30 Years of the Single Market

Written Submission for a European Law Institute Webinar

Summary

Where are we 30 years on from the establishment of the Single Market? What does it take to ensure that single market policies act as levers for further digitalisation of our industries and governments?

As 1 January 2023 marks the 30th anniversary of the establishment of the European Single Market, several upcoming debates and events are planned. Sweden, which will hold the Presidency of the Council of the European Union from 1 January to 30 June 2023, wishes to focus on the single market, notably to see what it takes to ensure that single market policies act as levers for further digitalisation of our industries and governments but also to look at barriers relating to our *acquis* that is no longer fit for purpose or challenges relating to the development of new business models.

The European Law Institute assembled a team to contribute to the above discussions in a '30 Years of the Single Market' Webinar that took place on 6 October 2022. The following speakers contributed to it:

- Pascal Pichonnaz (Chair; ELI President; Professor, University of Fribourg)
- Christiane Wendehorst (ELI Scientific Director; Co-Reporter of the ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights; Professor, University of Vienna)
- Aneta Wiewiórowska-Domagalska (ELI Executive Committee Member; Co-Reporter of the ELI Model Rules on Online Platforms; Senior Researcher at the University of Osnabrück)
- Juliette Sénéchal (Co-Reporter on ELI project on Blockchain Technology and Smart Contracts (until January 2021); Professor, University of Lille)
- Bernhard A Koch (Co-Reporter of the ELI Project on the Reform of the Product Liability Directive; Professor, University of Innsbruck)
- Teresa Rodriguez de las Heras Ballell (ELI Executive Committee Member; Drafter of the ELI Innovation Paper on Guiding Principles for Automated Decision-Making in the EU; Professor, Universidad Carlos III de Madrid)

Below are the written contributions of our speakers.

Table of Contents

Data Economy in the Digital Single Market – Between 'Open by Default' and 'Protection by Default'

By Univ-Prof Dr iur Christiane Wendehorst, LLM (Cantab)

Building a vigorous European data economy is key to economic prosperity in the EU in the 21st century. Ambitious action may be required at various levels to make it happen, including at the level of legislation. However, the breathtaking pace at which the European legislator is currently passing one data economy-related Act after the other also raises concerns about consistency and about the actual impact legislation will have on the European economy.

Data is a key driver of our modern economies. It used to be compared to the oil of the 21st century, but over time, and especially since the current energy crisis, it has become clear that this comparison is fundamentally flawed in several ways. While oil is both a consumable and a rival resource – if one person has it, that means others don't, and once one person burns it, no one else will be able to burn it ever again – this is not true of data. Data is a non-rival resource, which means it can be replicated at virtually no cost and used by a variety of different parties for a variety of different purposes. And it can be used over and over again without degradation or deterioration (notwithstanding the fact that some data can lose its market value very quickly). In addition, unlike with oil, the location of storage is largely irrelevant and transport from A to B can be done at virtually no cost and in fractions of a second. Together with the exponential increase in storage capacity and computing power, this means that the opportunities are more or less unlimited. These are opportunities for European companies, which must keep pace with global technological trends and strive to catapult themselves to the forefront of developments. It is important that Europe is a technology maker and not a pure technology taker, because those who are pure technology takers make themselves too dependent on others and must ultimately accept the rules dictated by them.

All this means that the availability of suitable data for European businesses, and in particular for SMEs, is key to a prosperous European data economy. Data must be suitable for the economy in terms of both quantity and quality, which means that the generation, the proper management and the sharing of data needs to be encouraged. Economic considerations have been reinforced by the fact that the world is facing a number of serious problems, ranging from a pandemic to under-development to climate change. Science and technology, much of them data-driven, are considered to be key tools for solving these problems. This is why more data and more data sharing within the European Single Market has become the mantra of data policies over the past five years. This is illustrated by generally accepted benchmarks such as the FAIR-Principles (FAIR = Findable, Accessible, Interoperable, Reusable), and by slogans such as 'open by default'. 'Open' stands for a whole range of goals we hope to achieve with the help of data, including any of the 17 UN Sustainable Development Goals (SDGs), economic prosperity, transparency, democracy, etc.

Conflicting Paradigms

Having 'open by default' as a generally accepted goal is all the more remarkable as there are conflicting mantras of 'data minimisation' and 'privacy by default'.

Both of the latter are enshrined in the General Data Protection Regulation (EU) 2016/679 (GDPR) and thus indirectly considered part of data protection as a fundamental right under Article 8 of the EU Charter of Fundamental Rights. While these concerns are specifically focused on personal data, ie data relating to an identified or identifiable natural person, similar concerns exist with regard to non-personal data: what is at stake more generally is the protection of important private and public interests, including (other) fundamental rights, national security, law enforcement, protection of intellectual property and fair and effective competition. This is so because all the benefits of data as compared with more traditional resources – such as being a non-rival, non-consumable, multi-purpose, remotely accessible, and intangible resource – not only work for activities we want to encourage, but equally for harmful activities we want to prevent. They work for privacy breaches, copyright infringements, total surveillance, fraud, espionage, terrorist attacks, as well as cyber and hybrid warfare. Data produced by a connected vehicle may serve a European SME to develop an innovative 'green' digital service and help cut emissions. The very same data, however, may give foreign competitors from other continents access to European trade secrets, disclose to organised crime the whereabouts of potential victims, enable psychopaths to spy on their ex-spouses, and allow foreign authoritarian governments to monitor the political activities of their citizens. A policy of 'open by default' is almost necessarily at odds with a policy of 'protection by default'. This is why the formula of 'open by default' is often replaced by the formula 'as open as possible and as close as necessary' – which does not, however, help a lot in terms of the underlying tension we need to resolve.

A Data Economy of Strictly Non-Personal Data, or 'Without Prejudice to' Protection?

Over time, various strategies to resolve the tension were pursued at the level of EU law making. The first strategy was carving out any personal data from data economy considerations and restricting data sharing legislation to non-personal data. This was very much the spirit of the Free Flow of Data Regulation (EU) 2018/1807. It stresses over and over again that it should be applied with regard to non-personal data only and that, in the case of a data set composed of both personal and non-personal data, it only applies to the non-personal data part of the data set.

However, given the very broad notion of 'personal data' under the GDPR and the fact that the demarcation line between personal and non-personal data is a moving target, it soon became clear that a thriving European data economy cannot be built without including personal data. So strategies were called for to integrate data protection in data sharing legislation. Already the Free Flow of Non-Personal Data Regulation mentioned that, where personal and non-personal data in a data set are inextricably linked, the Regulation 'shall not prejudice' the application of the GDPR. The Open Data Directive (EU) 2019/1024 repeated the same 'without prejudice to' formula, which has since become something like a standard clause in data-related EU legislation, from the Digital Content and Services Directive (EU) 2019/770 to the Proposal for a Data Act, COM(2022) 68 final.

As simple a solution as this appears to be, it fails to really resolve any tension and just shifts the burden of figuring out what this means to those who have to apply the law. This is all the more difficult for those who have to apply the law as the GDPR turns a blind eye on data sharing. The GDPR leaves largely open how data sharing fits into the legal grounds for data processing listed in Articles 6 and 9 and provides for detailed provisions on safeguards only with regard to the passing on of data to processors, but not to third party controllers. Not to speak of the fact that all this is restricted to data protection concerns – however, as has been explained above, the need for 'protection' arises also in the context of sharing non-personal data. Concerns range from national security to law enforcement to trade secret protection, and, indirectly, they may be even more relevant also for the protection of fundamental rights of European citizens than some genuine data protection concerns.

A Data Economy with Organisational, Technological and Legal Safeguards?

In 2017, when the author of this paper was advising the European Commission on how to boost the European data economy, her primary advice – also presented and discussed at an ELI conference in Hull – was establishing and promoting 'data trusteeship' or 'data trusts' in order to integrate personal data in the data economy. The concept was later also supported by the German Data Ethics Commission and other organisations and has meanwhile become one of the most well-known and most promising solutions on the horizon for reconciling data protection with

a strong data economy. These endeavours resulted in the Data Governance Act (DGA) – Regulation (EU) 2022/868 – which, inter alia, sets out a notification and supervisory framework for the provision of data intermediation services. The DGA may not go far enough in several respects, but it is a step in the right direction by stressing the central role of data intermediaries. At the same time, the DGA rightly extends the notion of data that calls for enhanced protection in the context of open public sector data to commercial confidentiality, statistical confidentiality and the protection of intellectual property rights of third parties. Enhanced protection may be provided, in particular, by modifying, aggregating or treating the data by any other method of disclosure control, by providing access to the data only remotely within a secure processing environment controlled by a public sector body, or even only within the physical premises of that body.

