional sectors operate, turning, for instance, more interest towards intangible goods and services[27].

2 Digital Asymmetries: A (New) Role for the Vulnerable Consumer-User?

The development of new digital technologies has had a profound impact especially on the legal relations between consumer-users and web-based economic operators, leading to the emergence of new issues concerning the digital consumer and his position in the digitised ecosystem.

We should start from the fact that "in the digital society, vulnerability is architectural because the digital choice architectures we navigate daily are designed to infer or even to create vulnerabilities"[28]. Hence, "digital choice architectures are designed to infer

[26] See on this point, Camera dei Deputati, Temi dell'attività parlamentare, XVII legislature, 'The Digital Single Market' <https://temi.camera.it/leg17/temi/il_mercato_unico_digitale_> accessed 25 October 2024, as well as 'Digitisation Index of the Economy and Society (DESI) 2021 (Italy)' (2021) 2, as well as DESI <https://digital-strategy.ec.europa.eu/it/policies/desi> 'The Digital Single Market: the Italian position' (2022) AgID, 2 <https://www.agid.gov.it/sites/default/files/repository_files/documentazione/position_paper_on_dsm_italia_0.pdf> accessed 25 October 2024.
In particular, reference is made to the Digitisation of Economy and Society Index (DESI), developed by the European Commission to assess the state of progress of the EU Member States towards a digital economy and society, as there are still considerable differences between the Member States.
See, in particular, European Commission, 'Shaping Europe's digital future 2023 Report on the state of the Digital Decade' (2023) <https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade> accessed 25 October 2024. "This report highlights the need to accelerate and deepen the collective efforts, including through policy measures and investment in digital technologies, skills and infrastructures. It includes concrete recommendations to Member States ahead of the adoption of their national strategic roadmaps and for their future adjustments'.

[27] Cf G Alpa, 'Il mercato unico digitale' (2021) 1 Contratto e impresa Europa 2; E Tulli, *Filosofia e rivoluzione digitale. Echi dal futuro* (Stilo Editrice 2020) 114; L Taddio and G Giacomini, *Filosofia del digitale* (Mimesis 2020); O Dimitru and AV Tomescu, 'European Consumer Law in the Digital Single Market' (2020) 10(2) Juridical Tribune 222; S Montaldo, 'Internet Governance and the European Union: Between Net Neutrality and the Implementation of the Digital Single Market' (2015) 3 Diritto dell'economia 601; C Riefa, 'Protecting Vulnerable Consumers in the Digital Single Market'(2022) 33(4) European Business Law Review 607.

[28] This situation might be related to dark patterns. See J Luguri and L Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43, 44; A Mathur, J Mayer and M Kshirsagar, 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' Proceedings of the 2021 CHI Conference on Human Factors Computing Systems (Article no. 360, 2021) 3 <https://doi.org/10.1145/3411764.3445610> accessed 25 October 2024; MR Leiser and M Caruana, 'Dark Patterns: Light to be found in Europe's Consumer Protection Regime' (2021) 10(6) Journal of European Consumer and Market Law 237, 251; OECD, 'Dark commercial patterns', OECD Digital Economy Papers, No. 336 (OECD Publishing 2022) <https://doi.org/10.1787/44f5e846-en> accessed 25 October 2024; M R Leiser, 'Dark Patterns: The Case for Regulatory Pluralism between the European Union's Consumer and Data Protection Regimes' in 'Research Handbook on EU Data Protection Law' (Edward Elgar Publishing, 2022) 240; M Leiser and C Santos, 'Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface' (2024) 15(1)

vulnerabilities, that can be considered the product of digital consumer markets. As consumers keep using the same services, apps, or platforms over time, the commercial entities offering those services, apps, or platforms will be able to collect and analyse more user data and, as a result, be better able to identify exploitable vulnerabilities. So far, the usual asymmetrical nature of commercial relationships become even more significant"[29].

The notion of vulnerability[30] is very complex and is not defined within rigid boundaries because it is universal and individual (it does not affect all individuals in the same way); potential, relational and contextual (we are vulnerable in a certain context and not in another)[31]. Very often the Society itself makes individuals vulnerable.

Vulnerability, to be understood as the widespread potential to be injured, also tends to be found in all those cases where there is a structurally asymmetrical legal relationship and where a subject, on the basis of personal and external factors, is considered the weak party of the relationship. It is necessary to try to identify which subject can be considered vulnerable in the digital environment (this is the case of the consumer operating on the web[32]), as it cannot simply be based on the assumption that in the face of technology

European Journal of Law and Technology *passim* "The term 'dark patterns' is commonly used to describe manipulative or exploitative techniques implemented into the user interface of websites and apps that lead users to make choices or decisions that would not have otherwise been taken. Legal academic and policy work has focused on establishing classifications, definitions, constitutive elements, and typologies of dark patterns across different fields. Regulators have responded to these dark patterns with several enforcement decisions related to data protection, privacy violations, and rulings protecting consumers". Specifically, "The term 'Dark patterns' or 'deceptive design', commonly refers to design practices that manipulate or exploit users to achieve specific outcomes, often at the expense of their autonomy, decision-making, or choices. The use of dark patterns has become a growing concern. The response to dark patterns has evolved from theoretical problem-based academic work and behavioural studies to active enforcement by regulatory bodies worldwide". This concept is also related to the one of 'Psychological Patterns'. In this sense, see also M Leiser 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface' (2024) 1(1) Journal of AI law and Regulation 5 which "emphasises the urgency of addressing the risks posed by AI-powered deceptive design strategies intricately woven into online platforms. These 'psychological patterns' mislead users into making decisions contrary to their intentions, exploiting psychological vulnerabilities"; CM Cascione, 'Art 5, co. 1, lett a)' in A Mantelero, G Resta and GM Riccio (eds), *Intelligenza artificiale. Commentario* (Kluwer 2025) forthcoming.

[29] See Alpa (n 11); D Susser, B Roessler and H Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World' (2019) 4(1) Georgetown Law Technology Review 27; J Strycharz and B Duivenvoorde, 'The exploitation of vulnerability through personalised marketing communication: are consumers protected?' (2021) 10(4) Internet Policy Review 1.

[30] A definition of vulnerability can be found in the document 'United Nations Report on the World Social Situation: Social Vulnerability: Sources and Challenges' (2003) United Nations Department of Economic and Social Affairs 3 <https://www.un.org/esa/socdev/rwss/docs/2003/RWSSOverview.pdf> accessed 25 October 2024 in which the following is stated: "In essence, vulnerability can be seen as a state of high exposure to certain risks and uncertainties, in combination with a reduced ability to protect or defend oneself against those risks and uncertainties and cope with their negative consequences. It exists at all levels and dimensions of society and forms an integral part of the human condition, affecting both individuals and society as whole".

[31] Cf E Ferrarese, 'Vulnerability: A Concept with which to undo the World as it is?' (2016) 17(2) Critical Horizons 149.

[32] See P Stanzione, 'Data Protection and Vulnerability' (2020) 2 European Journal of Privacy Law and Technology 9. In particular: "We can outline a basic notion of 'vulnerability' as a common connotation of the human condition, next to

everyone is vulnerable, but that it is necessary to go further, providing special protection mechanisms.

The examination of the different forms of vulnerability[33] inherent in these individuals has the twofold objective of improving aspects related to consumer protection[34] and of obtaining useful information to direct regulatory choices with a view to greater fluidity in the functioning of the markets, especially in view of the problems associated with the emergence of new forms of abuse and unfair commercial practices.

It is necessary to start from the assumption that consumers of digital products are less protected than consumers of traditional goods, probably due to opaque and fragmented legislation. This leads to a precise question: should all consumers, belonging to different social groups, be guaranteed equal protection, or should additional special protection measures for these categories be envisaged in the face of the emergence of 'new' vulnerable groups?

In this regard – albeit briefly and without claiming to be exhaustive – it is necessary to dwell on the legal notion of vulnerability[35], reconsidering the role it plays in strategic marketing and non-marketing choices[36].

This condition has always involved consumer-behaviour, according to which the vulnerable consumer is qualified as such due to a lack of resources and information, as well as a loss of control of the situation in which he becomes the object of deception. His fragile condition stems from his unawareness.

---

which it can be seen the variability of the situations in which it is declined: conditions due to age, gender, health and other discriminating factors. One of these conditions may however also be the relationship, legal and socio-economic, structurally asymmetrical, of which the subject is a weak part: so for the consumer or the user of digital platforms".

[33] On the more generic concept of vulnerability, see G Maragno, 'Alle origini (terminologiche) della vulnerabilità: vulnerabilis, vulnus, vulnerare' in O Giolo and B Pastore (eds), *Vulnerabilità. Analisi multidisciplinare di un concetto* (Carocci 2018) 13, 187.

[34] Cf C Goanta, 'European Consumer Law: The Hero of Our Time' (2021) 10(5) Journal of European Consumer and Market Law (EuCML) 177.

[35] On this topic see EC, 'Digital Fairness, Fitness check on EU Consumer Law' (2023) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumerlaw_en> accessed 25 October 2024; A Ruiz Arranz, 'The Commencement of Prescription (and what the Consumer's Awareness of the Unfairness is) within the Unfair Contract Terms Directive' (2023) 19(3) European Review of Contract Law 181, 214 <https://doi.org/10.1515/ercl-2023-2011> accessed 25 October 2024 at 181 "Closely linked to the phenomenon of the effectiveness of the UCTD is the idea of vulnerability, which is at the core of consumer protection and is the very reason that pushed consumer protection onto the EU policy agenda. Vulnerability is associated directly with the experience of consumption. Unlike the trader, the consumer is not doing business and lacks the experience to handle economic transactions and legal contracts. To that end, consumers need information and a means to prevent imbalanced relationships. This imbalance was traditionally expressed with the notion of the consumer as a 'weaker party' and has progressively emerged as a general principle of EU law. The Member States would be left free to provide the consumer with additional protective standards that, despite shared minimum rules, would indeed have enhanced the weaker position of consumers".

[36] M Durovic and J Poon, 'Consumer Vulnerability, Digital Fairness, and the European Rules on Unfair Contract Terms: What Can Be Learnt from the Case Law Against TikTok and Meta?' (2023) 46 Journal of Consumer Policy 419.

Inevitable is the need to innovate and expand this notion[37].

However, the economic concept of the consumer has appeared over the years to be far too restrictive, as technology, emerging as an amplifier of inequalities, has begun to require interpreters to look at the consumer from a perspective increasingly connected to his or her own social fragility.

This need stems from the fact that the role of the consumer in the new digital marketplace has changed radically, making it possible to speak of a Consumer 5.0[38] and, therefore, of a new phase in the evolution of consumer law.

A further reason indicating the need to innovate the notion is connected to the fact that, at present, the only and explicit regulatory reference, on the subject of vulnerability, at European level, derives from the dictate of Directive (EC) 2005/29 on unfair commercial practices[39], which has a particularly circumscribed scope of application.

In fact, it is inferred from the rule that some consumers may be considered constitutively vulnerable due to physical or sensory disabilities. This is because the hypothesis could also derive from a psycho-behavioural state that then flows into the social sphere, involving a consumer in perfect physical and mental condition, whose fragility depends, instead, on different so-called extrinsic factors (think, for instance, of the digital divide[40], which provides for an uneven distribution of ICTs in society)[41].

In this regard, the World Economic Forum's (WEF) Global Risks Report 2022[42] indicated that the excessive use of the web and digital platforms brings with it socio-psychological problems. Individuals/users are so affected by digital exposure that their physical and emotional well-being is severely affected[43].

---

[37] See L Cappello, *L'evoluzione del consumatore negli ecosistemi decentralizzati - L'impatto della digitalizzazione e della Blockchain* (Giappichelli 2022) 7, in which it is pointed out that "Even the subjective dimension of the role of economic actors changes in the new digital market in which consumer and producer not only converse on the same level, but also join to the point of blurring their respective roles with the diffusion of the figure of the prosumer, producer and consumer at the same time".

[38] ibid 5.

[39] Cf Recital 18 of the UCPD.

[40] See again G Pascuzzi, *La cittadinanza digitale* (Il Mulino 2021) 36, "The digital divide, as clarified by the OECD (2001) identifies the gap existing between individuals, households, businesses and geographical areas at different socio-economic levels with reference both to the opportunities to access information and communication technologies and to the use of the Internet for a wide variety of activities".
See, in this regard, also G Suffia, 'Smart cities and the digital divide: una proposta di analisi' (2021) 2 Ciberspazio e diritto 287, as well as G Pesci, 'The digital divide, l'uguaglianza sostanziale e il diritto all'istruzione' (2021) 2 Ciberspazio e diritto 259.

[41] See Article 13-bis of Decree-Law 179/2012.

[42] Cf 'Digital Dependencies and Cyber Vulnerabilities, in The Global Risks Report 2022' (2022) 3 The World Economic Forum (in collaboration with Marsh & Mclennan Companies, Sk Group and Zurich Insurance Group) 45 <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf> accessed 25 October 2024.

[43] V Bhargava and M Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction' (2021) 31(3) Business Ethics Quarterly 321.

Virtual reality (i.e. that reality altered by digital means) creates a sense of security in the user such that it engenders legitimate trust, but at the same time, it induces in the user false ideas about security, privacy and trust. The erosion of such trust can damage the relationship between users and traders/intermediaries, weakening their self-determination and also affecting their own decisions and conduct.

Digital consumption undermines this interaction of trust between human beings.

In particular, the relationship with digital platforms makes the consumer psychologically vulnerable.

Thus, in a context in which the dissemination of digital tools has become more complex, 'new' vulnerability hypotheses have arisen witnessing the reconsideration of socio-economic factors.

Then, the evolution and the critical analysis of the concept of consumer fragility/vulnerability posed in the digital economy become crucial to understand.

The central question, which raised several issues, is based on the admissibility of the concept of the vulnerable digital consumer, as well as the greater or special protections to be afforded to them.

On this point, some scholars appear to be divided: while on the one hand, it is believed that the creation of new forms of vulnerability, which require an adequate regulation by the legislator, should be admitted[44], on the other hand, it is argued that in the face of digital literacy, the consumer appears more aware and, for this reason, not in need of a different/increased degree of protection[45].

"In this regard, solutions to the previous questions may be found in the UCTD and also in the UCPD[46]. The universality of these two acts makes them a useful tool for incorporating new categories of interests into consumer law and extending their protection. Less straightforward, however, is the relationship between consumer protection and the new EU acts that directly concern new forms of individual market participation and the new interests that are pursued in this way"[47]. This is because EU law is still at the experimental stage, juggling intuitions and piecemeal solutions.

[44] F Pellicanò and R Petti, 'La vulnerabilità del consumatore nei settori delle comunicazioni elettroniche e dell'audiovisivo' (2022) Consumerism 2022 – Quindicesimo rapporto annuale – Il consumatore vulnerabile tra innovazione e diritti fondamentali, Università degli Studi Roma Tre 75 <https://www.consumersforum.it/ricerche.html> accessed 25 October 2024.

[45] See AL Sibony and G Helleringer, 'European Consumer Protection through the Behavioral Lens' (2017) 23 (3) Columbia Journal of European Law 607.

[46] M Grochowski 'Consumer Law for a Post-Consumer Society' (2023) 12(1) Journal of European Consumer and Market Law (EuCML) 1, 3.

[47] ibid. "This is particularly true of the Digital Services Act (DSA) and the Digital Markets Act (DMA), which largely address the relationship between an individual and a professional (a platform), which in many instances is a classical business-to-consumer liaison. Paradoxically, however, both acts partly deny their consumer nature. Many references to consumers are made in a 'negative' manner to indicate that certain issues they address do not interfere with consumer rules".

It has been ascertained how between users and web operators there exists a level of asymmetry determined by a disparity of technical knowledge and information that might affect the correct formation of the will, even contractual, of the user. In fact, the considerable difference between the knowledge of the contracting parties may, at the time of the conclusion of an online contract, generate erroneous expectations or unlawful reliance on the service provider to the point of vitiating the moment of formation of the will. Relevant, therefore, is the issue of transparency.

The imbalance of power between consumers and data-powered traders who control digital environments creates a foundation for unfair practices – and the consumer can do very little to prevent it. In the coming years, with the proliferation of AI systems and biometric technologies, the position of the consumer can only be expected to become ever weaker in the face of automated systems perfected for making money on human weaknesses and vulnerabilities.

Under conditions of digital asymmetry, the consumer is particularly susceptible to practices which exploit the differences in power to the detriment of the consumer. This resulting universal state of vulnerability, referred to here as digital vulnerability, applies to virtually all consumers who participate in the data economy and undermines their autonomy of choice.

In addition, the proliferation of AI systems (i.e. the use of AI systems to infer consumers' emotions) and biometric technologies may be expected to strengthen asymmetries between traders and consumers and as a tool to exploit vulnerabilities.

2.1 The Vulnerability of the Digital Consumer

New technologies, given their global dimension and the difficulty of finding timely regulation of the numerous legal issues related to their use, would leave the consumer increasingly vulnerable and without effective protection[48]. This raises a number of questions, most notably one concerning consumer law itself: Could it currently be considered equally effective? Or is it in need of innovation?[49]

[48] Durovic and Poon (n 36) 181, 188.

[49] Also on this point G Magri, S Martinelli and S Thobani, *Manuale di diritto privato delle nuove tecnologie* (Giappichelli 2022) 3.

The idea of the 'average consumer'[50] has now definitely entered in crisis[51]. That's because, the evolution of new technologies and the rapidity of their development in the digital ecosystem lead one to question the degree of care, diligence, prudence and information demanded of the average consumer.

Thus, this crisis in which the digital consumer finds himself is nothing more than the outcome of a series of issues that have arisen in recent years (attributable to technological evolution), which has rendered the traditional disciplines, introduced to date for consumer protection, incompatible or difficult to reconcile with the digital consumer relationship[52].

What makes the digital consumer even more vulnerable than the traditional one? One of the main obstacles for web users susceptible to automated decision-making processes is that of transparency: being able to make the logic of the algorithms used by the platform clear. In this respect, a properly informed user has greater freedom of choice in the digital marketplace.

[50] See S Sandulli, 'Vulnerabilità e consumatore al tempo della pandemia' in P Corrias (ed), *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati* (ESI 2022) 178 "For some time, doctrine and jurisprudence have formulated numerous theories on vulnerable subjectivity. On this point we refer to the studies by S Dodds, C Mackenzie and W Rogers, who refer to three different forms of vulnerability: inherent, situational and pathogenic. This distinction, on the one hand, calls into question the notion of the average consumer as a parameter of reference, on the other hand, in addition to human conditions and merely external factors, generates a different situation of vulnerability (the authors, in this regard, emphasise the polysemy of the term)". On this topic see also S Ranchordas, 'Vulnerable Consumers and Vulnerable Citizens - What Can Consumer Law Teach Other Fields of Law?' (2021) 10(6) Journal of European Consumer and Market Law (EuCML) 225; A Furia and S Zullo, 'Introduzione' in Id. (ed), *La vulnerabilità come metodo: percorsi di ricerca tra pensiero politico, diritto ed etica* (Carocci 2020) 9.

[51] On the topic of the 'average consumer' see Case C-465-98, *Verein gegen Unwesen in Handel und Gewerbe Köln eV v Adolf Darbo* AG EU:C:2000:184 [2000]. See also Case C-210/96 *Gut Springenheide* EU:C:1998 [1998]; Case c99/01 *Gottfried Linhart e Hans Biffl* [2002] ECR I-9375, paras 31-32; Case C-44/01 *Pippig* [2003] ECR I-03095, para 55; Case C-218/01 *Henkel KGaA* [2004] ECR. I-1725, paras 47, 52, 53 Case C-381/05 *De Landtsheer Emmanuel SA c. Comite´ Interprofessionel du Vin de Champagne, Veuve Clicquot Ponsardin* SA [2007] ECR I-3115, para 23; Case C-210/96 *Gut Springenheide* EU:C:1998:369 [1998]. See again Ouyang (n 13), "This legislative development followed the long-standing ECJ case law on misleading commercial practices, which postulates that average consumers are not easily misled. […] For the first time, in the case Gut Springenheide, the Court of Luxemburg defined the consumer as a reasonably well-informed person, observant, and circumspect. This implies that the 'informed consumer' can autonomously distinguish the characteristics of products and understand the message and content of advertising, with an 'average' ability that need to be ascertained, case by case, about the situation and the peculiarities of the case. In recent times, the ECJ argued that the formula of the 'reasonably well informed and reasonably observant and circumspect consumer', established in Gut Springenheide needed to be updated. The notion of consumer is a reference threshold for the current analysis as it represents a centrepiece of European consumer protection law". See also D Szilágyi, 'Empowering consumers: Towards a broader interpretation of the vulnerable consumer concept in the European Union' (2022) 63(3) Hungarian Journal of Legal Studies 279, 293; G Straetmans and J Vereecken, 'Towards a New Balance Between Private and Public Enforcement in EU Consumer Law' (2024) 32(1) European Review of Private Law 41, 80.

[52] On this issue, refer, among many others, to: S Lanni, 'Pregiudizi algoritmici e vulnerabilità' (2021) suppl 3 Rivista trimestrale di diritto dell'economia 72; A Jablonowska and others, 'Consumer Law and Artificial Intelligence. Challenges to the EU Consumer Law and Policy Stemming from Business' Use of Artificial Intelligence: Final Report of the ARTSY Project' (2018) European University Institute (EUI) Working Papers 11, who went much further by explicitly arguing that "Consumer protection law turned into consumer law without protection".

In this sense, the new and changing online activities have slowly led to an evolution of the notion of consumer - that is far removed from the conventional one – and laid the foundations for a new declination of the value of consumer awareness.

In fact, the consumer appears to be a figure with a polymorphous nature and an intrinsically evolutionary vocation (with respect to which the monolithic nature of the notion would contrast with the variety of spheres, specifically the digital markets in which this subject operates).

Economic factors (market fragmentation), legal factors (regulatory polycentrism) and intellectual factors (the greater degree of maturity in thinking about this issue) are pushing beyond the uniform category of the average consumer.

Technological innovation and data represent the central elements of the evolutionary process that characterises the new digital ecosystem, contributing to the creation of a renewed socio-economic scenario, in which several actors operate: companies, consumers, and providers of digital services and products[53].This has undoubtedly contributed to the emergence of a category of consumer, tending to be different from the traditional one, who, if, on the one hand, would seem to be endowed with an increased awareness of the exercise of his or her freedom of choice, on the other hand, could be made more vulnerable by the digitised ecosystem in which he or she operates[54]. The peculiarities deriving from digital make them particular consumers.

In fact, it is specified that all consumers at some point may become vulnerable due to external factors or their interaction with the market or due to the difficulties they face in accessing and understanding relevant consumer information.

In view of these considerations, it must be examined whether there is a concrete distinction between traditional (offline) and digital (online) consumers, what exactly makes a digital consumer (even) more vulnerable than the first one?

In this regard, one of the factors affecting the greater or lesser vulnerability of digital consumers may be linked to their educational process and digital literacy[55]. In addition,

[53] See S Agarwal, 'Consumer Protection in the Digital World' (2022) 3(2) Jus Corpus Law Journal 616; J Jakhar, 'Consumer Protection (E-Commerce Rules), 2020: Revolution for Consumer Protection in Digital Space' (2022) 5 International Journal of Law Management & Humanities 1919; A Fletcher and others, 'Consumer Protection for Online Markets and Large Digital Platforms' (2023) 40(3) Yale Journal on Regulation 875.

[54] L Gatt and IA Caggiano, 'Consumers and Digital Environments as a Structural Vulnerability Relationship' (2022) 2 EJPLT 8.

[55] In addition to being context-dependent, the phenomenon of vulnerability is inevitably linked to the socio-demographic characteristics and background of the consumer (to be understood not only as the individual's level of education and the technological skills acquired over time or the result of one's temperament and aptitude, but also as the level of knowledge of products and services that are the object of the consumer's attention). A 2016 European Commission study, entitled 'Understanding Consumer Vulnerability in the EU's Key Market', identifies the conditions and characteristics that can make consumers vulnerable. For a more in-depth analysis of the related study <https://commission.europa.eu/publications/understanding-consumer-vulnerability-eus-key-markets_en> accessed 25 October 2024.

there are issues related to digital consumption, such as accessing digital products or services online.

A fair and non-discriminatory approach to digital transformation should address the needs of user-consumers, who are often less accustomed to digital tools or less comfortable with them.

This leads to a concept of the consumer placed in a situational perspective, understood as objective, functional and dynamic. For this reason, even vulnerability itself must not be assessed in the abstract, but rather according to the specific situation in which the consumer finds himself, so as to extend protection not only to the average consumer but to all[56].

Therefore, this category of consumers obliges, in certain respects, to question the criteria of correct qualification as well as to rethink the traditional regulatory tools.

On this point, it is necessary to refer to the study carried out by Martha Fineman[57], who explored the concept by stating that the expression vulnerability should be understood as a universal and shared condition of human beings, an inevitable consequence of 'human embodiment' (within which the category of vulnerable consumers would also fall).

However, according to this approach, fragility, which at the societal level is constant and universal, at the individual level is characterised as particular and unique.

According to this new paradigm of human vulnerability, fragility is understood as a positive condition in order to realise equality of opportunity and access[58] which must commit institutions to remove the conditions that prevent them from addressing the challenges related to individual fragility. Consumer vulnerability, therefore, would not be the exception, but the rule[59].

Think also of the categories of children, older adults[60], the sick or the disabled, who are often the subject of 'paternalistic' discrimination based on an alleged lack of ability.

---

[56] Durovic and Poon (n 36).

[57] M Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 (1) Yale Journal of Law & Feminism 9. Fineman conceptualises vulnerability as a universal and ever-present experience that can be exposed at any time by our individual circumstances. The framing of the notion of vulnerability is necessary because by clearly identifying why consumers may qualify as vulnerable, and the factors that lead to that vulnerability, it is possible to construct an environment that respects consumer choice, while ensuring the appropriate protection of the vulnerable.

[58] M Fineman, 'Beyond Identities: The Limits of an Antidiscrimination Approach to Equality' (2012) 92(6) Boston University Law Review 1716.

[59] A Cole, 'All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerable Studies, an Ambivalent Critique' (2016) 17(2) Critical Horizons 260; C Riefa and S Saintier, 'Economic Theory and Consumer Vulnerability: Exploring an Uneasy Relationship' in Id. (eds), *Vulnerable Consumers and the Law. Consumer Protection and Access to Justice* (Routledge 2021) 17.

[60] On the topic of the older consumer see CM Cascione, *Il lato grigio del diritto. Invecchiamento della popolazione e tutela degli anziani in prospettiva comparatistica* (Giappichelli 2022) 207. A Fusaro, 'Persona vulnerabile e forme di condizionamento del volere', in P Corrias (ed), *I soggetti vulnerabili nella disciplina e nei mercati regolamentati* (ESI 2022) 59; H Berg and KT Liljedal, 'Elderly Consumers in Marketing Research: A Systematic Literature Review and Directions for Future Research' (2022) 46(5) International Journal of Consumer Studies 1640. See also L Berg, 'Consumer

These kinds of differences have led to hierarchical subordination and social exclusion of the person who possesses them, as being part of a 'weak category'[61].

It is emphasised that the concept in question cannot be relegated to rigid, pre-set canons, since there is a plurality of factors that, considered individually, affect the individual's economic choices in completely different ways.

What differs is that in the consumer-market relationship, vulnerability is more easily identifiable and to some extent governable through regulation that is attentive to the specificity of each group.

What is more, such a hypothesis entails the emergence of excessive discretion on the part of the judge in emphasising the vulnerabilities of the individual due to the difficulty of anchoring the judgement in objective data.

Once the different sources and states of digital vulnerability have been identified[62], one should ask what legal effects flow from the assessment of a situation of vulnerability.

In particular, the criterion of inclusiveness is relevant.

We must, then, start from the relationship with the consumer and reconsider the role of vulnerability, so that their digital fragility is respected.

The concatenation between exogenous factors, dependent on the external environment and endogenous factors[63], linked to the intrinsic characteristics of the individual, determine the optimal conditions for the manifestation of vulnerability phenomena.

Thus, more generically, consumer vulnerability is posited as a state of powerlessness generated by an inability to control a situation or condition that, in a specific market context, causes the consumer harm or a disadvantageous situation such as to interfere with his or her purchasing and consumption behaviour.

In light of these issues, it may be considered that consumer vulnerability is a dynamic concept, since are the people and contexts that generated it, and that it is identified in the potential of the subject to be harmed.

Although numerous contributions have been made to give an account of the complexity of the phenomenon, to date there is still no unanimous consensus on what constitutes a

Vulnerability: are Older People More Vulnerable as Consumers than Others?' (2015) 39(4) International Journal of Consumer Studies 284.

[61] Cf G De Cristofaro, 'Legislazione italiana e contratti dei consumatori del 2022: l'anno della svolta. Verso un diritto "pubblico" dei (contratti dei) consumatori?' (2022) 45(1) Le nuove leggi civile commentate 38.

[62] See F Luna, 'Identifying and Evaluating Layers of Vulnerability – A Way Forward' (2019) 19(2) Developing World Bioethics 86.

[63] See S Chatratha, GS Batra and Y Chabac, 'Handling Consumer Vulnerability in E-Commerce Product Images Using Machine Learning' (2022) 8 Heliyon 2, which states that vulnerability can also be influenced by personal factors/circumstances that include (among many) even temporary health problems (physical or mental), emotional trauma or abandonment, physical impairment, weak language skills, dependency difficulties.

state of vulnerability and what its effects are on consumers[64], as the legislation dealing with it is still disorganized and fragmented[65].

2.2 Is There A Digital Consumer Vulnerability?

The notion of vulnerability[66] suffers from indeterminacy, due precisely to its legal, economic and sociological origin[67], such that it is highly versatile in its application in the most diverse contexts[68].

The extension of protection in terms of vulnerability is therefore undeniable, with regard to web users only, when referring to a specific group of consumers[69].

With regard to the legal situations of vulnerability, there is a growing trend towards a concept that serves as a heuristic device[70] as well as a qualitative and/or quantitative indicator in the identification of situations potentially detrimental to dignity, in order to identify corrective and implementing solutions, oriented towards the promotion of the principles of equality and autonomy of the person, not only of protection and safeguard.

One hopes, therefore, for the construction of a common law for vulnerable persons (minors, older persons, digital consumers) that approaches the instruments of protection

[64] See again M Durovic and J Poon (n 36). See EU Digital Markets Act (DMA) itself, Regulation (EU) of the European Parliament and of the Council of 14 September 2022 on fair and contestable markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Regulation) (Text with EEA relevance) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925> accessed 25 October 2024, proposed by the Commission in December 2020 and approved by the European Parliament and the Council in March 2022, in which no mention is made of vulnerable consumers. On this topic, see also Press Release, 'Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter Into Force' (2022) European Commission <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423> accessed 25 October 2024, as well as 'The Digital Markets Act: Ensuring Fair and Open Digital Markets (2022), <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed 25 October 2024. The same goes for the Digital Services Market (DSA), proposed in December 2020 and 25 March 2022 by the European Commission to improve the rules governing digital services in the EU <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 25 October 2024, in which the identification of vulnerable consumers is only hinted at and, where it is hinted at, the conceptualisation of vulnerability is still severely limited, with groups of consumers influenced by factors such as gender, race, ethnic origin, religion, belief, disability, age or sexual orientation as factors that make specific groups or persons vulnerable or disadvantaged in the use of online services.

[65] E Bettelli, 'Dal concetto di debolezza alla nozione di vulnerabilità' in P Corrias (ed), *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati* (ESI 2022) 37.

[66] FD Busnelli, 'La dimensione della fragilità lungo il percorso della vita umana' in Id. (ed), *Persona e famiglia. Scritti di Francesco D Busnelli* (Pacini 2017) 239, in whose opinion the condition of vulnerability requires recovering, as a necessary premise, the fundamental principle of human dignity.

[67] See also Fusaro (n 60) 56.

[68] A De Giuli, 'Sul concetto di 'vulnerabilità' secondo la Corte di Giustizia UE' (2020) 10 Diritto penale e uomo (DPU) 1.

[69] G Berti De Marinis, 'La vulnerabilità nei mercati regolamentati' in P Corrias (ed), *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati* (ESI 2022) 89.

[70] M Fineman, 'Il soggetto vulnerabile e lo Stato responsabile', in MG Bernardini and others(eds), *Vulnerabilità etica, politica, diritto* (IF Press 2018) 166, Trad. it. by B Casalini and L Re, (article first published as 'The Vulnerable Subject and the Responsive State' 2010 (60) Emory Law Journal 151, 275).

in a more ductile manner[71], as distinct from the merely patrimonial law that today pervades the various negotiation situations of simple informational weakness or disparity of bargaining power.

This context calls for a rethinking of the protection tools.

Some authors[72] have dwelt on the idea of an effective differentiation between vulnerable and non-vulnerable consumers, assuming that consumers can adopt very different attitudes depending on the circumstances in which they find themselves, so the group of vulnerable consumers cannot be considered a homogeneous group, but diversified according to assumptions and circumstances.

They found that if all consumers were considered vulnerable, the relevance of the concept of vulnerability and its operation would be lost[73].

Despite the fact that this concept is more realistic and fluid, the standardisation of the notion of vulnerable consumer, whether on the one hand leads to greater malleability, on the other hand produces greater vagueness and legal uncertainty.

Therefore, it is possible to choose to give rights to a vulnerable group of consumers, adjusting the rules on a case-by-case basis, and without making any discrimination.

However, as has already been ascertained, various subjective aspects interfere in the consumer relationship and exacerbate the vulnerability of the contracting party; these are the personal conditions of certain consumers or social groups, which increase inequalities and determine a greater fragility, due to age, socio-economic conditions, cultural and psychological factors, which constitute the so-called 'aggravated vulnerability' or 'hypervulnerability' of the consumer (for example, the consumer's weakness and ignorance may be included in the context of hypervulnerability). These categories of subjects, therefore, require special protection, on pain of violation of the principle of equality.

This phenomenon, together with the traditional assumption of vulnerability, intensifies the fragility of the consumer, justifying greater protection for the hyper-vulnerable.

[71] Battelli (n 65) 58.

[72] See S Fernandes Garcia and J Morais Carvalho, 'Vulnerabilidad y Consumo: ¿Tiene Sentido Distinguir entre Consumidores Vulnerables y no Vulnerables?' in E Soto Isler and D Jarufe Contreras (eds), *Vulnerabilidad y Capacidad - Estudios sobre Vulnerabilidad y Capacidad juridica en el Derecho Comùn y de Consumo* (Rubicón 2022) 43, in which it is pointed out that "Portugal will follow a similar path in the near future. The measure, little applied so far, is based on the establishment of a set of criteria and rights corresponding to the vulnerable consumer status, which seems to aim at the approval of a cross-cutting legislative instrument".

[73] This explains why the concept of hypervulnerability has been created in some countries. The concept can be used to distinguish consumers precisely to overcome the idea that everyone is vulnerable. If everyone is vulnerable, we must distinguish between consumers who are more vulnerable than others and the concept of hypervulnerability.
See also F Barletta and M Maurilio Casas, 'A Proteção dos Vulneráveis e o Direito Civil: Um Mandamento Constitucional? Breves Reflexões' (2022) 31(141) Revista de Direito do Consumidor (RDC) 227; M De Souza Ciocchetti and D De Souza Freitas, 'As Pessoas em Situação de Pobreza nas Relações de Consumo: a Hipervulnerabilidade e os Direitos Humanos' (2022) 31(141) Revista de Direito do Consumidor (RDC) 180, 188; D Mendes Thame Denny and others, 'COVID-19 Magnifies the Vulnerabilities: The Brazilian Case' (2021) 21(3) International Journal of Discrimination and the Law 279.

Indeed, applying the same treatment to all consumers, without assessing the subjective characteristics of certain purchasers or groups, would represent a new inequality.

In the digital society, the creation of new legal transactions in electronic commerce and the abuse of the use of personal data of web users by ISPs and third parties leads to the risk of increased vulnerability, hence the notion of hypervulnerability.

Thus, many concerns arise about the effectiveness of the regulatory instruments for consumer protection.

In such cases, governments must take care not only of the vulnerable, but especially of the hypervulnerable, as these are the ones who, as part of a minority that is often discriminated against or ignored, suffer the most prejudice. Protecting the hypervulnerable benefits the entire community, respecting the principle of social inclusion.

The subjective aspects of hypervulnerability must be balanced and evaluated in favour of the most fragile consumers in order to ensure the restoration of material equality and respect for the dignity of the individual in contractual relations. Therefore, the hypervulnerable deserve special attention, aimed at finding a means to pursue individual equality.

The concept should only be used in cases where the consumer is in a particularly vulnerable condition.

Thus, the distinction between vulnerable and non-vulnerable consumers may make sense, but at the same time, such a distinction implies going beyond the scope limited to consumer law alone to consider the individual as a citizen.

There is a need to look at digital vulnerability in the widest possible context by examining the impact that new technologies have on consumers. Therefore, in the digital context, in which all individuals may be potentially vulnerable, the understanding of who is a vulnerable consumer needs to be updated as soon as possible.

The way forward, therefore, would be to do the backward reasoning, i.e. to embrace the concept of vulnerability as the norm rather than the exception. This would allow the current consumer protection framework to be recalibrated (without necessarily having to wait for an actual reform, which, as is often the case, would be delayed) to assist consumers where they are unable to do so themselves[74].

2.3 Platform Economy Contracts and Consumers

In order to prevent consumers and businesses from being unfairly discriminated against when accessing content or purchasing goods and services online within the EU, one of the objectives of the DSM Strategy is to outline an appropriate regulatory framework for e-commerce.

[74] See in this respect the final considerations by C Riefa, 'Protecting Vulnerable Consumers in the Digital Single Market' (2022) 33(4) European Business Law Review 633.

Among the various regulatory initiatives, it is also worth to mention Regulation 1150/2019[75] ('P2B'), which "originates precisely from the need to answer to the issue relating to the protection of commercial users who offer their goods and services through online platforms, mainly intended as 'online intermediary service providers' and search engines. In particular, many studies conducted in recent years have revealed a number of abusive practices in the relationship between digital intermediaries and users that have shed light on the shortcomings of the system and the need to strengthen the position of the latter[76]".

Continuing the analysis on cross-border e-commerce[77], one of the reasons that has made consumers and smaller businesses skeptical is that the rules applicable to transactions can be complex, unclear and possibly differ from one member State to another. The duty to adapt to different national regulations on consumer protection and contracts has always discouraged businesses from engaging in cross-border trade, preventing consumers from taking advantage of the cheapest offers and the full range of online offerings[78].

Further criticism is raised with regard to platform economy contracts[79]. Compared to traditional standard contracts drafted by the trader and submitted to the consumer, the terms and conditions of the contract are drafted by the platform and signed by its users and, unless otherwise specified, the same clauses apply to suppliers and users, both being qualified indiscriminately as users of the services provided by the platform. While it is true that the terms and conditions of contract practised by platforms would attribute rights and establish duties symmetrically for providers and users, it is also true that, by controlling the entire negotiation process, platforms exercise considerable power over their users, which is reflected in the terms and conditions of contract relating to the relationship between users and the platform, containing many of those provisions that highlight a condition of asymmetry between the contracting parties[80].

[75] Cf Among these, Regulation 1150/2019 should also be mentioned and, in this regard, see G Maggiore and L Lo Presti, *La responsabilità del marketing digitale, difendere il consumatore vulnerabile* (Giappichelli 2022) 2, 4; G Versaci, 'Le tutele a favore del consumatore digitale nella "Direttiva Omnibus"' (2021) 3 Persona e Mercato 583.

[76] ibid.

[77] See Fact Sheets on the European Union (n 20).

[78] Cf A Kuczerawy, 'To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive' (*Ku Leuven*, 10 July 2019) <https://balkin.blogspot.com/2019/05/to-monitor-or-not-to-monitor-uncertain.html> accessed 25 October 2024; K Osei Bonsu, 'An Economic Analysis of Consumer Right Protection in E-Commerce: Testing Efficiency Using the Principles of Contract Law' (2019) 15(1) International Journal of Progressive Sciences and Technologies 186. See L Bozzi, 'Le proposte di direttiva sui contratti di vendita online e sulla fornitura di contenuti digitali e la disciplina delle obbligazioni restitutorie – un tentativo (riuscito?) di bilanciamento dei contrapposti interessi' (2018) 116(4) Rivista del Diritto Commerciale e del diritto generale delle obbligazioni 603; VV Cuocci, 'Contratti online e mercato unico digitale: l'approccio (minimalista) del legislatore europeo in tema di clausole abusive' in A Addante (ed), *Tutela del consumatore nei contratti telematici e nuove frontiere del diritto europeo della vendita* (Cedam 2017) 73.

[79] F Möslein, 'Digitized Terms: The Regulation of Standard Contract Terms in the Digital Age' (2023) 19(4) European Review of Contract Law 300.

[80] See Fact Sheets on the European Union (n 20).

The main issues concerned contractual clauses reserving to platforms the right to unilaterally modify the contract, which is almost always accompanied by a presumption of acceptance of the users resulting from the continuous use of the platform[81].

The analysis conducted so far leads to one consideration: while platforms help to make the relationship between providers and users more balanced with regard to the provision of services, the same cannot be said with regard to the legal relationship that the platform has with its users, as many clauses used by online platforms strongly prejudice individual users[82].

Indeed, the prejudices stemming from digitisation undermine the digital platform-consumer interaction, making the latter particularly vulnerable[83].

In such a context, in which the spread of digital tools is becoming increasingly complex, 'new' vulnerability hypotheses have arisen, thus witnessing the reconsideration of socio-economic factors, which are once again relevant[84].

It becomes crucial to understand the evolution and critical analysis of the concept of consumer fragility/vulnerability in the digital economy, and the impact of the platform economy on the digital consumer (which may make it even more vulnerable).

In this respect, one consideration could be made with regard to consumer protection issues often arise from the informal production of services and insufficient transparency with regard to liability rules and resolution or redress mechanisms if problems occur in the platform economy[85], which creates benefits but also risks.

European consumers have been exposed to new ranges of illegal goods, activities and content, while new online businesses struggle to enter a market dominated by large platforms. Connecting many businesses with many consumers through their services and their access to large amounts of data gives big platforms leverage to control and set standards for important areas of the digital economy. The EU wants to regain the initiative to shape those areas at the European level and set standards for the rest of the world[86].

---

[81] P Hausemer and others 'Exploratory Study of consumer issues in peer-to-peer platform markets' (2017) Brussels: European Commission <https://eprints.soton.ac.uk/411699/1/FinalreportMay2017pdf_2_.pdf> accessed 25 October 2024.

[82] ibid.

[83] Cf RP Kanungo and others, 'Digital Consumption and Socio-Normative Vulnerability' (2022) 182 Technological Forecasting and Social Change 2.

[84] Others include those that can be traced back to a social cause or economic condition inherent to the poor; immigrants, refugees, workers.

[85] Eurofound, European Foundation for the Improvement of Living and Working Conditions <https://www.eurofound.europa.eu/en/platform-economy-consumer-protection> accessed 25 October 2024. See also, JP Vazquez Sampere, 'Why Platforms Disruption Is So Bigger Than Product Disruption' (2016) 4 Harvard Business Review <https://hbr.org/2016/04/why-platform-disruption-is-so-much-bigger-than-product-disruption> accessed 25 October 2024.

[86] EU legislation needs to catch-up with online developments and that is why the EU worked on a new legislative framework called the Digital Services Act (DSA) and the Digital Markets Act (DMA), which aim to set guidelines for the new online landscape, including online platforms, to ensure a better, safer digital environment for users and companies throughout the EU.

Indeed, the growing emergence of the platform economy is having a distorting effect on both the established economic models and the related regulatory system[87] and on the issues related to digital platforms[88]. Resorting to a broad conceptualisation, one can consider that the existing regulatory systems do not seem fully capable of providing adequate legal solutions to the numerous problems related to the platform economy, its nature and function.

In this sense, the question is: Which regulatory measures should be applied to strike a harmonious balance between promoting healthy innovation and ensuring a safe digital transactional environment for all classes of users contracting with platform operators?

It is now clear that in the platform economy contracts are often concluded in a condition of total asymmetry of bargaining power to the advantage of platforms; what is not clear, however, is whether, and to what extent, solutions capable of counteracting these inequalities are actually emerging. Although, in some cases, the protection of the weaker contracting party in the platform economy may be guaranteed through recourse to traditional protections, in other hypotheses it may not be possible to disregard the implementation of a regulatory intervention – to be added to the ordinary remedies of common rights – that guarantees the balance between private autonomy and contractual equity.

In such a framework, it is essential to interpret the general terms and conditions prepared by platforms through technological tools, taking into account the operating systems and structure of sites, apps and algorithms.

3 Standard Contracts and Platforms: Benefits and Detriments from the Digital World

The objective envisaged by the European legislator, through its recent numerous regulatory initiatives, has been to adapt the European Single Market to the Digital Age, thus making it imperative to frame the regulation of contracts in the broader context of digitisation-related phenomena, including contracts for the provision of digital content and services[89].

[87] See C Bush and others, 'The Rise of the Platform Economy: A New Challenge for EU Consumer Law?' (2021) 5 Journal of European Consumer and Market Law 3.

[88] European Commission 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Online Platforms and the Digital Single Market – Opportunities and Challenges for Europe' (2012) <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52012DC0673> accessed 25 October 2024; M Colangelo and V Zeno-Zencovich, 'Online Platforms, Competition Rules and Consumer Protection in the Travel Industry' (2016) 5 Journal of European Consumer and Market Law 75.

[89] G Guerra, 'Il contenuto digitale nel contratto di vendita di beni e servizi. Note a margine della nuova disciplina di armonizzazione (massima) europea' [2020] Giustiziacivile.com 1-10.

"Within the context of the Strategy for a Digital Single Market, the European Commission introduced new rules that harmonise collective enforcement of consumer protection laws to better safeguard consumers' interest put forward the Digital Services Act package"[90].

We have seen how digital transformation has also led to a change in standard contract terms. In effect, with the emergence of online platforms, supported by algorithmic data analysis and self-enforcing technologies, platform terms and conditions have become increasingly common. Since these clauses deviate strongly from traditional standard terms for many reasons, several authors[91] have, after careful examination, questioned whether the current regime of unfair contract terms is still appropriate for the evolving category of the digital consumer-user.

The emergence of online platforms, supported by algorithmic data analysis and self-enforcing technologies, is increasingly replacing traditional standard terms with platform terms. Generally speaking, the emergence of the platform economy modifies the regulatory framework within which transactions occur.

Hence, "it is necessary to amend the UCTD to, on the one hand, improve consumer protection online against unfair contract terms of DSPs and, on the other hand, to provide more legal certainty to DSPs as to what terms and conditions are considered fair"[92].

Perhaps, the regulatory instruments developed for the standard terms of bilateral agreements (transparency requirements, review of fairness and restrictions on contracts) seem inadequate to meet the new challenges of digital transformation. In order to strike the right balance between protecting private autonomy and avoiding significant imbalances, a new regulatory strategy is needed. Therefore, the regulatory objective should be to ensure the impartiality of platforms by focusing on the structural conditions of their regulation[93].

The European legislator adopted the same regulatory approach in the broader context of digital legislation: the P2B Regulation refers to transparency in its title and makes it one of its main regulatory objectives[94]. In particular, Article 3 requires online intermediary service providers to ensure transparency in various aspects. However, it is considered that the regulatory instrument of transparency is not sufficient to preserve private autonomy

[90] See literature described (n 15).

[91] On this subject, see C Poncibò, 'The UCTD 30 Years Later: Identifying and Blacklisting Unfair Terms in Digital Markets' (2023) 19 (4) European Review of Contract Law 321, 345; DT Apostolos, 'The Court and the Sleeping Beauty 2.0: Filling the Contractual Gap, or Making Valid Consumer Contracts to the Detriment of the Non-consumer?' (2023) 19(4) European Review of Contact Law; M Ginestri, 'Equality or Superiority of the Weak Party? Consumer Protection and the Issues at Stake' (2023) 19(4) European Review of Contract Law 375; P Hacker 'Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law' (2021) 29 European Law Journal 142.

[92] MBM Loos and J Luzak, 'Update the Unfair Contract Terms directive for digital services' (2021) European Parliament - Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies 17-22.

[93] MBM Loos, 'Crystal Clear? The Transparency Requirement in Unfair Terms Legislation' (2023) 19(4) European Review of Contract Law 281.

[94] P2B Regulation (EU 1150/2019) Art 1(1).

in the face of digitised standard terms. Although transparency regulations may help to overcome information asymmetries and promote informed choices, they prove ineffective when restrictions on private autonomy have other causes.

That's why specific prohibitions should be introduced into the UCTD to address some of the most common transgressions.

On the other hand, other scholars have pointed out that the discipline laid down by the UCTD is sufficient and can also be extended to the online world, at most being supplemented[95].

The emergence of online platforms, supported by algorithmic data analysis and automated technologies, is increasingly replacing traditional standard terms with platform terms. In this respect, there is a need to assess the adequacy of the existing regime of unfair contractual terms to digitised terms or whether a new regulatory approach is needed. The regulatory tools developed for standard terms in bilateral agreements, relating to transparency requirements, fairness review and restriction on contracting, do not longer seem adequate to meet the challenges of digital transformation.

Through these legislative initiatives, the EU's main aim would be to adopt appropriate measures aimed at the establishment or functioning of the internal market, while contributing to the achievement of a high level of consumer protection, and to ensure the right balance between this achievement and the promotion of the competitiveness of enterprises (especially SMEs)[96].

Starting from these premises, therefore, the aim will be to investigate the actuality of the inequality of bargaining power in the digital market economy, in order to demonstrate how the risk arising from this imbalance has not diminished (on the contrary) and how the numerous European regulatory initiatives appear ambiguous, lacking and still totally insufficient to guarantee appropriate protection for the vulnerable digital consumer.

3.1 Unfair Terms Regulation and Vulnerable Subjects

As is well known, the numerous regulatory initiatives envisaged by the European legislator in recent years highlight a further issue: the need to protect the vulnerable position of users in the digital market and operating in e-transactions. This has had a particular impact on the necessary reframe of certain regulations, first of all the UCTD[97], leading interpreters to wonder whether the UCTD itself may be sufficient for the protection of this 'new' category of subjects or whether the adoption of *ad hoc* measures as well as a constant updating of the list of unfair contract terms (especially the updating

[95] See B Hajek, 'Online Platform Service Providers on Platform 9¾: A Call for an Update of the Unfair Contract Terms Directive' (2020) 28(5) European Review of Private Law 1143, 1174.

[96] Cf Recital 1, Dir. (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the supply of digital content and digital services (22 May 2019) OJEU L 136/1.

[97] C Gardiner, *Unfair Contract Terms in the Digital Age. The Challenge of Protecting European Consumers in the Online Marketplace* (Edward Elgar 2022).

of blacklists) is essential. Indeed, the UCTD needs updating to address the challenges posed by digital services. "This concerns in particular the fundamental research question of identifying new unfair terms of DSPs so that they can be included in a new blacklist"[98]. The scope is to guarantee the evolution of consumer law, in the digital age, and promoting a fair and transparent environment for consumers in an ever-changing digital landscape[99].

In this sense, the work will examine whether general terms in contracts of digital service providers, in the event of a significant imbalance between the rights and obligations of the parties aimed at harming consumers, can be brought within the scope of the UCTD, whose framework was mainly developed for the offline world[100].

Indeed, numerous new marketing practices are based on the use of sophisticated technologies that also allow for large-scale processing of data that may include personal consumer data.

The evolution of algorithmic practices will be evaluated based on specific normative thresholds set by EU consumer law. As we know, consumer law does not offer the sole or optimal normative framework for assessing the development of algorithmic business practices. Crucially, to effectively analyse the impact of digitisation on legal relationships, it is essential to clearly define and articulate these different perspectives[101].

Thus, in this context, it is also crucial to assess the online transparency of digital service providers' clauses and the penalties to which they might be subject in the event of violation of the current consumer protection framework[102].

Overall, the digitisation of standard terms poses challenges to the existing regulatory model of the Unfair Contracts Terms Directive – recently amended by the *Omnibus* Directive – in several aspects. Although the UCTD was never genuinely reformed in the over thirty years since it entered into force, it needs updating to address the challenges posed by digital services.

Whereas platform terms are not considered part of "contracts concluded between a seller or supplier and a consumer" (Art 1 par 1 UCTD), but are provided by a third party, and personalised terms may not be "drafted in advance" (Art 3 par 2 UCTD), technological self-enforcement threatens to create significant imbalances (Art 3 par 1 UCTD).

In order to preserve the architecture of choice for private contracts, it is necessary to consider a new legal strategy. This is because, the measures once developed for standard

[98] These updates are necessary for the development of the study on the 'Fitness Check of EU Consumer Law' concerning the evolution of consumer law in the digital sphere.

[99] See G Hiwatashi Dos Santos, 'A "New Deal for Consumers"? The European Regulatory Framework for Online Search Queries and Rankings under the Omnibus Directive (Directive (EU) 2019/2161)' (2020) 2 Anuário do NOVA Consumer Lab 66.

[100] Loos and Luzak (n 92).

[101] Ouyang (n 13).

[102] Recommendations are made to improve the effectiveness of this framework through: the introduction of a black list and a grey list of unfair terms, the strengthening of existing sanctions and the introduction of new obligations for digital service providers.

terms in bilateral agreements – transparency requirements, fairness review, and restrictions on contracting around – seem inadequate to meet the new challenges of digital transformation.

Perhaps, in this context, the current European framework regarding unfair contract terms may not effectively protect when they enter into contracts with DSPs. This is because, although the digital sphere has brought about many benefits, it has also placed consumers in a more vulnerable position.

On this point, the digital revolution, which has overwhelmed the European market, has led the legislator to draw up new regulations aimed at implementing and innovating the DSM – with particular reference to the field of European online contract law, trying also to protect the 'weak' party of digital contracts: the consumer-user (taking into account, for instance, the DCD concerning contracts for the supply of digital content and services, and the SGD concerning contracts for the sale of goods)[103].

This is in response to the boundless economic potential of the Internet for commerce, which enables the aggregation and globalisation of markets.

The use of digital platforms in contracting, governed at European level by the P2B Regulation, requires a reevaluation of traditional civil law profiles. The evolution of telematic contracts and the protection of digital consumers call for a fresh approach that goes beyond established legal frameworks.

For this reason, the legal models should be technologically neutral – allowing for flexibility and adaptation to evolving business models and technological advancements in the platform economy – and should also balance the interests of platform operators, users, and regulators, promoting fair and transparent contractual practices.

In light of these considerations, online platforms are one of the main technological drivers providing alternative regulatory infrastructures based on their standard terms and conditions.

In this sense, the research analyses different types of digital-specific unfair terms used by DSPs: the ones concerning digital services and contents, automation and personalisation, and finally, the ones concerning consumers' data rights. It would be

[103] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the supply of digital content and digital services L 136/1 <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32019L0770> accessed 25 October 2024; Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects of contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32019L0771> accessed 25 October 2024.
Turning to the analysis of the transposition of Directive (EU) 2019/770, on contracts for the supply of digital content and services, and Directive (EU) 2019/771, on contracts for the sale of goods, the European delegation law does not provide for any particular criteria regarding the transposition of the relevant regulatory provisions into Italian law. The Directives, complementing each other, are qualified as 'Twin Directives'; however, despite their common peculiarities, they also present clear differences. See I Férnandez Chacòn, 'Some Considerations on the Material Scope of the New Digital Content Directive: Too Much Work Out for a Common European Framework' (2021) 3 European Review of Private Law 517.

necessary to examine the regulatory options, aimed at defining the vulnerability of users and, particularly, the possibility of establishing a new blacklist of digital-specific unfair terms and integrated them with some guidelines for fairness assessment under the UCTD.

The need to change the directive emerged only in the past year, through the *Omnibus* Directive (also known as Modernisation Directive – MD). This change is limited to increasing the effectiveness of the UCTD sanctions and facilitating the enforcement of unfairness in the Member States. The specific aim is "to propose measures increasing the effectiveness of the UCTD framework in the provision of digital services. To that effect, the study presents an overview of commonly encountered terms used by digital service providers and evaluates whether they may cause a significant imbalance, contrary to good faith, in the parties' rights and obligations to the detriment of consumers. Where this is indeed the case, such terms could be considered unfair"[104].

"In effect, the aforementioned digital landscape has unique features that were not present in traditional face-to-face transactions. In particular, consumers interact with a wide range of digital service providers and online platforms, and these interactions are governed by terms and conditions which lay out the contractual obligations and rights of both consumers and service providers and should be designed to protect the interests of all parties. These terms and conditions often disadvantage consumers, putting them in a more vulnerable condition caused by the digital asymmetry"[105].

This is fundamental for the evaluation of the need for amending this directive in order to improve, on the one hand, the protection of online consumers against unfair contractual terms of digital service providers and, on the other hand, to give more legal certainty to digital service providers concerning terms and conditions that are considered unfair[106].

In this regard, the purpose of this work is to deal with the question of contract supplementation and the revision of unfair contractual terms, enlightening the main problems the digitisation has encountered.

3.2 Types of Digital-Specific Unfair Terms

The current European framework against unfair contract terms may not be an effective regulatory tool for consumer protection, especially when consumers conclude contracts with DPSs. As member States offer more consumer protection than the UCTD, DSPs may be faced with a different assessment of unfairness in the different member States, resulting in unequal conditions for digital service providers.

[104] The EU Parliament published a preliminary list of updated unfair or potentially unfair clauses that can be found in the terms and conditions of contracts concluded between consumers and Digital Service Providers (DSPs) see on <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006(SUM01)_EN.pdf> accessed 25 October 2024.
[105] Gardiner (n 97).
[106] See Fact Sheets on the European Union (n 20).

It has been noted that in recent years, new unfair contract terms have emerged in specific sectors, leading to the need to innovate the discipline. Nevertheless, identifying digital-specific unfair terms used by DSPs in consumer contracts poses new challenges trying also to understand if the UCTD differs in the digital world.

Firstly, digital services and digital content: the analysis of "common terms in contracts of digital service providers, indicating when they could significantly distort the balance between the parties' rights and obligations to the detriment of consumers and should, therefore, fall within the scope of the Unfair Contract Terms Directive"[107].

In particular, digital services could only be provided in the online environment by DSPs and not provided offline. At times, consumers may not be certain whether they have acquired a digital content or a digital service and, therefore, what protection they are entitled to. The MD recognises this ambiguity, as the supply of digital content could also be a series of individual acts of supply or even continuous supply throughout a period of time, which characteristics are normally associated with the provision of digital services (Recital 30 MD). A recommendation that could be made for the revision of the UCTD, in this respect, is a recognition of unfairness of such terms and conditions of DSPs, which do not transparently or correctly identify the nature of the contract, as well as statutory rights and obligations of parties following from it.

This is just one example of a situation, where a standard term of a contract for the provision of digital services could implicitly undermine consumer protection and discourage or even stop consumers from claiming their rights[108].

Numerous other clauses, however, can be taken into account and, therefore, brought under the UCTD, including: Contract terms which oblige the consumer to conclude an additional digital content contract or another contract pertaining to hardware with a third party; Contract terms preventing consumers from exercising rights under copyright law; Contract terms misrepresenting a service as acquisition of content, using tacit consent and 'browsewrap' contracts or misrepresenting the service as free where the trader monetises their personal data, time or attention; Contract terms forcing the consumer to waive ownership of content they share on the service (videos they produce, photos uploaded on social media, etc.); Contract terms giving the trader the right to unilaterally delete a consumer's user account (this can have a huge impact on consumers, for many their online accounts are an important part not only of their social but also their professional activity)[109].

[107] See again Gardiner (n 97).

[108] BEUC, 'EU Consumer Protection 2.0 - Protecting fairness and consumer choice in a digital economy' (2022) 3-9 <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf> accessed 25 October 2024.

[109] N Helberger and others, 'Towards Digital Fairness' (2024) 13(1) Journal of European Consumer and Market Law (EuCML) 24-30; N Helberger and others, 'Digital Fairness for Consumers' (BEUC 2024) 262.

However, at the moment these terms are just indicative of unfairness and are included in a non-exhaustive and exhaustive list.

The other hypothesis involving the possible identification of new abusive clauses concerning Contract Terms derived from automated systems as the digital landscape expanded, so did the complexity and opacity of the processes underpinning digital services. Many DSPs began leveraging sophisticated algorithms, and AI systems, to make decisions that directly affected users.

While these automated systems often brought about efficiency and personalisation, they also introduced challenges, notably in transparency and equity. Users were often unaware of how decisions were made on their behalf and with what implications. This lack of transparency made it difficult for consumers to make informed decisions and left them vulnerable to potential biases and unfair practices embedded within these algorithms.

The whole issue related to automated systems only serves to highlight the inadequacy of consumer protection instruments, due to the numerous gaps and significant flaws in legislation (e.g. the most recent AI legislation)[110].

Finally, some unfair terms may involve intricate technological aspects, such as data collection, processing, and sharing practices. It is essential to discuss about the peculiarities of the assessment of online transparency of terms of digital service providers and sanctions they could face if they breach the current consumer protection framework and their personal data. For that reason, recommendations have been proposed in order to improve the effectiveness of this framework by: introducing a black and grey list of unfair terms, strengthening current sanctions, and introducing new obligations for digital service providers. If DSPs do not comply with such obligations, they could find themselves in breach of the GDPR[111]. This may either provide consumers with additional remedies[112].

To strengthen legal certainty in the relationship between DSPs and consumers, it could be recommended to extend the principle of transparency from the UCTD to apply to DSPs providing information as to which of their online disclosures are part of their terms and conditions.

Practices based on data exploitation can render consumers entirely powerless in situations where insights from their data allow the trader to exploit their vulnerabilities and pressure points against them. In effect, at the level of contractual clauses, consumers purchasing goods and services can be put in a situation of particular disadvantage where the 'fine print' in the contract terms requires them to enter into yet another contract to use their newly purchased device (e.g. connected devices proving to be useless without a

[110] S Pant, 'EU Rules on AI Lack Punch to Sufficiently Protect Consumers' (2023) Press Release 1.

[111] F Zuiderveen Borgesius, N Helberger and A Reyna, 'The Perfect Match? A Closer Look at the Relationship between Eu Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1451.

[112] For example, an option to withhold performance, not allow DSPs to rely on their liability exclusion or limitation clauses or allow courts to terminate the contract if this is more advantageous to the consumer than merely leaving the term contradicting the GDPR out of consideration.

contract with a service provider), or when they are prohibited from using the device in ways which are allowed by law[113].

As a result, certain clarifications are necessary to improve the online consumer protection against unfair contract terms of DSPs and to provide more legal certainty to DSPs as to what terms and conditions are considered fair.

In this sense, even the possibility to deliver special guidelines was outlined, but that said, given the emergence of new unfair contractual terms, additional guidance for DSPs is needed for defining how compliant terms and conditions in digital business should look like (e.g. in relation to consent to the collection and use of personal data in line with GDPR, or to changes to terms and conditions, or to copyright and ownership of consumer-generated content); and how they would best be presented online (digital design).

However, a problem is that guidance is not legally binding. Consequently, only some market participants actually look at the guidance and are familiar with the detailed examples and supporting case law provided[114].

In conclusion, since digital contracts adopt and adapt traditional clauses to suit online interactions, it is crucial to differentiate between known unfair terms that are repackaged for the digital context and the new one specifically tailored to digital markets. As a matter of fact, while these terms may not be entirely novel, their implementation and impact in the digital realm can differ from what happens in traditional settings.

Distinguishing reiterations of known terms and original ones is crucial for effectively addressing the root causes of consumer harm.

Hence, to promote gap-filling regulations, an additional regulatory mechanism is needed to encourage the emergence of balanced conditions. Rather than sanctioning conflicting regulators, such a regulatory instrument should favour those regulators that appear to be particularly reliable. Such an approach would benefit from the fact that platforms are, in principle, particularly well-positioned to design rules that mimic the market, as they have access to data on market participants' preferences that are not usually available to regulators.

3.3 The '*Omnibus*' Directive: Towards (and Beyond) the Modernisation of Consumer Protection in the Digital Society

These years of technological changes have not only identified a regulation that catches up with the changes, but have also provoked a shift in the relationship between regulation and interpretation of the abovementioned legal framework. This has made the current system more complex and, at the same time, has led to the ineffectiveness of traditional regulation and protection techniques, making it necessary, finally, "to adopt new logics

[113] See R Montinaro, 'Online Platforms: New Vulnerabilities to be Addressed in the European Legal Framework. Platform to Business User Relations' (2020) 2 European Journal of Privacy Law & Technologies 38.
[114] Durovic and Poon (n 36).

to recompose a system (that despite the implementation of a European discipline of maximum harmonisation is still persistent) that is jagged[115]". Among the most significant changes affecting this process we can list: the pluralism of sources that undermines Consumer law (not only at the national level), which is naturally destined to continuous revisions necessary to adapt it to the new European legislation; the globalisation of the economy and competition between systems; the crisis of the 'average' consumer, whereby the provisions merely indicate the protected interest and the purpose of protection, leaving the interpreter with the task of filling in the gaps; finally, the sectoral and vertical legislation, which is sometimes too analytical (sterile or repetitive).

The main and direct consequence of these changes is the shift from the traditional unity of the system to its current unevenness, characterised by a plurality of sectoral disciplines (sometimes overlapping, sometimes intersecting) and general rules.

The further (negative) effect of the changes brought about by the technological revolution was the direct (and partial) obsolescence of pre-existing provisions.

This has been recognised following the advent of the aforementioned 'New Deal for Consumers[116]' and, above all, the '*Omnibus*' Directive (MD), although on the whole the rules appear inadequate and become quickly obsolete.

On closer inspection, the modernisation of consumer protection rules has been driven by increasing societal demands. Several gaps in national consumer laws have been identified due to breaches in the transposition of previous directives and new digital tools. Furthermore, another important aim of this Directive is to strengthen the transparency and information requirements already well established in other legislation[117].

What appears ineliminable, notwithstanding the additions and subtractions due to the continuous impact of legislative evolution, is the presence of general principles and rules of a cross-sectoral nature that are suitable for guaranteeing a statute of general consumer rights and protections, which can then find their declination in special rules.

It is precisely by looking more closely at the transposition disciplines of the two UCTD and UCPD, that we can already see the non-univocal nature of the notion of consumer[118].

