1. Digital platforms: protagonists of the self-age

1. WHAT WE TALK ABOUT WHEN WE TALK ABOUT DIGITAL PLATFORMS

The first issue to face is giving a definition. It is not difficult to understand what a digital platform is. It is harder, however, to give a suitable definition of it, for at least two reasons.

The first is that the market provides services, to which the platform becomes instrumental: there is no conceptual idea of a platform in itself, which can then find sectoral applications. Going back from practice to a technical formula is therefore not easy, since the constituent element risks being so general that it becomes useless for classification purposes.

The second reason is that the definition is always functional to an objective: the engineers qualify the digital platform based on the technical characteristics, the economists focus on the market, the jurists consider the balancing of protected interests operated by the legislator and from private autonomy, and therefore highlight regulatory and contractual aspects.

1.1 Definitions from the Technological Perspective

The engineers’ main aim is to open the technological black box of digital platforms and understand their technical and innovation content. Studies adopting this view focus on the technical developments and functions. Hence, a platform can be defined as an extensible codebase of a software-based system complemented by third-party modules;¹ a building block that provides an essential function to a technological system and serves as a foundation upon

which complementary products, technologies, or services can be developed; a set of components used in common across a product family whose functionality can be extended by applications; a set of subsystems and interfaces that form a common structure for/from which derivative applications can be developed and distributed. Key aspects, depending on the definition, may be: ease of use and immediate appeal for users; trustworthiness and security (clear terms and conditions are necessary as well as privacy protection and guarantees in terms of intellectual property and data ownership); connectivity through the use of APIs that allow third parties to extend the ecosystem of the platform and its capabilities; facilitation of exchanges between users (producers and consumers); providing value to the community and as a function of the size of the community (the bigger the community, the more value the platform can provide to all parties involved); ability to scale up without causing performance degradation.

Digital platforms are simultaneously governed by centralized and distributed control (i.e. the paradox of control), so that the core unit of analysis should not be the core of the platform, but its boundary resources: distributed actors who collectively determine boundary resources. These reconstructions, albeit technical, have a significant impact on the legal qualification of digital platforms in terms of multinational or transnational companies, if we consider

---

control not only in terms of governance but also of technology (Chapters 2, 3 and 4).

1.2 The Market-Based Definition According to Economists

Economists define the digital platform as a two-sided market, a place for exchanges of information, goods, or services between producers and consumers as well as the community that interacts with the platform, or a business based on enabling value-creating interaction between external producers and consumers. The community itself is an essential piece of the digital platform. Hence, classifications are based on the services provided: social media platforms like Facebook, Twitter, Instagram, and LinkedIn; knowledge platforms like Wikipedia, StackOverflow, Quora, and Yahoo! Answers; media sharing platforms like YouTube, Spotify, and Vimeo; service-oriented platforms like Uber, Airbnb, and GrubHub.

---

9 J.-C. Rochet, J. Tirole (2003), Platform competition in two-sided markets, *Journal of the European Economic Association*, 1(4), 990–1029. Platforms deliver ‘a digital service that facilitates interactions between two or more distinct but interdependent sets of users who interact through the service via the Internet’ (OECD (2019), *An Introduction to Online Platforms and their Role in the Digital Transformation*, OECD Publishing). A platform is an undertaking operating in two (or multi)-sided markets which uses the Internet to enable interactions between two or more distinct but interdependent groups of users so as to generate value for at least on of the groups … Platforms are generally known as ‘two-sided’ or ‘multi-sided’ markets where users are brought together by a platform operator in order to facilitate an interaction (exchange of information, a commercial transaction …). European Commission Staff Working Document, Online Platforms accompanying the document Communication on online platforms and digital market, 15 May 2016, SWD 2016 172, p. 2.1. This definition appears to be very similar to the one provided by T.K. Koh, and M. Fichman (2014), *Multi-homing users’ preferences for two-sided exchange networks*, *MIS Quarterly*, 38(4), 977–996, at 977. We can find the same definition in European Commission (September 2015), Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy, available at https://ec.europa.eu/digital-single-market/en/news/results-public-consultationregulatory-environment-platforms-online-intermediaries-data-and-cloud.


11 One challenge for digital platforms is the chicken-and-egg problem: the platform needs both the producer and the consumer sides to ensure a valid value proposition, but neither side is willing to join as long as the other side is not populated: see B. Caillaud, B. Jullien (2003), *Chicken & egg: competition among intermediation service providers*, *RAND Journal of Economics*, 34(2), 309–328.
The reason for this definition lies in the need for economists to apply already existing (conventional) categories and practices: those typical of multi-sided markets, from which direct and indirect network externalities originate.

As the economic research on two (multi)-sided markets is mostly focused on financial and pricing dynamics of competition, this is the main topic that economists are investigating, also with reference to digital platforms. One of the main difficulties inherent in the definition is to include both platforms that are based on an economic exchange (e.g. Uber, Airbnb) and those based on a non-economic exchange (typically, the data of community participants, for social networks). Hence, the need to give an economic value to the data, to include the latter in the definition and (among other things) subject them to the

---

12 A. Gawer, M.A. Cusumano (2002), Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation, Harvard Business School Press. M. Pagani (2013), Digital business strategy and value creation: framing the dynamic cycle of control points, MIS Quarterly, 37(2), 617–632 at 625, points out that a multisided platform … exists wherever a company brings together two or more distinct groups of customers (sides) that need each other in some way, and where the company builds a below structure (platform) that creates value by reducing distribution, transaction, and search costs incurred when these groups interact with one another.


13 Network externalities imply that a technology grows more useful as its installed base of users increases. They are direct when the value of the platform depends on the number of users in the same user group, and indirect when it depends on the number of users in a different user group. See M.A. Schilling (2002), Technology success and failure in winner-take-all markets: the impact of learning orientation, timing, and network externalities, Academy of Management Journal, 45(2), 387–398.
typical antitrust dynamics – and rules – which would otherwise be ineffective.\textsuperscript{14} It is a case in which the theory influences the practice or, according to another approach, constitutes one of those self-fulfilling prophecies. Constitutional protections are the losing party (below, section 5).

If these are the aims and the needs, we can understand how the classifications of digital platforms inferred from this economic definition depend on their business model, their form of interaction, their governance, their ownership structure.\textsuperscript{15}


1.3 Legal Definitions

The definition of digital platforms by jurists is both contractual and regulatory, as it must satisfy the needs of both private and public regulation (below, section 2). It is also peculiar, and revealing of the inherent difficulties and pitfalls, that no definitions of digital platforms can be found in binding regulations. The EU expressly chose not to adopt a one-size-fits-all approach and to rely on a sector-specific, problem-driven approach. It is therefore clear that, since the definitions are functional, and the function with respect to digital platforms is regulatory, jurists have not provided definitions other than those functional to antitrust, competition or regulatory analyses. Recent examples are the European Commission’s proposals for the Digital Services Act, the Digital Market Act and the Digital Governance Act, focused on the regulation of platforms, of which, however, the rules do not provide a definition other than that of gatekeepers, for platforms enjoying very special positions on the market.

16 The study Liability of online platforms (Panel for the Future of Science and Technology, European Parliamentary Research Service, STOA, February 2021) defines online platforms as entities which: (i) offer ‘over the top’ digital services to users; (ii) are or can be operated as two- or multi-sided market business models; and (iii) allow the overall facilitation of interaction between the different sides of the market, even when there is no direct interaction among them.


18 The 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, designates (Article 3) as gatekeepers:

1. A provider of core platform services shall be designated as gatekeeper if: (a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future. 2. A provider of core platform services shall be presumed to satisfy: (a) the requirement in paragraph 1 point (a) where the undertaking to which it belongs achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or where the average market capitalization or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 65 billion in the last financial year, and it provides a core platform service in at least three member states; (b) the requirement in paragraph 1 point (b) where it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10,000 yearly active business users established in the Union in the last financial year; for the purpose of the first subparagraph, monthly active end users shall refer to the average number of monthly active end users throughout the largest part of the last financial year; (c)
1.4 A Functional Definition

At present, I believe that the most adequate definition, being general (it includes all existing platforms and also future ones) but not generic, is the following. Digital platforms are hardware or software structures that provide technological services and tools, programs and applications for the distribution, management and creation of free or paid digital content and services, including through the integration of multiple media (integrated digital platform). A digital platform can be open source or commercial and can be structured for public access or for a limited target, subject to registration. It may include information, interactive services, file sharing, downloading and uploading, and streaming services, as well as communication and sharing of multimedia content.

Digital platforms constitute real communities, closed or open, depending on whether they require registration or not. Operating system platforms like Android (Google) and iOS (Apple), social networks (Facebook, LinkedIn), payment platforms (PayPal, Apple Pay, Square), consumer communication apps (Twitter, Instagram, Skype, WhatsApp, Telegram, WeChat, Line, TikTok, etc.), Fintech apps (Kickstarters), health care apps (PatientsLikeMe), as well as permissioned blockchains, are closed communities. Search engines such as Google, or sales platforms, are open ones, ranging from simple marketplaces with or without intermediation (eBay, Airbnb, Home Away) to intermediate forms such as transport applications (from Uber to car/motorbike/bicycle sharing), to platforms that sell directly, distribute and deliver, such as Amazon, to permissionless blockchains.

Whether the platform is closed (a social network, a mobility app), open (a search engine) or partially open (a marketplace) is relevant as regards the requirement in paragraph 1 point (c) where the thresholds in point (b) were met in each of the last three financial years.

economic definition, which qualifies the platform as a ‘waterproof’ or ‘porous’ ecosystem. But it is even more so as regards the legal definition, for the more the platform is closed, the more the ecosystem may be legally qualified as a private legal order (see Chapters 2 and 3).

The common features of digital platforms are, on the one hand, the ability to process a large amount of data and, on the other, the use of algorithms for data extraction, and also for the purposes of customer or user profiling. The profiling mechanisms are now so refined (through ‘recommendation algorithms’) that they are de facto individual, and determine a knowledge of the preferences and habits of each user so profound as to allow the supply of tailored goods and services under economic conditions ad hoc for each (‘reserve price’).20

If we abstract from the daily life of the markets and investigate the path that digital platforms are taking, it is clear that in the coming years the Internet of Things (IoT) will make digital much of the world that is still partially analogic (or physical). It will imply an interoperativity (via API and standards) that will let platforms operate and integrate each other.21 Hence, digital platforms are becoming interconnected digital structures: real ecosystems.22 The development of the blockchain strengthens this trend.

The evolution and progressive ‘aggregation’ of these ecosystems accelerates, albeit in an original way, the overcoming of gaps through the transition from public ordering (via ex post verification through independent agents) to

---

20 The reserve price is the price that the digital sales platforms offer to each potential buyer, determining it on the basis of his/her previous purchasing experiences and on a series of additional data that allows it to accurately qualify the spending capacity and the propensity to purchase. The price of each asset is therefore not fixed, but is tailored to each prospective buyer.

21 For instance, the agreement between Google and Apple that in the spring of 2020 allowed their respective operating systems (Android and iOS) to interface in order to create a unique base platform worldwide for tracking and notification of exposure to Covid-19.

private ordering (via private employees), theorized by Williamson with the ‘fundamental transformation’ in the development of firm theory.\textsuperscript{23}

Moreover, even on a legal level, the ‘technological’ notion of ecosystem should lead to that of ordering, which despite having similar characteristics arises differently in closed, waterproof platforms, and in open, porous ones. Taking note of these evolutions makes it possible to make up for the current gaps in the legal definition. We shall look more closely into this aspect in Chapters 2, 3 and 4.

2. DIGITAL PLATFORMS FACING THE REGULATORY ENVIRONMENT: THE TWENTY EUROPEAN MILESTONES

Digital platforms operate in the market and create the rules that govern it. Let’s start with the latter. For the sole purposes of interpretation, to define the framework and outline the scenario, we start from some assumptions (twenty). Let’s call them European milestones, since they are the foundations on which the European Union intends to carve out a role in the global digital economy, via regulation. Since European standards constitute the highest standards and at the same time a measure of legal protection, they become de facto paradigmatic, and are therefore a good starting point for the investigation.

2.1 One: The Era of the Necessary European Policy of Sustainable and Inclusive Growth

We are in a new phase of the European Union: the era of the ‘necessary European policy of sustainable and inclusive growth’.\textsuperscript{24} Growth must be sustainable and inclusive: Germany, the economic engine of the Union, is aware that the regionalization of globalization makes the European market even more strategic, so that competition between member states’ legal systems is no longer an interest to be pursued but a danger to avoid.\textsuperscript{25} This also produces

\textsuperscript{23} See O. Williamson (1991), \textit{The Nature of the Firm: Origins, Evolution, and Development}, Oxford University Press; O. Williamson (2002), The theory of the firm as governance structure: from choice to contract, \textit{Journal of Economic Perspectives}, 171–195. We shall see in section 2 that the two positions, respectively of Calabresi and Williamson, are compatible with each other and consistent with the regulatory evolution, in which public and private regulation constitute communicating vessels and their relationship depends on contingencies.

\textsuperscript{24} F. Bassan (2020), La nuova Unione Europea: una politica di crescita sostenibile e solidale necessaria, \textit{Astrid Rassegna}, 320.

\textsuperscript{25} In the European Union, the combined provision of powers attributed to European institutions for some policies (some exclusively, such as monetary policy, others
direct effects on regulation and on the tools used to implement it: increasingly European regulations (not directives) and a single, general body of legislation.\textsuperscript{26}

Sustainability and solidarity are now linked: the former no longer refers only, typically, to the environment or corporate governance, and also integrates the principle that value must be kept as close as possible to the link in the chain that produced it.\textsuperscript{27} Hence, the focus is on the extraction of value achieved by digital platforms via algorithms and the need for a regulation consistent with this evolution.\textsuperscript{28} Hence also, the link with solidarity, since the production chain is no stronger than its weakest link.\textsuperscript{29}

\section*{2.2 Two: The Rules Embedded in Technology}

In the current evolutionary framework, the hardware (terminals, networks) is Chinese, the cloud predominantly American, and all that remains for the European Union is to define the rules.

However, two clarifications are important to interpret the real data. The first: technological evolution drives intelligence, which was once centralized in the cloud, towards distributed ledger technology (DLT) or decentralized systems (today the cloud edge, or proximity data centre, tomorrow directly into objects), or combinations of these. Among the consequences of this evolution is that there is reasonably greater competition between companies to occupy spaces that are still empty. The instruments of competition, if concentrated on

\textsuperscript{26} Regulations are directly applicable in the member states, while directives must be transposed into their respective law systems. Therefore, the use of regulations makes EU law stricter. This is combined with the recent codification, via regulation, of entire sectors. The codes replace (via regulations) a set of rules (regulations and directives) stratified over time, and by so doing they standardize and simplify. Specific rules for different applications (which can also be numerous) originate from this clear and simplified regulatory basis.

\textsuperscript{27} M. Mazzucato (2018), \textit{The Value of Everything – Making and Taking in the Global Economy}, Penguin. According to the author, platform-based models are not necessarily data-extractive, but they are and will continue to be data-intensive.

\textsuperscript{28} Financialization and digitalization have led to the emergence of new ways of doing business, in which value creation and value extraction are increasingly separated. See M. Mazzucato (2018), Mission-oriented innovation policies: challenges and opportunities, \textit{Industrial and Corporate Change}, 803–815.

the repression (USA) or prevention (EU) of monopoly structures, could therefore only be partially useful to regulate the transition phase.

Second: the rules, in the digital world, are embedded in technology (below section 7). Failing to understand this leads to serious mistakes, like the one Germany recently made, for example, when it adopted a law on the notification of exposure to Covid-19 which provided for a centralized database, and had to modify it after two weeks because it was incompatible with the decentralized model that Google and Apple had spread in the meantime on all mobile terminals.30 Therefore, defining the rules means guiding technology, directing it towards the protection of rights that the European Union believes are the basis of its shared continental welfare.31

The digital welfare of continental Europe now proceeds in two directions: access and protection. It includes data protection as per the General Data Protection Regulation (GDPR), but also solidarity (which is necessary as it applies to states, but also to companies: hence contractual tools to allow equality and overcome the asymmetries of abuse of dependence) and sustainability (environmental, corporate and value-chain).32 Digital platforms cannot be asked to be responsible for this too: it is up to the states to take action.

The most important among the tools in the toolbox is interoperability, more effective even than break-ups,33 and guaranteeing both competition between platforms and also the setting up of new ones. After all, the European project GaiaX, a federation of national clouds to foster minimum protocols and stand-

---

30 Google and Apple have thus agreed on a fundamental choice that has divided governments and has forced some of them to reverse the choices (database centralization) already made (Austria, Germany, United Kingdom, Sweden even with GPS). France remained the only one to have maintained a centralized system despite its limited compatibility with the Apple and Google platform.

31 Think not only of freedom of expression but also, in the Internet of Things, of health protection, transportation, provision of essential services, etc. Only if taken into account right from the outset, in the development of protocols and technological standards, can these rights be guaranteed. European welfare must therefore be reviewed and integrated into technology.

32 Above, note 27. Bringing value creation and value extraction back to the same plan is one of the functions of sustainability, as it is understood today by the European Commission.

33 We shall see in section 3 that the US antitrust approach, which justifies intervention in the market only in the event of an intent to monopolize and admits it in the most disruptive form (the break-up, in fact) is less efficient than the ‘regulated competition’, an approach that the European Commission has been supporting since 2020 with a series of proposals for regulations, which base the opening of markets on the interoperability of platforms and technologies.
ards consistent with European welfare, goes exactly in this direction. This is a fundamental prerequisite for the transition – which is already taking place – from the (centralized) platform economy to the (distributed) blockchain economy, to the (decentralized) artificial intelligence economy, in which the data multiplies exponentially because data is no longer generated only by users but also by things (IoT).