All this is part of a whole bundle of measures that aim at creating organisational, technological and legal safeguards for reconciling the need for more data sharing with the need for better protection. This bundle of measures also includes, inter alia, European data spaces as safe and reliable infrastructures for data sharing purposes and supporting the development and deployment of Privacy Enhancing Technologies (PETs). One of the data spaces, the European Health Data Space, will be the subject of an entirely new piece of EU legislation, see the proposal for a regulation COM(2022) 197 final. It is extremely interesting in various respects as, besides addressing primary use of health data (eg by medical professions), it also establishes a highly regulated data access regime for secondary use of health data (eg for developing new drugs or combating threats to public health). This access regime is to be managed by health data access bodies designated by Member States. It includes a limited set of purposes for which health data may be accessed and used, a set of prohibited purposes, and various mechanisms for supervision and the prevention of abuse.

A Data Economy of 'Empowered' Individual Parties?

The Proposal for a Data Act – and, in a certain way, already the Digital Markets Act – marks yet another turn in the quest for opening up old and new data silos by taking a new stab at data portability. The Proposal has been, in various respects, heavily influenced by the ALI-ELI Principles for a Data Economy, for which the author of this paper served as the European Reporter. Data portability refers to rights of a party that can, on whatever basis, consider data held by another party as being also 'their' data (a situation for which the ALI-ELI Principles established the concept of 'co-generated data', which seems to be now widely recognised). Where a party has a portability right, that party may request that the data holder give access to the data to that party or to a third data recipient identified by that party.

The first data portability right in Article 20 GDPR has, for a variety of reasons, never had much effect. This is in particular due to various restrictions in scope and to its static nature as a one-off right to be exercised on rare occasions. Both the Digital Markets Act (for gatekeeper platform services) and the Proposal for a Data Act (for IoT devices and related services provided by large companies) try to significantly enhance data portability. This is mainly by extending portability rights to real-time portability and, in particular as far as the Proposal for a Data Act is concerned, to non-personal data generated by an IoT device or related service.

The underlying idea of data portability is that the party to whom a portability right is afforded has a property-like legally protected interest with regard to the data. It is therefore only logical that the party is free in its discretion whether and to whom and under what conditions they make the data available. This means that the legislator – unlike in the situation of health data under the future European Health Data Space – refrains from defining which third party data recipients may use the data for which kinds of purposes. Rather, this decision is entirely put in the hands of the individual party to whom the data portability right is afforded. Whether the individual party to whom the portability right afforded is actually in the position to make an informed decision, and who will influence this decision (not to say: manipulate – although coercion or manipulation is of course prohibited by the Proposal), or make the decision a condition for delivering a product or service, is largely left open. We may therefore expect that we will be seeing the same phenomena we have seen in the context of consent under the GDPR – a largely fictitious notion of 'autonomy' and 'empowerment' of individual actors which finds little reflection in reality on the ground. In any case, for this to work at large scale, the right data intermediary services need to be in place. This is why one would have expected more references to, and better alignment with, the Data Governance Act,

or maybe a separate section on data intermediaries in the Data Act.

Horizontal and across-the-board data portability is a tool that is not very targeted, ie we do not know for sure who will benefit most from it. This could indeed be European SMEs developing innovative new products and services, it could be big companies in other parts of the world that already now have the best data skills and computing capacities, or it could be malicious actors using insights for espionage, terrorism and hybrid warfare. Theoretically, much of this is prevented by the prohibitions listed under Article 6 of the Proposal, but these prohibitions can easily be circumvented, and malicious actors may anyway care very little about prohibitions on paper. It should be stressed in this regard that Article 5 even includes a limited obligation of, eg, a large European IoT device manufacturer to share trade secrets with any third party chosen by the user, provided 'all specific necessary measures agreed between the data holder and the third party are taken' to preserve confidentiality. A lot of trust will therefore have to be put on the technical protection measures mentioned in Article 11 of the Proposal, and on other safeguards that will hopefully be applied.

Concluding Remarks

The GDPR of 2016 had obviously been modeled on 20th century economies and still turned a blind eye on data sharing. Recent years, by contrast, have seen the EU fostering data sharing and the data economy with a breathtaking number of different pieces of legislation, and at a breathtaking pace. Within less than five years, we have seen, *inter alia*, the Free Flow of Data Regulation, the Open Data Directive, the Digital Markets Act, the Data Governance Act, the Proposal for a European Health Data Space and the Proposal for a Data Act. This is not to mention the numerous legislative activities in specific other sectors, such as the automobile, energy or payment services sectors, or individual data economy-related provisions in other 'horizontal' Acts, such as the provisions on sandboxing in the Proposal for an Artificial Intelligence Act, COM(2021) 206 final. Different units within the EU institutions have been in charge of each of these pieces of legislation, and each of them has chosen different strategies for coping with the fundamental tension between 'open-by-default' and 'protection-by-default'. It is increasingly unclear how all these different strategies and all these different legal regimes will ultimately relate to each other, and to the previous generation of data legislation, in particular the GDPR.

The pace at which things have been moving may not come as a surprise in the light of the significance of interests at stake and of the potential impact one or the other policy choice may have on our societies and of the role European economies – and ultimately Europe as such – will play globally in the 21st century. However, it is precisely because of this that it is of utmost importance to get things right and to act only upon a sound and independent impact assessment. Once large IoT businesses in Europe have been forced to share their data treasures with the rest of the world, for instance, this may trigger developments that can be neither halted nor undone. This is why careful evaluation and consolidation may be called for, to find the right balance between 'open' and 'protection', even if it comes at the price of some delay. What may also be called for is a more holistic approach that takes a fresh look at all the different 'horizontal' pieces of data-related legislation in order to consolidate them – maybe in a future 'European Data Code'.

Online Platform Regulation in the European Union Awaiting the Effectiveness Assessment

By Dr Aneta Wiewiórowska Domagalska

This author stresses the difficulties of transposing EU platforms legislation in an effective way. It underlines how difficult it will be to transpose horizontal Acts (DSA & DMA) as various provisions belong to different areas of law and will therefore require a great deal of coordination at national level to ensure effectiveness. The other online platforms-related provisions are scattered and do not reflect a thought through approach. A challenge will be to have a more holistic approach on platforms legislation at EU level in such a way, however, that ensures greater effectiveness at Member State level.

Introduction

The European Union as the Standard Setter

The European Union aspires to be in the vanguard when it comes to addressing emerging phenomena with a profound impact on markets and society. As illustrated by the General Data Protection Regulation (GDPR)[1] or proposed legislative approaches towards Artificial Intelligence,[2] the European Union consistently aims at creating standards that will influence market standards globally. Online platforms, a social and economic phenomenon that, feeding on technological advancements, redefined global markets and changed the functioning of modern societies, were therefore a natural addressee of the EU law maker.

The transformation brought about by the platformisation of the market created disruptive effects in many areas, and consequently generated multileveled challenges for national and pan-national law makers. While the European Law Institute in its Model Rules on Online Platforms[3] opted for a private law oriented approach that introduced nuanced liability regime for contracts concluded via platforms, depending on the level of influence (control) that the platform operator had over the contract, the EU legislative reaction followed the traditional EU style. It aimed at building upon the existing legal structure (by introducing changes to existing instruments), and at the same time at adopting new instruments (a process that has not come to an end yet).

Given that the first hard law instrument that targeted platforms directly was introduced in 2019 only and the most recent set of rules have not been published yet, it is far too early to evaluate whether the rules are well targeted and effective, but at the same time, it

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 11, 4.5.2016, p 1.

[2] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021 COM(2021) 206 final.

[3] <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf>.

is too late to advocate specific solutions. Considering the legislative density that already exists and the fact that instruments that will affect the platform economy are still early in the legislative pipeline, one can safely assume it will still take time, before a well-grounded evaluation will be possible. For these reasons this paper briefly presents the legislative Acts that apply directly to platforms and limits itself to pointing out potential challenges that stem from the structure and organisation of the platform related rules.