[115] Cappello (n 37).

[116] Cf S Perugini, 'La normativa comunitaria' in G Cassano, M Dona and R Torino (eds), *Il diritto dei consumatori* (Giuffrè 2021) 42.

[117] Gardiner (n 97).

[118] See in this regard G De Cristofaro, 'Rimedi privatistici "individuali" dei consumatori e pratiche commerciali scorrette: l'art. 11-bis Dir. 2005/29/UE e la perdurante (e aggravata) frammentazione dei diritti nazionali dei paesi Ue' (2022) 2 Jus Civile 269; M Maugeri, 'Invalidità del contratto stipulato a seguito di pratica commerciale sleale?' (2022) 2 Jus Civile 319, 320; L Guffanti Pesenti, 'Pratiche commerciale scorrette e rimedi nuovi. La difficile trasposizione dell'art 3, co. 1, n. 5), Dir. 2019/2161/UE' (2021) 4 Europa e diritto privato 635; C Camardi, 'Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista' (2021) 4 Jus Civile 885, in which it is found that "The very recent Directive 2019/2161, on the modernisation of consumer rights has intervened inter alia to amend those already introduced on unfair terms, unfair commercial practices, price indications, by reinforcing the information obligations also incumbent on platforms, especially with reference to whether or not the operator offering goods and services through it is a

The first, which essentially looks at the contract and its content, focusing on the clauses intended to make it up, refers to a notion that we could call 'concrete' of consumer, useful to delimit the scope of application of the rules.

The second, which essentially considers the activity and not the act, refers to an abstract figure of the consumer, which the legislator seems to use to indicate the objectives pursued through legislative action (by shifting the focus from the act to the activity, the figure of the consumer expands and emerges from the rigidity that usually characterises it).

It follows from this that there is no single legal concept of the consumer and this also generates critical issues in terms of consumer protection[119].

There is thus an apparent need not to limit the broad topic of the protection of subjects who, although differently identified and defined, are still bound by the same need for protection (despite criticisms have been raised on this point[120]). In such a context,

professional (a circumstance that the consumer purchaser must be aware of in order to determine the rules applicable to the contract, consumer law or common law)"; Finally, for an overall assessment of the new Directive, see F Cafaggi, 'Rimedi e sanzioni nella tutela del consumatore: l'attuazione del New Deal' (2020) 2 Questione Giustizia 4. For a more general perspective on consumer law see, instead, G De Cristofaro, '40 anni di diritto europeo dei contratti dei consumatori: linee evolutive e prospettive future' (2019) 2 I Contratti 177; S Pagliantini, *Il diritto privato europeo in trasformazione – Dalla direttiva 771/2019/EU alla direttiva 633/2019/EU e dintorni* (Giappichelli 2020) 2.

[119] On this issue, a comparison should be made with the findings of P Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti* (3rd edn, ESI 2020) 510, where it is expressly stated that "consumer protection is not always achieved through the protection of consumption: sometimes the subject is protected as a citizen, sometimes as a person the quality of consumer is only an aspect of the person, a partial aspect of a complex reality, where individuals cannot be distinguished exclusively between producers and consumers, since they are first and foremost men". A similar thesis is supported by A Barba, Consumo e sviluppo della persona (Giappichelli 2017) 294, who, on this very point, expressly declares that "the transformation of the social and economic category of consumer into a legal category that is characterised by the structural relationship between consumption, weakness and protection, is included and absorbed in the situational connotation of protection: the weakness of the consumer in fact only comes to the fore in the situations typified by the legislator. The natural person is protected not by reason of the state of inferiority with respect to the producer or distributor of goods or services that he chooses to - or is induced to - consume, but by reason of the diminished or compromised power of negotiating self-determination that is determined in particular relational market situations. The situational connotation is derived precisely from the need for normative typification, i.e. a selective strategy of the deservingness of protection of the relational situations that make up the internal market; if the need for protection were immanent to the person, who, moreover, can only live by consuming, typification would not be necessary". P Stanzione (ed), *La tutela del consumatore tra liberismo e solidarismo* (ESI 1999) 307. "Therefore, it is useful to separate the rules defending the consumer as a market protagonist, from the provisions guaranteeing the person and/or the citizen [...] In reality, the status of person and citizen have an absolute value; on the contrary, the consumer is a condition linked to the concrete circumstances and to the actual modalities of contracting. Different is the consumer in the financial market, where there are special guarantees and to which some persons cannot even gain access. [...] The consumer is not a status, but a contractual position to be identified and ascertained from time to time; the subject is now a consumer, now a producer or entrepreneur in a condition of economic or technological dependence".

[120] On this issue, however, see F Denozza, 'Fallimenti del mercato: i limiti della giustizia mercantile e la vuota nozione di "parte debole"' (2013) 1 Orizzonti del diritto commerciale 3. According to the authors' view, the consumer is not always weak, but weakness derives from the compromised ability to self-determine in consumption, thus, it is not a pre-existed status, but only exists when the ability to self-determine is compromised, in which case, it would seem, one could speak of a weak consumer.

reference should be made to the 'fractionated' consumer[121], increasingly mentioned because of the activities with which he or she is connected.

This is because the generic concept of consumer usually refers to the person who participates in one or more of the phases of the consumption cycle (which can be considered, at least in general terms, the persuasion phase, the purchase phase and the fruition phase).

This concept, however, does not specify which behaviour distinguishes the consumer. This has long led to the subject being regulated on the assumption that consumer behaviour is the result of a choice made by a rational agent.

More recently, on the other hand, the theory based on cognitive psychology and behavioural economics[122] has been widely affirmed, according to which the image of the consumer as '*homo oeconomicus*' "does not automatically provide a causal explanation for consumer behaviour, nor is it a tool for predicting such behaviour, but is a regulatory ideal that is only efficient if it is actually followed by the recipients, otherwise consumer behaviour is irrational"[123]. The cognitive bias[124] becomes the new critical issue, on which the legislator tends to focus its attention.

Nevertheless, a common and unambiguous notion of a digital vulnerable consumer has not been proposed, as it is a particularly broad and ever-changing concept.

Concretely, the digital consumer has been more generically qualified as the consumer who concludes contracts by digital means and/or who purchases (or accesses) goods, services or content of a digital nature[125]. This consumer may be qualified as that subject placed in a condition of vulnerability with respect to the most dominant platforms, amplified and conditioned by external factors created by the modern digital ecosystem.

Indeed, while there is no agreement on a single definition of vulnerable consumers, the concept of consumer vulnerability that emerges from the academic literature, including sociology, marketing and law is wider than the one defined in the UCPD.

---

[121] Please see F Bassan, M Rabitti and L Rossi Carleo, 'Consumerism 2019 – Dodicesimo rapporto annuale – Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione?' (2022), Il consumatore vulnerabile tra innovazione e diritti fondamentali 8 https://www.consumersforum.it/ricerche.html accessed 25 October 2024.

[122] Cf L Herzog, P Kellmeyer and V Wild, 'Introduction to the Special Issue Digital Behavioral Technology, Vulnerability and Justice: Towards an Integrated Approach' (2022) 80(1) Review of Social Economy 807; P Kellmeyer, 'Digital Vulnerability: A New Challenge in the Age of Superconvergent Technologies' (2019) 12(1/2) Bioethica Forum 60.

[123] Bassan, Rabitti and Rossi Carleo (n 121).

[124] ibid.

[125] See, N Helberger and others, 'EU Consumer Protection 2.0. Structural Asymmetries in Digital Consumer Markets' (BEUC 2021) 1 <https://www.beuc.eu/publications/beuc-x-2021 018_eu_consumer_protection.0_0.pdf> accessed 25 October 2024 i quali pongono il seguente interrogativo: "what protection can the concept of consumer vulnerability offer the digital consumer, is the distinction between the average and the digital consumer still fit for the digital age, and if not, do we need a new understanding of 'digital vulnerability' and what would its elements be?". Tuttavia, tali interrogativi non presentano una risposta univoca. See also European Parliament, 'Vulnerable Consumers' (2021) 2, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690619/EPRS_BRI(2021)690619_EN.pdf> accessed 25 October 2024.

Obviously, even this perspective is not self-sufficient, but it contributes to weakening the systematic value of the traditional notion of the consumer[126] as a natural person acting for purposes unrelated to the professional activity carried out and leads, rather, to distinguishing the activity of the offline consumer from the online consumer[127] (to whom, moreover, a central and dynamic role should be recognised).

In this respect, the communication on the New Deal turned the spotlight on the digital consumer (the consumer-user who buys goods and services on online marketplaces).

This is seen as a more evolved consumer who, faced with the way digital platforms operate, may find himself disarmed and lacking clear and sufficient tools to protect his position in the same way as in traditional markets.

Despite the fact that the '*Omnibus*' Directive aims to amend the UCTD, it is pointed out that "the changes made to the directive did not specifically concern consumers accessing goods and services of a digital nature, nor those accessing goods and services of a physical nature by digital means (for this reason, there is no shortage of calls for a more significant update of the UCTD that takes into account the peculiarities of the digital economy)"[128].

4 Final Remarks

The analysis outlined so far leads to some fundamental considerations.

- The first one is related to the defining aspects of the concept of vulnerability as well as the contextual proposition of the problems connected to the phenomenon.

At this point, it is possible to outline some reconstructive hypotheses considering the figure of the vulnerable digital consumer and the possibility of innovating the discipline and the protection tools for these users in case of unfair digitalised clauses.

It is essential, then, to start from an assumption: the contemporary world, in regulatory silence, requires that the protection of the most vulnerable individual be raised beyond

[126] L Ammannati, 'Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?' (2019) 1 Rivista trimestrale di diritto dell'economia 8, which specifies that with the new consumer provisions, the European Commission intended to strengthen digital consumer protection policies. Indeed, the new package of measures is largely tailored to the future challenges for consumer policy in a rapidly changing economic and technological environment. It is therefore considered that the DSM Strategy can be interpreted as the framework for EU actions to modernise consumer protection instruments and adapt them to the digital consumer.

[127] See R Petti, 'La tutela del consumatore nel settore delle comunicazioni elettroniche' Consumerism 2019 – Dodicesimo rapporto annuale – Dal codice del consumo al Digital Service Act. Quella dal consumatore al cittadino digitale è vera evoluzione? Università degli Studi Roma Tre (2019) 42 <https://www.consumersforum.it/files/eventi/2019/CF_Consumerism-2019.pdf> accessed 25 October 2024; P Occhiuzzi, 'Trasporti e vulnerabilità: i diritti dei consumatori alla prova dell'evoluzione digitale e della transizione sostenibile' - Consumerism 2022 – Quindicesimo Rapporto Annuale – Il consumatore vulnerabile tra innovazione e diritti fondamentali (2022) Università degli Studi Roma Tre 29 https://www.consumersforum.it/ricerche.html accessed 25 October 2024.

[128] Loos and Luzak (n 92).

traditional assumptions; this is because not all individuals benefit equally from the changed technological and market environment.

The vulnerable digital consumer, therefore, is understood as that subject placed in a condition of vulnerability with respect to the most dominant platforms, which is exacerbated, moreover, by external factors created by the modern digital ecosystem.

For these reasons, the article has led to consider the vulnerable digital consumer as belonging to a dynamic social category, evolved in a particular context (the digital one), influenced by a combination of old and new factors and which is identified in those particularly vulnerable individuals who risk not having access to essential services, being exposed to forms of manipulation that violate fundamental rights and being discriminated.

This is a consumer endowed with a mainly situational vulnerability, which arises as a result of particular situations or contexts, occurring several elements capable of determining or aggravating such forms of vulnerability[129]. This condition of vulnerability, therefore, requires different protection, which ensures the function of the right to concretely protect the new needs of consumers[130].

Given an answer to the first question, it is necessary to move on to the second question concerning the probable protections that the renewed value framework of domestic and supranational law could grant to the category thus delineated.

On this point, the concept of 'consumer empowerment' identified as that set of processes capable of increasing the level of information and knowledge, bargaining power as well as the ability to communicate with the economic operator[131] deserves special consideration.

However, legal protection is still segmented, as the institutions have not prepared a plan that favours uniformity of protections and their instruments.

It is interesting to note that in some jurisdictions it is possible to identify a remedy specifically applicable to the situation described.

In the Spanish legal system, in fact, one of the first to respond to the objectives set by the 2020-2025 Agenda[132], a specific regulation on vulnerability has been introduced, which is extended to new categories, including the digital consumer.

The aim of the legislation, by strengthening consumer protection, is to promote and strengthen digital literacy, transparency, contracts, the right of withdrawal and the ability of users to access[133]. These issues are no longer related to the traditional categories of

[129] Sandulli (n 51) 194.
[130] ibid 197.
[131] Occhiuzzi (n 127).
[132] Cf European Commission, 'New Consumer Agenda – Strengthening consumer resilience for sustainable recovery' (2020) <https://commission.europa.eu/document/ac73e684-1e7f-4d36-a048-8f8a0b874448_en?prefLang=it> accessed 25 October 2024.
[133] MJ Marín López, 'El Concepto de Consumidor Vulnerable en el Texto Refundido dela Ley General para la Defensa de los Consumidores y Usuarios' (2021) 37 Revista CESCO De Derecho De Consumo 112; R Barceló Compte, 'El Consumidor

the most vulnerable, but rather to those with limited financial means. In these hypotheses, the Authority is recognised as having the power to undertake a series of actions capable of offering these categories of consumers a system of guarantees, safeguards and protection, extending these instruments and its intervention also to the digital environment. Hence the urgency of incorporating the notion of vulnerable consumer into the Spanish legal system in the single text of Ley 4/2022[134], so as to avoid loopholes in the previous legislation that would lead to an obvious lack of protection for this category of consumers. The law in question, going beyond the traditional allusion to the economic situation of consumers in determining their situation of vulnerability, not only identifies a notion of vulnerable consumer but also provides a series of remedies for the same.

Only the practical application of these provisions will be decisive in understanding their real impact in the different systems.

From the wording of the legislation, it is clear, therefore, how the Spanish legislature wished to introduce a supplementary discipline to the instruments of consumer protection that were vulnerable, especially with regard to information obligations.

The solution adopted by this framework assumes that concrete measures, may be identified in self-regulatory initiatives, in the form of codes of conduct, or in the use of standardised practices that enable institutions and organisations to identify specific groups of vulnerable people and to develop appropriate inclusive and protective practices.

It is necessary to ensure that markets, which are oriented and controlled by law, are seen as a resource and not as a possible threat to the protection of the vulnerable (digital consumer).

The hope, at this point, is that the intervention to define the vulnerable consumer-user and identify specific forms of protection will not remain isolated.

- The second consideration regards standardised contracts and the need for the identification of 'new' unfair terms.

The evaluation of the current context has allowed the reflection on the different issues that the digital, or rather, algorithmic society raises with regard to consumer-user protection; in effect, the regulatory framework described above is causing some mystification, particularly because of the risks of the legal uncertainty[135].

As a natural consequence of this reasoning, in fact, on the one hand it was possible to examine the considerable European initiatives and the most recent proposals for a better

Especialmente Vulnerable: de la Protección Class-Based a la Protección State-Based' (2022) 16 Actualidad Jurìdica Iberoamericana 626.

[134] Cf Ley 4/2022, 25 febbraio, BOE-A-2022-3198, in Boletìn Oficial del Estado, Artículo primero: Modificación del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-3198> accessed 25 October 2024.

[135] Cf G Sartor, 'Algorithmic Price Discrimination and Consumer Protection – A Digital Arms Race?' [2022] Technology and Regulation 41.

and more efficient DSM; on the other hand, attention was also paid to the role of the consumer, today understood as a digital user placed in a vulnerable condition, as well as to the application and necessary integration of the discipline of unfair terms in the platform economy, due to the emergence of increasingly digitalised standard contractual terms. Indeed, online platforms provide regulatory infrastructures that can be combined with algorithmic data analysis and automated technologies, thus enabling regulatory learning processes that work faster and more effectively than traditional legal instruments such as default rules and bilateral standard terms. Future regulation of standard terms should take advantage of this superior knowledge without underestimating the risks of digitised terms. The current UCTD regulatory instruments (transparency requirements, fairness review and opt-out restrictions) are increasingly inadequate to deal with these new challenges of digitised terms because they are adapted to standard terms in bilateral agreements. Although these findings may also support the European Commission's current digital fitness check, they underline the fundamental need for legal reform. An architecture of choice for digital contracts requires a completely new regulatory strategy.

To strike the right balance between protecting private autonomy and avoiding significant imbalances, the regulatory objective should be to ensure the impartiality of platforms by focusing on the structural conditions of their regulation rather than trying to assess the substantive content of their terms.

Notably, the investigation of such terms in the digital world encounters specific challenges, requiring new methodologies and protection tools[136], a fact that underlines the uniqueness of the digital environment compared to traditional contexts. On this point, it has been noted that simply changing the UCTD may not be sufficient, and that a different approach is needed. For this reason, two avenues were envisaged: on the one hand, the creation of a new, updated blacklist incorporating the clauses considered unfair for digital (which must be implemented repeatedly) and, on the other hand, the development of European Commission guidelines for assessing fairness in the context of the UCTD. These criteria could act in synergy to provide a robust and up-to-date regulatory framework to ensure fairer and more transparent contractual conditions for consumers in the digital environment[137] (online contractual imbalance would not be corrected simply by amending the directive on unfair terms in contracts, but also by strengthening the effectiveness of the framework of the UCTD through its simultaneous revision).

[136] 'Introducing EnfTech: A technological approach to consumer law enforcement' (Geneva, UNCTAD 2022) <https://unctad.org/meeting/introducingenftech-technological-approach-consumer-law-enforcement> accessed 25 October 2024.
[137] Gardiner (n 97).

Helena Verhuyck[*]

SPECIAL SECTION

THE ACHILLES HEEL OF THE PLATFORM-TO-BUSINESS REGULATION: NO UNFAIR TERM PROTECTION FOR PLATFORM WORKERS?

Abstract

The rise of digital labour platforms has significantly altered traditional employment dynamics, creating diverse working conditions and employment relationships. Platforms create an ecosystem in which they prescribe standard contract rules, allowing more actors to efficiently find and connect with each other. In order for both consumers and platform workers to use the platform and connect, they need to accept the pre-dictated contractual terms by accepting the terms and conditions. Even though these standard contracts contribute to efficiency and reduce bargaining costs, these potential advantages can be hollowed out if there is a complete lack of actual bargaining power, which may result in unfair contract terms.

This article examines the power imbalances and unfair terms that can often be perceived in platform work contracts, particularly focusing on how these imbalances manifest in platform's terms and conditions. This article highlights the contractual vulnerabilities of platform workers by analysing the terms of five major platforms, namely Deliveroo, Uber, Upwork, Clickworker, and Amazon Mechanical Turk. It further scrutinises the effectiveness of existing legal frameworks in addressing these imbalances from a platform worker point of view, focusing on the Unfair Contract Terms Directive (UCTD) and the Platform-to-Business (P2B) Regulation while briefly touching on the new Platform Work Directive.

The UCTD provides protection against unfair terms that have not been individually negotiated, though limits this protection to consumers captured in business-to-consumer relationships. This limitation renders the UCTD inapplicable to most platform workers, as the majority are self-employed and therefore fall outside the consumer protection realm.

In the P2B Regulation, requirements for the clarity, content and modification of the terms are imposed. The question is, however, how effective this instrument is for remedying the contractual power balance and what impact this Regulation has specifically on labour platforms. While the European Commission clearly intended all online platforms to fall within the Regulation's scope, it is not entirely clear if and to what extent the Regulation applies to labour platforms. This article therefore analyses whether platform workers can be considered "business users" and whether labour platforms can be considered "online intermediation

[*] Helena Verhuyck is a PhD researcher and teaching assistant at the University of Antwerp, lecturing labour law and researching the power dynamics in digital labour platforms with a focus on platform workers. She holds an LL.M from the University of Connecticut and a master in law from the University of Antwerp. Her research is funded by FWO under the project number G040422N.

 DOI 10.13135/2785-7867/11331

service providers". In this analysis, significant gaps are revealed that consequently leave platform workers inadequately protected. Furthermore, an apparent discrepancy in conception between the Commission and the Court of Justice is discovered, since the former seems to believe the Regulation applies to Uber and other transportation platforms while the latter has ruled in its *Elite Spain* judgment that Uber is to be excluded from the information society service definition. A (potentially unintended) consequence of this judgment is the fact that Uber has now been seemingly precluded from the Regulation's scope, meaning that Uber drivers cannot benefit from its protective provisions. Further, the analysis of the terms and conditions showcases which of the five platforms are in compliance with the P2B Regulation and highlights substantial non-compliance, even multiple years post-implementation.
The conclusion emphasises the need for a holistic legislative approach to protect all platform actors and ensure fairness and transparency in platform relationships. It advocates for a unified framework that promotes compliance through effective public enforcement mechanisms.

JEL CLASSIFICATION: K2

SUMMARY

1 Introduction

Over the last decade, the world has witnessed a rapid emergence of digital labour platforms engaging platform workers to provide services. Some forms of platform work are physically visible in our society, for instance Deliveroo delivery couriers or Uber drivers, while other forms of platform work happen purely online, such as AI training or the performance of microtasks. Several factors may explain the proliferation of platform work, including technological, economic, and sociocultural influences. However, there is a general trend towards the precarisation of work, driven by the need for easily accessible job opportunities among vulnerable labour profiles, such as people with migration backgrounds - a trend that labour platforms often take advantage of.[1] Especially the structural vulnerability of *inter alia* low-wage migrant workers due to their regular

[1] Niels van Doorn, Fabian Ferrari and Mark Graham, 'Migration and Migrant Labour in the Gig Economy: An Intervention' (2023) 37 Work, Employment and Society 1099, 1101.

exclusion from standard employment relations, makes platform labour and its low thresholds particularly appealing.[2]

These platforms have reshaped the traditional notions of employment, creating a diverse array of working conditions and employment relations. Eurofound defines platform work as "a form of employment that uses an online platform to enable organisations or individuals (workers) to access other organisations or individuals (clients) to solve problems or to provide services in exchange for payment."[3] Platform work is therefore a broad term covering a wide range of both physical and online work forms, each with highly individualised working conditions, employment relations and policies.[4]

Due to the important differences within platform work, there is no universal work classification or set of rules that can be implemented to regulate the platform economy as a whole. Despite this diversity, one feature that almost all digital labour platforms share, is the fact that they classify platform workers as self-employed rather than as employees. In the EU, it is estimated there will be 45 million platform workers by 2025, 93% of which are – *contractually* - classified as self-employed, often involuntary.[5] *Legally*, however, it is disputed whether these platform workers are genuinely self-employed or whether this is a form of false self-employment. Numerous national courts have been confronted with the complicated task of qualifying platform workers, with varying legal outcomes that consequently cause legal uncertainty.[6] Many platforms impose this self-employed status on their platform workers to avoid steep employee costs and the related employer responsibilities.[7] Labour laws generally protect employees against unfair terms in their contracts, such as *inter alia* unjustified or arbitrary terminations or unilateral variation clauses. However, since most platform workers are classified as self-employed, the majority is excluded from the protective labour law scope and therefore unable to enjoy the same safety net as employees.[8]

In the platform economy, as opposed to standard employment, it is not unusual to witness sudden changes in the terms and conditions or seemingly arbitrary dismissals of platform workers. This can be explained by the fact that platform workers are usually not employed by individual labour contracts but rather merely need to agree to the pre-

[2] ibid 1101.
[3] Eurofound, 'Employment and Working Conditions of Selected Types of Platform Work' (Publications Office of the European Union, Luxembourg 2018) 9.
[4] James Duggan and others, 'Algorithmic Management and App-Work in the Gig Economy: A Research Agenda for Employment Relations and HRM' (2020) 30 Human Resource Management Journal 114, 116.
[5] European Council and Council of the EU, *Spotlight on digital platform workers in the EU*, <https://www.consilium.europa.eu/en/infographics/digital-platform-workers/> accessed 12 October 2023.
[6] See for example the Dutch Supreme Court ruling that requalified Deliveroo riders as employees while the Belgian court (in the first instance) contrastingly ruled that they should remain classified as self-employed; Hoge Raad 24 maart 2023, ECLI:NL:HR:2023:443 and Arbrb. Brussel (Fr.) (25e k.) nr. 19/5070/A, 8 December 2021, *JLMB* 2022, afl. 9, 390.
[7] European Commission, '*Q&A: Improving Working Conditions in Platform Work*' <https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6606> accessed 9 March 2023.
[8] World Economic Forum, '*The Promise of Platform Work: Understanding the Ecosystem*' (White Paper REF 10122019 12, 2020) <https://www.eurofound.europa.eu/et/data/platform-economy/records/the-promise-of-platform-work-understanding-the-ecosystem-0> accessed 28 February 2023.

dictated contractual terms by accepting the platform's terms and conditions. Most platform workers do not have the ability to bargain about these terms before entering into a contractual arrangement with the platform while traditionally, self-employed workers are able to negotiate their own terms and conditions. All activities that take place within the platform ecosystem are thus subject to the contractual regulation that is unilaterally provided by the platform through its terms and conditions.[9] This raises concerns about the consequent power imbalance between the platform and its platform workers and puts the latter at risk of unfair terms.

Given that this power imbalance is often encapsulated within the platforms' architecture through its terms and conditions, I have conducted empirical research of five platforms' terms and conditions in order to exemplify the apparent contractual power imbalance and unfair terms. The following five platforms were chosen for analysis: Deliveroo, Uber, Upwork, Clickworker and Amazon Mechanical Turk (hereafter: AMT). These platforms represent a diverse range of labour platforms of both U.S. and European origin and include both platforms with location-based and online platform work.[10] The difference in geographical origin allows for a potential uncovering of cultural differences embedded in the terms and conditions. Further, the legal approach can vary based on whether platform work is location-based and bound by national laws or conducted purely online, transcending national borders.

As labour law is considered a *lex specialis* of general contract law, this article will verify whether contract law might be successful in remedying this apparent power imbalance in section 2. There are two main European instruments that protect against unfair terms. Firstly, the Unfair Contract Terms Directive (UCTD) protects against non-negotiated terms if they cause a significant imbalance in the parties' rights and obligations. In section 3, this article first examines whether, and to what extent, platform workers can rely on this Directive for protection against unfair terms. Secondly, the Platform-to-Business Regulation promotes fairness and transparency specifically for platform business users and implements a set of requirements for platforms' terms and conditions. Even though the European Commission envisioned to capture the *entire* platform economy, this article uncovers some significant gaps in application and protection in the context of labour platforms in section 4. Within this section, the article evaluates the P2B Regulation three years post-implementation and assesses whether the five chosen platforms are in compliance with its requirements. Lastly, section 5 provides a brief overview of the current legal landscape of unfair term protection for platform workers and in section 6, the conclusion follows.

[9] Silvia Martinelli, 'The Vulnerable Business User: The Asymmetric Relationship between the Business User and the Platform' (2020) 2 European Journal of Privacy Law & Technologies 84.

[10] Uber (U.S.) and Deliveroo (U.K.) are platforms that offer location-based services, respectively transportation and food delivery services, whereas Upwork (U.S.), Clickworker (Germany) and Amazon Mechanical Turk (U.S.) are platforms that have a global reach with purely online services, mostly consisting of online freelancing and the crowdsourcing of various microtasks such as data entry and online surveys.

2 Contract law remedies to a power imbalance

Traditionally, there are various legal instruments to remedy a concentration of power and the resulting power imbalance. Generally, labour law, competition law and contract law have all developed some mechanisms to regulate situations where information deficits and unequal bargaining positions reduce the weaker party's freedom.[11] As labour law is mostly inapplicable to self-employed platform workers and is considered a *lex specialis* of general contract law, the scope of this article is limited to contract law solutions that could remedy the contractual power imbalance and the related risks of unfair terms.

There is a spectrum of possible legal responses to new disruptions: on one end is the option of extending the reach of existing legal rules and principles to the specific challenges brought about by the disruption, possibly with minor adjustments.[12] On the other end is the option to start from the specific challenges and develop new and tailored legal solutions to effectively deal with those. In this section, I will discuss and evaluate both ends of this legal spectrum: firstly, I will focus on current legal remedies in contract law, and more specifically on the Unfair Contract Terms Directive (UCTD) to assess whether those provisions can be used to remedy the power imbalance in labour platforms. Secondly, in section 4, I will look at a recent and more specifically tailored European intervention, namely the Platform-to-Business Regulation 2019/1150 and assess whether and to what extent it could resolve the existing challenges.

2.1 General contract law in a platform context

Platforms provide the architecture that shapes how supply and demand are matched and how a vast number of individual contracts are formed.[13] Digital technologies and algorithms are used to find, select and connect potential contractual counterparties. This digitalisation has been considered by the legislators, mostly from the demand side from the consumers' perspective. However, challenges also emerge on the supply side, concerning the supply of services by platform workers through the use of digital platforms.[14]

Classic contract law is based on the conception of a contract as a static, bilateral consensus, which sets the conditions for all future transactions.[15] In traditional contracts, a revision of the contract happens through a mutual renegotiation. Platform contracts, on the contrary, get perpetually revised and changed through the unilateral updating of the

[11] Ton Hartlief, 'Freedom and Protection in Contemporary Contract Law' (2004) 27 Journal of Consumer Policy 253, 258.
[12] Christian Twigg-Flesner, 'The EU's Proposals for Regulating B2B Relationships on Online Platforms – Transparency, Fairness and Beyond' (2018) 7 Journal of European Consumer and Markets Law 4.
[13] Christoph Busch and others, 'The Rise of the Platform Economy. A New Challenge for EU Consumer Law?' (2016) 5 (1) Journal of European Consumer and Market Law 3.
[14] Paola Iamiceli, 'Online Platforms and the Digital Turn in EU Contract Law: Unfair Practices, Transparency and the (Pierced) Veil of Digital Immunity' (2019) 15 European Review of Contract Law 392, 397.
[15] Ole Hansen and Hamish Ritchie, 'Unilateral Variation Clauses in Professional Platform-User Agreements' (2023) 8 CEPRI Studies on Private Governance.

platform's terms and conditions. All five investigated platforms had 'unilateral variation clauses' stating that the terms or the agreement could be changed or revised at any time. Some platforms such as Uber and Clickworker incorporated that the business users would be informed in advance and had the right to terminate their account in case they did not agree. Upwork's terms stated that there would be a 30 days' notice period though only for "substantial changes". Other platforms like AMT stated that they may modify, suspend or discontinue the agreement at any time and without notice, while continued use of the site constitutes the worker's acceptance of the modified terms. These examples demonstrate that the practice of unilaterally modifying the terms to an agreement is widespread in the platform economy. These unilateral variation clauses are therefore a borderline feature of contract law, undermining the fundamental premise in contract law that requires a reciprocal consensus.

2.2 Unfair Contract Terms in Adhesion Contracts

Contracts of adhesion, also called *standard form contracts*, are a welfare-enhancing feature of modern commercial life. To make commerce more efficient, templates where all terms and conditions are already prepared by one party - 'adhesion contracts' - were introduced.[16] These contracts of adhesion are offered on a take-it-or-leave-it basis to the weaker party since the economic power of the business prohibits any meaningful negotiation of the pre-dictated terms.[17] Both for firms and consumers, the uniformity of such contracts could be a benefit, reducing the transaction costs and energy that go into reading, understanding and negotiating every term.[18] Regardless of the benefits, the party 'adhering' to the contract (*in casu*, platform workers and also consumers) is always in a position of inferiority towards the stipulant and is consequently considered vulnerable and in need of protection, regardless of their quality.

However efficient adhesion contracts may be, there is always a risk that the platform's terms will favour its own position given that platform workers find it difficult, if not impossible, to (attempt to) negotiate more balanced terms.[19] Thus, platforms may impose unfair terms to the adherent, either because the latter consents without knowing the contractual clauses (for example when ticking a box without actually reading the contract) or even while knowing the contractual terms but accepting because they felt constrained by the need to conclude the contract.[20] In today's global trade, adhesion contracts are a

[16] Dr Rukhsana Shaheen Waraich, Muhammad Fayaz and Hayyan Zahid, 'Consent Theory and Adhesion Contract: A Critical Analysis of Contemporary Global Business Practices' (2022) 14 Business & Economic Review 73, 74.
[17] Martijn W Hesselink, 'Unfair Terms in Contracts between Businesses' in J Stuyck and R Schulze (eds), *Towards a European contract law* (2011) 133.
[18] Carmen Tamara Ungureanu, 'Cyberspace, The Final Frontier? Concluding and Performing Agreements. Unfair Terms in B2B in Adhesion Contracts' (2021) 67 Analele Stiintifice Ale Universitatii Alexandru Ioan Cuza Din Iasi Stiinte Juridice 9, 10.
[19] Twigg-Flesner (n 12) 3.
[20] Ungureanu (n 18) 12.

useful tool to form agreements in a more expeditious way. However, the power balance needs to be restored to ensure a predictable market that is characterised by fair trade and fair contracts.[21]

3 The Unfair Contract Terms Directive (UCTD)

3.1 European rules for unfair terms

As far as legislative intervention goes, the European Union has harmonised rules in relation to unfair contractual terms in the Unfair Contract Terms Directive ("UCTD").[22] The "unfair term" notion is defined in this Directive as "a contractual term which has not been individually negotiated, if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."[23] The UCTD contains an Annex in which it exemplifies terms that can be regarded as "unfair", such as *inter alia* terms which enable the supplier to alter the terms of the contract unilaterally without a valid reason specified in the contract (Annex (1)(j)), terms which enable the supplier to terminate the contract without reasonable notice except where there are serious grounds for doing so (Annex (1)(g)) and terms which authorise the supplier to dissolve the contract on a discretionary basis where the same facility is not granted to the consumer (Annex (1)(f)).

As previously discussed, in almost all cases of platform-to-worker as well as platform-to-consumer contracts, the terms and conditions are unilaterally drafted by the platform in advance. When assessing terms and conditions of digital labour platforms, it can therefore be assumed that they have not been individually negotiated and potentially cause a significant imbalance in the parties' rights and obligations. Whether the UCTD effectively applies to platform-to-worker contracts and whether platform workers can consequently benefit from its unfair term protection, will be discussed below.

3.2 Scope of protection: platform workers excluded?

The *ratio legis* of this judicial review of contract terms provided in the UCTD is a form of weaker party protection that is meant to compensate for unequal bargaining, information asymmetries and to protect against abuse of power in one-sided standard contracts.[24] This *ratio legis* is well entrenched in European law as the UCTD explicitly refers to this reason as the justification for the control of unfair terms. Moreover, since

[21] ibid 22.
[22] Council Directive (EEC) 93/13/EEC on unfair terms in consumer contracts [1993] OJ L 95, 29, 34.
[23] ibid 3.
[24] Hesselink (n 17) 133.

the *Océano* judgment[25], the Court of Justice of the European Union has consistently explained the rationale of the UCTD in terms of weak or non-existent bargaining power. Even though this weak bargaining power is just as pervasively present in B2B contracting as it is in B2C contracting, the scope of the UCTD is limited to B2C contracts, making consumers the sole beneficiaries of its provisions.[26] As the vast majority of workers are self-employed (*supra*), the UCTD and its unfair contract term protection are inconsequential for most platform workers.

This seemingly makes sense as traditionally, self-employed entrepreneurs are able to negotiate their own terms and conditions in B2B contracts. However, in the current platform economy, many regular individuals have had no other choice than to take the (micro)entrepreneur route to be able to perform flexible platform work. Most labour platforms use adhesion contracts that all users need to accept in order to use the application. This puts platform workers in a weak position without bargaining power. For consumers, through legislative intervention and many consumer protection laws, the balance in platform-to-consumer contracts has mostly been restored throughout Europe. For platform workers, however, the power imbalance vis-à-vis the platform and unfair contract terms have only recently become a pressing matter. The power dynamics within platforms have made clear that that line of reasoning and the rebalancing of contractual power is and should not be constrained to consumer contracts.

Nowadays, standard contract terms play an important part not only in consumer contracts, but also in trader contracts and it should therefore be borne in mind that many of the weaker-party-protection arguments apply equally to business contracts.[27] Being in a weak bargaining position vis-à-vis the platform and having to agree to terms and one-sided contracts drawn up in advance is not a condition in which only consumers find themselves. In the Explanatory Memorandum of the UCTD, it can be read that some envisaged a wider application that should not be confined to consumer protection. However, given the difficulties which would be involved in obtaining acceptance of the common rules applicable to *all* contracts, the Commission decided that the Directive should be confined to consumer contracts.[28] The issue of unfair terms in B2B contracts has nonetheless been on the agenda of the European legislator, who in 2011 discussed a proposal from a European Commission expert group to evaluate whether this Directive could be extended to B2B contracts.[29] However, this proposal was withdrawn in 2014. Even though an extension of the UCTD to B2B contracts definitely would have benefited self-employed platform workers, there is an important caveat in Article 4(2) of the UCTD,

[25] *Océano Grupo Editorial SA v Roció Murciano Quintero (C-240/98) and Salvat Editores SA v José M Sánchez Alcón Prades (C-241/98), José Luis Copano Badillo (C-242/98), Mohammed Berroane (C-243/98) and Emilio Viñas Feliú (C-244/98)* [2000] CJEU Joined cases C-240/98 to C-244/98.
[26] Hesselink (n 17) 134.
[27] Paolisa Nebbia, *Unfair Contract Terms in European Law* (Hart Publishing 2007) 86.
[28] Explanatory Memorandum to the 1990 Proposal, COM (90) 322 final 12.
[29] Commission Expert Group on European Contract Law, *Feasibility study for a future instrument in European Contract Law*, 3 May 2011.

which states that the assessment of the unfair nature of the terms shall not relate to the adequacy of the price and remuneration in so far as these terms are in plain intelligible language. Consequently, the widespread issue of the unfairly low wages of platform workers would in any case have fallen outside the scope of the UCTD.[30]

3.2.1 Peer platform workers

Nowadays, offering goods and services through platforms is no longer the exclusive domain of professional actors. In the platform economy, there has been an expanding peer platform market where non-professionals (so-called peers) offer all sorts of services to consumers.[31] Examples include BlaBlaCar, where individuals list empty seats in their car for long-distance rides or in some cases Airbnb, where regular individuals list spare rooms or apartments. These so-called 'peer providers' (*in casu*, peer platform workers) refer to the private individuals supplying the goods or services to 'peer consumers' who purchase, acquire or rent those goods and services.[32] These types of peer-to-peer platform markets pose all sorts of challenges for the existing rules and principles in consumer law, as it can be difficult to apply consumer protection frameworks such as the UCTD to (platform) business models that blur the boundaries between consumers and businesses.[33] The EU consumer *acquis*, as well as national consumer protection laws, operate under a dual system that applies exclusively to business-to-consumer transactions (*supra*). Consequently, any non-business-to-consumer transactions such as peer-to-peer transactions are excluded from this *acquis* as both the peer provider and the peer consumers are considered consumers.[34] However, while these peer platform workers provide services to consumers, they simultaneously appear to be in a consumer relationship with the platform. Therefore, when peers use platforms to provide services and insofar as these peer providers act for purposes outside their trade or profession[35] and do not demonstrate the durability to be considered enterprises, this platform-to-peer-provider relationship could mirror that of a business-to-consumer relationship. Consequently, the UCTD would extend to these peer platform workers, including them in the consumer protection framework for unfair terms and conditions.

[30] In relation to the generally low levels of remuneration for platform workers, the Minimum Wage Directive 2022/2041 could play a role as this instrument applies to "workers", but this falls outside the scope of this article.
[31] Helberger Natali, 'Protecting Consumers in Peer Platform Markets' (OECD 2016).
[32] ibid 7.
[33] ibid 6.
[34] Directorate-General for Justice and Consumers 'Exploratory Study of Consumer Issues in Peer-to-Peer Platform Markets' Annex 5 (2017) 41.
[35] In the Consumer Rights Directive 93/13/EEC, article 2 defines a consumer as 'any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession'.

3.2.2 National expansions of unfair contract term protection

Since the UCTD provides only a minimum harmonisation for unfair contract terms in consumer contracts, there are still differences between Member States in relation to the scope of protection. In the absence of a more specific categorisation of unfair contract terms, protection against unfair contract terms varies across Member States, as each country can choose whether or not to expand the protection offered by the UCTD to B2B contracts. As of today, many Member States have some sort of review of unfair terms in B2B contracts based on general contract law, though with varying scopes of protection. Examples of national legislation on this matter include the Belgian Code of Economic Law[36], the French Civil Code[37], the German Civil Code[38], the Scandinavian Contract Act[39] and the Unfair Contract Terms Act in the UK[40]; all legislative initiatives that strive to remedy the power imbalance in B2B contracting. However, there is a rather diverse legal landscape among the different Member States in evaluation of unfairness in B2B relationships, with a wide and variated range of protection.[41] This national approach can lead to a fragmented and uncertain platform-landscape. A concern in using private law principles and *inter alia* contract law to remedy global issues like platformisation is the level where regulation takes place. While Member States can successfully adopt national legislation to remedy the power imbalance, this may only be a cornerstone of a platform's world-wide digital arena. Boilerplate laws that transcend state's territories could result in a more global (or at least European) change, redrawing platforms' arena.

3.3 Interim conclusion

Platforms continuously reshape how contracts are formed and revised through their digital frameworks, often unilaterally. This practice of unilaterally drafting and changing the contractual terms challenges traditional contract law principles which are based on a bilateral consensus and mutual (re)negotiations. The use of adhesion contracts in the platform economy further exacerbates the power imbalance, putting platform workers in a vulnerable position and at risk of unfair terms.

In the EU, there is protection against unfair terms in the UCTD. Despite its *ratio legis* being a form of weaker party protection, the sole weaker party able to benefit from its protection are consumers under B2C contracts. Consequently, only peer platform workers acting for purposes outside their trade or profession are considered to be in a consumer-like relationship with the platform and therefore able to benefit from the UCTD. This

[36] Article VI.91/1 and following Belgian Code of Economic Law.
[37] Article 1171 French Civil Code.
[38] Article § 305 and 307 (1) German Civil Code.
[39] Article 36 Scandinavian Contract Act.
[40] Hesselink (n 17) 142.
[41] For a more in-depth discussion of where exactly the differences lie in terms of protection and evaluation of unfairness, see Johannes Koenen, Ferdinand Pavel and Stefan Krüger, *Study on Contractual Relationships between Online Platforms and Their Professional Users - Final Report* (Publications Office 2018) chapter 2.1.1.

limitation renders the UCTD inapplicable to the majority platform workers, as they are self-employed and therefore outside the consumer protection realm.

Since the UCTD provides only a minimum harmonisation, multiple Member States have opted to expand the UCTD's scope to B2B contracts through their national legislation. As a result, self-employed platform workers are able to benefit from unfair term protection in these respective Member States, albeit not based on a supranational instrument. While national legislation can mitigate power imbalances, the global nature of digital platforms necessitates a more unified approach. In the next section, it is evaluated whether the Platform-to-Business Regulation is successful in providing platform workers with this unified framework for unfair term protection.

4 The Platform-to-Business-Regulation: restoring the power balance?

In 2019, the European legislator (re)affirmed the need to protect not only consumers but also entrepreneurs from unfair terms when contracting with other professionals in positions of power, particularly in the platform economy.[42] As part of the Digital Single Market Strategy review, the Commission announced that it would take concrete actions against unfair contracts and trading practices in platform-to-business relations.[43] As a result, Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the 'Platform-to-Business' or 'P2B' Regulation) has been adopted.[44] This Regulation recognises that digital platforms have a superior bargaining power and enter into contracts with (micro)entrepreneurs to use their services, "which enables them to in effect, behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union."[45] Platforms may abuse this stronger position in order to impose unfair terms and conditions upon platform workers. Thus, the P2B Regulation takes a contract- and transparency-based approach in which it seeks to address the identified issues through the contents of platform-to-business contracts.[46] The P2B Regulation aims to tackle these issues at a Union level and establish "a fair, predictable, sustainable and trusted online business environment, while maintaining and further encouraging an innovation-driven ecosystem around online platforms across the EU."[47]

[42] Ungureanu (n 18) 17.
[43] Caroline Cauffman, 'New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' (2019) 26 Maastricht Journal of European and Comparative Law 469, 474.
[44] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (hereinafter: P2B Regulation).
[45] ibid 2.
[46] Twigg-Flesner (n 12) 20.
[47] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services para 7.

4.1 Material scope: does the P2B Regulation apply to labour platforms and platform workers?

As the name of the Regulation suggests, the focus of the Platform-to-Business Regulation is the relationship between a platform, defined as an "online intermediation service provider" (hereafter 'OISP') and a "business user". But does the Regulation target all sorts of online platforms, including labour platforms, and all forms of business users, including platform workers? In the Recitals, some types of platforms such as e-commerce marketplaces, app stores and social media platforms are explicitly mentioned, but there is no specific mention of labour platforms.[48] In this chapter, it will be discussed whether and to what extent the P2B Regulation applies to digital labour platforms and consequently, to what extent platform workers can benefit from its provisions.

4.1.1 Are all platform workers "business users"?

Both of the targeted users have definitions in article 2 of the Regulation. The first relevant actor is the "business user", which is defined as "any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession."[49] The question is now whether platform workers can be considered as business users for the purposes of the Regulation. There are multiple concerns that complicate whether platform workers fall under this definition.

4.1.1.1 Impact of national caselaw requalifying platform workers as employees

Worldwide, the legal status of platform workers has been disputed with varying legal outcomes as a result. Firstly, a lot of national courts have been confronted with the difficult task of classifying platform workers according to their national labour laws. The classification of platform workers has been the subject of over 100 court decisions across the EU, the majority of which classified the platform workers as employees.[50] An important caveat here is that the majority of cases have been about location-bound platforms where the work is performed physically. Platform workers who perform the work purely online – often called 'crowdworkers' - have rarely been considered employees, since there is a lack of court cases on the matter. The first judgment on online platform work – in this case: crowdwork, a type of online platform work where tasks are distributed to a large, undefined group of individuals often referred to as "the crowd" - was issued at the end of 2020, in which the German Bundesarbeitsgericht rather

[48] Recital (11) P2B Regulation.
[49] Art 2(1) P2B Regulation.
[50] For an overview of European judgments, see Christina Hießl, 'Case Law on the Classification of Platform Workers: Cross-European Comparative Analysis and Tentative Conclusions' [2022] Forthcoming in Comparative Labour Law & Policy Journal <https://papers.ssrn.com/abstract=3839603> accessed 2 February 2024.

surprisingly classified the platform worker as an employee.[51] This demonstrates an inherent difference within the denominator of 'platform work' between location-bound platform work and online (crowd)work when it comes to the national practice of requalifying platform workers. As mentioned briefly in the introduction, platform work encompasses a diverse range of work arrangements with differences in terms of the nature of the work, the platform control, the level of autonomy, and the associated risks. However, a regulatory distinction based on the (physical or online) nature of the work cannot be similarly witnessed in European initiatives such as the P2B Regulation or Platform Work Directive (*infra*, section 5).

At first glance, national caselaw qualifying platform workers as employees and the P2B Regulation seem to be mutually exclusive: if platform workers were to be qualified as employees, they would be excluded from the scope of the P2B Regulation since employees cannot be business users. Furthermore, a duplication of protection would be unnecessary as employees would not usually need the protection of the P2B Regulation; national labour laws are better fit to their contractual role and would generally be more favourable than the transparency rights under the P2B Regulation.[52] Therefore, the P2B Regulation seemingly excludes platform workers who have been (re)classified as employees under national law. As a result, national caselaw can seemingly influence which platform workers the P2B Regulation applies to.

However, another interpretation is possible, namely that "business user" in the sense of the P2B Regulation should be interpreted autonomously and subsequently does not take into account national labour law or judgments.[53] Generally, protective EU laws tend to have autonomous interpretations, as is the case in most labour laws. For example, for the purpose of the Treaty on the Functioning of the EU (TFEU) and EU labour law regulations, the European Court of Justice (CJEU) has continuously held that the concept of a 'worker' or 'employee' must be determined autonomously, independently and regardless of the national law.[54] If we borrow from consumer law the relevant case law and literature on the term "trader"[55], it can be assumed that "business user" should be interpreted broadly in order to extend the circle of protected persons.[56] Thus, it can be argued that this principle can be transferred to the P2B Regulation as well, thereby making national labour laws and judgments inconsequential for the application of the Regulation. This would

[51] Bundesarbeitsgericht 1 December 2020, 9 AZR 102/20, ECLI:DE:BAG:2020:011220.U.9AZR102.20.0.
[52] Hans Schulte-Nölke, 'The Gig Economy and the European Platform-to-Business Regulation' (2020) 4 Pravovedenie 496, 503.
[53] ibid 504.
[54] See Case C-47/14, *Holterman Ferho Exploitatie BV ea v Friedrich Leopold Freiherr Spies von Büllesheim* [2015] ECLI:EU:C:2015:574, par. 36.; and more recently Case C-603/17, *Peter Bosworth and Colin Hurley v Arcadia Petroleum Limited and Others* [2019] ECLI:EU:C:2019:310, par 24-25.
[55] In art. 2(2) of the 2011/83/EU Consumer Rights Directive, "trader" is defined as "any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts covered by this Directive".
[56] Schulte-Nölke (n 52) 506.

mean that, in the case of national case law granting platform workers an employee status, those platform workers fall under the protective scope of the national labour laws as well as under the P2B Regulation. In this case, the platform employee would be entitled to invoke all more favourable provisions of the applicable national labour law in addition to the P2B Regulation.[57] This interpretation would ensure that national labour classifications do not hinder the Regulation's protective scope, allowing platform workers to benefit from both national labour laws and the P2B Regulation concurrently. This way, the P2B Regulation forms a legal safety net with minimum protections in cases where national labour or case law does not see platform workers as employees. On the downside, this means that when platform workers are considered "business users" for the purposes of the P2B Regulation and simultaneously employees under national law, the P2B Regulation would not bring about a full harmonisation of the relationship between platforms and the platform workers, leaving some leeway for more favourable national labour law.[58]

Secondly, at the end of 2021, a more supranational approach followed when the European Commission recognised this grey zone for many platform workers when it comes to their employment status and published a proposal for a Directive.[59] This recently approved "Platform Work Directive" has the aim of remedying the frequent misclassification of platform workers and the related lack of social rights and protection, by establishing a legal presumption of employment for platform workers if there are facts indicating control and direction. The Platform Work Directive therefore serves as a gateway for self-employed platform workers to gain access to all relevant national labour law protections through national caselaw requalifying them as employees. Even though Member States have time until April 2026 to incorporate the Directive's provisions into their national laws, it is interesting to already think about what the implementation of this Directive could mean against the background of the P2B Regulation. If the term "business user" in the sense of the P2B Regulation were to be interpreted autonomously, this would render national caselaw irrelevant for its application, even when based on a supranational Directive. This would create a peculiar situation in which requalified platform employees benefit from national labour law provisions based on a European presumption of employment, while at the same time being categorised as a "business user" for the purposes of the P2B Regulation. This dual protection highlights the need for clarity to ensure a coherent legal framework for platform workers.

4.1.1.2 The limitations of the "business user" definition

Besides the qualification issue, there are some other concerns that arise when analysing the Regulation's scope. Firstly, in the context of meal delivery platforms that are in a

[57] ibid 507.
[58] ibid.
[59] Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work 2021 [COM/2021/762] 2021/0414/COD.

four-sided relationship with the platform, the consumer and the restaurant, the following question arises: are both the restaurant and the food delivery person captured by the "business user" definition? At first glance, it seems evident that the business user in this quadrilateral relationship would be first and foremost the restaurant who offers the food to consumers.[60] The delivery people, however, merely deliver the food to the consumer and therefore do not really offer any goods to consumers themselves. It could be argued, however, that the delivery people offer their services (i.e. meal delivery) to consumers and therefore still fall within the scope of the P2B Regulation. In this case, the P2B Regulation would then have impact on both the platform-to-restaurant and the platform-to-delivery-person relationship.

A second concern is the fact that the scope of the Regulation explicitly excludes peer-to-peer services in the absence of business users.[61] In this regard, it is relevant and important to discover which platforms are considered to be peer-to-peer, as a lot of labour platforms have originated from the peer-to-peer sharing idea but have evolved to a new business model with commercial users.[62] Furthermore, in some cases of platform work, it is unclear whether platform workers provide the services as private persons or as business users. Many peer platforms allow both commercial providers to operate alongside private peers, which complicates this peer-to-peer exemption.[63] For example, even though Deliveroo is not considered to be a peer-to-peer platform, the Deliveroo platform in Belgium allows workers to deliver meals under two capacities: either as a peer under the peer-to-peer system if you stay under a yearly wage cap, or as a self-employed delivery person. Consequently, the P2B Regulation only applies to Deliveroo and its terms and conditions for its self-employed riders, but not to the people performing the exact same work under a peer-to-peer system. In this regard, it is remarkable that this exemption has resulted in a notable difference in the terms and conditions for Deliveroo couriers in Belgium, depending on whether they provide the services as a peer or as a self-employed courier. This finding will be discussed more under section 4.3 where the terms and conditions of the five selected platforms are discussed based on compliance with the P2B Regulation.

It is important to stress that in the sense of consumer law, seeing peer providers as professional traders – i.e. business users in the context of the P2B Regulation - is often not feasible or fair, considering that peers generally lack the technical and legal skills or

[60] Andreja Schneider-Dörr, 'Die Neue Richtlinie 2019/1152 Und Die P2B-VO 2019/1150 – Ein Dilemma Für Crowd Work' (2020) 68 Arbeit und Recht 358, 363.
[61] Recital (11) P2B Regulation.
[62] Uber started off with its "UberPop" business model where regular individuals without a commercial taxi license or permit could provide taxi services (peer-to-peer). For that reason, UberPop was prohibited and Uber subsequently launched UberX where drivers were required to have a commercial license and insurance (thereby steering away from peer-to-peer services). Freelance platform "Fiverr" also initially focused on small tasks offered by peers for $5, but has now evolved to a wide range of service conducted with many professional freelancers and businesses offering the services at varying price points.
[63] 'Exploratory Study of Consumer Issues in Peer-to-Peer Platform Markets' (n 34) 8.

resources that professional traders have when having to comply with extensive information disclosures, dispute resolution services, etc.[64] However, in the sense of the P2B Regulation, peers would be the *beneficiaries* of its provisions and the related information and transparency rights. For this reason, it would have been feasible to include peer platform workers in the scope of the Regulation, thereby establishing a more level playing field by granting all forms of platform workers, both self-employed and peers, the same baseline protections. In doing so, the P2B Regulation could serve as a minimum harmonisation whose core transparency rights are applicable to *all* platform workers regardless of status. In the case of *peer* platform workers, this could then be complemented by the more extensive unfair term protection as provided by the UCTD.

4.1.1.3 Conclusion

In conclusion, it seems that platform workers can fall under the definition of "business user" as long as they are self-employed and offering services to consumers for purposes relating to their trade. The business user definition thereby seemingly excludes platform employees. Given that employees typically enjoy more robust protections under national labour laws, the necessity of the P2B Regulation for this group seems redundant. However, it is still desirable to determine whether the term "business user" in the context of the P2B Regulation has an autonomous interpretation, as is common with most protective EU laws. An autonomous interpretation would ensure that national caselaw does not hinder the Regulation's protective scope, allowing platform employees to benefit concurrently from labour laws on a national level and the P2B Regulation on a European level.

Peer platform workers cannot fall back on the P2B Regulation for unfair term protection since they are not considered "business users" acting for purposes relating to their trade or profession. In this regard, a comprehensive list of true peer-to-peer platforms would provide clarity as to which platforms are excluded from the Regulation's scope, consequently preventing the potential circumvention of the Regulation's provisions through the establishment of purported "peer-to-peer" services. Even though the purpose of the P2B Regulation is to close a gap in protection for platform workers, the exclusion of peer-to-peer services opens up another gap. This is exemplified by the fact that there are notable differences in the terms and conditions for Deliveroo couriers in Belgium, depending on whether they provide the services as a peer or as a self-employed courier (*infra*). Including peer platform workers in the P2B Regulation would create a more level playing field by granting all platform workers, both self-employed and peers, the same fundamental protections, which could be further complemented by the UCTD's unfair term safeguards.

[64] Natali (n 31) 20.

4.1.2 Are all labour platforms "online intermediation service providers"?

The P2B Regulation uses the term "online intermediation service provider" ('OISP') for online platforms, and in order to be considered an OISP, three requirements need to be met. Firstly, it has to be a service which is an information society service as defined in art. 1(1)(b) of the Information Society Services Directive (2015/1535/EU), namely "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[65] Secondly, the service has to allow business users to offer goods or services to consumers with a view to initiating direct transactions between them, irrespective of where these transactions are ultimately concluded.[66] Thirdly and lastly, the services have to be provided to business users on the basis of contractual relationships between the platform and business users which offer goods or services to consumers.[67] With this definition, the Commission envisioned to capture the entire online platform economy, consisting of approximately 7000 online platforms operating in the EU.[68] If we apply these criteria to labour platforms, it would seem that at first glance, labour platform's services fall under the definition of an information society service, that allows the business users – platform workers – to offer services to consumers which happens on the base of a contractual relationship between the labour platform and the platform worker, consequently fulfilling all three requirements. However, it appears to not be that simple.

4.1.2.1 Elite Spain judgment: transportation platforms excluded?

In 2017, the CJEU investigated whether Uber can be considered to provide 'information society services' (in this case, for the purpose of falling under the e-commerce Directive) or purely services in the field of transport in the *Asociacion Profesional Elite Taxi v Uber Systems Spain* case.[69] This is relevant because in order to be considered an OISP under the P2B Regulation, the services provided by the platform need to be information society services ('ISS'). The CJEU started the judgment by stating that, in principle, an intermediation service that uses a smartphone app to transfer information between the passenger and the driver meets the criteria for classification as an information society service.[70] However, ultimately, the CJEU decided that Uber's app constitutes an integral

[65] Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 2015 art 1(1).
[66] Art. 2(2)(b) P2B Regulation.
[67] Art. 2(2)(c) P2B Regulation.
[68] 'Digital Single Market: EU Negotiators Agree to Set up New European Rules to Improve Fairness of Online Platforms' Trading Practices' (*European Commission Press Corner*, 14 February 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168> accessed 7 December 2023.
[69] Case C-434/1, *Asociación Profesional Élite Taxi v Uber Systems Spain SL* [2017] ECLI:EU:C:2017:981.
[70] ibid para 35.

part of an overall service whose *main* component is a transport service, and therefore, Uber's services cannot and must not be classified as information society services.[71]

It can be assumed that the (potentially undesired) consequence of this judgment is the fact that Uber and more importantly, its drivers are excluded from the protective scope of the P2B Regulation. In distinguishing whether Uber is a 'mere' provider of ISS, or instead more directly involved in providing the underlying services, the Court found Uber's far-reaching algorithmic control of crucial importance. The 'level of control' exercised by a platform through *inter alia* algorithms, including the setting of prices, are therefore amongst the key criteria in deciding whether the platform provides ISS or not.[72] Therefore, it might be unlikely that platforms which exercise considerable algorithmic employer control over its workforce would fall within the scope of the P2B Regulation.[73] As most labour platforms exercise decisive levels of control over their platform workers, it is uncertain whether they are considered to provide ISS and whether the P2B Regulation applies. This would result in a precarious situation: the more control platforms exercise over their platform workers, the less likely it gets that the P2B Regulation applies. Thus, the more platform workers experience employer-like control and are unable to set their own prices, the less protection they likely receive under the P2B Regulation.

Moreover, since the *Elite Spain* judgment, some doctrine has assumed that the court's reasoning entails that platform services in the field of transport are not to be considered information society services.[74] Even though the CJEU has not rendered judgments on meal delivery platforms, it can be speculated that if we were to extend the Court's line of reasoning, meal delivery platforms could also be seen as a form of organising transport and therefore also fall outside the definition of an ISS. This depends on whether the CJEU would consider the transport and home-delivery of the food as the *main* component of meal delivery platform's services.[75]

However, it is plausible that the CJEU in the *Elite Spain* judgment only considered the way Uber's services are perceived by the *consumer*, rather than by Uber's business users, ie the Uber drivers. When looking at the platform-worker-to-consumer relationship, it is logical that the main component of that service is transportation. Nevertheless, when considering the platform-to-platform-worker relationship and the underlying service provision, it would not be accurate to say that Uber provides its drivers with transportation services. Consequently, when taking a platform-worker-centric approach, there is room

[71] ibid para 40.
[72] Jeremias Adams-Prassl, 'Regulating Algorithms at Work: Lessons for a "European Approach to Artificial Intelligence"' (2022) 13 (1) European Labour Law Journal 16.
[73] ibid.
[74] Pieter van Cleynenbreugel, 'Will Deliveroo and Uber Be Captured by the Proposed EU Platform Regulation? You'd Better Watch Out…' (*European Law Blog*, 12 March 2019) <https://europeanlawblog.eu/2019/03/12/will-deliveroo-and-uber-be-captured-by-the-proposed-eu-platform-regulation-youd-better-watch-out/> accessed 20 December 2023.
[75] Jan Blockx, 'Welke Richting Op Met de Deeleconomie? Open Vragen Bij de "Uber" Arresten' (2018) 119 Droit de la consommation 73, 74.

for arguing that Uber does provide its drivers with ISS, thereby potentially warranting inclusion within the scope of the P2B Regulation.

4.1.2.2 Study on the Evaluation of the P2B Regulation: transportation platforms included?

In September 2023, the European Commission published a Study on the evaluation of the P2B Regulation in which it *inter alia* collected data from 300 sets of terms and conditions of 300 selected platforms to evaluate compliance.[76] For this Study, the Commission chose a representative sample of 300 OISPs in terms of size and type of platforms. One could assume that the Commission would only evaluate a platform's terms and conditions when the P2B Regulation is relevant and applies to the platform. Evidently, this reasoning does not work the other way around, the absence of certain platforms in the Study does not mean that they would fall outside the scope of the P2B Regulation. The Study made a representative categorisation of chosen platforms, including e-commerce marketplaces, social media platforms, search engines, but more importantly for this article: transportation and delivery platforms. Out of the five investigated platforms in this article, only the terms and conditions of AMT and Deliveroo were assessed in this Study. When it comes to online platform work, very little other crowdsourcing platforms other from AMT were included in the Study, though Upwork does get mentioned in the Study when it discusses the social media channels used to post about the P2B Regulation.[77] Even though Uber's terms were not assessed, similar transportation platforms like Bolt, Heetch and FREE NOW were assessed. Uber, however, does get mentioned as an example in the categorisation of platforms used in the Study, under "specialised service platforms, eg Uber".[78] The fact that Deliveroo and similar meal delivery and transportation platforms[79] were included in the Study suggests that the Commission generally assumes that meal delivery and transportation platforms fall within the scope of the P2B Regulation. This raises questions about whether the *Elite Spain* case did in fact successfully preclude Uber from the scope of the P2B Regulation or not, while other similar transportation platforms still fall under the Regulation. Strangely enough, among the five assessed platforms, Uber is the only platform whose website has a separate and dedicated tab with information and links to the P2B Regulation that allows business users to file a complaint regarding any alleged non-compliance.[80] If Uber would in fact be

[76] European Commission and others, *Study on Evaluation of the Regulation (EU) 2019/1150 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services (the P2B Regulation) – Final Report* (Publications Office of the European Union 2023).
[77] ibid 23.
[78] ibid 15.
[79] Examples of other meal delivery platforms included in the Study are UberEats, Foodora, Thuisbezorgd, Glovo, CoopCycle, etc.
[80] Uber P2B regulation at <https://help.uber.com/driving-and-delivering/article/platform-to-business-P2B Regulation - business-user-contact-form?nodeId=eff934bc-17c5-466e-bef7-e37f5c3f4539> accessed 26 September 2023.

successfully precluded from the scope of the Regulation, it seems Uber itself is not aware of this fact.

4.1.2.3 Conclusion

Since the CJEU decided that Uber's services cannot and must not be considered to be ISS in the *Elite Spain* judgment, it is likely that Uber and its drivers are excluded from the scope of the P2B Regulation. Some doctrine has assumed that the court's reasoning in the *Elite Spain* judgment entails that platform services in the field of transport are not to be considered information society services, and more generally, that platforms which exercise considerable algorithmic employer control over its workers fall outside the scope of the P2B Regulation.[81] It is thus not clear whether transportation platforms and labour platforms in general fall under the definition of online intermediation service provider and therefore within the scope of the P2B Regulation.

The fact that transportation platforms are assessed in the Commission's Study evaluating the P2B Regulation could mean that there is a discrepancy between the Commission and the CJEU based on whether transport platforms fall under the definition of 'information society services'. Thus, while the Commission clearly intended to target all European online platforms, there seems to be some unclarity about the full reach and limitations of the P2B Regulation. This unclarity and gap should be resolved through a broader definition of online intermediation services that include all online platforms and goes beyond the 'information society service' definition. This will help ensure legal certainty for platform workers using labour platforms to provide services.

4.2 Geographical scope

Article 1 of the P2B Regulation states that it applies to "online intermediation services" that are provided to business users that have their place of establishment in the Union and that offer goods or services to consumers located in the Union. From this, a two-fold test can be derived: firstly, the business users (in this context: the platform workers) need to have their establishment or residence in the EU and those platform workers need to offer goods or services to consumers who are located in the EU. The Regulation further clarifies that since digital platforms have a global dimension, the Regulation applies to platforms regardless of whether they are established in a Member State or outside the EU. In summary, this means that the platforms need to have both a European consumer and a European worker base.