2.3 Three: Rules and Extra Costs: Who Is Going to Pay?

The issue for the Union is how to make efficient a system in which the rules make technologies more expensive instead of cheaper. Without some form of public intervention, the market is based on an inexorable Darwinian process in which, all other features being equal, the least expensive product survives. Assigning these extra costs is a choice of industrial policy, which we can re-categorize today in the necessary European sustainable and inclusive growth policy. The answer to the question ‘who is going to pay?’ was the origin of the awarding of many Nobel Prizes for economics and is, however, often the most pragmatic starting point.

One can assume that states pay the extra costs, to promote their own welfare. Sharing mechanisms can be created alternatively, as has already been done in the past, for example with the universal service. According to a third

34 The European GaiaX project is still at an initial stage and may evolve in two directions, or in a third one consisting of an integration between the two. The first is the least ambitious: a federation of national clouds aimed at sharing protocols and standards (‘GSM model’). The second sees an intervention by governments and an industrial policy, which is expressed in an ‘Airbus model’ collaboration, and therefore with European companies that actively participate in the development of technologies which integrate the rights that the Union wants to guarantee.

35 This was the case, for example, with GSM, a European technology that at the beginning of the 1990s competed with others (CDMA, in the United States) and then prevailed all over the world thanks to its efficiency and reduced costs.

36 Much of the debate on the use of National Recovery and Resilience Plans is based on the costs attributable to the member states of the European Union for achieving the goals of sustainable digital development.

37 The solutions chosen by the European Union in the 1990s for overcoming state monopolies in public services were numerous and different from each other. In telecommunications, the justifications for public monopolies were based on cross-subsidies (for example, between local and long-distance calls), unsustainable in a competitive environment, in which newcomers would have attacked the richer (long-distance) market. The solution was to allow competition on all services, identifying a ‘cluster’ of essential services that each member state decided to guarantee, quantifying the net cost of providing these services, and attributing it to all operators on the market in proportion to the market share achieved (starting from a minimum deduction of 4%).
scenario, the market pays for these costs, provided that they correspond to a welfare shared by EU and some non-EU countries and that therefore the companies themselves believe they apply everywhere, making themselves part – if not promoters – of that higher level of protections on a global scale. This is what happened, for example, with the GDPR, initially opposed by digital platforms but then used (by Facebook, for example) as a justification for not sharing data, or (by Apple and Google) as the basis of the shared platform for Covid-19 notification applications, demonstrating that companies can easily turn risks into opportunities.

The Brussels effect is not automatic, and the degree of effectiveness of the rules is measured by the market.38

2.4 Four: The European Regulatory Matrix Is Blowing Up

The regulated markets in Europe constitute a ‘matrix’, composed of vertical silos (banking, insurance, financial markets, energy, transport, etc.) each subject to specific regulation, and horizontal silos, applicable to all sectors (competition, personal data protection, consumer protection). In the matrix, each box corresponds to an interconnection point between vertical (sectorial) and horizontal (general) rules, regulations and standards.39

The ‘matrix’ approach provides answers to many legal questions, not least that of the hierarchy of sources, which is clear in continental national legal systems but less evident in the relationships between legal systems. In the event of a conflict between vertical and horizontal silos indeed, reference has often been made to the hermeneutic criterion of specialty (the special rule prevails over the general one), which has generated a series of regulatory misunderstandings. The matrix simplifies the work of the interpreter, replacing the notion of prevalence of the rules with that of coordination (of the rules) and cooperation (of the competent authorities).40

39 I developed the regulatory matrix theory in detail in: F. Bassan (2019), Potere dell’algoritmo e resistenza dei mercati in Italia. La sovranità perduta sui servizi, Rubbettino.
40 According to the reconstruction and interpretation that I provided in ‘The power of the algorithm’ (Potere dell’algoritmo, above, note 39), the matrix provides for cooperation between independent national authorities, which should be adequate to resolve conflicts of competences and fill gaps. Nevertheless, there have been difficulties in the application, because independent authorities – and the courts – have applied the general criteria of interpretation: to overcome the conflicts they have therefore classified as ‘special regulations’ those of vertical silos and ‘general regulations’ those of horizontal silos. Hence, special rules have prevailed, in all the cases where the vertical silos could
Matrix regulation, which has worked satisfactorily up to now, is, however, imploding under the pressure of digital evolution. Vertical silos are no longer parallel: they converge or spread apart according to contingent urgencies and needs. A few examples: banks sell insurance, financial and mixed products, and the regulatory issue is raised here again in terms of prevalence or cross-regulation.\footnote{V. Colaert, D. Busch (2019), Regulating finance in a post-sectoral world: setting the scene, in V. Colaert, D. Busch, T. Incalza (eds), European Financial Regulation: Levelling the Cross-Sectoral Playing Field, Hart Publishing.} The convergence between telecommunications and television is prehistoric and the frontier has shifted to the audiovisual content of digital platforms, which grew in their {	extit{ante litteram}} sandbox (in Europe, the 2000 Directive on electronic commerce, in the USA, the Telecommunications Act and the Communication Decency Act both of 1996, which over the years have guaranteed them exemption from liability)\footnote{In the European Union, the e-Commerce Directive imposed a ‘notice and take down’ procedure, according to which internet service providers (ISPs) were not responsible for the content disseminated on the websites they hosted, but were required to remove it or disconnect them as a result of a request from the authorities. Similar provisions were in the US Communication Decency Act. When digital platforms took over from the ISPs, the rules were not changed consistently, and the guarantees – justified if applied to small operators, i.e. internet connectivity providers – were also applied to the platforms, which therefore operated for twenty years in the absence of rules, or at least of those rules that governed the activity of companies that competed on the same markets but originated from regulated sectors.} and are now too big to care.\footnote{Speaking to the European Parliament’s Internal Market Committee, Internal Market Commissioner Thierry Breton said that digital platforms may have become ‘too big to care’ (6 October 2020). He stated this in the context that they ‘tend to neglect the consequences of their actions in our daily environments, whether it be in work [or] in our social lives, but also when it comes to our democracy’.} And what about the convergence in transport, where the degree of substitution has long since exceeded the threshold of the markets?

As for horizontal silos (competition, protection of personal data and consumer protection), they are overcoming the historical constraints that have now become unbearable.\footnote{Below, sections 3 and 4.} This is the territoriality for data protection (\textit{Schrems I} and \textit{II}),\footnote{In \textit{Schrems I} (CJEU, 6 October 2015, Case C-362/14, \textit{Max Schrems v. Data Protection Commissioner} – ‘Safe Harbour’), the CJEU ruled that national data protection authorities have the right to investigate individual complaints related to EC deci-
ernization’), and the definition of the consumer as the beneficiary of the protection.

2.5 Five: The Transition Regulation

The fifth assumption concerns the regulatory reaction: the classic regulation by subjects has rapidly become regulation by activity and then by products. Recently, the failure of a regulation that follows the evolution of the markets and legal instruments based on these decisions, but also made very clear that only the CJEU is authorized to declare such a decision or instrument invalid. The CJEU also declared the Safe Harbour agreement invalid. The main reason for this ruling appeared to be the fact that the CJEU found that in adopting Article 3 of the Safe Harbour agreement, the EC exceeded its powers by making a shortcut to the adequacy procedure that should be followed according to Directive 95/46/EC. Following the invalidity of the Safe Harbour agreement, the EU–US Data Protection Shield (Privacy Shield) mechanism was implemented in order to replace the Safe Harbour agreement and to function as an instrument for EU/US data transfer.

In Schrems II (CJEU, 16 July 2020, Case C-311/18 Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems), while the Court of Justice invalidated Decision 2016/1250 on the adequacy of the protection provided by the Privacy Shield, Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries was deemed valid.


was commonly recognized. A new era has begun, which recent events (the pandemic, too) have accelerated.

We are presently halfway, fording the river when it is in flood – not exactly the best situation for developing strategies. The old rules are no longer effective, the new ones are not yet in force. The European Commission that took office on 1 December 2019 has taken exceptional decisions to face an exceptional crisis (the pandemic), but has also structured a medium- to long-term intervention to address the market.49

2.6 Six: The Regulatory Circle

The Commission’s strategy has now been simplified by the withdrawal from the European Union of the United Kingdom, which had brought into the EU with it an aversion to the codification of continental Europe. Legal traditions thus return to their origins, each in their own way.50 The EU Commission can therefore now move towards a new regulatory paradigm, no longer spurious, based on a general codification typical of civil law, applicable to all sectors, and therefore based on general principles, with specific applications (not ‘sectoral’, but based on single products or services) that arise from the market, according to the ‘regulatory circle’, which I illustrated in my previous writings.51

In a nutshell: the best practices on the market are adopted by the national regulatory and supervisory authorities as benchmarks and brought to the forum of the European authorities, which develop technical standards or, when necessary, proposals to the EU Commission, which then adopts executive acts, or launches legislative acts that the EU Council and EU Parliament then approve, making them binding. The advantage of the ‘regulatory circle’ is that the best practices are binding (self-binding the companies that adopt them) immediately, or as soon as the national and European authorities propose them as standards or guidelines.

49 DSA, DMA, DDA, Recovery Plan for Europe, ESM, are all tools that, together with the interventions of the European Central Bank (Pandemic emergency purchase programme (PEPP) and longer-term refinancing operations (LTROs)), intend to promote the sustainable technological development of the European Union.

50 In the European Union, member states and European institutions have attempted to make civil law systems compatible with common law ones. The civil law system is based on the framework of Roman law, with core principles codified into a referable system, which serves as the primary source of law. Common law (judge-made law, or case law) is the body of law created by judges and similar quasi-judicial tribunals by virtue of being stated in written opinions. With the United Kingdom’s exit from the Union, European legislation is now based on a single legal model, i.e. continental civil law. The harmonization process therefore tends to be more effective and faster.

51 F. Bassan, Potere dell’algoritmo, above, note 39, at 23–45.
The application rules of the codes are therefore no longer defined by ‘silos’ but by product. Hence there are a few rules of public regulation, which have been codified, and numerous specific applications that change in real time due to market practice. In this pragmatic way, and also dictated by the pandemic emergency, the regulatory dilemma that has seen opposing principles of prevalence and cross-regulation for a decade has been resolved.52

2.7 Seven: Enhanced Cooperation Regulation

This evolution produces direct effects in terms of technological innovation and digital platforms, since in the modernization of the regulatory framework, the national authorities of several member states can coordinate and negotiate jointly,53 as well as effectively sanction any non-compliance (with what, however, is an agreement reached on the basis of a commitment made by the platform). This applies to competition, and should also apply to the regulatory authorities, coordinated with each other both vertically (with the supervisory or regulatory authorities of the same sector in the other member states and with the European one or, failing that, with the European Commission) and horizontally (with authorities from other sectors in the country of origin).

2.8 Eight: Ethical Regulation

What has been said is also relevant on a peculiar front of technological innovation, not ignored by scholars, but still without solution: the relationship between ethical principles and legal rules, separated by the curtain created over two centuries of general theory of law and now torn down by artificial intelligence. When we remain on the level of rules, the responsibility of the algorithm seems ineffable, since the algorithm can be, depending on the case, more

---

52 A common solution to regulating mixed (hybrid) products or activities is represented by the principle of prevalence (or predominance). The issue has typically arisen in the market for unit-linked and index-linked insurance policies (plans offered by insurance companies that integrate both life insurance – covering the risk of death – and investments, which offer the opportunity for the investor to generate capital). On this topic, see N. Dacev (2017), The necessity of legal arrangement of unit-linked life insurance products, UTMS Journal of Economics, 8(3).

or less autonomous from both its creator and its users, and often the choice is one of opportunity; therefore credible representations must be created.54

The regulatory circle is part of the solution, not of the problem: it permits human intervention (thus, the algorithm will not do it by itself) to select the best practices, which are transformed into benchmarks and therefore into rules and, in this perspective, it also implements the rules of Asimov (rules 3 and 1).55

The European Union is now beginning to regulate these issues, differentiating regimes according to the degree of risk that the use of the algorithm produces and the activities in which the risk can be generated.56 The principle according to which human intervention is in any case necessary, in one of the phases of production or use of the algorithm, to prevent its autonomy from turning into independence, constitutes the fundamental prerequisite of the legislation under discussion.

2.9 Nine: The Communicating Vessels of Regulation via Subsidiarity

Public and private regulation are two communicating vessels. Public regulation intervenes when private regulation fails: subsidiarity applies, since private self-regulation may be sufficient, and public regulation only intervenes to fill any existing gaps.57 However, one must not confuse the failure of regulation with that of the market.58 It is more than a reconstructive hypothesis because it

---

54 Below, section 6.
55 The Three Laws of Robotics (known as Asimov’s Laws) were introduced in Asimov’s 1942 short story ‘Runaround’. The Three Laws are: (1) A robot may not injure a human being or, through inaction, allow a human being to come to harm. (2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law. (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Law. Asimov also added a fourth, or zeroth law, to precede the others: (0) A robot may not harm humanity, or, by inaction, allow humanity to come to harm.
56 Below, section 6.
58 J. Tirole (2017), Economics for the Common Good (translation by S. Rendall), Princeton University Press, 160 ff. argues that economic regulation addresses six prototypes of market failures: (1) negative externalities or spillovers; (2) informational asymmetry; (3) buyers can become victims of their own actions; (4) implementing the exchange may exceed the individual’s capacities; (5) market power; (6) inequality.
always works and therefore becomes a general rule. If put in this perspective, we understand the strategy of the new European Commission, which entrusts the concrete application of the rules and principles to the market and the regulatory circle. And one also understands the EU Court of Justice, which (Schrems II) does not limit itself to cancelling the flawed public regulation but suggests developing the private one in the meantime (the standard contractual clauses), to be possibly framed within the other. Here, the task of regulators, guarantors and supervisors becomes decisive, in the role they must exercise in the ‘circle’.

2.10 Ten: Regulation and Codification of Uniform Law

From this point of view, the activity of subjects unfairly ignored in the last historical phase, which has effectively produced the codification of uniform law, becomes decisive again. UNIDROIT and UNCITRAL are the venues in which international contracts have found standards commonly applied today and are again (the most) appropriate in the current phase in which European rules have territorial constraints, and public intervention must be residual, limited to providing the guarantees that the rules between private individuals fail to ensure (see Chapter 5).

2.11 Eleven: Co-Regulation, Clearing House

This evolution is fully part of the mainstream thinking on which the European regulation of the last two decades has been based, according to which co-regulation, necessary if self-regulation is ineffective, is a clearing house for communicating vessels, where private and public regulation meet, and public and the railways in Britain and Germany, Journal of Public Policy, 22, 271–297; P.N. Grabosky (1995), Counterproductive regulation, International Journal of the Sociology of Law, 23(4), 347–369; C. Sunstein (1990), Paradoxes of the regulatory state, University of Chicago Law Review, 57, 407–441; R. Merton (1936), The unintended effects of purposive social action, American Sociological Review, 1, 894–904.

59 F. Bassan, Potere dell’algoritmo, above, note 39.

60 On 16 July 2020, the Court of Justice of the EU (CJEU) issued its judgment in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (Case C-311/18, ‘Schrems II’).

intervention is allowed on a subsidiary basis and in compliance with the principle of proportionality. Co-regulation is to be understood here, obviously, as cooperation between regulatory authorities and the market in the formation of the rules that the latter is unable to establish via self-regulation.62

2.12 Twelve: Co-Regulation and Enhanced Regulatory Cooperation

It follows from the above that co-regulation finds specific application no longer in vertical silos (indeed, they no longer exist) but in intersectoral applications and often beyond the borders of a member state. Hence the need for that cooperation between authorities in both vertical and horizontal directions referred to in milestone six, which allows for a differentiated regulatory evolution based on the legal needs and sensitivities prevailing in the various legal systems.

2.13 Thirteen: Regulation and Digital Platforms

Digital platforms are the new players in the market (autonomous ecosystems) and cannot be the recipients of classic regulation, which is ineffective: it is a radar against which they fly too high, or too low (depending on the cases and interpretations). Because they were born unregulated.63 Because they have so far operated in the absence of regulation.64

Therefore, today – and this is one of the objectives of this research – the issue arises of their placement in the legal space in which they actually operate, and which is national, transnational and probably, as we shall see, international.

---


64 Below, section 5.
2.14  **Fourteen: Digital Platforms and AI – The Relationship between Ecosystems**

Algorithms and artificial intelligence are independent and self-regulated ecosystems which, when inserted into the ecosystem of digital platforms, become their operational tools and impose their implementation rules. The issue of an intervention (co-regulation) is therefore raised to regulate artificial intelligence in a way that is independent from the regulation of the platform, but consistent with it. The two sets must have autonomous but coherent rules, since both must be applicable in the subset constituted by their intersection (below, section 7).

2.15  **Fifteen: Responsible Ecosystems**

The regulation referred to in the previous point is legitimate and necessary, when it comes to digital platforms, to guarantee and protect the rights on a contractual level, but also to identify and distribute the responsibilities on a non-contractual level (when the damage is produced by an illicit act – below, section 6); public regulation, subsidiary, via the regulatory circle. Old rights are no longer enforceable, new ones must be guaranteed. However, it is a matter of understanding (and accepting) that the rules cannot be imposed from top down, but are developed through cooperation via the regulatory circle. With digital platforms, the best that states can achieve is to negotiate, influencing best practices and establishing which of them should become benchmarks and standards on the basis of the welfare that the Union wants to guarantee (see Chapter 3).