The EU Legislative Style

The approach of EU law (at least within the area classified at national level as private law) is to follow specific market developments, rather than proposing a unifying approach and rules of general application. While such a legislative approach allows for a swift reaction to changing market situations, it also creates challenges at the level of the application of rules. It is only at the moment of the rules' application when inconsistencies due to a fragmented approach or differentiated foundations (from the point of view of national legal systems) of various legal instruments come to light. This is also the case with the EU rules that apply to platforms. While the EU gives the leading role in the field to the proposed Digital Services Act (DSA)[4] and the proposed Digital Markets Act (DMA)[5] (which still have not been published, which makes discussing them quite problematic), they do not exhaust the legal landscape, even if one restricts oneself to provisions directly aimed at platforms. Other applicable rules include Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services,[6] Regulation 2021/784 on addressing the dissemination of terrorist content online[7] and changes introduced to consumer acqui by Directive 2019/2161 on better enforcement and modernisation of Union consumer protection rules (the Omnibus Directive[8]).

The Legislative Landscape

The DSA and the DMA

The legislative package consisting of the DMA and the DSA, that is now in the final stage before publication, sets up a multilayered, multidimensional normative structure to the functioning of platforms in the European Union. The two introduce horizontal rules that complement existing sectoral regulation. The rationale behind them is the traditional one – the internal market perspective (around 10,000 platforms that operate in the EU, over 90% of which are small and medium enterprises, must deal with 27 different sets of national rules, which generates costs that are bearable only for the largest companies).

The DSA

Aimed at amending Directive 2000/31/EC on e-Commerce, the DSA clarifies conditions for liability exemptions, according to which platforms are not liable for users' unlawful behaviour, unless they are aware of it and fail to remove it. It does not, however, provide for a general monitoring obligation when it comes to user content. The DSA introduces rules of an extremally wide range. They include measures to counter illegal goods, services and content (a mechanism that allows the flagging of such content and the establishment of cooperation between platforms and 'trusted flaggers'); obligations regarding traceability of business users; safeguards for users, including the possibility to challenge platforms' moderation decisions; and transparency requirements in relation to algorithms used for recommendations. At the same time, the DSA introduces rules on the protection of minors, crisis response mechanisms in case of serious threats to public health and security, and bans targeted advertising and use of 'dark patterns'.

[4] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.
[5] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.
[6] OJ L 186, 11.7.2019, p 57.
[7] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.
[8] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJEU L 328/7.

In addition, the DSA introduces a separate provision for very large online platforms (VLOPs, with 45 million or more users). They are going to be required to conduct annual risk assessments to identify and mitigate systemic risks – illegal content, negative impact on fundamental rights and intentional manipulation of their services. In addition, they will be obliged to subject themselves to independent transparency and due diligence audits.

The enforcement of the DSA will be primarily in hands of national authorities (the Digital Service Coordinators). When it comes to VLOPs, however, the exclusive power to enforce obligations will be with the Commission.

The DMA

The DMA targets 'gatekeeper platforms', ie, platforms which due to their size have an impact on the internal market, as they are in control of a getaway between business users and final end users and hold entrenched and durable positions. Under the DMA gatekeepers will have a specific responsibility to operate in a way that safeguards open online environment. To ensure that, the DMA will impose certain obligations and restrictions on gatekeeper platforms, in particular – interoperability of messenger services. The DMA will be enforced by the European Commission solely, which 'matches the inherently cross-border activities of the gatekeepers and the objective of the DMA'.[9] The Commission will be able to impose severe sanctions (up to 10% of the company's total worldwide annual turnover or 20% in the event of repeated infringements and periodic penalty payments of up to 5% of the company's total worldwide daily turnover, and additional remedies in case of systematic infringements). The Commission will cooperate with competition authorities, which will conduct investigations to determine non-compliance with the DMA by gatekeepers and report to the Commission, and courts, which will adjudicate damages stemming from non-compliance.

Regulation on Promoting Fairness and Transparency for Business Users of Online Intermediation Services

Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services introduced B2B legislations that specifically targets the online platform economy. The Regulation focusses on 'transparency, fairness and access to redress'. It establishes transparency requirements, some of which are secured by a nullity sanction. The Regulation does not ban specific practices, but focuses on their explainability and the possibility to understand platforms' decisions and the mechanisms governing the functioning of the platform (ie rankings, differentiated treatment, access to data). The Regulation requires a notice period in the case of a termination of services by the platform (a private law angle) and an obligation to provide an internal complaint-handling system and resort to mediation (a regulatory private law).

The Regulation recognises the risks relating to private enforcement by businesses operating on platforms and addresses it by establishing the right of organisations and associations that have a legitimate interest in representing business users and corporate website users, as well as public bodies, to take action to stop or prohibit any non-compliance by the platform of the Regulation. Moreover, the Regulation encourages the drawing up of codes of conduct by platforms and by organisations that represent them (together with business users).

To complement the Regulation, the Commission issued guidelines on ranking transparency pursuant to Regulation 2019/1150.[10] It aims at facilitating compliance with and the enforcement of the Regulation, as well as assisting providers in applying the requirements and helping to optimise the manner in which the main parameters determining rankings are identified and presented to business users and corporate website users.

[9] Questions and answers: Digital Markets Act: Ensuring fair and open digital markets, Brussels 23 April 2022.
[10] Commission notice, Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council, 2020/C 424/01.

Regulation on the Dissemination of Terrorist Content Online

Regulation 2021/784 on addressing the dissemination of terrorist content online, which applies as of 7 June 2022, adopts a completely different approach. It aims at helping counter the spread of extremist ideologies online. Platforms are under an obligation to remove terrorist content referred to them by Member States' authorities within 1 hour. Based on the Regulation, Member States can sanction non-compliance and decide on the level of penalties, proportionately to the nature of the infringement (considering the size of the platform).

A similar angle was employed earlier in a Code of Conduct on countering illegal hate speech online, that was signed on 31 May 2016 by the Commission and Google, Facebook, Twitter, Microsoft hosted services, and joined in 2018 and 2019 by Instagram, Google +, Dailymotion, Snapchat and Jeuxvideo. com. By 2019 the Code covered 96% of the EU market share of online platforms that may be affected by the hateful content.[11] The Code set up rules and community standards that prohibit hate speech and put in place systems and teams to review content that is reported to violate these standards. It requires the review of the majority of the content flagged within 24 hours and the removal or disabling of access to hate speech content, if necessary; regular training of staff; engaging in partnerships and training activities with civil society in order to enlarge the network of trusted reporters; working with trusted flaggers on promoting independent counter-narratives and educational programs; the designation of national contact points, in particular by national authorities, to receive notices; promoting transparency towards users as well as the general public. As follows from the progress report published by the Commission,[12] the Code of Conduct contributed to achieving quick progress, regarding, in particular, the swift review and removal of hate speech content (28% in 2016 and 72% in 2019; 40% of notices reviewed within 24 hour in 2016, 89% in 2019).

Platform Related Changes in Consumer Acquis

When it comes to consumer acquis, it was Directive 2019/2161, the Omnibus Directive, that introduced platform related changes to Directives 2005/29/EC on Unfair Commercial Practices and Directive 2011/83/EU on consumer rights.

The Unfair Commercial Practices Directive now includes, as material information under Article 7(1) for products offered on online marketplaces, information whether the third party offering the product is a trader or not, on the basis of the declaration of that third party to the provider of the online marketplace, and (2) the main parameters determining the ranking of products presented to the consumer and the relative importance of those parameters as opposed to other parameters when consumers are provided with the possibility to search for products offered by different traders or on the basis of the keyword, etc. Also, where a trader provides access to consumer reviews of products, they are obliged to provide information about whether and how they ensure that the published reviews originate from consumers who have purchased or used the product.

Changes to the Directive on Consumer Rights added specific pre-contractual information requirements for contracts concluded on online marketplaces that included: information on the main parameters determining rankings (referring to the Unfair Commercial Practices Directive), whether a party offering goods or services is operating as a trader or not and, consequently, whether the consumer protection rules apply to contracts concluded by a consumer.

The Possible Challenges

Given the stage of development of EU legislation that addresses platforms, it is too late to propose specific legislative options, since legislation has already been adopted, but much too early to evaluate its impact, as the official texts of the DSA and the DMA that have fundamental importance for this area are yet to be published.

[11] https://gs.statcounter.com/social-media-stats/all/europe, as referred to in Information note from the European Commission to the Permanent Representatives Committee/Council on Assessment of the Code of Conduct on Hate Speech on-line, State of Play, Brussels 27 September 2019, 12522/19.