Disregarding the material scope, there is no doubt that Uber and Deliveroo fall under the geographical scope of this Regulation as these platform services are location-bound and consequently offered to European customers and performed by EU-based platform

[81] Adams-Prassl (n 72) 16.

workers. The other platforms, Clickworker, Upwork and AMT are all microtasking platforms with a global reach that allow platform workers to perform the tasks purely online. Clickworker asserts on its website that its worker community comprises "more than 4.5 million people from all of the world", with 30% originating from Europe[82] while Upwork states it has a "network of global freelancers in over 180 countries" including many European ones.[83] On top of their European supplier market, both Clickworker and Upwork allow European consumers to order tasks from their platform workers, thereby rendering the P2B Regulation fully applicable. Lastly, AMT states on its website that European consumers are allowed to register, though offers very little transparency on its worker demographics. Upon trying to register as a "Turker" both from Belgium and Germany, a rejection email was received stating that it was "not permitted to work on Mechanical Turk at this time" and to "please note that Customer Support is unable to change this decision and cannot share insight into invitation criteria." However, a study from 2018 continuously monitors the worker demographics of AMT through an ongoing survey that uses geolocalisation.[84] These results show that the top-20 countries of AMT workers in 2018 included Germany, France and Italy, that were ranked 7th, 8th and 9th, accounting for a little over 1% of workers. Despite the vast majority (over 90%) of Turkers being American, this could mean that there is in fact a European worker base. Since the P2B Regulation does not require a 'substantial amount' of EU-based platform workers, this 1% could still trigger the full applicability of the Regulation. Furthermore, the fact that AMT was included in the Study evaluating the P2B Regulation could be an assumption of the Commission that AMT falls under the Regulation's scope. As the Regulation does not require any compulsory data sharing, this raises a concern about platforms' ability to potentially circumvent European legislation by not providing transparent data about worker demographics or residency. Without making any statement as to the potential applicability and solely for the purposes of this article, AMT's terms and conditions are evaluated against the P2B-provisions in the next chapter.

4.3 Three years after the P2B Regulation: are platforms' terms and conditions in compliance?

4.3.1 Provisions relevant for labour platforms

Overall, the P2B Regulation contains rules that are not really designed to protect workers from the power of the platform, but are rather designed to enable a certain

[82] Clickworkerc community page <https://www.clickworker.com/clickworker-crowd/> accessed 14 September 2023.
[83] Upwork eligibility page <https://support.upwork.com/hc/en-us/articles/211067778-Eligibility-to-Join-and-Use-Upwork> accessed 14 September 2023.
[84] Djellel Difallah, Elena Filatova and Panos Ipeirotis, 'Demographics and Dynamics of Mechanical Turk Workers', *Proceedings of the Eleventh ACM International Conference on Web Search and Data Mining* (Association for Computing Machinery 2018) <https://doi.org/10.1145/3159652.3159661> accessed 7 August 2023.

minimum level of entrepreneurship, such as the transparency of ranking criteria, access to data and portability of reputational data.[85] While the P2B Regulation might not have been specifically designed for labour platforms, it does contain certain provisions that are relevant for digital labour platforms.[86] The Regulation imposes requirements as to the clarity, the content and the modification of terms and conditions used by online platforms, which are relevant for platform workers. The phrase "terms and conditions" is broadly defined to cover all terms and conditions or specifications, irrespective of their name or form, which are unilaterally determined by the platform and govern the contractual relationship between the platform and its business users.[87] The requirement that the terms are "unilaterally determined by the platform" is different than the UCTD, which applies to "terms which have not been individually negotiated". The deviation of the negotiation requirement could be to avoid situations where platform operators create "pretend negotiations" to try and remove the terms from the ambit of the Regulation.[88]

While it contains some specific requirements for platforms' terms and conditions, it does not set out legal criteria for generally assessing the potential unfairness of terms like the UCTD. Specifically, article 3(1) of the Regulation requires *inter alia* that terms and conditions need to be, 'drafted in plain and intelligible language', 'easily available to business users at all stages of their commercial relationship, including in the precontractual stage' and 'set out the grounds for decisions to suspend or terminate the provision of their online intermediation services to business users'. Further, article 3(2) requires platforms to notify any proposed changes of the terms and conditions to the business users, on a durable medium such as e-mail. This notification must take place at least 15 days before implementing the envisaged changes, but in general the notice period must be reasonable and proportionate to the nature and extent of the envisaged changes and to the consequences for the concerned business users.

Apart from mandatory notice periods and statements of reasons, the Regulation contains no clear substantive limitations on the platform's use of unilateral variation clauses. The Regulation does however illustrate that certain predictability and transparency requirements are placed upon platform businesses as a condition for market access. These provisions demonstrate the Regulation's focus on procedural fairness, laying out detailed procedural requirements. These systemic expectations limit the platform's space for one-sided commercial manoeuvring enabled by unilateral variation clauses.[89]

For the purposes of this article, the terms and conditions of the five chosen platforms were analysed against the background of the previously mentioned provisions of the P2B Regulation that proscribe rules for fair and transparent terms.

[85] Eva Kocher, 'Reshaping the Legal Categories of Work: Digital Labor Platforms at the Borders of Labor Law' (2021) 3(3) Weizenbaum Journal of the Digital Society w1.1.2, 18.
[86] ibid.
[87] Art 2(10) P2B Regulation.
[88] Twigg-Flesner (n 12) 10.
[89] Hansen and Ritchie (n 15) 946.

4.3.2 Overview of platform's compliance

More than three years post-implementation, it seems that definitely not all platforms comply with the provisions of the P2B Regulation. Before diving into a more in-depth analysis of compliance in the subsections below, Table I below provides a general schematic overview that illustrates which platforms comply with which of the previously discussed provisions.

Table I. Schematic overview of compliance with the P2B Regulation

Based on the author's research into the five aforementioned platforms' terms and conditions, Table I provides a schematic overview that signals which platforms comply with certain provisions of the Platform-to-Business Regulation. The provisions were selected based on their relevance specifically in the context of digital labour platforms and platform work.

A question mark in *Table I* signals that there is either not enough information to judge compliance on or that it is uncertain whether the terms (fully) comply with the provision, e.g. when the terms specify that business users are informed in advance of changes but no time period is specified while the P2B Regulation requires a notice period of at least 15 days.

	Uber	Upwork	AMT	Deliveroo	Clickworker
Country of origin	*U.S.A.*	*U.S.A.*	*U.S.A.*	*U.K.*	*Germany*
Drafted in plain & intelligible language	?	✓	?	?	?
Easily available to business users at all stages of commercial relationship	✗	✓	✓	✗	✓
Set out grounds for decisions to suspend or terminate services to a business user	✓	✓	✗	✗	✓
Notify the business users concerned of any proposed changes of their terms	?	✓	✗	?	?

Uber, Upwork and AMT have been strategically placed next to each other as these are platforms with an origin in the U.S.A., while Deliveroo and Clickworker - platforms with a European origin – are placed on the right. This overview makes clear that the geographical origin of the platform has little impact on its compliance or familiarity with the P2B Regulation. The only platform out of five whose terms and conditions consistently complied with the provisions of the P2B Regulation, is American platform Upwork. Second-best is German platform Clickworker, that complies with 2 out of 4 investigated provisions and potentially complies with the other two. It is rather curious that while Uber is the only platform with a separate tab on its website for P2B-related complaints, it only certainly complies with only one of the discussed provisions, violates another, and leaves its compliance with the remaining two uncertain. The two lowest-scoring platforms are Deliveroo and AMT that fragrantly violate 2 out of the 4 investigated provisions, which is

striking as the former was founded in Europe (the U.K.), targets European consumers and platform workers and has Europe-specific terms, while the latter is American-based and targets its services mostly to Americans, combined with only one set of terms for all users.

Overall, these five investigated platforms manage to tick only 8 out of 20 boxes in *Table I* with certainty. These findings are in line with the conclusions in the Commission's Study of the P2B Regulation, that also alerted a rather low level of compliance with the P2B Regulation and associated this issue with the lack of responsible enforcement authorities (*infra*, section 4.4 on enforcement).[90]

4.3.3 Drafted in plain and intelligible language

To ensure that the terms and conditions enable business users to determine the conditions for the use, termination and suspension of the platform work and to achieve predictability, article 3(1)a of the P2B Regulation requires that terms and conditions should be drafted in plain and intelligible language. The Commission clarified that where the terms are vague, unspecific or lack detail on important commercial issues and thus fail to give business users a reasonable degree of predictability, they are not considered to be plain and intelligible.[91]

While this remains a mostly subjective criterion, it urges platforms to provide the terms and conditions in accessible language. Out all five platforms, there was only one platform that seemed to have made an active effort to help business users understand its terms and conditions. Upwork's Terms of Use give the reader the option to click an icon that gives a simple summary of each section. Furthermore, in its User Agreement, it is explicitly stated that "to make these terms a little easier to understand, we capitalize certain terms and capitalizing them means they have a special meaning."[92] In today's reality where less and less people take the time to read terms and conditions[93], this is a great initiative to help guide the readers through lengthy documents and offer them a quick overview of their duties and rights. Upwork effectively does this while simultaneously still stressing that it is advised to read the sections completely to get all the details of what you are agreeing to. The terms of the other four platforms remained rather standard, with no apparent efforts to make the terms more intelligible for its business users, without being particularly unintelligible. Subsequently, it seems that Upwork is the only platform that can be said to *certainly* comply with article 3(1)a of the Regulation, while the other four potentially comply.

[90] Directorate-General for Internal Market and others, *Executive Summary of Study on evaluation of the P2B Regulation* (Publications Office of the European Union 2023) 7.
[91] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services l (15).
[92] See Upwork's User Agreement <https://www.upwork.com/legal#useragreement> accessed 12 June 2024.
[93] In the EU, four out of five respondents say that they only sometimes or never read the terms and conditions as can be read in European Union Agency for Fundamental Rights (FRA) (2020), *Your rights matter: Data protection and privacy, Fundamental Rights Survey*.

4.3.4 Easily available to business users at all stages of their commercial relationship

Pursuant to article 3(1)b of the P2B Regulation, business users need to be able to easily find the terms and conditions in all stages of the commercial relationship, including the precontractual stage so they are aware of the rules that (would) apply to them. So, from the moment that business users decide to offer their services through the labour platform, they should be able to access and refer to the terms.

Starting with the two location-based platforms, a striking conclusion after researching Deliveroo's terms and conditions is the fact that no worker-specific terms and conditions can be found on the website, and not immediately after signing up to be a rider either. The only "terms of service" on the website are specifically tailored towards consumers, demonstrated by the consumer-specific phrasing to "please read these Terms carefully before ordering any items from our Application" and that "our [Deliveroo's] objective is to link you to the restaurants we partner with and allow you to order items for delivery by a delivery rider."[94] Even though there is a separate website for Deliveroo riders[95], clicking on the "legal" tab redirects you to the general terms of service tailored towards consumers. Deliveroo is the only platform out of five whose website or rider-application process does not provide any worker-specific terms and conditions. The Study evaluating the P2B Regulation stated that a platform that only makes available its business-user-specific terms and conditions *after* registering on the platform, fails to comply with Article 3(1)b.[96] Thus, since business users are not able to find, let alone easily find, the terms and conditions that would apply to them in the precontractual stage, it seems that Deliveroo fragrantly violates article 3(1)b of the P2B Regulation.

Uber has made the terms and conditions for consumers easily available on its website, organised per country and in multiple languages.[97] However, similarly to Deliveroo, these terms and conditions are only applicable to Uber consumers ordering rides. In order for prospective Uber drivers to access the applicable terms and conditions (so-called "Uber Community Guidelines"), multiple steps had to be undertaken such as applying to become an Uber driver and completing information forms with details including your full name, address, car's brand and license plate before finally gaining access to these Community Guidelines. This difference in availability for consumers and business users proves the imbalance between different platform actors. Furthermore, it enables Uber to gather a lot of personal information before business users can even assess whether they agree to these terms, causing a precontractual information asymmetry. Compared to Deliveroo's complete lack of availability, even this multi-step process could be considered an improvement. However, following the same reasoning as with Deliveroo, Uber too violates

[94] See preface and article 2 of Deliveroo Terms of Service <https://deliveroo.be/nl-be/legal> accessed 12 June 2024.
[95] Site of the Deliveroo <https://riders.deliveroo.be/> accessed 12 June 2024.
[96] European Commission and others (n 76) 30.
[97] See Uber's General Terms of Use <https://www.uber.com/legal/nl/document/?name=general-terms-of-use&country=belgium&lang=en> accessed 12 June 2024.

article 3(1)b of the P2B Regulation by only making the business-user-specific terms available after registering on the platform.[98]

Thus, the platforms with location-based services do not seem too eager to clearly share or make available the terms and conditions for their business users. The three assessed crowdworking platforms generally performed better at making the terms and conditions easily available. Out of all five platforms, Clickworker is the only one to make a very clear distinction in its terms and conditions based on both location (North-America and 'rest of world') and type of user (clients and workers) on its website.[99] Upwork has the "Upwork Terms of Service" available on its site which is comprised of over 18 different documents including the User Agreement, Terms of Use and Direct Contract Terms.[100] Throughout these documents, the terms differentiate depending on the "account type" (client or freelancer), making it possible for business users to discern the relevant terms that apply to them. Lastly, AMT has an easily accessible "participation agreement" that states that references to "you" and "your" may apply to either requesters, or workers, or both.[101] While this certainly complicates the business users' ability to easily see which terms do or do not apply to them, the terms are easily accessible on the website which seems to comply with the P2B Regulation.

4.3.5 Set out grounds for decisions to suspend or terminate services to a business user

In order to provide business users with legal certainty, article 3(1)c of the P2B Regulation requires the platform to set out the grounds for potential decisions that can lead to a suspension or termination of a business user's account in advance. This provision is particularly important as the restriction, suspension or termination of user accounts – especially without giving any prior warning or providing meaningful reasons - is one of the most severe measures a platform worker can receive.

Uber and Clickworker's terms and conditions both clearly set out the grounds for a potential suspension or termination. In Uber's Community Guidelines, the different grounds that can cause you to lose access to the Uber platform are set out in a detailed manner and are mostly related to violating any terms of the agreement including violence, sexual misconduct, discrimination, etc.[102] Similarly, Clickworker's terms stated that the platform has a right to terminate the contract if the worker violates the terms and

[98] European Commission and others (n 76) 30.
[99] See Clickworker's Terms & Privacy Policy <https://www.clickworker.com/terms-privacy-policy/> accessed 12 June 2024.
[100] See Upwork's Terms of Service <https://www.upwork.com/legal#terms> accessed 12 June 2024.
[101] See preface of Amazon Mechanical Turk's Participation Agreement <https://www.mturk.com/participation-agreement> accessed 12 June 2024.
[102] See section "How Uber enforces our guidelines" in Uber's Community Guidelines <https://www.uber.com/ug/en/drive/basics/uber-community-guidelines/> accessed 12 June 2024.

conditions or other contractual obligations.[103] Next, Upwork's Terms of Use state that it can take away the platform worker's right to use its services at any time, and further concretises that the access to Upwork can be taken away in case of violation of the Terms of Use.[104] Since all three sets of terms set out the expected behaviour of its workers and connect the grounds for termination to this conduct, these terms seem to be in accordance with article 3(1)c of the P2B Regulation.

Contrastingly, Deliveroo has a contractual provision that grants Deliveroo the right to terminate the agreement with the business user at any time and for any reason, with one week's written notice.[105] This is in clear violation of the Regulation that requires the platform to set out the grounds to terminate the platform services. The same goes for AMT, whose Participation Agreement states that the agreement and the business user's account can be terminated or suspended immediately, without notice and for any reason.[106] This leaves the platform workers with a very uncertain and unpredictable work environment, which is exactly what the Regulation wants to remedy.

4.3.6 Notify the business users concerned of any proposed changes of their terms and conditions

As discussed before, unilateral variation clauses grant platforms the right to update and change the contractual terms that apply to the platform worker. The sudden introduction of changes without (sufficient) notice can take the business user by surprise and lead to unwanted effects.[107] To avoid this, article 3(2) of the P2B Regulation regulates this use of unilateral variation clauses by requiring that business users are notified of any proposed changes with a notice period reasonable and proportionate to the nature of the envisaged changes, which is in any case at least 15 days before implementing the changes. Within this period, the business user has the right to terminate the contract with the platform. It is important to note that the Regulation does not specify in what situations a unilateral change or variation is permissible, meaning that platforms preserve the freedom to unilaterally change the terms as long as the required period of notice is adhered to.

As discussed before, all five platforms contain unilateral variation clauses in their terms and conditions. Against the background of the P2B Regulation, however, it is important to verify whether the required notice period is adhered to. Uber, Upwork and Clickworker all have provisions in their terms stating that platform workers get informed of upcoming changes. Upwork concretely states there is 30 days' notice though only for "substantial

[103] See article § 3.1 of Clickworker's Terms and Conditions <https://workplace.clickworker.com/en/agreements/10123> accessed 12 June 2024.
[104] See section 4.1 of Upwork's Terms of Use <https://www.upwork.com/legal#terms-of-use> accessed 12 June 2024.
[105] Article 9.2 of Deliveroo's Model Service Provision Agreement for self-employed couriers (not publicly available).
[106] See section 11 of Amazon Mechanical Turk's Participation Agreement <https://www.mturk.com/participation-agreement> accessed 12 June 2024.
[107] Twigg-Flesner (n 12) 13.

changes"[108], while Clickworker and Uber remain more vague, stating the business users will respectively "be informed in advance" and "within a reasonable time period".[109] As long as Upwork makes sure business users get informed at least 15 days in advance, also for non-substantial changes, it seems that this is in compliance with article 3(2) of the Regulation. Uber and Clickworker potentially comply with the Regulation, although it is advisable that they specify a minimum notice period of 15 days is given to ensure compliance.

In light of the previous discussion on how peer-to-peer platform services are excluded from the Regulation's scope, an interesting finding occurred when comparing Deliveroo's terms for peer delivery couriers with the terms for self-employed couriers. For peers, the terms contain a provision that gives Deliveroo the right to modify the terms at any time by giving a mere notification.[110] On the other hand, the terms for the self-employed couriers make no mention of Deliveroo's right to change or update the terms and therefore no longer contain a unilateral variation clause. This exemplifies the gap in protection of the P2B Regulation, where peer platform workers can still legally be confronted with a lot of uncertainty. It is unsure whether Deliveroo complies with the legal notice period for its self-employed couriers as the terms make no mention of unilateral changes or a notice period. Interestingly, the terms and conditions for Deliveroo customers also contain a unilateral variation clause that grants Deliveroo the right to change these terms from time to time.[111] This demonstrates that these three different forms of platform users, all have different terms and conditions applied to them depending on the distinct regulatory frameworks that govern their interactions with the platform (*infra*, section 5). In the unlikely case that Deliveroo simply did not grant itself that contractual variation right and consequently never unilaterally changes or updates the terms to the agreement, article 3(2) would be redundant.

Lastly, AMT states that they may modify, suspend or discontinue their website at any time and without notice, and that the continued use of the website constitutes the acceptance of the modified terms.[112] In other words, AMT puts the burden on the platform workers to regularly check and notice whether the terms and conditions have changed. Not only is this in violation of article 3(2) of the Regulation, it also opens the door for a lot of unfair terms.

[108] See section 15.2 of Upwork's User Agreement (n 92).
[109] See section 16.1 of Uber's General Terms and Conditions (n 97) and section § 1.3 of Clickworker's General Terms and Conditions (n 99).
[110] Article 3.4 of Deliveroo's Model Service Provision Agreement for peer couriers (not publicly available).
[111] See article 14 of Deliveroo Terms of Service (n 94).
[112] See section 12(b) of Amazon Mechanical Turk's Participation Agreement (n 106).

4.4 Enforcement of the P2B Regulation

In order for the P2B Regulation to achieve its goal of providing a baseline of transparency and procedural fairness, effective enforcement needs to be ensured. The Regulation relies on a mix of both public and private enforcement, combined with some collective enforcement elements – leaving the choice of how to ensure effective enforcement to the Member States.[113] This entails that Member States are not required to create new enforcement bodies to ensure public enforcement. The Commission associated the issue of low compliance, as demonstrated in the previous section, with the lack of responsible enforcement authorities.[114] In Member States that relied on private enforcement via courts, the effectiveness of the P2B Regulation proved to be very limited. One of the risks of using private enforcement, especially in situations of a power asymmetry, is the fact that business users are often reluctant to initiate legal action against the powerful (platform) business as they fear costly and lengthy litigation, or potential retaliation from platforms.[115]

The Commission's Study showed that public enforcement through monitoring, investigations and proactive communication was the most effective way to ensure compliance with the P2B Regulation.[116] Public authorities could launch monitoring exercises and initiate *ex officio* investigations, as well as develop guidelines that facilitate compliance for platforms.[117] In Member States that opted for private enforcement, this approach has resulted in the absence of bodies responsible for monitoring platforms' terms and conditions in order to detect non-compliance.[118] A lack of (pro)active monitoring makes the enforcement of the Regulation merely complaint-based, which only works if there is sufficient awareness with platform business users about their rights. The Study shows, however, that this was not the case as there was a major lack of awareness among the business users about the existence of the Regulation, let alone their rights.[119] This lack of awareness further contributed to the lack of compliance on the platform side, as it appeared that large numbers of platforms were not yet aware of the P2B Regulation, even three years post-implementation. For these reasons, Member States that have opted for private enforcement should consider establishing dedicated enforcement authorities. This shift to public enforcement would ensure a more effective application of the P2B Regulation.

[113] Christoph Busch, 'Platform Regulation beyond DSA and DMA: Which Role for the P2B Regulation?' (2024) 12 (2) Journal of Antitrust Enforcement 201.
[114] Directorate-General for Internal Market and others (n 90) 7.
[115] Recital (44) Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
[116] 'Commission Staff Working Document Accompanying the Report on the First Preliminary Review on the Implementation of Regulation (EU) 2019/1150 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services' (European Commission 2023) SWD(2023)300 23.
[117] Busch (n 113).
[118] Directorate-General for Internal Market and others (n 90) 7.
[119] ibid.

4.5 Sanctions of non-compliance

With regards to the sanctions, the P2B Regulation is rather light on or unclear about the consequences of non-compliance by the platforms. The Regulation merely states in article 3(3) that any terms and conditions which do not comply with its provisions shall be null and void.

For some provisions, this sanction is self-explanatory, e.g. for article 3(2) that imposes the mandatory notice period before implementing unilateral changes to the terms, the failure to give notice would result in the ineffectiveness of that variation. However, for other provisions, it is uncertain how exactly this sanction would take effect in practice. For example, not complying with article 3(1)c of the Regulation that requires to set out the grounds for a potential suspension or termination could mean that any decision that the platform makes to suspend or terminate the service on the basis of the insufficiently specific term, would be ineffective. However, it is unclear whether the requirement in article 3(1)c of the Regulation is merely a transparency obligation or whether it would effectively preclude the suspension or termination of the platform worker's access to the platform.[120]

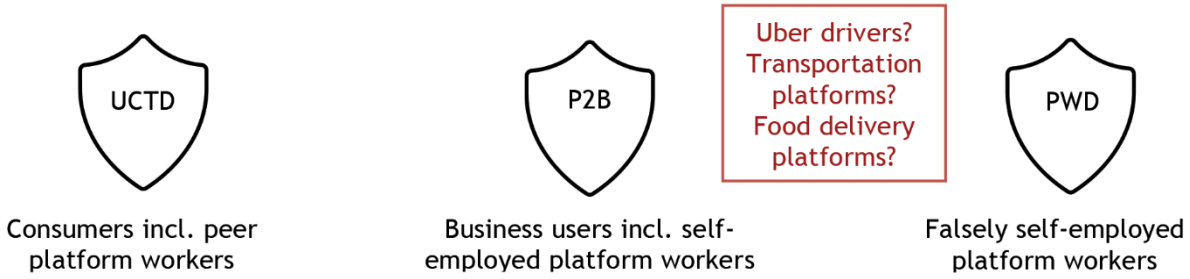
Thus, it remains unclear what the consequence would be for a failure to suspend or terminate a business user's account on objective grounds, even though that is one of the most far-reaching measures for business users. Because the Regulation does not specify a consequence for some cases of non-compliance, the only route to challenge the platform is either through its own internal dispute resolution procedures, or through legal action.[121]

5 Overview: diverse legal protections for various platform users

Today, the legal landscape for platform workers is fragmented, with different protections applying to various categories of platform users, such as self-employed platform workers, peer platform workers, platform employees and consumers. This section and *Figure I* below provide a brief overview of the existing legal shields that protect these groups of platform users and highlight the gaps and/or inconsistencies that arise from this fragmented approach.

[120] Twigg-Flesner (n 12) 12.
[121] ibid 21.

Figure I. Different shields of protection for platform workers



This Figure illustrates three existing legal instruments that have the ability to shield different categories of platform workers from unfair terms imposed by digital labour platforms.

Firstly, consumers and peer platform workers are shielded by the UCTD against unfair terms imposed by platforms. Despite the *ratio legis* being a form of weaker party protection, the UCTD's scope is limited to B2C contracts, thereby excluding the majority of platform workers as they are self-employed under B2B contracts.

Secondly, self-employed platform workers could rely on the P2B Regulation for unfair term protection and procedural fairness in their relationship with the platform. While the UCTD contains more substantive rules on what is unfair and not, the P2B Regulation has more formal and transparency requirements. However, the *Elite Spain* judgment of the CJEU has raised serious doubts about whether Uber drivers and by extension, other labour platforms fall within the scope of the P2B Regulation. Following the Court's reasoning, platforms that exercise considerable employer control over their workers might be excluded from the P2B Regulation, leaving those platform workers without its protections.

Either way, neither the UCTD nor the P2B Regulation tackles other crucial issues for platform workers such as fair wages, health safeguards and the risk of discrimination. Beyond the contractual power imbalance and unfair terms, these issues are of paramount importance for the overall well-being of platform workers and can therefore not be left unaddressed. This is where the third instrument, the Platform Work Directive, has the ability to offer an indirect avenue to address these critical issues by establishing a presumption of employment when factors indicating control and direction are found. This creates the potential for falsely self-employed platform workers to be reclassified by national courts and thereby gain access to national labour laws that include protections for fair minimum wages, health and safety standards, as well as anti-discrimination measures.

None of these three legal instruments makes a distinction or uses a separate regulatory approach based on the physical or online nature of the platform work. It seems undesirable that general fairness mechanisms such as the UCTD and P2B Regulation differentiate based on the precise nature of the platform work, as fairness and transparency should be equally

afforded to all sorts of platform users. However, the practical impact of the Platform Work Directive may be different based on whether the platform work happens physically or online. As discussed under section 4.1.1.1, national caselaw rarely requalifies online crowdworkers as employees, with the first (and only) judgment being rendered in Germany in 2020. Therefore, the presumption of employment – that applies equally to all platform workers, both physically and in the online realm – could be particularly impactful and make a difference for falsely self-employed crowdworkers. This way, the Platform Work Directive could tilt the balance of national caselaw that has almost exclusively reclassified location-bound platform workers. The Directive's uniform application, both across the EU and types of platform work, has the ability to mitigate the existing disparities in protection that arise from differing national approaches.

In conclusion, while various legal instruments act as protective shields for platform workers, the misalignment of these shields due to regulatory gaps leaves certain platform workers vulnerable and at risk of unfair terms. If these shields do not align seamlessly, the protections intended to safeguard workers fall short, exposing them to significant risks.

6 Conclusion

The rise of digital labour platforms utilising self-employed "platform workers" to provide services to consumers has disrupted the traditional labour market. In order to gain access to the platform, all platform users are required to accept and adhere to the predetermined contractual terms outlined in the terms and conditions, often called 'adhesion contracts'. In today's modern contracting world, the efficiency of adhesion contracts is an indispensable feature. Subsequently, it is not desirable that each individual platform contract would have to be negotiated. However, the lack of bargaining power of platform workers vis-à-vis the platform poses a risk for the unilateral imposing of unfair contract terms and causes a power imbalance. Hence, the status quo of unilateral and potentially unfair contracts is not attainable either. Therefore, there is need for a legislative intervention that tackles these unfair terms and the subsequent power imbalance. As labour law is mostly inapplicable to self-employed platform workers and is considered a *lex specialis* of general contract law, this article looked at whether and to what extent contract law solutions could remedy the contractual power imbalance and the related risks of unfair terms.

While there are various legal instruments that offer protection to different categories of platform users (*supra*, section 5), the overall framework is not always consistent and leaves significant gaps, particularly for self-employed platform workers. Since the UCTD's scope is limited to B2C contracts, it only protects consumers and peer platform workers acting for purposes outside their profession. Consequently, the majority of platform

workers are unable to benefit from its unfair term protection as they are self-employed and outside the consumer protection *acquis*.

Further, there is the P2B Regulation that attempted to tackle unfair and untransparent terms in the entire European platform economy. Even though the P2B Regulation is a first brave step towards interfering in B2B contracts at a supranational level, its intervention is rather limited and does not interfere too heavily in the contractual relationships between a platform and its business users.[122] In relation to its scope of application, the requirement that platforms need to provide 'information society services' makes the P2B Regulation fall short in protecting all platform workers comprehensively. Furthermore, there is an apparent discrepancy between the European Court of Justice and the European Commission as to whether transportation platforms can be considered to provide 'information society services'. In 2017, the CJEU excluded Uber from the ISS definition in its *Elite Spain* judgment, while the Commission now included Uber in its Study on the P2B Regulation, which only applies to platforms that provide ISS. Firstly, the P2B Regulation could resolve this unclarity about whether or not transportation platforms provide 'information society services' by adopting a broader definition of 'online intermediation services' without limiting them to providers of information society services. Secondly, for more legal certainty within the European Union, these two essential European bodies should find common ground and take a clear stance on this. This modification would further be in line with the vision of the European Commission to capture *all* European online platforms in the scope.

The potential exclusion of Uber from the P2B Regulation after the *Elite Spain* judgment raises questions about whether platform workers may be excluded from the P2B Regulation depending on the level of control exercised by the platform. Since these self-employed platform workers are simultaneously excluded from the UCTD, this exclusion creates a critical gap where the platform workers who experience significant employer-like control and therefore need the protection the most, are left without sufficient legal safeguards. This lack of a unified approach results in a non-level playing field, with different categories receiving varying levels of protection against the platform. Since the actions of platforms affect *all* ecosystem actors, regardless of capacity, this necessitates a more streamlined legislative initiative that treats all ecosystem actors with an equal and appropriate degree of fairness and transparency. Thus, there is a growing need for a more holistic approach towards online platforms, in which a legal framework is developed that ensures that *all* platform actors, no matter business users, peers or consumers, are protected against actions taken by the online platform. In this regard, the P2B Regulation could adopt a more general concept of a "platform user" rather than solely focusing on business users and excluding peers working through platforms. Adopting a supranational

[122] ibid 25.

definition of "platform user" would include all forms of platform workers and also consumers that could consequently benefit from the Regulation's baseline of protection.

Furthermore, the questions remains whether the P2B Regulation's transparency-based approach will be particularly effective in remedying the power imbalance in labour platforms. Transparency and information obligations have long been the hallmark of EU consumer laws, but this approach has been widely criticised for overestimating the consumer's ability to process such information in full.[123] Consequently, as many of the intended 'business users' are regular individuals who have taken on the self-employed role in order to perform platform work, the outcome here may be similar to that in the consumer field.

When it comes to enforcement of and compliance with the P2B Regulation, it appears that more than three years after implementation, there are rather low levels of compliance by the platforms. Empirical research of the terms of Uber, Deliveroo, Upwork, Clickworker and AMT demonstrated that only one out of five platforms, i.e. American platform Upwork, consistently complied with all investigated provisions while others fragrantly violate them. These findings align with the conclusions drawn in the Commission's Study of the P2B Regulation, which similarly highlighted low levels of compliance with the P2B Regulation. In order for the P2B Regulation to achieve its desired impacts and higher levels of compliance, a public enforcement authority needs to be established to ensure compliance by responding to complaints from business users, launch administrative investigations, and generally raise awareness about the provisions of the P2B Regulation.[124] Following the general idea that rules envisioning a change are only as strong as their enforcement, a lack of (pro)active enforcement stands in the way of an effective societal change. Without more effective mechanisms of (public) enforcement, there will be less meaningful consequences for tackling the power imbalance and information asymmetries in the platform economy.

[123] Anne-Lisse Sibony and Genevieve Helleringer, 'EU Consumer Protection and Behavioural Sciences: Revolution or Reform?' in Alberto Alemanno and Anne-Lisse Sibony (eds), *Nudge and the Law : A European Perspective* (2015).
[124] Directorate-General for Internal Market and others (n 90) 8.

*Ronald Serwanga**

SPECIAL SECTION

ASSESSING NEW TESTING GROUNDS FOR ONLINE MONEY SAFETY IN UGANDA

Abstract

This research critically examines Uganda's regulatory sandboxes in mobile money services, comparing them with frameworks in Kenya and the United Kingdom (UK). Regulatory sandboxes play a crucial role in fostering innovation while managing digital financial risks, particularly those posed by foreign information and communication technology (ICT) service providers. However, previous studies have not adequately addressed the alignment of Uganda's sandboxes with international standards and the specific risks associated with foreign operators. This research aims to determine how Uganda's regulatory sandboxes align with global practices, assess digital financial risks, and suggest risk mitigation strategies. Using a qualitative approach that includes comparative analysis, the research explores coordination between national and regional legal frameworks. The findings reveal that Uganda's regulatory sandbox framework is less developed in cross-border testing and lacks comprehensive consumer protection measures seen in Kenya and the UK. The research highlights the need for improved regulatory coordination and integration of best practices to improve the resilience of Uganda's financial sector. This research provides valuable information on the refinement of Uganda's regulatory framework, highlighting the importance of harmonised regulations that support innovation and ensure data security, thus improving consumer confidence and service continuity in the digital financial landscape.

JEL CLASSIFICATION: G28, E42, O33

SUMMARY

* Holds an LLM (Master in Rule of Law for Development) from Loyola University Chicago, an LLM (Masters in Business Law) from the University of Rwanda, and an LLB (Bachelor of Laws) from Makerere University.

DOI 1.13135/2785-7867/11333

1 Introduction

The growing attention to regulatory sandboxes in digital financial services (DFS) is driven by the increasing complexity and innovation in financial technologies, particularly in countries such as Uganda, Kenya and the United Kingdom. The rapid adoption of mobile money services, driven by technological advances and the entry of foreign economic operators, has required robust regulatory frameworks to manage associated risks and protect consumers. Regulatory sandboxes provide a controlled environment for fin-tech companies to test new products under regulatory supervision, offering a crucial mechanism to address challenges such as data security and service continuity risks posed by foreign ICT service providers. This research is essential as it explores how these frameworks operate in Uganda compared to Kenya and the UK, identifying gaps and opportunities for regulatory improvement.

This research conducts a comparative analysis of Uganda's regulatory sandboxes in mobile money services, examining their alignment, challenges and risk mitigation strategies compared to the frameworks in Kenya and the United Kingdom. The paper discusses how Uganda's regulatory sandboxes align with international best practices, explores the coordination between national and regional legal frameworks, and critically evaluates digital financial risks in Uganda, particularly those linked to foreign ICT service providers. It also assesses the implications of these risks for service continuity and data security and suggests risk mitigation strategies based on successful practices from other jurisdictions.

The significance of this research lies in the valuable information it provides on how regulatory sandboxes can address unique challenges within Uganda’s DFS landscape, especially in terms of the integration of foreign economic operators and ICT service providers. By highlighting best practices from Kenya and the UK, the research contributes to a more robust, coordinated, and adaptive regulatory framework in Uganda that supports innovation while protecting consumer rights. These insights are crucial for forming policy reforms that can refine the regulatory approach of Uganda, ultimately improving the resilience and inclusion of the financial sector. Key terminologies used in this research include 'regulation sandboxes,' 'digital financial services,' and 'Consumer safety.'

The paper is structured into several sections. The first section provides an overview of regulatory sandboxes and their evolution in different jurisdictions. The second section examines the comparative analysis of regulatory sandboxes in Uganda, Kenya, and the United Kingdom, focussing on their structure, challenges, and alignment with best practices. The third section delves into the specific digital financial risks in Uganda,

particularly those associated with foreign ICT service providers. The final section proposes risk mitigation strategies based on successful practices from other jurisdictions, offering recommendations to improve Uganda's regulatory framework. This structured approach allows a comprehensive assessment of Uganda's regulatory landscape and the identification of actionable insights for policy improvements.

1.1 Background of the research

Uganda's financial sector has undergone significant transformation due to the rise of digital financial services (DFS), which are now essential for the country's efforts to grow economic and financial inclusion. Mobile money services such as MTN Mobile Money and Airtel Money[1] have been at the forefront, enabling unprecedented access to banking and payment services, especially among the unbanked and under-banked populations. MTN Mobile Money, launched in 2009, has grown to more than 15 million active users by 2023, making it the leading mobile money provider in Uganda. Similarly, Airtel Money, introduced shortly thereafter, serves over 10 million users, illustrating the sector's rapid expansion.[2]

However, the extensive adoption of DFS technologies requires a robust regulatory framework to manage associated risks. A key concern is 'risk-washing', a scenario where fintech risks are minimised under the guise of innovation, potentially compromising financial stability and consumer protection.[3] Regulatory sandboxes-controlled environments established to allow fintech companies to test innovative products under regulatory supervision offer a crucial mechanism to address these challenges.[4] Regulatory sandboxes also reduce regulatory barriers, offering startups a platform to test products with fewer constraints and ongoing regulatory guidance, promoting responsible innovation and financial inclusion in Uganda.[5]

The objectives of the research are to evaluate how Uganda's regulatory sandboxes align with international best practices, explore the challenges of coordinating national and regional legal frameworks, particularly with regard to digital financial risks associated with foreign ICT service providers, and evaluate the effectiveness of Uganda's risk mitigation strategies drawing insights from successful practices in other jurisdictions. These objectives align with the mandates outlined in the 2021 National Payment Systems Regulatory Sandbox Framework, which emphasises the promotion of innovative business models that improve financial inclusion, improve service quality, and establish robust consumer protection safeguards.[6]

[1] MTN Mobile Money <https://www.mtn.co.ug> accessed 15 April 2024.
[2] Airtel Money <https://www.airtel.ug accessed> accessed 15 April 2024.
[3] Eric Brown and Dóra Piroska, 'Governing Fintech and Fintech as Governance: The Regulatory Sandbox, Riskwashing, and Disruptive Social Classification' (2021) 27(1) New Political Economy 19-32.
[4] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 3(2).
[5] The National Payment Systems (Agents) Regulations 2021 No. 19, Regulation 6.
[6] Bank of Uganda, The National Payment Systems Regulatory Sandbox Framework 2021 in Uganda (2021).

The introduction of regulatory sandboxes has become a key regulatory innovation, allowing financial institutions and fintech startups to test new technologies in a controlled environment that balances innovation with consumer protection.[7] The importance of regulatory sandboxes extends beyond merely fostering innovation; they serve as a bridge between technology and regulation, enabling the regulatory environment to adapt to the evolving landscape of digital financial services.[8] In Uganda, regulatory sandboxes play a critical role in promoting financial inclusion, enhancing consumer protection, and supporting market stability by mitigating risks associated with unregulated innovations.[9]

This research uses a qualitative research design grounded in a review of the legal literature and desktop research methods. The comparative analysis focuses on Uganda's regulatory sandboxes in mobile money services, evaluating their alignment, challenges, and risk mitigation strategies with respect to Kenya and the United Kingdom. This approach enables an analysis of the potential hazards in digital finance in Uganda, specifically those related to foreign ICT service providers. The research design is anchored in doctrinal analysis, which systematically examines legal rules, principles, and precedents to identify how Uganda's sandbox regulations compare with international frameworks.[10]

Data collection involved a review of secondary sources, including academic articles, regulatory guidelines, legal statutes related to regulatory sandboxes. The sources were selected based on their relevance, credibility, and focus on digital financial services and regulatory environments. The collected literature was systematically analysed to identify patterns, key themes, and regulatory divergences across the jurisdictions studied.[11] This method enabled the identification of the effectiveness of Uganda's regulatory sandboxes in mitigating risks associated with foreign economic operators.

The analysis techniques included content and thematic analysis of qualitative literature collected from legal and regulatory documents. This facilitated a detailed examination of cross-jurisdictional insights, allowing research to highlight best practices and identify regulatory gaps that could be addressed by adapting successful strategies from other jurisdictions. The comparative analysis provided a structured approach to evaluating risk mitigation strategies within Uganda's sandboxes and aligning them with global standards.[12]

---

[7] Baker McKenzie, 'A Guide to Regulatory FinTech Sandboxes Internationally' (May 2020) <https://www.bakermckenzie.com/-/media/files/insight/publications/2020/05/a_guide_to_regulatory_fintech_sandboxes_internationally_8734.pdf?la=en>accessed 30 May 2024.

[8] ibid.

[9] Regulation 18 (n 5).

[10] Hilary J Allen, 'Regulatory Sandboxes' (2019) 87(3) Geo Wash L Rev <https://ssrn.com/abstract=3056993> or <http://dx.doi.org/10.2139/ssrn.3056993> accessed 30 April 2024.

[11] Baker McKenzie (n 7).

[12] AllahRakha Naeem, 'Regulatory Sandboxes: A Game-Changer for Nurturing Digital Start-Ups and Fostering Innovation' (2023) 3(8) Евразийский журнал права, финансов и прикладных наук 120, 128.

2 Overview of regulatory sandboxes

The terminology used in this research is essential to understand the context and scope of the research. 'Sandbox' refers to a provisional trial of innovative financial products, services, business models, or delivery methods within the payment systems ecosystem.[13] "Regulatory sandboxes" refer to controlled environments where financial service providers can test new products and services under regulatory supervision. "Consumer safety" refers to the measures and mechanisms in place to protect consumers from financial fraud, data breaches, and other risks associated with digital financial services. "Digital financial services" encompass a range of financial activities conducted through digital platforms, including mobile money transfer, online banking, and digital lending.[14]

Regulatory sandboxes are regulatory frameworks that allow fintech companies to test new products, services, and business models within a controlled environment under regulatory supervision. These sandboxes provide a 'safe space' for financial innovation while maintaining oversight to protect consumers and ensure compliance with regulatory standards. The concept was first introduced by the UK as part of its Project Innovate initiative, designed to support fintech companies in navigating the UK's complex regulatory landscape and gain market entry under regulatory guidance.[15] This approach has since become a benchmark globally, promoting technological advancement while safeguarding consumer interests and promoting financial inclusion.[16]

The evolution of regulatory sandboxes reflects a significant shift towards accommodating financial innovation while managing associated risks. The UK's Financial Conduct Authority (FCA) was the first to introduce this model in 2015, setting a precedent for other countries, including Kenya and Uganda, to adopt similar frameworks tailored to their regulatory priorities.[17] The sandbox has facilitated the testing of innovative financial products and services, allowing regulators to monitor real-time impacts and adjust regulations as necessary.[18] Sandboxes in Kenya emphasise stringent data protection protocols and licencing requirements, consolidating various regulatory guidelines under the Central Bank's supervision, while Uganda's sandbox still faces challenges in cross-border testing capabilities.[19]

[13] National Payment Systems Act (2020), Cap. 59, Section 1.
[14] United Nations Capital Development Fund, 'Digital Credit in Uganda: Where Are We, Where Do We Want to Go?' (UNCDF, 13 April 2021) <https://www.uncdf.org/article/8341/digital-credit-in-uganda-where-are-we-where-do-we-want-to-go> accessed 28 April 2024.
[15] Financial Conduct Authority, 'Annual Report 2015/16' (2015) <https://www.fca.org.uk/publication/corporate/annual-report-2015-16.pdf> accessed 19 August 2024.
[16] Allen (n 10) 580.
[17] Financial Conduct Authority (FCA) Regulations (United Kingdom); Financial Services Act (2012), (c 21), (United Kingdom).
[18] Ramona Rupeika-Apoga and Eleftherios I Thalassinos, 'Ideas for a Regulatory Definition of FinTech' (2020) VIII(2) International Journal of Economics and Business Administration 136, 154.
[19] Jackson Macharia Githu, *Legal & Regulatory Framework for Digital Financial Services in Kenya - A Case for Urgent Reforms* (KBA Centre for Research on Financial Markets and Policy Working Paper Series, Kenya Bankers Association, May 2023).

Types of Testing Grounds

Sandbox Environments

Sandbox environments are structured frameworks established by financial regulators, such as the central bank, to allow businesses to test innovative financial products or services in a controlled setting without obtaining a full licence, which is crucial to managing the balance between enabling innovation and ensuring consumer protection.[20]

Commonly referred to as regulatory "sandboxes," these programmes represent an attempt by authorities to build supervisory capacity through participation and state-sponsored innovation and experimentation. In some instances, sandboxes may be offered as part of a larger regulatory "Innovation Hub" designed to offer firms assistance with navigating compliance burdens and testing their ideas against specific real-world problems. The sandbox arguably provides a genuinely new addition to the regulatory arsenal, different from past practices on which policymakers have relied to accommodate financial innovation.[21]

The regulatory sandboxes in the UK similarly provide a "safe space" for experimentation. As noted by Christopher, they are designed to promote competitive innovation, market competition, and efficiency, particularly in fintech sectors.[22] The sandbox regime operates under specific criteria and minimum requirements, ensuring that all activities are closely monitored by the regulatory authorities. These environments typically require detailed applications that outline the scope of testing, which must be accessible and transparent to the regulator.

Beta Testing

Beta testing in the financial sector involves releasing a new product or service to a limited audience outside of the company but within the controlled environment of the sandbox, which is critical for gathering user feedback on the functionality of the product in real-world scenarios without the full regulatory burden.[23] Similar beta testing phases are integral to the regulatory sandboxes in the UK , and beta testing helps identify any potential issues or improvements, ensuring that the product meets both customer expectations and regulatory standards before wider release.[24]

[20] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 1.
[21] Chris Brummer and Yesha Yadav, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235 <https://ssrn.com/abstract=3054770 accessed 30 April 2024> accessed 29 April 2024.
[22] Christopher Chao-hung Chen, 'Regulatory Sandboxes in the UK and Singapore: A Preliminary Survey' in Mark Fenwick, Steven Van Uytsel, and Bi Ying (eds), *Regulating FinTech in Asia: Global Context, Local Perspectives* (Forthcoming, August 2020) <https://ssrn.com/abstract=3448901> or <http://dx.doi.org/10.2139/ssrn.3448901> accessed 29 April 2024.
[23] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 5(1)(d).
[24] Chen (n 22).

Pilot Programmes

Pilot programmes are a more extensive form of testing financial products or services, in which the product is introduced to a broader audience under real-world operating conditions, which is essential to observe the performance of the product and its interaction with other elements of the financial ecosystem.[25] Pilot programmes help to assess the overall impact and suitability of the product for larger-scale implementation. They are a critical step in confirming that the financial product not only adheres to regulatory standards but also fulfils its intended role in enhancing consumer safety and contributing to financial inclusion.

Together, these testing grounds play an essential role in fostering innovation within the regulatory framework, ensuring that new financial technologies can be safely integrated into Uganda's financial landscape, enhancing consumer protection, and promoting financial inclusion. The impact on consumer safety is an important objective of sandboxes globally.[26] Initiatives in Kenya, for example, have shown how sandbox environments can significantly enhance the safety and reliability of financial products before they are introduced to the wider market.[27]

2.1 Comparative analysis of regulatory sandboxes in Uganda, Kenya, and the UK

The landscape of regulatory sandboxes varies significantly across jurisdictions, with each model offering unique approaches to balancing innovation and regulatory oversight. In Kenya, the success of M-Pesa exemplifies how innovation can outpace regulatory frameworks. The necessity for dialogue between regulators and stakeholders in the FinTech ecosystem is critical, as demonstrated by Kenya's M-Pesa, highlighting how regulatory frameworks can often lag behind technological advancements and stifle innovation.[28] This underscores the importance of a proactive regulatory approach that accommodates the rapid evolution of mobile money services.

In contrast, the UK's regulatory sandbox model allows for the testing of innovative financial products in a controlled environment, offering a more agile response compared to the slower regulatory responses observed in Kenya.[29] This model emphasises collaborative interactions between innovators and regulators, enabling a dynamic approach to compliance and innovation that could enhance the competitive landscape for

[25] Seunghwan Kim and others, *Digital Money, Cross-Border Payments, International Reserves, and the Global Financial Safety Net: Preliminary Considerations* (IMF, 4 January 2024) eISBN 9798400253478.
[26] Baker McKenzie (n 7).
[27] World Bank, 'Global Experiences from Regulatory Sandboxes' (11 November 2020) <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912001605241080935/global-experiences-from-regulatory-sandboxes> accessed 28 April 2024.
[28] Anton Didenko, 'Regulating FinTech: Lessons from Africa' (2018) 19 San Diego Int'l L J 311.
[29] Johann Jacques Crouse, 'Fintech and the Financial Services Industry in South Africa' (Masters thesis, Nelson Mandela Universuty 2019).

mobile money services in Uganda. The UK approach serves as a benchmark, highlighting the potential benefits of a more flexible regulatory framework.

The landscape of online money services in Uganda has seen significant expansion, driven by the widespread adoption of mobile money platforms and electronic banking services. This growth is supported by a robust legal framework, including the Contract law, which outlines the essential elements of lawful agreements and ensures the enforceability of digital financial contracts.[30] This growth is largely attributed to the increased accessibility of mobile devices and the Internet, which have transformed the traditional banking scene into a more dynamic and user- friendly environment. This growth is corroborated by findings which highlight that 86% of micro-entrepreneurs own a mobile money account, yet only 49% are active users, indicating unmet opportunities in the sector.[31]

Agents operating under the regulations are required to maintain proper records of all transactions, ensuring transparency and accountability.[32] However, according to the UNCDF report, while digital financial services (DFS) have enabled more Ugandans to access formal financial services, the gains are still restricted to basic account services and payments. For instance, 66% of Ugandan adults are estimated to have access to an account, yet formal saving and borrowing remain low at 32% and 29%, respectively.[33] This pattern of growth is also evident in the UK, where regulatory sandboxes have facilitated the adoption of innovative financial technologies.[34] As a result, a substantial portion of Uganda's population now enjoys the convenience of digital transactions, ranging from simple money transfers to complex financial operations.

Uganda’s regulatory sandbox is closely aligned with international best practices, offering a testing ground for mobile money services to promote innovation while protecting consumer interests. However, differences arise due to unique market conditions and external influences, particularly in managing risks posed by foreign ICT service providers and economic operators.[35] While Kenya’s model integrates comprehensive consumer protection measures and consolidated regulatory oversight, Uganda’s framework remains less developed, lacking specific operational guidelines on cross-border testing.[36] Comparatively, the UK’s sandbox fosters a collaborative environment between regulators and innovators, allowing for incremental exposure to regulatory requirements, thereby enhancing compliance and innovation .[37]

Previous studies highlight that digital financial services pose significant risks, including data breaches, fraud, and compliance challenges, particularly with regard to foreign ICT

[30] Contracts Act (1963), Cap. 284 (Uganda), Section 10.
[31] Jana S Hamdan, Katharina Lehmann-Uschner and Lukas Menkhoff, 'Mobile Money, Financial Inclusion, and Unmet Opportunities: Evidence from Uganda' (2022) 58(4) The Journal of Development Studies 671.
[32] Regulation 12 (n 5).
[33] United Nations Capital Development Fund (n 14).
[34] Chen (n 22).
[35] Bank of Uganda (n 6).
[36] Allen (n 10).
[37] Rupeika-Apoga and Thalassinos (n 18).

service providers. These risks are prevalent in markets with evolving regulatory frameworks like Uganda, where legal and regulatory oversight often lags behind technological progress.[38] The law in Uganda mandates reporting of suspicious transactions, addressing threats like money laundering and ensuring service continuity and data security.[39] These studies underscore the importance of sandboxes in mitigating these risks, facilitating a balanced approach to innovation and regulation through controlled testing environments.[40]

By examining the successful practices of the UK and Kenya, this research aims to propose tailored risk mitigation strategies to enhance Uganda's regulatory framework, improve data security, and ensure the continuity of digital financial services.

3 Structure and Function of Uganda's Regulatory Sandbox and Online Money Services

Uganda's regulatory sandbox, provides a critical mechanism for promoting innovation within the digital financial services sector.[41] This sandbox offers a controlled environment in which fintech companies and other digital financial service providers can test new products, services, and business models under regulatory supervision before they are introduced to the market. The primary objectives of the sandbox include increasing the potential for innovative business models that advance financial inclusion, improving competition and service quality, and implementing consumer protection safeguards.[42]

Uganda's sandbox framework is designed to meet the specific market needs of the country, allowing fintech companies to operate temporarily with reduced regulatory restrictions. This approach encourages technological innovation while maintaining market integrity through stringent oversight measures. Regulatory authorities enforce data protection standards, requiring all participants to implement secure data handling procedures, which safeguard consumer information and ensure compliance with existing financial regulations.[43]

Popular Platforms

Among the most popular platforms that facilitate digital financial services in Uganda are mobile money systems, which enable users to store, send, and receive money through their mobile phones. Leading the market is MTN Mobile Money, launched in 2009, which has become the country's foremost mobile money provider with over 15 million active users as of 2023. This platform offers a variety of services, including money transfers, bill

[38] United Nations Capital Development Fund (n 14).
[39] Anti-Money Laundering Act (2013), Cap 118 (Uganda), Section 6A and 9.
[40] Naeem (n 12).
[41] National Payment Systems Regulatory Sandbox Framework 2021.
[42] Bank of Uganda (n 6).
[43] Regulation (n 4).

payments, and savings options, making it a vital tool for both urban and rural populations in Uganda. The United Nations Capital Development Fund (UNCDF) has extensively documented the significant impact of MTN Mobile Money on financial inclusion, noting its role in providing accessible financial services to the unbanked and under-banked segments of the population.[44]

Airtel Money, another prominent platform introduced shortly after MTN Mobile Money, has also established a substantial presence in Uganda's digital financial landscape. With a wide range of services, such as money transfers, utility bill payments, and school fees payments, Airtel Money caters to millions of users across the country. The research of GSMA highlights the contribution of Airtel Money to financial inclusion, highlighting its ease of use and comprehensive service offerings, and integration with traditional banking services has further enhanced its usability, making it a cornerstone of financial activities for many Ugandans.[45]

The regulatory framework in Uganda has played a crucial role in supporting the growth and adoption of these mobile money platforms. The Bank of Uganda's Financial Stability Reports regularly underscore the importance of mobile money services like MTN Mobile Money, and Airtel Money in the country's financial ecosystem.[46] The law, along with its accompanying regulations, provides a robust legal foundation that ensures the security and reliability of mobile money services.[47] These regulations mandate strict compliance with customer due diligence protocols, transaction limits, and liquidity requirements, thereby maintaining the stability and trustworthiness of these platforms.[48] Consequently, mobile money systems have become integral to everyday financial activities for many Ugandans, significantly contributing to the country's financial inclusion efforts. The integration of mobile money services with traditional banking services has further

[44] United Nations Capital Development Fund, 'Digital Financial Services in Uganda: Status and Opportunities' (2022) <https://www.uncdf.org> accessed 30 April 2024; International Finance Corporation, 'Building Resilience Through Digital Financial Services: Uganda' (IFC 2022) <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099048506102239760/idu015b939b60217b045f0094060078519414c2d> accessed 1 May 2024; World Bank, 'The Impact of Mobile Money on Poor Rural Households' (World Bank 2019) <https://documents1.worldbank.org/curated/zh/134341561467884789/pdf/The-Impact-of-Mobile-Money-on-Poor-Rural-Households-Experimental-Evidence-from-Uganda.pdf> accessed 1 May 2024.

[45] Ali Ndiwalana, Olga Morawczynski, and Oliver Popov, 'Mobile Money Use in Uganda: A Preliminary Study' (2023) <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2012/06/m4dmobilemoney.pdf> accessed 1 May 2024; GSMA, '2020 Impact Innovation Award in Digital Wallets: Airtel Money Uganda' (GSMA 2020) <https://www.gsma.com> accessed 1 May 2024 accessed 10 October 2024; The Monitor, 'Airtel Money Bags Two Digital Impact Awards' *The Monitor* (18 November 2022) <https://www.monitor.co.ug/uganda/business/technology/airtel-money-bags-two-digital-impact-awards-4031888> accessed 1 April 2024.

[46] Bank of Uganda, 'Financial Stability Report' (Bank of Uganda 2023) <https://archive.bou.or.ug/bou/download_archive.html?path=/bou/bou-downloads/financial_stability/&title=Publications&subtitle=Financial%20Stability%20Reports&restype=binary&secname=Financial%20Stability%20Report&year=Rpts&month=All> accessed 1 April 2024.

[47] National Payment Systems Act (2020), Cap. 59.

[48] GSMA, 'State of the Industry Report on Mobile Money' (GSMA 2023) <https://www.gsma.com/sotir/wp-content/uploads/2024/03/GSMA-SOTIR-2024_Report.pdf> accessed 1 April 2024.

improved their usability, making them a cornerstone of everyday financial activities for many Ugandans.[49]

Current Regulations

The regulatory framework that governs online money services in Uganda is designed to ensure the safety and reliability of these services.[50]As per the law, agreements must have legal consideration and objectives, and this forms the basis for establishing secure customer registration systems and other regulatory requirements.[51] Similarly, the Kenyan regulatory approach, governed by the National Payment Systems Act and the Banking Act, provides detailed guidelines on payment service providers, requiring strict compliance with licencing, consumer protection and data security measures.[52] This comprehensive regulatory oversight has ensured that both markets prioritise consumer safety, although the Kenyan model also emphasises the need for harmonisation of regulations across various financial service providers to avoid regulatory overlaps and inefficiencies.[53]

The legal effects of electronic records, the authenticity of data messages and the retention of information or records are provided for by law, and the importance of robust security measures and the duty of care of financial institutions was underscored in the case of ***Aida Atiku v Centenary Rural Development Bank Limited***.[54]The court held that the bank is not liable for unauthorised transactions if it can demonstrate that it has implemented commercially reasonable security procedures. This ruling emphasises the need for financial institutions and customers to follow security protocols to reduce fraud risks.[55] Regulatory sandboxes according to Hilary, help in balancing the promotion of financial innovation with the need for consumer protection and financial stability by allowing limited tests of fintech products under regulatory supervision.[56]

The subsequent regulations outline stringent measures for electronic money issuers, including liquidity requirements, transaction limits, and customer due diligence protocols.[57] Additionally, the law ensures that access to computer systems and data is secure and authorised, further enhancing the legal framework.[58] In addition, guidelines that provide clarity on mobile money services, stipulate roles and responsibilities, and foster consumer protection also exist.[59] Despite these regulations, the UNCDF highlights that traditional lending methods still pose significant barriers for the informal sector.

[49] Financial Institutions Act (1993), Cap. 57 (Uganda), Section 3.
[50] The National Payment Systems (Sandbox) Regulations, 2021.
[51] Contracts Act (1963), Cap. 284 (Uganda), Section 19.
[52] Banking Act (,1995), Cap 488, (Kenya); National Payment Systems Act (2011), (Kenya).
[53] Githu (n 19).
[54] Electronic Transactions Act (2011), Cap.99 (Uganda), Section 5, 7, and 9.
[55] Civil Suit No. 0754 of 2020.
[56] Allen (n 10).
[57] National Payment Systems Regulations, 2021 No. 18, Part III, Regulation 17-18; Financial Institutions Act (1993), Cap. 57 (Uganda), Section 12.
[58] Computer Misuse Act (2011), Cap. 96, Section 3, 4, and 5.
[59] Bank of Uganda (BOU) Mobile Money Guidelines, 2013.

Digital credit, an emerging fintech model in Uganda, offers a potential solution, but is still in its early stages and is primarily focused on consumer lending.[60]

The guidelines mandate electronic money issuers to establish secure customer registration systems that provide proof of successful registration and ensure the activation of accounts through secure processes.[61] Additionally, the it emphasises the importance of maintaining the integrity and security of the activation process, thereby safeguarding consumer interests and enhancing trust in digital financial services. The Bank of Uganda empowers the bank to supervise, regulate, control, and discipline all financial institutions, ensuring the integrity and security of their operations.[62] For example, the law details the regulations for electronic money issuance and circulation, including customer due diligence requirements and transaction limits.[63]

These regulatory measures are crucial in promoting a safe environment for the adoption and growth of online money services, ensuring that both service providers and consumers operate within a framework that supports financial inclusion while protecting consumer rights and data.[64] Penalties for breaches of these regulations, as outlined in the Regulations, ensure strict adherence and accountability among agents and principals.[65] In the case of ***Kayondo v Bank of Uganda***, the High Court ruled on issues related to the Bank of Uganda's regulatory directives affecting cryptocurrency transactions. This case highlights the regulatory complexities and the importance of clear guidelines and consultations with industry stakeholders to avoid arbitrary and irrational regulatory actions, as emphasised in the judgment.[66]

In the case of ***Katuntu v MTN Uganda Ltd & Anor***, the plaintiffs challenged the proper operation and regulation of mobile money services provided by telecommunications companies, arguing that these services should be classified as financial services and subject to stricter regulatory oversight. The court's ruling underscored the necessity of stringent regulatory measures to protect consumers, similar to those outlined in the National Payment Systems Act, 2020, which mandates secure customer registration and transaction processes to enhance consumer trust and safety in digital financial services.[67]

3.1 Comparison with Kenya's and the UK's Frameworks

Comparatively, Kenya's regulatory sandbox, mirrors Uganda's objectives of fostering innovation and improving consumer protection.[68] However, Kenya's framework integrates

[60] United Nations Capital Development Fund (n 14).
[61] Bank of Uganda Financial Consumer Protection Guidelines, 2011, Part II, Paragraph 5; Electronic Signatures Act 7 of 2011.
[62] Bank of Uganda Act (1993), Cap. 54 (Uganda), Section 4(2)(j).
[63] National Payment Systems Act (2020), Cap. 59, Section 47-60.
[64] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 12.
[65] Regulation 23 (n 5).
[66] (Miscellaneous Cause No. 109 of 2022) [2023] UGHCCD 113 (24 April 2023).
[67] (HCCS 248 of 2012) [2015] UGCommC 83 (29 May 2015).
[68] Central Bank of Kenya (Digital Credit Providers) Regulations (2022).

a more comprehensive approach by consolidating diverse regulatory guidelines under a unified oversight, which addresses data security and licencing requirements for digital lenders, providing a more streamlined regulatory environment.[69] This consolidation strengthens Kenya's position in managing data security challenges that are prevalent in the fintech sector.[70]

The UK's regulatory sandbox, established by the Financial Conduct Authority as part of its Project Innovate initiative, is a pioneer in the regulatory sandbox landscape. The UK model emphasises collaborative interactions between innovators and regulators, facilitating a proactive approach to compliance and innovation. Unlike the Ugandan sandbox, the UK framework allows cross-border testing, enhancing its effectiveness in managing the global nature of fintech innovations. This international focus enables the UK to set a precedent for other jurisdictions, highlighting the importance of flexible regulatory environments that adapt to rapid technological changes.[71]

3.2 Coordination between national and regional legal frameworks

Coordinating legal frameworks in Uganda, Kenya, and the UK presents significant challenges, particularly in aligning regulatory standards for fintech operations. Uganda's regulatory sandbox, while effective in domestic settings, lacks clear guidelines for cross-border testing, limiting its applicability compared to more developed models such as those of the UK. The absence of such operational guidelines restricts Uganda's ability to fully integrate its sandbox framework within regional and international contexts, posing challenges for fintech firms that want to scale their operations across borders.[72]

The different regulatory approaches in East Africa further complicate harmonisation efforts, with the consolidated Kenya framework offering a more unified regulatory approach compared to the segmented structure of Uganda. This disjointed regulatory landscape creates compliance challenges and reduces the effectiveness of cross-border financial services, underlining the need for coordinated efforts to align national sandboxes with regional best practices. Enhanced cooperation and standardisation are crucial to improving the regulatory landscape, promoting innovation, and ensuring robust consumer protection across jurisdictions.[73]

Uganda's regulatory sandbox plays a vital role in the advancement of digital financial services by providing a controlled environment for innovation. However, to fully exploit its potential, Uganda must improve its framework by adopting successful Kenyan and United Kingdom practices, focussing on improving the coordination of national and

[69] National Payment Systems Act (2011) (Kenya), Section 3.
[70] Githu (n 19).
[71] Rupeika-Apoga and Thalassinos (n 18).
[72] Ahmad Alaassar, Anne-Laure Mention, and Tor Helge Aas, 'Exploring a New Incubation Model for FinTechs: Regulatory Sandboxes' (2021) 103 Technovation 102237.
[73] Naeem (n 12).

regional legal frameworks. This will enable Uganda to effectively address digital financial risks, particularly those related to foreign ICT service providers, and to improve data security and service continuity within its rapidly evolving financial sector.

4 Digital Financial Risks in Uganda

Uganda's digital financial services (DFS) sector, heavily dependent on foreign ICT service providers, faces significant risks related to data security, service continuity, and regulatory gaps. A primary risk involves the management of sensitive financial data by foreign entities, which may not fully align with Uganda's local data protection regulations, thus exposing the sector to potential data breaches and unauthorised access. These security vulnerabilities are exacerbated by the inconsistent global regulatory standards, which can create loopholes in the protection of consumer data held by foreign service providers.[74]

Another critical concern is the risk of service continuity, arising from the dependence on foreign ICT infrastructure that might not be fully compliant with Uganda's operational standards. Interruptions in the ICT providers' networks due to cyberattacks, technical malfunctions, or geopolitical influences can severely disrupt financial services, impacting millions of mobile money users.[75]

Regulatory gaps also present a substantial risk, particularly in the oversight of foreign ICT providers. The cross-border nature of these services complicates the enforcement of compliance with Ugandan laws, increasing exposure to unregulated practices that could undermine service reliability and data security. For example, the law requires financial institutions to conduct comprehensive risk assessments and implement appropriate measures to manage these vulnerabilities, underscoring the importance of stringent regulatory oversight.[76]

The implications of these identified risks are profound and directly affect service continuity and data security in the financial landscape of Uganda. Disruptions caused by ICT failures or security breaches not only lead to financial losses, but also erode consumer trust and threaten the stability of the entire DFS ecosystem. According to the law, stringent measures such as mandatory reporting and ongoing risk assessments are vital to mitigate the risks posed by foreign ICT service providers.[77]

Data security breaches, in particular, expose consumers to fraud and identity theft, further compromising the integrity of digital financial services. Regulatory sandboxes, such as those established under the 2021 National Payment Systems Regulatory Sandbox Framework, play a crucial role in addressing these issues by allowing the controlled testing

[74] Regulation (n 4).
[75] The National Payment Systems Regulatory Sandbox Framework 2021 in Uganda.
[76] Anti-Money Laundering Act (2013), Cap 118 (Uganda), Section 6A and 9.
[77] ibid.

of new technologies in compliance with local security standards before their public release.[78]

Comparative analysis with the UK and Kenya reveals that although Uganda's regulatory frameworks share some alignment with international best practices, they still fail to manage specific risks related to foreign ICT service providers. The UK's sandbox model emphasises collaborative interactions between regulators and service providers, creating a secure testing environment that balances innovation with stringent compliance requirements, offering a potential pathway for Uganda to strengthen its regulatory approaches.[79]

5 Risks Posed by Foreign Economic Operators

The entry of foreign economic operators into Uganda's digital financial services, particularly in the mobile money sector, has reshaped the dynamics of the local market. Although these entities introduce advanced technologies and significant capital investment, they also pose risks, such as market dominance, data privacy breaches, and disruptions to service continuity that can compromise local market resilience. Foreign firms often exploit regulatory inconsistencies between national and regional frameworks, thus disadvantaging local companies that lack similar resources and influence. For example, the participation of international technology companies in Uganda's mobile money market has intensified competition but raised concerns about data security and consumer privacy. These foreign entities often control critical infrastructure and manage large volumes of sensitive customer data, which are vulnerable to exploitation if they are not adequately protected under Uganda's legal jurisdiction.