2.16  **Sixteen: Middle Enterprises**

This regulatory approach is opposed by the ‘middle enterprises’ (nothing to do with medium sized enterprises). I refer to companies that have no bargaining power with transnational digital platforms, and cannot count on a regulatory basis that, on the one hand, protects them, and on the other, guarantees the legitimacy of their work, if compliant. Legislative, regulatory, judicial solutions – rules by principles, ‘mercatory’ applications – leave middle enterprises exposed to both negotiation (they have no power) and compliance risks (they have no certainties).

Here, too, the old rules are sheet music without instruments. The solution exists and has been indicated and practised by the European institutions in

---

recent years as a priority: it is called co-regulation (see above, milestones six and eleven) and provides for the participation in the formation of the *lex mercatoria* by the regulatory authorities to compensate for market asymmetries. It allows companies to guarantee certainty, as regards compliance and strength, in negotiating with digital platforms.

Co-regulation also includes the reconstruction of a level playing field on a contractual level, a regulatory competition tool that the European Commission’s proposal for a Digital Market Act has introduced as an *ex ante* measure.66

Regulation must push these companies towards environments (distributed today, decentralized in the near future) where competition is not yet driven by gatekeepers. Pushing the ‘middle enterprises’ towards market segments still open to competition and which are the prerequisites for the progressive digital evolution, is a typical act of industrial policy. Or rather, what I have indicated here to be the ‘necessary sustainable and inclusive growth policy’.

2.17 Seventeen: Lockdown Economy

On these assumptions, the pandemic has had a significant impact. The persistent lockdown (2020–2021)67 changes the picture. On the one hand, the power of digital platforms has grown, to the point of exceeding the psychological threshold of abuse (the US Federal Trade Commission’s intervention against Facebook and that of the US Department of Justice against Google are historic events and will have consequences).68

The fact that the German government had to change a law adopted a few days earlier (on the notification of exposure to Covid-19) because it provided for a centralized database, incompatible with the decentralized system imposed a few days later by Google (Android) and Apple, with the additional aim of better protecting personal data, did not get the publicity it deserved.69 An agreement between duopolistic operators on the global market has the power to impose itself on governments as it is instantly applied to all active smartphones and not notified to any regulatory or supervisory authority.

From this first point of view, therefore, even if experienced, in fact, as a revolution (game changer), the pandemic has rather produced an acceleration of the evolution already under way (game accelerator).

---

66 Below, milestone 19, and section 3.
67 I’m referring to the effects of the Covid-19 pandemic.
68 Below, section 3.
69 Below, sections 3 and 4.
2.18 Eighteen: The Superstition of Algorithm Transparency

On the other hand, the pandemic has accelerated the transparency of the processes of artificial intelligence. This is an important point, for the transparency of the processes was precisely what was missing to allow digital transnational platforms to submit products and services to the regulatory and supervisory authorities and finally enter the regulated markets.

The notorious transparency of the algorithm, which cannot go to the origin of the source code due to industrial property rights,\(^70\) settles on the process level: disclosure about the steps, the instructions provided to the algorithm, must be sufficient for the supervisory authorities.\(^71\) What they produce, by virtue of machine learning, can become reasonably predictable if the initial instructions are known. However, this is certainly not a final solution. The

---


\(^71\) Below, sections 4, 5 and 6.
battle is about to begin, the regulation must be ready and modernization of the rules is not enough.

2.19 Nineteen: Regulation, Today

Therefore, the European Commission is accelerating the Digital Services Act (DSA), the Data Governance Act (DGA) and the Digital Market Act (DMA), also addressed to platforms,\textsuperscript{72} to which the Platform-to-Business Regulation (2019/11501) already applies. It provides indeed for general rules and contractual application.\textsuperscript{73}

The DSA stands as a core of fundamental rules for the digital economy, equivalent to the GDPR and with the same goal of ‘globalizing’ rights.

At the same time, the Commission launches the modernization of competition rules, to make them effective in the new framework and with the new digital market structures.\textsuperscript{74}

We shall see the contents and impacts of these new tools, which are still being defined, in the next section. Again, the European Strategy for Data\textsuperscript{75} is not corollary; rather, it closes the perimeter; similarly with the ‘Digital Finance Strategy’\textsuperscript{76} the ‘Retail Payment Strategy’\textsuperscript{77} and the legislative proposals for a


\textsuperscript{73} The platform-to-business (P2B) regulation of the European Union has provided, since 2019, an encompassing legal framework for the relations of digital platforms and businesses. The rules require online intermediation services and online search engines to follow certain restrictions regarding their behaviour in the internal market. In particular, the P2B regulation requires a higher degree of transparency from platforms on their terms and conditions, the ranking parameters, the differentiated treatment of their own products and products of third parties (self-preferencing), access to data, exclusivity clauses or price parity agreements. The rules primarily require transparency, but do not prohibit specific behaviours. The P2B-regulation is to be reviewed as early as 2022, only a short period of time after its implementation.

\textsuperscript{74} The Commission is about to adopt a Proposal for a Regulation on new complementary tool to strengthen competition enforcement.

\textsuperscript{75} Proposal for a Regulation on European Data Governance (Data Governance Act), COM(2020) 767, 25 November 2020. As well as this proposed regulation, the European strategy for data intends to adopt legislative measures on data governance, access and reuse.

\textsuperscript{76} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of Regions on a Digital Finance Strategy for the EU, COM/2020/591 final.

\textsuperscript{77} Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on a Retail Payments Strategy for the EU, COM/2020/592 final.
‘DLT Pilot Regime’ and for more ‘digital resilience’ in the financial sector (including a proposal for ‘Markets in Crypto-Assets Regulation’ – MiCA).

Legislative initiatives are about to be launched by the Commission to ascribe the responsibilities in the artificial intelligence ecosystem (below, section 6) by applying the principles of subsidiarity and proportionality, but also of precaution.

So much for the Commission. The EU Council and therefore the EU member states provide development policy support to the Commission’s regulatory instruments. For example, it launches the initiative for a European cloud, which among the various objectives also aims at guaranteeing the territoriality of data and therefore the application of Union welfare, since the ‘Brussels effect’ alone cannot guarantee extraterritoriality and prevents exceptions to jurisdiction (and the Court of Justice has now clarified this on several occasions).

The European Parliament and the Council have passed the rules for European collective action, thus legitimizing consumer representatives as active players in the regulatory circle.

The European Central Bank (ECB) also plays its part, and develops rules and standards for the digital euro and, as we shall see later, for private crypto-currencies.

In the United States, existing antitrust instruments are used and refined. The two paths seem diametrically opposed but, as we shall see, in some cases they converge (below, section 3).

---


80 For a general investigation on the precautionary principle see: F. Bassan (2006), Gli obblighi di precauzione nel diritto internazionale, Iovene.

81 GAIA-X is a project for the development of a federation of data infrastructure and service providers for Europe, which is supported by representatives of business, science and administration from European countries. The project was first presented to the general public at the Digital Summit 2019 in Dortmund (Germany) and has been continuously developed since then.

82 Below, section 4.


2.20 Twenty: Regulatory Discontinuity and Market Codification

The evolutionary process—traditionally, the legislative process—that provides for the application of existing rules to new challenges, becomes revolutionary when placed on the path started by the new European Commission: general principles and rules, implementation by ‘market codification’. As in the case of the Payment Services Directive 2 (PSD2), both recently\textsuperscript{85} and following the standard of liberalization of the 1990s, in the era of crisis of the system or technological discontinuity, regulation stops chasing innovation (if the turtle chases Achilles the paradox does not work anymore) and rushes forward, dictating the new perimeter of the game in which operators can compete. It is an act of courage that defines the European industrial policy (\textit{recte}: necessary sustainable and inclusive growth policy) and deserves support. Today, we are in a \textit{terra incognita}.

However, something seems to escape the regulatory evolution that I summarized above, interpreting it. What is missing, more than what is there, is the subject of investigation in this book.

Ecosystems (according to the technological and economic definitions) do not allow for a regulation totally imposed from the outside. Recent practice shows that digital platforms are partially porous.

This is why I have emphasized in this section the profiles of co-regulation, a negotiated discipline, an intersection between private and public regulation. If these tools and the resulting methodology are always valid, they must be

taken, in legal terms, from the level of market regulation to a higher level, of
general theory. I shall do so in Chapters 2, 3 and 4.

3. DIGITAL PLATFORMS AND THE REGULATED COMPETITION

Competition law (in the EU) and antitrust law (in the US) have moved from
an economic approach that starts from the definition of a digital platform as
a two-sided market (above, section 1), with certain substantial differences,
which I shall briefly illustrate here. As for the competition law of the European
Union, I shall restrict the review to the European Commission, since the
national cases show more specific but also partially contradictory approaches.

The focus is not on illustrating in detail all the elements of digital platforms
that are relevant for the purposes of antitrust law (in the USA) and competition
law (in the EU). Rather, my intention is to verify whether the direction taken
by states and regulators is correct, and whether it is exhaustive or can be inte-
grated, and possibly whether this integration, aimed at filling possible gaps,
allows a partially different approach, not just regulatory.

The issue mentioned in the previous section is that of the communicating
vessels between private and public regulation. From this basic approach, the
relationship between regulation and competition is inserted within public
regulation.

3.1 Abuses of Dominant Positions by Digital Platforms

By implementing the practice and the case law on multiverse markets, the
European Commission has sanctioned Google (Google shopping, 86 Google

86 Commission Case No. COMP/AT.39740 of 27 June 2017 – Google Search
(Shopping). The EC considered Google to be leveraging from the dominated market
for general search services into markets for comparison shopping services. Conversely,
the FTC closed (in 2013) a similar investigation concluding that Google did not change
its search results primarily to exclude actual or potential competitors but to improve
the quality of its search results: see Statement of the FTC Regarding Google’s Search
Practices, In the Matter of Google Inc., FTC File Number 111-0163, 3 January 2013,
available at http://ftc.gov/os/2013/01/130103gogoosearchstmtofcomm.pdf (accessed
24 December 2016).
Android, Google AdSense, launched investigations against Amazon and Apple on the basis of what had already happened, in the digital innovation sector, with Microsoft. Contiguity of the markets, extension of the dominant position on contiguous markets, ‘leveraging strategy’ and economic dependency are the tools used to sanction abuses and bring digital platforms back to a path that is, if not virtuous, at least consistent with the typical protections of a non-inclined plane.

In the wake of the European tradition, the investigations launched (and the fines imposed) by the Commission start from the evaluation of the effects of the conduct on the market, not the way in which they are produced, nor the intentions of the platforms. Therefore, not only the subjective element (intention) but also the tool (algorithm) remain outside the perimeter of the analysis. The toolbox has proved to be only partially effective for surveillance of the digital platform markets, and the need for reform, on a legislative or executive level, is unanimously felt.

87 The EC fined Google for abuse of its dominant position: (i) in the national markets for general search services; (ii) in the worldwide market for licensable smart mobile OSs, and (iii) in the worldwide market for app stores for the Android mobile OS. Commission decision of 18 July 2018 in Case No. COMP/AT.40099 – Google Android. Conversely, in the US – Feitelson v. Google Inc, 80 F. Supp. 3d 1019, 1022 (N.D. Cal., 20 February 2015) – the California District Court rejected the complaint because the plaintiff was unable to demonstrate the foreclosure effect due to the exclusivity agreements concerning the pre-installation of Google’s apps. On this topic, see J.M. Newman (2016), Antitrust in zero-price markets: applications, Washington University Law Review, 94(2), 101. For a comment on the European decision, see V. Kathuria (2019), Greed for data and exclusionary conduct, Computer Law & Security Review, 35, 89–102.

88 Commission decision of 20 March 2019 in Case No. COMP/AT.40411 – Google Search (AdSense). According to the EC, Google abused its dominant position in the EEA-wide market for online search advertising intermediation.

89 On July 2019 the Commission launched an investigation against Amazon to assess whether the online marketplace, in its dual role of online platform and retailer, had put in place (along with independent sellers that are part of its network) anticompetitive agreements under Art. 101 Treaty on the Functioning of the European Union (TFEU) and/or had abused its (alleged) dominant position (in the market for online intermediation of e-commerce) under Art. 102 TFEU (Case AT.40462 – Amazon Marketplace, started on 17 July 2019).

90 The EC investigation announced on 3 June 2019 started from a complaint lodged by Spotify, according to which Apple allegedly: (1) unfairly limits competitors in their access to the Apple Music streaming service; and (2) imposed a 30% fee levied on content-based service providers for using Apple’s in-app purchase system (IAP) for any subscriptions sold in its Apple store.

Hence, as in the case of abuse by exclusion, the economic tests on predatory prices are useless when the service is sold for an economic consideration that is, however, non-monetary (hence the superstition about services that are free of charge). On the one hand, there is an undeniable advantage for the consumer, which can only be measured following an economic evaluation of the data transferred by the consumer in exchange for the service: an analysis which is still imperfect. On the other hand, the difficulty of shifting price discrimination from abuse by exclusion (in respect of competing companies) to exploitation (in respect of consumers) when the price is ‘reserved’, is tailored to the availability and attitude of the individual, as profiled up to that point.

On the other hand, again, the presumed irrationality of predatory prices in the face of the difficulty of recovering losses (in the USA), or the objective assessment of the non-coverage of average variable costs or the avoidable average and incremental long-term cost (in the European Union) can hardly be brought more up to date, there being no adequate checks, although they clearly contrast with the world of digital innovation: Amazon has built an entire philosophy and a consequent business strategy (even included in its by-laws) on losses in the medium term.

Furthermore, the qualification of the markets is cumbersome, but this is normal in the evolution of the case law that pursues the market. Thus, the European Commission considered the ‘search engine market for general surveys’ to be relevant, but has and will have difficulty in grasping the relevance of data acquisition and data management. Moreover, new criteria for assessing dominance in multiverse and networked markets on digital

---


93 Unless we transform price discrimination into legal discrimination: A. Ottolia (2017), Big Data e innovazione computazionale, Giappichelli, 317, or we consider personalized prices as exploitation prices because they are able to extract from consumers all their willingness to pay: S. Mannoni, G. Stazi (2018), Is Competition a Click Away?, Editoriale Scientifica, 40, and M. Maggiolino (2018), Big Data e il diritto antitrust, Diritto dell’economia, 320.


95 European Commission, Case AT.39749, p. 28.
innovation have only been outlined in Germany, and it is significant that the intervention was legislative.96

The theory of the absence of true barriers to access to markets characterized by technological innovation, which in the United States too, above all, takes pride in recognized and unanimous practice and jurisprudence, yields to the evidence of economies of scale and self-powered network effects. The aggressive, all-US strategy of start-up acquisitions that made it completes the picture.97

Moreover, qualifying the infrastructure used by digital platforms as essential, as has been authoritatively supported98 (as well as, in the future, DLTs or blockchains) to force their opening with non-discriminatory conditions and reasonable prices, appears to be a complex operation, since it requires (in Europe, from Bronner onwards),99 in addition to the evidence of dominance on the upstream and downstream markets, the proof of the essentiality of the infrastructure and therefore of the absence of alternative platforms or, at least, the proof that the platform constitutes a bottleneck because it holds a product or service that it does not sell (IMS Health).100

Finally, it appears objectively difficult to impose data sharing (another authoritative proposal101) because the data are only partially relevant – it is the ability to process them that is crucial. Data processing leads to the algorithm

---

96 The German legislator has listed five criteria for determining dominance in multiverse or networked markets: direct and indirect network effects; parallel use of multiple services costs of migrating from one to another (the so-called multi-homing); economies of scale in relation to network effects; access to competitively sensitive data; pressure exerted by innovation on competition (Neuntes Gesetz sur Anderung des Gesetzes gegen Wettbewerbsbeschrankungen, 2017, chapter 2, para. 18.3a).

97 Difficulties made evident by the Commission’s investigation, European Commission, Case AT.39740, Google Search (Shopping), 27 June 2017, p. 67.


99 According to Bronner, refusal to deal can violate Article 102 TFEU under the three exceptional circumstances that the refusal concerns an indispensable input; that no objective justification excusing such refusal exists; and that the refusal eliminates competition downstream. See among others: R. Nazzini (2011), The Foundations of European Union Competition Law. The Objective and Principles of Article 102, Oxford University Press, 262 ff.; J. Temple Lang (2000), The principle of essential facilities in European Community competition law. The position since Bronner, Journal of Network Industries, 1, 375–405.

100 The IMS Health judgment specifies that where the refusal relates to access to intangible property protected by IP rights it must show the ability to prevent the emergence of new product(s) for which there is consumer demand. See: N. Dunne (2020), Dispensing with indispensability, Journal of Competition Law & Economics, 16(1), 77.

and transparency operates within certain limits (constrained by industrial property rights) and is also ineffective, since what is relevant is the ability to generate data. This is also a dead end.

Hence, there are sanctions for abuses but they remain marginal. In the Google Search case, the Commission found classic abuses by discrimination (leverage and tying), similar to those that Microsoft had faced a decade earlier and always connected to the browser. 102 No different are the abuses claimed by the Commission against Qualcomm to guarantee the exclusivity of chips on Apple products, 103 against Apple, which rejected a version of Spotify IOS in favour of an Apple Music one, 104 or against Amazon, which imposed on publishers contracts with a most favourable treatment clause, which allowed Amazon to control the market, 105 to the point of forcing the counterparties to the paradox of a defensive agreement, itself sanctioned because it was anti-competitive. 106

However, the real moves on the market remained outside the scope of the Commission’s intervention, relating for example to proprietary APIs (application programming interfaces) which make the migration of advertisers between platforms sticky if not impossible, and it is a paradox, if even the American Federal Trade Commission (FTC) intervened on the point. 107 This tells a lot about the difficulty of struggling in retrospect against the walled garden, the hortus conclusus enclosed by proprietary terminals and platforms.