[12] Information note from the European Commission to the Permanent Representatives Committee/Council on Assessment of the Code of Conduct on Hate Speech on-line, State of Play, Brussels 27 September 2019, 12522/19, p 1.

While the most recent legislative platform package (the DSA and the DMA) attempts to introduce comprehensive, horizontal regulation for platforms, the legislative landscape that emerges in the EU will come with its challenges. The characteristics of EU law, combined with the characteristics of the problems created by the platformistation of the market and society, create a combination that is, at the outcome, particularly complicated and will probably require particular efforts of all the engaged parties, to ensure the expected effectiveness to EU law. At this moment, however, in terms of the general overview, one can reasonably focus on the legislative method that has been used to address platforms and point out the potential challenges that can be generated by it. Those comments, in their essence, do not depart from the comments that address EU law in general, as the EU adopted its traditional law-making method to platforms. Yet, the special characteristics of platforms as a social and economic phenomenon, with enormous market power will most probably give it an extra twist.

The legislation introduced by the EU with a view to addressing problems created by the platform economy reflects the diversity of challenges that online platforms create for the market and society. It would, therefore, be utterly naïve to expect that the legislation that aims to address them will be systematic, ie constructed in a way resembling national legal systems. The EU's legislation on platforms, follows the construction of EU norms which at the same time tries fit it into existing structures (consumer acquis, the e-Commerce Directive) and is supplemented by new legislation that at national level belong to various branches of law with different enforcement mechanisms. The Regulation on promoting fairness and transparency for business users of online intermediation services consists of mostly private (regulatory) law (that at national level translates into the law of obligations). The DSA is a conglomerate of private and public law, sometimes tackling one particular issue in a holistic manner that will be very difficult to apply. For example: illegal content (according to the initial proposal), is information, which, in itself or by its reference to an activity, including the sale of products or provision of services, is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law. The DMA is basically a competition law.

This means that at national level, proper enforcement of the EU platform regulation will require coordinated approaches across several branches of law. The lack of recognition at EU level of the public-private law division that exists at national level can instigate potential problems with the effects that private law enforcement is supposed to produce at national level (as proven by consumer law acquis). Private law enforcement, which is left in the hands of individuals whose rights have been infringed, is normally difficult to be taken up against entities with great market power, as is the case with platforms. Here, however, enforcement will be problematic not only for private parties (enforcing the Fairness and Transparency Regulation could mean exclusion from the platform), but also for public enforcement (the impact that platforms have on national economies can contribute to the effectiveness of enforcement at national level). What follows is that the effectiveness of the enforcement at EU level will be of a crucial importance.

Another dimension of the current legislation is the diverse legislative techniques (hard-law, soft-law and self-regulation). Also here, achieving the expected effectiveness will require cooperation and coordination at national and EU levels. Here, however, one more aspect should be considered. Given that VLOPs will be involved in the evaluation of their own impact on the market, it will in fact reinforce their position as private lawmakers, which theoretically speaking was supposed to be prevented by EU legislation.

What it comes down to then is how effective will EU be in supervising and enforcing the new laws. It goes without saying that significant success has already been achieved – simply by managing to adopt the platform rules at EU level that includes a potential for severe sanctions for violations. Now, the question is: 'Will it be possible to establish if there is a need to use those sanctions?'

The Single Market and the Uptake of Digitalisation Platforms, Blockchains and NFTs

By Prof Dr Juliette Sénéchal

Centralised online platforms and decentralised blockchains are two technical, economic and legal realities that are usually analysed separately.

However, while it was initially envisaged that centralised online platforms would be linked to decentralised blockchains to enable payment for products or services purchased on the platform, the current approach may envisage the articulation between the centralised platform and the decentralised blockchain, by means of Non-Fungible Tokens (NFTs), in order to produce a renewed form of exclusivity on digital content or digital services, which holders could use, either in the real world, or in the parallel world of the platform (metaverse).

The use of NFTs raises many questions that are of interest to both industry and government: what are the legal and economic values of the exclusivity conferred? Does this exclusivity have the same meaning in the real world or in a metaverse?

These questions are not currently addressed in the new European instruments regulating digital services or digital assets.

The Birth of the Attention Economy: from the Internet to Online Platforms, Two-Sided Market Interfaces

While the decentralisation of IT infrastructures is at the origin of the creation of the web and the internet, with an operation based on the use of browsers and hypertext links,[1] the plethora of information and offers of products, services and content that have gradually become available on the web has given rise to an 'attention economy',[2] that has in turn given rise to highly centralised technical infrastructures and highly concentrated economic players offering services to classify this plethora of information by targeting recipients on the basis of a massive collection of their personal data, with a view to contributing to the conclusion of e-commerce contracts.

Those online platforms that have become essential not only offer targeted recommendations and advertisements, finely tuned to the needs of the actors they connect, to the point of potentially influencing their consent, but also provide, in addition to their intermediation services, complementary services which, in certain circumstances, may have given them

[1] D Cardon, *Digital Culture,* Presses de Science Po, 2019.

[2] J Tirole, *L'économie du bien commun,* PUF, 2016, p 499; C Zolynski, F Levin and M Le Roy, 'L'économie de l'attention saisie par le droit – Plaidoyer pour un droit à la protection de l'attention', D IP/IT, 2019 No 11, Nov 2019, pp 614-622; Conseil national du numérique, dossier: 'Quels leviers face à l'économie de l'attention?', 13 Jan 2022, available at: <cnnumerique.fr/files/uploads/2022/Dossier%20Attention/CNNum_Votre_attention_s_vous_plait_!_D ossier_VF. pdf>.

the appearance of being much more than simple neutral and transparent 'infomediaries'.

Neoclassical economists, foremost among them Jean Tirole, holder of the prize in economic science in honour of Alfred Nobel awarded by the Bank of Sweden in 2014,[3] has made a major contribution to the conceptualisation of online platforms,[4] interfaces regulating exchanges between two or more groups of economic actors (the group of customers, the group of suppliers, the group of advertisers and data brokers, etc) on so-called two-sided or multi-sided markets.[5] In this sense, Jean Tirole, in one of his books aimed at a wide audience, presents a reassuring vision of an order being built around central pillars, online platforms in their capacity as 'guardians' of the economy,[6] regulating economic actors, while at the same time self-regulating.

The dominant operators that implement these platforms will be called *'gatekeepers'* of pieces of information and offerors of products, services or content in a proposal for a regulation on digital markets dated 15 December 2020, which was provisionally agreed on 25 March 2022 and will soon enter into force,[7] due to their activities as providers of 'core platform services' (online intermediation services, online search engines, online social networking services, video-sharing platform services, non-dial-up interpersonal communication services, operating systems, cloud computing services, and advertising services provided by a provider of any of the core platform services).[8]

From Platforms to Public ... or Private Blockchains

This strong technical centralisation and economic concentration of digital markets has generated a swing towards greater technical decentralisation of IT infrastructures providing digital services, without this being accompanied by genuine economic deconcentration, with the appearance of several large decentralised and globalised blockchain infrastructures. Each of these blockchain infrastructures has no legal personality because it is supported by an epistemic community of computer scientists who are responsible for promoting, preserving and operating, anonymously or pseudonymously, a register/ledger of financial transactions and algorithms that are improperly referred to as 'smart contracts' and for producing new digital representations of values and rights, including cryptocurrencies. The aim of these new platforms, which are both economically concentrated and technically decentralised, is not only to compete with public currencies that are legal tender, issued by states, federations or confederations of states, but also to avoid the use of large private financial intermediaries for the provision of services relating to these financial transactions.[8]

This technical decentralisation of the production of digital representations of securities and rights has given rise to a new swing of the pendulum, the outcome of which is still difficult to ascertain, initiated by the major online platform operators,

[3] The notion of an online platform operating in a two-sided market was conceptualised by J Tirole and JC Rochet in the 2000s in the light of competition issues: J Tirole, JC Rochet, 'Platform, Competition in Two-Sided Markets', Journal of the European Economic Association, vol Rochet in the 2000s, in the light of competition issues: J Tirole, JC Rochet, 'Platform, Competition in Two-Sided Markets', *Journal of the European Economic Association,* vol 1, No 4, 2003, pp 990-1029; J Tirole, JC Rochet, 'Two-Sided Markets: A Progress Report', *Journal of Economics,* vol 37, no 3, 2006, pp 645–667; J Tirole, JC Rochet, 'Competition Policy in Two-Sided Markets, with a Special Emphasis on Payment Cards', in P Buccirossi, *Handbook of Antitrust Economics,* MIT Press, 2008, pp 543–582.