In Kenya, similar issues have arisen with the influence of foreign economic operators in shaping the digital financial sector. The regulatory measures of the Central Bank of Kenya, such as the 2022 Digital Credit Providers Regulations, were introduced to address concerns about data privacy and prevent exploitation by foreign companies, setting a precedent that Uganda could follow.[80] In Kenya, the dominance of foreign-influenced companies such as Safaricom highlights the challenges local markets face. Safaricom's significant market share has led to regulatory interventions to address concerns about monopolistic behaviour and consumer data security, including data localisation mandates and stricter consumer protection rules.[81]

The UK has also managed similar risks associated with foreign fintech operators. The Financial Conduct Authority has established stringent compliance requirements that

[78] Bank of Uganda, The National Payment Systems Regulatory Sandbox Framework 2021 in Uganda.
[79] Data Protection Act (2018), (c 12), (United Kingdom); Allen (n 10).
[80] Central Bank of Kenya (Digital Credit Providers) Regulations (2022).
[81] Githu (n 19).

include comprehensive vetting processes and ongoing supervision to ensure that foreign firms adhere to local data protection and anti-money laundering standards.[82]

These examples illustrate the importance of a robust regulatory framework that not only fosters innovation, but also mitigates the risks posed by foreign economic operators. Drawing lessons from Kenya and the UK, Uganda can improve its regulatory landscape to better protect local markets and ensure the integrity of consumer data.

6 Key regulatory challenges in Uganda

Technical Barriers

Implementing regulatory sandboxes in Uganda faces significant technical barriers. Although the law details the licencing requirements, corrective actions, and regulatory sandbox framework, one of the primary challenges is the integration of new financial technologies with existing systems.[83] Concerns have also been raised about the implications of mobile money for the conduct of monetary policy in Uganda.[84] The adoption and use of mobile money imply a gradual substitution of real cash balances for bank deposits, which often requires substantial upgrades to the current infrastructure, which can be costly and time consuming.[85] Clear and enforceable contracts, as outlined in the contract law, particularly regarding the capacity to contract, play a crucial role in mitigating these challenges by ensuring that all parties are legally competent and their agreements are binding.[86]

The Bank of Uganda's oversight framework, as outlined in the National Payment Systems Oversight Framework, addresses these challenges through a cooperative oversight approach, involving collaboration with other domestic and cross-border authorities.[87] This cooperation helps to align new technologies with existing regulatory requirements, thereby facilitating smoother integration and ensuring the robustness of Uganda's payment systems. In addition, there is the challenge of ensuring that these new technologies are secure and can handle the complexities of real-world financial transactions without failure. Similar challenges are observed in other regions, such as the UK. In his research, Christopher highlights that "the sandbox approach can buy some time for regulators, incumbent financial institutions, and new technology firms to try out new services with minimal legal risk".[88]

[82] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, (2017) (SI 2017/692), (United Kingdom); Rupeika-Apoga and Thalassinos (n 18).
[83] National Payment Systems Act (2020), Cap. 59, Sections 7-13 and 16-18.
[84] Brown and Piroska (n 3).
[85] Joseph Mawejje and Paul Lakuma, 'Macroeconomic Effects of Mobile Money: Evidence from Uganda' (2019) 5 Financial Innovation 23 <https://doi.org/10.1186/s40854-019-0141-5> accessed 30 April 2024; National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 5(1)(a); Bank of Uganda (BOU) Mobile Money Guidelines, 2013.
[86] Contracts Act (1963), Cap. 284 (Uganda), Section 11.
[87] Bank of Uganda, The National Payment Systems Oversight Framework (June 2021).
[88] Chen (n 22).

Another prominent challenge is to address the risks posed by foreign ICT service providers, which often operate under varying legal conditions that can conflict with local data protection and consumer safety laws. Uganda's framework struggles to harmonise its regulations with broader regional and international standards, highlighting the critical need for regulatory reforms that address these specific challenges. [89]

Another technical hurdle is the development of systems that can effectively monitor and evaluate the performance of new services within the sandbox. These systems must not only track performance, but also ensure compliance with regulatory standards, which can vary significantly from one service to another.

Regulatory Hurdles

Regulatory hurdles also pose a significant challenge in the implementation of testing grounds. Existing legal frameworks may not always be adaptable to the flexible nature required by sandboxes. For example, laws, guidelines, and regulations can provide a structured regulatory environment, but may need amendments to accommodate the dynamic testing of financial technologies in a sandbox setting. For example, the guidelines provide a requirement for the suitability of advice and ensure that the financial products recommended to consumers are appropriate. [90] Furthermore, the process of obtaining approval for sandbox operations involves navigating through extensive bureaucratic procedures. Sandboxes in South Korea have also faced similar technical and regulatory hurdles, necessitating extensive coordination among regulators and iterative improvements to the sandbox framework. This can delay the launch of innovative projects, discourage stakeholders and potentially hinder innovation.[91]

The decision in the case of ***Kayondo v. Bank of Uganda*** underscores the importance of regulatory clarity and proper stakeholder participation in the implementation of financial regulations. The court's findings on the procedural flaws and irrationality in the Bank of Uganda's directives provide critical insight into the need for a more adaptable and consultative regulatory approach to support innovation without compromising legal propriety.[92]

User scepticism

User scepticism is another critical challenge. The ruling in ***Aida Atiku v Centenary Rural Development Bank Limited*** illustrates the consequences of negligence on the part of the customer. The court held that the customer, who allowed a third-party access to his device and security information, was at risk of unauthorised transactions. This case highlights the importance of user adherence to security protocols and the need for

[89] Anti-Money Laundering Act (2013), Cap 118 (Uganda), Sections 6A and 9.
[90] Bank of Uganda Financial Consumer Protection Guidelines, 2011, Part II, Paragraph 6(3)(a).
[91] World Bank (n 27).
[92] (Miscellaneous Cause No. 109 of 2022) [2023] UGHCCD 113 (24 April 2023).

continuous consumer education on the risks associated with digital financial services.[93] Despite the potential benefits of new financial technologies tested in regulatory sandboxes, users may be hesitant to adopt these innovations due to concerns about their security and reliability.[94] Building user trust requires transparent operations within the sandbox, clear communication of the benefits, and demonstration of robust security measures to protect user data and transactions.

Additionally, there is a need for ongoing education and awareness campaigns to help users understand how these new technologies work and the safeguards put in place to protect their interests.[95] Without strong user buy-in, even the most innovative financial products may see limited adoption, undermining the objectives of financial inclusion and market competition.[96]

6.1 Analysis of the legal framework: Uganda, Kenya, and the UK

The regulatory sandbox frameworks in Uganda, Kenya, and the UK demonstrate both convergences and divergences in their approaches. Uganda's regulatory sandbox is governed by the law and its accompanying regulations, which establish a legal foundation for controlled testing environments for financial innovations. However, the framework lacks clear guidelines on cross-border testing, limiting its effectiveness in a broader international context.[97]

Kenya's approach, defined under the Regulations, consolidates various regulatory guidelines under the Central Bank's supervision, addressing critical issues of data security and regulatory compliance.[98] In contrast, the UK's sandbox, introduced by the law as part of its Project Innovate initiative, emphasises collaborative regulation and tailored exemptions that support fintech innovation while protecting consumer interests.[99]

The analysis underscores that Uganda needs to adopt more adaptive regulatory measures, learning from the UK's customised sandbox programmes, which strike a balance between fostering innovation and maintaining robust consumer protections.[100]

[93] Civil Suit No. 0754 of 2020.
[94] Radostina Parenti, 'Regulatory Sandboxes and Innovation Hubs for FinTech: Impact on Innovation, Financial Stability and Supervisory Convergence' (Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf> accessed 30 April 2024.
[95] National Payment Systems (Consumer Protection) Regulations, (2022) No. 103, Regulation 9.
[96] Jimmy Ebong and Babu George, 'Financial Inclusion through Digital Financial Services (DFS): A Study in Uganda' (2021) 14(393) Journal of Risk and Financial Management 393.
[97] National Payment Systems Act (2020), Cap. 59, Section 16.
[98] Githu (n 19).
[99] Rupeika-Apoga and Thalassinos (n 18).
[100] Allen (n 10).

6.2 Operational Challenges in Implementing Regulatory Sandboxes

Operational challenges in implementing sandboxes in Uganda include limited regulatory capacity, insufficient technical expertise among regulators, and inadequate collaboration between the government and private sector innovators.[101] Furthermore, the absence of standardised evaluation metrics for innovations can lead to extended testing phases, further complicating the process of bringing fintech solutions to market.[102]

The lack of defined feedback and engagement mechanisms between regulators and participants further restricts the ability of the sandbox to evolve in response to technological advancements. There is a pressing need for Uganda to incorporate best practices from Kenya and the United Kingdom, focussing on better coordination across legal frameworks, streamlined testing procedures, and capacity building initiatives for regulators and participants.[103]

7 Overview of Risk Mitigation Approaches in Regulatory Sandboxes

Regulatory sandboxes serve as essential tools for managing the risks associated with digital financial services (DFS) by providing a controlled environment in which new technologies can be tested under regulatory oversight. In Uganda, these sandboxes help mitigate risks related to foreign ICT service providers, economic operators, and digital financial products, striking a balance between innovation and consumer protection. Successful sandbox implementations in other jurisdictions, such as the UK and Kenya, provide information on effective risk mitigation strategies that Uganda can adopt.

In the UK, the Financial Conduct Authority operates a sandbox that emphasises proactive interactions between regulators and innovators. This approach allows companies to test compliance and operational aspects incrementally, thus minimising systemic risks and consumer harm.[104] Similarly, the Kenyan Sandbox, regulated by the Central Bank, mandates rigorous data protection and consumer safety standards, requiring digital lenders to comply with stringent data security protocols and licencing requirements to protect consumer interests.[105]

Monitoring and compliance

Financial regulators in Uganda play a crucial role in monitoring and ensuring compliance within the digital financial services sector.[106] Their main responsibility is to supervise the activities of electronic money issuers and ensure that they comply with the regulations

[101] ibid.
[102] National Payment Systems Regulatory Sandbox Framework 2021 in Uganda.
[103] Bank of Uganda, The National Payment Systems Regulatory Sandbox Framework 2021.
[104] Allen (n 10).
[105] Githu (n 19).
[106] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 4(1)(d).

set forth in the law.[107] This includes overseeing the functions of the central bank, enforcing licensing requirements, and monitoring payment systems.[108] This includes monitoring the daily and weekly submissions by electronic money issuers of reconciliation statements and reports on the balances in trust accounts.[109] Regulators are also tasked with overseeing the security and integrity of electronic money services, ensuring that activation processes are secure and that customer identities are protected during transactions. In addition, the law requires the recording and reporting of cash and monetary transactions to prevent money laundering activities, thereby supporting the regulatory framework's aim to safeguard financial integrity.[110] The Bank of Uganda, under its mandate, advises and informs the Government on financial matters, ensuring compliance with established standards.[111]

The Katuntu case further illustrated the critical role of financial regulators in the oversight of mobile money services to ensure that they operate within legal frameworks and protect consumer interests. The court's decision in this case reinforced the importance of regulatory bodies in maintaining the integrity and security of financial transactions, which aligns with the responsibilities outlined for regulators in the law.[112]

Guidelines

Regulators develop and enforce guidelines that govern the digital financial landscape.[113] In Uganda, the regulatory framework governing digital financial services is designed to ensure both stability and consumer protection. This framework includes specific guidelines developed and enforced by the Bank of Uganda, which is the central authority responsible for the oversight of the financial sector. Furthermore, the regulation of trust accounts, which requires approval from the Bank of Uganda, provides an additional layer of security for customer funds, mitigating the risks associated with mismanagement or fraud.[114]

Consumer protection is another critical aspect of Uganda's regulatory framework. The National Payment Systems Act requires transparency, accountability, and data protection measures for electronic money issuers. These issuers must fully disclose service-related information and protect consumers from unfair trade practices. Complementing these efforts, the law requires financial institutions to maintain accurate records of electronic funds transfers, thus improving accountability and ensuring that financial transactions

[107] Financial Institutions Act (1993), Cap. 57 (Uganda), Section 62 and 64; Bank of Uganda Financial Consumer Protection Guidelines, 2011, Part II, Paragraph 5.
[108] National Payment Systems Act (2020), Cap. 59, Sections 4-15 and 19-23; Parma Bains and Caroline Wu, 'Institutional Arrangements for Fintech Regulation: Supervisory Monitoring' (26 June 2023) eISBN 9798400245664.
[109] Electronic Transactions Act (2011), Cap.99 (Uganda), Section 8 and 10.
[110] Anti-Money Laundering Act (2013), Cap 118 (Uganda), Section 8.
[111] Bank of Uganda Act (1993), Cap. 54 (Uganda), Section 32(1).
[112] *Katuntu v MTN Uganda Ltd & Anor* (HCCS 248 of 2012) [2015] UGCommC 83 (29 May 2015).
[113] Bank of Uganda (BOU) Mobile Money Guidelines, 2013; Bank of Uganda Financial Consumer Protection Guidelines, 2011.
[114] National Payment Systems Act (2020), Cap. 59.

adhere to stringent standards of transparency and data integrity. [115] In the event of fraud or security breaches, they are required to report these incidents promptly to the central bank. Laws, guidelines, and regulation further improve consumer safety by requiring robust systems for the integrity and security of customer transactions. [116] These measures collectively ensure that consumers are well protected in the digital financial landscape.

Efforts to promote financial inclusion are also embedded in Uganda's regulatory guidelines. Policies aimed at expanding mobile money networks into rural areas, reducing transaction fees, and improving financial literacy are vital to overcome barriers to financial access. These initiatives are supported by various studies and reports, such as those by the United Nations Capital Development Fund (UNCDF), which highlight the importance of expanding financial services to underserved populations.[117] The comprehensive approach taken by the Bank of Uganda in developing and enforcing these guidelines underscores the commitment to creating a secure, inclusive, and stable digital financial ecosystem in Uganda.[118]

Guidelines also include setting liquidity requirements and transaction limits as prescribed under the National Payment Systems Act. These guidelines ensure that electronic money issuers maintain sufficient liquidity to meet their obligations and impose limits to manage risks effectively. Furthermore, policies regarding the opening and operation of trust accounts are strictly regulated and require approval from the central bank to ensure proper management and safeguarding of customer funds. The research emphasised the importance of policy measures such as expanding mobile money networks in rural areas, reducing transaction fees, and improving financial literacy to overcome barriers to financial inclusion.[119]

7.1 Successful Practices of Other Jurisdictions

The UK's regulatory sandbox, developed by the Financial Conduct Authority (FCA), provides a collaborative environment that encourages engagement between regulators and fintech companies. This model allows fintechs to test innovative solutions while gradually complying with regulations, facilitating real-time identification of potential risks before broader market deployment. One of the successful practices includes the issuance

[115] Anti-Money Laundering Act (2013), Cap 118 (Uganda).
[116] Bank of Uganda, Mobile Money Guidelines 2013; National Payment Systems (Consumer Protection) Regulations 2022, SI 103; Bank of Uganda, 'Mobile Money Guidelines 2013' (Bank of Uganda 2013) <https://www.bou.or.ug/bouwebsite/bouwebsitecontent/acts/other_acts_regulations/Mobile-Money-Guidelines-2013.pdf> accessed 5 April 2024; National Payment Systems (Consumer Protection) Regulations 2022, SI 103 <https://www.bou.or.ug/bouwebsite/PaymentSystems/legal.html> accessed 5 April 2024.
[117] UNCDF, 'Digital Financial Services for Development' (UNCDF 2023) <https://www.uncdf.org/article/3521/digital-financial-services-in-uganda> accessed 5 April 2024.
[118] Bank of Uganda, Regulatory Sandbox Framework Bank <https://www.bou.or.ug/bouwebsite/bouwebsitecontent/MediaCenter/press_releases/2021/Jun/BoU-Launches-a-Regulatory-Sandbox-Framework.pdf> accessed 5 April 2024.
[119] Jana S Hamdan, Katharina Lehmann-Uschner and Lukas Menkhoff (n 31).

of tailored regulatory waivers that allow companies to innovate under specific conditions without the immediate burden of full compliance.[120]

The Kenyan regulatory sandbox emphasises consumer protection and data security through stringent requirements outlined in the Regulations.[121] This framework ensures that sandbox participants adhere to rigorous data protection standards, providing a secure environment for testing new digital financial products. The focus of the Kenyan model on aligning sandbox operations with national and regional regulations has been effective in managing cross-border risks and improving the resilience of the financial ecosystem.[122]

7.2 Recommendations for the Ugandan regulatory framework

Adopt collaborative regulatory approaches: Uganda should improve collaborative efforts between regulators and innovators, drawing on the model of the United Kingdom, which promotes ongoing consultation and feedback within the sandbox. This approach helps identify compliance issues early and aligns innovative activities with regulatory standards.

Strengthen Data Protection and Consumer Protections: Using Kenya's focus on stringent data protection measures, Uganda should ensure that all participants in the sandbox implement robust security protocols to protect consumer data. Enhancing data protection will mitigate the risks associated with cyber threats and unauthorised access to data.

Develop Cross-Border Testing Guidelines: Uganda should incorporate cross-border testing provisions into its regulatory framework, establishing protocols that facilitate cooperation with regional regulators. This will improve Uganda's ability to manage international risks effectively, particularly those associated with foreign ICT service providers.

Implement Incremental Compliance Measures: Uganda could introduce incremental compliance requirements, similar to the UK approach, allowing companies to gradually meet regulatory obligations. This strategy fosters a more adaptive regulatory environment, supporting innovation while maintaining high standards of consumer protection.

These recommendations aim to strengthen Uganda’s regulatory sandboxes, ensuring that they support financial innovation while effectively mitigating risks in the landscape of digital financial services.

[120] Baker McKenzie (n 7).
[121] Central Bank of Kenya (Digital Credit Providers) Regulations (2022).
[122] Githu (n 19).

8 Key Features and Benefits of Regulatory Sandboxes

Regulatory sandboxes provide a controlled environment that enables fintech companies to test new products and services under regulatory supervision without the full regulatory burden that would normally apply. This safe space promotes innovation while allowing regulators to monitor and manage the risks associated with emerging technologies. In Uganda, the sandbox framework facilitates experimentation with digital financial services (DFS), specifically mobile money, by providing customised regulatory guidance and temporary exemptions from standard regulations, thus improving service continuity and data security. The regulations specifically outline the procedures and criteria for participating in the sandbox, emphasising the importance of maintaining market integrity during the testing phase.[123] Unlike other countries, the UK's sandbox approach promotes proactive regulator-innovator contacts, creating a collaborative environment that balances innovation and regulation. These interactions allow companies to offer goods slowly while meeting regulatory requirements, eliminating financial system disruptions. Kenya's sandbox allows digital credit providers to test compliance and security before launching new services.

Regulatory sandboxes include consumer protection to ensure that creative goods meet data security and consumer rights standards from the start. Electronic money issuers must comply with central bank consumer protection regulations, such as transparency, accountability, and data protection. The law mandates the transparency of the payment system and the protection of consumers' data. These standards protect users from unfair trade practices and require complete service disclosure. Electronic money issuers must promptly report fraud, security breaches, and significant service interruptions to the central bank to protect consumer interests and the integrity of the financial system.

Regulatory sandboxes have improved consumer safety, but also raise concerns about data privacy because they test new financial technologies with sensitive personal and financial data. The law requires electronic money providers to maintain strong systems for transaction integrity and security, supporting strict data privacy safeguards. All electronic money issuers must follow strict data handling and privacy rules under the law. Similarly, the UK sandbox enforces stringent consumer protection rules, including enhanced data protection protocols and risk management frameworks to prevent financial fraud and protect consumer interests during product trials. Kenya's approach mirrors this by mandating digital lenders within the sandbox to obtain licences and adhere to data protection guidelines, creating a secure environment that minimises consumer risk.

Financial inclusion is promoted through regulatory sandboxes, which remove fintech company entry hurdles and encourage financial services competition and innovation. Sandboxes have helped Ugandans adopt new business models that offer affordable and accessible financial services, especially to the unbanked. This has boosted mobile money

[123] The National Payment Systems (Sandbox) Regulations, (2021) S.I. No. 20 of 2021.

services, advancing financial inclusion. The impact of sandboxes on market efficiency is also evident as they promote interoperability among financial service providers, reducing transaction costs, and enhancing service delivery. In Kenya, the sandbox environment has facilitated the development of interoperable platforms that allow seamless transactions across different mobile money operators, improving overall market efficiency and consumer access to services.[124] The UK's regulatory sandbox also exemplifies this by supporting the entry of innovative payment systems that enhance competition and efficiency in the digital financial landscape.[125]

9 Implementation of Testing Grounds in Uganda

The Ugandan government has been proactive in establishing a regulatory framework conducive to the growth of digital financial services (DFS). Allen highlights the need for a well-structured regulatory sandbox that provides ongoing regulatory engagement and lowers barriers to entry for new fintech firms. This approach aligns with Uganda's efforts to create a supportive regulatory environment for DFS innovation. A significant part of this initiative is the implementation of regulatory sandboxes, which allow for the testing of new financial technologies under a controlled regulatory environment. The law supports this initiative by stipulating the prevention of unauthorised access, modifications, and electronic fraud, ensuring a secure testing environment.

The law provides for the establishment, application, and approval process for operating a sandbox.[126] The regulation provides the legal backing for these initiatives, ensuring that all electronic money issuers adhere to stringent guidelines concerning liquidity, transaction limits, and customer due diligence.[127] In comparison, the UK has also adopted regulatory sandboxes to foster innovation while ensuring compliance with regulatory standards. Based on the author's survey, "the sandbox approach allows small-scale, live testing of innovations by private firms in a controlled environment operating under a special exemption, allowance, or other limited, time-bound exception".

To improve the implementation of testing grounds, the Ugandan government collaborates with various technology companies. This partnership focuses on integrating advanced technological solutions into the financial sector to address specific regulatory challenges, for example, the use of blockchain technology is explored to improve the security and efficiency of transactions. These collaborations are essential to tailor the regulatory environment to the dynamic needs of the financial market, ensuring that innovations align with consumer protection standards.

[124] Githu (n 19).
[125] Baker McKenzie (n 7).
[126] National Payment Systems Act (2020), Cap. 59, Section 16-18.
[127] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Part III.

The implementation of testing grounds in Uganda has shown notable success through various case studies. An exemplary case involves Beyonic, a company that provides a digital payment toolbox to small and medium enterprises (SMEs). Through the sandbox, Beyonic was able to enhance its cross-border payment capabilities by partnering with MFS Africa, thus extending its services to more than 40 countries in Africa. This partnership not only expanded their geographical presence but also added value-added services, significantly enriching the customer experience while ensuring compliance with regulatory standards.[128] Additionally, there was a collaboration between MTN Uganda and Stanbic Bank, which used the sandbox to test a mobile money platform. This initiative significantly reduced fraudulent transactions and enhanced user verification processes, showcasing the sandbox's role in allowing firms to refine their technology in a secure environment before a broader rollout. This case illustrates the critical importance of testing grounds in mitigating the risks associated with new financial technologies.[129]

Another significant case is Pezesha, a Kenyan-based capital enabler platform that connects SMEs in sub-Saharan Africa with working capital and other financial services. Pezesha leveraged Uganda's regulatory sandbox to test its debt-based crowdfunding platform. Following a successful one-year testing period, the Capital Markets Authority (CMA) granted Pezesha a letter of 'No Objection' to operate in Kenya's capital markets. This allowed Pezesha to provide financial education and proprietary credit scoring technology to match SMEs with appropriate financial institutions, showcasing the sandbox's role in facilitating innovation and compliance within a controlled environment.[130]

Uganda's proactive financial sector technological innovation management is shown in these case studies. Uganda is a model for balancing innovation and regulation by providing a regulated environment for companies to test and improve their products. MTN Uganda, Stanbic Bank, and Xente Tech Ltd. demonstrate the benefits of the regulatory sandbox in customer safety and regulatory compliance. As these initiatives continue to evolve, they provide valuable lessons for enhancing the stability and security of digital financial services.[131] This case highlights the sandbox's role in allowing the firm to refine its technology in a secure environment before a broader rollout. Another case involved a digital payment service that used the sandbox to experiment with cross-border payment solutions, which helped to establish robust mechanisms to handle international transactions securely and efficiently.[132]

[128] FinTech Showcase: Regulatory and Supervisory Approaches to Financial Technology (Alliance for Financial Inclusion 2021) <https://www.afi-global.org/wp-content/uploads/2021/07/FinTech-showcase_SR_27.7.2021.pdf> accessed 1 May 2024.
[129] Background to the Budget 2021/22 (Ministry of Finance, Planning and Economic Development 2021) <https://budget.finance.go.ug/sites/default/files/National Budget docs/Background to the Budget 2021_22.pdf> accessed 1 May 2024.
[130] ibid.
[131] Background to the Budget 2021/22 (n 129).
[132] Bank of Uganda, 'The National Payment Systems Regulatory Sandbox Framework, 2021' (June 2021).

10 Impact on Consumer Safety and Market Stability

10.1 Enhanced security measures

The implementation of regulatory sandboxes in Uganda has significantly improved the security measures for digital financial services (DFS). The rapid expansion of mobile money has attracted much debate about its implications for the growth of the financial sector and the effectiveness of monetary policy.[133] These controlled environments facilitate rigorous testing of new financial technologies, ensuring that vulnerabilities are identified and mitigated before full-scale deployment.[134] For example, the activation process for electronic money services now includes secure messaging systems that protect the customer's identity, which is crucial for preventing identity theft and fraud.[135] The UK has similarly used regulatory sandboxes to improve consumer protection.[136]

The Bank of Uganda, guided by the National Payment Systems Oversight Framework, plays a critical oversight role, ensuring that all payment systems adhere to safety and efficiency standards.[137] This oversight includes rigorous monitoring and assessment protocols that address vulnerabilities in DFS, ensuring compliance with the Principles for Financial Market Infrastructures (FMIs) as recommended by the BIS-IOSCO. The rapid expansion of mobile money services requires such robust oversight to mitigate systemic risks and support monetary stability in the financial sector.

Additionally, the legislation requires electronic money issuers to maintain strong systems for the integrity and security of customer transactions, further enhancing consumer safety. The Katuntu case highlighted significant security concerns associated with the operation of mobile money services, which the court addressed by highlighting the need for regulatory oversight to prevent fraudulent activities and protect consumer interests. This case underscores the importance of regulatory sandboxes that facilitate the testing and refinement of security measures before new technologies are fully deployed.[138] In light of the ruling in the case of ***Kayondo v. Bank of Uganda***, it is evident that regulatory actions must be balanced and well informed to prevent adverse impacts on innovation and consumer protection. The case highlights the need for regulatory

[133] Mawejje and Lakuma (n 85).
[134] National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 5; World Bank, 'How to Build a Regulatory Sandbox - A Practical Guide for Policymakers' (World Bank 2020) <https://cdn.sanity.io/files/hr4v9eo1/production/c329a5672d38adb9ec3970c5e4338ec89ba844a8.pdf> accessed 30 April 2024.
[135] National Payment Systems Regulations, 2021 No. 18, Regulation 19; National Payment Systems (Consumer Protection) Regulations, 2022 No. 103, Regulation 6; Electronic Transactions Act (2011), Cap.99 (Uganda), Section 7 and 11; Bank of Uganda (BOU) Mobile Money Guidelines, 2013.
[136] Chen (n 22).
[137] Bank of Uganda, The National Payment Systems Oversight Framework (June 2021).
[138] *Katuntu v MTN Uganda Ltd & Anor* (n 112).

measures that do not arbitrarily disrupt market activities. but instead promote secure and reliable financial transactions within a well-structured legal framework.[139]

10.2 Improved user experience

In digital finance, regulatory sandboxes have improved security and user experience. These sandboxes test new products and services in real life to ensure they meet consumer needs. Sandboxes in the UK has demonstrated the importance of real-world testing to improve user interfaces and functionality, directly leading to higher user satisfaction and increased adoption rates of digital financial.[140] This approach enables financial institutions to refine their offerings based on direct customer feedback, leading to more intuitive interfaces and functionality that cater to the specific needs of the Ugandan populace. As a result, consumers enjoy a more seamless and satisfying interaction with digital financial platforms, which encourages the continued use and trust in these services.

The future of digital financial services (DFS) in Uganda looks promising with plans to expand existing regulatory sandboxes. This is also supported by the law which provides for the legal framework for the establishment, application, and approval of sandboxes, facilitating the safe introduction of innovative financial technologies.[141] These initiatives aim to further enhance the robustness of the financial ecosystem by allowing more comprehensive testing and integration of new technologies.[142] This scale-up is expected to attract a broader range of fintech innovations, fostering a more inclusive financial environment. The focus will be on expanding the capabilities of these sandboxes to cover more extensive and complex financial operations, thus providing a safer and more reliable DFS landscape for consumers.[143]

Integration with Blockchain

Blockchain technology is set to play a crucial role in the evolution of Uganda's digital financial services. The integration of blockchain within regulatory sandboxes is expected to increase transaction security and transparency significantly.[144] This technology offers immutable record-keeping and enhanced security features that are crucial for the

[139] Miscellaneous Cause No. 109 of 2022 [2023] UGHCCD 113 (24 April 2023).
[140] World Bank (n 27).
[141] National Payment Systems Act (2020), Cap. 59, Sections 16-18.
[142] Bank of Uganda, 'National Financial Inclusion Strategy 2023-2028' (2023) <https://bou.or.ug/bouwebsite/bouwebsitecontent/FinancialInclusion/2023/Signed_2023_2028_National-Financial-Inclusion-Strategy_.pdf> accessed 30 April 2024; OECD, 'The Role of Sandboxes in Promoting Flexibility and Innovation in the Digital Age' (2020) <https://cdn.sanity.io/files/hr4v9eo1/production/8b7b30586373ff16ac1c52283c6142375a998eff.pdf> accessed 30 April 2024.
[143] African Development Bank Group, Understanding the Importance of Regulatory Sandbox Environments and Encouraging Their Adoption (2022) <https://cdn.sanity.io/files/hr4v9eo1/production/3f899a31581b2cc704a44ae96a2c736288699488.pdf> accessed 30 April 2024.
[144] Seunghwan Kim and others (n 25).

integrity of financial transactions.[145] By incorporating blockchain, Uganda can address some of the persistent challenges such as fraud and cyber threats, thereby increasing consumer confidence in digital platforms.[146]

Increased public awareness

To maximise the benefits of regulatory sandboxes and blockchain integration, there is a planned increase in public awareness campaigns. Similarly, the challenges to ensure active and secure use of mobile money accounts are evident in the findings which discuss the need for improved financial education and reduced transaction fees to promote active use among micro-entrepreneurs.[147] These campaigns will inform customers about new financial technology safety and digital economic benefits. To build confidence and promote new financial services, awareness is the key. Uganda can strengthen consumer protection and participation in digital financial services by informing consumers. These prospects seek to strengthen financial services operations and prioritise customer protection in Uganda's changing financial landscape.

10.3 Operational Challenges in Implementing Regulatory Sandboxes

Preventing fraud and financial crimes in Uganda's digital financial ecosystem requires regulatory sandboxes. Sandboxes allow fintech firms to test antifraud methods in a regulated setting, validating their effectiveness in reducing financial crime fraud. The law requires financial institutions to perform risk assessments and implement robust measures to counteract risks related to money laundering and terrorist financing when introducing new technologies.[148] Additionally, court cases such as ***Aida Atiku v Centenary Rural Development Bank Limited*** underscore the importance of stringent regulatory oversight to prevent unauthorised transactions, highlighting the role of sandboxes in refining security measures before full deployment.[149]

These measures collectively demonstrate the significant impact of regulatory sandboxes on improving consumer safety and ensuring market stability within Uganda's digital financial services. By fostering secure and user-friendly environments, sandboxes not only protect consumers, but also support the resilience and integrity of the broader financial market.

[145] Electronic Transactions Act (2011), Cap.99 (Uganda), Section 5 and 7.
[146] Agnieszka Butor-Keler and Michał Polasik, 'The Role of Regulatory Sandboxes in the Development of Innovations on the Financial Services Market: The Case of the United Kingdom' (2020) 19(4) Ekonomia i Prawo. Economics and Law 621 <http://www.economicsandlaw.pl> accessed 30 April 2024.
[147] Hamdan, Lehmann-Uschner and Menkhoff (n 31).
[148] Anti-Money Laundering Act (2013), Cap 118 (Uganda), Section 6A and 9.
[149] Civil Suit No. 0754 of 2020.

11 Conclusion

Comparing Uganda's mobile money regulatory sandboxes with Kenya and the UK shows similarities and differences. Ugandan regulatory sandboxes have helped test financial innovations while minimising risks from overseas ICT service providers and economic operators. These sandboxes enforce strict data security measures to protect consumers and comply with regional and international frameworks, but Uganda's regulatory framework is hampered by the lack of clear operational guidelines on cross-border testing. Kenya and the UK have more developed sandboxes.

The analysis shows that Uganda's regulatory sandboxes need policy changes to expand. Uganda should implement an integrated approach to expedite cross-border testing and link its regulatory system with international norms, such as Kenya's comprehensive Central Bank-supervised regulatory guidelines. Stronger engagement between regulators and fintech innovators, like the UK's sandbox model, might combine innovation with consumer protection and data security, addressing foreign economic operator risks.

A future study should broaden Uganda's regulatory sandboxes and examine how blockchain and artificial intelligence (AI) could reduce digital financial hazards. The effectiveness of sandboxes in promoting financial inclusion, especially among underserved populations, should be studied, as should their adaptability to changing technological challenges, to keep Uganda's framework responsive to the dynamic landscape of digital financial services.

Judy Yueh Ling Song[*] *and Esther Tan*[*]

SPECIAL SECTION

BEYOND TRADITIONAL CONTRACTS: THE LEGAL RECOGNITION AND CHALLENGES OF SMART CONTRACTS IN MALAYSIA AND SINGAPORE

Abstract

The dawn of blockchain technology and smart contracts has instigated a transformative shift in digital transactions, challenging and expanding legal boundaries in both Malaysia and Singapore. This paper examines how these common law jurisdictions have adapted to these challenges, integrating traditional legal frameworks with the distinct characteristics of blockchain, such as automation, decentralisation, and cost efficiency. Through an analysis of key legal cases, the study demonstrates the adaptability of common law in responding to technological innovations.

A key focus is placed on the application of smart contracts in sectors such as Islamic finance, where both common law and Sharia law coexist. Malaysia and Singapore offer unique examples of legal pluralism, having successfully harmonised these legal systems even before the advent of smart contracts. The integration of smart contracts into these frameworks showcases the ability of these jurisdictions to balance innovation with tradition, effectively governing both conventional and digital transactions.

However, the paper identifies significant legal uncertainties, particularly concerning the enforceability of smart contracts, mechanisms for dispute resolution, and the integration of digital assets into existing legal norms. Rather than advocating comprehensive reforms, the paper suggests targeted regulatory updates and strategic legal guidelines to address these issues. By adopting this approach, Malaysia and Singapore can strengthen their legal systems to fully harness the potential of blockchain and smart contracts. Through comparative analysis and empirical case law, the study highlights how these jurisdictions can remain at the forefront of legal and technological innovation in Southeast Asia.

SUMMARY

[*] Research Fellow, University of Turin, Italy; Advocate & Solicitors (non-practising) of High Court of Malaya, Malaysia
[*] Partner, Zul Rafique & Partners, Advocate & Solicitors of High Court of Malaya, Malaysia

 DOI 1.13135/2785-7867/11334

1 Introduction

The blockchain technology introduced by Satoshi Nakamoto's seminal 2008 white paper[1] has ignited a global re-evaluation of traditional financial and transaction systems. This technological innovation has not only established the foundation for cryptocurrencies but has also facilitated the broader adoption of blockchain technology across various domains. This is achieved through the use of peer-to-peer networks, digital signatures, and a proof-of-work/proof-of-stake mechanism, enabling electronic transactions without the necessity for trusted intermediaries. Among these applications, smart contracts stand out for their ability to automate complex agreements with precision and enforceability[2], mirroring the impact of the Transmission Control Protocol/Internet Protocol (TCP/IP) on the development of the Internet[3]. However, it is important to recognise that the rigidity of smart contracts can be a challenge for certain complex agreements. The focus is on how smart contracts excel within their predefined parameters. While they offer significant advantages in automation and precision, it is crucial to consider their current limitations regarding flexibility when applying them to highly complex or adaptive contracts.

There are various advantages to using smart contracts, including enhanced transparency, reduced transaction costs, faster settlements, user-controlled networks, and a shift towards decentralisation[4]. Additionally, the open-source nature of the distributed ledger and its elimination of intermediaries streamline transactions, providing high security through their decentralised structure. This model promotes a system that is theoretically centralised but politically and architecturally decentralised, disrupting conventional models and offering a cohesive computing framework that is resilient against single points of failure[5].

Despite the swift growth of the digital economy in Malaysia and Singapore, the disruptive nature of smart contracts and blockchain technology also raises some concerns regarding legal and regulatory aspects. These technologies continue to be bound by a legal and regulatory environment that is continually evolving, therefore it is important to examine how these technologies fit into the current legal framework and what amendments may be needed to account for their special attributes.

Our paper seeks to explore the legal position by examining the existing case law related to smart contracts and blockchain technology. We specifically aim to address the question: How do the current legal frameworks in Malaysia and Singapore accommodate the unique

[1] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [2008] Decentralized Business Review 1.
[2] A Savelyev, 'Contract Law 20: "Smart" Contracts as the Beginning of the End of Classic Contract Law' (2017) 26(2) Information & Communications Technology Law <https://doi.org/10.1080/13600834.2017.1301036> accessed 2 March 2024.
[3] Richard W Stevens, *TCP/IP Illustrated*, Volume 1: The Protocols (Addison-Wesley 1994).
[4] Y Li, W Yang, P He, C Chen and X Wang, 'Design and Management of a Distributed Hybrid Energy System through Smart Contract and Blockchain' (2019) 248 Applied Energy 390, 405.
[5] M M Abu-Bakar, *Shariah analysis of bitcoin, cryptocurrency, and blockchain. Shariah Analysis in Light of Fatwas and Scholars* Opinions 14, 19. (Blossom Labs, Inc 2018); J Poon and V Buterin, 'Plasma: Scalable Autonomous Smart Contracts' (White paper, 2017).

features of blockchain and smart contracts, and what legal and regulatory challenges do these technologies pose within these jurisdictions?

Through our investigation, the paper will delve into the benefits and challenges presented by blockchain and smart contracts, examine the existing legal frameworks in Malaysia and Singapore, and propose recommendations for addressing the identified legal and regulatory challenges. We believe that this analysis is crucial for understanding the implications of these technologies for the future of digital transactions and agreements in both countries, setting a precedent for legal and regulatory adaptations in the digital age.

2 Smart contract vs traditional contract

The origin of the “smart contract” term was coined by Nick Szabo as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises"[6]. Szabo emphasised the increased functionality of smart contracts compared to non-coded contracts and consequently did not assume a detachment from the law. In light of this, a smart contract is nothing more than the encoding or digital memorialisation of a contract or parts thereof. Its legal evaluation depends on the law applicable to the underlying contract. Naturally, the conclusion of a contract and its digital representation in a smart contract can coincide. However, most smart contracts will most likely be based on an additional written or electronic agreement in natural language.

Smart contracts and traditional contracts exhibit notable differences. In the formation of a classic contract, it must contain these requisites: offer, acceptance, and consideration, which are typically fulfilled by the document being physically signed. In the event of a breach, the wronged party usually takes the other party to court or arbitrates the dispute to enforce the terms of the contract or to receive compensation from the breaching party. Similarly, disputes over the interpretation of a term may require a third party (such as a court, arbitrator, or pre-agreed authority) to make the final decision to settle the issue[7]. This may involve several third parties, lawyers representing each contracting party, and a judge/arbitrator, resulting in an inevitably costly and time-consuming dispute resolution process. Even with a favourable judgement/award, execution may still be a challenging last step.

In contrast, smart contracts operate differently. By utilising technology to encode contracts, parties avoid the ambiguity that could arise when obligations are

[6] N Szabo, ‘Formalizing and Securing Relationships on Public Networks’ (1997) 2(9) First Monday <https://firstmonday.org/ojs/index.php/fm/article/view/548> accessed 10 October 2024 ; Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996) 1, 5.

[7] M Kasatkina, ‘Dispute Resolution Mechanism for Smart Contracts’ (2022) 16(2) Masaryk University Journal of Law and Technology 143, 162; A Schmitz and C Rule, ‘Online Dispute Resolution for Smart Contracts’ [2019] J Disp Resol 103.

expressed in traditional contract terms[8]. This clarity is achieved through smart contracts, which are computer programs comprised of "if/then" clauses detailing every obligation and possible situation. Once established and legally agreed upon by all parties, these smart contracts operate on the principle of self-enforcement[9]. In the context of smart contracts, "self-enforcement" refers to the automatic execution of transactions involving cryptocurrency or crypto assets when predetermined conditions are met. This feature ostensibly removes the need for human intervention in the performance of contractual duties, leveraging the immutable nature of blockchain technology to prevent parties from reneging on their commitments due to deliberate refusal or human error. Consequently, it is posited that the deployment of smart contracts on a blockchain eliminates the potential for contractual breaches by the parties involved.[10]

Unlike conventional contracts, which often rely on intermediaries for enforcement and dispute resolution, smart contracts are executed and enforced by the code itself, directly on a blockchain. This shift not only enhances trust between parties by ensuring compliance through code but also streamlines transactions by removing the need for third-party involvement[11].

Feature	Smart Contracts	Traditional Contracts
Digital Lifecycle	Entirely online, without the need for external entities.	Often occur offline or require manual intervention.
Automated Execution	Executed by automated systems according to pre-programmed rules.	Execution may involve discretion, reasonableness, or judgement. Described in human languages.
Immutable Record	Cannot be altered once deployed; adjustments require a new contract.	Can be modified through amendments or renegotiations.

[8] JM Sklaroff, 'Smart Contracts and the Cost of Inflexibility' (2017) 166 U Pa L Rev 263; E Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9(2) Law, Innovation and Technology 269, 300; C Poncibò, L Di Matteo and M Cannarsa, *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019); P De Filippi and A Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2019).

[9] M Raskin, 'The Law and Legality of Smart Contracts' (2016) 1 Geo L Tech Rev 305.

[10] P Ortolani, 'Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36(3) Oxford Journal of Legal Studies 595, 629.

[11] S Wang and others, 'Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends' (2019) 49(11) IEEE Transactions on Systems, Man, and Cybernetics: Systems 2266, 2277.

Binary Outcomes	Perform actions based on clear, algorithmically determinable conditions.	Outcomes may depend on complex conditions or subjective assessments.
Trust	Trust in the smart contract and codes.	Trust in one another or intermediaries.
Reduced Transaction Costs and Risks	Potentially lower costs by automating execution and enforcement, minimise risk of defective performance, and address informational asymmetry.	Higher transaction costs due to manual processes and risk of non-performance or disputes.

The various types of smart contracts[12] span a spectrum, accommodating various needs and preferences, including:

- Pure Code Contracts (Mere Code): At one end of the spectrum, smart contracts exist solely as code on the blockchain, with no accompanying legal agreement. These contracts represent mere transactions in the technical sense, focused solely on automated execution without any legal implications or natural language terms. This format is ideal for parties seeking to bypass intermediaries entirely, relying solely on the blockchain's distributed ledger technology.
- Code-Enhanced Traditional Contracts: A tool to execute a legal agreement, with the legal agreement existing off-chain. This approach incorporates coded clauses within conventional contracts, enabling certain operations or entire contract executions on the blockchain while maintaining the traditional format.
- Hybrid or Merged Contracts: A smart contract that either constitutes a legally binding declaration of will (such as an offer or acceptance) or merges with the legal agreement to exist simultaneously both on-chain and off-chain. In this form, the smart contract can be partially or fully integrated with the legal agreement, and it should be determined by the parties whether the agreement should be treated primarily as on-chain or off-chain.
    - Ricardian Contracts: Although some do not regard Ricardian contracts as smart contracts in the strict sense, they are often discussed within this category. Ricardian contracts bridge traditional legal agreements and

[12] G Dobrauz-Saldapenna and MA Schrackmann, 'Economics of Smart Contracts: Efficiency and Legal Challenges' in *Disintermediation Economics: The Impact of Blockchain on Markets and Policies* (Springer International Publishing 2021) 33, 46; UK Jurisdiction Taskforce of the Lawtech Delivery Panel, Public Consultation: The Status of Cryptoassets, Distributed Ledger Technology and Smart Contracts under English Private Law (May 2019) 'Lawtech Delivery Panel, Public Consultation' 31 and 32; European Law Institute, 'ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection' (2023) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_Blockchain_Technology__Smart_Contracts_and_Consumer_Protection.pdf> accessed 25 July 2024.

> blockchain execution, including both human-readable text (legal terms) and machine-readable code that can be executed on a blockchain. This hybrid nature facilitates understanding by the parties and automated enforcement of certain aspects.

Hence, the three key characteristics that distinguish smart contracts are immutability, automation, and decentralisation. Smart contracts are crafted to operate independently based on predetermined conditions, leveraging blockchain technology to facilitate transactions securely and transparently without the need for intermediaries[13]. Smart contracts are designed to be immutable once they are activated, which ensures strict adherence to predetermined terms. These contracts abide by the terms they were designed to autonomously supervise, carry out, or record events and actions that have legal consequences. The technology is versatile, embracing both contracts solely based on code and hybrid forms that integrate natural language to enhance legal comprehension. Additionally, the security of blockchain-recorded data is reinforced by decentralized nodes and hashing techniques, rendering unauthorised access or alterations to the decentralized ledger notably difficult[14]. This framework not only solidifies the security paradigm of blockchain transactions but also underscores the intricate balance between technological innovation and enforceability in the realm of digital contracts.

2.1 The Self-Executing Nature of Smart Contracts and Their Enforceability

Smart contracts represent a significant innovation in the digital age, automating the execution of contractual terms upon the fulfilment of predefined conditions. This mechanism eliminates the possibility of voluntary breaches, as exemplified in a scenario where a smart contract facilitates a transaction between two parties, such as Party A agrees in exchange for Party B's services to pay a fee of £430. By using a smart contract, which is similar to an escrow manager, the fee of £430 paid by A will be released to B when A is satisfied with the services provided by B[15]. This self-executing functionality automatically carries out the agreed-upon actions without requiring external intervention.

This functionality suggests a potential future where smart contracts could supplant certain traditional legal functions, including those performed by transactional lawyers. Blockchain technology underpins the creation of smart contracts, serving as a digital ledger that records any amendments to the contracts or their terms. Real-world applications, such as Etherisc's development of index-based insurance products on the

[13] F Rahman, C Titouna and F Nait-Abdesselam, 'Fundamentals of Blockchain and Smart Contracts' in *Blockchain and Smart-Contract Technologies for Innovative Applications* (Springer Nature Switzerland 2024) 3, 37.
[14] JM Sklaroff (n 8) 263; KJ Yong, ES Tay and DW Khong, 'Application of Blockchain Smart Contracts in Smart Tenancies: A Malaysian Perspective' (2022) 8(1) Cogent Social Sciences 2111850.
[15] B C Cheong and H Kishen, 'Legal Risks beneath Blockchain-Enabled Smart Contracts' (The Singapore Law Gazette, 23 January 2021) <https://lawgazette.com.sg/feature/legal-risks-beneath-blockchain-enabled-smart-contracts> accessed 29 January 2024.

Ethereum blockchain, demonstrate the practical utility of smart contracts[16]. For example, Etherisc's decentralised application (dApp) for flight delay and cancellation insurance automates premium payments and claims based on specific flight status changes, showcasing a more efficient and direct process compared to traditional insurance models[17].

Despite their potential, smart contracts face challenges regarding enforceability and adaptability, particularly in sustaining long-term commercial relationships characterised by complexity and the need for flexibility. Critics argue that the term "enforcement" might be misleading when applied to smart contracts as traditional enforcement mechanisms involve state intervention to protect contractual rights[18]. The binary logic of smart contracts, which operates without discretion, struggles to accommodate the fluid dynamics of ongoing business relationships, that often rely on negotiation and adjustment[19]. This limitation highlights the difference between self-execution, which is the automatic performance of contract terms based on predefined conditions, and self-enforceability, which concerns the ability to ensure compliance and address non-performance. In the latter, the code ensures compliance by preventing breaches through blockchain immutability[20], but this doesn't guarantee legal enforceability under traditional laws, which still need to adapt to smart contracts[21].

Moreover, the immutable and transparent nature of smart contracts, while advantageous for security and efficiency, presents difficulties in integrating these digital agreements into the existing legal frameworks, which are designed to manage disputes and relationships with a degree of subjectivity[22]. Undoubtedly, coding errors, unforeseen situations, or misinterpretation of coded terms may cause potential disputes, highlighting a need for innovative dispute resolution mechanisms designed for smart contracts[23].

Many scholars have explored ways to resolve disputes arising from smart contracts. Kasatkina[24] suggests a hybrid model combining traditional arbitration with blockchain online dispute resolution (ODR) to address smart contract disputes, leveraging the

[16] C H Hoffmann, 'A Double Design-Science Perspective of Entrepreneurship–The Example of Smart Contracts in the Insurance Market' (2021) 13 Journal of Work-Applied Management 69.
[17] Chester Cheong and Kishen (n 15).
[18] Mik (n 8).
[19] Weiqin Zou and others, 'Smart Contract Development: Challenges and Opportunities' (2021) 47(10) IEEE Transactions on Software Engineering 2084, 2106; Z Zheng and others, 'An Overview on Smart Contracts: Challenges, Advances and Platforms' (2020) 105 Future Generation Computer Systems 475, 491.
[20] Akmaral Mukhtarova and NI Lesnova, 'Smart Contracts in International Trade in Services in the Field of Intellectual Property' (2019) Proceedings of the International Scientific and Practical Conference on Digital Economy (ISCDE 2019), available on <https://doi.org/10.2991/iscde-19.2019.100> accessed 03 August 2024.
[21] Alex Norta, 'Self-Aware Smart Contracts with Legal Relevance' (2018) International Joint Conference on Neural Networks (IJCNN) 1-8. Available at doi: <10.1109/IJCNN.2018.8489235> accessed 03 August 2024.
[22] M Giancaspro, 'Is a "Smart Contract" Really a Smart Idea? Insights from a Legal Perspective' (2017) 33(6) Computer Law & Security Review 825, 835.
[23] JH Xue and R Holz, 'Applying Smart Contracts in Online Dispute Resolutions on a Large Scale and Its Regulatory Implications' in M Ragnedda and G Destefanis (eds), *Blockchain and Web 3* (2019); R Koulu, 'Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement' (2016) 13 SCRIPTed 40.
[24] Kasatkina (n 7).

efficiencies of smart contracts while retaining the thoroughness and flexibility of conventional dispute resolution. Schmitz and Rule advocate ODR as an effective means to resolve conflicts, with potential applications in blockchain ODR start-ups[25]. Other scholars[26] further discuss the scalability and applicability of smart contract technology in ODR, highlighting its potential to autonomously resolve disputes in specific contexts, such as cross-border e-commerce[27].

These discussions underscore the ongoing effort to align the technological advances of smart contracts with traditional legal principles, ensuring that legally binding agreements remain enforceable and adaptable within the established judicial system.

2.2 The operation of smart contracts

Smart contracts embody an innovative fusion of automation and legal precision, but there is a reluctance to fully transition to code-based agreements due to the nuanced language of traditional legal documents. Research underscores the critical need to bridge computational transactions with natural language contracts for legal validity, highlighting efforts to develop machine-readable modules that mirror contractual elements and address dispute resolution[28]. Additionally, the complexity of traditional contracts necessitates a nuanced understanding of smart contracts' legal enforceability, alongside a methodical approach to formalize contract law within the digital realm[29]. These studies reflect the ongoing challenge of melding the deterministic nature of code with the interpretive flexibility of legal language, revealing a complex interplay between technological advancements and established legal frameworks.

A contract established on straightforward conditions[30] can be seamlessly translated into both machine-readable code and natural language. In contrast, translating nuanced legal concepts such as "reasonableness" or "emotional distress" into code, or designing code to

[25] Schmitz and Rule (n 7).
[26] P Ortolani, 'Chapter 21 Recognition and Enforcement of the Outcome of Blockchain-Based Dispute Resolution' in *Blockchain and Private International Law* (Brill | Nijhoff 2023); A Palombo, R Battaglini and L Cantisani, 'A Blockchain-Based Smart Dispute Resolution Method' in LA DiMatteo, A Janssen, P Ortolani, F de Elizalde, M Cannarsa and M Durovic (eds), *The Cambridge Handbook of Lawyering in the Digital Age* (Cambridge University Press 2021) 122, 139; Christoph Salger, 'Decentralized Dispute Resolution: Using Blockchain Technology and Smart Contracts in Arbitration' (2024) 24 Pepperdine Dispute Resolution Law Journal 65; Ortolani (n 10).
[27] Xue and Holz (n 23); Koulu (n 23); Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' [2015] SSRN <http://dx.doi.org/10.2139/ssrn.2580664> accessed 28 October 2024.
[28] Goldenfein and Leiter, 'Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct' (2018) 29 Law and Critique 141, 141, 149; L A DiMatteo and C Poncibó, 'Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies' (2018) 26 European Review of Private Law 6.
[29] Kritagya Upadhyay et al, 'Paradigm Shift from Paper Contracts to Smart Contracts' in 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (2021) 261, 268 <https://doi.org/10.1109/TPSISA52974.2021.00029> accessed 28 October 2024; Eric Tjong Tjin Tai, 'Formalizing Contract Law for Smart Contracts' Social Science Research Network (2017) 6 Tilburg Private Law Working Paper Series.
[30] Zheng and others (n 19); Giancaspro (n 22).

reflect complex legal principles without losing interpretative depth, poses significant challenges to the dual existence of contracts in both code and legal prose[31].

Blockchain oracles play an essential role in bridging the gap between isolated blockchain environments and the dynamic external world[32]. Oracles operate as intermediaries, enabling smart contracts to respond to external real-world events and data, beyond the limitations imposed by the blockchain. Oracles are platforms that retrieve, verify, and transfer external data to the blockchain. This allows smart contracts to operate on accurate and timely data that comes from sources outside of their enclosed ecosystems[33].

This integration of oracles addresses a fundamental challenge in the execution of smart contracts: the blockchain's inability to independently access or verify external data[34]. Oracles not only enhance the operational scope of smart contracts but also introduce a layer of trust in external sources, ensuring that the data influencing contract outcomes is reliable and impartial[35].

The reliance on oracles, however, introduces potential vulnerabilities, particularly the risk associated with external data sources. Manipulation of data by malicious actors can compromise the integrity of smart contract executions.[36] To mitigate such risks, it is crucial to employ a robust selection process for data sources, coupled with cross-referencing mechanisms, to ensure the reliability and security of the data feeding into smart contracts.

The development and execution of smart contracts intersect technological efficiency and legal complexity. While blockchain oracles significantly expand the capabilities of smart contracts by incorporating real-world data, they also underscore the importance of cautiously managing the trust placed in external data sources[37]. As smart contracts continue to evolve, the integration of blockchain oracles is instrumental in harmonising the need for external data with the inherent decentralisation of blockchain technology, paving the way for more sophisticated and legally robust automated contracts[38].

In adverse situations where the contract goes unperformed, the traditional option would be to enforce it by going to court or via arbitration. However, due to the high levels of grey areas in the execution of smart contracts, this may cause the plaintiff to incur costs and time spent in legal proceedings. It is almost impossible to code every possible

[31] Chester Cheong and Kishen (n 15).
[32] S K Ezzat, Y N Saleh, and A A Abdel-Hamid, 'Blockchain Oracles: State-of-the-Art and Research Directions' (2022) 10 IEEE Access 67551, 67572; Wang and others (n 11).
[33] ibid.
[34] ibid.
[35] F Bassan and M Rabitti, 'From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation' (2024) 55 Computer Law & Security Review 106035.
[36] MD Sheldon, 'Auditing the Blockchain Oracle Problem' (2021) 35(1) Journal of Information Systems 121, 133.
[37] A Albizri and D Appelbaum, 'Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts' (2021) 35(2) Journal of Information Systems 1, 16.
[38] Sklaroff (n 8); Mik (n 8).

"if-then" scenario into the smart contract and therefore it may not align well with real-world business settings and legal dispute resolution methods.

3 Legal position of Smart Contracts in Singapore

Singapore's contract law is primarily influenced by the English common law system[39]. This influence means that the legal principles applied by Singapore's courts often reflect those used in English common law[40]. When Singaporean cases lack direct precedents, the legal approach typically follows the English model. Unlike its neighbours, Malaysia and Brunei, Singapore chose not to codify its contract law after gaining independence in 1965, leading to a body of contract law that is mainly composed of judicial decisions.

Smart contract can be seen as an evolved form of electronic contracts[41]. These smart contracts are unique for their capacity to automatically execute and enforce terms based on predefined rules within a blockchain platform. Despite the modernity of smart contracts, traditional legal principles from common law, such as offer, acceptance, consideration, and the intention to create legal relations, still apply[42]. These principles, while not formally codified, draw heavily from English law and are essential for the legal recognition of smart contracts.

The Electronic Transactions Act[43] acknowledges electronic contracts by granting legal recognition to electronic records[44] and signatures[45], thus affirming that contracts formed electronically are as valid as their written counterparts. However, Singapore law does not specifically define "smart contracts". The term, attributed to Nick Szabo, refers to contracts that automate execution through digital means, often reducing the potential for breach and facilitating various commercial functions, from ensuring performance to managing credit.

For a smart contract to be an actual contract under Singapore law, it must fulfil all traditional contractual formation requirements[46] ie, - offer and acceptance, the intent to establish legal relations, the presence of consideration, free consent and capacity to enter

[39] AB Phang and G Yihan, *Contract Law in Singapore* (Kluwer Law International BV 2021) 32, 67; S Donohoe, 'Contractual and Statutory Liability for Building Defects in Singapore' (1999) 17(1) Structural Survey 32, 35 <https://doi.org/10.1108/02630809910258719> accessed 10 October 2024.

[40] Application of English Law Act 1993 (Singapore) available at <https://sso.agc.gov.sg/Act/AELA1993> accessed 25 July 2024; AB Phang and Yihan Goh, *Contract Law in Singapore* (Kluwer Law International BV 2012).

[41] Electronic Transactions Act *2010 (Singapore) (Act of 2010),* available at: <https://sso.agc.gov.sg/Act/ETA2010> accessed 25 July 2024.

[42] Application of English Law Act 1993 (Singapore) available at <https://sso.agc.gov.sg/Act/AELA1993> accessed 25 July 2024; Phang and Yihan Goh (n 40).

[43] Electronic Transactions Act 2010 (n 41).

[44] ibid 9.

[45] ibid 8.

[46] Application of English Law Act 1993 (n 40); Phang and Yihan Goh (n 40); Tan Cheng Han, 'Contract Formation in Singapore' in Mindy Chen-Wishart, Alexander Loke, and Stefan Vogenauer (eds), *Formation and Third Party Beneficiaries* (Oxford 2018) accessed on 25 July 2024.

a contract. Provided these criteria are met, smart contracts, in general, possess the potential for legal enforceability within the Singaporean jurisdiction.

The enforceability of each smart contract requires careful examination. As smart contracts execute entirely on code and due to their self-executing nature, they often bypass traditional legal enforcement. This does not, however, relieve them from legal oversight. Contracts rooted in illegal activities or those made under duress will likely be declared void by the courts.

Conversely, smart contracts that are written with clear and simple code, which may include provisions for resolving disputes through legal channels, generally do not face issues with enforceability. A striking consideration arises when parties explicitly state their intent not to create legal relations within the contract, this could potentially impact the contract's enforceability. In this situation, Singaporean courts may adopt an approach similar to their UK counterparts, scrutinising the broader context to ascertain the parties' genuine intent regarding legal bindingness and enforceability, despite the absence of local precedents on this matter.

In certain domains, like ship transfers, hire-purchase agreements, and real estate transactions, additional stipulations may apply. In most cases, these transactions require that the contract or the supporting documentation be duly signed and in writing. In Singapore, the capacity of entirely code-based smart contracts to satisfy these formal requirements remains an open question. For contracts predominantly in natural language, the prerequisites of writing and signature pose fewer challenges to enforcement.

When it comes to smart contracts involving cryptocurrencies, Singapore has set up a solid and forward-thinking legal structure through laws like the Securities and Futures Act 2001[47], the Payment Services Act 2019[48] and the Financial Services and Markets Act 2022[49]. These regulations aim to safeguard consumers and maintain the integrity of the market while promoting innovation. The Monetary Authority of Singapore plays a critical role in granting digital payment token licences and overseeing a regulatory environment that distinguishes between regulated and unregulated cryptocurrencies[50]. This framework ensures an organised and secure ecosystem for cryptocurrency transactions by extending beyond licensing requirements to include sales regulations, anti-money laundering, counter-terrorism financing compliance, and taxation.

The recognition of crypto assets as a form of property capable of being held on trust by the Singapore High Court in ByBit Fintech Ltd v Ho Kai Xin and others [2023][51] further strengthens the legal basis for transactions involving digital assets, aligning Singapore with other common law jurisdictions. This legal clarity around the status of cryptocurrencies

[47] Securities and futures Act 2001 (Singapore) available at <https://sso.agc.gov.sg/Act/SFA2001> accessed 20 July 2024.
[48] Payment Services Act 2019 (Singapore) available at <https://sso.agc.gov.sg//Act/PSA2019> accessed 20 July 2024.
[49] Financial Services and Markets Act 2022 (Singapore) available at <https://sso.agc.gov.sg//Act/FSMA2022> accessed on 20 July 2024.
[50] WaiWai Wong, *The Law of Smart Contracts* (Sweet & Maxwell 2022).
[51] ByBit Fintech Ltd v Ho Kai Xin and others [2023] SGHC 199.

as property is particularly significant for smart contracts, as it affirms that digital assets managed through these contracts have a recognized legal standing.

Smart contracts might also fall under the jurisdiction of applicable data protection regulations. In Singapore, the Personal Data Protection Act 2012[52] governs the collection, use and disclosure of personal data. The purpose of the Act, in Section 3, does not specifically address blockchain technology or smart contracts, nor have any directives been issued regarding this matter. Consequently, uploading an individual's unencrypted personal data to a public, permissionless blockchain network, resulting in its public disclosure, is analogous to a third party posting personal data on the internet for public access. If such an action is taken without the individual's consent or does not fall under any legal exemptions, it would represent a violation by the third party[53].

The distinctive characteristics of blockchain technology present challenges to its integration with existing data protection regulations, leading to inherent incompatibilities between the two. To address the clash between blockchain technology and data protection laws, the blockchain community[54] advocates for using private, permissioned networks for personal data management and employing off-chain transactions to prevent direct data recording on the blockchain.

3.1 Case Analysis

The first landmark case that presents the understanding of the legal standing of smart contracts and algorithmic trading within the framework of Singapore law is the decision of the Singapore Court of Appeal's in Quoine Pte Ltd v B2C2 Ltd[55]. This case scrutinises several key legal questions concerning the formation, enforceability, and potential nullification of contracts executed by automated systems without human intervention.

At the core of the dispute was whether a contract formed solely through algorithmic trading software could be considered legally binding. The Court of Appeal delineated the contractual relationships, emphasising that trading contracts were directly formed between B2C2 and the counterparties without human intervention, but through deterministic algorithms. This finding underscores the acceptance of contracts generated

[52] Personal Data Protection Act 2012 (Singapore) available at <https://sso.agc.gov.sg/Act/PDPA2012> accessed 20 July 2024.

[53] International Association for Trusted Blockchain Applications, Report on Data Protection Regulations Applicable to Blockchain Technology in Different Jurisdictions Worldwide (December 2020) <https://o.inatba.org/wp-content/uploads/2021/01/2020-12-Privacy-WG-Report-on-Data-Protection-005.pdf> accessed 20 July 2024; WaiWai Wong (n 50).

[54] J Quintais, B Bodo, A Giannopoulou, and V Ferrari, 'Blockchain and the Law: A Critical Evaluation' (2019) 2(1)Stanford Journal of Blockchain Law & Policy 86; B Arruñada, 'Blockchain's Struggle to Deliver Impersonal Exchange' (2018) 19 Minn JL Sci & Tech 55; Y Liu and others, 'An Overview of Blockchain Smart Contract Execution Mechanism' (2024) 41 Journal of Industrial Information Integration 10067; J Li and M Kassem, 'Applications of Distributed Ledger Technology (DLT) and Blockchain-Enabled Smart Contracts in Construction' (2021) 132 Automation in Construction 103955.

[55] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.

by algorithms under Singapore law, provided they operate within their programmed parameters.

The appeal raised the question of whether a contract could be voided due to a unilateral mistake, particularly when that mistake led to trades being executed at rates significantly divergent from the market price. The court clarified the application of the unilateral mistake doctrine in the context of algorithmic trading, emphasising the need to consider the programmer's knowledge and intentions at the time of programming the algorithm. The court found no unilateral mistake, either at common law or in equity, as the trades executed at the "Deep Price" were consistent with the programmed algorithm's operations, and there was no evidence to suggest that the programmer had actual or constructive knowledge of a mistake affecting the contract's fundamental terms[56].