Nor can the protection of personal data become a discriminating criterion, for abuses and concentrations, despite the attempt by the German

102 Namely, the abuses would consist in having forced manufacturers to pre-install the Google Search application and its browsing application (Chrome) as a condition for granting the licence relating to the Google application sales portal (Play Store); in having paid some large manufacturers and mobile network operators to pre-install the Google Search application on their devices exclusively; and in preventing manufacturers who wanted to pre-install Google applications from selling even a single smart mobile device running on alternative versions of Android not approved by Google (Android forks). For comments, on both sides, about the correctness of the analysis, see: M. Granieri, V. Falce (2016), La search neutrality tra regolazione e abuso di posizione dominante, Mercato Concorrenza Regole, 2, 305–306; S. Mannoni, G. Stazi, (2018), Is Competition a Click Away?, Editoriale Scientifica, 37 ff.
106 Case COMP/AT.39847 E-Books.
Bundeskartellamt, which has taken it as one of the parameters of abuse.\textsuperscript{108} There is no damage and, in this case too, there are no tests (quantitative parameters, output and price). If the value of the data is not scientifically defined and the price in monetary terms is zero, the tools developed by the practice so far and the jurisprudence produced by the Court of Justice and the national courts can build the perimeter walls but fail to protect, for the roof is uncovered.\textsuperscript{109}

Unless the system is modernized, its inadequacy emerges even more clearly when measured in relation to the blockchain. This technology decentralizes consensus and facilitates exchanges and, by distributing information, tends to eliminate asymmetry and reduce access barriers, supporting competition. This, however, in addition to raising relevant issues for the protection of personal data, makes the market extremely transparent to the nodes of the blockchain which, especially in private markets often constituted of important financial institutions, can be a small number, due to the high costs of node management and of the necessary authorization. The number of operators is limited, the market is transparent, the barriers are high: the perfect environment for tacit collusion. Measures that also prevent network nodes from accessing information that generates consent are difficult to imagine with current tools, if not a posteriori, in case of abuse; a priori, preventive measures may only apply in cases of mergers and acquisitions. European regulation, in this case, must help.

In conclusion, the \textit{ex post} nature of the intervention by the competition authorities, which is by definition backward looking, and the power to impose only financial sanctions, are the structural and procedural limits of the Commission’s action. Hence the need, on the one hand, for greater coordination with regulation (with what until recently constituted vertical silos), and on the other hand, for a steady use of the ‘regulatory instruments’ typical of European competition law: behavioural and structural obligations that can be imposed not only in case of concentrations but also of abuses of dominant position.

3.2 Mergers and Acquisitions

As for the rules on concentration, the 2007 Google/Double Click case (concentration in the search engine market) was a mistake by the European


\textsuperscript{109} The irrelevance of privacy – but, one would argue today, not of data protection – has been clearly sanctioned by the Court of Justice in the \textit{Asneft-Equifax} judgment of 23 November 2006 (C-238/05): ‘since any questions relating to the confidential nature of personal data do not fall, as such, under competition law, they can be resolved on the basis of the relevant provisions on data protection’.
Commission, and even shared by the FTC. Similarly, the EU Commission did not consider the Microsoft/LinkedIn, Apple/Shazam and Facebook/WhatsApp mergers to be dangerous for competition.


11 Federal Trade Commission, 20 December 2007, Case 071-0170 – Google/Double Click. The main argument which led to the approval was the competitive pressure exerted on Google:

[A] number of Google’s competitors have at their disposal valuable stores of data not available to Google. For instance, Google’s most significant competitors in the ad intermediation market, Microsoft, Yahoo!, and Time Warner have access to their own unique data stores. These firms own popular search engines, and will have access to consumer information from their internal ad servers, ad intermediation services, other web properties, and software. The entry and expansion of these well-financed competitors has transformed the ad intermediation marketplace over the last six months. All of these firms are vertically integrated, and all appear to be well-positioned to compete vigorously against Google in this new marketplace. (pp. 12–13)

As to privacy-related concerns (DoubleClick possessed highly personalized datasets, specializing in targeted advertising), the FTC concluded that their assessment in the context of merger review was neither possible nor desirable: ‘not only does the Commission lack legal authority to require conditions to this merger that do not relate to antitrust, regulating the privacy requirements of just one company could itself pose a serious detriment to competition in this vast and rapidly evolving industry’ (p. 2). In her dissenting opinion, Commissioner Pamela Harbour feared that the transaction would have combined not only the two firms’ products and services, but also their vast troves of data about consumer behaviour on the internet. Thus, the transaction reflected an interplay between traditional competition and consumer protection issues. The FTC was uniquely situated to evaluate the implications of this kind of data merger, from a competition as well as a consumer protection perspective. Therefore, the FTC should have maximized its opportunity to do so, given that, following the transaction, the merged firm would have been capable of dominating the ‘Database of Intentions’ (p. 4). Absent intervention, she expected data foreclosure as a result of the merger (§ 359). See: D. Srinivasan (2020), Why Google dominates advertising markets. competition policy should lean on the principles of financial market regulation, Stanford Technology Law Review, 24(1), 55–175; P.J. Harbour, T.I. Koslov (2010), Section 2 in a Web 2.0 world: an expanded vision of relevant product markets, Antitrust Law Journal, 76(3), 769 ff.

12 Case COMP/M.8124, Microsoft/LinkedIn, 6 December 2016.


14 Case COMP/M.7217, Facebook/WhatsApp, 3 October 2014.
Yet, the one relating to concentrations is the only a priori intervention by competition authorities and allows up-to-date assessment of the market. It also allows the imposition of measures and the monitoring of compliance. In a market based on innovation, the acquisition of competitors who have developed the right idea or technology is one of the main tools of market control, in which the big corporations usually stumble.

Nevertheless, so far the concentration of data has not constituted a threat to competition, and this can be admitted for the 2008 case of Google/DoubleClick,115 less so for the acquisition of WhatsApp by Facebook (2014), authorized in the United States but also by the European Commission and without conditions.116 The errors in that decision, relating both to the relevant markets (online advertising, communications between users and social networking, but what about the data?) and to the existence of alternative (potential?) platforms emerged with evidence when, three years later (2017), the aggregation of the two databases led to minor consequences for Facebook (financial penalties imposed by the European Commission and national authorities).117

The proposed solutions, i.e. lower the threshold of the relevant turnover for notification, or parameterize it to the value of the transaction (as the German legislator imposed) fail to hit the mark, because they encounter the difficulty, on one hand, of identifying the relevant market data processing and management, which constitutes a secondary, indirect, slippery, hypothetical market,118 and on the other, of imposing the transparency of the algorithm that processes the data.119 Only in 2020 did the Commission impose behavioural conditions on Google in relation to an acquisition operation.120

115 Case COMP/M.4731, Google/DoubleClick.
116 Case COMP/M7217, Google/Facebook.
117 In Italy: AGCM, Provvedimento n. 26597, 11/5/2017, WhatsApp-Trasferimento dati a Facebook, with which the Competition Authority considered the imposition of the modification of the contractual conditions of WhatsApp as an aggressive practice, instrumental in consenting to the integration of the two platforms.
120 Case COMP/M9660 – Google/Fitbit. These obligations will clearly determine ‘how Google may use the data collected for advertising purposes’, ‘how interopera-
‘Killer acquisitions’ or ‘platform envelopment’ strategies, the balance between \textit{ex ante} and \textit{ex post} assessments, theories of ‘balance of harms’ and jurisdictional thresholds proved to be only partially effective, due also to the digital platforms’ strategy of purchasing small start-ups with initially low turnover but a quickly growing user base and a high future market potential (i.e., Facebook/Instagram and Google/Waze mergers originally escaped the Commission’s scrutiny). In all these cases, it is difficult to distinguish pro-competitive or neutral deals from anti-competitive ones. Old assumptions, such as efficiencies from vertical transactions, should be abandoned and new ones, such as the unlawfulness of a merger between dominant platforms and substantial competitors, or uniquely likely future competitors, should be implemented.

3.3 The Path towards the Modernization of Competition Law

Hence the need, alternatively or cumulatively, for a ‘modernization’ of competition rules and their integration with complementary \textit{ex ante} regulation. As for the first, both the market definition and the assessment of market dominance should change in order to address properly not only the multi-sided nature of digital platforms but also the transactions conducted in this market, which often do not involve the transfer of monetary consideration.\textsuperscript{121}

3.4 Competition and Regulation, and Regulatory Competition

As for the second need, symmetric or asymmetric \textit{ex ante} regulatory models are often invoked as complementary tools to address competition concerns and provide for competition \textit{for} the market, when competition \textit{in} the market is unachievable (due to market failure, customer inertia or abusive strategic

\textsuperscript{121} Above, note 74. The typical instruments of competition remain, but with a limited burden of proof for the Commission.
market behaviour). Again, the participatory design of remedies involves a co-regulatory pattern (ex ante guidelines) based on the regulatory circle.

The two European Commission regulation proposals of December 2020, the Digital Market Act (DMA) and the Digital Services Act (DSA), propose a combination of regulation and competition, ex ante and ex post intervention, entrusting both to the European Commission. The DMA and the DSA thus resolve in a pragmatic way an issue that dates back to the relationship between competition law and regulation and between their respective competent authorities.

The DMA accurately lists the criteria for identifying the gatekeepers, recipients of the rules of regulated competition (operating systems, platforms,

---

122 P. Alexiadis, A. de Streel (2020), Designing an EU intervention standard for digital platforms, EUI Working Papers RSCAS 2020/14, at p. 17; J. Crémer, Y. de Montjoye, H. Schweitzer (2019), *Competition Policy for the Digital Era*, European Commission; O. Lynskey (2017), Regulating ‘platform power’, LSE Law, Society and Economy Working Papers 1/2017. See also J.E. Cohen (2019), *Between Truth and Power*, Oxford University Press; Common Understanding of G7 Competition Authorities on ‘Competition and the Digital Economy’, June 2019. ARCEP, the French telecommunications authority, in Systemic digital platforms, December 2019, proposes a test of systemic digital platforms based on three main criteria: the existence of bottleneck power, a certain number of users in the EU, the existing integration of that firm into an ecosystem enabling leverage effects. The proposed 10th Amendment of the German competition law (new Section 19a(1) of the German Act against Restraints of Competition) introduces the concept of an undertaking of paramount significance, which would be determined on the basis of six criteria: a dominant position on one or more markets; financial strength or access to other resources; vertical integration and activities on otherwise related markets; access to data relevant for competition; importance of activities for third parties’ access to supply and sales markets; and related influence on third parties’ business activities.

123 The discussion was initially on the prevalence of competition over regulation, or vice versa. The theses are well known: from the US ‘supermandate’, for which the general discipline of competition prevailed over regulation, which in any case had to be interpreted in a manner consistent with the first (and, in case of conflict, yielded); to the thesis of regulation limited in time as it is functional to compensate for market asymmetries that regulation had to help eliminate; to the opposite thesis according to which regulation remained in every competition policy, as it was aimed at addressing the economic issues that competition leaves unresolved and the social problems that competition cannot solve. The failure of the theses that started from the assumption of incompatibility has shifted the debate on the methods of exercising control: ex ante and prognostic for regulation; ex post for competition. The implicit consequence was a diversity of purposes: the restoration of the violated legality for the first, the repression and punishment of the violation for the second. The refrain of ex ante – ex post, however rough (the nuances are lost in this kind of analysis, but they do not cease to exist) has long framed the debate.

clouds and search services) and put into three lists (black, grey, white\textsuperscript{124}) the actions that they must take to prevent investigations for abuse of dominant position, adding to this the abuse of economic dependence.\textsuperscript{125} The remedies plan is also improved in terms of penalties (up to 10\% of the turnover) and of the behavioural and structural measures (up to a typical US break-up) that the Commission can impose.

The DSA, on the other hand, qualifies the responsibility of digital platforms in terms of content, imposing the removal of illegal content (but only by recommendation of third parties) with responsibility in case of non-compliance, as well as protection of third-party content (traditional media) and transparency of system profiling to counter fake news.\textsuperscript{126}

3.5 The Intent to Monopolize, Reloaded

Overseas, the reforms under discussion are those of a regulatory authority with specific competence in digital matters, which could enforce remedies for antitrust violation, and a reform of antitrust law through a common law-like process or new legislation (through a general tightening).\textsuperscript{127} Furthermore, the assessment of an intent to monopolize led the US Department of Justice to sue

\textsuperscript{124} The black list indicates prohibited behaviours. The white list illustrates positive behaviours, such as data sharing. The grey list concerns the most sensitive measures for the activity of the platforms (for example, the interoperability of the systems), which can be negotiated, in advance, between undertakings and the Commission.

\textsuperscript{125} The abuse of economic dependence, adopted as a criterion by some member states, was opposed by the European Commission (under the Barroso Presidency: 2004–2009) and has now become instead a useful tool on a European level; another example of the virtuous functioning of the regulatory circle.


\textsuperscript{127} Stigler Center (2019), Committee for the Study of Digital Platforms – Market structure and Antitrust Subcommittee, Report, 1 July 2019, Chicago. According to this study new answers should be given to old questions, among others: how to assess consumer welfare in a two-sided market; how to assess potential competition from new or small firms or not-yet-identified future innovators and entrants; how to assess the quality-adjusted price paid for a good or service sold in a barter transaction with zero or close to zero monetary price. Again, ancient doctrines should be changed, such as: the circumstances under which a refusal to deal can be prohibited; the paradigm of predatory pricing law; the harms theories; the proof requirements imposed upon antitrust plaintiffs, etc. See also: J. Furman et al. (2019), Unlocking Digital Competition, Report of the Digital Competition Expert Panel, HM Treasury, 10 and 55; Stigler Center (2019), Digital Platforms, Markets and Democracy: A Path Forward, Conference, Chicago.
Google\textsuperscript{128} in October 2020; in December 2020, in an independent initiative, ten US states also sued Google, and the Federal Trade Commission sued Facebook.\textsuperscript{129} All these cases were initiated after a document of Congress at the end of the legislature (October 2020)\textsuperscript{130} identified paths and defined constraints and which, reasonably, the new administration will follow.

3.6 What Is Lacking

Again, however, as already seen on the level of regulation (above, section 2), something seems to be lacking. In this case, it is the notion of the ecosystem, which is also the basis of the economic definition of digital platform (above, section 1) and is consistent with a legal definition of order (see Chapter 3). As an ecosystem, independent from the others (other platforms, but also artificial intelligence), but in an increasingly strict relationship with them, the digital platform cannot be considered, in a traditional way, a company that operates in a market competing with other companies.

The ecosystem can include integrated services: the operating system, a marketplace for applications, a payment system, a cloud service, a range of smart home applications, online services (videos, emails, books, games, storage, maps, communications systems), some complementary, connected through private APIs.

\textsuperscript{128} US Department of Justice suit against Google LLC, of October 2020. The DoJ accused Google of illegally protecting its monopoly over search and search advertising, by locking up deals with giant partners like Apple and throttling competition through exclusive business contracts and agreements.

\textsuperscript{129} The Federal Trade Commission sued Facebook, alleging that the company is illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct. Following a lengthy investigation in cooperation with a coalition of attorneys general of 46 states, the District of Columbia, and Guam, the complaint alleges that Facebook has engaged in a systematic strategy – including its 2012 acquisition of up-and-coming rival Instagram, its 2014 acquisition of the mobile messaging app WhatsApp, and the imposition of anticompetitive conditions on software developers – to eliminate threats to its monopoly. According to the FTC, this course of conduct harms competition, leaves consumers with few choices for personal social networking, and deprives advertisers of the benefits of competition.

\textsuperscript{130} House Report, Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations – Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary, 2020. The subcommittee investigated the following markets: online search; online commerce; social networks and social media; mobile app stores; mobile operating systems; digital mapping; cloud computing; voice assistant; web browsers; digital advertising.
3.7 Digital Platform as a Market

As an independent ecosystem, each platform is a market. The combination of economies of scale and scope and indirect network effects allows digital platforms to aggregate and match massive amounts of users on both sides of the market, reaching a tipping point where, in the light of the winner-takes-all situation and of the existing barriers to entry, dislodging the Big Tech becomes very difficult. It is a common statement that, when such conditions are met, platforms: (i) become the market (competition for the market); (ii) constitute the point of access to that market (platforms as gatekeepers); (iii) contribute, at least de facto, to setting the rules for operating within that market (platforms as regulators). Platforms are often vertically integrated and, in addition to providing the intermediation service, offer products and/or services on the business side of the market. This dual role is quite insidious because it might lead to conflict of interest and to neutrality problems, broadly defined as ‘self-preferencing’.

---


133 I. Graef (2019), Differentiated treatment in platform-to-business relations: EU competition law and economic dependence, Yearbook of European Law, 448–499. A more sophisticated analysis separates ‘pure self-preferencing’, ‘pure secondary-line self-preferencing’ and hybrid self-preferencing. Pure self-preferencing occurs when a vertically integrated platform treats its affiliated services more favorably than non-affiliated services (e.g. the more prominent display of Google’s comparison shopping service in its general search results as compared to rival comparison shopping services). A secondary line self-preferencing occurs when a non-vertically integrated platform engages in differentiated treatment among non-affiliated services in a market in which it is not active itself (e.g. a hotel booking platform providing hotels that pay higher commission fees with a higher ranking). Finally, a hybrid self-preferencing occurs when a platform engages in differentiated treatment among non-affiliated services in an effort to favour its own business (e.g. a platform blocking an app that interferes with its ability to gain revenues through advertising would be an example).
3.8 From a Market to a System

Hence, according to EU competition case law, one should shift from the definition of the market to that of a ‘system’. In a ‘system’, primary and secondary markets are by definition strictly correlated, and the digital platform operator (as system operator) should guarantee a minimum set of rules or a certain level of competition in the markets of the system.

The issue is therefore to ensure that the rules of the market constituted by each platform (system) are, if not fully compatible, at least consistent with the rules that guarantee full competition, and that are different in the national orders in which the digital platforms operate: the comparison between US antitrust and European competition law is only the simplest one.