[4] On this notion, J Rochfeld and C Zolynski, 'La 'loyauté' des 'plateformes', quelles plateformes, quelle loyauté?', *D IP IT*, Nov 2016, p 520.

[5] On the notion of a two-sided market, N Colin, A Landier, P Mohnen and A Perrot, 'Économie numérique', *Les notes du Conseil d'analyse économique*, No 26, Oct 2015, p 8 et seq.

[6] J Tirole, *L'économie du bien commun, op cit*.

[7] Proposal for a Regulation on fair and contestable contracts in the digital sector (Digital Markets Act)–COM 2020 842 final (DMA); <https://www.consilium.europa.eu/fr/press/press- releases/2022/03/25/council-and- european-parliament-reach-agreement-on-the-digital-markets-act/> 8 Art 2 of the DMA proposal.

[8] J Sénéchal, *'Blockchains* 'publiques', *smart contracts*, organisations autonomes décentralisées et gouvernance', in H Jacquemin, A Cotiga and Y Poullet (dir.), *'Les blockchains et les smart contracts à l'épreuve du droit',* Larcier, 2020, p 51–96.

who are technically centralised and economically concentrated, and who have formed a consortium with a view to creating a new register/ledger. This register/ledger could complement their activity of providing intermediation services for the supply of products, services or content and make it possible to avoid the use of cash to pay for them.[9] While one of the main projects seems to have been abandoned in January 2022, the articulation between online platform operators and blockchains is raising new questions through the recent appearance of Non-Fungible Tokens (NFTs). The articulation between the centralised platform and the decentralised blockchain, by means of NFTs, is no longer used to allow payment for products or services purchased on the platform, but to offer a renewed form of exclusivity on digital content or digital services, either in the real world or in the parallel world of the platform (metavers).

From Platforms and Blockchains to Non-Fungible Tokens

Beeple: Professor of Computer Science and Mathematics Jean-Paul Delahaye, introducing the notion of NFTs, states the following: *'When you first hear about NFTs (non-fungible tokens) and the extravagant sums of money that are exchanged to obtain them, you get the feeling that you are dealing with a collective madness or a scam. How can a digital token associated with a digital image file that is freely available to everyone buy itself for $69 million, as was the case for the NFT of artist Beeple's digital work Everydays: the First 5000 Days! And there are many other examples. Yet it is not possible that so many people and money are rushing into irrational actions of valuation for 'things' that would be worth nothing!'*[10]

An abyss of questions: From a contractual point of view, finding the meaning of the legal exchanges that take place in relation to the NFTs implies confronting an abyss of questions of qualification ... Which qualification should the contractor receiving the NFT receive? Is he or she a consumer, a professional, a purchaser, a client, a speculator, a donor or a victim?

Which qualification should the contractor providing the NFT be given? That of author, copyright holder, influencer, vendor, supplier, online platform operator providing an intermediation service, marketplace, digital asset service provider or crypto-asset service provider?

How should the contract formalising this exchange be classified? Is it a sales contract, a contract for the provision of digital content and services, a contract for the provision of financial services or a contract for the provision of services on digital assets?

What exactly does the contracting party who receives an NFT get in exchange for cryptocurrencies or fiat currencies: a line of code, an absolute intangible asset, a right in rem, a personal right, a line of code referring to an underlying tangible or intangible asset or to a person's reputation, an accessory to a right to an underlying item (tangible or intangible asset) or to an overlying item (service), a category of evidence, a 2.0 or 3.0 title deed, the means of appropriating the body or fame of a physical person, the only means of securing one's virtual life in a metaverse? On the side of the *'buyer'* of the NFT, does the NFT really offer an additional and distinct advantage from the real or personal right conferred by contract? How, for example, could an NFT in particular confer a form of exclusivity in relation to a digital work of art that circulates and is otherwise duplicable more or less freely on the Internet? Would the NFT really only be of interest to this *'purchaser'* in the hypothesis of a metaverse? Indeed, metaverses have the ambition of converging digital technologies to create a virtual, persistent, interactive and immersive world,[11][12] a heterotopia[13] which could need a 'cadaster', a virtual register or ledger (of the blockchain type), on which it could be recorded, via an NFT, not only the

[9] L Nardon, 'The Biden administration could well put an end to the libertarian dream that the launch of cryptocurrencies has been for some', *Le Monde*, 3 Dec 2021, available at: <www.lemonde.fr/idees/article/2021/12/03/l-administration-biden-pourrait-bien-mettre-fin-au-revelibertarien-qu- a-ete-pour-certains-le-lancement-des-cryptomonnaies_6104589_3232.html>.

[10] JP Delahaye, Beyond Bitcoin, 8. Central Banks and NFT, p 200, Dunod, 2022.

[11] P Guitton, N Roussel, Le métavers, quels métavers ?, blog binaire du journal Le Monde, 25 February 2022 (1/2) and Le métavers, quels métavers?, blog binaire du journal Le Monde, 3 March.

[12] (2/2).

[13] M Foucault, Le Corps utopique, Les Hétérotopies, Nouvelles Éditions Lignes, 2009; Ph Sabot, 'Langage, société, corps Utopies et hétérotopies chez Michel Foucault', *Materiali Foucaultiani*, vol 1, 1, 2012.

beneficiaries of a form of exclusivity over a parcel of this virtual territory, but also the beneficiaries of a form of exclusivity over the digital content, works of art, images or games that would be exhibited within this virtual parcel. In other words, the meeting of a metaverse and a blockchain could contribute to the emergence of a new normative order, competing with state legal orders as described by Santi Romano,[14] and which would depart from the legal requirements of these state orders, in order to allow effective forms of exclusivity to be conferred on a digital asset *via* an NFT.

What exactly does the contractor, who receives an NFT, get in exchange for cryptocurrencies or fiat currencies? Is it a digital content, a digital service, a financial service, a digital asset or a crypto- asset …?

This last issue is likely to be further complicated by the entry into force of the future MiCA Regulation, which will amend the French Monetary and Financial Code. Indeed, under the terms of the provisional political agreement reached on this text by the three European institutions, it appears that NFTs are to be excluded from the material scope of the MiCA Regulation, the regulation governing crypto-assets, the European counterpart to the French concept of digital assets, and which will lead to profound changes to Articles L 54-10-1 et seq of the Monetary and Financial Code,[15] relating to the nature and regime of these digital assets.

From the *nexus* of technical operations to the duality of contracts and platform roles: To answer all these questions, it is important to highlight the duality of the contracts present on the websites of online platform operators (of the marketplace type) dedicated to NFTs.[16] An analysis of the technical operations carried out on NFT trading platforms highlights the fact that the platform operator fulfils a dual contractual role, not only as the issuer of the NFT, but also as an intermediary in the *'sale'* or *'resale'* of the complex contractual objects consisting of the NFT and a reference to an *'underlying'* or an *'overlying'* item, or possibly the NFT and rights to the *'underlying'* or *'overlying'* item on the basis of which this NFT was created.

The platform operator as issuer of the NFT: The breakdown of the technical operations relating to the NFT highlights the fact that a prerequisite for its circulation, in return for payment, is its issuance via a centralised platform operator. NFTs are *'nonduplicable and individually identifiable tokens; they are said to be 'non-fungible' ... This can be done by associating to each of the issued tokens a unique number, or information that distinguishes it, these numbers or information being part of the token, which is an item on a registry associated with a specific account. The registry will follow the tokens; they will be objects of the world; they will move from one account to another, but at any given moment each token will be unique and deposited in a specific account, also unique ....Most often, NFTs are created by smart contracts, and quite often, it is the Ethereum blockchain ... that carries it ... The issuance of NFTs is a process that is not totally decentralised because ... an issuer is needed ... The issuer is a trusted third party. The circulation of the NFT benefits from the decentralisation of the smart-contract that allows its resale and the blockchain that manages it. However, because of the issuer, an NFT is never fully decentralised. We are therefore still in the situation of a partially distributed application, but with a privileged actor who is a trusted third party, the issuer.'*[17]

[14] Romano, *L'ordre juridique*, Dalloz, coll Tiré à part, comments by JS Bergé, 2015.