A crucial aspect to note is how the Court of Appeal considered whether the controversial trades might be nullified because of mistakes made by one party or by both parties involved. The Court dismissed Quoine's claims that there were unilateral mistakes (as recognised by both common law and equity) and a common mistake, confirming that a valid contract was in place and that the trades occurred because the algorithms worked exactly as they were supposed to.[57] This aspect of the decision highlights the court's approach to algorithmic trading, emphasising that clarity in programming and the intentions behind algorithmic trading strategies play a crucial role in determining the validity of the contracts they create. The case underscores the legal recognition of contracts formed through automated processes, including smart contracts, in Singapore's legal system.

In another instance, Quoine's unilateral cancellation of the disputed trades, due to what it considered an aberrant execution rate caused by a technical oversight, was challenged by B2C2. The CA scrutinised the terms of the Agreement and the Risk Disclosure Statement, particularly focusing on clauses related to trade reversals and amendments to the agreement terms. The court concluded that Quoine could not unilaterally amend the agreement or cancel the trades without giving prior notice to the platform users, thereby upholding the integrity of the contractual terms as agreed upon by the parties[58].

Indeed, in analysing this case, it is noteworthy that Quoine should have established an express contractual provision that allowed for the cancellation of a smart contract under certain conditions. The presence of such a condition would have allowed for the application of a measure such as the restoration of the situation that existed before the conclusion of the smart contract.

Furthermore, the court's decision emphasises the importance of transparency and notice in contract modifications, as seen in its exploration of Quoine's unilateral actions to cancel the trades. The ruling suggests that for platforms and parties engaging in smart

[56] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 [96] – [128].
[57] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 [48] – [58].
[58] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.

contracts, clear communication of terms and any subsequent changes is essential to maintain the enforceability of the contracts.

On the claims of unjust enrichment and whether Quoine held the cryptocurrencies on trust for B2C2, the CA found no unjust enrichment, stating that the enrichment of B2C2 was a consequence of a valid contract[59]. Moreover, the judges concluded that there was no intention to create a trust relationship between Quoine and its users regarding the cryptocurrencies, further clarifying the legal nature of cryptocurrencies and their treatment under trust law in Singapore.

Contrary to the majority's decision, the dissenting judgement of Mance IJ offers a distinctive perspective on the application of unilateral mistake in contracts facilitated by deterministic algorithms[60]. Mance IJ proposed a broader interpretation of equitable mistake that considers the hypothetical awareness of B2C2, specifically Mr. Boonen, regarding the transactional errors, based on the circumstances at the time they transpired[61]. Mance IJ suggested that, had Mr. Boonen anticipated the transactions beforehand or been directly involved when they occurred, he would likely have recognised that the transactions were mistakenly executed. This approach by Mance IJ in adapting legal principles to accommodate the distinctive context of the case opens the door for ongoing discussions and potential evolution of legal doctrines in future cases involving similar technological complexities.

3.2 Clear position or unleashing a floodgate?

The Quoine v B2C2[62] case shines a light on key issues at the intersection of technology and legal principles, focusing on contracts created by deterministic algorithms, the responsibility tied to AI-driven decisions, the legal standing of cryptocurrencies, and the need to find the right balance between courts adapting to new realities and the need for predictable transactions.

The court’s decision in affirming algorithmically formed contracts highlights a milestone in the legal precedent as it acknowledges the transformation of digital transactions. The court’s assertion may potentially open Pandora's box when considering the implications of machine learning and AI technologies that can grow beyond their original programming. This development may present challenges to the conventional contract law concepts of intent and consent because the results can deviate significantly from the programmer's original intentions, thus putting pressure on the existing legal rules that govern automated contracts.

The difficulties in finding who is responsible for what AI systems do make legal matters even more complicated. This can be exemplified in situations where an AI chatbot learns

[59] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 [130] – [136].
[60] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 [152]-[203].
[61] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02 [183].
[62] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.

offensive language and spreads it to the users. In such cases, who is at fault? Is it the programmer who allowed the AI to learn it, or the users who provided the offensive words that enabled the AI to learn it? Situations like this put the traditional notions of blame and intention to the test in the digital world, making us reconsider who should be held accountable.

This case[63] also raises a discussion regarding the legal standing of digital assets by posing the question of whether cryptocurrencies should be regarded as property. The concept that cryptocurrencies might align with traditional property concepts is both innovative yet uncertain, particularly in explaining the specific nature of these digital assets. This uncertainty affects not just the applicability of trust law but also extends to taxation, inheritance, and insolvency, thereby stressing the need for a clearer legal assessment of cryptocurrencies.

The dissenting decision calls for a sophisticated response to the mistakes made by the algorithms of smart contracts to safeguard economic stability and ensure fair justice[64]. A potential misalignment between traditional legal approaches and the demands of modern technology-driven transactions can be illustrated by the hypothetical example of a hacking incident leading to mistaken transactions. This highlights the difficulty in applying age-old legal doctrines to the complexities of the digital economy.

While the case identifies these emerging challenges[65], it stops short of fully exploring avenues for legal adaptation to technological advancements. The discussion around AI hints at a critical concern but does not delve into potential legal reforms or frameworks that could effectively govern its evolving capabilities.

There seems to be a hinted tension between the judicial ability to adapt and the need for businesses to have certainty, possibly overlooking how legal principles can evolve to both embrace technological advancements and provide stable outcomes for businesses. To achieve a balance between innovation and predictability, future developments could consider hybrid approaches that incorporate technology-specific regulations or specialised dispute resolution mechanisms.

4 Legal position of smart contract Malaysia

Malaysia operates under a dual legal system that incorporates both common law principles and Sharia law. The primary legislation governing contracts is the Contracts Act 1950[66], which is rooted in English common law. The Act does not require contracts to be in a specific format, thereby implicitly recognizing the legality of contracts made through digital platforms, including smart contracts. The technological neutrality stance suggests

[63] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.
[64] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.
[65] Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.
[66] Contracts Act 1950 [Act 136] (Malaysia) available at <https://lom.agc.gov.my/ilims/upload/portal/akta/LOM/EN/Act%20136.pdf> accessed 25 July 2024.

that smart contracts could be considered legally binding if they meet the essential requirements outlined by Malaysian law: offer[67], acceptance[68], consideration[69], intention to establish legal relations, capacity to contract[70] and free consent[71].

Although the Act primarily addresses traditional contracts, the legitimacy and legal status of a smart contract depend on meeting these basic criteria outlined in the Act[72]. Compared to traditional contracts, smart contracts streamline the process of securing and documenting transactions from start to finish. The use of blockchain technology also guarantees that contract data is stored across a decentralised network, making it difficult to challenge the contract's validity after it has been executed[73]. Smart contracts stand out from traditional contracts in two main ways: how transactions are recorded and the use of automated ledgers[74].

Parties can automatically register a smart contract on the blockchain's distributed ledger by agreeing upon its conditions and adding their digital[75] or electronic signatures[76]. After the contract's execution, the computer program autonomously updates the next action, as regulated by the network's overseers. The ultimate disposition of a blockchain smart contract, particularly those devised by a specific entity, remains under their definitive supervision and control[77]. Smart contracts, being self-executing contracts, operate on an automated basis. Their supervision and control are achieved through embedded rules, blockchain transparency, immutability, and third-party verification[78]. While these features provide a high degree of automation and security, the ultimate control lies with the entity that deploys the smart contract. They design, deploy, and may potentially update the contract, ensuring that it aligns with their intended objectives. Blockchain's attribute of confidentiality governs the management and disclosure of contract particulars among the involved parties. Typically, the considerations within a

[67] ibid 2 (a).
[68] ibid 2 (b).
[69] ibid 2 (d).
[70] ibid 11.
[71] ibid 10.
[72] Wong (n 50).
[73] SM Nzuva, 'Smart Contracts Implementation, Applications, Benefits, and Limitations' (2019) 9(5) Journal of Information Engineering and Applications 63.
[74] Li and Kassem (n 54).
[75] Digital Signature Act 1997 [Act 562] (Malaysia) s. 62; Digital Signature Regulations 1998 [P.U.(A) 359/98] (Malaysia), available at <https://lom.agc.gov.my/ilims/upload/portal/akta/LOM/EN/Act%20562.pdf> accessed 25 July 2024.
[76] Electronic Commerce Act 2006 [Act 658] (Malaysia), s.9, available at <https://aseanconsumer.org/file/post_image/Act%20658%20-%20Electronic%20Commerce%20Act%202006.pdf> accessed 25 July 2024.
[77] C D Clack, V A Bakshi, and L Braine, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' [2016] arXiv:1608.00771 [preprint].
[78] D Maesa, P Mori, and L Ricci, 'A Blockchain Based Approach for the Definition of Auditable Access Control Systems' (2019) 84 Computer Security 93.

smart contract may encompass digital (or on-chain) assets and physical (or off-chain) assets[79].

Digital assets, especially cryptocurrencies, offer a frictionless and rapid means of executing payment transactions directly from users' cryptocurrency wallets or accounts, epitomising the convenience of instant payment systems. This stands in contrast to the handling of physical assets, which involves the exchange of stocks, currency, gold, or other valuables, with each transaction meticulously recorded on the blockchain's distributed ledger. The adoption of this technology into legal agreements signifies a remarkable transformation in legal practices, presenting both challenges and opportunities for recognizing and implementing smart contracts within established legal paradigms[80]. The regulatory framework for digital assets in Malaysia is currently shaped by the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019[81]. This regulation serves to define "digital currency" and "digital tokens," collectively referred to as "digital assets," as securities under the securities laws of Malaysia, thereby broadening the scope of "securities" under the Capital Markets and Services Act 2007[82] (CMSA) and bringing its oversight under the jurisdiction of the Securities Commission Malaysia (SC).

In response to this regulation, the SC revised the “Guidelines on Digital Assets”[83] and “Guidelines on Recognised Markets"[84] to specify the requirements and regulatory framework for digital asset platform operators on the Digital Asset Exchange. DAX is an online platform that facilitates the trading of digital assets. Per these guidelines, operators of the DAX must obtain registration as Recognised Market Operators under Section 34 of the CMSA and comply with the specified guidelines.

The crucial provisions that could be relevant to smart contracts within the Contract Acts 1950[85] are *amongst others:*

[79] A Deshpande, K Stewart, L Lepetit and S Gunashekar, Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards. Overview Report (The British Standards Institution (BSI) 2017) 40(40) 1-34.

[80] AJ McNamara and SM Sepasgozar, 'Intelligent Contract Adoption in the Construction Industry: Concept Development' (2021) 122 Automation in Construction 103452.

[81] Capital markets and services (Prescription of services) (digital services and digital token) Order 2019 [P.U (A) 12/2019] (Malaysia) available at <https://www.sc.com.my/api/documentms/download.ashx?id=8c8bc467-c750-466e-9a86-98c12fec4a77> accessed on 25 July 2024.

[82] Capital markets and services Act 2007 [Act 671] (Malaysia) available at <https://www.sc.com.my/api/documentms/download.ashx?id=70b43137-9a48-4540-b955-f1114ceb3445> accessed on 25 July 2024.

[83] Securities Commission, Guidelines on Digital Assets SC-GL/1-2020 (R2-2024) (Malaysia) available at <https://www.sc.com.my/api/documentms/download.ashx?id=e63db44c-b6d8-4ae9-adf1-afdf9b548d54> accessed on 25 July 2024.

[84] Securities Commission, Guidelines on Recognized Markets SC-GL/6-2015(R11-2024) (2024) (Malaysia) available at <https://www.sc.com.my/api/documentms/download.ashx?id=a36e1d80-9afd-4913-8dd8-51c889a60fec> accessed on 25 July 2024.

[85] Contracts Act 1950 (n 66).

- Section 10 (1) emphasises that all agreements constitute contracts if made by freely consenting parties competent to contract, for a lawful consideration and object, and not expressly declared void.
- Section 2 (a) defines a proposal as the expression of willingness by one party to do or refrain from doing something to gain the other's assent.
- Section 5(1) allows for revocation at any time before the acceptance communication is complete.
- Section 2(b) describes acceptance as a final and unconditional agreement to the offer's terms.
- Section 2 (d) explains that any act, abstinence, or promise by the promisee or another person at the promisor's desire constitutes consideration for the promise.

As previously mentioned, the integration of smart contracts into the Malaysian legal system is being shaped by the Contracts Act 1950[86]. However, the potential application of smart contracts in Islamic banking and financing introduces a unique blend of legal traditions, as it implies the application of Shariah principles. This interplay presents distinct challenges and opportunities for recognizing and enforcing smart contracts within the established legal framework.

While both common law and Shariah law influence Islamic banking, they operate within distinct frameworks. Common law governs the procedural aspects of disputes, while Shariah law ensures that financial contracts comply with Islamic principles[87]. Islamic banking disputes remain under the jurisdiction of civil courts due to the need to apply federal laws like the Contracts Act.

Civil courts may face challenges when Shariah non-compliance is raised, as not all judges are experts in Islamic finance. Therefore, special references to the Shariah Advisory Council are sometimes required for interpreting Shariah-related matters[88].

Scholars have observed that smart contracts, powered by blockchain technology, align well with the traditional paradigms of contract law[89]. This observation requires a strict

[86] ibid.

[87] A Trakic, 'The Adjudication of Shari'ah Issues in Islamic Financial Contracts: Is Malaysian Islamic Finance Litigation a Solution?' (2013) 29(4) Humanomics 260, 275.

[88] H Hasshan, 'Islamic finance litigation: Problems within the Malaysian civil courts structure' (2016) 20(1) Jurnal Undang-Undang dan Masyarakat 33, 39; S Miskam, NAM Puad, & NJ Rafdi, 'Reference to the Shari 'ah Advisory Council in Islamic Finance: Preliminary Analysis on Civil Court Decisions', in *Proceedings of the Social Sciences Research* (2014) *ICSSR*, 9-10; Bank Negara Malaysia, Manual Rujukan Mahkamah dan Penimbangtara kepada Majlis Penasihat Shari'ah (Bank Negara Malaysia 2015) available at <http://www.bnm.gov.my/?ch=7&pg=1038&ac=419&bb-file1> accessed 14 June 2015.

[89] NRBM Zain, ERAE Ali, A Abideen, and HA Rahman, 'Smart Contract in Blockchain: An Exploration of Legal Framework in Malaysia' (2019) 27(2) Intellectual Discourse 595, 617; N Ismail, Z Ismail, O Musa, and C Loy, 'Malaysia Zakat Smart Contract Architectural Framework Design' (2023) 13(5) International Journal of Academic Research in Business and Social Sciences; DN Bolhassan and others, 'Towards Adoption of Smart Contract in Construction Industry in Malaysia' (2022) 30(1) Pertanika Journal of Science & Technology; A Aborujilah, MNBM Yatim, and A Al-Othmani, 'Blockchain-Based Adoption Framework for Authentic Land Registry System in Malaysia' (2021) 19(6) TELKOMNIKA (Telecommunication Computing Electronics and Control) 2038-2049; KJ Yong, ES Tay, and DW Khong (n 14).

adherence to the requirements prescribed in the Contracts Act 1950[90]. Although the regulator has made some progress in updating its policies regarding digital assets and navigating the new technological landscapes introduced by blockchain, there is a significant push for broadening the legal definition of electronic transactions to comprehensively include the activities facilitated by smart contracts and blockchain technology.

In Malaysia, the Personal Data Protection Act 2010[91] is the cornerstone of data protection legislation, setting out the obligations for data users and granting rights to data subjects regarding their personal data. Additionally, it outlines seven principles for processing personal data[92]. Although the Act doesn't specifically mention blockchain technologies and smart contracts, its provisions may conflict with blockchain's fundamental traits. The retention principle[93], which mandates the deletion of personal data when no longer needed, contradicts blockchain's core feature of permanently recording transactions on decentralised ledgers. This requirement challenges the feasibility of aligning blockchain's immutable record-keeping with conventional data protection norms.

Section 12 of the Act[94] allows individuals to access and correct their personal data, but this right clashes with the immutable nature of blockchain technology, where changes require network consensus. To reconcile this, the blockchain community proposes using permissioned blockchains for better control and conducting off-chain transactions to isolate data, aligning with data protection laws while preserving blockchain's essential characteristics[95].

Although smart contracts are theoretically compatible with Contracts Act 1950[96] and other regulations related to them, their unique features, such as the ability to execute transactions automatically, bring up important issues about their enforceability, especially when disputes arise. The conventional mechanisms of dispute resolution and contract enforcement within the Malaysian jurisdiction are built on judicial intervention, a paradigm potentially at odds with the inherently autonomous nature of smart contracts. Therefore, while it's possible to recognize smart contracts within existing legal frameworks in theory, there are real challenges to their practical enforceability and the resolution of conflicts.

[90] Contracts Act 1950 (n 66).
[91] Personal Data Protection Act 2010, [Act 709] (Malaysia) available at <https://mia.org.my/wp-content/uploads/2022/05/Personal.Data_.Protection.Act_.2010.pdf> accessed on 25 July 2024.
[92] ibid 5.
[93] ibid 10.
[94] ibid 12.
[95] International Association for Trusted Blockchain Applications, Report on Data Protection Regulations Applicable to Blockchain Technology in Different Jurisdictions Worldwide (December 2020) <https://o.inatba.org/wp-content/uploads/2021/01/2020-12-Privacy-WG-Report-on-Data-Protection-005.pdf> accessed 10 October 2024; Wong (n 50).
[96] Contracts Act 1950 (n 66).

4.1 Case analysis

The case of Robert Ong Thien Cheng v Luno Pte Ltd & Anor[97] cements a pivotal position on the legality and enforceability of smart contracts.

During the cryptocurrency surge of 2017, a conflict emerged between Luno Pte Ltd, a renowned digital currency exchange in Malaysia, and one of its customers, Robert Ong Thien Cheng[98]. Robert, the appellant, deposited a sum of RM300,000 into Luno's account, which was converted into 11.3 BTC and transferred to his Bitfinex account. Due to a system error, an additional 11.3 BTC was mistakenly sent to Robert. Robert acknowledged the mistake but did not return the additional bitcoins. Instead, he used the bitcoins for trading activities, which resulted in a loss, and later proposed to repay RM300,000. This amount was considered insufficient because of the volatility in Bitcoin's price. Consequently, Luno initiated legal action to recover the 11.3 BTC or its equivalent market value, prompting a legal review based on Section 73 of the Contracts Act 1950, which deals with the recovery of mistakenly received property[99].

The legal action initiated by the Appellant under Section 73 of the Contracts Act 1950[100], which mandates the restitution of money or property received by mistake or coercion, brought to light the legal quandary of categorising Bitcoins. The Appellant argued against the classification of Bitcoins as a 'thing' returnable in the context of Section 73 of the Contracts Act 1950.

The High Court's decision underscored the imperative for the Contracts Act 1950 to evolve in tandem with advancements in technology and commercial practices. The court held amongst others that:-

> *"[15] The Respondents were also correct that it cannot be disputed that it is a form of 'commodity' as real money is used to purchase the cryptocurrency. In this regard, there is indeed value attached to the Bitcoin in the same way as value is attached to 'shares'.*
>
> *[16] I also agree with the view that the Contracts Act, 1950 having been drafted some 7 decades ago ought to be construed to reflect changes in modern technology and commerce.*
>
> *[17] Hence, rightfully Bitcoins ought to fall under the ambit and application of the term 'anything' under Section 73 of the Contract Act 1950 and therefore, the Appellant is bound to return the same to the Respondents if the circumstances*

[97] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143.
[98] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143; Tan Zu Hao, 'Malaysia: Crypto Law In Malaysia' (Mondaq, 7 November 2022) <https://www.mondaq.com/fin-tech/1248146/crypto-law-in-malaysia> accessed 10 February 2024.
[99] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143; Tan Zu Hao, 'Malaysia: Crypto Law In Malaysia' (Mondaq, 7 November 2022) <https://www.mondaq.com/fin-tech/1248146/crypto-law-in-malaysia> accessed 10 February 2024.
[100] Contracts Act 1950 (n 66).

warrant it. In this regard, the term 'anything' is plainly wide enough to cover Bitcoins"[101].

The High Court acknowledged the Respondents' assertion that, although cryptocurrency does not constitute 'money' or legal tender in the conventional sense, it has been classified as a form of 'security' by the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019[102]. The Court also observed that cryptocurrency acts as a "commodity" because it is bought with real money and carries intrinsic value, similar to shares.[103] It further acknowledged that the legal framework, which was put in place seven decades ago, needs to be applied in a way that takes into account the advances in technology and changes in the commercial environment of today. As a result, the Court ruled that Bitcoin fall under the definition of 'anything' as specified in Section 73 of the Contracts Act 1950[104], making it obligatory for the Appellant to return the Bitcoin under appropriate circumstances.

The court judgment demonstrates the readiness of the judiciary to adapt established legal norms to align with the changing landscapes of contemporary technology and business practices. Additionally, the recognition from the judiciary further cements the legal standing of cryptocurrencies within the legal framework, highlighting the judiciary's responsiveness to the current evolving state of law and technology.

5 The Diverse Applications of Smart Contracts Across Industries

The exploration of smart contracts, highlighted by scholars and legal experts in Singapore and Malaysia, focuses on streamlining contractual processes across various domains, including landlord-tenant agreements[105], banking and fintech[106], retail, manufacturing, healthcare[107] and construction contracts. This represents a significant intersection between technological advancements and the legal framework of the nation.

A study conducted on the potential use of smart contracts in tenancy agreements emphasises how blockchain technology seeks to improve the efficiency, transparency, and security of transactions[108]. However, the authors also highlight that the integration of such

[101] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143.
[102] Capital markets Act (n 81).
[103] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143.
[104] Contracts Act 1950 (n 66).
[105] Yong, Tay and Khong (n 14).
[106] V Nienhaus, 'Blockchain Technologies and the Prospects of Smart Contracts in Islamic Finance' in *Fintech in Islamic Finance* (Routledge 2019) 183, 210; M F Roslan, O Bamahriz, A Muneeza, J Chu, Z Mustapha, and M Z Ahmad, 'Application of Tawarruq in Islamic Banking in Malaysia: Towards Smart Tawarruq' (2020) 7(2) International Journal of Management and Applied Research 104, 119; O Chowdhury, M A S A Rishat, M H B Azam and MA Amin, 'The Rise of Blockchain Technology in Shariah Based Banking System' in Proceedings of the 2nd International Conference on Computing Advancements (March 2022) 349, 358.
[107] Muhammad Izdihar Sahalan, Fathi Yusof, and Hafiza Abas, 'The Challenges of Using Blockchain Technology for Medical Data in Public Hospitals in Malaysia' (2023) 11(2) Open International Journal of Informatics 90, 105.
[108] Yong, Tay and Khong (n 14).

technologies introduces complex legal considerations regarding their validity, adherence to regulatory standards, and implications for established legal procedures. Smart tenancies leverage blockchain's architecture to automate contractual obligations, demanding conformity with principal legislation in Malaysia such as the Stamp Act 1949[109] and the Electronic Commerce Act 2006[110], ensuring that smart tenancy contracts are legally recognised. Despite the automation, the necessity for conventional dispute resolution frameworks remains, given the legal system's safeguards against self-execution of eviction, thus protecting tenants' rights amidst technological advancements.

Scholars have pointed out that Malaysian regulators are urged to view smart tenancy solutions as instruments for enhancing tenancy management efficiency rather than as disruptive innovations[111]. This highlights the need for a review to clarify the legal status of smart tenancies, promoting innovation while ensuring robust legal and consumer protections.

Smart contracts have revolutionised Islamic finance in the banking sector[112]. The contracts allow the automation of Murabaha transactions, a foundation of Islamic banking, ensuring compliance with Shariah principles. Smart contracts guarantee transactional integrity via immutable public ledger recordings, preserve anonymity, and preclude disputes by strictly adhering to contract conditions[113]. This approach reduces uncertainties, minimises the risks of default, simplifies financial processes[114], cuts operational expenses, and removes the need for paper-based documentation, thereby bolstering the efficiency and dependability of financial services[115].

Moreover, integrating Sharia governance into smart contracts introduces a layer of compliance, which is crucial for Islamic finance institutions. Once regulators like Bank Negara Malaysia are integrated into the blockchain, transactions can be validated for Sharia compliance in real time[116]. If non-compliant transactions are detected, they will be automatically rejected[117].

This innovation aligns seamlessly with the ethical principles of Islamic finance, while also enhancing financial transparency and ensuring strict adherence to regulatory standards[118].

---

[109] *STAMP ACT* 1949 [Act 378] (Malaysia) available at <https://phl.hasil.gov.my/pdf/pdfam/Stamp_Act_1949_as_at_01072014.pdf> accessed on 20 July 2024.
[110] Electronic Commerce Act 2006 [Act 658] (Malaysia), available at <https://aseanconsumer.org/file/post_image/Act%20658%20-%20Electronic%20Commerce%20Act%202006.pdf> accessed 25 July 2024.
[111] Yong, Tay and Khong (n 14).
[112] Nienhaus (n 106).
[113] ibid.
[114] Roslan, Bamahriz, Muneeza, Chu, Mustapha, and Ahmad (n 106).
[115] Nienhaus (n 106).
[116] Roslan, Bamahriz, Muneeza, Chu, Mustapha, and Ahmad (n 106).
[117] ibid.
[118] ibid.

This technological advancement also extends to the realm of Islamic finance management, notably in the context of zakat[119]. The application of smart contracts to zakat highlights how easily technology can integrate with religious obligations, demonstrating the flexibility and wide range of uses for blockchain technology. By automating zakat collection and distribution, blockchain enhances the efficiency, transparency, and security of these transactions. It ensures that zakat reaches the correct beneficiaries, thereby reducing the risk of mismanagement or corruption[120]. Compliance with Islamic law and honouring the religious significance of zakat are crucial in this process. With blockchain's immutability offering transparent and accountable transactions, the deployment of smart contracts for zakat management aims to bolster public trust in zakat institutions, demonstrating the profound impact of technology on fulfilling religious obligations[121].

The application of smart contracts in Islamic finance operates within Malaysia's dual legal framework[122], which uniquely combines common law and Islamic law. In cases of disputes arising from Islamic banking contracts, the principles of contract law, derived from common law, remain applicable. However, their interpretation and application must be harmonised with Islamic principles, underscoring the importance of both legal systems in shaping Malaysia's legal landscape. This dual legal framework not only ensures that Islamic financial products comply with Shariah principles but also integrates them into the broader legal system, providing a comprehensive approach to resolving disputes and enforcing contracts.

In the construction industry, the potential adoption of smart contracts could offer substantial advantages such as automation and efficiency, improved risk apportionment, enhanced transparency, and trust, alongside payment security and cash flow improvements[123]. Automation simplifies contract management, minimises time consumption, and effectively resolves conflicts and disputes. The self-executing nature of smart contracts ensures a clear distribution of risks and responsibilities without manual intervention or intermediaries. Digitising contracts within blockchain technology provides all parties with equal access to information, reducing misunderstandings and fostering a transparent environment[124]. Additionally, smart contracts automate payments upon

[119] ibid.
[120] Ismail, Ismail, Musa, and Loy (n 89).
[121] ibid.
[122] Hasshan (n 88); Miskam, Puad, & Rafdi (n 88); Bank Negara Malaysia (2015). Manual Rujukan Mahkamah dan Penimbangtara kepada Majlis Penasihat Shari'ah Bank Negara Malaysia, accessed 14 June 2015, <http://www.bnm.gov.my/?ch=7&pg=1038&ac=419&bb-file1> accessed 1 November 2024.
[123] Bolhassan and others (n 89).
[124] A Abdelghany, 'Navigating the Complexity of Construction Contracts and the Value of Blockchain Technology: A Systems Dynamics Perspective - Review Paper' (2024) 3(1) International Journal of Automation and Digital Transformation 44, 64.

meeting predefined conditions, addressing the industry's challenge of delayed payments and positively impacting cash flow[125].

However, the widespread adoption of smart contracts in the construction sector, as well as other industries, faces challenges such as legal and regulatory uncertainties, technical and infrastructure challenges, and the volatility associated with cryptocurrency transactions[126]. These challenges highlight the need for legal clarifications, technological infrastructure investments, and broader acceptance of digital currencies to fully leverage the benefits of smart contracts.

Similar to the discussion on smart tenancies and the deployment of smart contracts for zakat management, the application of smart contracts in the construction sector and other industries raises legal and regulatory considerations. It requires a thorough review of existing laws and may necessitate regulatory amendments, or the introduction of new guidelines tailored to the use of blockchain technology in various sectors.

Together, these explorations into smart tenancies, zakat management, and the construction sector via smart contracts signify the transformative potential of smart contracts. They highlight the need for a collaborative effort among technology developers, legal professionals, regulatory bodies, and industry stakeholders. This collective approach aims to harmonise technological innovations with the legal and regulatory frameworks in Singapore and Malaysia, ensuring that the benefits of smart contracts are maximised while safeguarding the interests of all stakeholders involved.

6 The adaptability

The inherent adaptability within the legal systems of Malaysia and Singapore, deeply rooted in their common law heritage, is particularly evident in their handling of smart contracts amidst the rapidly evolving landscape of digital innovation. This adaptability is supported by the technology-neutral orientation of the Malaysian Contracts Act 1950[127], and equally, by the flexible nature of Singaporean Contract Law, which allows for the execution of contracts in diverse formats without strict legal mandates. Such legislative openness, paired with the common law tradition's focus on judicial interpretation and the principle of precedent, facilitates the smooth incorporation of technological advancement[128], particularly digital agreements, including those executed on blockchain platforms. The capacity for case law to evolve in response to technological advances, sidestepping the lengthy processes often linked to legislative change, showcases the

[125] Katharina Sigalov, Xuling Ye, Markus König, Philipp Hagedorn, Florian Blum, Benedikt Severin, Michael Hettmer, Philipp Hückinghaus, Jens Wölkerling and Dominik Groß, 'Automated Payment and Contract Management in the Construction Industry by Integrating Building Information Modeling and Blockchain-Based Smart Contracts' (2021) 11(16) Applied Sciences 7653.
[126] Bolhassan and others (n 89).
[127] Act 136, Contracts Act 1950 Act 136 (Malaysia) (n 66).
[128] LB Moses, 'Adapting the Law to Technological Change: A Comparison of Common Law and Legislation' (2003) 26(2) The University of New South Wales Law Journal 394-417.

adeptness of both the Malaysian and Singaporean legal frameworks in navigating the swift shifts that define the modern digital era.

The judiciary's role in adapting its interpretations in line with new technological advancements further highlights its flexibility. Through landmark case law[129], courts have demonstrated their readiness to extend traditional legal doctrines to cover digital transactions and assets as well as to set a precedent for the legal standing of contracts created by automated systems, such as smart contracts. This willingness to apply well-established legal principles—such as those found in the Electronic Transactions Act (ETA)[130] and Singapore's principles of contract law—in modern times without the need for new legislation demonstrates the common law system's effectiveness. It guarantees that the legal system will continue to be flexible and capable of handling the complexities brought about by digital innovations.

Both legal systems have shown progressive stances in acknowledging digital assets. In Malaysia, cryptocurrencies are explicitly recognised as a form of "security," integrating digital currencies into the legal and regulatory framework of the financial market[131].

The recognition and acknowledgment of contracts generated by algorithms and of digital assets are crucial for the enforcement and adjudication of smart contracts involving digital assets, offering a degree of legal clarity and stability amidst the fast-paced evolution of digital transactions.

The flexibility of the common law system is one of its advantages but given the speed at which technology is developing and the unique qualities of digital contracts, further guidance from the regulatory body would be helpful. Proactive legislative steps will strengthen the legal framework's resilience in adapting to the ever-changing nature of digital transactions while also assisting the judicial system in rendering well-informed verdicts. This strategy would improve Malaysia's standing as a jurisdiction that both upholds legal traditions and welcomes technological advancement by ensuring a more consistent and predictable legal environment for the growth of digital commerce.

This approach aims to ensure a more cohesive and predictable legal environment for digital commerce's expansion, enhancing Malaysia and Singapore's positions as countries that preserve legal traditions while embracing technological advancements.

7 Technological Neutrality versus Operational Specificity

Although contracts carried out on digital platforms, such as smart contracts, are supposedly covered by the Act's inherent technological neutrality, applying it to these modern contractual forms is more complex. The essence of smart contracts—predominantly characterised by their automation and reliance on blockchain technology—

[129] Robert Ong Thien Cheng v Luno Pte Ltd & Anor [2020] 3 AMR 143; Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02.
[130] Electronic transaction Act 2010 (Singapore) (n 41).
[131] Capital markets Act (n 81).

introduces a paradigm shift in how transactions are executed and recorded, diverging significantly from traditional contract law's manual and judicially supervised processes.

The integration of smart contracts within the framework established in the Contracts Act 1950 in Malaysian law poses several intricate issues that require a thorough assessment of potential legislative and procedural adjustments. This change calls for an examination of how the technological neutrality of the Act, while beneficial for accommodating the formative stages of digital contracts, may fall short in addressing the complex realities of blockchain technology and smart contract execution. Although the contract law in both Malaysia and Singapore can accommodate smart contracts, certain complexities require clarity in specific contexts, especially regarding the unique attributes of smart contracts—automation, blockchain dependency, and self-executing mechanisms. These attributes deviate from the traditional approach to contract execution and enforcement, potentially leading to differing judicial interpretations in both jurisdictions.

A supporting example can be drawn from the UK's Law Commission[132], which similarly recognised that while existing legal frameworks are robust enough to accommodate smart contracts, further clarification is needed to ensure legal certainty. The UK Law Commission concluded that the current legal framework is sufficiently robust to support smart legal contracts, with only incremental developments needed to adapt to specific contexts. The challenges posed by smart contracts are not fundamentally different from those of traditional contracts. While some novel legal issues may arise, such as the interpretation of coded terms, the flexibility of English common law allows it to accommodate these challenges without necessitating a separate legal regime.

This example from the UK suggests that contract law in Singapore and Malaysia can similarly support smart contracts, but it underscores the need for clearer legal guidance to ensure that emerging issues are adequately addressed. The UKJT Legal Statement[133] further highlights that minor, focused reforms, rather than the creation of a new legal regime, can provide the necessary legal infrastructure to foster confidence in smart contracts. By drawing on these lessons, Malaysia and Singapore could issue legal statements or guidelines to harmonise the interpretation and enforcement of smart contracts within their own jurisdictions. Such proactive measures would not only enhance legal certainty but would also support the broader adoption of smart contracts in these jurisdictions, ensuring that both Malaysia and Singapore remain at the forefront of legal adaptability and technological advancement in their common law systems.

[132] Law Commission, Smart legal contracts, advice to government, CP563 (2021) at <https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2021/11/Smart-legal-contracts-accessible.pdf> accessed 21 October 2024.

[133] UK Jurisdiction Taskforce, Legal statement on cryptoassets and smart contracts (2019) ("UKJT Legal Statement"), <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> accessed 21 October 2024.

Although there are two landmark cases in both countries, the case from the Court of Appeal in Singapore provides a strong binding precedent, whereas one of the landmark cases from the High Court in Malaysia does not yet have the same level of influence. While some degree of stare decisis and legal certainty exists, future cases may deviate from the current understanding until the Federal Court of Malaysia establishes its position. A misinterpretation in future case law could complicate and destabilize the status of smart contracts. Therefore, as courts grapple with the challenge of interpreting smart contracts within the framework of established legal doctrines, the introduction of explicit statutory guidance could enhance certainty. For instance, the UKJT Digital Dispute Resolution Rules[134], chaired by Sir Geoffrey Vos, offers a framework specifically designed to resolve disputes arising from smart contracts, digital assets, and distributed ledger technology. These rules emphasise rapid arbitration, on-chain resolution with private keys, and tailored procedures for digital assets—key innovations that could serve as instructive examples for Malaysia and Singapore. By adopting similar mechanisms, such as expert-led determinations and the possibility of direct on-chain execution of decisions, Malaysia and Singapore could ensure that their legal systems are responsive to the technological demands of automated contracts and digital assets.

Moreover, the UKJT's focus on ensuring that disputes are resolved by individuals with both legal and technical expertise is critical in a landscape where smart contracts and digital assets are highly technical. This could help minimise judicial inconsistencies and foster more informed interpretations in Malaysia and Singapore. Additionally, the provision for party anonymity and rapid dispute resolution, with clear enforcement mechanisms, could be beneficial for cross-border transactions involving decentralised technologies, which frequently span multiple jurisdictions. The adoption of similar guidelines could reduce legal uncertainty, promote consistency in judicial interpretation, and further strengthen Malaysia and Singapore's positions as favourable jurisdictions for handling disputes involving novel digital technologies This situation, exemplified by the findings on smart tenancies[135], illustrates a tangible example of the complexities involved. The study highlights the reluctance of tenants to adopt cryptocurrency payment methods due to the necessity of upfront payments and the volatility of cryptocurrencies, which complicates the conversion to fiat currency for periodic rent payments. These practical difficulties, alongside concerns about the acceptance of cryptocurrency as a payment method and its legal status as tender, underscore the broader issue of technological adaptability within legal practices. The Act's technological neutrality, while intended to be inclusive, may instead lead to a legal landscape characterised by divergent outcomes and varied judicial interpretations. This variability risks creating a legal environment of

[134] UK Jurisdiction Taskforce, Digital Dispute Resolution Rules (2021) <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp- content/uploads/2021/04/Lawtech_DDRR_Final.pdf> accessed 10 October 2024.
[135] Yong, Tay and Khong (n 14).

inconsistencies, posing a significant challenge to the legal certainty and predictability that are crucial for the growth of the digital economy.

This potential for legal fragmentation underscores the imperative for a nuanced strategic approach that transcends mere accommodation of technology to actively sculpting the legal landscape to address the intricacies of smart contracts. By instituting explicit legal guidelines that cater to the distinctiveness of smart contracts—clarifying their legal status, operational boundaries, and the framework for dispute resolution—the legislature can significantly reduce the ambiguity that currently permits wide judicial discretion[136]. Following steps like those taken in the UK[137] could be highly beneficial. In the UK, non-binding statements and guidelines have been issued to clarify the legal issues of smart contracts and digital assets.

Building on the proactive strategies seen in the UK, Australia offers an added perspective by demonstrating how existing legal frameworks can effectively accommodate smart contracts without the need for new legislation[138]. Smart contracts are considered enforceable as they meet essential contract criteria—agreement, consideration, and intent. The Electronic Transactions Act 1999[139] further supports their validity as electronic transactions, while the Australian Consumer Law[140] extends protections, such as unfair contract term provisions, to smart contracts, ensuring fairness and transparency comparable to traditional contracts. Australia emphasizes clarity in coded terms, encouraging businesses to provide plain language explanations to make smart contracts accessible to consumers, thereby addressing potential imbalances in technical literacy[141]. Regulatory bodies, notably the Australian Competition and Consumer Commission, actively monitor smart contracts for unfair practices. Australia has also taken steps to integrate smart contracts within its legal system, with initiatives such as the Australian National Blockchain[142] aiming to provide a platform for legally enforceable smart contracts.

These examples illustrate how common law jurisdictions can evolve their legal systems to accommodate technological advancements effectively. This shall not be taken as a proposal to introduce new legislation but merely a guideline. Such guidelines could clarify the legal status, operational boundaries, and dispute resolution mechanisms of smart contracts, providing a framework that guides judicial interpretation without restricting

[136] Zain, Ali, Abideen, and Rahman (n 89).
[137] UK Jurisdiction Taskforce, Legal statement on cryptoassets and smart contracts (n 133).
[138] ST Nguyen, 'Consumer Protection Against Unfair Contract Terms in the Age of Smart Contracts' (2023) 51(4) Federal Law Review 487.
[139] Electronic Transactions Act 1999 Act No 162 of 1999 (Australia) <https://www.legislation.gov.au/C2004A00553/latest/text> accessed 10 October 2024.
[140] Competition and Consumer Act 2010 No 51 of 1974 (Australia) <https://www.legislation.gov.au/C2004A00109/latest/text> accessed 10 October 2024.
[141] ST Nguyen (n 138); Matthew McMillan et al, 'Australia: Smart(er) Contracts in 2020' Mondaq (Web Page, 9 August 2020) <https://www.mondaq.com/australia/new-technology/974460/smarter-contracts-in-2020> accessed 25 October 2024.
[142] Australia developing national blockchain for legal contracts at <https://www.ledgerinsights.com/australian-national-blockchain-smart-legal-contracts/> accessed 25 October 2024.

the existing legislative framework. This targeted action would serve to guide judicial interpretation without restricting the Act, channelling it within a framework that reflects the technological specificities and societal implications of smart contracts.

Moreover, beyond legislative reform, there is a pressing need for a comprehensive strategy that includes judicial education and the development of jurisprudential guidelines on smart contracts. This approach would ensure that the judiciary is not only informed by a clear legislative framework but is also equipped with the understanding necessary to interpret smart contracts in a manner that is consistent, predictable, and aligned with the technological realities of the digital age.

The enforceability of smart contracts within the Malaysian legal system represents a critical junction at which traditional legal doctrines encounter the innovative mechanisms of digital transactions. The foundational legal principle, viewing contracts as agreements necessitating human oversight for both execution and dispute resolution, is challenged by the advent of smart contracts. These digital agreements, characterised by their autonomous execution upon predefined conditions, introduce a paradigm where judicial intervention may be bypassed, raising profound questions about the available mechanisms for resolving disputes that arise from such contracts.

The immutable and decentralised nature of blockchain technology, which underpins smart contracts, further complicates this scenario. It disrupts traditional methods of legal recourse and contract amendment, presenting a unique conundrum for the legal system. The resolution of disputes stemming from smart contracts necessitates a departure from conventional approaches, due to the technology's ability to execute transactions without direct human control and to record these transactions in a manner that is both permanent and resistant to unilateral modifications.

In the Malaysian case of Robert Ong Thien Cheng v Luno Pte Ltd & Anor[143] illuminates the Malaysian judiciary's capacity to adapt legal principles to the realm of emerging technologies, showcasing a notable flexibility in dealing with the intricacies of digital transactions and smart contracts. This case underscores the judiciary's adaptability, yet it simultaneously signals a pressing need for a more structured and systematic legal framework. Such a framework would adeptly address the nuances inherent in digital transactions, especially those involving smart contracts, aligning the autonomous operations of these contracts with the core tenets of contract law and dispute resolution. The evolution of technology necessitates a legal system that is both responsive and effective, ensuring that foundational legal principles can be applied reliably in the context of technological advancement.

To address the emerging legal challenges posed by smart contracts and digital transactions, the establishment of a specialised technological division within the judiciary of countries like Singapore and Malaysia represents a forward-looking approach to

[143] *Robert Ong Thien Cheng v Luno Pte Ltd & Anor* [2020] 3 AMR 143.

modernising the legal framework. Singapore has made notable progress in this area with the creation of the Technology, Infrastructure and Construction List (TIC List) within the Singapore International Commercial Court (SICC)[144]. This list is specifically designed to handle disputes involving technology, infrastructure, and construction projects, showcasing innovative case management protocols and optional voluntary processes such as the Simplified Adjudication Process and the Pre-Action Protocol. These measures are aimed at efficiently managing technically complex disputes as well as ensuring that cases are heard by experts in the field, thereby improving the transparency and effectiveness of legal proceedings.

On the other hand, Malaysia's commercial courts, which already have divisions specialising in areas like admiralty, construction, and intellectual property, hint at a framework that is adaptable to specialised needs. However, the need of having a division dedicated to technology would significantly enhance the judiciary's ability to deal with disputes arising from digital contracts by combining the legal insight of judges and lawyers with the technical insights of engineers and IT specialists. This would bridge the existing gap between traditional legal practices and the specialised requirements of digital contracts, thus reinforcing the judiciary's capability to navigate technology-centric legal issues and demonstrating a proactive stance towards integrating the legal system with the digital economy.

The adoption of alternative dispute resolution (ADR) tailored for smart contracts suggests a viable solution to efficiently resolve conflicts within the digital context of these agreements. By embodying the decentralised and automated nature of smart contracts, such ADR mechanisms could offer a dispute resolution process that is both swift and equitable, resonating with the operational dynamics of smart contracts.

In addressing disputes arising from smart contracts, two distinct methods have emerged: smart dispute resolution[145] and blockchain-based arbitration. Smart dispute resolution mechanisms are online platforms that aim to resolve disputes without traditional recognition and enforcement procedures. This method leverages crowd-sourced adjudication to resolve disputes. A group of users votes on the outcome, and oracles, acting as neutral intermediaries, input this decision into smart contracts[146]. While efficient for small-value, high-volume disputes involving on-chain assets, this approach raises concerns about the quality of decision-making, impartiality, and lack of legal enforceability[147]. It essentially reshapes dispute resolution, prioritising speed and automation over procedural fairness and justice[148].

[144] Singapore International Commercial Court, 'The Technology, Infrastructure and Construction List (SICC)', <https://www.judiciary.gov.sg/singapore-international-commercial-court#:~:text=The%20Technology%2C%20Infrastructure%20and%20Construction%20List%20(%E2%80%9CTIC%20List%E2%80%9D,to%20infrastructure%20and%20construction%20projects> accessed 25 October 2024.
[145] Palombo, Battaglini and Cantisani (n 26).
[146] ibid.
[147] Ortolani (n 26).
[148] ibid.

On the other hand, an innovative development in this area is blockchain-based arbitration[149], which aims to combine the benefits of distributed ledger technology with the enforceability of traditional arbitration. This approach seeks to create legally binding procedures that produce enforceable awards, potentially recognised under international conventions like the 1958 New York Convention. This method involves a predefined number of impartial arbitrators who conduct proceedings in compliance with legal standards, resulting in legally binding and enforceable awards. The arbitration clause and procedures are embedded within the smart contract from the outset, allowing the arbitral award to be recognised by the smart contract and automatically enforced on the blockchain. Blockchain-based arbitration combines the enforceability of traditional arbitration with the efficiency of blockchain technology, making it suitable for complex, higher-value disputes that require legal expertise. However, it faces challenges in integrating arbitration procedures into smart contracts, enforcing decisions involving off-chain assets, and potentially reintroducing complexities and costs associated with traditional arbitration. However, practical implementation may prove arduous.

A critical point to consider is the scenario in which an arbitral award is granted to a party utilising a smart contract, especially when the monetary arbitration award is not encompassed within the original terms of the smart contract[150]. To ensure effectiveness, the arbitration procedures must be integrated into the smart contract from the outset. This means that the smart contract should inherently include the option for arbitration, thereby standardising the contract to accommodate such resolutions[151]. For the award to be recognised and implemented by the blockchain infrastructure, it would need to be introduced into the system via an oracle by the arbitral tribunal. This incorporation allows the smart contract to execute the tribunal's award.

Despite the appeal of combining blockchain technology with arbitration, implementation faces significant challenges. Parties may be unwilling to lock significant amounts of cryptocurrency in escrow for extended periods due to liquidity needs and the volatility of cryptocurrencies. This economic consideration limits the viability of blockchain-based, self-enforcing arbitration for higher-value disputes. Moreover, the self-enforcing nature of blockchain mechanisms is limited to assets that exist on the blockchain. Disputes involving "off-chain" assets or requiring remedies beyond the blockchain's scope cannot be fully resolved through blockchain mechanisms alone, necessitating reliance on traditional legal enforcement procedures.

The key difference between the two methods lies in their approach to legal enforceability and procedural fairness. Smart dispute resolution offers speed and automation but lacks legal recognition and may compromise justice due to its reliance on

[149] Salger (26).
[150] Wong (n 50).
[151] D W Allen, A M Lane and M Poblet, 'The Governance of Blockchain Dispute Resolution' (2019) 25 Harv Negot L Rev 75.

economic incentives and non-expert adjudication. Blockchain-based arbitration provides legally enforceable outcomes and adheres to due process but may conflict with the decentralised nature of smart contracts and requires more complex integration and higher costs. These differences have significant implications for legal frameworks, as they determine the extent to which dispute resolution outcomes are recognized and enforceable under existing laws.

To effectively address disputes arising from smart contracts, it is crucial to design dispute resolution mechanisms that align with traditional legal principles while leveraging technological innovations. This means ensuring that mechanisms like blockchain-based arbitration are carefully integrated into smart contracts to provide both on-chain efficiency and off-chain legal enforceability. Such integration helps bridge the gap between the capabilities of smart contracts and the requirements for enforceable judgments and awards, ensuring that technological advancements enhance rather than undermine the legal safeguards essential for fair and just dispute resolution.

In light of potential abuses, Cuttell[152] suggests the appointment of a neutral adjudicator to resolve disputes between parties, such as landlords and tenants, within smart tenancy agreements. This adjudicator would have the authority to enforce decisions by instructing the smart tenancy program to issue payments to the rightful party as necessary[153]. However, this approach seemingly contradicts the inherent purpose of smart contracts, which aim to reduce the need for third-party enforcement and thereby achieve cost savings in enforcement and compliance. Moreover, integrating third-party adjudicators introduces challenges regarding the independence and impartiality required for arbitration, and may not meet the legal standards necessary to qualify as an arbitral process. This highlights a tension between the theoretical advantages of smart contracts and the practical need for dispute resolution mechanisms in certain contexts.

Therefore, while blockchain technologies and smart contracts offer promising avenues for innovative dispute resolution mechanisms, integrating these with existing legal frameworks remains complex. The limitations of self-enforcement, especially for off-chain assets, and the challenges in ensuring legally enforceable outcomes necessitate careful consideration. As the technology evolves, there may be potential for broader application, but for now, reliance on traditional recognition and enforcement procedures remains essential for certain types of disputes.

Furthermore, it is crucial for Malaysia and Singapore to proactively update its legal and regulatory framework to incorporate smart contracts and digital assets. Such updates should clearly define the guidelines for the creation, execution, and enforcement of smart contracts, considering the unique aspects of digital assets and blockchain technology.

[152] Henry Cuttell, 'Blockchain-based Smart Tenancy Agreements' (Individual Project Report, Imperial College London, 2017) at <https://www.imperial.ac.uk/media/imperial-college/faculty-of-engineering/computing/public/1617-ug-projects/Henry-Cuttell---Blockchain-based-Smart-Tenancy-Agreements.pdf> accessed 25 October 2024.
[153] Yong, Tay and Khong (n 14).

Establishing clear legal parameters for smart contracts would enhance clarity and predictability for participants in digital transactions. This step is essential for maintaining both Singapore and Malaysia's position as a technologically inclusive and progressive jurisdiction, ensuring that its legal system remains equipped to handle the complexities of digital innovation. By drawing on the experiences of the UK and perhaps some common in integrating smart contracts into their legal systems, Singapore and Malaysia can develop robust guidelines that support technological advancement while safeguarding legal certainty and consumer protection.

8 Conclusion

Our comprehensive examination of smart contracts and blockchain technology within the legal frameworks of Malaysia and Singapore in the context of Malaysian and Singaporean law demonstrates a complex interaction between long-standing legal customs and cutting-edge technological advancements. Both jurisdictions, grounded in the common law principles inherited from the United Kingdom, exhibit a remarkable level of adaptation and flexibility. This common law foundation equips them to manage the complex challenges introduced by blockchain and smart contracts, benefiting from the adaptability that judicial precedent allows. Nonetheless, the incorporation of these technologies poses distinct obstacles that need for a methodical approach to judicial and regulatory adjustment that honours both technological progress and legal tradition.

Central to these challenges is the imperative to balance technological neutrality with operational specificity. While existing laws permit the inclusion of digital contracts, the unique attributes of blockchain technology and the self-executing nature of smart contracts underscore the need for legislative and judicial advancements to ensure clarity, predictability, and consistency. Initiatives inspired by the UK's approach, including the UKJT Legal Statement on Cryptoassets and Smart Contracts[154], and the Law Commission Report on Smart Legal Contract[155], serve as valuable models. Given the UK's historical influence on Malaysian and Singaporean law, UK frameworks provide a reliable basis for adaptation. Instead of overhauling traditional legal theories, Malaysia and Singapore could benefit from implementing targeted legal clarifications that formally identify the unique characteristics of smart contracts inside their common law systems. These revisions could specifically clarify coded agreements' contractual nature, ensuring that essential principles like as offer, acceptance, and consideration are clearly applicable to smart contracts. This approach would not only bridge the gap between established legal principles and modern technology, but it would also provide courts and legal practitioners with clear, practical direction when interpreting digital contracts.

[154] UK Jurisdiction Taskforce, Legal statement on cryptoassets and smart contracts (n 133).
[155] Law Commission, Smart legal contracts, advice to government (n 132).

Case studies demonstrate the judiciary's existing capacity to adapt traditional doctrines to novel digital contexts. However, the swift nature of digital transformation calls for more structured guidance. Malaysia and Singapore could consider issuing official statements or guidelines that establish a clear legal basis for smart contracts without the need for additional legislation. This approach would clarify foundational contract principles within the scope of smart contracts, reinforcing the position of coded agreements within the legal system while providing flexibility for judicial interpretation. Such guidelines would support consistent application and predictability, which are crucial in ensuring that businesses and individuals engage confidently in digital transactions.

Guidelines should provide clear definitions of key Sharia-compliant terms in Islamic finance smart contracts, such as "interest-free," "profit-sharing," and "ethical investment". These definitions will help courts bridge the gap between common law principles and Islamic finance practices by appropriately interpreting digital financial agreements. Regulators should encourage the development of common code libraries for smart contracts in order to create a safe and legal environment for digital transactions. These libraries, which have been validated to meet legal and regulatory criteria, have the potential to speed up contract execution and ease interpretation, particularly for complex contracts or high-stakes transactions. Certification processes that check code for safety, data handling, and consumer protection would make contracts function better and be easier to enforce legally. Also, adding ways to resolve disputes directly within smart contracts could help prevent unexpected issues, ensuring both safety and fairness, especially in high-value transactions.

Further, these regulatory efforts should place consumer protection at the forefront. Adopting user-friendly interfaces and requiring "cooling-off" periods would safeguard users who might not completely comprehend the terms contained within the contracts, as smart contracts allow for a wider spectrum of participants, including non-technical individuals. Complying with national and international data protection laws, including the PDPA and GDPR, would add a vital layer of security to contracts that deal with sensitive information. Moreover, aligning smart contract frameworks with anti-money laundering and financial compliance standards, especially for transactions involving substantial assets, is essential for upholding the financial system's integrity and meeting global compliance standards.

The wide use of smart contracts, from tenancy agreements to financial services and public sector management, illustrates both their transformative potential and the intricate legal considerations required to fully leverage this technology. These applications underscore areas where additional, specific guidance is necessary—particularly for cross-border transactions, where jurisdictional conflicts and differing regulatory standards may complicate enforcement and adjudication. Provisions for the cross-border recognition and enforcement of Sharia-compliant contracts could also be included in guidelines to facilitate international transactions in Islamic finance. This would make it clearer how these agreements relate to other jurisdictions and Islamic finance

regimes. Clear statutory definitions around cross-border enforceability are essential to create a seamless framework that can uphold the rights and obligations of all parties involved, even across jurisdictions. Providing clarity on issues like cross-border enforceability of judgments, mechanisms for enforcing awards related to smart contracts, and criteria for recognising international smart contract frameworks would significantly bolster legal certainty and support cross-jurisdictional transactions.

Malaysia and Singapore can create a framework that is future-ready while respecting their own legal, cultural, and economic contexts by utilising the UK as a model and taking inspiration from its adaptable regulatory approaches. This approach would set a precedent for integrating traditional legal frameworks with modern technologies. Establishing a regulatory framework that is clear yet adaptable—ensuring guidelines are precise but not overly rigid—will allow Malaysia and Singapore to strike an effective balance between safeguarding their common law principles and embracing innovation. The framework would also enable the smooth integration of Islamic finance principles with these developments, maintaining Malaysia and Singapore at the forefront of digital finance that complies with Sharia law while fostering global competitiveness. As the legal landscape changes with technology, this dual approach maintains justice, fairness, and openness at its core while simultaneously fostering development and efficiency in digital commerce. Both countries are in a strong position to take the lead in digital legal frameworks in Southeast Asia and beyond because they place a high priority on consumer protection, flexibility, and clear rules.

Aviv Gaon and Yuval Reinfeld *

SPECIAL SECTION

ADVANCING FAIR DIGITAL COMPETITION:
A CLOSER LOOK AT THE DMA FRAMEWORK

Abstract

The emergence of digital platform firms has escalated international antitrust inquiries, especially targeting the "Big Five"—Meta, Apple, Microsoft, Amazon, and Alphabet. These enterprises have significantly impacted the economy and society, exceeding conventional sectors in terms of market value, making antitrust legislation, particularly within the European Union, inadequate. *The Digital Markets Act* (DMA) was created to serve as a regulatory framework to curb the misuse of power by these dominant players and safeguard consumer interests. The DMA monitors digital gatekeepers and promotes equitable competition while safeguarding the rights of EU citizens and encouraging openness and equitable competition in the digital space. The DMA enhances current competition regulations by clarifying "gatekeepers" and establishing guidelines for their conduct within the digital marketplace. Gatekeepers adhere to DMA regulations, which ban unfair practices such as data misuse and favouritism toward their services. The European Commission can identify gatekeepers and monitor compliance, providing a schedule for businesses to meet DMA standards. Additionally, the DMA imposes fines and penalties for violations, highlighting the significance of compliance. This paper examines the DMA framework, the requirements for identifying gatekeepers, the regulatory responsibilities assigned to them, and the enforcement strategies established. The DMA emphasises the EU's dedication to combating anti-competitive behaviour and preserving an equitable digital marketplace, positioning the DMA as essential for protecting consumer rights and promoting fair competition worldwide. While the DMA' 's framework aims to tackle anti-competitive behaviour and promote transparency in the digital marketplace, it is essential to question whether the DMA can strike the right balance between competition and innovation. Could its strict obligations on gatekeepers unintentionally stifle innovation or discourage new market entrants? Moreover, as the digital economy continues to evolve rapidly, is the DMA' 's broad scope truly adaptable, or might it impose unnecessary burdens on emerging technologies? These concerns underscore the importance of a nuanced evaluation of the DMA' 's impact on competition without hindering progress in the digital space.

JEL CLASSIFICATION: K21

* Aviv Gaon is a senior lecturer at the Harry Radzyner Law School, Reichman University; Yuval Reinfeld is a research fellow, Ben Gurion University; Adjustment Professor, Reichman University. The authors thank Deborah M. Broyde for her excellent research and express their gratitude to the anonymous reviewers for their insightful feedback and suggestions.

 DOI 1.13135/2785-7867/11335

SUMMARY

1 Facing Digital Competition: Tackling Risks Head-On

The profound transformation in the global economic landscape, propelled by the ascent of digital platform corporations, has catapulted antitrust investigations to the forefront of legal discourse on a global scale. Notably, the "Big Five" tech giants- Meta, Apple, Microsoft, Amazon and Alphabet (MAMMA) - have exceeded the market capitalisation of traditional industry behemoths.[1] This unparalleled financial prowess, exemplified by Apple's historic achievement of reaching a $1 trillion market capitalisation in August 2018, highlights MAMMA's economic significance and position as formidable actors with influence permeating multiple dimensions of societal functioning.[2]

'The shift in market dynamics necessitates a meticulous examination. Comparative analyses highlight the ascendance of Big Tech over formerly dominant entities, emphasizing a paradigmatic change in economic power structures and the consequential legal implications. In recent years, Big Tech have become a focal point for competition scrutiny.[3]

EU competition law is essential for protecting the economy from market power issues. Its main principles aim to prevent dominant market entities from abusing their power and solidifying their positions through agreements that harm consumers. However, traditional competition law faces challenges, particularly in the EU. The European Commission, responsible for enforcement, struggles to adequately respond to threats to free competition posed by Big Tech.[4] The limitations of competition law in addressing the nuanced dynamics of the digital economy prompt a paradigm shift toward regulation. This shift is the changing role of economics within the competition framework, which is

[1] The term "Big Tech" progressively associated with the quintet of major technology corporations, encapsulates the collective influence wielded by those entities.

[2] JP Whittaker, *Tech Giants, Artificial Intelligence and the Future of Journalism* (1st edn, Routledge 2019).

[3] M Moore and D Tambini, *Regulating Big Tech: Policy Responses to Digital Dominance* (Oxford University Press 2022). Recent developments in antitrust cases against Big Tech firms underscore the heightened scrutiny these companies are facing. The ongoing *United States vs. Google LLC (2023)* case, which has seen significant evolution recently, involves allegations that Google maintained its monopoly in the search engine market through anti-competitive deals with companies like Apple. This case, which draws comparisons to the historic Microsoft antitrust trial, saw a crucial update when the court reaffirmed Google's monopolistic behaviour under the *Sherman Act of 1890*. Additionally, in July 2024, the European Commission issued preliminary findings against Meta's "pay or consent" model under the DMA, arguing that it fails to provide users with a less intrusive, yet equivalent, service option. Furthermore, the U.S. Department of Justice has recently filed an antitrust lawsuit against Apple, accusing the company of leveraging its locked-down iPhone ecosystem to suppress competition, including blocking "super" apps, mobile cloud streaming services, and cross-platform messaging apps. This marks the third time the DOJ has sued Apple for antitrust violations in the past 14 years. See Office of Public Affairs – (United States of America and Others v Apple Inc, Complaint, No. 2:24-cv-04055 (D NJ, 11 June 2024).

[4] EM Fox and D Gerard, *EU Competition Law: Cases, Texts and Context* (2nd edn, Edward Elgar Publishing 2023).

increasingly shaping the understanding and application of competition law.[5] Examining the intricacies of competition law's limitations is crucial considering these challenges. A detailed exploration of specific cases and examples reveals the shortcomings of existing regulatory approaches. These failures underscore the urgency of reassessing and adapting legal mechanisms to effectively address the complex challenges at the intersection of technology and market dominance.

Moreover, the EU's commitment to addressing damages to digital competition complements the normative idea of the Unions' policy, *Technical Normative Power* (TNP), which places citizen protection at the core.[6] Effectively, challenging technology giants requires supervision by the EU's regulatory authority, establishing a normative framework within the tech giants' environment and thereby diffusing its standards globally. This framework extends to organisations and companies dependent on their interfaces, benefiting consumers with more transparent information, competitive prices, and expanded options. From the perspective of EU institutions, regulating these aspects also ensures the protection of other fundamental rights, such as privacy and data protection, offering a comprehensive approach to address the complexities arising from the intersection of technology and market dominance.[7]

Our paper explores *the extent to which the current Digital Markets Act (DMA) framework is equipped to address the growing complexity and rapid evolution of digital markets*. While the regulation attempts to capture gatekeepers through quantitative thresholds, there is concern that powerful players may evade legal scrutiny by exploiting its weakness. We argue that the DMA lacks precise definitions of key terms such as 'more favourably' and 'rivals,' creating significant ambiguity in its implementation. This absence of clarity risks leading to inconsistent enforcement, potentially undermining both competition and innovation in digital markets.[8] Furthermore, we wish to address an even bigger question: *Does the interventionist approach of the DMA risk creating an overly rigid regulatory environment that disproportionately burdens smaller businesses and new market entrants?* In light of these concerns, one must consider whether the DMA might end up hindering the competition it seeks to protect.

[5] H Schmidt, *Competition Law, Innovation and Antitrust: An Analysis of Tying and Technological Integration* (2nd edn, Edward Elgar 2023).

[6] The integration of normative principles and regulatory power, often encapsulated as TNP, is palpably evident in the DMA, manifesting through key provisions that underscore the normative underpinnings guiding the regulatory framework. A notable instance is discerned in Recital 80, which establishes the normative imperative that gatekeepers must adhere to the obligations delineated in the regulation concerning each core platform service specified in the relevant designation decision. This foundational principle emphasises compliance within the conglomerate position of gatekeepers, introducing a normative thread that recognises the interconnectedness of their services and the need for a comprehensive approach. A further demonstration of TNP within the DMA is evident in Recital 105, which highlights the Commission's commitment to evaluating the DMA's impact on contestability and fairness in the online platform economy reflects a normative dedication to maintaining a high level of protection and respect for common rights and values.

[7] See the *Digital Markets Act* (DMA) and the "sister" regulation of the *Digital Services Act* (DSA).

[8] C Carugati, *How to Implement the Self-Preferencing Ban in the European Union's Digital Markets Act'* (Bruegel 2022) Policy Contribution 22/2022 <https://www.bruegel.org> accessed 25 October 2024.

The paper's methodology is based on a comprehensive legal and economic analysis of the DMA framework, focusing on the role and responsibilities of digital gatekeepers. We employ a doctrinal research approach to examine the DMA, the Treaty on the Functioning of the European Union (TFEU), and prominent cases. We further illustrate the practical enforcement of the DMA, such as actions taken against major technology firms. This comprehensive approach demonstrates the DMA's influence on major tech companies like Google and Meta. The analysis also considers comparative approaches, drawing on competition law's limitations and examining the intersection of market power and technology in the digital economy. The methodology extends beyond legal doctrine by assessing the economic implications of the DMA, particularly its impact on competition, innovation, and consumer protection in digital markets.

We begin by introducing the governing gatekeepers, providing a foundational understanding of their role and the need for oversight in digital markets. We then delve into the primary goals of the DMA, examining its regulatory framework and objectives. Finally, we offer an in-depth analysis of enforcement measures supported by relevant case studies to illustrate the practical application.

2 The DMA's Objective and Foundations: Regulating Digital Gatekeepers

The DMA, effective since May 2, 2023, marks an important milestone in the European Union's regulatory framework, targeting digital entities referred to as "gatekeepers."[9] These gatekeepers provide core platform services, including online intermediation, search engines, and social networks. The DMA was introduced to prevent gatekeepers from exploiting their power to the detriment of competition, consumers, and innovation.

The DMA complements existing EU competition law, particularly the prohibitions outlined in Articles 101 and 102 of the TFEU.[10] While Articles 101 and 102 aim to prevent anti-competitive agreements and the abuse of dominant market power, the DMA's emphasis on "fairness" and "contestability" distinguishes it from merely focusing on undistorted competition within the internal market.[11] The regulation mandates that gatekeepers adhere to obligations designed to curb practices that harm competition and consumer choice. These obligations include prohibiting combining personal data from different services without user consent, restricting unfair practices in advertising, and preventing gatekeepers from favouring their products over competitors. By enforcing these rules, the DMA aims to create a more transparent and competitive digital space, benefiting both businesses and consumers.