3.9 Digital Platforms’ Internal System/External Market

Once the problem has been identified, the analysis plan is twofold, internal and external. The one internal to the platform (as a system), and of which whoever manages and regulates it must ensure the consistency with the general principles of competition, and the external one, of the relationship between platforms, which must compete with each other in a way that is not only consistent with, but in compliance with competition law – including the new regulated competition – applicable in the countries in which they operate.

3.10 Current Practice and System Framework Mismatch

The misalignment between practice, case law, and reality consistent with the theoretical reconstruction elaborated here, is thus evident. As for the internal plan, of the platform as a market in itself (as a system), the European Commission has so far investigated trying to apply multiverse market case law and jurisprudence on exclusionary and exploitative abuses in ‘innovation markets’, looking also at conglomerate effects (and related theories of harm).

---

135 A proposal, related to the introduction of an EU Market Investigation Regime (P. Marsden, R. Podszen (2020), Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement, Konrad-Adenauer-Stiftung) provides for the following remedies applicable to digital platforms: interoperability; data portability; access to data; open APIs; transparency regarding nodes or algorithmic patterns; prohibition of certain dark patterns; standards for consumer choice; code of conduct for the use of default menus or drop-down menus; ranking parameters; digital sandboxes for innovative activities; opening up of public sector information.
imposing, with little success, compliance with – and not mere consistency with – competition law. As for the external level of the relationship between platforms, in which this compliance should instead be imposed (as well as interoperability between platforms, via APIs, protocols, standards, data), the Commission has not yet investigated.

The ‘regulated competition’ pictured with the DMA and the DSA offers a limited evolution and a partial solution in this regard. The DMA proposes a regulation in support of the instruments of competition, and the DSA reinforces the autonomous regulatory constraints (not functional to competition). Both, however, refer – in equal measure and with the same force – to both the inner plane and the outer plane. But, as we have seen, the degree of coercion that can be imposed on digital platforms when they operate on the market (external level) and when they operate in their own system (internal level) is different.

An evolution that the DMA (especially) and the DSA could enable is to make the self-assessment tools of digital platforms more refined, to verify compliance with regulated competition. This is a relevant point for the autonomous development of the platform as a ‘system’ consistent with – not necessarily compliant with – the ‘external’ regulation. This solution highlights the ‘regulatory circle’, strengthens the self-assessment of platforms for compliance purposes, enhances the function of platforms as ecosystems (on an economic level) and – we shall see – of legal orders, on a legal level.

However, it is necessary to bring the rules back to the level of systems, and bring these into unity. I shall try to do that in Chapters 2, 3 and 4, to draw later in Chapter 5 the consequences of the conclusions.

4. DIGITAL PLATFORMS BETWEEN DATA ACCESS AND DATA PROTECTION

The protection of personal data in the digital environment is one of the most controversial and constantly evolving issues, on both a regulatory and judicial level. I do not claim to examine its relevant aspects here. In line with the approach I have proposed, I shall focus on seeking, on the one hand, if not a lowest common denominator, at least a line of consistency in the regulation, i.e. in the relationship between states and digital platforms, and, on the other, a continuity also in the gaps and in the errors (if any) occurring the regulatory approach.

Algorithm-based data management is the core business of digital platforms, their lowest common denominator and, at the same time, what differentiates them most from all other companies, for which data management is only one of the ways of developing business, an additional tool – and not even a necessary one until a few years ago.
4.1 Regulation and the Market

It is therefore not surprising that data protection has been one of the main battlegrounds between regulation and the market. The most advanced regulatory frontier is obviously the European Union, and the applicable discipline is the GDPR. The European regulation focuses on the fundamental rights of the individual: because incorrect data management might violate them, and because data are themselves considered fundamental rights, when personal. Hence the need to separate personal and non-personal data, subject to different rules: the former are protected, the latter are mostly not regulated. Therefore, the debate is still ongoing and based on the economic value of the data, and the possibility of granting monetary consideration (not only the supply of a service) to those who generate personal data (data subjects). A possibility that is denied, though, if we consider personal data as a fundamental right inalienable by the individual and subordinate only to a ‘more fundamental’ right; public health, for example, as the pandemic has shown.

The European regulation on personal data was initially opposed by digital platforms, to be then used at a later stage – especially by closed platforms – as a shield, not to share data. That was until the paradox, highlighted by the notification of exposure to Covid-19, of the agreement between Google (Android) and Apple which, through an interoperable software, allowed all mobile terminals to interface with each other to send notifications, managing data in a decentralized way, in full compliance with the constraints of the GDPR which, on the contrary, some European governments risked violating.

This demonstrates that while data protection rules affect the costs of providing a service, being burdened by the weight of rights, they can be used as any other lever on the market, for competitive purposes or for providing a more complete or higher-quality service, transforming the regulatory risk into an opportunity (see above, section 2).


137 The right to the protection of personal data is provided for by Article 8 of the Charter of Fundamental Rights, incorporated into the Treaties since 2009, with the relative competence attributed to the Union by Article 16 of the TFEU. This fundamental right is today a protection no longer of the private sphere but of the identity of the individual, as guaranteed by the Charter of Rights, a rule of primary European law. We have gone from the I-fortress to the I-controller.

138 Above, note 30.
4.2 From Ownership to Control

The lawfulness of data processing under the regulation in force (GDPR) is based on principles that, if correctly implemented, appear adequate for regulating the circulation of data and their processing by digital platforms. This is also due to the partial change of the proprietary vision of data (strictly connected to the protection of the personal dignity and identity) in favour of a guarantee, for data subjects (and indeed for any natural person), of having control over the data concerning them, regardless of and even before any acquisition and processing of data.

Hence the new centrality of consent and the functional remodelling of the rights of access, rectification, opposition, deletion (oblivion), restricted processing, data portability, the right to learn about the automated decision-making processes, including profiling, which can also be communicated by the data controller by means of standardized icons and applications, which should be submitted in advance to the national competent authorities and to the European Data Protection Board (EDPB) for preventive assessment.

4.3 Privacy by Design and by Default

Among the ex ante remedies, there are privacy by design and privacy by default. Through the first, the controller undertakes to set the parameters for data processing in the preparatory phase, in order to collect only the relevant data and only for the necessary period. With the second, the controller implements appropriate technical measures to ensure that, by default, only the personal data necessary for the specific purpose for which they are collected are processed, according to the principles of necessity and proportionality. Furthermore, the Data Protection Regulation governs the data subjects’ right to revoke consent and delete the data, the right to be forgotten, and the right to the pseudo-anonymization of data (and their not being re-identified): algorithms are the basis of digital identity, profiling, and self-determination of information, all connected to fundamental rights, the essential core of European welfare.

---

139 The European Data Protection Board is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). It contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU’s data protection authorities.
4.4 Data Protection Compliance

The Data Protection Regulation operates within the context of integrated risk management (Article 24 of the GDPR expressly deals with prevention) which is one of the focal points of the multisectoral regulatory perspective. The risks borne by the data controller – who is required to carry out a preventive and updated assessment consistent with a dynamic vision of protection – are different from those borne by the data subject. The latter is allowed to control not only his data but also the risks generated by their processing by the controller or controllers, within the algorithmic chain of digital circulation. Risks that affect, among other things, the freedom of choice. In this perspective, the data subject’s right (Article 22 of the GDPR) to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him, or affects him significantly, applies.140

The notion of personal data is extended to new cases, some of which are subject to enhanced protection (subject to prior notification to the national supervisory authority: i.e. biometric and genetic data, or health services): however, this list is not exhaustive and atypical cases are allowed. The quality of the data is then highlighted in the GDPR for the purposes of rectification and deletion – which extends to implying for the controller the obligation to advise all those to whom the data have been transferred during processing – but it will probably constitute one of most relevant issues, being a measure of the processing.

4.5 Protection and Free Movement of Personal Data

The intersection, evident in the ex ante remedies, between protection of personal data and competition is direct: the rules are two-sided. This is also why they seem so ponderous to US operators and regulators, accustomed to a market freedom limited only by the intent to monopolize. Therefore, the principle of accountability emerges as a cornerstone of the new European regulation, in the broad sense of the taking of responsibility (and risks) by the company, which is no longer required to notify the processing of data to the supervisory authority but to independently assess the risk (by means of a preventive impact assessment) and manage it. Such an approach based on risk assessment in advance implies a dynamic, and no longer static, data pro-

---

140 This has become standard enough to be a guideline for artificial intelligence as well.
tection. The transition from mere bureaucratic compliance to efficient data processing is the objective of the reform, which imposes a true obligation in terms of results and not of means.

Such a step is not dissimilar, mutatis mutandis, from the one taken in competition law for the notifications of concentrations, originally mandatory, and then entrusted to the undertaking’s autonomous assessment of the anti-competitive effects. Similarly, the European reform proposal (DMA) operates by listing areas of actions (black, grey, white) that undertakings can use as a parameter to evaluate (self-evaluate) in advance the legitimacy of their behaviours and actions on the market. The law of digital platforms starts from self-regulation.

### 4.6 Remedial Safeguard

A key role, as the necessary counterpart of accountability, is thus taken by remedial safeguard, which guarantees the compliance of self-regulation with the regulatory principles and with the approach – widely used in competition law and at the basis of privacy by design – of compatibility tests, aimed at allowing compliance with GDPR protocols (Articles 40–41) and already tested in vertical regulations. The new environment is also consistent with the new powers granted to national data protection supervisory authorities, who can now not only adopt sanctions but also impose behavioural or structural remedies.

### 4.7 Data Protection and Algorithms

It is difficult to assess the degree of applicability of the European regulation to the protection of personal data when it comes to the algorithm, one of the main tools used by digital platforms. The effectiveness of the protection will depend on the extension of the notion of personal data and on the application of the rules on data subject consent that will be established by national supervisory authorities and by national and European judges.

---


142 Above, note 46.
The ‘Charter of Digital Rights’ currently applicable in the EU guarantees to data subjects the right to: (i) get information relating to the processing of their data in a concise, transparent, intelligible and easily accessible form (Article 12); (ii) know how their personal data will be used and for how long they will be kept (Articles 13 and 14); (iii) access the personal data that are processed by the controller and by third parties (Article 15); (iv) rectify their personal data (Article 16) and obtain from the controller their deletion (Article 17); (v) restrict the processing when the accuracy of the personal data is challenged by the data subjects, the processing is unlawful, or the controller no longer needs the personal data for the purposes of the processing (Article 18); (vi) rectify or delete their personal data or restrict their processing, when the data subjects have objected to the processing (Article 19); (vii) receive the personal data concerning them provided to a controller, in a structured, commonly used and machine-readable form (Article 20); (viii) object to the processing (Article 21).

4.8 Rights and Principles

One should interpret and apply the data subjects’ rights in compliance with certain principles. The first consists of restricting the purpose of the processing of personal data, which prevents their secondary use if incompatible; each purpose requires a specific collection of data and the consequent consent from the data subject, so retaining data for future purposes is prohibited. This principle is functional to the circulation of high-quality data and is therefore aimed at providing a guarantee to both the data subjects (who have the right to verify and review the accuracy and quality of the data concerning them) and to the data controllers, who risk processing data that are flawed in their original form.

The second is the principle of data minimization, according to which the data processed must be adequate, relevant and limited.

The third is the right to data portability, whereby data subjects can transfer their data from one data controller to another. Individual identity is protected against the acquisition of information, which is an allowed activity, and the data subject’s consent operates as an authorization, a removal of the obstacle for the exercise of the activity. The data subject has therefore the right to object, even after having given consent, and that right is absolute when the data is processed for marketing or profiling purposes. Again, the enforcement of the rule requires guidelines to be issued by the national supervisory authorities, and market standards.
4.9 Data Protection and Blockchain

The Data Protection Regulation appears scarcely compatible with blockchain technology, for the latter shows a disruptive function and represents a qualitative break with the past (market) and the present (regulatory) systems.

The Data Protection Regulation seems to be only partially compatible with the blockchain, which: (i) discloses the participants’ personal data (starting from the public key) to each node in the chain (regardless of the reason for which they were collated), (ii) does not allow deletion or modification, (iii) does not provide for centralized control (nor for a Data Protection Officer) and (iv) is based on a fully automated procedure of data management processes.\(^\text{143}\)

The definitions of data subject, data controller and processor are not applicable in either a permissioned or permissionless blockchain. The nodes of the chain may be considered as controllers in a permissioned blockchain, while it is difficult not to consider them as mere processors in a permissionless chain, in which the prohibitive costs of the operations required to identify the participants are such as to restrict the group of controllers. The purpose of using the blockchain also affects the qualifications as data subject and controller, as the purpose of an investor is different from that of whoever merely concludes transactions. One should therefore find ways of applying the rules that allow their useful effect, for example through anonymization or pseudo-anonymization techniques consistent with GDPR constraints.

Furthermore, the centrality of informed consent, the main novelty of the GDPR, seems to yield in the face of practice, which already highlights a collection of personal information obtained through the analysis of reprocessed

data: restricting the purposes and minimizing the data looks like sandbags along the banks of a flooding river.

**4.10 Data Protection and Jurisdiction**

A potentially relevant aspect, not only for the protection of personal data but also for the law of digital platform ecosystems, is the qualification in the GDPR of the right of establishment for the purposes of attributing the responsibility for data processing. The competence (of the supervisory authorities) and the jurisdiction (of the European courts) are based on the establishment of the company in the EU, both the place (EU or extra-EU) of the processing and the nationality of the data controller being irrelevant, provided that (this is the objective limit of application) the processing relates to the offer of goods, or the provision of services, or the monitoring of behaviour (the so-called targeting principle, already elaborated by the EU Court of Justice in the *Google Spain* and *Schrems I* and *II* judgments). No extraterritorial claim to the rule, therefore; only the application of the general principles of the EU, modernized.

But the GDPR goes so far as to apply the principle of jurisdiction of the country of destination of the service and therefore of the data subject, even in the absence of any payment for the service. A correct application of this principle would allow the establishing of a compliant practice of the main operators

---

and the overcoming of the competition between legal systems that is inherent in the right of establishment, which risks attributing competence and entrenching jurisdiction over these issues to the Irish supervisory authority and judges, respectively, entrusting harmonization to the collaboration among national supervisors and, ultimately, to the Court of Justice of the European Union.

The lack of approval, at present, of the e-privacy regulation proposal also prevents the principle from being applied (at a subjective level) to the manufacturers of devices (smartphones, PCs, etc.) and – on an objective level – to metadata; however, it is probable that, as for the latter, the broad notion of personal data will allow an extension of protection to metadata.

4.11 Data Circulation and Regulatory Circle

In the digital environment, personal data deserve protection, their anonymization must be implemented at every stage, their portability becomes a decisive competitive tool but is based on the data subjects’ right to consent (revocable), which is not a hindrance but a guarantee. Personal data must circulate but are also a fundamental right, and protection cannot be compressed by a legitimate interest in the processing. This is a part of the European welfare that the Union shares with extra-EU countries in an inclusive way.

When it comes to data protection, the regulatory approach is uniform, as regards both the internal and external action of digital platforms. It is always the data subject’s consent that is the pivot around which the use of the data by the platform (internal level) and the transmissibility of the data to other subjects (external level) rotate.

The role of national supervisory authorities is decisive for a correct and effective digital circulation of the data. Not only in terms of sanctions (now the authorities’ powers of investigation and sanction are expanded), but also in terms of prevention, because the national authorities can assess the techniques and conditions of the controllers’ data processing and launch guidelines, approve standards, give opinions, fostering or endorsing codes of conduct or certification tools. They will probably also differentiate the compliance requirements related to the platforms’ internal activity from those relating to their external activity.

The reforms, implemented through directly applicable European regulations, reduce the autonomy of the member states. To comply with the revolutionary speed of the markets is then up to the national supervisory authorities, which decide on the changing balances between use and reuse, protection and freedom, in ascending and descending subsidiary links with the European authority, the European Protection Board.
4.12 Data Protection and the Digital Platform Ecosystem

The protection of personal data has clear limits, both in terms of territoriality (as highlighted by the two Schrems judgments of the Court of Justice), and of keeping pace with the technological evolution: we have already seen how the rules, when not embedded in technology, risk being poorly effective or, at worst, illusory (section 2).

As for the first limit, geo-blocking tools make it possible to adapt compliance to the legal patchwork in which the digital platforms operate; but they can do little when the data are transferred from one regulatory area to another.

As for the second limit, technology allows the use of forever new and refined tools, functional to the achievement of new and changing objectives, and/or created to circumvent a particular regulation.

When efficient, regulations (see section 2) go at linear speed, while technology runs at exponential speed. The consequence is that the platforms develop an internal law of their own that provides users with other protections than those granted by the public national regulation. Sometimes, after scandals (Facebook and Cambridge Analytica) or disruptive events (the pandemic), a true ‘competition between ecosystems’ arises which, at the end of this book, we shall qualify as a ‘relationship between legal orders’.

5. DIGITAL PLATFORMS AND DEMOCRACY

If we apply the outline and principles that are beginning to take shape in relation to all aspects of the organization and activity of digital platforms and their impact on democratic principles, the topic must also be divided into two different lines of research.145

---

The first concerns the internal part, the ecosystem of the platform, closed or partially open depending on the type, qualified according to the proposed taxonomy. This topic is generally approached in terms of freedom of speech, and of how the platforms respect rules and principles which, to date, are not mandatory, even if based on different rules, on both sides of the Atlantic.

The second concerns the external part, the relationship between platforms, and between these and the national legal systems. The theme has very broad contents and boundaries. As I have already made clear, I shall limit myself here to highlighting the relevant aspects for the purposes of our investigation. I shall look closer at the two profiles on the legal level in Chapters 2 and 3 with reference to the relationship between legal systems and (in Chapter 4) to legal subjectivity.