[15] Council of the European Union Communiqué of 30 June 2022, Digital Finance: Agreement on the EU Regulation on Crypto-Assets (MiCA): 'Non-fungible tokens (NFTs), ie digital assets representing real objects such as works of art, music and videos, will be excluded from the scope of the MiCA Regulation unless they fall within the existing categories of crypto-assets. Within 18 months, the European Commission will be invited to prepare a full assessment and, if deemed necessary, to evaluate the need to propose a specific regulatory regime for NFTs and to address the emerging risks of this new market', available at: <https://www.consilium.europa.eu/fr/press/press- releases/2022/06/30/digital-financeagreement-reached-on-european-crypto-assets-regulation-mica/>.

[16] Eg OpenSea (https://opensea.io/), Rarible (https://rarible.com/), Mintable (https://mintable.app/), Nifty gateway (https://niftygateway.com/what-is-an-nft).

[17] JP Delahaye, Beyond Bitcoin, 8 Central Banks and NFT, op cit, pp 201–203.

The platform operator as an intermediary in the *'sale'* of the complex contractual object consisting of the NFT and a reference to an *'underlying'* or *'overlying'* item or possibly the NFT and a right to the said underlying and overlying Item: At the stage of post-issuance circulation, the prerequisite is the existence of an NFT value. However, *'for the NFT to have a value, it must be attached to something specific that personalises it ... Billions of NFTs can be created without any problem, but it is unlikely that they can be sold without being linked to something specific. The trusted third party, in creating the token, will therefore generally establish a link between the token issued and the a priori holder of rights to a digital artistic creation or a digital object (eg a tweet) or even a non-digital object. If it is a digital creation, as in the case of Beeple's work, the internet address of a page where the digital work is deposited can be entered in the NFT; it would be too costly in terms of memory space to deposit the entire work in the NFT and therefore on the blockchain that manages it. In the NFT, it will also be possible to place an imprint of the work'.*[18]

What will be circulated after the NFT has been issued, via the centralised platform operator, will therefore be a set formed by the NFT and the element that personalises it, an element that can be of many kinds. It may be a reference to or a right to a pre-existing underlying item, such as an intangible or tangible asset, a person (one thinks of the arm of a tennis player whose advertising fate has been sealed by an NFT) or it may be a reference to or a right to a later *'overlying'* item, such as a future experience, a future service (a *chat* with one's favourite star) or a piece of another person's fame (a famous sportsman or woman), etc.

In this ecosystem, the decentralised blockchain is only a means an instrument for the issuance, but also for the circulation of NFTs.

Both the issuance and circulation of this NFT presuppose the existence of a key operator, centralised by nature, the online platform operator, through which the NFT is issued and then potentially circulates repeatedly. This is a seemingly strange situation in which the manufacturer of *'the thing'* is also the recurrent intermediary for its *'sale'* and *'resale'.*

Two Categories of Contractual Relationships

This situation gives rise to a number of quite distinct contracts, each dealing with a distinct contractual subject matter:

- the NFT issuance contract between the issuing platform and the creator of the NFT, who may have rights to an *'underlying'* or *'overlying' item*;
- the triangular contractual relationship whereby the platform acts as a simple intermediary in the *'sale'* (or *'resale'*) between the *'seller'* and the *'buyer'* of the complex contractual object composed of the NFT and a reference to or rights on an *'underlying'* or *'overlying'* item.

The triangular contractual relationship between the NFT exchange platform, the *'seller'* and the *'buyer'* concerns a complex contractual object consisting of the NFT and the reference to an *'underlying'* or an *'overlying'* item or consisting of the NFT and the rights on an 'underlying' or an 'overlying' item. This contractual relationship not only highlights the question of the legality of this complex contractual object, but also the growing influence of consumer law, regardless of the qualification finally chosen to apprehend this relationship between the *'seller'* and the *'buyer'* under the auspices of the platform, ie the contract for the provision of digital content or services or the contract for the provision of financial services or crypto-assets.

[18] Ibid, JP Delahaye, Beyond Bitcoin, 8 Central Banks and NFT, pp 202–203.

Updating Product Liability for the Digital Age*

By Prof Dr Bernhard A Koch

Products and markets have changed substantially since the original Product Liability Directive was drafted and introduced. A recent draft of a revised Directive aims at adjusting the liability regime to the digital age. This is a first brief assessment of the key changes proposed.

Evolution of Products and Markets

The 1985 Product Liability Directive (PLD)[1] was drafted in the mid-1970s,[2] long before the advent of private access to the Internet and even before the arrival of affordable personal computers on the market. Manufacturers finalised their products before these entered the stream of commerce and thereby gave up influence and control over the fate of their output. It therefore made perfect sense at the time to mark the moment when a product was put into circulation as the turning point which was decisive for attributing the risks of potential defects that the products may subsequently manifest. Every feature (both positive and negative) a product had at that very moment or earlier could fairly be presumed to have originated from within the sphere of the producer, and any subsequent modification was obviously no longer within the latter's control. Once software reached the consumer market, it was distributed on tangible disks, again finished once saved on that carrier, with no further influence of the developer on its features thereafter.[3] Needless to say, products and markets have substantially changed ever since.

Key Moment of the Original Directive No Longer Equally Relevant

'Many products available today have characteristics that were considered science fiction in the 1980s.'[4] Purely digital products are traded purely digitally online. Even types of products that were already available in the 1970s now have features that were unimaginable at the time, often allowing the manufacturer to either directly alter them once the products are in the hands of the final users or at least give the latter the possibility to install updates provided by the original manufacturer, blurring or even eliminating the relevance of the moment when the product was first put onto the market as a determinant of who should bear the risks of

---

* The European Law Institute has already expressed its position on the need to adjust the current product liability regime in several documents: Guiding Principles for Updating the Product Liability Directive for the Digital Age (ELI Innovation Paper Series (2021): <https://europeanlawinstitute.eu/fileadmin/user_upload/ p_eli/Publications/ELI_Guiding_Principles_for_Updating_the_PLD_for_the_Digital_Age.pdf>, hereinafter 'ELI Guiding Principles'); European Commission's Public Consultation on Civil Liability: Adapting Liability Rules to the Digital Age and Artificial Intelligence (Response of the European Law Institute (2022): <https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Public_Consultation_on_Civil_ Liability.pdf>); ELI Draft of a Revised Product Liability Directive (2022): <https://www.europeanlawinstitute.eu/ fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf>, hereinafter ELI Draft PLD).

[1] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administra-tive provisions of the Member States concerning liability for defective products [1985] Official Journal (OJ) L 210/29, later amended by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 [1999] Official Journal (OJ) L 141/20.

[2] The first draft was published in 1976: Proposal for a Council Directive relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective prod-ucts, COM(76) 372, OJ C 241, 14.10.1976, 9–12.

[3] It was therefore easy for Lord Cockfield on behalf of the Commission to confirm in 1988 that 'the Directive applies to software in the same way … that it applies to handicraft and artistic products' (OJ C 114, 8.5.1989, 42), as it was at the time believed to always be 'incorporated into another movable', ie saved on a disc or pre-installed on some gadget.

4 [Fifth] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), COM(2018) 246 final, 7.5.2018, 1.

potentially harmful aspects of the product. Resort of the moment of entry into the market is therefore questionable even though it can be determined that such risks were already inherent in the product at the time it was distributed or that they were added by a subsequent update. Resort to the above moment also makes it more difficult to rely on presumptions regarding in whose sphere the origin of the harmful features of the product was, as it may well have been external influences or problems attributable to the sphere of the user that made the product cause damage, but since the original manufacturer retains at least potential influence on the product until then, one can no longer draw a sharp line at the moment of initial distribution.

The magic moment of the PLD at present has therefore lost its relevance even for products of a kind already available in 1985, and for that reason alone it is imperative to adjust the PLD accordingly.

Are Purely Digital Products Within the Scope of the Directive?

The second key change needed is an express clarification whether products falling under the PLD need to be tangible, or whether it also extends to purely digital products. This is not as equally urgent as the former aspect, which undoubtedly already affects products within the PLD's scope. Denying its application to digital products would not affect the viability of the PLD, as one could imagine a separate instrument tailormade for software and other non-tangible items. However, this would clearly only be a second-best solution, if only for the problems of drawing the line between those (then two) liability regimes – would updates to the firmware of a hardware product sold separately by the manufacturer of the latter fall under the PLD or within the scope of the alternative regime? It is for that reason alone preferable to expand the scope of the PLD itself to include (purely) digital products as well.