[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) [2022] OJ L265/1, Article 2(1).
[10] Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47.
[11] J Van den Boom, 'What Does the Digital Markets Act Harmonize? – Exploring Interactions between the DMA and National Competition Laws' (2022) 19 European Competition Journal 57.

Gatekeepers under the DMA are identified based on strict qualitative and quantitative criteria, including their annual turnover within the European Economic Area (EEA) and the company's presence as a core service in at least three member states. Gatekeepers are companies that serve as essential gateways for businesses to reach consumers, often wielding significant economic power. They are assessed based on their market presence and user base, with thresholds of at least 45 million active end users and 10,000 active business users within the EU. Gatekeepers must also demonstrate that they hold an entrenched position in the market for three consecutive years, underscoring their long-term dominance. Companies under this category face regulatory scrutiny designed to prevent them from exploiting their gatekeeper role to stifle competition or innovation.[12]

The obligations imposed on gatekeepers focus on preventing unfair practices that hinder market contestability. For instance, gatekeepers are not permitted to incorporate personal data obtained from their subsidiaries, limit business users' dealings with end users, use the personal data of customers who use third-party services operating over their platforms, or bundle or prefer proprietary goods and services sold by the gatekeeper in a manner that stifles third-party competition.[13]

In terms of scope, the DMA targets a wide range of digital services, including online search engines, social media networks, video-sharing platforms, messaging services, cloud computing, and online advertising services. These platforms are vital to the EU's internal market, and their regulation is crucial for safeguarding competition and innovation. The regulation's extraterritorial reach ensures that companies providing these services, even if based outside the EU, must comply with its rules if they serve EU users. This reflects the EU's commitment to extending its regulatory influence globally, akin to the impact of the General Data Protection Regulation (GDPR).

The regulatory measures under the DMA are not limited to preventing anti-competitive behaviour but also seek to safeguard broader consumer rights, such as privacy and data protection. By establishing clear rules for digital gatekeepers, the DMA ensures that consumers benefit from greater transparency and choice while business users are protected from unfair practices. This aligns with the EU's broader objective of fostering a digital environment that upholds fundamental values like fairness, innovation, and the protection of individual rights.

A key milestone in the enforcement of the DMA was reached on July 3, 2023, when major tech companies, including Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Samsung, were required to notify the European Commission of their alignment with the DMA's criteria for gatekeepers. The European Commission, following a 45-working-day

[12] Regulation (EU) 2022/1925 of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) [2022] OJ L265/1, Article 3.
[13] Council Regulation (EU) 2022/1925 Of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1. <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en> accessed 24 August 2024.

evaluation period, officially designated six gatekeepers—Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft—on September 6, 2023.[14] These companies, providing 22 core platform services, were given six months to comply with the DMA's requirements, signalling the beginning of a new era of compliance and regulation in the digital economy.[15]

By extending its regulatory purview beyond the EU's borders, the DMA solidifies the EU's role as a global standard-setter in digital governance. This extraterritoriality mirrors the precedent set by the GDPR, where the EU successfully exported its data protection norms to companies worldwide. The DMA's global reach reflects the EU's commitment to fostering a competitive digital market that is both fair and open, regardless of the geographical location of service providers.

The DMA's objective is clear: to regulate digital gatekeepers and prevent them from exploiting their dominant market positions to the detriment of competition and consumers. While the DMA outlines strict obligations for these gatekeepers, such as prohibiting the combination of personal data from different services without consent and ensuring interoperability, the regulation raises essential questions.

A critical concern is whether these regulatory mechanisms can prevent gatekeepers from manipulating their dominant positions. Although the DMA forbids gatekeepers from restricting business users' access to end users, whether these rules will be sufficient to prevent similar manipulations in practice remains to be seen.

Moreover, the DMA' 's centralisation of enforcement powers at the EU level may risk privileging gatekeepers by limiting the role of national authorities. With national laws aimed at ensuring contestability and fairness being potentially inapplicable to gatekeepers, gatekeepers could exploit this centralisation to avoid stricter national regulations. This raise concerns that' the DMA might unintentionally facilitate gatekeepers' dominance instead of enhancing fair competition, creating enforcement delays and complicating timely regulatory action.[16]

3 Regulation Structure Oversight

Compared to other EU digital legislations, the DMA is a succinct regulation comprising fifty-four articles distributed across five chapters. *Chapter I* addresses fundamental aspects of the DMA's applicability, while Chapter II is dedicated to the designation of gatekeepers, and Chapter III outlines the obligations imposed on gatekeepers. The scope

[14] 'Commission Designates Six Gatekeepers under the Digital Markets Act' (*Digital Markets Act (DMA)*, 6 September 2023) <https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en> accessed 24 August 2024.

[15] 'Potential Gatekeepers Notified the Commission and Provided Relevant Information' (*Digital Markets Act (DMA)*, 4 July 2023) <https://digital-markets-act.ec.europa.eu/potential-gatekeepers-notified-commission-and-provided-relevant-information-2023-07-04_en> accessed 24 August 2024.

[16] J Hoffmann, L Herrmann, and Lukas Kestler, 'Gatekeeper's Potential Privilege—the Need to Limit DMA Centralization' (2024) 12(1) Journal of Antitrust Enforcement 126, 147.

of the regulation extends to core platform services provided or offered by gatekeepers to business users or end users within the Union, regardless of the gatekeepers' location or the applicable law.[17] The regulation explicitly states that it does not prejudice the application of Articles 101 and 102 of the TFEU and allows for applying national competition rules in certain contexts.

Under the DMA, an undertaking qualifies as a gatekeeper if it satisfies specific criteria, with presumptions based on financial and operational indicators. These criteria include demonstrating a significant impact on the internal market,[18] providing a core platform service crucial for business users to reach end users,[19] and holding an entrenched or durable position or having the foreseeable potential for such a position soon. This highlights the DMA's unorthodox approach, which is designated for Big Tech.

Gatekeepers meeting the specific criteria must notify the Commission within two months and provide relevant information. The Commission holds the authority to designate gatekeepers within 45 working days, considering the information provided by the undertaking.[20] Additionally, the Commission may designate an undertaking as a gatekeeper even if it does not meet the quantitative thresholds, considering factors such as size, operations, network effects, and other structural characteristics. The Commission continuously publishes and updates a list of gatekeepers and their relevant core platform services, promoting transparency in compliance. These reviews do not suspend gatekeepers' obligations, ensuring continuous evaluation and adherence to the DMA's provisions.[21]

Articles 5 to 7 underscore the obligations to ensure fair competition, non-discrimination, and user choice in the digital sector, emphasizing a unique TNP impact on tech companies. For example, Article 5 delineates specific obligations for gatekeepers concerning their core platform services. These obligations include restrictions on processing personal data for online advertising without user consent, limitations on combining personal data from different services and ensuring user consent for signing in to other services. The gatekeeper is also prohibited from preventing business users from offering diverse products or services through third-party online intermediation services,[22]

[17] Excluded from the DMA's realm are the enchanting number-independent interpersonal communication services, guided by the regulatory prowess of the European Electronic Communications Code (EECC) under Directive (EU) 2018/1972. This purposeful exclusion orchestrates regulatory efficiency, avoiding duplicative oversight and allowing these services to gracefully dance under the EECC's watchful guidance, see Article 1(3) of the DMA.

[18] According to Article 3(2)(a), an undertaking is presumed to be a gatekeeper if it has an annual Union turnover equal to or exceeding EUR 7.5 billion in each of the last three financial years, or an average market capitalization or equivalent fair market value of at least EUR 75 billion in the last financial year, and concurrently provides the same core platform service in at least three Member States.

[19] For core platform services, Article 3(2)(b) presumes an undertaking as a gatekeeper if it provides service with a minimum of 45 million monthly active end users in the last financial year, established or located in the Union, and has at least 10,000 yearly active business users in the Union. The identification and calculation of these figures should adhere to the methodology and indicators outlined in the Annex.

[20] Digital Markets Act, art 3(4).

[21] Digital Markets Act, art 4.

[22] Digital Markets Act, art 5(3).

and business users must be allowed to communicate freely with end users acquired through the gatekeeper's platform.[23] Additionally, Article 5 addresses issues related to end-user access to content and services,[24] non-restriction of reporting non-compliance with the law to public authorities,[25] and non-mandatory use of identification, web browsers, and payment services.[26] The gatekeeper must also provide advertisers and publishers with information on advertising metrics.[27]

Article 6 outlines obligations that may be further specified under Article 8. This includes the prohibition of gatekeepers using non-publicly available data from business users for competition and requirements related to the uninstallation of software applications and changing default settings.[28] The gatekeeper is also mandated not to treat its services preferentially in ranking and indexing (e.g., Google Search Ranking Systems)[29] and not to restrict end-users' ability to switch between different applications and services (e.g., App Store).[30] Article 7 focuses on the interoperability of number-independent interpersonal communications services. Gatekeepers providing such services must make basic functionalities interoperable upon request.[31]

Article 8 introduces provisions for gatekeepers to comply with the obligations outlined in Articles 5, 6, and 7. The gatekeeper is required to ensure and demonstrate compliance through effective measures aligned with the objectives of the DMA and relevant laws, including data protection, cyber security, consumer protection, and product safety. The Commission is empowered to open proceedings, adopt implementing acts, and specify measures for compliance. Gatekeepers can request the Commission's engagement to assess the effectiveness of their compliance measures, providing a reasoned submission for consideration. The Commission's powers include communicating preliminary findings, specifying measures, and reopening proceedings based on material changes, incomplete information, or ineffective measures.

In addition, within six months of designation pursuant to Article 3, the gatekeeper must submit a detailed and transparent report to the Commission describing the measures taken to comply with the obligations in Articles 5, 6, and 7. This report should be updated at a minimum annually. Gatekeepers must publish and provide the Commission with a non-confidential report summary within the same timeframe. The Commission, in turn, will link to the non-confidential summary on its website. This reporting mechanism ensures transparency and accountability in the gatekeeper's adherence to regulatory obligations.[32]

[23] Digital Markets Act, art 5(4).
[24] Digital Markets Act, art 5(5).
[25] Digital Markets Act, art 5(6).
[26] Digital Markets Act, art 5(7) and (8).
[27] Digital Markets Act, art 5(9).
[28] Digital Markets Act, art 6(3) and (4).
[29] Digital Markets Act, art 6(5).
[30] Digital Markets Act, art 6(6).
[31] Digital Markets Act, art 7(1).
[32] Digital Markets Act, art 11.

Like other digital regulations, the DMA strategically employs a meticulously crafted enforcement system to establish comprehensive standards. This system is purposefully designed to substantiate the faithful implementation of the law's objectives, thereby upholding core values and principles integral to the functioning of the common market. The intricacies of this enforcement mechanism are particularly concentrated and elucidated within *Chapter V* of the Regulation, affirming its central role in fortifying the regulatory framework and promoting the desired EU norms. Consequently, the Commission is vested with the authority to requisition essential information from undertakings crucial for fulfilling its duties under the regulation.[33] This also includes imposing fines under Articles 30 and 31.[34] The foundational competencies of the CJEU, as outlined in Article 45, come to the forefront by invoking its oversight authority in conjunction with Article 261 TFEU.[35] Concurrently, Article 47 empowers the Commission to issue guidelines, adding another layer to the regulatory landscape. These guidelines, designed to address various facets of the regulation, play a pivotal role in enhancing the effective implementation and enforcement of the DMA. Serving as interpretative tools, they contribute to a nuanced understanding and application of the regulatory framework.[36] Furthermore, Article 48 introduces a dimension of standardisation, allowing the Commission, under circumstances deemed appropriate and necessary to delegate standards development to European standardisation bodies.[37]

This comprehensive initiative reflects the EU's commitment to upholding fundamental values in the evolving digital landscape. The DMA safeguards the rights of EU citizens, addresses gatekeepers and competition concerns, and ensures a fair, transparent digital ecosystem. The efficacy of the DMA as a foundational element in the EU's digital regulatory framework and its global influence can be further assessed by examining the best practices in Commission enforcement and the rulings of the CJEU while positioning the EU as a global leader in digital regulation. The practical application of the DMA by the

[33] Digital Markets Act, art 21. Article 22 grants the Commission the power to conduct interviews and gather statements from natural or legal persons who consent to be interviewed. The Commission also possesses the authority to conduct inspections, outlining the scope of powers, including entering premises, examining records, and requesting explanations. Article 24 responds to urgent scenarios, granting the Commission authority to enact interim measures to avert serious harm to businesses or end users of gatekeepers.

[34] In the event of a non-compliance decision, the Commission is authorised to impose fines on gatekeepers, capped at 10% of their total worldwide turnover in the preceding financial year. The Commission also grants a power to impose penalties, not exceeding 1% of the total worldwide turnover, on undertakings and associations of undertakings for various infractions. The fines take into consideration the gravity, duration, recurrence, and any delays caused to the proceedings. This penalty is applicable when gatekeepers intentionally or negligently violate obligations outlined in Articles 5, 6, and 7, as well as measures specified in decisions pursuant to Article 8(2), remedies in Article 18(1), interim measures in Article 24, and commitments legally binding under Article 25. Notably, the escalation of fines to a maximum of 20% is sanctioned when a gatekeeper repeats a similar infringement within eight years.

[35] Digital Markets Act, art 45. Under this provision, the CJEU is endowed with expansive jurisdiction, granting it the power to meticulously examine Commission decisions that impose fines or periodic penalty payments. Within this overarching scope, the Court holds the authority to either annul, reduce, or augment the fines or periodic penalty payments levied by the Commission.

[36] Digital Markets Act, art 47.

[37] Digital Markets Act, art 48.

Commission, including its enforcement decisions and the subsequent impact on digital market players, will provide valuable insights into the effectiveness of the regulatory measures. By scrutinizing these enforcement actions and judicial interpretations, it becomes possible to gauge the DMA's success in achieving its intended goals, ensuring fair competition, and maintaining the fundamental values of EU citizens.

The centralised enforcement model that the DMA adopts raises concerns about the European Commission' 's capacity to handle the scale of compliance monitoring and enforcement required to regulate such vast digital ecosystems effectively. Although the DMA seeks to position the Commission as a central regulator, we question whether it is feasible for the Commission to simultaneously manage the regulatory responsibilities of multiple gatekeepers while also dealing with broader antitrust enforcement issues.

Enforcement challenges are compounded by the risk that gatekeepers, backed by vast legal and financial resources, will exploit ambiguities in the DMA to delay compliance or dilute the impact of enforcement actions. The DMA stipulates hefty fines for non-compliance, but does the Commission possess the investigative and enforcement capacity to implement such penalties consistently and effectively across different member states? The centralised enforcement model may lead to inefficiencies, as national competition authorities are sidelined in the process, potentially causing gaps in enforcement, especially in more localised market contexts.

Furthermore, the regulation' 's success depends on the Commission' 's ability to update its enforcement strategy in response to the rapid evolution of technology and business models. A potential limitation of the DMA is its prescriptive nature—by setting rigid rules for gatekeepers, it may struggle to adapt to new technologies or platforms that fall outside its initial scope. Thus, critics might argue that the DMA lacks the flexibility necessary to remain relevant in an industry of constant innovation.

4 Commission Oversight: A Pragmatic Analysis of Enforcement Measures

The EU Competition Policy ensures a fair marketplace by enforcing rules that promote innovation and protect consumers. The European Commission monitors competition, addressing abuses of dominant positions and anti-competitive agreements, such as cartels. It also scrutinises mergers and state aid to ensure they benefit consumers without distorting competition. The policy covers key sectors like energy, finance, and technology. To enhance transparency, the Commission provides a platform for the public to access updates on competition cases, particularly under the DMA, reflecting its commitment to openness and accessibility for all stakeholders.

The European Commission, under the DMA, has centralised more essential competencies to ensure the proper implementation. European regulators actively pursue investigations into major tech companies, raising concerns over antitrust issues and market dominance. Microsoft's decision to unbundle Teams from Office to avoid potential

antitrust fines is part of the EU's broader scrutiny.[38] Microsoft, having faced 2.2 billion euros in EU antitrust fines in the past decade, was at risk of further penalties, with a 2020 complaint by Slack triggering the investigation. This scrutiny focuses on Microsoft's market position in productivity software, specifically in the European communication and collaboration products market.[39]

On May 2, 2022, the European Commission issued a Statement of Objections to Apple, asserting that Apple abused its dominant position in the mobile wallet market on iOS devices. The Commission argued that Apple's limitation of access to NFC technology restricts competition and innovation. Specifically, Apple's decision to favour its own Apple Pay solutions by restricting third-party access to NFC input raises concerns of potential anti-competitive behaviour. The Commission contended that Apple's dominant position hampers competition, violating Article 102 of the TFEU.[40]

On June 14, 2023, the European Commission issued a Statement of Objections to Google, alleging that the company violated EU antitrust rules in the advertising industry. The Commission argues that Google has abused its dominance in European markets for publisher ad servers and programmatic ad-buying tools by favouring its ad exchange, AdX, since 2014. This conduct allegedly distorted competition, harming advertisers and publishers, and may require Google to divest part of its services to address these concerns. If confirmed, these actions would breach Article 102 of the TFEU.[41] This recent antitrust action against Google builds on previous regulatory interventions. In 2017, the Commission fined Google €2.42 billion for abusing its dominance as a search engine by giving illegal advantages to its comparison-shopping service. Google strategically promoted its service and demoted rivals in search results, stifling competition. The fine considered the duration and gravity of the infringement. It was based on the value of Google's revenue from its comparison-shopping service in the relevant European Economic Area countries. The decision required Google to cease its illegal conduct within 90 days or face penalty payments. This case underscores the Commission's commitment to addressing anti-competitive practices by tech giants, setting a precedent for subsequent investigations

[38] P Sawers, 'Microsoft Unbundles Teams from Microsoft Office in Europe to Appease Regulators' (*TechCrunch*, 1 September 2023) <https://techcrunch.com/2023/08/31/microsoft-office-teams-europe-unbundle> accessed 24 August 2024.

[39] S Kar-Gupta and C Chee, 'Microsoft in EU Antitrust Crosshairs over Teams, Office Tie-Up' (*Reuters*, 27 July 2023) <https://www.reuters.com/technology/eu-antitrust-regulators-investigate-microsoft-over-teams-office-tying-2023-07-27> accessed 24 August 2024.

[40] 'Antitrust: Commission Sends Statement of Objections to Apple over Practices Regarding Apple Pay' (*European Commission*, 2 May 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP222764> accessed 24 August 2024. The Statement of Objections focuses on NFC access for in-store payments, excluding online restrictions or alleged refusals of access to Apple Pay for specific rival products.

[41] 'Antitrust: Commission Sends Statement of Objections to Google over Abusive Practices in Online Advertising Technology' (*European Commission*, 14 June 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip233207> accessed 24 August 2024.

into Google's conduct, including those related to the Android operating system and Ad Sense.[42]

In July 2024, the Commission sent preliminary findings to Meta regarding its "Pay or Consent" advertising model, highlighting potential DMA violations. This model, introduced in November 2023, forces EU Facebook and Instagram users to either pay for an ad-free experience or continue using the platforms with personalised ads based on their consent to data processing. The Commission's preliminary view suggests that Meta's approach may be non-compliant with Article 5(2) of the DMA, which requires gatekeepers to provide users with a clear alternative to consent. This service is less reliant on personal data but is otherwise equivalent in functionality. Meta's binary choice, however, fails to offer such an alternative, essentially coercing users into accepting data-intensive services if they wish to avoid payment.

In its preliminary findings, the Commission pointed out that Meta's current model does not allow users to freely exercise their right to opt out of data combinations while still accessing a comparable service, infringing upon their autonomy and privacy rights. This development illustrates how the DMA, alongside other regulatory frameworks (GDPR and DSA), is shaping the operational strategies of digital giants.

These examples highlight how the Commission employs its regulatory tools to monitor gatekeepers and other tech players within the EU market to ensure a fair, transparent and competitive environment. It also proves the Commission's resilience and motivation in engaging big-tech corporations.

Undoubtedly, the CJEU plays a crucial role in shaping the EU's normative regulatory power on the global stage. However, as the EU's enforcement model becomes more centralised, it may raise concerns about the broader implications of such a concentrated regulatory approach.

As we have argued in earlier sections of this paper, this model could potentially create enforcement delays, allowing gatekeepers to exploit legal ambiguities and placing smaller, less-resourced national authorities at a disadvantage.

Furthermore, while the CJEU has demonstrated its ability to impose significant penalties, the long-term impact of such fines on market structures remains debatable. Are they truly a deterrent, or do they simply become a "cost of doing business" for tech giants? These considerations call for a critical reassessment of whether the current centralised model, although effective in creating legal certainty and uniformity, is sufficiently adaptable to digital markets' dynamic and rapidly evolving nature. Without more flexibility and local engagement, there is a risk that the regulatory framework may struggle to keep pace with technological advancements and evolving market dynamics.

[42] 'Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service' (*European Commission*, 27 June 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784> accessed 24 August 2024.

5 Deciphering Competition: CJEU Rulings on EU Competition Cases

The CJEU has also been instrumental in reinforcing the EU's normative power in competition law concerning digital markets. In *Google and Alphabet v. Commission*, it was determined that Google took advantage of its market dominance by illegally favouring its comparison-shopping service to its competitors.[43] Although the decision set a significant legal precedent, it raises critical questions about its broader impact. Can even a substantial fine truly challenge the entrenched dominance of companies like Google, or is it merely a temporary setback, leaving their underlying market power intact? We argue that fines alone fail to address the structural issues of monopolistic power in digital markets, where companies often treat penalties as a cost of doing business rather than a genuine deterrent.

This case stems from the European Commission's June 27, 2017 decision, which found that Google abused its dominant position in the general online search market across 13 EEA countries by favouring its shopping comparison service over competitors.[44] For this violation, Google was fined an astronomical €2.4 billion. Google and Alphabet filed a lawsuit against the Commission's decision with the General Court (GC).

The GC rejected Google's claims, highlighting the anti-competitive nature of its practices. It ruled that Google abused its monopoly by favouring its shopping comparison service, distorting competition. The decision was based on three factors: the significant traffic generated by Google's search engine, users' focus on top search results, and Google's dominant, irreplaceable market position. While valid, these points emphasise regulators' difficulty in dismantling tech giants' entrenched advantages. Penalizing behaviour alone may not change the market dynamics that sustain their dominance.

The GC further noted that Google's self-preferencing behaviour would not occur without its dominant market power. It also emphasised the EU's requirement for equal treatment by Internet access providers and Google's deliberate actions to undermine competition. As a result, the Digital Markets Act (DMA) now incorporates principles to ensure a more competitive and secure market for European consumers.[45]

On September 14, 2022, the GC published another seminal ruling against Google in the Google Android case.[46] The GC confirmed the Commission's decision to restrict Android device manufacturers and mobile network operators to prevent the dominance of Google's search and related applications. The Commission had taken Google to task for hindering the development of rival mobile operating systems, applications, and services in the EEA. On July 18, 2018, the Commission fined Google for abusing its dominant position by

[43] Case T-612/17 *Google and Alphabet v Commission (Google Alphabet)* [2005] ECRII.
[44] Search results for products generated by the Google search engine were presented as more prominent and eye-catching when derived from the company's proprietary shopping comparison application relative to the results generated by competing services.
[45] Case C-48/22 P *Google and Alphabet v Commission (Google Shopping)*, pending before the Court of Justice of the European Union.
[46] Case T-604/18 *Google and Alphabet v Commission* (*Google Android*) [2022] ECLI.

imposing anti-competitive contractual restrictions on mobile device manufacturers and network operators. The Commission found that Google required mobile device manufacturers to pre-install Google Search and its Chrome browser and obtain a license from Google to use its Play Store application store. In addition, the Commission found that mobile device manufacturers could only obtain the operating licenses if they had undertaken not to sell devices running alternative Android operating system versions, contravening Google's services bundling. Finally, the Commission found that Google granted a portion of its revenues from advertising to device manufacturers in exchange for their commitment not to pre-install competing general search engines.

According to the Commission, these restrictions aimed to protect and enhance Google's dominant position in mobile operating systems. The Commission noted that, as of July 2018, Google's Android operating system was installed on approximately 80% of smart mobile devices in Europe. It concluded that the common objective of and interconnection between the restrictive practices in question led the Commission to classify them as a single and continuous infringement of Article 102 of the TFEU. The Commission imposed a fine of €4.3 billion on Google.

Google and Alphabet appealed the European Union's decision, which was rejected by the GC in most, if not all, relevant aspects. The GC confirmed all the findings of the Commission's decision regarding the anti-competitive effects in one of the most critical rulings in competition law, a ruling of precedential value with widespread lateral implications for other companies. It accepted the Commission's claims, according to which Google imposed illegal restrictions on manufacturers of Android mobile devices and mobile network operators to consolidate its dominant position.

The GC's findings carry implications in terms of their added value for other ongoing cases. One such case involves Google's activity in online advertising. In June 2023, the Commission filed charges against Google for its anti-competitive activity in "ad tech", a field in which Google dominates in the EEA. The Commission claims that Google has been abusing its dominant position by favouring its own ad exchange, AdX, in ad selection auctions and the way its Google Ads place bids on ad exchanges. So, Google is perpetuating its dominant position and shutting competitors out of the market. The *Google Android* case will also probably influence future enforcement actions and shape related legislation. In its ruling, the GC reiterated the importance of identifying the relevant market, determining its scope, and analysing its structure to assess market dominance and anti-competitive behaviour:

> *In that regard, it must be pointed out that the purpose of determining the relevant market and the dominant position held on that market by the undertaking concerned is not only to define the fact and extent of internal competitive constraints specific to that market, but also to verify that there are no external*

competitive constraints from products, services or territories other than those which form part of the relevant market under consideration.[47]

In Google's biggest legal defeat to date, the GC's ruling to reject Google's appeal compelled Google to discontinue some of its anti-competitive practices. The principles tested in these cases have since become the foundations of the DMA designed to render the European digital market more competitive for businesses and a better-protected space for consumers.

In another case, on September 27, 2023, the GC affirmed the Commission's decision, validating Valve's infringement on cross-border sales restrictions and five video game publishers operating on the "Steam" gaming platform. This legal development shed light on the intricate relationship between intellectual property (IP) rights and competition law concerning the cross-border provision of copyright-protected content within the EU.[48] As the operator of Steam, Valve permitted publishers to geo-block Steam keys, restricting users in specific countries from activating games purchased elsewhere. The Commission identified anti-competitive practices, leading to Valve's five Article 101 TFEU infringements. The GC upheld this decision, revealing that Valve and the publishers had engaged in anti-competitive agreements between 2010 and 2015, aiming to limit cross-border sales.[49]

Valve contended that it provided technical geo-blocking services, arguing that it did not fall under Article 101 TFEU. However, the GC disagreed, affirming that such conduct was within the Article's scope, even in vertical relationships with competition restrictions. The GC dismissed Valve's attempt to annul the Commission's decision, asserting that the Commission sufficiently demonstrated agreements or concerted practices between Valve and each publisher, intending to restrict parallel imports through geo-blocking.[50]

The Court emphasised the necessity of a "concurrence of wills" for anti-competitive agreements, noting Valve's active promotion of geo-blocked keys to restrict imports, demonstrating acquiescence in the restrictive agreements. The GC rejected Valve's claim that IP rights justified competition restrictions, asserting that IP rights could not be exploited to eliminate parallel imports, as the primary goal of the agreements was competition restriction.[51]

Notably, the GC clarified that geo-blocking was not aimed at protecting copyright but rather at eliminating parallel imports and safeguarding substantial royalty amounts collected by publishers or profit margins earned by Valve. The judgment delved into the intersection of EU competition law and copyright, emphasizing that copyright protection did not grant right holders the right to demand the highest possible remuneration or foster

[47] ibid para 191.
[48] Case T-172/21 *Valve Corporation v European Commission* [2023] ECLI.
[49] ibid para 6-11.
[50] ibid para 94.
[51] ibid para 192.

artificial price differences among national markets, as it hindered the completion of the internal market.

Valve's arguments challenging the categorisation of the conduct as harmful to competition and a restriction by object were dismissed by the GC. The Court underscored that Valve failed to undermine the overall assessment of the collusive conduct, emphasizing that the alleged pro-competitive effects of geo-blocking did not cast doubt on its harmful impact on competition.

This ruling addressed the intricate interplay between competition law and IP rights, deviating from established case law. It challenged the assumption of IP rights as insurmountable barriers, signalling a broader trend of reduced deference to intellectual property within competition policy.

Another example is the case of *ByteDance v. Commission*, 2023. ByteDance, the holding company of TikTok, was classified as a gatekeeper under the DMA. They challenged this classification, contending that they did not fulfil the required criteria and sought to overturn it while requesting temporary measures to suspend obligations outlined in Articles 5, 6, and 15. ByteDance argued that revealing confidential information as mandated by the regulation would negatively impact its competitive edge and that limitations on data usage would stifle innovation. They claimed such disclosures would give competitors unfair advantages and erode user trust.

In contrast, the Commission maintained that these claims were speculative and asserted that adequate legal safeguards were in place. The Court determined that ByteDance's evidence did not demonstrate significant and irreparable harm, stating that any financial damages could be remedied through compensation. It concluded that ByteDance failed to show the urgency for interim measures since the alleged harms were either speculative or insufficiently supported. As a result, their request for interim measures was rejected.[52]

6 Summary

This paper explored the anticipated developments and the critical importance of digital competition within the Digital Single Market (DSM) framework. The DMA seeks to harmonise rules and regulations across the EU, fostering a cohesive and unified approach to digital competition. This harmonisation is crucial to prevent fragmented regulatory landscapes that could impede the functioning of a unified digital market. The centrality of digital competition under the DSM prism is emphasised by the recognition that digital markets transcend national borders. By promoting fair competition, the DMA aims to stimulate innovation, encourage new market entrants, and provide consumers with greater choices. Viewed within the framework of the DSM, digital competition catalyses

[52] Case T-1077/23 *Bytedance Ltd v European Commission* [2024] ECLI.

economic growth, job creation, and the establishment of a dynamic, resilient digital economy.

Furthermore, the DMA is a pivotal tool in strengthening the EU's TNP. This strategic approach emphasises safeguarding fundamental rights while preserving the integrity of the single market regulatory regime. By setting forth regulations to ensure fair competition and prevent anti-competitive practices among digital gatekeepers, the DMA aligns with broader TNP objectives: upholding fundamental rights, fostering digital sovereignty, and maintaining a cohesive regulatory framework within the Digital Single Market. In this way, the DMA addresses both economic considerations and reinforces the EU's normative influence, shaping a digital landscape that prioritises fairness, innovation, and the protection of individual rights.

However, as this paper critically highlight, while the DMA represents an ambitious attempt by the EU to regulate Big Tech and foster fair competition in digital markets, significant challenges remain. The centralised enforcement model raises concerns about the Commission's capacity to manage compliance effectively, particularly given the scope and scale of Big Tech. Moreover, the rigid rules set forth by the DMA may, ironically, stifle the very innovation it seeks to promote, especially when faced with the complexities of rapidly evolving digital ecosystems.

Additionally, while the DMA aims to extend the EU's regulatory influence globally, its extraterritorial reach may lead to unintended consequences. The tangible risk is that services and innovation could be relocated to jurisdictions with less stringent regulatory frameworks, undermining the Act's objectives. The balance between regulation and market dynamism is delicate, and whether the DMA can strike this balance effectively remains to be seen.

Ultimately, the DMA's success hinges on the Commission's ability to enforce compliance and to remain flexible enough to adapt the regulations in response to the digital market's rapid evolution. Future research and scholarship will play a crucial role in continuing to assess the DMA's impact on both market competition and innovation, providing a critical lens through which to evaluate the effectiveness of Europe's regulatory framework in the ever-changing digital age.

Simona Ghionzoli *

GENERAL SECTION

AI SYSTEMS AT THE WORKPLACE LEGAL TRAJECTORIES BETWEEN PRIVACY AND DRONES 2.0 STRATEGY

Abstract

The case study exam shows that the civil use of drones also concerns production contexts, so talking about drones necessarily implies a reflection on the impact of technology on workers' rights and freedoms.

In fact, it is now recognised that the right to privacy is a principle on which identity and psycho-physical integrity, and therefore individual and collective health and safety, are based.

Firstly, the main national, international and EU regulations that have intervened over time to regulate the matter and that constitute the state of the art will be examined, namely the Chicago Convention of 7 December 1944 on International Civil Aviation, the special provisions made by the Navigation Code, Regulation (EU) No. 1139/2018 unifying the subject matter and the subsequent implementing Regulations No. 945 and 947 of 2019, in an attempt to systematise and understand whether the set of rules currently in force, starting with strict liability, adequately responds to the needs of the commercial development of the sector and to an effective protection of workers.

Market requirements, moreover, require that certain technical standards be met before the product is put into circulation.

Drones, although they have very high levels of automation and can be identified by artificial intelligence systems, according to Art 2 para 2 and Art 6 para 1, are, however, only partially affected by the recent Regulation establishing harmonised standards on artificial intelligence. They are classified as high-risk systems and the Regulation only reserves to them the application of certain provisions concerning product conformity requirements for placing on the market or their use, the first of which is the principle of human oversight. Furthermore, the prerogative of regulatory experimentation spaces (the so-called Sandbox) is provided for in article 57 of the AI Act.

Has an opportunity for the protection of fundamental rights been missed or are the instruments of legal protection, mainly of the psycho-physical integrity of the worker, also linked to the protection of personal data, still guaranteed by Regulation (EU) No. 679/2016 of 27 April 2016?

With this contribution, we intend to demonstrate that the legal institutions contained in the GDPR such as the principle of accountability and in particular privacy by design, DPIA, the tools of negotiation and consultation in the company such as codes of conduct and negotiation with the social partners remain the

* The author is Ph.D (c) in International Studies at l'Orientale University of Naples and Junior Researcher at Re.CEPL, Research Centre of European Private Law, at Suor Orsola Benincasa University of Naples.

DOI 1.13135/2785-7867/11338

most protective and effective for the purposes of implementing the principle of transparency and mitigation of the risks underlying operations that employ pervasive technologies such as drones.
In particular, the unifying Regulation (EU) No. 1139/2018, which shares with the GDPR the legal institution of privacy by design, will be examined.
Having said this, it will be appropriate to examine possible regulatory developments regarding the methods of assessing risk situations to be carried out, if possible, in a shared and preventive manner, right from the development of the software, in order to prepare suitable measures to avert dangerous situations and harmful consequences.
Studying an unprecedented technology such as drones in the context of work is, moreover, both an opportunity and a pretext to reflect on the legal strategies and instruments made available by the legislator to limit and control the exercise of employers' powers.
Mitigating the objective aspects of liability and allocating it in a different way and not only on the operator is another possible development of the legislation.
To the extent that UAVs will be deployed in production contexts, in fact, unprecedented scenarios will open up, which may configure profiles of liability on the part of the employer for the protection of privacy, but will also favour the emergence of unprecedented forms of union bargaining and new organisational models, aimed at strengthening the consent and information of workers as well as improving living and working conditions.

JEL CLASSIFICATION: K15

SUMMARY

1 General remarks[1]

In 1970, with the Statute of Workers' Rights (formerly article 4 of Law No. 300 of 20 May 1970 as amended by Art 23 D Lgs. 151/2015 of 14 September),[2] the Legislator introduced and recognised in the Italian legal system provisions protecting the privacy of workers, which, until then, had only been recognised indirectly and limited to certain

[1] This work is the result of reflections, many of which set out during the scientific internship at Aitronik S.r.l., in S. Giuliano Terme (PI), related to the Ph.D Programme in International Studies. A special thanks to EdgeLab S.p.a. in La Spezia, to l'Orientale University of Naples and to CNR IIT of Pisa for the support in the realisation of this research experience.
[2] Statute of Workers' Rights Art. 4 of Law No. 300 of 20 May 1970 (hereafter Statute of Workers' Rights) as amended by Art 23 par 1 D Lgs 151/2015 on 14 September, so-called Jobs Act (hereafter Jobs Act).

individual aspects, such as those in articles 14, 15, 21 and 2 of the Italian Constitutional Charter.[3]

The latter provision, in particular, absorbs privacy among the fundamental rights of the individual, similarly to what is stated, instead, expressly in articles 7 and 8 of the Charter of Rights of the European Union, signed in Nice on 7 December 2000.[4]

In production contexts, the protection of fundamental rights, first and foremost the right to privacy, is now a central issue, due to the spread and development of increasingly innovative and pervasive technologies, which open up unprecedented video surveillance scenarios.

Regulation (EU) No. 679/2016, reserves an article, namely article 88, entitled "Processing of data in the context of the employment relationship", for the processing of personal data that occurs by means of the use of technology and monitoring systems.[5]

Mobile video surveillance exercised by means of Unmanned Aircraft System, UAS (so-called drones), is used in various operational contexts to ensure first and foremost the safety and surveillance of workplaces, which could not be guaranteed through the use of fixed devices.

The production sectors that have decided to make use of these technologies have mainly been those of logistics and e-commerce for warehouse functions.

It is also worth mentioning the experiences of urban video surveillance in some municipalities, carried out by the municipal police by means of drones (road safety, pedestrian flows, parking times, access to areas closed to traffic, etc) and the surveillance of oil wells, pipeline safety, thermoelectric power stations and industrial plants.

In such areas, artificial intelligence solutions may accompany video surveillance systems, as so-called high-resolution eyes are able to monitor and control areas that are difficult to reach or dangerous and to do so in real time, recognising, through image processing and edge computing and deep learning mechanisms, dangerous situations.[6]

In such contexts, drones use special sensors (thermal imaging cameras, multispectral cameras, etc) to indicate and maintain their flight path and to detect and collect information, carry out surveillance and reconnaissance autonomously. They are equipped with radars, cameras, IR scanners.

Drones process personal data when combined with other technologies and are able to interact with location technology, based on GPS satellites. Integrated technologies could

[3] Domenico Fauceglia, 'Cybersecurity, concorrenza, contratti e cyber-risk' (2020) 1(1) EJPLT 1.
[4] Charter of Fundamental rights of the European Union [2016] OJ EU C 202/389.
[5] Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016 (hereafter GDPR) concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, art 88, par 2, which devolves to the member states the possibility of providing, by law or by means of collective agreements, more specific rules to safeguard the human dignity of the legitimate interests and fundamental rights of the data subjects, in relation to, inter alia, transparency of processing and monitoring systems in the workplace.
[6] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023) Discussion paper available at <https://www.osha.europa.eu> accessed 05 September 2023.

also include the ability to track devices equipped with Rfid chips and the people/vehicles wearing them. When used with geo-localisation devices, they can intercept communications and electronic devices, leading to the profiling of people.[7]

In fact, they are equipped with 'visual recording equipment' technology with facial recognition capabilities on board or from the ground that allows tracking and identification of persons and sensitive and personal data (see Art 4.1 and 9, para 1, Reg. (EU) No. 679/2016).

Most of them collect information on the daily life of users and their sensitive characteristics including physical and mental states.

Emotion recognition is a highly invasive form of surveillance that involves the mass collection of sensitive and less sensitive and unaccountable personal data, enabling the tracking, monitoring and profiling of individuals often in real time.

They can carry huge amounts of sensors, carry out systematic and penetrating surveillance inside buildings, confirming intrusiveness and potential danger.

In the workplace, one must not overlook the importance of 'movement and location' data as defined by Art 2 (c) of Directive 2002/58/EC as amended by Directive 2009/136/EC,[8] ie "any data processed in an electronic communications network or in an electronic communications service that indicates the geographic location of the user's terminal equipment in a publicly accessible communications service", because they are considered as an identifier, allowing one to identify one's position and trace one's movements and therefore capable of making any subject associated with it identifiable.[9]

This explains the non-existence of anonymous or non-personal location data, because every time the presence of a natural person is identified at a point in space, any information or data will in itself constitute the processing of personal data, which as such needs to be addressed.[10]

Article 4, para 1 of the GDPR mentions, in this respect, 'identifiers' accompanied by the adverb 'any', as elements capable of linking the information to the natural person in order to identify him or her.[11]

[7] Direzione Generale Per le Politiche interne, Dipartimento di Politica Diritti dei Cittadini e Affari Costituzionali, 'Privacy and Data Protection implications of the civil use of drones' (2015), available at <www.europarl.europa.eu/studies> accessed 4 November 2024.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] GU L201/37 consolidated version [2009] GU L337/11.

[9] Giovanni Maria Riccio, Guido Scorza, Ernesto Belisario (eds), *GDPR e normativa privacy. Commentario* (2nd Edition, Wolters Kluwer Press 2022) 790.

[10] Gianclaudio Malgieri, 'La titolarità dei dati trattati per mezzo dei droni tra privacy e proprietà intellettuale' in Erica Palmerini Maria Angela Biasiotti Giuseppe Francesco Aiello (eds), *Diritto dei droni: regole, questioni e prassi* (Giuffré Francis Lefebvre Press 2018) 194.

[11] For an in-depth discussion of the effectiveness of anonymisation and pseudo-anonymisation of personal data see GPDP Provv. n. 5, of 11 January 2024 available at <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9977020> accessed 08 March 2024.

1.1 Definitions and categories in national, international and EU legislation

Drones are legally defined as aircraft.

The 1944 Chicago Convention on International Civil Aviation referred in its article 8 to "aircraft capable of being flown without a pilot".[12] The Riga Declaration on Drones of 06/03/2015, states that "drones need to be treated as a new type of aircraft with proportionate rules based on the risk of each operation".[13]

Regulation (EU) No. 1139/2018 in Art 3, para 30, covers "unmanned aircraft" that "means any aircraft operating or designed to operate autonomously or to be piloted remotely without a pilot on board".

In order to correctly define and classify aircraft, reference should be made to article 2 of Regulation (EU) No. 947/2019, which contains the definition of UAS or Unmanned Aircraft System, unmanned aircraft and its remote-control devices. UAS means "an unmanned aircraft and the equipment to control it".

This definition is the one preferred by the ICAO (International Civil Aviation Organization). It is inclusive of the aircraft, but also of the network and personnel equipment required to control the aircraft. It differs from the acronym UAV or Unmanned Aircraft Vehicle, which is generically understood as an aircraft designed to operate without a pilot on board, carrying no passengers, remotely piloted, capable of autonomous flight, without reference to equipment.

The regulatory framework on drones consists of a number of acts, which are coordinated in a hierarchical manner with an international level, an EU level and a national level, the latter of which can be traced back to special laws and articulated as follows:

Convention on International Civil Aviation signed in Chicago on 07/12/1944;

Regulation (EU) No. 1139/2018 of 04/07/2018;[14]

Delegated Regulation (EU) No. 945/2019 of 12/03/2019;[15]

[12] Chicago Convention on International Civil Aviation of 07 December 1944 approved and made enforceable by Legislative Decree No. 616 of 06 March 1948 (hereinafter Chicago Convention).

[13] Risoluzione del Parlamento Europeo del 29 ottobre 2015 sull'uso sicuro dei sistemi aerei a pilotaggio remoto (Rpas) noti comunemente come veicoli aerei senza equipaggio (UAV - Unmanned aerial vehicles) nel settore dell'aviazione civile. [2017] GU C355 /09.

[14] Regulation (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in points (a) and (b) of Article 2(1) thereof, where it concerns unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned [2018] OJ L212/1, consolidated version [2021] C/2021/2102, corrected on 04 May [2023] OJ L116/30 (hereinafter Reg. (EU) No. 1139/2018).

[15] Regulation (EU) No. 945/2019 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems [2019] L152/1, consolidated version [2020] 09 August L/232 (hereinafter Reg. (EU) No. 2019/945).

Implementing Regulation (EU) No. 947/2019 of 24/05/2019;[16]

Navigation Code (Royal Decree No. 327 of 30/03/1942);[17]

Reg. ENAC UAS IT of 04/01/2021 (for aspects falling under the provisions of Art 2, para 3 of Reg. (EU) No. 1139/2018 and for aspects falling within the competence of the member states).

In the Implementing Regulation (EU) No. 947/2019 of 24 May 2019 on operating rules and procedures for the operation of unmanned aircraft, in force since 31.12.2020, in Art 3, operations are divided into three categories, based on risk. This classification originates from the previous Regulation (EU) No. 1139/2018 of 04 July 2018. This article defines and divides transactions into three categories, namely 'open', 'specific', and 'certified'.

The following UAS can be found in the Open category:

C0 to C4 marked with class identification label;

Unlabelled or marketed before 31/12/2023;

Self-built (for personal use);

With a maximum take-off weight not exceeding 25 kg;

Compliant with the technical requirements set out in Regulation (EU) 2019/945.

For such devices, the operator's registration on d-flight, the pilot's certificate is required, with the exclusion of means weighing less than 25 kg and the obligation of insurance coverage. The maximum flight height is 120 meters and they are required to fly by visual line of sight (Vlos), ie they must maintain a line of sight between the drone and the remote pilot, with a ban on flying over gatherings of people and transporting dangerous goods and releasing materials and substances. They are subdivided into further subcategories: A1, A2, A3. For class A1, operator registration is required when the drone is capable of capturing personal data.

The 'specific' category instead refers to:

drone operations that do not fall under the previous Open category;

operations that take place on standard national or Easa-defined scenarios, effective from 01/01/2024;

For this category, registration on D.flight of operators and operational authorisation (ENAC) is required if they fly over non-standard scenarios.

The categories are subdivided into subcategories that are relevant above all for the purposes of pilot training and operator registration, which are always envisaged, with the exception of subcategory A1 open, which is suggested in the first case, compulsory in the second, when the drone is capable of collecting personal data.

[16] Regular update of the AMC and GM to Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft OJ L/152/45, consolidated version of 4 April 2022 L105/3 (hereinafter Reg. (EU) No 2019/947) - Issue 1, Amendment 2 AMC and GM to the Annex to regulation (EU) 2019/947, Amendment 2, available at <https://www.easa.europa.eu> accessed 4 November 2023.

[17] Regio Decreto of 30 March 1942 approving the Navigation Code (Italy) (hereinafter Navigation Code).

The drones that concern the operational contexts that we are going to examine are mainly those that carry out loading operations, in Vlos as in the case of Ikea Variety drones or Amazon warehouses, or surveillance operations of gas installations or 'Variety Ikea' drones or those in use by the police for urban surveillance.

As of 1 January 2024, in order to place a UAS on the European market, a declaration of compliance with Reg. (EU) No. 945/2019 is mandatory.

Any drone placed on the market before 1 January 2024 without a class label is considered a so-called "legacy" drone, ie they may continue to operate in the Open A1 subcategory if they have a maximum take-off mass of less than 250 grams, including payload, or in the A3 subcategory provided they have a maximum take-off mass of less than 25 kg including fuel and payload. Drones that are not classified and placed on the market after 1 January 2024 are prohibited from use in the Open category if they do not meet the above requirements and may only fly in the specific category.

The 'certified' category presents the highest risk and therefore needs more stringent requirements and safety conditions to ensure high levels of safety. Their use requires the certification of the drone and the operator and the authorisation of the remote pilot when the operation takes place on assemblies of people and involves the transport of people, dangerous goods, or when the size of the drone is greater than three metros. This type of drone concerns future development models for mobility and transport called IAM Innovative Air Mobility and UAM International, Regional and Urban Air Mobility.

1.2 State of the art. The march of drones in national, international and EU legislation. Judicial intersections with AI Act

UAS profanely called drones have different types in terms of shape, size and weight.[18]

A review of the literature shows that even though unmanned vehicles have a separate technology from other classes of robots,[19] they are nevertheless part of the broader genus of robotics,[20] consisting generically of articulated arm robots, humanoid and social robots,

[18] Giovanni La Cava, Angelica Marotta, Fabio Martinelli, Andrea Saracino, Antonio la Marra, Endika Gil-Uriarte and Victor Mayoral-Vilches, 'Cybersecurity issues in robotics' (2021) 12 (3) Journal of wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (Jowua) 1, 28.

[19] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health', available at <https://osha.europa.eu> accessed 05 November 2023.

[20] Lara Merla, "Droni, privacy e tutela dei dati personali" (PhD Thesis, Università degli Studi di Torino 2016) 29. The author recalls some authors such as Ronald Leenes and Federica Lucivero who suggest "*Di cogliere l'intento regolativo del diritto nell'ambito della robotica, secondo una quadripartizione. In primo luogo si pensi alla disciplina dei progettisti e costruttori di robot, quali i droni, attuata attraverso la legge, come nel caso degli standard di sicurezza ISO o le norme sulla responsabilità civile e penale per produttori e utenti dei medesimi. In secondo luogo, il richiamo va alla regolazione del comportamento degli utenti e/o operatori dei droni, tramite il design di questi ultimi, vale a dire progettando queste macchine in modo tale che non sia consentito alcun comportamento illecito degli esseri umani. In terzo luogo si può pensare alla disciplina legale degli effetti dei comportamenti robotici per il tramite delle leggi approntate dal legislatore: è il caso ad es. della contrattualistica e della negoziazione a mezzo di agenti software. In quarto luogo, infine, la legge può mirare alla disciplina del comportamento robotico tramite il suo design, ossia immettendo direttamente i dettami della legge nel software dell'agente robotico. In questo caso AI metodi tradizionali*

unmanned vehicles, which are subdivided into land vehicles, Ugvs and other land robots, underwater vehicles (Uuvs) and aerial vehicles (Uavs).[21] What is important, however, is the difference between autonomous vehicles and remotely piloted vehicles, i.e. autonomous aircraft (SAPR) in which there is no human intervention and in which the flight is totally software-driven, and remotely piloted aircraft (or Apr), a category falling under the concept of unmanned aircraft, in which there is a pilot but operates from a remote station.

The ENAC Regulation of 16 July 2015 combined these two types, ie the SAPR in which there is no pilot but a software, including the APR, in which instead there is a pilot, albeit remotely.[22] Both were considered aircraft under the Chicago Convention on International Civil Aviation of 1944, to which article 743 of the Italian Navigation Code refers, which bases the qualification of an aircraft on a man-made constraint.

The destination constraint is that specified in article 743 of the Navigation Code, which in its first paragraph states that "Aircraft means any machine intended for transporting persons or things by air. Also considered aircraft are remotely piloted aerial means, defined as such by special laws, ENAC regulations and for military ones by decrees of the Ministry of Defence".

To all drones, apart from toy drones, ie drones complying with the Toys Directive 2009/48, which are not subject to registration and cannot be assimilated to aircraft (see Art 1, para 4) ENAC Regulation), the 1944 Chicago Convention on International Air Transport therefore applies.

The assimilation took place, based on Regulation (EU) No. 1139/2018 of 04 July 2018, on common rules in the field of civil aviation and aviation security, followed by implementing acts 945 - New European Regulatory Framework - and 947, which transposed

---

di regolamentazione giuridica, sul piano del dover essere kelseniano "se A, allora B", si affianca - o viene sostituita - da l'intento regolativo della legge tramite il design dei ricavati tecnologici: nel nostro caso i droni. Si tratta di una forma di tecno-regolazione giuridica sul piano dell'essere - o degli automatismi normativi - all'insegna del cosiddetto principio della privacy by design"; see also <https://osha.europa.eu> accessed 04 November 2023 on Unmanned aerial vehicles: implications for occupational safety and health, where UAVS are a class of devices including multirotor drones, as well as single-rotor and fixed-wing devices, hybrid versions, and, potentially, alternative propulsion systems. The common characteristic of these devices is that they are all able to move, with or without a load of some type, in the same (work)space inhabited by humans. In a simplistic view, UAVS are robots that can 'fly' and 'From all UAV types, drones are, unquestionably, the fastest growing class (both in sheer numbers and capabilities). Therefore, the term is often used for the full class of UAVS. As of May 2022, the FAA acknowledged 865,000 registered drones in the United States, including commercial and recreational, with an estimated annual increase of approximately 6.4%. In Europe, the annual increase is estimated between 5.3% and 6.3%, with an accelerating trend (from data available in Molina & Oña, 2017). In both markets, military applications represent the biggest value'; see also Guido Noto La Diega, Machine rules of drones. Robots, and the info-capitalist Society [2016] 2 ILJ 367, according to which (.) indeed, most considerations apply equally to robots and drones, moving from the unrefined, albeit practical, observation that the latter are robots equipped with wings.

[21] Cecilia Severoni, 'Il regime di responsabilità per l'esercizio dei mezzi a pilotaggio remoto', in Erica Palmerini Maria Angela Biasiotti Giuseppe Francesco Aiello (eds), *Diritto dei droni: regole, questioni e prassi* (Giuffré Francis Lefebvre Press 2018) 81.

[22] ENAC Regulation on remotely piloted aircraft of 17 July 2015, available at <www.enac.gov.it> accessed 10 September 2023.

the qualification of UAS, referred to in Art 2 Regulation (EU) No° 947/2019, replacing that of SAPR, in use until then in the legislation.

Regulation (EU) No. 1139/2018, which lays down common rules in the field of civil aviation, certainly also applicable to unmanned drones (see Cons. No. 26), assumed that even drones weighing less than 25 kg were potentially capable of causing harm to persons and property on the surface and, above all, pose a danger to the acquisition and processing of personal data.

It also lays down basic principles to ensure security, privacy and the protection of personal data, through the introduction of basic requirements (Art 55 ff) and a specific bureaucratic procedure to promote technological innovation, which provides for a common certification system.

All types of drones are integrated, regardless of weight and size, within the framework of Easa's Common Aviation Security.

It partly implemented the Riga Convention of 06 March 2015, whereby drones were all to be treated as a new type of aircraft, dictated key points for the future regulation of drones for civil use, including the protection of privacy, equated manned drones with unmanned drones, stipulated that safety rules were to be commensurate with the actual risk of each individual operation, which it is easy to see how it presents problems, especially in terms of privacy and security of data and networks.[23]

Under the pretext of privacy, the criterion of weight was overcome and additional elements emerged, for the purposes of the configuration of liability, such as the risks associated with the activity, such as that relating to the processing of personal data.

The recent measures of the EU legislator, such as the AI Act and the Cyber Resilience Act, proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) No. 1020/2019 (see Art 2, para 3), the former merely amends and supplements Regulation (EU) No. 1139/2018, and the latter excludes from its scope products with digital elements that have been certified in accordance with Regulation (EU) No. 1139/2018, which are drones, as they are treated in the same way as products with digital elements, in particular those for civil use, and those developed for exclusively military or national security purposes are also completely excluded from the regulatory scope.

The Regulation of the European Parliament and of the Council, which establishes a common framework of rules on AI, in Art 2, in the first version, stated “For AI systems

[23] Theresa Papademetrio, ‘Regulation of Drones: European Union’ (Report April 2016 USA, the Law Library of Congress, Global Legal Research Directorate), available at <http://www.law.gov> accessed 30 September 2022; the author outlines the key guiding principles to be considered in the future regulation of drones whereby Drones must be treated as a new type of aircraft and any safety rules imposed must be proportionate to the risk of each operation. It is crucial that the EU immediately establishes safety rules and standard technologies for the integration of drones into civil aviation. It notes how protecting people's privacy will lead to greater public acceptance. It reiterates that the operator of a drone is responsible for its use and in relation to this last principle the Declaration raised the issue of liability and insurance aspects.

classified as high-risk AI systems in accordance with Articles 6, para 1 and 6, para 2, related to products covered by Union harmonisation legislation listed in annex II, section B only article 84 of this Regulation shall apply. Article 53 shall apply only insofar as the requirements for high-risk AI systems under this Regulation have been integrated under that Union harmonisation legislation". Well, drones were included in Annex II, section B, and consequently, the Artificial Intelligence Regulation would apply to them, but only limited to certain provisions.

In the current version of the Regulation approved on 13 June 2024, article 2, para 2, refers to article 6, para 1, and classifies drones as high-risk artificial intelligence systems and confirms that only articles 102 to 109, article 112 and article 57, which govern sandboxes, are applicable to them, limited to cases in which the requirements for high-risk artificial intelligence systems, pursuant to the regulation, have been incorporated into union harmonisation legislation (see Art 108 AI Act, which calls for the requirements set out in chapter III section 2 AI Act to be taken into account).

According to Art 6, para 1, AI system is considered to be high-risk if two requirements are fulfilled, ie if it is intended to be used as a safety component of a product or is itself a product covered by the Union harmonisation legislation listed in annex I, and at the same time the product, the safety component of which within the meaning of (a) is the AI system or the AI system itself as a product, is subject to a third-party conformity assessment for the purpose of placing that product on the market or putting it into service again under the legislation listed in annex I, traceable to Regulation (EU) No. 1139/2018.

AI Act has a product-oriented approach.[24] This regulation shares with the GDPR and Regulation (EU) No. 1139/2018 the concept of privacy and security by design, certification mechanisms, risk assessment and measurement, and mitigation tools.

Furthermore, with the adoption of the Cyber Resilience Act, certain regulatory gaps will be resolved and consequently cybersecurity, too, will be considered a priority element in design, the lack of which may constitute a defect in the product.[25]

Recognition of the product's lack of security, also due to the lack of defence mechanisms against cyber-attacks, could reasonably lead to the assumption of a case of liability by omission.[26]

Statistics show, in fact, accidents to persons and acts of hacking, mainly involving drones flying over long distances (Bvlos).[27]

These are cyber-physical systems and therefore exposed to cybercrime more than other devices. The most exposed are precisely those for recreational or commercial use, which

[24] This feature of the AI Act also emerged at a conference, organised by the Cesifin Foundation 'Persona, dati personali, algoritmi, tra GDPR e AI Act' (17 June 2024 Florence). See speech by Professor Salvatore Orlando "Decisioni algoritmiche, diritto di spiegazione e tutela dei consumatori".
[25] Giovanna Capilli, 'I criteri di interpretazione delle responsabilità' in Guido Alpa (eds), *Diritto e Intelligenza artificiale* (Pacini Press 2020) 485.
[26] ibid.
[27] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023), available at <https://osha.europa.eu> accessed 05 November 2023.

are more vulnerable to hacker attacks because they are equipped with less sophisticated systems.

The danger therefore exists not only for privacy, but also extends to the security and protection of personal data.

Indeed, drones collect information and transmit it and can be connected to the internet, introducing the Internet of Drones (IOD) theme, are products that also consist of a software component that is often connected to or involves the cloud.[28]

Assuming proactive behaviour subsumed under the concept of privacy and security by design and, above all, anticipating threats is very important for designing software and averting possible external attacks or internal incidents, with inevitable liability profiles[29] and significant psycho-social impacts in the workplace.[30]

2 Drones at workplace. Case studies

The European Agency for Safety and Health at work conducted a study, called 'Drones inspecting worksites of gas infrastructure operators (ID 16)', from which it emerges that an increasing number of companies are using artificial intelligence or advanced robotics in work contexts, for reasons related to the efficient organisation of production and to ensure, also, greater worker safety, with the aim of reducing boring, repetitive and dangerous tasks.[31] These objectives, however, must be reconciled with the need to protect their fundamental rights, first and foremost that of privacy and data protection.

The case studies examined concern the use of drones to inspect work sites of gas infrastructure operators by means of drones and a visual system based on artificial intelligence, drones for efficient warehouse logistics, drones for surveillance of urban areas.

Drones for pipeline surveillance: In Norway there are interesting experiences with the use of drones for the maintenance and surveillance of gas infrastructures, located above ground and exposed to the weather. The use of drones, supported by artificial intelligence systems, is useful to minimise risks for workers, who have to move over different altitudes. Drones fly over very large areas to supervise sites and simplify maintenance.

[28] Domenico Raguseo, Rosita Galiandro, Giuseppe Marullo and Antonio De Chirico, 'Cybersecurity for Drones. Types of attacks', available at <www.ictsecuritymagazine.com> accessed 10 November 2023.
[29] G Alpa, *Manuale di diritto privato* (Wolters Kluwer Press 2020) 916. The author, while critical of such a jurisprudential approach, nevertheless reports that the assumption that "*La colpa per omissione ha quale presupposto l'esistenza di un obbligo di agire per evitare l'altrui danno o per rimuovere una situazione di pericolo dove l'individuazione del presupposto dell'illecito non riguarda soltanto la prevenzione di un fatto dannoso, ma anche quella di un fatto potenzialmente dannoso e non ancora attuale: di qui l'ammissione dell'esistenza di un "illecito di pericolo" da molti ignorato nelle elaborazioni dottrinali che proprio in materia di colpa omissiva manifesta i suoi aspetti essenziali*".
[30] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational safety and health' (2023), available at <https://osha.europa.eu> accessed 05 November 2023.
[31] European Agency for Safety and Health at Work, 'Drones inspecting worksites of gas infrastructure (ID 16)' (2023), available at <http://osha.europa.eu> accessed 15 September 2023.

The drones are supported by cameras and algorithms, searching for specific obstacles and dangers. The algorithm, pre-trained on a large database of indexed images, analyses the visual input of the camera specifically for fallen or forgotten objects on the ground, classifying the objects to be removed and informing the operator.

Through the quality of the image, a reliable result is guaranteed. The quality originates from the algorithms.

The visual inspection system is based on artificial intelligence-based back-end software, which performs a cognitive and informational task.

The analysis of the images is based on information, which leaves little or no room for human evaluation activities, which are limited to carrying out what comes out of the drone's analysis (recovery and removal of fallen objects, minor and major repair work).

The use of these devices contributes significantly to improving safety in the workplace and is also relevant at the psycho-social level, because it fosters the acceptance of digital innovation in the company, linked to the perception of the usefulness of these tools and interaction with them through the preparation and participation in appropriate training plans.[32] This will contribute to the enhancement of skills, self-esteem and trust in the company. There will also be benefits for the improvement of the climate and inter-human relations in the company, linked to the increase in time available for sharing and confrontation, taken away from production.

Space and working time will be progressively enhanced and made more efficient. This will correspond to an increase in the quality of life in the workplace especially if it is accompanied by a reconsideration of working time and working hours through bargaining.[33]

Verity drones: Ikea is the first retailer to use Verity for night-time inventory checks, ensuring product availability online and in shop.

Drones help improve inventory accuracy, increase productivity, lower labour costs for warehouse management, and increase efficiency and employee satisfaction. They are able to detect an error before it can turn into a system flaw. By means of drones, work automation systems are introduced, which although they may be repetitive, are characterised by dynamic elements such as the ability to analyse work processes.

Warehouse operators are able to detect errors in advance, ie before the pallet is picked, using images captured by drones. The inventory manager examines the report in the verity cloud before the start of the first shift, identifying errors to be corrected together with the workers, who are involved from the beginning in the analysis, correction of malfunctions and updates. Repetitive and boring tasks such as frequent cycle counts are significantly reduced. The drones are released at night and are supplemented by

[32] Tiziano Treu, 'La digitalizzazione del lavoro: proposte europee e piste di ricerca' (2022) 32 (1) Diritto delle Relazioni Industriali 17.
[33] Anna M Ponzellini, 'Tecnologie, fine della presenza e dilemmi del controllo nei nuovi pattern spazio-temporali del lavoro' (2020) 1 Economia & Lavoro 89 ff.

thermal infrared night vision sensors. They scan the pallets moved in the last 24 hours and the data collected is used to correct errors and provide feedback to workers to facilitate training and process improvement.

The implementation of automation processes in the company, by means of surveillance and AI systems, in this case increases motivation in employees and speeds up production processes, contributes to a greater involvement of the former in the production processes and gives responsibility to supervisors, who are called upon to take note of errors and resolve them.[34]

Drones for surveillance of urban areas: they are used for investigation activities, environmental and building police tasks, surveillance of public buildings or buildings of public interest, traffic accident detection and traffic monitoring, safety and security operations at public events, civil protection activities, prevention and fight against drug offences, rescue and search of missing persons in hard-to-reach areas.

During such operations, it is very easy to violate the privacy of both the workers who use the device and the people who happen to be filmed.

Many Italian municipalities have provided for the use of drones in their Municipal Police Regulations and in order to do so, some preparatory activities, inherent to the implementation of the principle of accountability, have been necessary.

They consist in the preparation of appropriate documentation for the data collection and processing activities, including the security measures adopted to protect personal data from the outset, the first of which is the pact for the implementation of urban security, signed by the Mayor and the Prefect (see Decreto Legge No. 14/2017, Art 5, para 2) (a), of 20 February 2017).[35]

The aforementioned plan outlines the path required to be in line with the GDPR and other sector regulations and to increase accountability, which starts with a description of the starting state of the organisation's video surveillance systems and its IT systems and ends with their compliance and the pursuit of certain objectives.

In this architecture, an important component is confirmed to be that relating to the performance of the DPIA to calculate the risk associated with processing, the purposes of which have already been defined and must be in line with the principles of Art 5 in conjunction with Art 24, which contains the principle of accountability, ie the implementation by the data controller of all technical and organisational measures to ensure and demonstrate that processing is carried out in accordance with the GDPR regulation, right from the early design stages.[36]

[34] Verity, 'Maximizing value. Client success stories in harnessing Verity's benefits' (2023), available at <http://verity.net> accessed 15 April 2023.
[35] For an in-depth examination see GPDP, Provv. No. 234, of 11 April 2024, available at <https://www.garanteprivacy.it> accessed May 2024.
[36] Luca Bolognini and Enrico Pelino (eds), *Codice della disciplina privacy* (Giuffré Francis Lefebvre Press 2019) 201.

Article 35 GDPR is compulsory when the processing involves, in particular, the use of new technologies, which entail risks for the rights and freedoms of persons (see Art 35 para 1) and must take place before the specifications for the purchase of hardware and software tools are prepared.[37]

DPIA is one of the most important declinations of the accountability principle, because it takes place before the treatment itself and also concerns the type of instruments that will be used.

The DPIA provides for the optional consultation of data subjects or their representatives (see Art 35, para 9), which confirms its meaning as an in advance risk assessment tool.

The risks refer to the rights and freedoms of data subjects (see Art 35, para 7, (c), Cons 90 for sources of risk and Cons 84) and relate to the assessment and management of processing risks in both the IT and organisational spheres. The DPIA must be carried out in respect of each of the elements described in article 35, para 7, in relation to each processing operation/tool used. Among these, data protection (also of employees) is very important.