5.1 Digital Platforms and Democracy: The Internal Face

The first issue, relating to the impact of digital platforms on the democratic structure within the platforms, does not arise in abstract terms: digital platforms are private ecosystems, hierarchically organized and not subject to democratic principles. Nevertheless, the evolution of the platforms highlights their progressive implementation of principles typical of public law, from the rule of law to the separation of powers (see Chapter 2, section 3) to strengthen their accountability.146 The issue that various authors – mainly American – have investigated, becomes therefore that of public laws enacted and enforced by private lawmakers, which undermines fundamental constitutional principles such as the ‘state action doctrine’ and the separation of powers, as well as the ‘no-delegation doctrine’, based on the distinction between private and governmental functions and on the limits of congressional power to delegate its legislative power directly to the private sector, for private actors are not sufficiently bound by constitutional principles of accountability, transparency and legitimacy and may not adequately represent the public interest.147
This freedom is now partially limited in the United States by a Presidential Executive Order,\(^\text{148}\) and challenged by legislative proposals, both in the United States and in the European Union,\(^\text{149}\) which point out that when the platforms’ activity (i.e. content moderation) is pursued through a system of artificial intelligence, public/private classifications largely lose their distinctive power.

In terms of their ‘internal’ law (platform law), digital platforms apply international law rather than domestic law – meaning the law of the place where the community member has registered. So it happens, for example, with regard to the protection of human rights, and also in relation to freedom of expression.\(^\text{150}\)

### 5.2 Digital Platforms and Democratic States: The External Face

As for the second issue, which concerns the external part (relationships between platforms and between platforms and states), while digital platforms are impermeable to obligations imposed from the outside, they can, however, accept them, to an extent that depends on many factors, the first of which is certainly the degree of sharing of the rules. And therefore, what can be achieved through co-regulation (and this is the direction chosen by the European Commission) is, for example, with reference to the principle of a rule of law, to require online platforms to work with independent, certified dispute settlement bodies where users can lodge complaints when they believe their contents have been wrongfully removed. Users should go through the

---

\(^\text{148}\) Executive Order No. 13925, Preventing Online Censorship, 85 Fed. Reg. 34079 (28 May 2020). The order instructs several federal agencies to take actions that threaten to limit the legal immunity of platforms for user-generated content and jeopardize the economic strength of platforms.

\(^\text{149}\) I am referring to the proposals to reform Section 230 of the Communications Decency Act, which grants internet platforms legal immunity for most of the content posted by their users in US, and to the Proposals for a Digital Services Act and for the Digital Markets Act in the EU.

\(^\text{150}\) The states’ regulatory power to change the digital platforms’ internal rules is limited. The transnational operation of digital platforms has moved them beyond traditional regulatory accountability, particularly where speech and content moderation are concerned (see Chapter 2, section 3).
Digital platforms: protagonists of the self-age

platforms’ internal complaint procedures before being entitled to call upon an independent dispute settlement body.¹⁵¹

Thus, as for the ‘external’ profile of the relations between platforms and between platforms and states, the impact is there and it is often associated with the influence of social media on election campaigns. This is what the European Commission said recently, affirming that the digital revolution has transformed democratic politics.¹⁵²

Yet, although this is the most obvious aspect, it is not the only one. However, economists and jurists often question what level of regulation would be the most apt to govern the way in which platforms operate, and which rules and principles they should follow within their own community, when these rules and principles would potentially affect the democratic life of state systems.¹⁵³ Recent examples have been provided by the use of social networks

¹⁵¹ The Digital Services Act provides for a mechanism similar to that of the ‘prior exhaustion of internal remedies’ (below, Chapter 3, section 1.3)

¹⁵² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Regions, on the European democracy action plan, COM(2020) 790 final, 3 December 2020. The Commission states that digital innovation gives political actors new opportunities to reach out to voters. It also brings new opportunities for civic engagement, making it easier for some groups – in particular young people – to access information and participate in public life and democratic debate. However, the rapid growth of online campaigning and online platforms has also opened up new vulnerabilities and made it more difficult to maintain the integrity of elections, ensure a free and plural media, and protect the democratic process from disinformation and other manipulation. Digitalization enabled new ways to finance political actors from uncontrolled sources, cyber-attacks can target critical electoral infrastructure, journalists face online harassment and hate speech, and false information and polarizing messages spread rapidly through social media, and also through coordinated disinformation campaigns. The impact of some of these steps is amplified by the use of opaque algorithms controlled by widely used communication platforms.

(Twitter, Facebook) by the President of the United States, Donald Trump, both during the 2020 election campaign and on 7 January 2021, before and during the attack on Capitol Hill. In the first case, the policies adopted by Twitter and Facebook differed, while in the second case – given the seriousness of the events – both platforms blocked the President’s account. The censorship in the second case was interpreted, by the parties involved, respectively as a limitation of a fundamental freedom (of expression) and as an intervention to safeguard public order and, ultimately, democracy. Hence the open debate about the opportunity to amend Section 230 of the Communication Decency Act of 1996, which guaranteed to digital platforms an exemption from editorial liability.

We have therefore seen, even in these recent cases, that the degree of pervasiveness and enforcement of state regulations is different with respect to the external activity of the platforms (in relation to other platforms and states) and their internal policy.

The question is evident in practice, and we shall deal with it on a juridical level in the following chapters (2, 3 and 4). A few clarifications, however, must be made at the outset.

The traditional dynamics that see industrial and intellectual property opposing (and prevailing over) competition, are now transformed into more complex dynamics between property (secrecy of the algorithm, directly proportional to its accuracy and precision) and democracy, and this time the former cannot prevail, since the values of the latter are constitutionally protected. The error in the assessment, however, lies in bringing the friction between the two rights back into a single ecosystem (for economists) or a single legal order (for jurists). As we have seen so far, the rules within the private system of platforms are one thing, while the effects that the relations within the platforms can produce externally, in state systems, for example, by influencing voting choices, are quite another.

---

154 In May 2020, as Twitter executives waded into a confrontation with President Trump, Facebook kept its head down. As a matter of fact, Twitter added a fact-check link to one of President Trump’s tweets criticizing mail-in voting. The company said the president violated rules regarding voter suppression. President Trump posted the same words on Facebook, which has similar rules around voter suppression. But Facebook didn’t do anything about it.

5.3 What Practice Is Teaching Us

For this reason, the mainly regulatory issues of algorithm transparency are, in my opinion, wrongly placed.¹⁵⁶ And so are, from another point of view, those of data access, which are also regulatory issues, but which have arisen recently and with precise arguments on a supranational level, of international law.¹⁵⁷

If we separate the internal from the external sphere, what state systems can impose on platforms concerns the effects that their behaviour and those of their members produce in state systems (external profile). States can therefore prescribe the achievement of certain objectives through the application of principles: accountability and transparency, among others. However, states cannot determine how these are to be achieved. In other words, they cannot affect digital platforms on the internal level in the same way and with the same force by which they are allowed to impose behaviours on the external level, in the platforms’ relations with other platforms and with states. The issue here is not so much the degree of extension of private autonomy, because the internal law of digital platforms escapes in many ways the legal system of the state that regulates it (or attempts to do so); partly due to the original choice of states not to regulate, partly due to the subsequent autonomy conquered by the platforms via technology (in which, as mentioned earlier, the rules are now embedded).

This requires, on the one hand, a new declination of the very notion of democracy and of the elements that constitute it – if we really want to apply this paradigm to the internal law of digital platforms – and, on the other, the creation of new tools, adequate to protect it, in terms of the internal law of platforms, of the (public and private) law of states, and finally of transnational and international law, as we shall see (Chapters 2, 3 and 4).


¹⁵⁷ E. Benvenisti (2018), Upholding democracy amid the challenges of new technology: what role for the law of global governance?, European Journal of International Law, 29, 76 et seq. The author points out that international law governs cyberspace, which becomes an accessible global commons. According to the author, ‘social networks and other internet service providers, such as Facebook and Google … invoking their private nature and their contractual relations with their users, expect to be exempted even from the discipline of domestic public law and envision a private cyber-space where they, and only they, make the rules’. The author argues that ‘it is entirely possible to argue that cyberspace is not only a private or domestic space but also simultaneously a global space and, hence, subject to international law’.
5.4 Digital Platforms, Fundamental Rights and the Rule of Law

Starting from 2020, the European Commission has set foot on this path, radically modifying the direction, previously followed, of a ‘stand alone’ development of the digital single market and its regulation, shifting the aim towards the relationship between digital technologies, fundamental rights and the rule of law. On the one hand, this entanglement explains the complexity; on the other, it allows the proposal for regulation of platform activity that is consistent with continental European welfare, as well as with the democracy protection tools that the European Union is adopting. This approach, consistent with the more comprehensive reform of digital regulation, provides for the intervention of national authorities and of the European Commission in terms of co-regulation, as opposed to the US model, which is still anchored to self-regulation. Co-regulation is consistent and compatible with the analysis that I have proposed, of a differentiated regulatory intervention with regard to the internal sphere of the platforms and to the external one.

Therefore, the relational plan of the relationship between digital platforms and state systems finds concrete application in the transition from a system of self-regulation to one of co-regulation, in which traditional cooperation between companies (market) and regulators, the prevailing instrument of European regulation in the last two decades, turns into a cooperation between legal systems (see Chapter 2).

Therefore, it is not only the platforms that have to evolve, paying greater attention to the effects of their activity ‘externally’, but state systems too, and these must do so in a way that is consistent with the protection of rights.

Such evolution is often misunderstood, and the cooperation between digital platforms and state systems is reduced to ethical principles, which involve aspects of the evolution of artificial intelligence. However, the two levels must be distinguished.

6. DIGITAL PLATFORMS, AI AND ETHICAL CONSTRAINTS

6.1 Ecosystems and their Intersection

Artificial intelligence (AI) constitutes an ecosystem in itself, which produces many applications and which is only partially used by the existing digital platforms; the intersection between the two systems produces a third ecosystem, not independent, but autonomous with respect to the two that generate it. This is the aspect of our interest here, since AI is relevant to the extent that it is used by digital platforms.
However, the ‘artificial intelligence’ ecosystem must be examined in itself first, and then in its interaction with the platforms and therefore in the subset it produces with them.

The topic is extremely broad and already investigated in the literature,\textsuperscript{158} but still unclear in its regulatory and also social developments. The intent here is to understand whether and to what extent the relationships between these ecosystems can take some legal significance; whether the approach I have proposed is consistent with the current evolution of a differentiation, in terms of regulations, between the internal and external law of the platforms, and finally, whether this internal law applies norms and principles of international law rather than domestic (national) law. Any positive outcome in this direction would strengthen the premises of the investigation which, in subsequent chapters, will move on to the topic of legal systems and legal subjectivity.

The goal is to understand not only which are the applicable rules but also which of these are ethical and which instead are legal norms that we can reduce to general principles.\textsuperscript{159} According to the mainstream, when it comes to

\begin{itemize}
  \item \textsuperscript{159} Article 5 of the European Parliament Resolution for a ‘Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies’ (2020/2012-INL), states as follows:

\begin{itemize}
  \item Ethical principles of artificial intelligence, robotics and related technologies
    \begin{itemize}
      \item Any artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in the Union in accordance with Union law and in full respect of human dignity, autonomy and safety and other fundamental rights set out in the Charter.
      \item Any processing of personal data carried out in the development, deployment and use of artificial intelligence, robotics and related technologies, including personal data derived from non-personal data and biometric data, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive 2002/58/EC.
    \end{itemize}
\end{itemize}
artificial intelligence, rules and regulations yield to ethical constraints. From a non-superficial examination, the reference to ethics, with the consequent renunciation of positive law, is perhaps unnecessary.

### 6.2 Regulatory Definitions for AI

Again, I propose to start from the definitions of AI, including the one on which the European regulatory perspective is based.

Niels J. Nilsson defined AI as ‘that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment’.\(^{160}\) AI can be also defined simply as a collection of technologies that combine data, algorithms and computing power.\(^{161}\)

The definition accepted by the European Commission is more precise:

> Artificial intelligence refers to systems that display intelligent behaviour by analysing their environment and taking actions — with some degree of autonomy — to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).\(^{162}\)

The Union and its Member States shall encourage research projects intended to provide solutions, based on artificial intelligence, robotics and related technologies, that seek to promote social inclusion, democracy, plurality, solidarity, fairness, equality and cooperation.

It seems clear that although the Article is titled ‘ethical principles’, it rather refers to compliance with legal rules. Likewise, Article 16 provides for the establishment of a ‘European Certificate of Ethical Compliance’.


\(^{162}\) European Commission (2018), Communication on AI for Europe, COM(2018) 237 final, p. 1. According to Article 3 of the 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, April 21 2021), “‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.”
Again, according to the High Level Expert Group of the European Commission, AI systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.\textsuperscript{163}

Various authors offer many other definitions of AI, and each captures relevant aspects of AI activity.\textsuperscript{164} Again, however, the definitions serve a primarily regulatory objective. They highlight the features (software or hardware) and the activities that AI can carry out, more or less autonomously, and also in relation to the relevance of machine learning in those activities. The European Commission’s attempt to bring AI back to a system is more ambitious: it intends to classify AI as an ecosystem in itself, and regulate it according to fundamental principles, compatible with those of the democratic systems of European Union member states, starting from the principle of the rule of law.

\textsuperscript{163} High Level Expert Group, A Definition of Artificial Intelligence, p. 8. When it comes to AI implementation, AI is already being massively used in a number of areas and can be broken down into many sub-domains and techniques. These include search and planning; knowledge representation and reasoning; machine learning, which has led to AI breakthroughs in fields such as search and product recommendation engines, speech recognition, fraud detection, image understanding, etc.; multi-agent systems; robotics; machine perception, including computer vision and natural language processing; and more: see A. Renda (2019), Artificial intelligence ethics, governance and policy challenges – Report of a CEPS Task Force Centre for European Policy Studies (CEPS), p. 14.

6.3 AI and Ethics: The Origin of a Misunderstanding

When we talk about AI and ethical rules, we often refer to the choices that machines have to make as a result of machine learning and the processing of algorithms for this purpose. The textbook case is the self-driving vehicle that must choose the lesser evil when it is impossible to avoid the death of one or more people, and the choice is reduced to which one (life or death decisions).165

In this perspective machines could be trained to be utilitarian (Bentham, Mill), and thus focus on the ultimate result of their action and the rationality of their behaviour. Alternatively, a deontology-focused approach (Kantian) would focus on the law, as well as on moral imperatives and actions that are considered to be ethical or unethical, regardless of the result. Conversely, virtue ethics166 (Aristotle) focus on motives and are relational rather than rational, in that they focus on following virtuous examples. Deontology and virtue ethics focus on individual decision-makers, while teleology considers all affected parties. None of these approaches provides uncontroversial, definitive ways to resolve conflicts.167 There are numerous lists of principles which, starting from the various approaches, are considered relevant for the purpose of solving the case.168

---


168 European Group on Science and New Technologies (2018), EGE statement on artificial intelligence, robotics and ‘autonomous’ systems; L. Floridi et al. (2018) compare the EGE statement with five other documents: the Asilomar AI principles; the Montréal Declaration for Responsible AI; the General Principles offered in the second version of the IEEE ‘Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems’; the five overarching principles for an AI code developed by the UK House of Lords (2018); and the Tenets of the Partnership on AI (2018). Already these documents lead to a total of 47 different principles, although with significant overlaps.

The European Parliament Resolution for a ‘Regulation on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies’ (2020/2012-INL) builds on the following principles: human-centric,
As fascinating as it is, the matter relating to the philosophical approach to algorithms – and to the lists of principles that follow from it – can, in my opinion, arise only at the end of a complex process that concerns the possibility, legitimacy, and enforcement of a verification (ex ante or ex post) of the algorithm, of its setting and of the degree of autonomy of machine learning which, based on the set algorithm, makes the choices. Yet, the process must differ according to the degree of danger, measured in relation to both industry area and activity.

6.4 AI Ethical Constraints and the Risk-Based Approach

The regulatory solutions to regulate AI in the EU are indeed those of a level of risk-based system of regulation that would go from no regulation for the most innocuous AI systems to a complete ban for the most dangerous ones. A risk-based approach ensures that the regulatory intervention is proportionate. However, it requires clear criteria for the differentiation between the various AI applications, in particular in relation to the question whether they are ‘high risk’ or not.

According to the European Commission, a given AI application should generally be considered high risk in the light of what is at stake, considering whether both its industry and its intended use involve significant risks. Again, the EU Commission is creating a ‘matrix’ with vertical silos (industries) and horizontal ones (intended use).

human-made and human-controlled artificial intelligence, robotics and related technologies; mandatory compliance assessment of high-risk artificial intelligence, robotics and related technologies; safety, transparency and accountability; safeguards and remedies against bias and discrimination; right to redress; social responsibility and gender equality in artificial intelligence, robotics and related technologies; environmentally sustainable artificial intelligence, robotics and related technologies; respect for privacy and limitations on the use of biometric recognition; good governance relating to artificial intelligence, robotics and related technologies, including the data used or produced by such technologies.

As for industries, health care, transport and energy are among the most sensitive ones in a longer list that should be gradually updated. As for high-risk AI applications, the requirements could consist of such key features as: training data;\textsuperscript{170} data and record-keeping;\textsuperscript{171} information to be provided;\textsuperscript{172} robustness and accuracy;\textsuperscript{173} human oversight;\textsuperscript{174} and specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.\textsuperscript{175}

\textsuperscript{170} Requirements aimed at providing reasonable assurances that: (i) the subsequent use of the products or services that the AI system enables is safe; (ii) it does not lead to outcomes entailing prohibited discrimination; (iii) privacy and personal data are adequately protected during the use of AI-enabled products and services.