Key Changes Proposed by the Recent Revised Draft Directive

Both concerns mentioned so far at least to some extent have already been taken care of by the proposed revised Product Liability Directive (rPLD):[5]

- The definition of a 'product' in art 4(1) rPLD now expressly includes 'electricity, digital manufacturing files and software'. By defining a 'component' as 'any item, whether tangible or intangible, or any related service, that is integrated into, or inter-connected with, a product by the manufacturer of that product or within that manufacturer's control' in art 4(3) rPLD, the concerns addressed by Guiding Principle 4 of the ELI Guiding Principles[6] seem to be adequately addressed.

- Art 6(1)(e) rPLD replaces the exclusive focus on the moment when the product was initially put into circulation in cases 'where the manufacturer retains control over the product after that moment' with 'the moment in time when the product left the control of the manufacturer'.[7] Also, the defence in art 10(1)(c) which allows the producer to escape liability if it was 'probable that the defectiveness that caused the damage did not exist when the product was placed on the market' is unavailable according to art 10(2) rPLD if 'the defectiveness of the product is due to' (inter alia) 'software, including software updates or upgrades' (lit b) or 'the lack of software updates or upgrades necessary to maintain safety' (lit c). However, as it stands, it seems that the victim will need to prove that the defect was in the software in order to challenge the otherwise given defence.[8] Also, the long-stop limitation periods in art 14(2) and (3) rPLD still starts when the product was 'placed on the market' even if the manufacturer continues to supply it with updates.

[5] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.
[6] It reads: 'The definition of 'product' in the PLD should be updated to cover (i) the combination of goods with digital elements and (ii) digital content and digital services supplied as 'digital products'.'
[7] Cf also art 6(1)(e) rPLD, which modifies the development risk defence inasmuch as the relevant time for identifying the state of scientific and technical knowledge and its potential to discover the defectiveness of the product is expanded to 'the period in which the product was within the manufacturer's control'.
[8] Cf art 10 of the ELI Draft PLD (fn*) which in lit a requires the defendant to prove that the defect 'neither existed at the time when they made the product available on the market, nor originated in any authorised up-date, nor was due to their failure to provide an update as required by Union or Member State safety laws'.

Addressing the Peculiar Features of Artificial Intelligence (AI)

If the scope of the PLD is expanded to include digital products as currently proposed by the rPLD, necessary follow-up questions arise, in particular with regard to AI and its peculiar features. Self-learning and self-adjustments are core elements of this technology, and if these built-in abilities themselves (without ongoing input by the original manufacturer) evolve in a way that renders the product harmful, this development seems to be no malfunction at first sight as the AI was purposefully given the ability to alter itself in that way. Particularly in light of possible flaws of the initial design of the AI and the question of the extent to which the algorithm should have had built-in barriers for such adverse changes, this primarily triggers the need for adjusting the notion of defectiveness, especially if consumer expectations play an ongoing role in that regard. Art 6(1) rPLD indeed addresses that problem and in lit (c) specifically lists 'the effect on the product of any ability to continue to learn after deployment' as one decisive factor determining 'the safety which the public at large is entitled to expect'.

The 'blackbox' nature of AI and more generally difficulties for victims to identify the true source of their harm particularly if software (including updates thereto) may have contributed thereto justify amendments to the PLD with respect to the claimant's burden of proof. Also in this regard the proposed rPLD already suggests some improvements of the claimant's position, starting with a requirement to disclose internal information (presumably including data collected by the AI and by the sensors etc that feed it with data) in art 8(1) rPLD: as long as the claimant can show 'plausibility of the claim for compensation', they can require the defendant 'to disclose relevant evidence that is at its disposal' (though subject to some qualifications in the following paragraphs). While this language is not limited to digital products, the aforementioned concerns would at least to some extent be met.

Burden of Proof

More importantly, art 9 rPLD shifts the burden of proof in two very significant scenarios. Art 9(2)(c) rPLD proposes a presumption of defectiveness if only the claimant can prove 'that the damage was caused by an obvious malfunction of the product during normal use or under ordinary circumstances'. More specifically aiming at (but not limited to) AI and similar digital technologies, art 9(4) reverses the burden of proving the defectiveness of the product and/or its causal link to the damage where 'the claimant faces excessive difficulties, due to technical or scientific complexity'. This is triggered as long as the claimant can also show that 'the product contributed to the damage' and that 'it is likely that the product was defective or that its defectiveness is a likely cause of the damage, or both'. The latter in particular effectively seems to lower the standard of proof in those jurisdictions which otherwise insist on a higher degree of probability than just 'likely' when determining whether the claimant's assertions are true.

Cybersecurity

A more general problem that modern-day products face is linked to their connectivity features. Cybersecurity issues are sometimes alluded to in the draft rPLD. In particular, art 6(1)(f) rPLD expressly mentions 'safety-relevant cybersecurity requirements' as key factors to consider when assessing the defectiveness of the product. This is already a given whenever EU or Member State law requires manufacturers to fortify their products against potential hacking or similar tampering.[9] More generally, one should not expect manufacturers to bear all cybersecurity risks. After all, these stem from intentional harmful conduct by third parties (hackers), and the extent to which the consequences of their wrongdoing should be borne by those who produce the attacked products is a legal policy question. Cybersecurity risks are large-scale problems which may not entirely be solved at the level of individual parties. One needs to bear in mind that producers of cars at present would also not be held liable for the harm caused by rock avalanches as long as their products provide the safety to be expected against the impact of the forces of nature on the vehicle. In such cases consumers would at best merely expect their cars to withstand individual rocks falling on them, but certainly not a massive rockslide. Buffering the consequences of criminal conduct (ultimately) through insurance premia divided among all buyers of the product does not seem to be the one-size-fits-all solution to the challenges of online hacking. It remains to be seen whether and the

[9] Cf recital 38 rPLD.

extent to which courts will take the proposed art 6(1)(f) rPLD seriously and in a manner that balances the competing interests at stake.

First Evaluation of the Current Proposal

In the little time available between the publication of the rPLD and this webinar, the proposed Directive seems to have taken a major leap in the right direction. Some of its language will still need to be put under closer scrutiny in light of the manifold scenarios that one may imagine. Since my task was only to specifically address the challenges impacting upon the uptake of digitalisation, I did not address some of the remarkable changes (but also the absence of changes) which are not peculiar to the digital world. These include the long-overdue abolition of the 500 € threshold of art 9(b) PLD, which is laudable, but also the retention of the development risk defence in art 10(1)(e) rPLD, which is deplorable, particularly because it continues to ignore the need to specify 'the objective state of scientific and technical knowledge' in times of Google and DeepL, if retained. Two further aspects of the definition of compensable harm in art 4(6) rPLD still deserve highlighting, though. As suggested inter alia by ELI Guiding Principle 7, art 4(6)(c) rPLD expressly extends the notion of 'damage' within the meaning of the rPLD to include 'loss or corruption of data that is not used exclusively for professional purposes'. Furthermore, while art 9(b)(ii) PLD was not given up entirely, at least art 4(6)(b)(iii) rPLD only excludes harm to 'property used exclusively for professional purposes' (emphasis added), thereby clarifying that dual-use property will be compensated under the proposed new regime.

ADM (Automated Decision-Making) and Algorithmic Contracts

By Prof Dr Teresa Rodríguez de las Heras Ballell

The potential of automation for the future of digital society as well as their inherent risks have not gone unnoticed for the EU. References to automation are scattered in EU legislation and a set of principles precipitate in legal provisions included in legislative proposals and recently adopted instruments, but a consistent, coherent, and all-embracing body of principles/rules governing ADM systems is still lacking.

A Digital Single Market for ADM will not thrive in the absence of a unified, clear, predictable, consistent, highly-coherent and well-balanced legal framework in the Union. To achieve this, efforts are to be made to review legacy rules, test the adequacy of our acquis to embrace and enable the use of ADM (ADM-readiness test), ensure consistency of EU instruments and prevent fragmentation at national level, and identify gaps and inconsistencies likely to raise barriers, increase 'legal distance' in the common market, or hamper innovation.

Unleashing the Potential of ADM: Benefits and Risks

The intensive and extensive use of algorithms has pervaded an immense and growing variety of tasks, activities, and decision-making processes in the digital economy. In an over-informed society, automation is key to manage complexity, curb uncertainty, and perform mass activities at an affordable cost and to ensure effectiveness in the processing of data, information, and digital content. From basic tasks (searching, comparing, ordering, prioritising), to more sophisticated added-value services (profiling, personalising, recommending, multi-attribute rating, filtering, content moderation, algorithmic management, complaint handling), they are performed by algorithm/AI-driven systems.