In all three cases considered, the DPIA is necessary, due to the innovative use or application of new technological or organisational solutions as referred to in Art 35, para 1, Reg. (EU) No. 679/2016, as well as due to the presence of at least two of the prerequisites set out in the list in WP 29 consisting in the large-scale systematic monitoring of publicly accessible areas and in the processing of personal data of the operator and/or employees (eg log files or navigation data tracked for security reasons), using the devices to perform work in the case of drones for plant surveillance and in the warehouse, which may give rise to predictive analysis and thus to automated processing, including profiling.[38]

2.1 Drones and employer control powers between GDPR and the Workers' Rights Statute, as amended by the Jobs Act

Legislative Decree No. 151/2015 (Cd. Jobs act), Art 23, as known, treated the matter of remote controls, in an opposite way to the discipline of Law No. 300/1970 (so-called Statuto dei Lavoratori), ie it abrogated the general ban on the use of equipment for the purpose of remote control of workers and revised the discipline, recognising the possibility of their use in typified cases (organisational and productive needs work safety and protection of company assets) and provided that they are accompanied by the stipulation of trade union agreements.

[37] See Cons. 75 and 78, as well as Art 35 par 3 GDPR and the Guidelines WP 248 rev. 01, GDPD, Provv. No. 467, of 11 October 2018, available at <https://www.garanteprivacy.it> accessed 10 January 2019 and at <https://www.ec.europa.eu> accessed 11 January 2024.

[38] See also GPDP Provv. No. 5, of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 March 2024.

Moreover, the legislator, taking into account the changes due to technological evolution, has made certain devices indispensable for work performance and has provided for specific rules for them, exempting them from the obligations set out in Art 4, para 1, preferring to intervene on the limits to the use of the data collected through them rather than prohibiting them.

The vagueness of the expression "working tools", which does not find a precise match on a semantic and regulatory level, gives way for the interpreter and opens up the configuration of different orientations. The first that brings back to the notion of work tools the individual devices assigned to the worker for organisational needs and directly used by the latter not only for the performance of work, but also to make it efficient[39], considering, on the contrary, to be excluded all the others, such as the device or the software program application, when they are not functional to this and instead have exclusive control purposes. According to the orientation set out above, what matters for the purposes of qualification and classification seems to be the usefulness of the device and its components to render the service, to be assessed taking into account the production and organisational requirements, so as to ensure the exact performance of the work service, deduced in the contract. The second, according to which the software allows the operation of the former, but also allows the massive storage of the data in transit of the workers (becoming instruments of remote control), consequently they may be considered instruments of work and fall within the facilitated regime under para 2, only on condition that they are coessential and indispensable for rendering the work performance, considering, on the contrary, that the exception regime must be excluded in the event the performance can nevertheless be rendered even without the aforesaid instrument.[40]

The latter orientation is confirmed by Art 15 of Recommendation CM/Rec (2015) 5 of 1 April 2015, of the Committee of Ministers to Member States on the processing of personal data in the employment context, which reiterates the necessary participation of trade unions in the employer's choices regarding the installation and use of electronic control and surveillance devices (in whatever form this takes place), which remain the ultimate hypothesis to be taken into consideration for the achievement of certain objectives of an organisational nature.[41]

In general, any technical device, including but not limited to the use of video-surveillance systems, which may result in the processing of personal data or which is even

[39] See Carlo Pisani, 'Gli strumenti utilizzati per rendere la prestazione lavorativa e quelli di registrazione degli accessi e delle presenze' in Carlo Pisani, Giampiero Proia and Adriana Topo (eds), *Privacy e lavoro la circolazione dei dati personali e i controlli nel rapporto di lavoro* (Giuffré Francis Lefebvre Press 2022) 445 ff; in jurisprudence see the recent decision of Cass. Civ., 03 June 2024, No. 15391, available at <https://www.dirittoegiustizia.it> accessed 8 June 2024, whereby if installed on company cars intended for the performance of specific services, the telepass must be considered a tool directly functional to the efficiency of the individual performance, as well as now strongly interpenetrated with it in today's working practice.

[40] See Riccio, Scorza and Belisario (n 9) 914.

[41] See CM/Rec (2015) 5, of 01 April 2015, available at <https://www.garanteprivacy.it> accessed 5 November 2024.

potentially capable of doing so, because it collects and processes employee information capable of identifying them or of making them identifiable (see Art 4, para 1, and Art 2 of the GDPR), is liable to result in direct and indirect control.[42]

Drones, although high-precision instruments, when equipped with cameras or sensors, theoretically allow the recording of movements and are able to capture images from the ground with a high level of precision, due to their discretion and versatility. The zoom makes it easy to track people. This means that from work tools[43] that can be used, among other things, for the defence of property, but also of health and psycho-physical integrity, they can be transformed into tools for control of work performance. Directly because of the use of surveillance technology (zoom, video cameras, sensors, etc.), indirectly because of the collection, detection, storage, processing and examination of data and the potential use that can be made of them, for the purposes of predictive, evaluative analyses, profiling of habits and behaviour.

Their use, in the above-mentioned cases, could lead to the transition from a mere presence detector to a remote-control tool[44] due to the collection and processing of data that takes place over a prolonged and continuous period of time; from this point of view, it can only take place after verifying the need to reach a collective agreement with the workers' representatives, pursuant to Art 4, para1, of the Workers' Rights Statute.

Article 88 on the "processing of data in the context of employment relations" devolves to the member states the possibility, through laws and collective agreements, to provide for rules that are more specific to guarantee the protection of rights and freedoms, with reference to the processing of employees' personal data in the context of employment relations and in the second paragraph also specifies how, ie guaranteeing and regulating the transparency of the processing, the transfer of personal data within a group of companies, or a group of companies carrying out a common economic activity and workplace monitoring systems.

Article 88 GDPR speaks of data processing in an all-encompassing way and referring to all workplace monitoring systems, not just video surveillance.

---

[42] *Soc. Italcementi Vs. Fillea CGIL* [1986] No. 1490 Cass Civ available at Arch Civ 1986 155 sofor which what is relevant is the installation of the system, from which remote control of the workers may result, despite the absence of activation of the same, which is such as to require the consent of the trade union or the labour inspectorate, the only ones able to assess the suitability of the instruments to harm the dignity of the workers and the actual compliance of the same with the technical production requirements also with reference to an instrument other than video surveillance; see also Cass. Pen. [2019] No. 50919, available at <https://Foroplus.it> accessed 5 May 2024 for which the violation of the guarantee procedure under Article 4, protecting interests of a collective and super-individual nature, is used to assess the suitability of the instrument to injure the dignity of workers and the effective compliance of the same with the technical production and safety requirements. In the same sense see Cass. Pen. [2014] no. 4331 for which "*c'è violation dell'Art. 4.1 n. 300/1970 anche se l'impianto non è messo in funzione: poiché il bene giuridico protetto è la riservatezza dei lavoratori e il reato in questione si configura come un reato di pericolo, la norma sanziona a priori l'installazione, prescindendo dal suo utilizzo o meno*", mentioned in Bolognini and Pelino (n. 36) 1385.

[43] Giulio Donzelli, 'L'interazione uomo macchina tra tecnologie digitali e successo industriale' in Guido Alpa (eds), *Diritto e Intelligenza artificiale* (Pacini Press 2020) 98.

[44] Cass.Civ. [2016] available at Just Civ Mass, 2016, mentioned in Giulio Donzelli (ibid); on this point see also Council of Europe Recommendation of 1 April 2015 CM/Rec (2015) 5 prohibiting prolonged, constant and indiscriminate controls, available at <https://www.garanteprivacy.it> accessed on 20 May 2020.

The processing of personal data carried out within the framework of the employment relationship, if necessary for the purposes of managing the relationship (see Art 6, para 1 (b) and (c) and Art 9, para 2 (b)) must, however, be carried out in compliance with the principles set out in Art 5 of the Regulation and in particular with the principle of lawfulness, according to which processing is lawful only if it complies with the applicable sectoral regulations (see Art 5, para 1 (a)).

The prerequisites of lawfulness brought by the specific regulations and guarantees of the sector, are those set out in article 4 of Law no. 300 of 20 May 1970, to which articles 113 and 114 of the Privacy Code refer, which are regulations bearing greater and more specific guarantees than those considered by article 88 GDPR.[45]

Article 4, para 1, of the Statute, as amended by Legislative Decree No. 151 of 14 September 2015, peremptorily identifies the cases in which video-surveillance instruments may be used in the workplace and if they give rise to the possibility or danger of remote monitoring of workers, precise procedural guarantees are established.

The case of drones could fall within this case, as there is also only the danger of remote control or profiling and predictive automated processing (in the event of data retention beyond a certain period of time).

Article 4, para 2, introduces an exception to the restrictive regime just considered in the case of instruments used to record presence on duty and to render work performance.

Access to the facilitated regime, at the centre of the doctrinal debate already examined, was recently the subject of a provision of the Privacy Authority, which resolved a similar case on the basis of the criterion of the retention time of e-mail logs, which may not exceed 21 days; otherwise they could be suitable to entail an indirect remote control of workers and therefore be framed under para 1 of Art 4 of the Statute, in so far as they are also potentially capable of collecting information relating to the personal sphere or opinions of the person concerned and therefore not relevant to the performance of the work.

Finally, Art 4, para3, introduces also further profiles of unlawfulness when there is further use of the personal data collected. According to para 3) of Art 4 of the Statute as amended by Art 23 Legislative Decree 151/2015, “the information collected pursuant to paragraphs 1 and 2 may be used for all purposes connected with the employment relationship provided that the employee is given adequate information on the manner of use of the instruments and of carrying out the checks and in compliance with the provisions of Legislative Decree no. 196 of 30 June 2003.

The processing of data in these cases must also be accompanied by an appropriate level of fairness and transparency towards the employees, who must have been adequately informed (see Art 5, para 1 (a) and arts 12, 13, 14 GDPR). To this end, in addition to following the indications contained in the provision on video surveillance of the Privacy

[45] See GPDP, Provv. No. 364, of 06 June 2024, available at <https://www.garanteprivacy.it> accessed 10 June 2024.

Authority of 08 April 2010, No. 1712680, it is also necessary to bear in mind the Guidelines No. 3/2019 of the European Data Protection Committee on the processing of personal data by means of video devices.

According to the latter, in the case of video-surveillance systems, the first-level information notice, by means of appropriate signs in the vicinity of the area concerned (purpose, data controller, data subject's rights, data retention times, data processing methods, etc.), must be accompanied by a second-level information notice, to which the first will expressly refer, so as to provide data subjects with the means of consulting the information notice in full and all the other elements indicated in Art 13 of the Regulation.[46]

The reference is therefore directed not only to the GDPR rules but also to the applicable sectoral regulations (see Art 5, para 1, (a)), so as to ensure a fair balance between the interests of the data controller and in particular the economic/organisational interests of the employer and the privacy needs of the data subject, so as not to incur abuses and so that processing is in compliance with the principle of fairness and loyalty (Art 5, para 1 (a)) as well as the conditions for the lawful use of technological tools in the work context (Art 88, para 2 GDPR).[47]

Article 88, on the one hand, did not affect the national rules of greater protection (ie the specific rules) aimed at ensuring the protection of the rights and freedoms with regard to the processing of workers' personal data, such as Art 23 of Legislative Decree No. 151/2015 (formerly article 4 of Law No. 300 of 1970), on the other hand, however, it opened up the possibility of delegating to collective agreements (including supplementary ones as it appears from Cons. 155), the regulation beyond and exceeding the distinction in paragraphs 1 and 2, provided that it is more specific and more protective for workers.[48]

The internal legislation, moreover, has been approved as a specific provision Art. 114 of Legislative Decree No. 196 of 30 June 2003, the Privacy Code, which among the conditions for the lawfulness of processing has established compliance with the provisions of Art. 4 of Law No. 300 of 1970, whereby if video surveillance systems can derive even

[46] On this point, there is a conforming orientation of the EDPB and the GPDP, mentioned in Provv. No. 5, of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 June 2024 and in case law Cass Civ [2024] No. 15391, available at <https://www.dirittoegiustizia.it> accessed 10 June 2024 whereby "*posto che il telepass installato su iniziativa datoriale sull'autovettura messa a disposizione del dipendente … consente la registrazione del transiti autostradali e che dunque, in questo modo, si può effettuare un controllo a distanza, seppure postumo, tale teorica o concreta possibilità di controllo rende utilizzabili i dati ricavati da tale strumento solo se il lavoratore è stato previamente ed adeguatamente informato delle modalità d'uso dello stesso e dell'effettuazione dei controlli nel rispetto di quanto previsto dalla normativa sulla privacy, come sancito dal comma 3, dell'Art. 4 Legge n. 300/1970*".

[47] Article 88 GDPR par 1 "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship".

[48] See Silvia Ciucciovino, 'Art. 88 commento' in Roberto D'Orazio, Giusella Finocchiaro, Oreste Pollicino and Federica Resta (eds), *Codice della privacy e data protection* (Giuffré Francis Lefebvre Press 2021) 948 ff.

only from the possibility of remote monitoring of employees they may only be used for purposes related to production and organisation, for the safety of work and the assets of the company. The relevant installation must be carried out subject to a collective agreement with the unitary or company trade union representatives or with the authorisation of the labour inspectorate, constituting a condition without which video surveillance systems cannot be installed, without running the risk of violating Art 171 of the Privacy Code.[49]

Violation of article 88 of the GDPR is, on the other hand, subject to the application of an administrative sanction under Art 83, para 5 (d).

There are, therefore, various and autonomous levels of guarantee, constituted first and foremost by the Privacy Code as well as by article 4 of Law 300/1970 (as amended by article 23 of Legislative Decree No. 151/2015) to which Art 88 refers in conjunction with arts 5 and 6 GDPR. The GDPR extends, however, bargaining with the social partners beyond and notwithstanding the differences contained in the internal regulations and with specific reference to the processing of personal data, which if pertaining to software and technological evolution, inherent in surveillance tools, is capable of favouring the storage and massive processing of data and which may concern, therefore, their use and the purposes of processing or other aspects that will be discussed in more detail below.

The distinction made in Legislative Decree No. 151/2015 allows for the expansion of a guarantor norm, which can open up interesting opportunities for protection and negotiating weapons in the hands of the worker in both the pathological and physiological phases of the employment relationship, where the guaranteed procedures, which are made safe by the GDPR, are not observed.[50]

In 2023, the European Agency for Safety and Health at Work adopted a document entitled “Automating physical tasks using AI-based systems in the workplace. Cases and recommendations”, in which, while emphasising that the use of drones in the workplace is intended to be a supportive tool for workers and for the company, capable of guaranteeing greater privacy for the former compared to traditional full-camera systems, it does not fail to recommend “the full inclusion of workers and managers in all technological implementations”, through trade unions and employers' associations. Any system that processes sensitive data should thus be accompanied, as the Agency writes, at least by Codes of Conduct. The latter, in addition to accompanying the software at the time of design and development, can also serve as guaranteed instruments at a later stage, ie, at the time of installation and use of AI systems.[51]

[49] See the extensive examination in GPDP, Provv. No. 58, of 02 March 2023, available at <https://www.garanteprivacy.it> accessed 5 November 2024.
[50] Ciucciovino (n 48) 950.
[51] European Agency for Safety and Health at Work, ‘Automating physical tasks using AI-based systems in the workplace. Cases and recommendations’ (2023), available at <https://www.osha.europa.eu> accessed 5 November 2024.

There are, in fact, situations in which drones are supplemented by thermal sensors for infrared night vision and are therefore apparently harmless to privacy, as is the case with Ikea's Verity drones, which can also be used in sectors such as agriculture and construction. In the future, these devices will be able to function completely independently and will contribute to the development of systems for the automation of physical and cognitive tasks in the workplace, with considerable impact on workers, privacy and data.

2.2 Drones and worker protections in the GDPR and the AI Act

The adoption of proactive behaviour, subsumed under the concept of diligence pursuant to arts 1218, 1176, 2087 of the Civil Code,[52] and accountability pursuant to article 24 of the GDPR, contribute to the social acceptance of these technological devices by workers, supported by the perception of the real utility and benefits that they are able to bring.[53]

The European Social Partners' Framework Agreement on Digitization of June 2020, between the European Trade Union Confederation (ETUC), Business Europe, SGI Europe and SME United, reaffirms, not incidentally, the centrality of the person at the helm of production processes and emphasises that digital systems must comply with existing law, but also with the GDPR, so as to make use of all the tools provided by the latter to respect human dignity and limit monitoring and surveillance.[54]

In artificial intelligence systems classified as high-risk, in which, drones result, the 'Human in the loop' principle, which provides for human oversight and supervision right from the design and development phase, is also guaranteed (see Art 14 AI Act).

If the principle of human oversight applies to drones, the same is not the case for the fundamental rights impact assessment under Art 27 of AI Act.

On this point, in fact, the AI Act provides for the possibility of carrying out an impact assessment of fundamental rights, but in a unilateral and compliance-oriented way, which does not seem to include drones, since Art 27 remains excluded from the regulatory perimeter of chapter III, sec II, AI Act, to which Art 108 AI Act refers. Art 2 para 2) AI Act provides, in fact, that to AI systems classified as high-risk, pursuant to Art 6, para 1, concerning “products” governed by the Union harmonisation legislation, listed in annex I, sec B, only, Art 6, para 1, articles 102 to 109, Art 57 and Art 112 apply.

In annex I, sec B, item 20 we find some areas of reference, among which Reg. (EU) 2018/1139 (Art 108 AI Act) is expressly mentioned, which refers to UAS, to be amended in Art 17, 19, 43, 47, 57, 58, in order to bring the products in line with the provisions of chapter III sec 2 of the AI Act, which requires certain conformity requirements for placing on the market or for their use.

---

[52] Regio Decreto 16 Marzo 1942 n. 262 on the approval of the Civil Code (Italy).
[53] European Agency for Safety and Health at work (n 6).
[54] The European Social Partners' Framework Agreement on Digitization available at <https://www.etuc.org/system/files/document/file2020-06/Final%2022%2006%2020_Agreement%20on%20Digitalisation%202020.pdf> accessed 5 November 2024.

These are a series of requirements to be fulfilled (Art 8), in particular, with regard to risk management (Art 9), data and data governance (Art 10), technical documentation (Art 11), transparency (Art 13), human oversight (Art 14) and IT security (Art 15).

Important remains, therefore, as a limit to the exercise of employer powers and for the purposes of assessing the risks inherent in the use of technology, the GDPR's protection system.

The reference is to the GDPR article 35 (DPIA), which remains one of the main instruments to be adopted before processing begins and which provides for the possibility of consulting data subjects and their representatives on the intended processing, in order to assess the impact of the processing in critical scenarios, such as those referred to in article 35, para 3.[55]

The DPIA under article 35 of the GDPR opens up an important dialectical opportunity with employees, not found in other disciplines.

In addition to Art 35, the GDPR has a special focus on the protection of rights contained in Art 32 on the security of processing in conjunction with Art 40 on voluntary codes of conduct, Art 25 on data protection by design and data protection by default, and certainly Art 88 GDPR.

The GDPR thus confirms itself as a regulation to ensure that even AI systems respect digital rights and workers' rights. It introduces specific rules to regulate the processing of workers' personal data in the context of work, with the burden of proof on the employer's side as to compliance and thus represents a bulwark of democracy, capable of controlling and limiting employer power, filling regulatory gaps, overcoming doctrinal and jurisprudential contrasts of national systems, such as the one concerning the interpretation and application of Art 4 of the Workers' Rights Statute, bringing back to unity and strengthening the system of protections.

In the dialectic between privacy protection and innovation, even Art 2 para 7) Artificial Intelligence Regulation expressly recognises the force attributed to the GDPR, which is considered superordinate to the former.

Art 2, para 7. of the Artificial Intelligence Regulation leaves Regulation (EU) No. 679/2016 unaffected, with the exception of Art 10 para 5 and Art 59 of the same Regulation, with the intention of introducing greater data protection measures through corrective measures and to avoid distortive effects and for the purpose of developing spaces for regulatory experimentation under Art 57, within which privacy and data are sacrificed for reasons of public interest.

[55] Art 35 paragraph 3 "A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9 (1), or of personal data relating to criminal convictions and offences referred to in Article 10; or © a systematic monitoring of a publicly accessible area on a large scale".

All of the above, together with respect for the principle of accountability, before adopting remote control tools, as well as respect for the general principles of processing (arts 5, 24 and 25 GDPR), so as to fully and exhaustively represent the processing before it begins means[56] contributing to the awareness of the data subject and to aspire to a result of reliable, person-friendly and socially accepted AI systems.

3 Drones and liability: limits of current regulation or lack of regulation?

The issue of liability is still unresolved and although the intention of the Community legislator is to develop a regulation with rules proportionate to the risk of each operation, the special rules of the Code of Navigation provide for strict liability which is mainly borne by the operator or the exerciser.

Article 874 of the Navigation Code, identifies the figure of the operator as the person who takes over the operation of the aircraft or the person responsible for events arising from the operation itself.

International regulations, on the other hand, identify the figure of the operator.

In the Riga Declaration of 06 March 2015 entitled "Framing the future aviation" it is reiterated that the "owner or operator" must always be identifiable.

Regardless of the definitions, the figures of the manager referred to in the international regulations or the operator of codified extraction, are both required to manage flight and systems activities. According to the prototypical Easa regulations, they are responsible for every aspect pertaining to the safety of the organisation, thus also for privacy, security, data collection, considered safety requirements for operations,[57] environmental protection, up to insurance obligations.[58]

This results in a very heavy liability on the part of the operator, albeit within the limits of the mandatory minimum insurance coverage.

[56] See GPDP, Provv. No. 364 of 06 June 2024, available at <www.garanteprivacy.it> accessed 10 June 2024; see also in Bolognini and Pelino (n 36) 490.

[57] See to that effect Reg. (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, Annex IX, Art 1, para 1 according to which Operators and remote pilots of unmanned aircraft are required to be familiar with national and Union rules on privacy, confidentiality protection, data protection, security, in order to ensure safe operations and separation distance between unmanned aircraft, persons on the ground and other airspace users. This provision is recalled by Recital 2 of the subsequent Delegated Regulation (EU) 945/2019 of 12 March 2019.

[58] Alpa (n 29) 921. According to the author, in the concept of indemnifiable unfair damage, interests particularly protected by law and corresponding to the most important values of society must be included: the values of the human person, on the one hand, and those of property on the other, identifiable with absolute subjective rights, which find direct recognition and protection in the Constitution. In this sense see also Amedeo Santosuosso, *Law, Science, New Technologies* (2nd edn, Wolters Kluwer 2016) 32 ff, who in citing Art 53 of the Nice Charter: Level of protection ie *"Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti … dalle Costituzioni degli stati membri; parafrasando il testo dell'articolo l'autore, dunque, afferma che in caso di contrasto tra Carta e costituzioni nazionali, non prevale la fonte astrattamente di grado superiore (e cioé la Carta), ma quella che garantisce il maggiore livello di protezione, di modo che la carta possa solo incrementare le tutele e mai limitare quelle esistenti a livello nazionale"*.

The position of the agent, if it coincides with the owner and/or responsibility of the processing, in the event of material or immaterial damage for breach of Regulation (EU) No. 679/2016 is, moreover, aggravated by further charges, pursuant to Art 82 GDPR, with the application of significant sanctions, which would seem to introduce liability for damages (material or immaterial) also by way of fault or intent (see Art 83, para 2 (b)), with reference both to the unlawful processing of data, but also and especially to the failure to adopt proactive behaviour.

In particular, the bridging rule, which allows liability profiles to be configured for the entire operation and therefore also for damage to persons and property, is that of Art 965 of the Navigation Code, and the rule generically speaks of aircraft in flight, referring to the typical scheme of strict liability.

Article 965 provides that the liability of the operator for damage caused by the aircraft to persons and property on the surface is regulated by the international rules in force in the republic, which also apply to damage caused on the national territory by aircraft registered in Italy. The same regulations also apply to State aircraft and equivalent aircraft referred to in articles 744 and 746.

We speak in a generic sense of aircraft and therefore also of UAS, and the assimilation of the latter to the category of aircraft allows the application of the code rules.

The compensation varies in relation to the weight of the aircraft (see Article 11 of the Rome Convention of 07 October 1952)[59] and thus there is a first limitation of the rule, which does not address the specific risk of the operation and clashes with other regulations, first of all with Regulation (EU) No. 1139/2018 and the subsequent implementing Regulations, but also with the AI Act itself, which intends to standardise the matter.

Even the new ENAC regulation of December 2021, which sought to align itself with European legislation, introduced three categories configured according to the hazard profiles of the operations (open, limited, certified) and the provision of specific compensation for the agent.

The weight criterion, the absence of specific risks for the purposes of commensuration of the indemnifiable damage, and the allocation of strict liability to the operator,[60] is not only inconsistent with other current legislation on the subject but is also out of time and not in line with technological development and also with the drone 2.0 strategy, which focuses on market and product development needs.

On the other hand, even in the rules of common law and specifically in the case of Art 2054 of the Civil Code (para 2), in the event of a maintenance defect or construction

[59] Convention on damage caused by foreign aircraft to third parties on the surface, signed in Rome 7 October 1952, hereafter Rome Convention.

[60] *Ceretti Vs. Crescini* [1997] Brescia Tribunal 28 July, according to which, in the event of the death of a passenger, the owner, who is not the driver of the aircraft, is not jointly and severally liable with the pilot, because aviation law does not provide for a principle such as that of article 2054 of the Civil Code, paragraph 3); the aircraft operator also lacks passive legitimacy, unless his capacity as a transport or charter company is proved.

defect, liability, although in the first instance falling entirely on the driver and jointly and severally on the owner of the vehicle, has been introduced as a residual rule, which some doctrine considers a *species* of the *genus* of corporate liability.[61]

In the case of drones, however, there may be problems introducing defective product liability to mitigate the effects of the special codicil rules, due not only to the absence of shared liability, similar to what happens in article 2054 of the Civil Code but also because the special codicil discipline prevails over all and on this point, it is necessary to reflect on the fact that the maritime sphere is the only one to have conferred a special position also on customs, which in the field under examination acquire a role equal and equal to that of ordinary laws.[62]

It follows from this that it is advisable to focus attention more on the codified rules already in force, hypothesizing an extension of them as regards the allocation of liability to various subjects in addition to the operator (who may be the owner, the person responsible for processing and not always the same as the employer), or rethinking a risk-based approach to liability, with the possible allocation of liability to various figures, such as the owner and the principal, developing specific situations on the discharge of the burden of proof as regards compliance with the techno-regulation, especially in relation to the phase prior to processing.

In summary, it is worth asking who takes the risk of dangerous operations, especially in the area of privacy and data security.

Only the operator or also the company that produced it, right down to the software designer and developer? It is also necessary to ask who is the operator in each operation and whether it coincides with the data controller and the employer.

All of the above confirms the importance of defining ex-ante the risks and making the most of what has already been established in Regulation (EU) 2018/1139 with regard to privacy and data security, which, among other things, provides for the principle of privacy by design, sharing it with the GDPR.

Another case of liability, subsumed under the heading of corporate liability, could occur in the case of the use of drones in production contexts, with infringement of the privacy and data security aspects of both the employees and the operator in charge of the mission. In such a case, the strengthening of the legislation should concern the allocation of liability to the operator, but also to the owner and the principal, identifying, on a case-by-case basis and in concrete terms, who is really the subject capable of affecting the processing of data.[63]

Transparency and the assessment and determination of risks in the case of drone operations could be based instead of adopting new rules by referring to new models, which can be tested from the sector in question, ie that of the working context.

[61] Alpa (n 29) 979 ff.
[62] Giovanna Visintini, *Nozioni giuridiche fondamentali: Diritto Privato* (Zanichelli Press 2021) 21.
[63] Ciucciovino (n 48) 955.

For the purposes of transparency and description of the context and devices used, it is also useful to resort to the voluntary codes of conduct under Art 40 of the GDPR, which would make it possible, due to their versatility, to avert the risk of technological development (which in the case of a defective product would entail penalizing consequences for injured parties due to the exemption of liability on the part of producers (see Art 118, letter e) of Legislative Decree No. 206/2005 of 06 September 2005)).

Such an instrument, especially if shared with the social partners from the outset or before treatment, would make it possible, to constantly adapt the product to the rules, map risks, including those in high-risk situations, circumvent the problem of special regulations on the one hand, while at the same time avoiding breaking the unity of the European regulatory system, especially in the area of techno-regulation, and could foster social acceptance of artificial intelligence systems, helping to mitigate strict liability, on a par with further accountability instruments.

3.1 From liability to accountability. The GDPR and the instructions supporting bargaining and consultation at the workplace

The combined provisions of articles 5 and 24 GDPR, fit right into the current European regulatory framework, which prefers an approach to the problems brought about by technological innovation, oriented towards risk rather than damage, in a dynamic of prevention rather than compensation and sanctioning. Precisely because of the speed with which the organisational and production changes linked to product manufacture occur, but also with regard to the contexts in which they are employed, the European legislator prefers to intervene at a physiological rather than pathological stage, in an attempt to avert burdensome budget items for companies and preferring to encourage, at the same time, the market needs to be linked to technological progress.

The criterion of the accountability of the data controller is understood as the one who has the capacity to determine in concrete terms the purposes and means of the processing referred to in Art 4, para 7, of the Regulation,[64] intersects with that of the employer, called upon in any case or even where it does not coincide with the owner of the processing to guarantee, on the basis of common law rules under Art 2087 of the Civil Code (which provides for a broader subjective scope than that of the GDPR), the psychophysical and moral integrity and therefore protecting the dignity of workers.[65]

The regulations referred to, one general and with a broader subjective scope providing for an obligation to protect, and the other more specific and pertaining merely to the ownership of the processing, share the principle of accountability, which is present at the organisational-managerial level, but also at the technical-operational level.

[64] ibid; see also personal data protection Authority, Provv. No. 9977020 of 11 January 2024, available at <https://www.garanteprivacy.it> accessed 10 March 2024.
[65] Alpa (n 29) 260.

The employer is called to answer if he has not taken all measures to protect the psychophysical integrity of the workers and is liable at least by way of *culpa in vigilando*, the burden of proof being solely on him. Similarly, the liability under Art 82 of the regulation, as well as that under the rules of the Navigation Code in the specific case of drones, provides for strict liability in the event that the rules of the regulation have been violated or proactive technical-organisational measures have been omitted, unless the owner proves that the damage is not attributable to him. Among the measures that help to perfect proof to the contrary, the Regulation provides for the demonstration of adherence to the codes of conduct under Art 40 or the certification mechanisms under Art 42 (Art 83, para 2 (j)). Account is also taken of the measures adopted to mitigate the damage (Art 83, para 2, (c)) and in particular of the technical and organisational measures referred to in Art 25 and Art 32 GDPR (Art 83, para 2 (d)), and this is for the purposes of the graduation of liability.

Adherence to the voluntary codes of conduct pursuant to Art 40 and recourse to the certifications pursuant to Art 42 GDPR, constitutes suitable elements for the fulfilment of the burden of proof, borne by the holder, of having complied with the obligations and measures, therefore also the proactive ones such as privacy by design, DPIA, Art 88, provided for in the GDPR.

3.2 Codes of conduct (referral)

The voluntary codes of conduct under Art 40 GDPR where adopted in production contexts, in order to have greater impact, should take into consideration, the opinion of the social partners, which is currently only envisaged as a possibility and is not mandatory (Cons. 99); by doing so they could really, constitute a hook with what is contained in Art 88 GDPR, but also in arts 25, 32 and 35.[66] Art 35 governs the data protection impact assessment and under para 8) the data controller is obliged to take codes of conduct into consideration when carrying out a DPIA, adherence to which helps to demonstrate, on the part of the controller, that appropriate solutions have been identified and implemented.

By means of the codes of conduct, the way for the adoption of proactive behaviour is reinforced and the procedure for the acquisition of informed consent by workers is also facilitated, restoring symmetry to the inequality inherent in it.

Consent is the legal basis for data processing especially where no other legal basis is provided, eg this happens in the cases already examined where the use of technology moves in a zone of uncertainty between paragraphs 1 and 2 of Art 3 of Legislative Decree No. 151/2015. In order to be free, informed, knowledgeable and above all unambiguous, it must give workers the opportunity to revoke it without prejudice, it must be subject to procedural simplification, possibly as when it was first given, traces of the consent must

[66] European Agency for Safety and Health at Work, 'Unmanned aerial vehicles: implications for occupational, safety and health. Recommendations to stakeholders' (2023), available at <https://osha.europa.eu> accessed 04 November 2023.

be kept, and it must be recorded and stored in order to trace back what and when workers consented. Consent can only be said to be free when there is real choice and, above all, control over monitoring.

For many of these aspects, codes of conduct, trade union agreements and impact assessment are appropriate instruments and strongly recommended also by the documents of the European Agency for Health and Safety at Work, in order to certify the correctness of the procedures adopted to protect privacy and for the social acceptance of complex technological systems.

The construction of a truly informed and conscious consensus on the product used in the work context, characterised by requirements of knowability, instead of unknowability, contributes to introducing elements of transparency and leads to a sharing of responsibility and widespread risk distribution for facts that affect the social sphere (such as health and safety). The latter are impossible to be taken care of solely and exclusively by the company, due to the high level of conflict they are capable of expressing and the high management costs associated with adapting to technological progress, as well as the multiplicity of regulations that accumulate different levels of liability.[67]

Transparency is an element that contributes to building a basis of trust with workers and is linked to the concept of fairness, equity and procedural fairness, as an element of rebalancing relations between the different subjectivities of the employment relationship (cf. Cons. 39 GDPR).

Managers and workers have the right to be informed about the collection and use of information concerning them and whether there are more or less hidden monitoring tools, the nature, purpose, and scope of which must be outlined. It is very important that workers, union representatives and managers know about the existence and functioning of AI and surveillance in the company.

Likewise, it is very important that there is adequate information on the use of such devices so that a clear representation of the processing carried out is provided to those concerned, before it begins and so that they are made aware of it.[68]

The high invasiveness of the processing necessarily corresponds to the timeliness of the information to the data subjects, who are asked to give their consent.

There is a thread that links procedural fairness to the knowledge and knowability of the product adopted, because only with timely knowledge is there a way to form an opinion

[67] Alpa (n 29) 950, according to which *"L'estensione della responsabilità d'impresa avanza con l'incremento della consapevolezza da parte dell'imprenditore dei suoi doveri sociali, con la composizione dei conflitti tra datori di lavoro e prestatori di lavoro, con l'acquisizione del consenso da parte dei consumatori, con la diffusione della coscienza ambientale. Aggiunge ancora l'autore Non credo sia possibile prevedere (…) una regola generale di presunzione di responsabilità; avrebbe maggior senso … la redazione di una regola generale di responsabilità per rischio, e quindi di responsabilità oggettiva. Ma si è visto che per ogni settore in cui si registrano danni derivanti dall'attività di impresa si riscontrano regole che presentano una loro peculiarità: regole che prevedono cause di esonero, ovvero prove specifiche, ovvero circoscrivono a taluni danni la responsabilità senza colpa, affidando poi al principio generale basato sulla colpa il regime ordinario di responsabilità"*.

[68] See GPDP, Provv. No. 364, of 06 June 2024, available at <www.garanteprivacy.it> accessed 10 June 2024.

in time and to give truly free and informed consent and, if necessary, exercise the right to object.[69]

Transparency, fairness, and timeliness are interlinked concepts.

Given the vulnerable position and the fragile nature of the consent expressed by workers, monitoring systems must be accompanied by a continuous discussion with the social partners and possibly shared with the workers, whose opinions should be constantly and carefully documented.

Through the codes of conduct, it is possible to identify the risks related to data processing, assess the origin, nature, likelihood, severity and the mitigation measures to be adopted, act as technical awareness-raising with regard to the regulation, determine the modalities and the concrete purpose of data collection, offer a cognitive framework of the technological products that will be used, facilitating, by anticipating it, the dissemination of knowledge of the product, so as to positively affect consent in terms of awareness, ensuring a concrete adversarial process with the interested parties.

Although not binding, moreover, once adopted they contribute to making market players trustworthy and less credible in the event of violation by customers, partners and employees, thus affecting the trust factor. Under Art 83, para 4 (c), moreover, an accredited supervisory body is subject to very heavy fines for "not having taken appropriate measures" in the event of a breach of a code of conduct by the controller or processor.

They are an additional tool to promote innovation, sustainable growth and risk minimisation, safeguarding data protection standards and customer confidence in the protection of personal data. They are an opportunity and not an end in order to concretely implement the principles of the GDPR, doing so in a shared way, to meet the needs of the market, of stakeholders, but also of employees (see also Cons. 78). Through the participation of the social partners, critical areas will in fact be highlighted and they will be able to know in advance and prepare for future bargaining topics. The contribution of technology is essential to restore value and dignity to the individual, doing so by means of the value (not necessarily the price) attributed to the data,[70] which are, finally, central to the bargaining processes between social and employer partners, not only in economic terms but also and above all in terms of improving living and working conditions as well as the overall enhancement of the discipline of Art 88 GDPR on bargaining, to be implemented in advance on the algorithm and subsequently on the data co-management.

[69] Gian Claudio Malgieri, *Vulnerability and data protection law* (Oxford University Press 2023) 38 ff, 132 ff .

[70] See also Vincenzo Ricciuto, 'Lo scambio dei dati con i contenuti e i servizi digitali: una nuova modalità di contrarre?' (2023) 1 EJPLT 20; Salvatore Orlando, 'Per un sindacato di liceità del consenso privacy' (2022) IV Diritto Persona e Mercato 527; Ilaria Amelia Caggiano, 'Il consenso al trattamento dei dati personali tra nuovo regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione' (2017) I Diritto Mercato Tecnologia 4; Francesco Gazzoni, *Manuale di diritto privato* (Edizioni Scientifiche Italiane Press 2003) 183.

4 Vulnerabilities in the GDPR and in the AI Act

The GDPR does not contain rules defining the worker as a vulnerable subject.[71] It is possible, however, to find traces of this in Cons. 43, which does not recognise consent as a valid legal prerequisite in the presence of a clear imbalance (of power) between the holder and the data subject, and in Cons. 42, which expressly mentions awareness as a requirement for the freedom of consent, placing the burden of proof on the holder to prove the formation of (valid) consent.

In the list annexed to the GPDP Order No. 467 of 11 October 2018, which in implementation of Art 35, para 4, indicates the types of processing to be subjected to the data protection impact assessment, referred to in Art 35, para 1 and Art 36, para 5, processing carried out in the context of the employment relationship, by means of technological systems, from which the possibility of remote monitoring of employees' activities is derived, is also mentioned, along with other non-occasional processing of data relating to vulnerable persons.[72]

In work contexts, there is an absence of balance and the doctrine traces the so-called vulnerabilities to relationships characterised by power asymmetry, where consent is originally flawed and not genuine.

This confirms what is already contained in WP 29, which traces vulnerability to a situation of imbalance of power or danger of high risk of harm, to fundamental rights and freedoms.

In order to bring such situations back into balance, first of all, a risk assessment of the excess of the processing is required, which can justify the limits to the freedom of the worker and the fundamental rights.

Secondly, it will be necessary to refer to other bases legitimising the processing (cf. arts 6 and 9 GDPR) or to reinforce the acquisition of consent with modalities capable of guaranteeing real and adequate information, which leaves workers free to form an opinion and possibly object to the processing, and therefore with the adoption of determined and predetermined procedures prior to the processing.

The AI Act, similarly to the GDPR, recognises without providing a definition, the vulnerabilities and takes into account the group vulnerabilities in Art 5. It therefore prohibits the placing on the market, commissioning, or use of AI that are intended to distort the behaviour of persons belonging to groups that are socially or economically disadvantaged and also prohibits the so-called social score. Art 5, para 1 (f) also prohibits the placing on the market, commissioning, and use of AI systems to infer a person's emotions in the workplace and educational establishments. In addition to prohibitions, the AI Act enhances product conformity through appropriate certification, accountability

[71] Malgieri (n 69) 87 ff, 115 ff.
[72] See in Bolognini and Pelino (n 36) 1382.

and compliance to respond to vulnerable situations. It makes accountability as objective as possible in order to protect the weakest.

The GDPR, on the other hand, responds to situations of vulnerability in two ways. The first aimed at implementing the principle of transparency (see arts 12, 13, 17), and the most important declination will be the information given to the interested parties; the second through a risk-based approach, similar to the AI act, ie with the provision of certain tools to create the conditions for transparency to be implemented.[73]

Some of these have already been examined in the course of this work and consist of the use of trade union agreements (Art 88), codes of conduct (Art 40) and DPIA (Art 35). Another very important tool is privacy by design under Art 25 GDPR, capable of guaranteeing the principle of minimisation (Art 5.1 (c) GDPR), linked to the principle of accountability and responsibility.[74]

Privacy by design not only constitutes a measure capable of exempting the data controller from liability profiles, but is also contained in the regulation on drones (EU) No. 1139/2018, which establishes the basic principles to guarantee security, privacy, and the protection of personal data, through the introduction of bureaucratic burdens, without losing sight of technological innovation in the civil aviation sector.

This regulatory framework gave rise to Regulations 945 and 947/2019, transposed by EASA and ENAC at the level of domestic law, which implemented the Aviation Strategy for Europe adopted by the Commission in 2015, which had as its objective the development of safe drone operations and legislation enabling the development of industry standards preordained for this purpose.[75]

5 Relevance of techno regulation and privacy by design for privacy and data security in regulation (EU) N. 1139/2018 and in art 25 GDPR. Juridical intersections with AI Act

The adoption of Regulation (EU) No. 1139/2018 was an important developmental moment in building a common European policy and framework on drones. It extended the scope of EU competence to all drones, without making distinctions on the basis of weight or size, as was the case in the previous regulatory framework, including the design, manufacture, maintenance, operation of propellers and engines, uninstalled parts, and equipment as well as equipment for remote control of unmanned aircraft. It contains a risk-oriented approach to all operations and by means of implementing and enforcing regulations and has sought to address the safety of operations through the use of

[73] Malgieri (n 69) 133 .
[74] On the principle of minimisation and privacy by design, see the decision of GPDP, Provv. No. 1712680 of 27 April 2010, which recommends the use of systems that are pre-set and allow anonymisation, available at <https://www.garanteprivacy.it> accessed 5 November 2024.
[75] An aviation strategy for Europe, COM. (2015) 598, available at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0207&from=EN> accessed 5 November 2024.

technology regulation, of which privacy by design is one of the most important declinations.

According to Regulation (EU) No. 1139/2018 fundamental requirement for drones is to "have the relevant specific features and functionalities that take into account the principles of privacy and data protection by design and by default" in order to "mitigate the inherent security risks to the protection of privacy to the protection of personal data, security, environment arising from their operation". So, there is an express reference to privacy by design, just as there is in Regulation (EU) No. 679/2016 (GDPR). The latter, however, cuts across all areas of technology use and therefore refers to processing whether it takes place on or off the platform. It is a regulation that aims to give citizens, in general, back control over their personal data, in a system, such as the current one, of digital and collaborative economy.

Article 2 of the GDPR is called the "material scope" and represents a novelty in the regulatory landscape because rather than distinguishing between subjective and objective scope, it takes care to specify in para. 1) that it "applies to the wholly or partially automated processing of personal data and to the non-automated processing of personal data contained in a file or intended to be contained therein".

Adhering to techno-regulation also means following the rules of privacy by design ex Art 25 and 42 GDPR, which will ensure that the dictates of the law are incorporated into the software of the robotic agent, so as to prevent unwanted acts[76] and to do so throughout the entire life cycle of the product.[77]

In the area of interest, drones, which can be likened to robots, can follow the European Commission's Robolaw Guidelines.[78] According to the dictates contained therein, certain principles such as informed consent, encryption and data access control can be integrated already at the design stage. The principle of minimisation (Art 5 GDPR) and purpose of processing may also be contained therein and continuously updated.[79]

With Commission Delegated Regulation 945 of 12 March 2019 on Unmanned Aircraft Systems and Third Country Operators of Unmanned Aircraft Systems, it is reiterated in Cons 1 and 2 that it is diriment for UAS, belonging to the open category of operations, to define, in advance, the risks arising from the operation of the devices, by referring to a framework of common and harmonised EU rules instead of referring to "classical" aeronautical compliance procedures. Cons 2 specifies that the said requirements should correspond to those in Art 55 of the Unmanned UAV Regulation No. 1139/2018, which should, in particular, take into account the specific characteristics and functionalities

[76] Merla (n 20) 44.
[77] Aude Cefaliello, Phoebe V Moore and Robert Donoghue, 'Making algorithmic management safe and healthy for workers: addressing psychosocial risks in new legal provisions' (2023) 14(2) European Labour Law Journal 117.
[78] European Commission's Robolaw Guidelines available at <https://www.robolaw.eu> accessed 10 December 2023.
[79] Merla (n 20) 35 ff. It is worth quoting the author's thought that *"il trattamento illecito dei dati personali ben può dipendere dal modo in cui il drone è stato disegnato o costruito, dalla negligenza del fornitore di connettività o di coloro i quali sviluppano determinati applicativi"*.

necessary to mitigate the risks inherent to flight safety, privacy protection, personal data protection or the environment arising from the operation of UAS.

Article 1 of the Delegated Regulation of March 2019 No. 945 provides that the Regulation is intended to establish requirements for the design and manufacture and of the additional remote identification components. For the requirements, it makes a reference to parts 1-6 of the annex, which is absorbent of the UAS remote control software devices, which according to part 6, would be those of direct remote identification.

The techno-regulation in Regulation No. 945/2019 also applies to the design, manufacture, maintenance and operation of unmanned aircraft to be understood to extend to software as well as engines and propellers. The use of terms such as "remote identification systems", would leave no room for doubt, a circumstance also confirmed by technical advice from engineers in the field.

This could also give rise to further liability profiles in the event of product malfunctioning, in addition to that of the operator, and thus configure (in the future) defective product liability hypotheses, also with reference to the violation of privacy regulations.

Assessing in advance and in a shared manner risk profiles and dangers inherent in automated activities, as required also in article 11 "Rules for the assessment of operational risks" of the subsequent Implementing Regulation (EU) No. 947/2019, concerning rules and procedures for the operation of unmanned aircraft, contributes to better delineate liability profiles and mitigate the strongly objective connotation, based on the special rules of the sector of the Navigation Code.

The regulations set out in Regulations (EU) No. 679/2016 and No. 1139/2018 also share the concept of privacy by design. The latter measure, in particular, in Art 55 refers for requirements to annex IX, for the mitigation of risks arising from security, privacy, data protection, environment, to be protected through specific purposes and characteristics by design and by default.

The Artificial Intelligence Regulation (see Art 108) amends, by supplementing it, Regulation (EU) No. 2018/1139, with the standards set out in chapter III sec. 2 of the AI Act. These rules concern high-risk systems and provide for corresponding compliance standards, which, in addition to providing for risk assessment and mitigation measures, must be designed in such a way as to ensure human oversight during their use (see Art 14).

The latter standard, although not aimed at workers, nevertheless intends to protect fundamental human rights and lays the foundation for ethically oriented robotics, which also seems to cover drones.

Considering that Art 69 of the AI Act also takes into account privacy by design and the value component of design by requiring the protection of personal data during the entire product life cycle and in a way that respects the principle of minimisation by design and by default.

In line with the considerations already made on the Artificial Intelligence Act and the vagueness of the rules on strict liability, which need to be adapted to the needs of the market and technological development, inherent in the drone sector (see also Strategy 2.0) Regulation (EU) No. 1139/2018 and the following 945 regulating the use of drones in the different flight scenarios as well as 947 on design requirements production and sale, as supplemented by the AI Act, are confirmed as essential tools to ensure the respect of fundamental rights, by means of adherence to the rules set forth in the GDPR and to continue to promote technological innovation and the market, promoted by the AI Act, which has as its legal basis arts 16 and 114 Treaty on the Functioning of the European Union.[80]

The application to drones of only the rules concerning the areas of regulatory experimentation (see Art 57 AI Act) confirms this assumption and opens up the possibility of experimental regimes, without prejudice to the application of liability rules.

5.1 Drones and sandbox. Article 57 of the AI Act

The techno-regulation, standardisation, and the product-oriented approach find a favourable scenario in the development of sandboxes, which are useful to address security problems and can remedy the rigidity of conformation, which could be a blocking factor for the development of the market and the sector.

The Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, in Art 2 para 1, classifies drones in high-risk AI systems and consequently considers only certain provisions applicable to them, the most important of which is article 57, which governs sandboxes, limited to cases in which the requirements for high-risk AI systems, pursuant to the regulation, have been incorporated in such union harmonisation legislation.

Article 3, para 55, defines "regulatory AI test space" as "a controlled framework established by a competent authority that offers providers or potential providers of AI systems the opportunity to develop, train, validate and test, where appropriate in real-life conditions, an innovative AI system, in accordance with a test space plan, for a limited period of time under regulatory supervision".

Article 3, para 54, on the other hand, defines the trial space plan, functional to the former, as a document agreed between the participating supplier and the competent authority in which the objectives, conditions, timetable, methodology and requirements for the activities carried out within the trial space are described.

They can be regarded as persuasive measures on a par with Codes of Conduct and co-regulation, whereby certification procedures are created for an early assessment of the risk brought by the technology being trialed.

[80] European Commission, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' COM(2022) 652 final, available at <https://www.ec.europa.eu> accessed 10 October 2024.

Unpublished rules are sought that are studied and tested for individual cases and considered concretely rather than abstractly, in order to arrive at new technological solutions, in which market efficiency passes through legal certainty because participation in the sandbox does not exempt participants from liability, for damage caused to third parties as a result of experimentation within it.

Pursuant to para 12, suppliers and participants of the experimentation spaces in the experimentation phase remain in any case and in fact liable under Union and national law for damages caused to third parties as a result of the experimentation taking place in the experimentation space.

Critical points of sandboxes are the indiscriminate use of personal data (see Art 54, para 1 AI Act), which, however, should not apply to drones, given the narrow scope of application of the regulation in Art 57 AI Act, and the legal and market fragmentation, with impact on product standards.[81]

The strengthening of the strict liability profiles from which the sector already suffers and which would confirm the technicality of the AI Act, oriented to product conformity rather than to better delineate liability profiles more functional to the market, are another of the critical points that characterise this legal institution.

5.2 Allocation of liability between regulatory developments and recommendations. New organisational models or new rules?

In 2019, the Commission adopted two implementing regulations.

Regulation (EU) No. 945/2019, in particular, establishes the technical requirements for unmanned aircraft, namely: product requirements for design and manufacture; obligations of economic operators importers and distributors; presumption of conformity requirement as well as type of drone whose design, manufacture and maintenance will be subject to certification; implementation of drones intended for use in the "open" category and remote identification add-ons; drone operators from third countries when conducting drone operations pursuant to the implementation Regulation (EU) No. 947/2019 within the single European sky space.

Regulation (EU) No. 947/2019, on the other hand, sets out detailed conditions for drone operations, including requirements for (remote) pilot qualification and airworthiness, risk assessment, cross-border operations, registration of the drone and its operator, competent authority.

[81] See Statement by Austria expressed at the Council's approval of the AI Act on 15 May 2024, which expresses concern about the indiscriminate use of personal data in the sandboxes provided for by the regulation, as the wording is considered vague and general and not suitable as a solid legal basis for the processing of personal data under Article 6 (1) (c) GDPR and would not comply with the principle of minimisation, as it lacks limits as to the scope of the processing and categories of personal data potentially processed available at <https://data.consilium.europa.eu> accessed 23 June 2024.

National competent authorities are required to establish and maintain registration systems for drones (whose design is subject to certification) and drone operators (whose operation may pose a risk to safety, security, privacy, and the environment).

Once again, the centrality of the operator is confirmed also for privacy and personal data protection aspects, who, under the special codified regulations, is the only responsible party.

The ENAC Reg. of 04 January 2021 referred, generically, to the GDPR for the respect of privacy (see Art 29).

The vagueness and residual nature of these regulations is mainly due to the absence of a penalty system in the event of violations, a circumstance that once again confirms the centrality and relevance of GDPR.

For privacy aspects, in particular, operators, where they operate in a specific and certified category, will be required to register and display their registration number on the UAS. The same rule is applicable in the case of open category where the weight of the UAS exceeds 25 KG or in any case if equipped with a sensor capable of detecting personal data.

Registration is an administrative procedure to which Art 14 of Regulation (EU) No. 947/2019 and 6 ENAC, link the qualification of drone operator (operator according to the aeronautical approach).

The principle of privacy by design and by security, which we find regulated both in Reg. (EU) No. 679/2016 and in Reg. (EU) No. 1139/2018, is a burden on designers and economic operators, pursuant to Reg. (EU) No. 945/2019 and which the National Authorities are obliged to verify before proceeding with the conformity certifications referred to in Reg. No. 947/2019.[82]

Both Regulations are required to comply with the provisions of Chapter III sec. 2 of the Artificial Intelligence Regulation, which provides for uniformity burdens on providers of high-risk AI systems, including drones.

The GDPR proves to be the most significant regulation in the current EU legislative landscape. In addition to prohibitions, it deals mainly with processing and provides rights for data subjects as well as duties for specific categories of persons, such as data controllers, who in the workplace do not always coincide with the person responsible for the drone operation.

With respect to processing, there are in fact in advance forms of protection based on proactive and widespread conduct and next, by means of remedies of a private,

[82] See to that effect Regulation (EU) No 679/2016 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, Art 25 and Reg. (EU) No. 1139/2018 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency [2018] OJ L212/1, Art 55 and Annex IX, Art 1.3, according to which the basic requirement for drones is "*Possedere le relative caratteristiche e funzionalità specifiche che tengano conto dei principi della riservatezza e della protezione dei dati personali fin dalla progettazione e per impostazione predefinita*".

repayment and compensatory nature,[83] with which the system intends to remedy unlawful processing under articles 82 and 83. The latter article inserts a fault-based liability, also based on the failure to adopt measures, such as privacy by design, the presence of which in some cases excludes liability (see Art 82, para 2) in others limits liability (see Art 83, para 2 (d and j)).

5.3 Codes of conduct and bargaining as functional tolls for consensus building, implementation of transparency and risk mitigation

The 2015 Riga Declaration on Drones had raised the issue of insurance, liability and compensation schemes for victims, affirming the need to develop norms inherent to technologies and standards capable of ensuring the integration of drones in the airspace. The voluntary codes of conduct under Art 40 of Regulation (EU) No. 679/2016, could help in the elaboration and configuration, concretely and in advance, of risk situations. The compulsory consultation of social partners and stakeholders, currently provided for only on an optional basis, could be the condition to make this tool truly effective for privacy protection purposes and beyond.[84]

Not only would transparency be enhanced, but also the acquisition of consent [85] would be truly informed, free, responsible and aware,[86] becoming a true and proper act of manifestation of will, from which to start evaluating the lawfulness of processing,[87] instead of being limited to a merely authorizing scheme.[88]

The codes of conduct under article 40 GDPR, are confirmed as useful, versatile and authoritative self-regulatory instruments due to their legitimacy at the public level (i.e., the approval of Public Supervisory Authorities, under Art 55 Reg. (EU) No. 679/2016 and Cons. 122). They allow for the introduction of compulsory consultation of the social partners and lend themselves to regulate any situation involving the use of technologies, including high-risk technologies, such as may be those related to data processing in production contexts. Once developed and approved, they can be used by suppliers to demonstrate compliance with the obligations brought by the GDPR, including for the

[83] Lucilla Gatt, Roberto Montanari and Ilaria Amelia Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del diritto 351.

[84] See to that effect Regulation (EU) No. 679/2016 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC [2016] OJ L119/1, Considering Art 99, which employs the verb "*Dovrebbero*" in relation to consultation by data controllers, of data subjects, when drafting, amending and extending Codes of Conduct.

[85] Federica Paolucci, "Consenso, intelligenza artificiale e privacy. Commento a: Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381" (2021) 1 MediaLaws <https://www.medialaws.eu/consenso-intelligenza-artificiale-e-privacy-commento-a-corte-di-cassazione-sez-i-civ-25-05-2021-n-14381/> accessed 25 October 2024.

[86] A Davola, 'L'acquisizione di dati da parte dei privati nelle operazioni con SAPR' in Erica Palmerini, Maria Angela Biasotti and Giuseppe Francesco Aiello (eds), *Diritto dei droni. Regole, questioni e prassi* (Milano 2018) 149.

[87] Orlando (n 70) 527.

[88] *Movimento Federativo Democratico Vs. Associazione Bancaria Italiana Banca Popolare Coop.a ARL Banca Fideuram Spa* [2000] Rome Tribunal available in Corriere Giuridico 00 496, mentioned in Gazzoni n 70 183.

purposes of discharging the burden of proof in the event of damages for breach of privacy and data breaches.[89]

Where there are data protection impact assessments to be carried out pursuant to Art 35 GDPR, as in the case of the use of artificial intelligence and particularly innovative and pervasive technologies, such as drones, with enormous potential, in future scenarios, in terms of surveillance, predictive analysis, profiling[90] and assessment of the individual, up to more sophisticated forms of monitoring inherent in automated processing, the adoption of the code of conduct (Art 35, para 8), will help to make the product more knowable and understandable and thus may have a positive impact on transparency.[91]

The codes of conduct in Art. 40 GDPR, unlike those in the AI Act (see Art 95), do not provide for the limitation of adoptability in low-risk situations and are therefore of wider application, ie in situations characterised by the use of technology, in general.

Also the Recommendation CM/Rec (2015) 5 of 1 April 2015, of the Committee of Ministers to Member States on the processing of personal data in the employment context, urges to bear in mind principles such as data protection and respect for private life and to "promote the acceptance and application of the principles set out in the appendix of the soft law document, through supplementary instruments such as codes of conduct so as to ensure that these principles are known, understood and applied by all persons in the employment sphere, including employers' and employees' representative bodies, and that they are taken into account in the design and use of ICT in the employment sphere".

The agreements with the social partners under Art 88 of the GDPR confirm this last meaning and are therefore suitable for defining the framework and the protection of fundamental rights, to safeguard the individual, through the negotiation carried out *ex ante* and *ex post*, i.e. in terms of bargaining on the constitutional values that regulate the algorithm and in terms of data co-management (determination of the purpose of processing, access, portability, transfer, modification and revocation of consent, right to rectification and control of data accuracy). The latter, above all, will be of great importance in very specific situations such as, for instance, the filming of workers for company promotional and advertising purposes.

Bargaining understood in this way will be able to have a significant impact on the quality of life of workers, impacting on working time and working hours in the company for example (so-called work life balance), and on the improvement of working conditions in a broader sense.[92]

[89] European Commission, 'New Rules for Artificial Intelligence - Questions and Answers' (2024), available at <https://commission.europa.eu> accessed 02 January 2024.
[90] Guido Noto La Diega, 'Machine rules. Of Drones, Robots and the info-Capitalist Society' (2016) 2 The Italian law Journal 401.
[91] *Filcams Cgil Torino Filt Cgil Torino Ndil Cgil Torino Vs. F.S.R.L.* [2023] Turin Tribunal 05 August, 6.
[92] Alessia Maccaferri, 'Sostenibilità, al centro la qualità della vita e del lavoro' *Il Sole 24 Ore* (25 February 2024) 20. According to the author, sustainability is increasingly understood as quality of life and work, and 89% of companies are increasingly interested in social sustainability, first and foremost internally, by committing themselves to improving the quality of life and work of their employees.

This, among other things, will be instrumental in overcoming the typically contractual scheme, based on the exchange and price of data, understood as goods to be regulated.[93]

Consent thus understood will not be ascribable to an act of private autonomy, but not even to a mere acknowledgement, but will be a truly free authorisation, because it will be conscious and informed, aimed at obtaining control over data and benefits not strictly related to economic value, the use of which will be the employer's responsibility in terms of accountability. This will allow for a balancing of interests, such as that (but not only) of profit-sharing for those concerned, allocating precise liabilities to the parties, mainly employers.[94]

The European Social Partners' Framework Agreement on Digitisation, while affirming the validity of technology in the company to guarantee and protect the health and safety of the working environment and workers, at the same time, reaffirms that the dignity of the human being, which could be violated when subjected to surveillance or performance monitoring systems, must be safeguarded, expressly mentioning collective agreements as the appropriate instruments to implement Art 88 GDPR, so as to enable workers' representatives to address data, consent, privacy and surveillance issues.

To this end, it will be important to link the collection of data to a concrete and transparent purpose that is, above all, current and not generically determinable in the future.

6 Conclusions

There is a unifying legislation on drones at EU level, contained in the aforementioned regulations, extensively commented on in the previous section.

The international discipline assimilates and conforms under the regime of special provisions, aircraft and drones in an all-encompassing manner; the intersections with other regulations have been examined, and at the same time, thanks to the contribution of Regulation (EU) No. 1139/2018, the need to rethink a risk-based approach has been raised, in order to configure liability cases also with regard to privacy and data security.

The current legislation has a number of limitations, including an excessive concentration of liability entirely on the operator, especially in the case of drones used for civil purposes, the extent of the damage commensurate with the weight and not with the concrete risks related to the operation, and therefore not in line with current market development needs; lastly, the legislation is generic in terms of privacy and acquisition of consent, and lacks a sanctioning apparatus, with respect to which reference should be made to the GDPR and the AI Act, limited to suppliers for high-risk artificial intelligence

[93] Salvatore Orlando, 'Il Coordinamento tra la Direttiva 2019/770 e il GDPR. L'interessato consumatore' (2023) II Persona e Mercato 232.
[94] Alessio Gramolati, *Contrattare l'innovazione digitale, Una cassetta degli attrezzi 4.0* (Ediesse S.r.l. Press 2019).

systems. In production contexts, where drones are mostly work tools, problems arise with regard to the allocation of liability on different subjects and not only on the operator and therefore also on the principal, who does not always coincide with the data controller and the owner

The employer is called upon, however, to answer, pursuant to Art 2087 of the Civil Code to the workers and is therefore obliged even before the start of processing to follow the principles of accountability and compliance, of privacy by design, resorting to advance consultation and negotiation, so as to do everything possible to guarantee the rights of the persons concerned.

The concept of privacy by design is a widespread aspect in all the disciplines examined and constitutes one of the most evolved aspects of the design of AI systems, beyond techno regulation. It is supposed to be shared with software developers and manufacturers, but also with suppliers, as is the case in high-risk AI systems.

It takes place before processing. Therefore, it must be promoted by data controllers and processors, but already at an earlier stage, and therefore necessarily also involves software developers and designers, making use of the GDPR's support tools, such as impact assessment, to incorporate certain constitutional and treaty values, such as those of privacy, data protection, non-discrimination, and transparency, within and from the outset.[95]

This reading is confirmed by Art 2 of GDPR called “material scope”, which seems to introduce a diffuse type of liability, ascribable to a very broad scope within which the concept of 'processing' also falls.

For this purpose, the importance of the techno-regulation present in all the disciplines referred to, from the GDPR to the regulations standardizing the matter up to the AI Act, which confirm the importance of the accountability dimension in a system centred on a strict liability. This absolute dimension of liability also reaffirmed in Art 57 of the AI Act on the spaces for regulatory experimentation, which strongly inhibits the market and is not able to respond incisively, like the GDPR, to situations of vulnerability, such as those concerning the protection of workers' data and privacy.

It is the company's burden, moreover, to demonstrate that it has taken all the measures set out in the GDPR when processing workers' data by means of the technology used in the company, and it will therefore be in the company's interest to demonstrate that it has adopted the proactive behaviours set out therein and the risk mitigation measures. The latter are to be found in Cons. 71 (processing accompanied by appropriate safeguards such as information, right to human intervention, prohibition of automated processing, expressing one's opinion and guaranteeing an adversarial process, right to an explanation, right to challenge, appropriate mathematical or statistical procedures for profiling, technical and organisational measures for correcting data inaccuracies, minimizing the

[95] Orlando (n 70) 538.

risk of errors, avoiding discriminatory decisions), in Cons. 78 for privacy by design, in Cons. 77 for codes of conduct, which, together with the agreements with the social partners under Art 88, contribute to the acquisition of consent, by means of procedural models appropriate to the risk.

Art 88 of the GDPR while respecting the guarantee rules of the domestic legal system and collective agreements such as Art 4 of the Statute of Workers' Rights, intends, with a forward-looking and forward-looking approach, to regulate the purpose of the collection and the use that will be made of the data, through unprecedented technological systems, seeking to avoid discrimination and violations of privacy and the identity of the worker from the outset.[96]

We can then understand why it is necessary to guarantee the knowledge and knowability of the algorithm, as well as the importance of recognising and incorporating constitutional values immediately from the design stage, that is, from the moment when the algorithms are put into the system and the data that qualitatively meet certain characteristics are chosen, in order to make the predictive and surveillance systems work, both on the platform (by means of automated processing and profiling) and off, as in the case of drones and artificial intelligence surveillance systems in general.

One therefore grasps the importance not only of the codes of conduct ex Art. 40 GDPR and the DPIA, but also of the collective bargains ex Art 88 GDPR, both in terms of algorithm bargaining and in terms of data co-management, and thus the importance of bargaining both in advance and next and during the entire product life cycle.

With the advancement of technological equipment and telematic resources that broaden the possibility of control over the worker, which can also take place by computer, national regulations must be adapted. Article 88, para 1, responds to this need and delegates to collective bargains the possibility of introducing bargaining aimed precisely at work organisation, management and planning. Para 2 further specifies that such agreements will be adopted to ensure transparency of processing, protection of dignity, where there are data transfers and in the case of the adoption of workplace monitoring systems.

The contribution of technology will have a significant impact on the bargaining of the future, increasingly focused, in the writer's humble opinion, on time and space at work, with relevant benefits for workers' freedom, quality of work and work-life balance, beyond and despite the pervasiveness of surveillance.

The adoption of new regulatory models will serve to re-establish fairness and restore symmetry to relations, together with the identification of higher legitimate interests, such as those of health protection, which alone can justify the use of invasive technologies and data processing, but which can become an easy pretext for improper and instrumental use against objectively weaker and more vulnerable subjects, such as workers.

[96] Santosuosso (n 58) 346 ff.

One understands, therefore, the reason why the Artificial Intelligence Regulation has re-proposed privacy by design and compliance, including drones among the high-risk systems, and has provided for the standardisation of regulations for them to bring them into line with the main rules concerning them, first and foremost the principle of human oversight.