\textsuperscript{171} The regulatory framework will prescribe that the following should be kept: accurate records regarding the dataset used to train and test the AI systems, including a description of the main characteristics and how the dataset was selected; in certain justified cases, the datasets themselves; documentation on the programming and training methodologies, processes and techniques used to build, test and validate the AI systems, including where relevant in respect of safety and avoiding biases that could lead to prohibited discrimination.

\textsuperscript{172} Firstly, clear information should be provided as to the AI system’s capabilities and limitations, in particular the purpose for which the systems are intended, the conditions under which they can be expected to function as intended, and the expected level of accuracy in achieving the specified purpose. Secondly, citizens should be clearly informed when they are interacting with an AI system and not a human being.

\textsuperscript{173} These requirements should ensure that: (i) the AI systems are robust and accurate, or at least correctly reflect their level of accuracy, during all life cycle phases; (ii) the outcomes are reproducible; (iii) AI systems can adequately deal with errors or inconsistencies during all life cycle phases; (iv) AI systems are resilient against both overt attacks and more subtle attempts to manipulate data or algorithms themselves; and (v) mitigating measures are taken in such cases.

\textsuperscript{174} The objective of trustworthy, ethical and human-centric AI can only be achieved by ensuring an appropriate involvement of human beings in relation to high-risk AI applications. Examples of human oversight manifestations are as follows: the output of the AI system does not become effective unless it has been previously reviewed and validated by a human (e.g. the rejection of an application for social security benefits may be decided only by a human); the output of the AI system becomes immediately effective, but human intervention is ensured afterwards (e.g. the rejection of an application for a credit card may be processed by an AI system, but human review must be possible afterwards); monitoring of the AI system while in operation and the ability to intervene in real time and deactivate (e.g. a stop button or procedure is available in a driverless car when a human determines that the car operation is not safe); in the design phase, by imposing operational constraints on the AI system (e.g. a driverless car shall stop operating in certain conditions of low visibility when sensors may become less reliable or shall maintain a certain distance in any given condition from the preceding vehicle).

\textsuperscript{175} The gathering and use of biometric data for remote identification purposes, for instance through the deployment of facial recognition in public places, carries specific
6.5 AI Risks and Liabilities

The European matrix is also useful to define, qualify and attribute liability for damages created by the use of AI.

The issue is that of AI responsibility and sustainability (social, environmental and now also by reallocating entitlements as close as possible to where value is generated). Generally, advocating responsibility implies acknowledging the potential risks of AI, and acting accordingly to mitigate them in the design, development and use of AI. Essentially, the idea of responsible AI stems from the acknowledgment of possible unintended consequences of AI development and use, acting on essential aspects of AI such as fairness, accountability, transparency and explicability.

The approach followed by the European Union – again, an example of the most advanced regulation, based on rules embedded in technology – is to extend the existing regulation on product responsibilities to artificial intelligence, updating it to specific needs. Such a regulatory evolution is consistent with the classic path of legislation, which advances by applying the rules that have proved effective to the new, and updating the old. But this is only partially useful when it comes to AI, as there are many cases in which it is difficult to attribute responsibility to a given AI system.

risks for fundamental rights. Hence, in accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards.


An update of the Directive is expected on certain aspects of it, such as the concepts of ‘defect’, ‘damage’, ‘product’ and ‘producer’. In this respect, key aspects will have to be clarified, including: (i) how to interpret damage predictability; (ii) how to construe the so-called ‘state-of-the-art’ liability exception; (iii) whether to include ‘as a service’ the use of AI within the scope of the Directive; and (iv) how to ensure that the definition of misuse of an AI product does not place too much risk on the side of the end users. On the other hand, the Machinery Directive sets general health and safety requirements for products, such as robots or 3D printers. Finally, the future EU liability regime will also have to be designed in combination with a suitable insurance framework.

This can happen due to any of the following scenarios: (i) a system causes given damage, but the specific contribution of AI to causing the damage is impossible to prove; (ii) an AI system does not incur any malfunction, but its interaction with human behaviour leads to damage; (iii) an interaction between two or more AI-enabled algorithms causes damage to third parties (e.g. the so-called ‘flash crashes’); (iv) the combination of two or more AI systems from different vendors in a single product leads to damage, where it is not easy to correctly distribute the liability between the system.
A path to identify a responsible entity for the damage caused by AI is linked to an ethical principle: the ‘human in the loop’ or the ‘human in control’ requirement should be replaced by a ‘human responsible’ requirement, to avoid imposing excessively burdensome obligations on AI developers, vendors and distributors in circumstances in which it is virtually impossible or useless to have a human in immediate control of the system, and at the same time guarantee that end users will be compensated for the damage caused and will therefore be more likely to accept and use the new systems.178

This approach to responsibility inevitably leads to the identification of a strict (not fault-based) liability regime. But questions still arise on whether such a regime would be absolute or relative; whether there would be one entity in the entire value chain that is primarily responsible vis-à-vis the end user; and whether there would be joint and several liability in case of joint participation in causing an accident.

Again, answers can differ depending on many elements. According to the ‘one-stop shop’ procedure, a single entity is responsible for consumer redress: the producer in the case of product liability, the vendor in the case of contractual guarantees in the sale of goods.179 The ‘one-stop shop’ allows the first responsible entity to sue other entities in the value chain to obtain redress.

Liability would be mitigated by the fact that end users have misused the product, or in any way taken insufficient care while using an AI-enabled system; coupling strict liability with contributory negligence can provide optimal incentives for both parties involved in a dangerous activity,180 pro-

---


180 M. Bashayreh, F.N. Sibai, A. Tabbara (2021), Artificial intelligence and legal liability: towards an international approach of proportional liability based on risk sharing, Information & Communications Technology Law, 30(2), 169–192; A. Renda
vided that consumers receive sufficient information and advice on how to handle a given AI product.

But in the case of a ‘flash crash’, or when damage is caused by the interaction between algorithms and the external environment, including other algorithms, it may be difficult to apportion liability among two or more entities.181 In these cases, the answer to the question ‘who is responsible, and for how much?’ depends on how AI is considered. Obviously, since AI is many things, the answer may differ depending on the type of AI. A few examples follow.

If the specific implementation of AI is considered as an extension of the human being, or a part thereof (as could occur in the case of augmented intelligence), then the liability rules applicable to humans would also apply to the AI system.182 Conversely, if AI is considered equivalent to an object, negligence can be presumed if one’s property causes harm to a third party.183 But where


no negligence is found on the part of the custodian, owner, or user, liability can be transferred to the manufacturer of the AI-enabled system. The alternative approach would be outright no-fault (strict) liability, which is construed by some authors also as a fault-based system, configuring a duty to exercise care in monitoring the objects under custody (*culpa in vigilando*).  

If a specific implementation of AI is used ‘as a service’, and causes damage, the question is whether the resulting responsibility should be of a contractual nature (i.e. provision of a service that does not conform to sufficient security requirements), which does not exonerate the purchasing party from liability towards the damaged parties, or of non-contractual nature (tort liability), which would then have to be extended to services.

If an AI system is considered to be similar to an animal (when it displays a certain degree of autonomy) it means that AI systems have no legal personhood, and that strict liability applies only in case of damage caused by dangerous AI.  

---


If AI is considered to be a ‘slave’, its master will be liable for any damage.\textsuperscript{187} If AI is considered to be an employee, it will be given legal personhood as well as the duty to exercise due care. Strict liability would still be attributed to their owners, but the AI system would be given legal personhood and could, in principle, be asked to compensate for the damage.\textsuperscript{188} Finally, AI systems (and robots in particular) might not be considered as employees but as outright legal persons, with no link to an ‘owner’ or developer.\textsuperscript{189}

Therefore, in the opinion of the European Commission, by operating in this direction, and considering the various possible applications of AI, the existing rules may apply from time to time, possibly ‘modernizing’ them to make them consistent with the evolution of AI. Therefore, those who believe that not AI itself but its applications should be subject to regulation, and that the existing

---


regulation allows for a solution to be found to all the possible questions regarding AI responsibility, would be right.

Therefore, if we take this approach to a systematic reconstruction, there would be no ‘AI ecosystem’, as AI would be nothing more than a tool, not an end, and least of all a ‘system’.

6.6 AI as a System and Liability

On the other hand, we can reconstruct the system if we adopt the presumptions that apply to cases in which, using the tools indicated above, it is not possible, in the specific case, to attribute responsibility to one or more operators in the value chain. In other words, we need a presumptive criterion of responsibility, be it objective or fault-based.

The approaches to these cases are many and divergent from each other. In the United States, the main one – due also to the numerous jurisprudential applications – is that of the ‘most efficient choice’ of the liability regime. According to this theory, the key criteria in designing an efficient liability regime are the identification of the ‘cheapest cost avoider’ (i.e. the entity that can avoid the emergence of system failures at the lowest cost); and/or the ‘superior insurer’ (i.e. the entity that can buy insurance most effectively and cheaply, thereby offering relief to the damaged party also due to voluntary or mandatory insurance – ‘deep pocket theory’).190

This paradigm distinguishes reciprocity and reasonableness of risk. If the risk is not reciprocal, the person who imposes it is liable for the damage (general principle of fairness). In that case, strict liability is justified.

Only partially different – and not opposed – is the European approach, which has developed (in its proposed regulation on AI) the principle of proximity of risk.

An assessment of law and economics in the US; and a legal assessment based on position responsibility in the European Union.191 Although starting


from different models, legal traditions, objectives and instruments, the US and European paths converge in the practice: in most cases they lead to univocal solutions.

6.7 AI Risks and the ‘Cloud Regulatory Jump’

We have seen that the solutions provided by researchers and legislators in the field of AI are in continuity with a past that needs to be modernized, and that, however, the diversity of approaches on the two sides of the Atlantic tends to reduce, if we qualify AI as a system.

In relation to another system contiguous to that of digital platforms, the European legislator was more courageous. Rather than applying the old to the new, adapting it, the European Commission proposed a ‘regulatory leap’, consistent with the technological discontinuity, certainly running the risk of directing the market, but not waiting for it to pass through evolution. I am referring to the cloud environment, in which the regulation anticipated the technological evolution from the current centralized cloud to a distributed one and then a decentralized one (edge), consistently supporting the industrial evolution of European companies that converges towards this outcome (above, section 2).

The direction traced for cloud regulation is that of a corpus of general rules indicating fundamental rights and general principles, and allowing specific applications that go well beyond vertical and horizontal ‘silos’ and depend on individual applications (above, section 2). A corpus that should be consistent and compatible with those of other ecosystems, starting with that of digital platforms and that of AI. Only in this way would the discipline applicable in the intersection between the ecosystems resolve (at least in abstract terms) conflicts, gaps and overlapping rules.

We would also have expected a similar regulatory ‘leap’ with reference to AI, based on a corpus of general rules and differentiated specific applications. This doesn’t seem to be the case at present, but could be the result of the dual path followed (regulatory in the EU versus jurisprudential in the United States).

This ‘system solution’ would find (at least) the following justifications. First of all, the current European regulation of product liability is not adequate for AI, in which the use of algorithms and machine learning produces a progressive fracture between manufacturer and end product which often goes beyond, if not the assumptions, at least the intentions of its creator. There is indeed an
inverse relationship between the degree of precision and accuracy of the AI and its explicability.

Secondly, when it comes to AI, the final product is so composite that it is particularly difficult to distinguish the responsibilities in the different phases of the chain, and also because in many of these it is not the man who intervenes, but the machine. The different forms of anthropocentrism of law, which put man at the centre on the level of responsibility (summarized in the principle of complementarity with humans – ‘human-centric AI’ – and which are resolved in the responsible human requirement) provide an instrument of useful interpretation, but which has not yet been transformed into norms.

Thirdly, product liability works in an extremely partial way when a service is connected to the product, as often happens in the IoT and, certainly, in digital platforms.

In relation to the object and tools of a specific regulation, in the event of a (desirable) ‘regulatory leap’, a subsidiary intervention by the European legislator and the regulators would be reasonable – and proportional – with respect to the contents of the contracts stipulated between the (numerous) parties involved in the production, distribution and use of products and services that make use of AI to some extent. Here, too, it is a question of applying the ‘regulatory circle’ and the subsidiarity relationship between public and private regulation (above, section 2), mainly to protect the user (intermediate or final).

Following this path, public rules should in any case attribute responsibility to one of the parties in the supply chain that produces, distributes, uses the algorithm and delivers the product based on AI, in the absence of a precise definition of responsibility in contractual relationships.

Such a provision would constitute an incentive for the clear definition in the contracts of the limits of liability of each ‘component of the chain’, and would be consistent with the multiplicity of jurisdictions involved in the contractual relationships typical of these systems. Furthermore, it would encourage a uniform law codification that would allow the reuniting of different typical contractual relationships under a shared contractual regime to a broader degree than the one relating to European Union law (see Chapter 5, section 3). Finally, and with reference to the use of AI in digital platforms, this solution would constitute an incentive for the harmonization of contracts, which represents the main engine for developing relations within the platform.

6.8 Intersection between AI and Digital Platforms

When the AI is used by digital platforms, an additional entry is added to the table of the original AI matrix (consisting of sectors – vertical silos – and applications – horizontal silos): that of the subjects. When digital platforms
qualified as gatekeepers (above, section 3) use AI, further constraints apply on a subjective basis.

The intersection between the two ecosystems (digital platforms and AI) therefore sees the application of both regulations, which must remain consistent in their overlap. This consistency is jeopardized if we consider the rules on AI which are of an ethical nature, rather than a legal nature. Even the ‘ethical principles’, the guidelines, the lists, can be traced back to general legal (often constitutional) principles, norms and rights. The connection with positive law is not the basis for abandoning an alleged contemporaneity, if this is confused with an autonomous *lex mercatoria* of platforms.

Furthermore, the consistency of the two ecosystems should be investigated, taking into account the difference between the internal and external faces of digital platforms, or at least differentiating the use of AI in the ecosystem of platforms and the effects that AI produces externally, in relation to domestic law, or to transnational or international law. It is up to digital platforms, in principle, to create an environment and a system compatible with the standards applicable to AI in state and regional or international organizations. But digital platforms cannot do the job of coordinating these rules, or making a synthesis of them. However, the issue needs to be further explored. I shall do so in Chapter 2.

7. DIGITAL PLATFORMS AND THE BLOCKCHAIN PATH

When the digital platform ecosystem meets the DLT ecosystem, the intersection between the two becomes a ‘strongbox’. Distributed ledger technology has several applications in fact, the blockchain being the most interesting and relevant for digital platforms. The blockchain is ‘closed’ by definition and makes the digital platform that uses it (whether closed or partially open) even more impermeable. This also applies to blockchain-specific applications, including cryptocurrencies and smart contracts. These two applications have a certain relevance for both the legal classification of digital platforms and the law applicable to them (Chapters 2, 3 and 4). It is therefore appropriate to provide an overview, albeit brief, as it is functional to this sole objective: to measure both its application by digital platforms and the effects produced, within the digital platform ecosystem and in the relationships between this and the other ecosystems or, as we shall better see in the following chapters, of the other legal orders.192

7.1 Blockchain

Distributed ledger technologies are commonly used and, among these, blockchains: private or public networks (permissioned and permissionless, respectively) made up of nodes (the servers of the participants) that contain blocks of information organized in a database. Each activity – a transaction, for example – is effective only if approved by all the blocks in the network, which therefore record and store it, automatically verifying (mining) its legitimacy and certifying its origin from an authorized subject (broadcast and consensus). Hence the characteristic of decentralization (the network does not have a centre and therefore a clearing house is not needed), security (it is not possible to trace the generating algorithms), transparency (the governance of the blockchain is shared and each exchange is visible from every node), immutability (of the data), confidentiality (the ‘wallet keys’ guarantee user pseudo-anonymization, a necessary counterpart to the transparency of the operations), reduction of costs (operational, transactional, counterparty). In a nutshell, the full implementation of the myth of control without government, of the efficiency of the self-regulated market, of legal certainty, of risk control.

All these advantages have been appreciated by the European Parliament which, however, after having listed them, highlighted their criticisms (scalability of control, volatility and uncertainty in the long term, technical limitations of the infrastructure, data confidentiality, absence of adequate governance structures which produces different consequences in the private blockchain, subject to the risk of control without accountability, and in the public one, where decentralization reduces the effectiveness of a reaction to a crisis). Many of these criticisms are a counterweight to the typical characteristics of DLT, and suggested a regulatory moratorium until a more mature stage of development, in compliance with the principle of proportionality and subject to an impact assessment.\textsuperscript{193}

\textsuperscript{193} The European Parliament Resolution of 26 May 2016 on virtual currencies (2016/2007(INI)), after pointing out (para. 18) that ‘key EU legislation, such as EMIR, CSDR, SFD, MiFID/MiFIR, UCITs and AIFMD, could provide a regulatory framework in line with the activities carried out, irrespective of the underlying technology, even as VCs and DLT-based applications expand into new markets and extend their activities’ observes, however, ‘that more tailor-made legislation might be needed’. Similarly, and more specifically on DLT, the European Parliament Resolution of 3 October 2018 on distributed ledger technologies and blockchain: building trust with disintermediation (2017/2772(RSP)) in which the Parliament also recalls the principle of neutrality, both technological and of business models. The inadequacy of the system appears evident if we look at the electronic signature systems and the double keys provided by the CAD system, not applicable in a permissionless blockchain (where authentication is subject only to the verification of the credentials and not also of the identity...
The market then acts alone and offers solutions to limit risks and strengthen trust: self-regulation, by applying tools created for other purposes and in other markets. A good example is trust service providers (TPS), who are subject to strong regulation in terms of long-term data retention, business continuity, compliance with high security standards, confidentiality of data and information; the TPS blockchain networks as trust-by-design platforms are an interesting entry point for future regulation. Another example, again from contiguous regulated markets: the repos (repurchase agreements) typical of overnight markets, in which smart contracts reduce – almost to zero – operational and counterparty risks, and to which the regulation on high frequency trading and therefore the Markets in Financial Instruments Directive II (MiFID II) might apply.