Algorithmic automation provides efficiency, dramatically reduces transaction costs, streamlines processes, and assists decision-making in complex contexts.

Rating, ranking, recommender systems or comparators are extremely helpful tools assisting users in adopting informed decisions. ADM systems' outcomes (ranking, rating, recommendation) are employed by users as complexity-reducing inputs in their decision-making processes. Users rely on recommended items, top-rated vendors, or highly ranked products and adopt contractual decisions accordingly. In that regard, the consent-forming process is influenced by the ADM's outcomes. Concurrently, non-recommended sellers, downrated products, or low-ranked offers are negatively impacted and affected in their competitive position.

Profiling, personalising or contextualising solutions enable companies to successfully reach their prospective customers with targeted communications, personalised offers, and customised services. Thus, ADM are key components of business strategies and commercial campaigns. Proposals to deal and offers are based on such personalising mechanisms and contractual terms and conditions are adapted to such customising goals.

Algorithms are also instrumental in rendering flagging, filtering, content moderation or content removal feasible, affordable, and effective. These activities are crucial in the digital economy and play a key role in the platform economy. Flagging, filtering,

and content moderation are complex, multifactorial decision-making processes that have substantial effects on the interests, rights, and legal status of affected persons and third parties. Removing or demoting content or closing users' accounts on grounds of illegality or incompatibility with community policy entails limiting certain rights.

Hence, along with the remarkable benefits and the undeniable potential, significant risks and undesired effects of algorithm-driven systems for our society are becoming more and more perceptible. Algorithmic logic may perpetuate past choices and preferences, radicalise speech and polarise public opinion in echo chambers and ideological silos, reduce diversity, enlarge bias and discrimination divides, standardise behaviours on the basis of stereotypes, lead to opaque decisions that leave victims undefended, stoke the virality of fake news, encroach upon free speech, or distort consumers' choices with misleading ratings, rankings, dark patterns, or recommendations.

Single Market for ADM: In Need of a Unified Legal Framework

The potential of automation for the future of digital society as well as their inherent risks have not gone unnoticed for the European Union. On the contrary, the principles of transparency, explainability, risk assessment, and human oversight of algorithm-driven systems are crystallising in EU legislative initiatives and in more recently adopted instruments.

Nonetheless, a Single Market for ADM will not thrive in the absence of a unified, clear, predictable, consistent, highly-coherent and well-balanced legal framework in the Union. To achieve this, efforts are to be made to review legacy rules, test the adequacy of our acquis to embrace and enable the use of ADM (ADM-readiness test), ensure consistency of EU instruments and prevent fragmentation at national level, and identify gaps and inconsistencies likely to raise barriers, increase 'legal distance' in the common market, or hamper innovation.

Even if important guiding principles can be inferred from the legislative scene and useful rules on algorithm-based systems and automated means can already be found in Union legislation, they do not form a consistent, coherent, and all-embracing body of principles/rules governing automated decision-making systems. A sound, clear legal framework for ADM is instrumental to unleashing ADM potential, and to fortifying the Single Market.

Uncertainties about the applicability of existing rules on ADM or the principles guiding a systemic use of algorithms and AI systems for commercial purposes and in economic activities make predictability difficult.

Yet, provisions dealing with ADM in Union legislation are scattered, apply to different extents and scopes, may overlap or even clash, and provide a fragmented, an inevitably incomplete, legal framework for ADM in the Union.

Inter alia, Article 22 GDPR[1] on decisions based solely on automated processing, including profiling, has long been the centerpiece of the EU's legal approach to ADM and embodies its main policy goals. But it is not its goal to set out a complete legal framework for the use of automated processing. Neither the natural scope of the Regulation, nor the content of the provision itself invite such high expectations. It is not indeed a legal regime for ADM.

The Platform-to-Business Regulation (P2B Regulation)[2] confirms that policy by laying down transparency requirements in the provision of ranking services. Likewise, algorithmic accountability, and transparency do also crosscut some obligations laid down in the proposed Digital Services Act (DSA)[3] – recommender systems, terms and conditions, content moderation. Risks arising from algorithmic decisions (automated decision-making) are acknowledged throughout the DSA proposal and accordingly, are included in the risk assessment and are subject to risk-mitigating measures as applied to very large online

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] 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.
[3] Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

platforms. The interplay between the P2B Regulation and the DSA raises multiple issues that require further and careful consideration.

Besides, the proposed Artificial Intelligence Act (AI Act)[4] represents a risk-based approach to AI systems and the consolidation of certain principles aimed at guiding the placing on the market and the use of AI on the basis of the intended purpose of the system concerned.

Yet, the recent Proposal for a Directive on improving working conditions in platform work[5] (Directive on Platform Work) devotes its Chapter III to algorithmic management under the principles of transparency, human monitoring, and human review of significant decisions.

All the references above show that automated decision-making systems are attracting regulatory attention in the EU agenda. Nevertheless, rules related to automated processes are scattered in different pieces of legislation, partial in their scope, and unharmonised. Some rules are sector-specific, while others apply solely to certain types of automated systems (rating, recommender systems, algorithmic management). Besides, despite the fact that the main policy goals are enshrined in a number of legal provisions (transparency, explainability, human monitoring), their implementation in practice is still uncertain, may be unfeasible or too costly, or become significantly complex.

With the aim of contributing to this exercise, ELI adopted 12 Guiding Principles for Automated Decision-Making in the EU[6] aimed at providing further guidance on establishing a legal framework for automated decision-making (ADM) in the EU.

The Use of ADM throughout the Contract Lifecycle: What is Needed to Consolidate the Digital Single Market?

The second dimension of the use of algorithms and AI systems in decision-making is the incorporation of such systems in the contract lifecycle and for contractual purposes. AI-driven systems can assist consumers in comparing offers, in negotiating and concluding contracts or in renegotiating contractual conditions; sophisticated smart products (smart fridge, smart home, autonomous vehicle) can enter into contracts in the name and on behalf of the consumer – doing shopping, renewing a subscription, reserving opera tickets, or booking a parking space before arrival – or smart contracts can self-execute remedies in cases of default – starter interruption of a device, transfer of crypto assets, removal of content, closing of an account.

A number of legal questions are raised, with special, but not exclusive, consideration to consumer protection legislation.

It has to be considered whether EU consumer protection acquis fully embraces the use of ADM throughout the contract life cycle and whether it is ready to apply to algorithmic contracting. An ADM-readiness test of the main consumer protection instruments in the Union is needed, as a first step to calibrate the actions required, if any, and the extent of such interventions – no action, clarification of existing rules and concepts (guidance), interpretation efforts (guidelines, and case law), gap-filling exercise, new rules).

ELI's Project on Guiding Principles and Model Rules on Algorithmic Contracts[7] aims at contributing to

[4] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final.
[5] Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work, COM(2021) 762 final, 9.12.2021.
[6] <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Innovation_Paper_on_Guiding_Principles_for_ADM_in_the_EU.pdf>.
[7] <https://europeanlawinstitute.eu/projects-publications/current-projects/current-projects/algorithmic-contracts/>.

this endeavour. It is planned in two phases that run in parallel. The main output of Phase 1 will be an annotation of existing EU consumer law directives indicating their degree of 'ADM readiness' and identifying those elements which may need to be amended or clarified: pre-contractual information – to the consumer or to the AI system; the AI system may collect and process information from other sources – right of withdrawal, form of the contract, durable medium (voice, chatbot), in plain and legible language, self-executed remedies, etc.

In Phase 2, a coherent set of principles and model rules for the use of ADM systems in contractual relations (expanding from B2C to B2B, M2M, P2P) will be drafted.

Some key contract law issues require proper consideration: validity and enforceability of contracts negotiated, concluded and/or performed on an automated basis; allocation of legal effects; attestation legal capacity; legal treatment of consent and identification of defects in consent; risk allocation in case of defective operations; duty to inform; right to object.

Additionally, liability rules should be revisited, revised where needed, and then aligned with the distinctive characteristics of AI systems – opacity, openness, autonomy, vulnerability, data-dependence. A modernised Product Liability Directive to effectively embrace smart products accompanied by specific rules for damages caused by AI system will complete the picture and underpin a Digital Single Market for ADM.