Giulio Cotogni *

GENERAL SECTION

THE EXPLAINABILITY OF AUTOMATED DECISION-MAKING: A HISTORICAL PERSPECTIVE THROUGH EU LEGISLATION

Abstract

There has been much discussion about the existence of a right to explanation of automated decision-making (ADM) in the General Data Protection Regulation (GDPR). However, little attention has been given to the evolution of the regulation of ADM, within the European Union, over the past thirty years. This paper aims to fill this gap in the literature, providing the reader with a look at this topic through the lens of a historical perspective, starting from the very first regulation of ADM in the Data Protection Directive, continuing with the GDPR and, finally, analysing how the right to explanation has ultimately been established in the Artificial Intelligence Act. We will also see how the EU has addressed the issue of transparency and explainability of ADM in other recent pieces of legislation (the 2019 reform of the EU consumer protection law, the Digital Services Act and the Platform Work Directive). Starting from this historical reconstruction of the EU regulation, a common thread will be identified: the tendency to impose increasingly stringent rules regarding the transparency and explainability of ADM. Lastly, three possible explanations for this regulatory development will be proposed.

JEL CLASSIFICATION: K10, K30, K38

SUMMARY

* Graduate in law from the University of Turin, Email: giulio.cotogni@edu.unito.it.

DOI 1.13135/2785-7867/11339

1 Introduction

The enormous amount of data available that characterises today's society[1], combined with the increase in computing capacity over the last thirty years[2], now allows Artificial Intelligence (AI) systems, especially those that exploit machine learning (ML) techniques, to render opinions, provide answers, and make decisions very quickly and accurately. Therefore, in many sectors, these systems are increasingly helping[3] (or replacing) humans, especially when it comes to making decisions. This process is called automated decision-making (ADM). This term refers to any process that allows, through the use of technological tools, to make decisions without, or at least with minimal human involvement[4]. Although ADM do not necessarily involve the use of AI technologies, most automated decisions today are made by AI systems.

Although these systems can be a booster for human prosperity, they don't come without risks[5]. In fact, it has been shown that the outputs produced by AI systems can be biased[6], erroneous[7], discriminatory[8] and can violate our privacy[9].

---

[1] See 'Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020' (*Statista*, 2024) <https://www.statista.com/statistics/871513/worldwide-data-created/> accessed 13 November 2024.
Camilla Tabarrini, 'Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?' (2019) 2 Il diritto dell informazione e dell informatica 555, argues that the growth in the amount of available data is mainly due to the so-called "user-generated content" and the Internet of Things (IOT).

[2] See 'Computational capacity of the fastest supercomputers' (*OurWorldinData*, 2023) <https://ourworldindata.org/grapher/supercomputer-power-flops> accessed 13 November 2024.

[3] '[Artificial Intelligence] will change our lives by improving healthcare (eg making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine'. See 'White Paper on Artificial Intelligence - A European approach to excellence and trust', COM(2020) 65 final 19 February 2020 1.

[4] Emiliano Troisi, 'Decisione algoritmica, Black box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione' (2022) 4 Juscivile 953.

[5] 'At the same time, Artificial Intelligence entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes', see White Paper on Artificial Intelligence (n 3) 1.

[6] Such bias stem mainly from the quality and choice of data with which the algorithms are trained. Kate Crawford, 'The Hidden Biases in Big Data' *Harvard Business Review* (1 April 2013) <https://hbr.org/2013/04/the-hidden-biases-in-big-data> accessed 13 November 2024, points out that 'Data and data sets are not objective; they are creations of human design. We give numbers their voice, draw inferences from them, and define their meaning through our interpretations. Hidden biases in both the collection and analysis stages present considerable risks, and are as important to the big-data equation as the numbers themselves'.

[7] For example, it has been shown that it is possible to induce the detection system of a self-driving car to misperceive a traffic signal, leading it to confuse a stop sign with a speed limit. See Kevin Eykholt and others, 'Robust Physical-World Attacks on Deep Learning Models' [2018] ArXiv <https://arxiv.org/abs/1707.08945> accessed 13 November 2024.

[8] Among the most famous cases is the case of COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), an algorithm used by several US states since 2001 as a tool for judges to assess the risk of recidivism of convicted offenders and which proved, all things being equal, to discriminate against African-American criminals, predicting a higher recidivism risk for them than for white offenders, precisely because it was trained on a set of precedents that reflected this discrimination (i.e. on a set of precedents in which African-American offenders actually had a higher recidivism rate than white offenders). See Ellora T Israni, 'When an Algorithm Helps Send You to Prison' (*The New York Times*, 26 October 2017) <https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html> accessed 13 November 2024.

[9] A famous example of this mechanism is the case of an algorithm used by the Target supermarket chain, which, on the basis of the purchases made by a girl (who was, moreover, underage), correctly predicted that she was pregnant (before

Finally, AI systems suffer from an additional problem, namely that of *opacity*[10]. This term refers to the fact that, especially with regard to more sophisticated systems, it is increasingly complex for human operators to understand *how* and *why* the software has produced a certain output. To refer to these opaque systems, the term "black boxes" has been coined in the literature[11], ie systems in which "the computing operations of algorithmic systems [...] become too complex or intricate to comprehend"[12] and therefore "we can observe its inputs and outputs, but we cannot tell how one becomes the other"[13]. The problem posed by these black boxes is all the greater in the light of what has been said above: if the outputs produced by these systems are anything but objective and infallible, but, on the contrary, can be biased, erroneous and discriminatory, then the claim to make these instruments more transparent and, therefore, to obtain an explanation for their output, appears all the more legitimate.

Furthermore, the phenomenon of black boxes entails a further significant critical issue: by hindering the transparency of the various stages of the procedure, and thus compromising the possibility of verifying the validity of the reasons supporting the decision taken, black boxes pose a major obstacle to the full legitimation of the use of automated decisions and, more generally, undermines citizens' trust in AI technologies[14]. Consequently, recent years have seen the proliferation of ethical charters, guidelines and recommendations worldwide, reflecting the growing demand for greater transparency and explainability of AI systems and ADM[15]. For example, at the EU level, the Recommendation on the human rights impacts of algorithmic systems states that "[t]he use of algorithmic systems in decision-making processes that carry high risks to human rights should be

her parents even knew) and sent her vouchers for baby products. See Kashmir Hill, 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did' (*Forbes*, 11 August 2022) <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/> accessed 13 November 2024.

[10] Opacity seems to be at the very heart of new concerns about 'algorithms' (operating on data) among legal scholars and social scientists", Jenna Burrell, 'How the machine 'thinks': Understanding opacity in machine learning algorithms' (2016) 3(1) Big Data & Society 1.

[11] The term was coined by Frank Pasquale, '*The Black Box Society. The Secret Algorithms That Control Money and Information*' (Harvard University Press 2015). According to the Author, the black box metaphor correctly represents contemporary reality, in which people are increasingly controlled and surveilled by private corporations and governments, but are unaware of how information and data concerning their lives are disclosed and used by these entities.

[12] Sylvia Lu, 'Data Privacy, Human Rights, and Algorithmic Opacity' (2023) 110 California Law Review 2098.

[13] See Pasquale (n 11) 3.

[14] Carlo Casonato and Barbara Marchetti, 'Prime osservazioni sulla proposta di regolamento dell Unione Europea in materia di intelligenza artificiale' (2021) 3 BioLaw Journal – Rivista di BioDiritto 427.

[15] An interesting, albeit now quite dated, research of 2019, identified 84 documents globally containing ethical principles and guidelines on AI. Analyzing these documents, eleven general principles appear to emerge: transparency, justice and fairness, non-maleficence, responsibility and accountability, privacy, beneficence, freedom and autonomy, trust, dignity, sustainability, and solidarity. Among these, although there is not one mentioned explicitly in all the documents, the one most referred to is the principle of transparency (found in as many as 73 documents), which is declined precisely in terms of "explainability". See Anna Jobin, Marcello Ienca and Effy Vayena, 'The global landscape of AI ethics guidelines' (2019) 1 Nature Machine Intelligence 389. The same conclusions are reached by Jessica Fjeld and others, 'Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center Research Publication 2020) 1.

subject to particularly high standards as regards the explainability of processes and outputs"[16] and "[a]ffected individuals and groups should be afforded effective means to contest relevant determinations and decisions. As a necessary precondition, the existence, process, rationale, reasoning and possible outcome of algorithmic systems at individual and collective levels should be explained"[17]. The principle of explicability is also affirmed in the Ethics Guidelines for Trustworthy AI, formulated by the High Level Expert Group on Artificial Intelligence, where it is said that "[e]xplicability is crucial for building and maintaining users' trust in AI systems. This means that processes need to be transparent […] and decisions […] explainable to those directly and indirectly affected"[18].

The possible risks posed by automated decisions, have created a debate about the need for a new right: on the assumption that, except in cases provided by law, a decision made by a human being does not give rise in the person concerned to a right to an explanation of the decision, the question was raised whether, if the decision is instead made by an algorithm, it is necessary to configure in the person concerned a *right to explanation*[19].

This paper examines the EU regulation of automated decisions and is structured as follows. Sections 2-3 look at EU regulation of automated decisions from a historical perspective, starting with the very first regulation of the subject with the Data Protection Directive (DPD), continuing with the General Data Protection Regulation (GDPR), and ending with the recent Artificial Intelligence Act (AI Act). Section 4 shows how transparency and explainability of automated decisions have also made their way into specific areas of EU legislation. Section 5 highlights what, in the writer's opinion, is the common thread that has characterised the evolution of EU regulation. Section 6 proposes three possible explanations of this thread. Finally, in Section 7, some conclusions are drawn.

[16] Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems CM/Rec(2020)1, 8 April 2020, para 4.1.

[17] ibid para 4.3.

[18] 'Ethics Guidelines for Trustworthy AI', 8 April 2019, 13. See, also, para 1.4., where it is stated that "Explainability concerns the ability to explain both the technical processes of an AI system and the related human decisions […] technical explainability requires that the decisions made by an AI system can be understood and traced by human beings. […] Whenever an AI system has a significant impact on people s lives, it should be possible to demand a suitable explanation of the AI system s decision-making process. Such explanation should be timely and adapted to the expertise of the stakeholder concerned (eg layperson, regulator or researcher). In addition, explanations of the degree to which an AI system influences and shapes the organisational decision-making process, design choices of the system, and the rationale for deploying it, should be available".
See also the OECD AI Policy Observatory definition of the principle of transparency and explainability: OECD, 'Recommendation of the Council on Artificial Intelligence' (2024), available at <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 15 October 2024 and, on the same topic, the UNESCO 'Recommendation on the Ethics of Artificial Intelligence' (*UNESCO*, 23 November 2021) <https://unesdoc.unesco.org/ark:/48223/pf0000381137> accessed 16 November 2024, (III) para 40.

[19] Jacopo Dirutigliano, 'Trasparenza a spiegabilità degli algoritmi' in Ugo Pagallo and Massimo Durante (eds), *La politica dei dati* (Mimesis edizioni 2022) 282.

2 The evolution of ADM regulation from the Data Protection Directive to the General Data Protection Regulation

The decision to analyse the DPD and the GDPR together derives from two reasons. First, the GDPR stands as the successor to the Directive in the field of personal data protection, since, with its entry into force in May 2018, it repealed the latter. Second, Article 15 of the DPD, which first regulated the topic of automated decisions, is taken up almost identically by Article 22 of the GDPR. The structure of the two Articles is, in fact, very similar: both enshrine the right of the individual not to be subjected to automated decisions[20], both provide for exceptions to this prohibition in specific cases[21] and both, in such cases, provide a number of safeguards for the person subjected to ADM.

Although Article 22 GDPR has not much changed from Article 15 of the DPD, a few changes are still noteworthy and, moreover, the practical importance of the provision has increased with augmented use of ADM in our society.

Firstly, although both mention, in the same words, "the right not to be subject to a decision", this "right" has been interpreted in two different ways[22]: whereas in the DPD it was considered to all intents and purposes a right, so that the person unfairly subjected to an automated decision has the burden of exercising it[23], in the GDPR, on the other hand, it is not a right, but a literal prohibition, so it is not necessary for the person concerned to take action[24].

[20] Article 15(1) states that 'Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.' Article 22(1) states that 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.

[21] Article 22(2) states that paragraph 1 shall not apply if the decision (a) is necessary for a contract between the data subject and a data controller; (b) is authorised by Union or Member State law; (c) is based on the data subject's explicit consent.
Article 15(2) allows derogations from paragraph 1 if the decision (a) is necessary for a contract, requested by the data subject, between the data subject and a data controller; (b) is authorised by a law.

[22] This divergence in interpretation is partly the result of the different regulatory nature of the two acts. In the case of the GDPR, in fact, the choice of the regulatory source instead of the directive entails the creation of uniform constraints that are directly applicable throughout the entire territory of the EU and removes from the Member States those margins of discretion that instead characterised the interpretation of the DPD and that most likely weakened it. See Barbara Marchetti and Leonardo Parona, 'La regolazione dell'Intelligenza Artificiale: Stati Uniti e Unione Europea alla ricerca di un possibile equilibrio' (2022) 51(1) DPCE online 237.

[23] Lee A Bygrave Dr., 'Minding the machine: Article 15 of the EC Data Protection Directive and automated profiling' (2001) 17(1) Computer Law & Security Report 17, 18 'Article 15(1) does not take the form of a direct prohibition on a particular type of decision making (profile application). Rather it directs each EU Member State to confer on persons a right to prevent them being subjected to such decision making [...]. This would leave the actual exercise of the right to the discretion of each person'.

[24] As clarified by the Court of Justice of the European Union (CJEU) in the 'SCHUFA case' (Case C-634/21 *OQ v Land Hessen* [2023] ECLI:EU:C:2023:957), para 52: 'Article 22(1) of the GDPR confers on the data subject the 'right' not to be the subject of a decision solely based on automated processing, including profiling. That provision lays down a prohibition in principle, the infringement of which does not need to be invoked individually by such a person'.
See also Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' (2019) 27(2) International Journal of Law and Information Technology 91, 99 where it is stated

Secondly, in the GDPR, explicit consent is included as a case in which ADM is allowed[25] and, finally, as opposed to the provisions in Article 15 of the directive, it is no longer necessary that the data subject requests the contract in order for the automated decision to be lawful[26].

However, the key distinction between the two provisions lies in the safeguards afforded to the person subjected to an automated decision, which, as has already been said, is admissible only when one of the exceptions outlined in Article 22(2) of the GDPR or Article 15(2) of the DPD applies.

Under the DPD, the only safeguard available to the person subjected to an automated decision, is the opportunity to "put his point of view", enshrined in Article 15. This provision is linked to Article 12 (right of access) which provides for the right to obtain from the controller: "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)".

In the GDPR, on the other hand, the rules dealing with the accountability of automated decisions are more numerous and are contained in Articles 13, 14, 15, 22(3) and Recital 71. All together, these provisions put in place "a broader, stronger, and deeper algorithmic accountability regime than what existed under the EU's Data Protection Directive"[27]. Article 22(3) of the GDPR, in fact, in addition to the right to express his or her point of view" (similar to the possibility to put his point of view" enshrined in Article 15 DPD), also guarantees the right to obtain human intervention on the part of the controller" and, above all, to contest the decision".

Articles 13(2)(f) and 14(2)(g) establish the data subject's right to be informed, while Article 15(1)(h) guarantees the data subject's right of access. All three provisions, with identical wording, require the data controller to provide the data subject with a range of information, including the existence of an ADM under Article 22 and, at least in those cases, "meaningful information about the logic involved" and "the significance and the envisaged consequences" of the decisions. In the GDPR, unlike the DPD, there is the addition of the term "meaningful", which means that the controller should convey information about the rationale and the criteria relied upon in reaching the decision,

---

that 'Interpreting Article 22(1) as giving data subject the right that she has to actively exercise could in consequence lead to detrimental effects for her and run contrary to the purpose of this provision […]. A systematic interpretation of Article 22 implies that only automated decisions fulfilling the requirements of paragraph 2 and allowing for safeguards from paragraph 3 of this provision are authorised by the GDPR. Therefore, […] it is more appropriate to construct the data subjects' 'right' as a prohibition of fully automated decision-making that the data controllers have to comply with'. This position is also confirmed by the EC 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP29 Guidelines), 22 August 2018, 20, where it is stated that Article 22(1) 'establishes a general prohibition' of automated decision-making meaning that 'individuals are automatically protected from the potential effects this type of processing may have'.

[25] See Article 22(2) GDPR (n 21).

[26] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7(2) International Data Privacy Law 76, 82.

[27] Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34(1) Berkeley Technology Law Journal 190, 193.

therefore the quality of being "meaningful" must be evaluated from the perspective of the data subject[28]. In order to make this information meaningful and understandable, the Guidelines on Automated individual decision-making and Profiling, drawn up by the Article 29 Working Party (WP29 Guidelines), state that "real, tangible examples of the type of possible effects should be given"[29]. The reference to the "significance" and the "envisaged consequences" of the decision refer back to the idea that, for the purposes of contestation (Article 22), it is essential to fully understand the concrete results and the risks emanating from the contextual use of the data[30]. In fact, the WP29 Guidelines clarify that "[t]he data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis"[31].

Lastly, Recital 71 takes over the content of Article 22(3) and, although it has no legal effect[32], constitutes the only provision in which the Regulation expressly mentions the term *explanation*: in fact, the Recital states that "In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision".

While it is common ground that Article 15 of the DPD did not enshrine any right to an explanation of automated decisions, the existence of such a right in the GDPR, on the other hand, has been the subject of a lengthy debate in the doctrine, between those who, on the one hand consider that the GDPR enshrines a genuine right to an explanation of the specific decision[33] and those who, on the other hand, argue for the existence of a much more limited "right to be informed"[34].

Regardless of this debate, the regulation certainly makes some important steps forward with respect to the discipline contained in the DPD on ADM accountability regime[35]: as

[28] Emre Bayamlıoglu, 'The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called right to explanation"' (2022) 16(4) Regulation & Governance 1058, 1067.
[29] WP29 Guidelines 26.
[30] See Bayamlıoglu (n 28) 1067.
[31] WP29 Guidelines 27.
[32] CJEU in Case C-355/95 *P Textilwerke Deggendorf GmbH (TWD) v Commission of the European Communities and Federal Republic of Germany* [1997] ECLI:EU:C:1997:241, para 21 states that 'the operative part of an act is indissociably linked to the statement of reasons for it, so that, when it has to be interpreted, account must be taken of the reasons which led to its adoption'.
[33] See Troisi (n 4); Emiliano Troisi, 'AI e GDPR: L'automated decision making, la protezione dei dati e il diritto alla "intelligibilità" dell'algoritmo' (2019) 1 European Journal of Privacy Law & Technologies 41; Gianclaudio Malgieri and Giovanni Comandè, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(4) International Data Privacy Law 243; Bryce Goodman and Seth Flaxman, 'European Union regulations on algorithmic decision-making and a right to explanation' (2017) 38(3) AI Magazine 50.
[34] Sandra Wachter and others (n 26); Lilian Edwards and Michael Veale, 'Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for' (2017) 16(1) Duke Law & Technology Review 18.
[35] About GDPR, Kaminski (n 27) 208, states that "[...] this regime, if enforced, has the potential to be a sea change in how algorithmic decision-making is regulated in the EU". About the DPD, Lee A Bygrave Dr. (n 23) 21 says that the right in Article 15(1) "resembles a house of cards [which], in the context of currently common data-processing practices, […] is quite easy to topple'. Interestingly, he also notes

already mentioned, the DPD simply configured the right to obtain "knowledge of the logic involved in any automatic processing of data" and the right to "put his point of view", whereas GDPR instead provides the data subject with three stronger tools: the right to obtain human intervention, the right to contest the decision and the right to obtain meaningful information.

Despite this, the GDPR has proven insufficient to fully ensure the explainability of automated decisions. Two main criticisms have been made. First, the regulation, does not elaborate much beyond suggesting the existence (never established by the CJEU case law) of a right to an explanation of automated decisions[36]. Moreover, the practical relevance of such a right has been almost meaningless, given the absence of litigation on the merits. Second, the scope of Article 22 is rather limited, since, for a decision made by automated means to fall under it, it must be based *solely* on automated processing (including profiling): hence, all those decision-making processes in which there is human intervention, albeit minimal, remain excluded from the scope of Article 22[37] and, therefore, from access to the guarantees offered by the GDPR. Moreover, as pointed out in doctrine[38], also the requirement that the decision produces "legal effects" on the individual or affects him or her "in a similar significant way" poses some interpretive problems that contribute to undermining the scope of the provision[39].

3 The right to explanation in the Artificial Intelligence Act

The AI Act explicitly recognises, for the first time in EU legislation, the existence of a right to an explanation of automated decisions.

Paragraph 1 of Article 86 states that any affected person subject to a decision which is taken by the deployer "on the basis of the output from a high-risk AI system" and which "produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights" has the

that: 'Nevertheless, this situation might well change in the future if, as is likely, automated profiling becomes more extensive".

[36] Themistoklis Tzimas, 'Algorithmic Transparency and Explainability under EU Law' (2023) 29(4) European Public Law 385, 400.

[37] Sandra Wachter and others (n 26). Other Authors, on the other hand, have preferred a broader interpretation of this requirement, deeming included in the definition all those decisions that are 'automated in substance', that is, those in which human intervention, while present, is essentially irrelevant in determining the final decision, see Emiliano Troisi, 'AI e GDPR: L'automated decision making, la protezione dei dati e il diritto alla "intelligibilità" dell'algoritmo' (2019) 1 European Journal of Privacy Law & Technologies 41, 47; Iole Pia Di Ciommo, 'La prospettiva del controllo nell'era dell'Intelligenza Artificiale: alcune osservazioni sul modello Human In The Loop' (2023) 9 Federalismi.it 68, 75.

[38] See Sandra Wachter and others (n 26) 92-93; Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 4(2) Seton Hall Law Review 995.

[39] However, we can refer to what the WP29 Guidelines state with respect to Article 22 of the GDPR, i.e. that a decision producing 'legal effect' is a decision affecting data subject's legal rights, legal status or her rights under a contract, while a decision producing 'similarly significantly affects' does not mean that this effect needs to have any legal implications for the data subject; rather, 'similar' refers to the significance and not the nature of the effect. Also, the Guidelines provide some examples of such significant effect: automated decisions affecting data subject's financial circumstances, access to health services or education. See WP29 Guidelines 21.

right to obtain from the deployer[40] "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken".

This provision applies to decisions made on the basis of the output from a "high-risk AI system". In the AI Act the different applications of AI technologies have been classified into three categories (prohibited AI practices, high-risk systems, low or minimal risk systems), based on the risk they may pose to the framework of fundamental values and rights of the EU. The choice of the EU regulator was to limit the right to an explanation to high-risk systems only. The rationale behind this choice is to avoid requiring the deployer to provide an explanation for outputs produced by AI systems that pose less risk to fundamental values and rights, because, as it has been pointed out in the literature, there is a certain trade-off between the explainability of an AI system and its degree of accuracy[41]. At the current stage, there are eight categories of AI systems considered to be high-risk: systems used for biometrics, systems involved in the management of critical infrastructures (e.g. the water, gas or electricity supply system), systems used for education and vocational training, systems used for employment and the management of workers, systems that determine access to essential private and public services, systems used for law enforcement, systems used in immigration management and border control, and systems used in the administration of justice and democratic processes (e.g. the elections)[42].

The scope of Article 86 is broader than that of Article 15 of the DPD or Article 22 of the GDPR, since the requirement that the decision be "based solely" on automated processing has disappeared[43], so Article 86 also applies in all those cases where the AI system is used merely as a support for the decision made by a human being. This is certainly an important step forward in the regulation of ADM, since, by equating fully automated decisions and those in which the AI system simply acts as a support to the human decision maker, the EU legislator is showing awareness of the tendency of the human decision maker to conform to algorithmic reasoning and not to deviate from it, considering it to tend to be

[40] According to Article 4(4) 'deployer' means any 'natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity'.
[41] '[U]nfortunately, in many contexts, the better-performing systems are the less explainable ones. In particular, neural networks are often the most effective approach to deal with pattern recognition and natural language processing. Thus, predictive performance and transparency are often conflicting objectives and there will have to be a trade-off between the two.', Mateusz Grochowski and others, 'Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises' (2021) 8(1) Critical Analysis of Law 43, 48.
Also, the 'Ethics Guidelines for Trustworthy AI' (n 18), 18, admits that 'trade-offs might have to be made between enhancing a system's explainability (which may reduce its accuracy) or increasing its accuracy (at the cost of explainability)'. For more on this topic see also Alex A Freitas, 'A Critical Review of Multi-objective Optimization in Data Mining: A Position Paper' (2004) 6(2) ACM SIGKDD Explorations Newsletter 77; Philipp Hacker and others, 'Explainable AI under Contract and Tort Law: Legal Incentives and Technical Challenges' (2020) 28 Artificial Intelligence and Law 415, 430-431.
[42] See Annex III AI Act.
[43] Article 86, in fact, speaks of a decision which is taken by the deployer "on the basis of the output from a high-risk AI system".

infallible ("moutunnier effect"[44]). In addition, unlike previous legislation, the AI Act regulates the issue of the explainability of the ADM, regardless of whether or not personal data processing takes place.

Nevertheless, in other respects, the scope of the provision is more specific. In fact, since under Article 3 of the AI Act[45] an AI system is only defined as such if it possesses a certain degree of autonomy, this means that if a system does not possess a minimum degree of autonomy, it will not fall within the scope of Article 86.

For the person subject to the automated decision to be able to assert this right, the decision must produce "legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights". The rationale behind this requirement is to avoid requiring the deployer to provide an explanation for outputs that do not substantially affect the individual, because of the aforementioned trade-off between the explainability of an AI system and its degree of accuracy[46]. Nevertheless, the provision bases the existence of "legal effects" or "similarly significantly affects" on the subjective perception of the individual, which will probably make it quite easy to prove.

Turning, finally, to the content of the right to an explanation, Article 86 states that the person is entitled to obtain from the deployer "clear and meaningful explanations of (i) "the role of the AI system in the decision-making procedure and" (ii) "the main elements of the decision taken". To clarify the practical content of the right to explanation, we can appeal to other provisions contained in Section 2 of the AI Act, which sets out the requirements for high-risk AI systems.

Article 11 states that before a high-risk AI system is placed on the market or put into service, detailed technical documentation must be prepared (and kept updated during the entire lifetime of the AI system). This documentation serves to prove that the system complies with the requirements set out in Section 2, with a view to ensuring a form of *ex ante* transparency. The technical documentation should include certain key elements[47], including information on: (i) the general logic of the AI system and of the algorithms, (ii) the main classification choices and the relevance of the different parameters, (iii) the description of the expected output and output quality of the system, (iv) the training methodologies and techniques and the training data sets used, including a general description of these data sets and (v) information of the human oversight measures needed in accordance with Article 14.

[44] The expression, invoked with regard to the justice sector, is due to Antoine Garapon and Jean Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique* (PUF 2018) 239.

[45] Article 3(1) defines an AI system as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

[46] See Grochowski and others (n 41).

[47] See Annex IV AI Act.

Article 12 deals with ensuring the traceability of actions performed by the AI system during its operation. In fact, it states that high risk AI systems "shall technically allow for the automatic recording of events (logs) over the lifetime of the system". The rationale behind this requirement is to ensure greater transparency *during* the operation of the AI system. The importance of the principle of traceability is highlighted both by Recital 27 of the AI Act, which links transparency with traceability and explainability[48], and by the Ethics Guidelines for Trustworthy AI, which state that traceability "facilitates auditability as well as explainability"[49].

Article 13 deals with ensuring that AI systems are designed and developed in such a way as to ensure that their operation is sufficiently transparent to allow deployers to interpret the system's output and use it appropriately. To this end, Article 13 affirms that these systems shall be accompanied by "instructions for use"[50]. These instructions shall contain, at least, (i) information about the intended purpose of the AI system, (ii) the level of accuracy, robustness and cybersecurity of the AI system, (iii) any known or foreseeable circumstance which may lead to risks to the health and safety or fundamental rights, (iv) its technical capabilities to provide information to explain its output (so the deployer knows whether the system is a "black box" or not), (v) its performance regarding specific individuals or groups of individuals on which the system is intended to be used and (vi) specifications for the input data[51]. This provision is particularly relevant for the purpose of ensuring that the right to an explanation is effective, since, under Article 86, the deployer is the party responsible for providing an explanation to the person subject to the automated decision made through a high-risk AI system.

The last important provision regarding high-risk AI systems is Article 14, which enforces the principle of human oversight. In particular, natural persons to whom human oversight is assigned should be enabled to (i) monitor its operation (e.g. to detect anomalies); (ii) be aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system […] in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons" ("moutunnier effect"[52]); (iii) correctly interpret system s output; and (iv) decide not to use the high-risk AI system" or to otherwise disregard, override or reverse the output of the high-risk AI system" and to interrupt the system through a stop" button[53]. This

[48] Recital 27 affirms that '[t]ransparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability'.
[49] Ethics Guidelines for Trustworthy AI 18.
[50] 'In an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers', see Article 13(2) AI Act.
[51] See Article 13(3) AI Act.
[52] See Garapon and Lassègue (n 44).
[53] Furthermore, paragraph 5 of Article 14, strengthens the principle of human in the loop with regard to the outputs produced by remote biometric identification systems (see point 1(a) of Annex III), which are considered particularly dangerous to the fundamental rights of individuals. It is stipulated that in order for the deployer to take a decision/action on the basis of the identification resulting from the system, that identification must be confirmed by at least two natural persons with the necessary competence, training and authority.

provision aims to ensure the principle of human in the loop and requires that high-risk systems be developed with a design that allows for human oversight (principle of transparency-by-design). The rationale behind this principle is that human oversight may prevent or minimise the risks to health, safety or fundamental rights arising from the use of the AI system.

Finally, although it does not directly deal with the issue of transparency and interpretability, Article 10 is also worth mentioning, which requires that the training, validation and testing data of the AI system meet certain quality criteria[54]. The principle of data quality (already enunciated in Article 5 of the GDPR with references to personal data), assumes particular relevance in the field of ML, given that decision-making algorithms learn and make decisions on the basis of the data they are provided with and, moreover, as mentioned earlier (see Section 1), much of the bias that afflicts the outputs of AI systems derives precisely from poor quality data.

In conclusion, the provisions we have analysed aim to impose greater transparency and explainability of the decisions produced by AI systems at three different stages:

-in the *ex ante* phase (i.e., before the high-risk system is placed on the market) with the obligation to drawn up the technical documentation (Article 11);

-during the operation of the system, both through the obligation to keep log files of the AI system (Article 12) and through the principle of human oversight and human in the loop (Article 14);

-in the *ex post* phase (i.e., after the system has produced the output) by ensuring that the deployer correctly interprets and uses the system's output (Article 13) and is therefore able to provide an explanation to the person subjected to the automated decision (Article 86).

The right to explanation, along with the other rules on transparency and explainability of ADM outlined in the AI Act, hold significant practical relevance in contemporary society. In fact, Recital 171 emphasises that the explanation mandated by Article 86 “should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights”. Therefore, within the AI Act, transparency and explainability are more than just broad principles: they are seen as essential tools to enable the exercise of fundamental rights and to safeguard key principles of the legal system, which are also guaranteed by the Charter of Fundamental Rights of the European Union (CFREU)[55]. Recitals from 54 to 61 identify, for each of the eight categories of high-risk AI systems, the fundamental rights and legal principles safeguarded by the rules on transparency and explainability. Recital 54, which deals with AI systems used for remote biometric identification, emphasises the principle of non-discrimination[56]; Recital 55, which deals with AI systems used in critical infrastructures, highlights the protection of human life and

[54] See paragraphs 2-5 Article 10 AI Act.
[55] Charter of Fundamental Rights of the European Union 2012/C 326/02 of 26 October 2012 [2012] OJ C326/391 (CFREU).
[56] Article 21 CFREU.

health and the protection of social and economic activities; Recital 56 recalls the right to education and training[57]; Recital 57 refers to workers' rights[58]; Recital 58, which deals with AI systems used to determine an individual's access to essential public and private services[59], focuses on the right to social protection, human dignity and the right to an effective remedy; Recital 59 stresses that transparency and explainability of ADM are necessary to enable the individual to exercise important procedural fundamental rights, such as the right to an effective remedy and to a fair trial[60], as well as the right of defence[61] and the presumption of innocence[62]; Recital 60, which deals with the AI systems used in the management of migration, asylum and border control, refers to the rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration[63] and, finally, Recital 61 emphasises the importance of transparency in the AI systems used in the administration of justice as a necessary condition for safeguarding democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial.

In light of the above, it can be affirmed that the right to explanation, as well as the other rules of the AI Act on transparency and explainability, are considered by the EU legislator to be instruments of fundamental importance for protecting a number of concrete rights of the individual, as well as key principles of the EU legal system.

4 Explainability of ADM in other pieces of EU legislation

In Sections 2 and 3 it has been described the historical path that led the EU legislator to finally recognise the right to an explanation in the AI Act, nevertheless, the issue of transparency and explainability of automated decisions is increasingly present within EU legislation, and has also been addressed in other recent pieces of EU legislation. This Section briefly recalls some of the regulations on the subject, contained in the 2019 reform of the EU consumer protection law, in the Digital Services Act[64] (DSA) and in the Platform Work Directive[65].

[57] Article 14 CFREU.
[58] Articles 15 and 31 CFREU.
[59] Articles 34 and 36 CFREU.
[60] Article 47 CFREU.
[61] Recital 59 states that 'The impact of the use of AI tools on the defence rights of suspects should not be ignored, in particular the difficulty in obtaining meaningful information on the functioning of those systems and the resulting difficulty in challenging their results in court, in particular by natural persons under investigation'.
[62] Article 48 CFREU.
[63] Article 41 CFREU.
[64] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277.
[65] The Proposal for a Directive of the European Parliament and of the Coucil on improving working conditions in platform work COM(2021) 762 final was approved by the European Parliament in April 2024 and is still awaiting Council's 1st reading position.

4.1 Explainability of ADM in the 2019 reform of the EU consumer protection law

As recognised by the EU Resolution 2019/2915[66], the development of ADM in the business-consumer relation, on the one hand, "is expected to make a significant contribution to the knowledge economy and offers benefits […] for consumers through innovative products and services and for businesses through optimised performance", but, on the other hand, it "also presents challenges for consumer trust and welfare, especially in terms of empowering consumers to identify such processes, to understand how they function, to make informed decisions on their use, and to opt out"[67].

In this field, ML algorithms and ADM can be used to profile consumers, enabling businesses to personalise the prices of goods and services offered to them, a practice known as price discrimination. More generally, these tools can be used to alter consumers' freedom of choice and manipulate their decisions in a way that, before the advent of these technologies, was unthinkable. In fact, even though such attempts at manipulation are not new in the context of the business-consumer relation, the use of AI technologies offers significant possibilities for enhancing these practices, as these tools make it possible to predict consumer behaviour more accurately, in real time, and based on huge amounts of data, which can be derived both from online interactions (through, for example, clicks, likes or purchase history) and from the offline world (Internet of Things)[68]. The new possibilities introduced by AI have therefore transformed previous, "static and undifferentiated"[69] manipulation strategies into "dynamic, interactive, intrusive, and incisively personalisable choices architectures-decision-making contexts that can be specifically designed to adapt and to exploit each individual user's particular vulnerabilities"[70]. Consequently, the use of these tools has increased the information asymmetry between consumer and business, which was already historically present in this field[71].

In light of what has been said so far, the need to enforce greater transparency and explainability of the work of ADM systems has also arisen in the consumer discipline[72], so, in 2019, the EU intervened by amending the regulation.

---

[66] European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services [2020] OJ C294.
[67] ibid letters B) and C).
[68] Nathalie De Marcellis-Warin and others, 'Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools' (2022) 2(4) AI and Ethics 259, 260.
[69] ibid 261.
[70] Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Online manipulation: Hidden influences in a Digital World' (2019) 4(1) Georgetown Law Technology Review 1, 3-4.
[71] Martin Ebers, 'Liability For Artificial Intelligence And EU Consumer Law' (2021) 12(2) Journal of Intellectual Property, Information Technology 204, 208.
[72] The European Parliament resolution (n 66) paragraph 1, states that consumers 'should be properly informed about how [ADM] function, about how to reach a human with decision-making powers, and about how the system s decisions can be checked and corrected'. See, also paragraph 13, which stresses that 'in light of the significant impact that automated decision-making systems can have on consumers, especially those in vulnerable situations, it is important for those systems not only to use high-quality and unbiased data sets but also to use explainable and unbiased algorithms'.

First, with Directive 2019/2161, Article 7 of the Unfair Commercial Practices Directive 2005/29/EC was amended: the new paragraph 4(a) requires traders to disclose the "main parameters determining the ranking of products presented to the consumer […] and the relative importance of those parameters". Also in 2019, the EU regulator intervened, through Regulation 2019/1150, to impose a similar obligation on online search engine providers: Article 5(2) of the Regulation requires online search engine providers to set out the "main parameters, which individually or collectively are most significant in determining ranking" and "the relative importance of those main parameters". Recital 22 of the 2019/2161 Directive and Recital 24 of the 2019/1150 Regulation both clarify that "main parameters" means any "general criteria, processes, specific signals incorporated into algorithms or other adjustment or demotion mechanisms used in connection with the ranking". Finally, the EU legislator, through Directive 2019/2161, has specifically addressed the practice of price-discrimination implemented by means of algorithms. With the aim of imposing greater transparency on this tool, the new Article 6(1)(ea) of the Consumer Rights Directive[73], stipulates that the trader must inform the consumer "that the price was personalised on the basis of automated decision-making".

Therefore, in the field of business-consumer relations, transparency and explainability of automated decisions are essential to protect consumer rights, such as the right to make free and informed decisions and to rebalance, also guaranteed by Article 38 CFREU.

4.2 Explainability of ADM in the Digital Services Act

Also, in the DSA there is a number of provisions that deal with enforcing the transparency and explainability of automated decisions, particularly those used by online platforms in content moderation processes and recommender systems (RSs).

Both these processes are carried out by algorithms[74], since the huge growth of so-called user-generated content[75] and online user interactions (through clicks, likes, shares, etc.), on the one hand makes it impossible for providers to delegate content moderation activities to human operators alone, and, on the other hand, provides a huge amount of

[73] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304.

[74] See Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance' (2020) 7(1) Big Data & Society 1.
For instance, algorithms currently control more than 95% of content removal and bans on Facebook (up from 23% in 2017); YouTube now reports that 98% of the videos removed for violent extremism are flagged by machine-learning algorithms", and Twitter revealed that 93% of "terrorist content" is reported by proprietary internal tools (i.e., algorithms for detecting terrorist content) and removed. See Sergio Sulmicelli, 'Algorithmic content moderation and the LGBTQ+ community s freedom of expression on social media: insights from the EU Digital Services Act' (2023) 2 BioLaw Journal – Rivista di BioDiritto 471, 478; see also 'Twitter Transparency Report' (5 April 2018) <https://blog.twitter.com/official/en_us/topics/company/2018/twitter-transparency-report-12.html> accessed 14 November 2024.

[75] In 2022, about 500 hours of videos were uploaded every minute on Youtube. See 'Hours of video uploaded to YouTube every minute' (*Statista*, 2024) <https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/> accessed 14 November 2024.

information about the users themselves, which can be used to profile them and show them personalised content that may interest them (through the RSs). The two phenomena (moderation and recommender systems) are thus connected, since when there is a need to work with large amounts of data, algorithms become an indispensable tool. Nevertheless, the use of algorithms in these fields poses a number of ethical and legal problems that the EU has sought to address by requiring greater transparency and explainability.

Beginning with the activity of moderation[76], in this field there is a need to balance the efficiency of the moderation activity performed by algorithms with the principle of freedom of expression online, especially because, even for the most sophisticated algorithms, it is difficult to understand the context behind a certain sentence[77] (with the risk of causing numerous false positives), so if the moderation activity is performed by an algorithm, it is necessary both to make explicit the role it plays and to make the reasons behind its intervention understandable.

To this end, Articles 14 and 15 of the DSA stipulate, respectively, the obligation for providers of intermediary services to outline (in the terms and conditions) information on any policies, procedures, measures and tools used for the purpose of content moderation, "including algorithmic decision-making and human review[78]" and the obligation to, at least once a year, make publicly available a report on the moderation activity carried out on their platform, which must contain, among other things, a disclosure on "any use made of automated means for the purpose of content moderation"[79]. Even though these provisions do not deal with the explicability of algorithmic outputs (i.e., the reasons behind the decision to moderate or not moderate a piece of content), they nonetheless impose a general obligation of transparency on the use of automated systems, similar to what is enshrined in consumer protection law (as reformed in 2019) with respect to the use of ADM in price-discrimination.

[76] Article 3(t) of the Regulation clarifies that 'content moderation means "the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient s account".

[77] Natasha Duarte and Emma Llansò, 'Mixed messages? The limits of automated social media content analysis' (*Center for Democracy and Technology*, 28 November 2017) <https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/> accessed 14 November 2024, 5: Among studies using NLP to judge the meaning of text (including hate speech detection and sentiment analysis), the highest accuracy rates reported hover around 80%, with most of the high-performing tools achieving 70 to 75% accuracy. These accuracy rates may represent impressive advancement in NLP research, but they should also serve as a strong caution to anyone considering the use of such tools in a decision-making process. An accuracy rate of 80% means that one out of every five people is treated wrong in such decision-making; depending on the process, this would have obvious consequences for civil liberties and human rights".

[78] Article 14(1) DSA.

[79] "[I]ncluding a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied", Article 15(1)(e) DSA.

The explainability of moderation activity is addressed in Article 17 DSA, which requires providers of hosting services to provide a clear and specific "statement of reasons" to the affected uploader for each content moderation decision. This statement shall include "information on the use made of automated means in taking the decision, including information on whether the decision was taken in respect of content detected or identified using automated means" and "the facts and circumstances relied on in taking the decision". The purpose of Article 17 is twofold: on the one hand, it aims to make moderation activity knowable to the user (with a view to countering practices such as shadow banning[80]); on the other hand, it seeks to make moderation activity explainable[81]. Although even Article 17 does not explicitly mention a right to an explanation of the algorithmic decision (i.e., the decision to moderate a piece of content), such a right could perhaps be derived on the basis of the general obligation to justify the moderation activity performed, since this is, in the vast majority of cases, carried out through algorithms.

As for recommender systems, the DSA defines them as "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed"[82]. This definition highlights the method ("fully or partially automated"), aim ("to suggest"), content ("specific information"), target ("recipients of the service"), input ("as a result of a search initiated by the recipient") and output ("determining the relative order or prominence of information displayed") of a recommendation process[83].

Recommender systems thus influence a central aspect of the user experience on the online platform, namely what content is shown to them[84]. Moreover, because algorithm-based recommender systems often rely on implicit personal data, such as browsing and click-through history, their functioning is not explained to users, and their influence is not

[80] "Shadow banning" is a term used to refer to a moderation action that allows a particular user to be hidden from an online community, or to make content posted by him invisible to other users. It differs from "banning" proper in that the profile of the affected user is not banned and/or deleted from the platform, and his or her content is not deleted, but is, instead, rendered unavailable to other users. As a result, the user in question remains completely unaware of the sanction and continues to behave normally. For more on this topic, see Paddy Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation' (2023) 48 Computer Law & Security Review 1.

[81] ibid 6.

[82] Article 3(s) DSA.

[83] Matteo Fabbri, 'Self-determination through explanation: an ethical perspective on the implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union', *AIES '23: AAAI/ACM Conference on AI, Ethics, and Society* (ACM 2023) 653 <http://dx.doi.org/10.1145/3600211.3604717> accessed 14 November 2024.

[84] These systems allowed people to "filter what they want to read, see, and hear", not coming "across topics and views that you have not sought out", Cass R Sunstein, Republic: *Divided democracy in the age of social media* (Princeton University Press 2018). Furthermore, "automated recommendations determine not only what we see on platforms, but also our potential interest for new or different categories of content. This influencing potential can be interpreted as an instance of the "new emerging grey power" of tech companies, which is exercised about which questions can be asked, when and where, how and by whom and hence what answers can be received in principle", Luciano Floridi, 'The new grey power' (2015) 28 Philosophy & Technology 329, 332.

accountable. Furthermore, the use of RSs raises a number of problems: it can lead to the creation of so-called "echo chambers" and the consequent polarization of online debate[85]; it can foster nudging practises[86] and, finally, it incentivises the circulation of viral content[87] that can prove harmful[88].

With the DSA, therefore, an attempt was made to implement greater transparency and explainability of these systems in order to reduce the impact of those harms by increasing users' awareness. Article 27 DSA states that providers of online platforms "shall set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems". The aim of this provision is to "explain why certain information is suggested to the recipient of the service"[89]; therefore, the parameters need to include, at least, "the criteria which are most significant in determining the information suggested to the recipient of the service" (i.e., content) and the reasons for its "relative importance"[90] (i.e., ranking). Also, non-binding Recital 70 DSA states that online platforms "should clearly present the main parameters for such recommender systems in an easily comprehensible manner to ensure that the recipients understand how information is prioritised for them". According to some, a right to explanation for RSs' outputs could be identified in this formulation: in fact, the "easily comprehensible manner" of presenting the parameters of RSs so that "the recipients understand how information is prioritised for them" can come to effect only if RSs are explainable[91].

Therefore, with respect to content moderation and the activity of recommender systems, the transparency and explainability of ADM are functional to the protection of important individual rights, such as the freedom of expression and information, both guaranteed by Article 11 CFREU.

4.3 Explainability of ADM in the Platform Work Directive

The issue of transparency and explainability of automated decisions has also arisen with reference to the world of labour and, in particular, to the regulation of work on digital

[85] The polarisation of online debate occurs as opinions are no longer exposed to confrontation (since the individual is only exposed to messages that confirm his or her opinions), but, on the contrary, are continually reinforced within "bubbles" in which the same ideas are always circulating.
[86] According to the original definition proposed in behavioural economics, nudges are the features of a choice architecture "that have an influence on which decisions people make", Richard H Thaler, Cass R Sunstein, '*Nudge: Improving Decisions about Health, Wealth, and Happiness*' (Penguin Books 2009).
[87] Recital 70 DSA states that RSs "play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour".
[88] A case of absolute harm of inclusion covered by the international press concerns the blackout challenge" on TikTok, which encourages users to film themselves as they choke themselves to the point of fainting and then regain consciousness on camera: various cases emerged in which minors died while trying the challenge, Kari Paul, 'Families sue TikTok after girls died while trying 'blackout challenge' (*The Guardian*, 6 July 2022) <https://www.theguardian.com/technology/2022/jul/05/tiktok-girls-dead-blackout-challenge> accessed 14 November 2024.
[89] Article 27(2) DSA.
[90] ibid.
[91] Fabbri (n 83) 657.

platforms. The EU Commission addressed this issue with its recent proposal for a Directive on the improvement of working conditions in digital platform work (PWD), which was approved by the EU Parliament in April 2024.

Recital 4 of the PWD clarifies the link between the coming of "algorithm-based technologies, including automated monitoring or decision-making systems" and "the emergence and growth of digital labour platforms". Recital 8, on the one hand, recognises the increasingly central role played by algorithm-based ADM and monitoring systems, which "increasingly replace functions that managers usually perform in businesses, such as allocating tasks, the pricing of individual assignments, determining working schedules, giving instructions, evaluating the work performed, providing incentives or imposing sanctions", on the other hand, also recognises that persons performing platform work "often do not have access to information on how the algorithms work, which personal data are being used and how their behaviour affects decisions taken by automated systems [and] often do not know the reasons for decisions taken or supported by automated systems and lack the possibility to obtain an explanation for those decisions".

The PWD devotes the entire Chapter III to the topic of algorithmic management and, in particular, deals with regulating the use of automated monitoring systems[92] and ADM systems by digital labour platforms.

The latter are defined in Article 2(9) as "systems which are used to take or support, through electronic means, decisions that significantly affect persons performing platform work including the working conditions of platform workers". The PWD, like the AI Act, expressly includes in the definition of "ADM systems" also those cases where these systems are used simply as a support for the final decision. Moreover, as in previous legislation, there is the expression "significantly affect", but the directive gives some examples of what this term means, namely those decisions "affecting their recruitment, access to and organisation of work assignments, their earnings including the pricing of individual assignments, their safety and health, their working time, their access to training, promotion or its equivalent, their contractual status, including the restriction, suspension or termination of their account"[93].

In the regulation of automated decisions, the PWD has three objectives: (i) to impose transparency on the use of automated monitoring systems and ADM systems (Article 9), (ii) to ensure the principle of human in the loop (Article 10), and (iii) to guarantee the data subject's right to an explanation of the automated decision (Article 11).

With a view to fostering transparency on the use of ADM, Article 9 requires digital labor platforms to inform platform workers and platform workers' representatives (and also, upon request, competent national authorities) about the use of automated monitoring

[92] Which are, according to Article 2(8), "systems which are used for, or support monitoring, supervising or evaluating the work performance of persons performing platform work or the activities carried out within the work environment, including by collecting personal data, through electronic means".
[93] See Article 2(9) PWD.

systems or decision-making systems. In particular, regarding ADM systems, the directive requires digital labor platforms to inform workers about (i) "the categories of decisions that are taken or supported by such systems", (ii) the "main parameters that such systems take into account" together with their "relative importance" and "the way in which the platform worker's personal data or behaviour influence the decisions", and (iii) the "grounds" for a subset of especially significant decisions including refusal of remuneration, termination of the worker's account, or any decision of "equivalent or detrimental effect"[94]. Nevertheless, the information required by Article 9 is quite general and assumes only an explanation of the general operation of the system ("global" explanation), rather than the specific decision made ("local" explanation), especially because this information must be provided on the first day of work[95] and because it is generic to all workers.

Article 10 deals with ensuring human oversight of the operation of these systems. Firstly, paragraph 5 prohibits the use of ADM for making certain particularly significant decisions, such as any decision to "restrict, suspend or terminate the contractual relationship or the account of a person performing platform work or any other decision of equivalent detriment". These decisions, under Article 10, can only be made by human beings. Furthermore, Article 10 requires platforms to staff themselves with the necessary competence, training and authority to, at least every two years, oversee and evaluate "the impact of individual decisions" taken or supported by automated monitoring and decision-making systems, used by the digital labour platform, on workers, including "their working conditions and equal treatment at work"[96]. The PWD is concerned with making sure that this control activity is effective and not merely formal: in fact, it stipulates that controllers must have the authority and expertise to be able also to override automated decisions and must be protected from disciplinary or other "adverse treatment" for exercising their functions[97].

Nevertheless, the most relevant provision with respect to automated decisions is Article 11, which states that platform workers "have the right to obtain an explanation from the digital labour platform for any decision taken or supported by an automated decision-making system without undue delay". This explanation (in oral or written form) shall be presented in a "transparent and intelligible manner". Article 11 regulates in detail the procedure by which the worker can obtain this explanation. Digital labour platforms have to provide platform workers with access to a contact person (who has to possess the necessary competence, training and authority to exercise that function) "to discuss and to clarify the facts, circumstances and reasons having led to the decision". For particularly

[94] See Article 9(1)(c) PWD.
[95] See Article 9(3) PWD.
[96] See Article 10(1) PWD.
[97] See Article 10(2) PWD.

significant decisions (such as the decision to terminate the worker's account[98]), the worker must be provided also with, at the latest on the day which the decision takes effect, a "written statement of the reasons"[99]. If then, the worker is not satisfied with the reasons given to him by the contact person or the written statement, he shall have the right to request the digital labour platform to review that decision, to which the platform will have to respond with a "a sufficiently precise and adequately substantiated reply" within two weeks of receipt of the request. Finally, Article 11(3) states that if the decision "infringes the rights" of the worker, the platform shall rectify that decision within two weeks of the adoption of the decision and shall take the necessary steps, including, if appropriate, a modification of the ADM system or a discontinuance of its use, in order to avoid such decisions in the future.

In conclusion, the EU legislator is concerned about the impact that automated monitoring systems and ADM systems, used by digital labour platforms, may have on the world of work. Consequently, imposing greater transparency and explainability on the functioning of these systems is functional to the protection of workers' rights, which are also recognised by Articles 15 ("Freedom to choose an occupation and right to engage in work") and 31 ("Fair and just working conditions") CFREU.

5 The common thread in EU legislation regarding ADM regulation

Sections 2 and 3 analysed the evolution of EU ADM legislation from the DPD to the AI Act; then, Section 4 demonstrated the growing necessity of regulating ADM across three distinct fields. Two considerations can be drawn from this.

First, the heterogeneity of the areas in which the EU legislator has intervened to regulate the use of ADM (consumer protection law, online content moderation, the use of recommender systems and the regulation of work on digital platforms) demonstrates, in the writer's opinion, the increasing pervasiveness of ADM in today's society: wherever it is necessary, or convenient, to operate with large amounts of data, there is a need to use algorithmic decision-making processes and, as a result, the regulator intervenes to impose greater transparency and explainability on ADM.

Second, looking at the evolution of ADM regulation that took place between the DPD, GDPR and the AI Act, the chronological factor would seem to play a role in the standard of ADM transparency and explainability required by regulation: more recent regulatory acts have higher standards. In fact, the DPD only recognised the data subject's right to

[98] Any decision "to restrict, suspend or terminate the account of the person performing platform work, any decision to refuse the payment for work performed by the person performing platform work, any decision on the contractual status of the person performing platform work, any decision with similar effects or any other decision affecting the essential aspects of the employment or other contractual relationships", see Article 11(1) PWD.

[99] Even if this written statement of reasons "may give the sense of human involvement, it seems plausible that such a statement could be pro forma—or even created by a text generation system", Michael Veale and Michael Six Silberman, Reuben Binns, 'Fortifying the algorithmic management provisions in the proposed Platform Work Directive' (2023) 14(2) European Labour Law Journal 308, 316.

obtain “knowledge of the logic involved in any automatic processing of data” and the right to “put his point of view”; subsequently, the GDPR also recognised the data subject's right to obtain human intervention, the right to contest the decision and the right to obtain meaningful information and, finally, the AI Act expressly provided for the right to an explanation of the decision made through a high-risk AI system. This analysis suggests the existence of a common thread in EU regulation of ADM, namely the tendency to impose increasingly stringent rules on transparency and explainability.

6 The reasons behind this common thread

Sections 2 and 3 highlighted how the call for greater transparency and explainability of automated decisions has been translated by the EU legislator into EU law, starting from the very first regulation of automated decisions in 1995 with the Data Protection Directive, to the most recent EU legislation on the subject, the AI Act. It has also been shown (Section 4) how demands for transparency and explainability of ADM have made their way into the regulation of specific sectors at the EU level. Adopting this historical perspective, a common thread in EU legislation was highlighted, namely the tendency to impose increasingly stringent rules on the transparency and explainability of ADM. It now remains to understand the rationale behind this intervention, i.e., what reasons have prompted the EU regulator to address this issue with increasing frequency.

Here, three possible causes are suggested: (i) the increased pervasiveness of ADM in our society due to the technological progress occurred in the field of AI and ML, (ii) the EU regulator attempt to strengthen citizens’ trust in AI technologies and (iii) the overconfidence in human decision-making process (HDM).

The first reason is that automated decisions, since 1995, have occupied an increasingly central place in our society. In turn, the increased pervasiveness of ADM is due to the technological progress in the field of AI and ML. In fact, the term "Artificial Intelligence" encompasses several techniques and approaches (symbolic AI, ML, neural networks, decision tree, deep learning, etc.), which differ not only in their accuracy and predictive ability, but also in their degree of explainability[100]. In recent years, the most widely used AI systems are those based on ML. What distinguishes these systems from the rest is their ability to learn automatically from the data provided to them: the software, in order to produce the output, does not follow pre-specified rules of behaviour in an operator-

[100] For example, the field of so-called Symbolic AI” requires software to provide pre-defined, step-by-step specifications of the rules, facts, and structures that define the characteristics of the evolving calculations of probabilities made by the computer programme. Symbolic AI is tied to representations provided by humans undertaking the programming, consequently, it allows, in principle, for explanations on the outcome of specific calculations as well as documenting programme specific requirements. See Herwig C H Hofmann, ‘An Introduction to Automated Decision-Making (ADM) and Cyber-Delegation in the Scope of EU Public Law’ [2021] University of Luxembourg Law Research Paper No. 2021-008 1.

defined way (i.e. it does not rely on explicit "if-then rules[101]), but “it autonomously and dynamically develops the decision rule by applying learning and adaptive algorithms[102]”. This feature, on the one hand, makes the system more efficient and capable of performing more complex tasks, but on the other hand, makes it less understandable[103]. The success of ML[104] is due both to the increase in the amount of data available and to the increase in computational capacity that has occurred in the last thirty years[105]. The combination of these two factors has made ML-based AI systems more accurate and efficient and, therefore, more popular. Nevertheless, because these systems are less explainable and act with a greater degree of autonomy than other AI technologies, this has increased the demand for transparency and explainability.

The second reason that may explain the choice of the EU regulator to devote more attention to the discipline of ADM could be civil society's distrust of AI and, consequently, of automated decisions made through it: this distrust may have increased the demand for transparency and explainability. In fact, whereas a decision made by a human, except in cases expressly provided for by law, does not give rise to a right to an explanation on the part of the person concerned, on the other hand, when the decision is made by an “artificial” decision-maker, a right to an explanation has been established. It could be said that this choice is legitimised by the fact that the outputs produced by AI systems are still imperfect[106] (as discussed in Section 1). Nevertheless, to this assertion, which is certainly true, it could be objected that also human decisions can be erroneous, can be affected by bias[107], can lead to episodes of discrimination and can be opaque[108]. Moreover,

[101] The system is given only rules about how to learn from data”, as pointed out by Yavar Bathaee, ‘The Artificial Intelligence Black Box And The Failure Of Intent And Causation’ (2018) 31(2) Harvard Journal of Law & Technology 890, 898.
[102] Troisi (n 4) 954.
[103] As early as the 1950s, Alan Turing noted that a machine capable of learning could operate in ways that were not anticipated by its creators and trainers, even without their understanding of the machine's internal workings. See Alan M Turing, ‘Computer Machinery and Intelligence’ (1950) LIX(236) Mind 433.
[104] In fact, these systems are now used in a very wide plurality of areas: to make loans, select candidates for a job, set the premium for an insurance policy, target advertising to individual consumer preferences, but also to detect tax evaders, drug trafficking, as well as to conduct the fight against terrorism, see Jenna Burrell (n 10). Furthermore, it is unthinkable for certain activities (such as content moderation) to be performed by human beings, both because the amount of data to be processed is incomputable for a human, and because technological progress (i.e., the increase in the computational capacity of computers and the consequent lowering of costs) has made it inefficient to entrust these processes to humans.
[105] See Tabarrini (n 1).
[106] One might wonder whether, if we were somehow certain that algorithmic decisions were always perfect”, we could dispense with an explanation of the decision. Carlo Casonato, ‘AI and Constitutionalism: The Challenges Ahead’ in Bertrand Braunschweig and Malik Ghallab (eds), *Reflections on Artificial Intelligence for Humanity* (Springer 2021) 138.
[107] It has been amply demonstrated in the psychological literature that human reasoning can be affected by bias and can be conditioned in many ways. See Cameron Buckner, ‘Black Boxes or Unflattering Mirrors? Comparative Bias in the Science of Machine Behaviour’ (2023) 74(3) The British Journal for the Philosophy of Science 681.
[108] Buckner (n 108) points out how human decision-making can also be, like algorithmic decision-making, affected by bias and can take the form of a real “black-box”. See also Vincent Chiao, ‘Transparency at Sentencing: Are Human Judges More Transparent Than Algorithms?’ in Jesper Ryberg and Julian V Roberts (eds), *Sentencing and Artificial Intelligence* (Oxford Academic 2022) 34, who explores the topic the transparency and explicability of human decision-making in reference to judicial decisions and comes to the same conclusions.

algorithmic decisions are, to a certain extent, exposed to less risk than human decisions: when making decisions, AI systems are not influenced by feelings, they cannot lie, and, for example, they are not intrinsically racist; on the contrary, they make decisions based on statistical probability and the analysis of large amounts of data. Conversely, none of this can be said across the board with regard to human decisions. Therefore, one of the causes of this distrust, far from being based on rational grounds, could be precisely the artificial nature of the decision-maker.

Another part of civil society's distrust of AI could stem from the fact that humans often do not understand them, both because of the computational gap between humans and AI and because of the aforementioned black-box problem. Lastly, another source of this distrust may stem from our (perhaps excessive) fear of these technologies, probably, in part, because we are conditioned by the science fiction literature of the last century[109], which has often depicted robots (think Terminator) or "supercomputers" (such as the famous HAL 9000) as dangers to humans.

Whatever the cause of this distrust, the EU regulator has sought to fight it by making ADM more transparent and by explaining the reasons behind the outputs of AI systems, with the aim of strengthening EU citizens' trust in these technologies[110]. This approach recalls to that taken by the EU with the GDPR: the purpose of the latter, in fact, far from being to restrict the circulation of data, was precisely to strengthen the confidence of EU citizens in such a way as to increase the circulation of data within the EU market[111]. After all, the "trustworthiness" of AI, is one of the central themes of EU regulation: it is identified, on several occasions[112], as the key to spreading more trust in this technology and encouraging its use by citizens and businesses.

The third possible reason behind the increasing regulation on transparency and explainability of ADM could be the overconfidence placed in the transparency and explainability of HDM[113] that, perhaps, raises the standards required of ADM explainability. This overconfidence in HDM leads people to expect standards of transparency and explainability from ADM that, in reality, are not guaranteed even in human decision-making[114]. As a result, there is a "double standard" between the level of explainability demanded of ADM and that demanded of HDM[115]. This double standard, then, would result

[109] Giorgio Buttazzo, 'Artificial Consciousness: Utopia or Real Possibility?' (2002) 34(7) Computer 24.
[110] On the link between transparency and trust, see Heike Felzmann and others, 'Transparency you can trust: transparency requirements for artificial intelligence between legal norms and contextual concerns' (2019) 6(1) Big Data & Society 1.
[111] In fact, not surprisingly, the very name of the GDPR speaks of the 'free movement' of such data.
[112] See White Paper on Artificial Intelligence 3, which expresses the EU will to create an 'ecosystem of trust' because 'Building an ecosystem of trust is a policy objective in itself, and should give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to innovate using AI'. Moreover, in the text of the AI Act, the word 'trust' (in the form of 'trust', 'trustful', 'trustworthy' and 'trustworthiness') appears 24 times.
[113] John Zerilli and others, 'Transparency in Algorithmic and Human Decision- Making: Is There a Double Standard?' (2019) 32 Philosophy & Technology 661.
[114] ibid.
[115] ibid.

not so much from an excessive distrust of machines but, rather, from an excessive trust placed in the transparency and explainability of decisions made by humans[116], which sets the bar for ADM explainability very high.

7 Conclusions

The objectives of this contribution were twofold. The first was to analyse EU regulation of automated decisions from a historical perspective to highlight a certain trend: the increasing focus on transparency and explainability of automated decisions. Moreover, it was also highlighted how the issue of transparency and explainability in ADM has also emerged in EU regulation of specific sectors (consumer protection law, online content moderation, recommender systems and the regulation of work on digital platforms).

The second objective of this contribution was to suggest some explanation for such a normative development. Three causes were proposed in Section 6: (i) the increased pervasiveness of ADM in our society due to the technological progress in the field of AI and ML, (ii) the EU regulator attempt to strengthen citizens' confidence in AI technologies and (iii) the overconfidence placed in human decision-making that, perhaps, raises the standards required of ADM explainability.

Although the intent of the EU legislator to enhance the transparency and explainability of ADM is reasonable, it is not without consequences. This topic cannot be discussed in depth here, nevertheless, the growing demand for explainability of AI systems poses a number of balancing problems with other interests. First, there is the issue of protecting trade secrets and intellectual property rights (IPRs) involved[117]. Second, keeping an AI system opaque can also be important for ensuring its effectiveness (for example to prevent spambots from using the disclosed algorithm to attack the system or prevent people from cheating the system by tilting the outputs of an AI system in a desired direction)[118]. Moreover, it has been pointed out in the literature that there is a certain trade-off between the degree of explainability of an AI system and its accuracy[119]: the more explicable one makes the AI system, the more one reduces its accuracy and vice versa. This raises a critical dilemma: either one pursues the goal of making AI systems (and their decisions) as transparent and explainable as possible (while reducing their accuracy) or

[116] 'While we do not deny that transparency and explainability are important desiderata in algorithmic governance, we worry that automated decision-making is being held to an unrealistically high standard here, possibly owing to an unrealistically high estimate of the degree of transparency attainable from human decision-makers', ibid 662. Nevertheless, other authors have pointed to different explanations for this 'double standard', see, for example, Mario Günther and Atoosa Kasirzadeh, 'Algorithmic and human decision making: for a double standard of transparency' (2022) 37(1) AI & SOCIETY 375.

[117] See Paul B de Laat, 'Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?' (2022) 24(17) Ethics and Information Technology 16.

[118] Martin Ebers, 'Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework(s)' in Liane Colonna and Stanley Greenstein (eds) *Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence* 103.

[119] See Grochowski and others (n 41).

one pursues the goal of making them as accurate as possible, while giving up explaining their outputs.

Finally, another potentially negative effect of transparency concerns privacy and data protection: making available the training data of the ML algorithm (which is a way of making them more transparent) may violate privacy law and the GDPR, if the dataset enables identification of personal data[120].

In light of this tension between the explainability of ADM and other conflicting interests, this study could contribute to a dual purpose: (i) raising greater awareness about the direction taken by the EU legislator over the past thirty years regarding ADM regulation, and (ii) proposing some possible explanations behind this regulatory development.

[120] In 2020, a Swedish administrative court of second instance granted a journalist access to the source code of the algorithm (despite the fact that it was protected by trade secret) used by the town of Trelleborg to automate decisions in welfare services. A particularly interesting aspect of the case was that when the disclosure of the source code took place, at the same time the personal data of some 250 citizens (first name, last name, and social security code) who had had dealings with the municipality to access welfare services were made public, because these data were included in the source code. This highlights one of the possible problems with source code disclosure: in addition to the infringement of the economic freedom of companies, this solution may also infringe on the privacy rights of third parties. See Katarina Lind, 'Central authorities slow to react as Sweden s cities embrace automation of welfare management' (*Algorithm Watch*, 17 March 2020) <https://algorithmwatch.org/en/trelleborg-sweden-algorithm/> accessed 14 November 2024.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 3 - 3/2024