Apparently, the playing field on which to measure the resilience of blockchain technology will be that of financial transactions, both because it amplifies and enhances the advantages and opportunities offered by the blockchain but also because it highlights its limits (transparency versus confidentiality, for example), and because it brings out the contrast between a highly regulated sector – that of financial services – and another in which regulation is suspended. It is the classic Drake Passage, where the perfect storm rises, against which emergency regulations are trying to fight.

Born for financial transactions (i.e., electronic money), the blockchain pattern is applicable to all cases of traded assets, certified by public and shared registers, as they are based on distributed (or distributable) databases.

---

194 Trust service providers (TSP) are authorized pursuant to EU Regulation 910/2014-eIDAS and create, check and validate electronic signatures, digital certificates, digital archives, etc. The eIDAS regulation makes the authorization of TSPs subject to compliance with stringent conditions and requirements in the provision of services and high security standards, as well as internal audits for the prevention and management of risks, compliance with consumer protection regulations, with data security measures, etc.

195 Namely, Directive 2014/65/EU (MiFID II) governs, in Article 17, algorithmic trading, to which Regulatory Technical Standards (RTS) adopted by ESMA must apply. RTS can therefore modify the rules in the application, to make them flexible and consistent with market and technology changes.
The exchange is based on the token, a set of digital information over which a subject exercises the right of ownership, as it is registered on the blockchain and therefore transferable through a protocol.¹⁹⁶

On the other hand, there are the smart contracts, self-executing digital transactions that use decentralized cryptographic tools (the blockchain, of which they are one of the terminals) to guarantee their enforcement – clear and precise because there is no room for interpretation.¹⁹⁷ Hence the importance of semantics for the management of future payments, made by the tokens automatically upon the occurrence of conditions that the token itself monitors, or for standardized or periodic payments, or for the provision of services, or again, simply, as an asset itself, with its own specific value (the ownership of the information collected in the token). What distinguishes these contracts from others that also circulate in the digital environment (data-oriented or computable contracts) is

¹⁹⁶ There are various classifications: utility tokens are those that allow the use of services; asset-based are those that guarantee a future payment linked to a real asset; investment tokens are comparable to financial instruments as they are transferable, negotiable and standardized. Other tokens are mere virtual currencies (cryptocurrencies). Among the recent evolutions is the so-called token +, with associated Big Data, indivisible, and traceable in its history (chain of ownership). Obviously, different types of tokens match with different applicable disciplines, each with different rights and obligations.

Among the most used applications are, on the one hand, the multiple signature (multi-signature or multi-sig) which allows the completion of the transaction without transferring the availability of the asset (tangible or intangible) upon positive verification by a third party, acting almost like an internal arbitrator to the relationship.

that the digital code in smart contracts does not constitute a representation of the agreement: it is the agreement (the code is law).  

7.2 Smart Contracts

Currently, the objectivity of a smart contract, software programmable to automatically execute the coded functions when certain conditions occur, can be admitted on the level of execution, but not on that of the elaboration of the code that is executed, which is the result of a deterministic algorithm (identical results in identical conditions) but programmed and therefore never neutral. Hence the need for the immutability of the contractual data, the certification and reliability of the sources and methods of controlling behaviour. In short, all the guarantees that a blockchain can provide.
There are many other applications in contexts in which the role of the intermediary becomes superfluous, since the activity or transaction can be regulated directly by the parties who, by inserting the smart contract in a blockchain, overcome the distrust that limits the circulation of wealth.201

The instruments of competition law in Europe appear to be of little use in dealing with the phenomenon (above, section 3), but also the regulations in the various industry sectors seem (some indeed more than others) not very suitable to regulate this game change (section 2).

Smart contracts, included in the blockchain and therefore not only irrevocable but also able to automatically evolve the contractual relationship by regulating all the negotiations (and therefore also pre-contractual ones) and application phases,202 seem at first sight incompatible not only with the institutions of the civil codes of continental Europe (think of the requirements of form, effectiveness, binding nature, underwriting, etc.) but also with external regulatory instruments. Compliant with the case law of common law, these contracts provide for all possible developments and can prevent, even before

201 From the land register to copyright protection, to brand protection, to the management of original spare parts; from the Internet of Things to the traceability of the production and distribution chain (at the basis not only of food safety but also of the circular economy); from data retention to voting mechanisms and public affairs management; from insurance to trading platforms; from banking and financial markets to payment systems; from peer-to-peer (loans, energy exchange, etc.) to regulatory compliance; from logistics (identification of customers and suppliers) to the tracking of industrial chains; from health care (management of patient data shared by medical facilities) to public administration (to build digital identities, reduce tax evasion, fight crime, automate procurement processes by means of tenders, etc.).

We continue to refer to national markets, as the European strategy for a digital single market does not contain specific rules. Again, there is room to increase competition between the legal systems in the EU through regulation, or to transform it into a sustainable inclusive growth. After all, with more than 25 billion interconnected objects in 2020, smart contracts will allow these terminals to operate autonomously, share resources and information, and exchange data without the need for centralized management.

regulating, flaws that are eliminated at the root, together with the subjective and discretionary elements in the application of the contract (software is by definition trustless).

Therefore, being self-executing but also self-enforcing, smart contracts represent, each separately, a reproposal of that medieval ‘common law’, a unique ius mercatorum for all legal systems, outside and with no need for any legal system. Self-sufficient, as if it were a ‘private legal system’, it does not require rules other than those encoded in the software, nor a judicial review, or tools for resolving disputes, because non-compliance is simply impossible.203

Many tend to reduce the scope and impact of this possible innovation and believe, even on the basis of the first applications, that smart contracts are nothing more than tools to simplify and certify the formation of the agreement, strengthen its evidentiary effects, guaranteeing its execution within the framework of the codes. To regulate this new structure of the agreement, a similar supervisory procedure would therefore be sufficient.204

However, on closer inspection, the juridical categories slip and the legal institutes do not hold firm. The capacity of the parties does not matter. The blockchain does not verify the validity of a contract, but only that a transaction has taken place (not even that this constitutes execution of the contract). And how can consent be certified, when it is between two machines?205 And what is the meaning of consent, given that the distinction between the pre-contractual and contractual phases, both potentially integrated in smart contracts, disappears? And then, the flawed consent becomes irrelevant for the algorithm, which does not care about the intention and is not required to interpret.206 Even fulfilment is no longer part of the relationship of the algorithm, so non-fulfilment (by the parties, of course) becomes impossible. No breach exists any longer, except that of the integrity of the algorithmic code (hence the necessary protection and possibly insurance measures) or of the verification of the external data entered (off-chain events, the occurrence of which affects the relationship ascertained by third parties, the ‘oracle’ that the parties choose

---

203 M. Raskin (2017), The law and legality of smart contracts, Georgetown Law Technology Review, 1, 305.
together with the external databases from which the relevant information must be collected).

A bitter debate followed the DAO affair, about whether theft is legitimate when it constitutes correct execution of an algorithmic code.\textsuperscript{207} Furthermore, smart contracts no longer present the asymmetries that justify the protection of the weak party (i.e., the consumer), guarantees that the proponent will eventually be able to use as a competitive asset, and here the role of the regulatory authorities can be relevant. And what about the cause of the contract, which is irrelevant and has no lawfulness of its own, if not inserted in a legal system that qualifies it? And finally, if the legal system cannot impose the execution of a smart contract (because there is no need for it, but even more so because the relationship goes beyond the legal system) one can seriously doubt that we are still faced with a contract.

It is therefore evident that the use of smart contracts by digital platforms, and within their ecosystem, constitutes a further step that distances them from the law of the states, which smart contracts can free themselves from almost completely, if the territorial constraint of jurisdiction is lost.

\section{Current Misunderstandings on Smart Contracts}

However, it is necessary to avoid a misunderstanding on which supporters and critics are currently clashing: smart contracts do not find universal application, since their characteristics allow the overcoming of the problems inherent in many contractual relationships (e.g. international trade, financial markets, insurances, etc.), but their rigidity advises against their use in many others, where flexibility and even efficient violation are a primary requirement. Smart contracts therefore do not revolutionize contract law and do not replace it.

Instead, we can imagine a regulation of smart contracts based on those shared rules that constitute the lowest common denominator (a rule of law).\footnote{In 2016, a system bug allowed one or more subjects to subtract 50 million from the total of 160 million US dollars that the DAO had raised via crowdfunding. The action was not prohibited by the algorithmic code and the debate among lenders who participated in the crowdfunding campaign focused on how to qualify the act (lawful or illegal) and therefore on what actions to take. The issue ended with the classic child split in half: in the absence of an agreement, the code was modified and the participants who updated their system obtained the return of their funds, which in the meantime had been frozen, while those who considered making the principle prevail (the code is law) maintained the old code (both are still in force today). See, among others: A. J Kolber (2018), Not-so-smart blockchain contracts and artificial responsibility, Stanford Technology Law Review, 21, 198; B. Carron, V. Botteron (2019), How smart can a contract be?, in Daniel Kraus et al. (eds), Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law, Edward Elgar Publishing, 101.}
elaborated by international organizations or institutions that deal with contractual harmonization (UNCITRAL and UNIDROIT above all). It is public law that affects smart contracts, not private law (the *lex cryptographia*, a new *lex mercatoria* also authoritatively envisaged, being still utopic); however, we have already said that such distinction is useless, now that the two are communicating vessels.

Hence the urgency of further research on the compatibility and coherence of the regulation of the markets, with vertical silos not communicating with each other, with the technological revolution that integrates the markets and does not care about the regulation, because, if it is applied at all, it is only on the terms accepted by the parties. It is no longer a question of defining the boundary between regulated and non-regulated activities, or of regulating their hybridization with classic tools (precedence, with a focus on the activity and not on the subjects); the issue is more radical and concerns the defence of the legal system, the survival of which depends – like everything in nature – on its necessity.

Now, given the speed of technological evolution, the wariness of international and European institutions, the still largely incomplete and partially inadequate nature of the rules governing digital negotiations, the progressive irrelevance of the member states, which have delegated the necessary competences to the European Union and are now almost completely disintermediated in the implementation phase that the EU has reserved to independent national authorities, either coordinated with each other or with the European agencies, or with the Commission as appropriate, it is clear that in the European Union a possible regulatory response can only come from the national regulatory authorities. With the typical instruments of vertical subsidiarity, national regulatory authorities will have to transform interventions on the markets into best practices, and then into benchmarks and into rules that become executive acts or legislative proposals of the European Commission approved by the Parliament and the Council (above, section 2). The ‘regulatory circle’ exists and works, and we shall soon see whether it is sufficient and adequate, since we know the limits of the evolution of regulation: it is linear, while technological growth, via the blockchain, appears exponential. Therefore, a ‘regulatory leap’ is needed, from the current field of comparison (the code is law) to a potential one (the law is code) and the intent of this research is to understand in which direction this should move.209

209 See P. De Filippi, A. Wright (2018), *Blockchain and the Law: The Rule of Code*, Harvard University Press. Some rules are beginning to be seen above all, at state level, in the USA. For a first list see: M. Dell’Erba (2018), Demystifying technology. Do smart
7.4 Artificial Responsibility

When the algorithm is elaborated or used within a DLT, in one of its implementation procedures (the blockchain with its applications: smart contracts, cryptocurrencies) the liability attribution mechanism does not differ from that illustrated in the previous paragraph on AI. The solutions are also the same, and lead to determining risk categories in relation to which instruments and responsibilities are ranked. This also governs the case in which the algorithm is processed by another algorithm, in an algorithmic chain that becomes independent from the initial programmer, to whom a causal link cannot be attributed. The system of algorithms processes the data, organizes them in various ways, uses them for a series of purposes, allows some developments and prevents others, according to an objectively abstract model, but which is actually functional to the goal it is intended to achieve, which is different each time.

The nuances are many and find numerous applications in the blockchain environment. Think of the advice of robot advisors, the progressive automation of the intellectual professions, crowdfunding (the case of the DAO is emblematic), alternative bonds, stock exchange contracts (futures, swaps, derivative transactions, if they govern cash flows), consumer contracts, cases in which the algorithm not only executes but decides (in home automation, automatic driving, etc.).

A further question arises for public blockchains, in which transparency and sharing would lead, in terms of responsibility, to the opposite short-circuit (collective co-responsibility of the participants), which is also unreasonable, even applying different jurisdictions to the nodes of the network.

It is therefore about separating and classifying, with the old methods of jurists, and looking for new solutions. What is visible (in nautical terms, the topsides of the web) is different from what remains unseen (the hull). For the first, the previously codified and traditional tools are valid and can still play an important role: transparency, information, consent, self-discipline, tools and practices for the prevention and management of risks, and through regulatory compliance, etc.

can one attempt to provide solutions, which can also go in the direction of creating an ‘artificial responsibility’, attributable to decentralized autonomous organizations (DAO) – open-source organizations consisting of a set of smart contracts that operate absent a central organization and, this is the issue, presently often without legal personality – to which the security of the infrastructure, of the data and values that pass through it (blockchain, smart contracts but also cryptocurrencies) is delegated.\(^\text{210}\) And here separation is again necessary, since a violation of public blockchains such as Bitcoin or Ethereum appears extremely complex, as their hacking requires – considering their development – a computational capacity that is currently unavailable, while a private blockchain (permissioned) is subject to greater risks, inversely proportional to its diffusion.

### 7.5 The Intersection between the Digital Platforms’ and the Blockchains’ Ecosystems

The intersection area between the two ecosystems of DLT and digital platforms, seems still completely unexplored, however.

If, on the one hand, the regulatory gap can be justified, due to the fact that the possible evolutions of technology have not yet had evident developments and have not yet consolidated, on the other hand the absence of specific research by experts and regulators raises more questions. Via DLT (smart contracts, cryptocurrencies) digital platforms can indeed close the environment hermetically (the ecosystem, for economists, the legal system, for jurists), in the case of closed platforms (social networks), or they can lock parts of them in watertight compartments, in the case of partially open platforms. It seems to me that, in this case too, the error – from which the current underestimation originates – lies in considering DLTs not for what they are (ecosystems) but as tools, worthy of attention only in relation to the goals that they achieve. Basically, the path started with ‘the code is law’ was not brought to its final conclusion, which is more than the mere slogan with which it was reclassified, and reveals a world behind it: that of the new matrix, which is replacing the regulatory matrix (section 2). This error, if placed in the right legal perspective, could prove to be fatal. We shall address these issues in Chapter 2, section 4.

8. CURRENT MISUNDERSTANDINGS ABOUT DIGITAL PLATFORMS

So far, we have examined some of the main issues usually raised in relation to digital platforms. Competition, regulation, data protection, impact on democratic principles, ethical rules, DLT and blockchain. We have seen the interconnection between the rules applicable to platforms and those of other ecosystems (those of AI, DLT and within it, the blockchain) and the need for these rules to be compatible with each other (interoperability, engineers would say), to make them consistent with the environment that is created at their intersection.

We have seen some misunderstandings that are slowing down the race in the necessary direction and sometimes diverting the path. Examples of those misunderstandings are: that the regulatory matrix is still existing and adequate, and that a few modernization adjustments are sufficient; that competition policy is still an adequate tool for those that are thought to be nothing more than multinational companies, and potential gatekeepers; that the protection of personal data is an adequate tool to guarantee data sovereignty; that it is possible (and sufficient) to impose specific governance rules on digital platforms to ensure that they will not interfere with the democratic processes of state systems; that public laws cannot fully regulate the evolution of AI and in that case, ethical rules and principles are necessary; and that the blockchain and its applications (smart contracts, cryptocurrencies) are subject to current, modernized regulation.

However, we have also seen that, in this overall perspective, the regulatory issues assume a different importance and can be looked at from a different perspective. The convergence of regulation, regulated competition, protection of personal data, defence of democratic principles and ethics becomes a tool and an end towards new regulatory developments.

As a matter of fact, if the internal side (the relations within the platform) and the external one (the relations between the platform and the other platforms and the states) are clearly distinct, as this research seems to highlight, the regulatory development should tend towards self-regulation of the platforms (private regulation), and forms of co-regulation (public regulation), differently scaled, as regards the internal and external sides. The intervention of public regulation should be allowed on a subsidiary basis, where self-regulation is inadequate, measured by the tools of compliance based on the outcome of preventive checks, according to the principles of subsidiarity and proportionality and to accountability rules.
This evolution is consistent with the notion of the platform ‘as a system’, according to the technical definitions given by economists, as well as jurists (even if limited, for the time being, to regulatory issues).

So far, we have investigated markets and regulation. The conclusions reached require further insight, in legal terms, on the level of internal law of the platforms and on the level of external law, relating to the relationships between platforms, state legal systems, transnational law, international law. This approach still seems to me not sufficiently investigated, or in any case not in a unified way. It is possible that this derives from an excessive compartmentalization of the law, which makes the approach to the issues that the platforms propose, which are evidently cross-disciplinary, too complex. It is also probable that the technological component constitutes a barrier, if its legal qualification is a topic that is placed on the level of the theory of legal systems.

Whatever the reasons for the gap, the aim of this research is to study these aspects further. I shall start from an overall vision, which requires bringing the analysis to the highest level of transnational law and international law, of legal subjectivity and of the relationship between legal systems. This is the direction towards which the traces we have found on the markets are leading, sometimes directly and sometimes as a reflection (and a consequence) of the regulators’ actions.